



Informatica® Multidomain MDM
10.4 HotFix 2

보안 가이드

Informatica Multidomain MDM 보안 가이드

10.4 HotFix 2

2020년12월

© 저작권 Informatica LLC 2001, 2021

이 소프트웨어와 설명서는 사용 및 공개에 대한 제한 사항이 포함되어 있는 별도의 사용권 계약에 따라서만 제공됩니다. 본 문서의 어떤 부분도 Informatica LLC의 사전 통지 없이 어떠한 형태나 수단(전자적, 사진 복사, 녹음 등)으로 복제되거나 전송될 수 없습니다.

미국 정부 권한. 미국 정부 고객에게 제공되는 프로그램, 소프트웨어, 데이터베이스, 관련 문서 및 기술 데이터는 해당하는 연방 입수 규정 및 기관별 보안 규정에 따라 "상용 컴퓨터 소프트웨어" 또는 "상용 기술 데이터"입니다. 따라서 사용, 복제, 공개, 수정 및 조정은 해당하는 정부 계약에 규정된 제한 사항 및 라이선스 조건을 따르며, 정부 계약 조건에 의해 적용 가능한 한도 내에서, FAR 52.227-19, 상용 소프트웨어 라이선스에 규정된 추가 권한이 적용됩니다.

Informatica 및 Informatica 로고는 미국과 전 세계 여러 관할 국가에서 Informatica LLC의 상표 또는 등록 상표입니다. Informatica 상표의 현재 목록은 <https://www.informatica.com/trademarks.html>에서 확인할 수 있습니다. 다른 회사 및 제품명은 해당 소유자의 상표 또는 등록 상표일 수 있습니다.

이 소프트웨어 및/또는 설명서의 일부에는 타사의 저작권이 적용될 수 있습니다. 필요한 타사 고지 사항은 제품에 포함되어 있습니다.

이 설명서의 정보는 예고 없이 변경될 수 있습니다. 이 문서에서 문제가 발견되는 경우 infa_documentation@informatica.com으로 보고해 주십시오.

Informatica 제품은 제품이 제공될 당시의 계약 조건에 따라 보증됩니다. Informatica는 상품성과 특정 목적에의 적합성에 대한 보증 그리고 비침해에 대한 보증 또는 조건을 포함하여 어떠한 종류의 명시적이거나 묵시적인 보증 없이 이 문서의 정보를 "있는 그대로" 제공합니다.

발행 날짜: 2021-01-14

목차

서문	7
Informatica 리소스	7
Informatica 네트워크	7
Informatica 기술 자료	7
Informatica 설명서	7
Informatica Product Availability Matrix	8
Informatica Velocity	8
Informatica Marketplace	8
Informatica 글로벌 고객 지원 센터	8
장 1: MDM Hub 보안 소개	9
MDM Hub 보안 개요	9
MDM Hub 콘솔	10
Dynamic Data Masking	10
보안 액세스 관리자	11
인증	11
권한 부여	12
보안 리소스 및 권한	12
역할	13
보안 구현 시나리오	13
내부 정책 결정 지점	14
외부 사용자 디렉터리	14
역할 기반의 중앙 집중식 정책 결정	15
종합적인 중앙 집중식 정책 결정	15
보안 시나리오를 위한 태스크 구성	16
기본 관리자 비활성화	16
장 2: 리소스	18
리소스 개요	18
보안 및 개인 리소스	19
리소스 그룹	19
리소스 그룹 계층	20
보안 리소스	20
보안 리소스 도구	20
보안 리소스 구성	20
MDM Hub 리소스의 상태 설정	20
리소스 필터링	21
리소스 그룹 구성	21
리소스 그룹 추가	21

리소스 그룹 편집 및 삭제.	22
리소스 목록 새로 고침.	22
기타 보안 변경 내용 새로 고침.	22
Data Director 비즈니스 항목 서비스에 대한 보안 구성.	23
비즈니스 항목 서비스를 보안 리소스로 구성.	23
비즈니스 항목 서비스에 역할 권한 할당.	23

장 3: 역할..... 24

역할 개요.	24
역할 구성.	24
역할 추가.	25
역할 편집 및 삭제.	25
권한.	25
내부 역할 및 외부 역할.	26
역할에 리소스 권한 할당.	26
다른 역할에 역할 할당.	27
역할에 대한 리소스 권한 보고서 생성.	27
생성된 보고서를 HTML 파일로 저장.	27

장 4: 사용자 및 사용자 그룹..... 28

사용자 및 사용자 그룹 개요.	28
사용자 구성.	28
MDM Hub 리소스에 대한 사용자 액세스.	29
사용자 계정 추가.	29
사용자 계정 편집 및 삭제.	30
보충 사용자 정보 편집.	30
사용자 계정의 암호 설정 변경.	31
연산 참조 저장소에 대한 사용자 액세스 권한 구성.	31
암호 정책 구성.	31
암호 정책 설정.	32
글로벌 암호 정책 관리.	32
개인 암호 정책 관리.	32
JDBC 데이터 소스 보안 구성.	33
보안 JDBC 데이터 소스에 대한 사용자 이름 및 암호.	33
Oracle SID 연결 유형에 대한 데이터베이스 ID.	33
Oracle 서비스 연결 유형에 대한 데이터베이스 ID.	34
IBM Db2 연결 유형에 대한 데이터베이스 ID.	34
Microsoft SQL Server 연결 유형에 대한 데이터베이스 ID.	34
마스터 데이터베이스의 데이터베이스 ID.	34
암호 암호화.	35
사용자 그룹 구성.	35
사용자 및 그룹 도구 시작.	35

사용자 그룹 추가.....	35
사용자 그룹 편집 및 삭제.....	36
사용자 그룹에 사용자 및 사용자 그룹 할당.....	36
현재 ORS 데이터베이스에 사용자 할당.....	36
역할과 사용자 및 사용자 그룹 간의 연결.....	37
역할에 사용자 및 사용자 그룹 할당.....	37
사용자 및 사용자 그룹에 역할 할당.....	37
장 5: 보안 공급자.....	38
보안 공급자 개요.....	38
보안 공급자 관리.....	38
공급자 파일 관리.....	39
공급자 파일 업로드.....	39
공급자 파일 삭제.....	40
보안 공급자 설정.....	40
보안 공급자 설정 변경.....	40
보안 공급자 활성화 및 비활성화.....	40
처리 순서에서 보안 공급자 이동.....	41
공급자 속성.....	41
공급자 속성 추가.....	42
공급자 속성 편집.....	42
사용자 지정 공급자.....	42
샘플 providers.properties 파일.....	43
외부 인증.....	43
로그인 모듈 추가.....	44
로그인 모듈 삭제.....	44
장 6: 응용 프로그램 수준 보안.....	45
응용 프로그램 수준 보안 개요.....	45
Informatica Data Director.....	46
프로비저닝 도구.....	47
ActiveVOS.....	47
Dynamic Data Masking.....	48
Dynamic Data Masking과 MDM Hub의 통합.....	48
MDM Hub에 대한 Dynamic Data Masking 모범 사례.....	48
연산 참조 저장소를 사용하도록 Dynamic Data Masking 설정.....	49
Linux에서 WebLogic T3S 채널 설정.....	50
WebSphere 응용 프로그램 서버에서 보안 Siperian 버스 활성화.....	51
보안 Siperian 버스에 대한 cmxserver.properties 구성.....	52
장 7: 인증서 기반 인증.....	53
인증서 기반 인증 개요.....	53

인증서 기반 인증 및 외부 클라이언트.....	53
트러스트된 응용 프로그램.....	54
외부 응용 프로그램을 트러스트된 응용 프로그램으로 추가.....	54
인증서 및 키 관리.....	54
보안 구성 유틸리티.....	55
장 8: 암호 해시.....	56
암호 해시 개요.....	56
암호 해시 옵션.....	57
사용자 지정 해시 알고리즘.....	57
암호 재설정 프로세스.....	57
보안 구성 유틸리티.....	58
문제 해결.....	58
부록 A: 용어.....	59
인덱스.....	63

서문

Multidomain MDM에서 보안을 활성화하는 방법을 알아보려면 Informatica® *Multidomain MDM 보안 가이드*를 사용하십시오. 보안 액세스 관리자를 사용하여 MDM Hub 리소스를 보호하고 Dynamic Data Masking을 사용하여 중요 데이터에 대한 액세스를 차단하는 방법을 이해할 수 있습니다. 사용자 및 그룹을 구성하는 방법과 사용 권한, 권한 및 역할을 사용하여 사용자 보안을 관리하는 방법에 대해서도 알아볼 수 있습니다.

이 가이드에서는 사용자가 운영 체제, 데이터베이스 환경 및 응용 프로그램 서버를 알고 있다고 가정합니다.

Informatica 리소스

Informatica는 Informatica Network 및 기타 온라인 포털을 통해 다양한 범위의 제품 리소스를 제공합니다. 리소스를 통해 Informatica 제품 및 솔루션을 최대한 활용하고 다른 Informatica 사용자 및 주제별 전문가로부터 배울 수 있습니다.

Informatica 네트워크

Informatica Network는 Informatica 기술 자료, Informatica 글로벌 고객 지원 센터 등 여러 리소스로 연결되는 관문입니다. Informatica Network를 시작하려면 <https://network.informatica.com>을 방문하십시오.

Informatica Network 멤버인 경우 다음 옵션이 가능합니다.

- 기술 자료에서 제품 리소스를 검색할 수 있습니다.
- 제품 사용 가능 여부에 대한 정보를 봅니다.
- 지원 사례를 생성하고 검토할 수 있습니다.
- 거주 지역의 Informatica 사용자 그룹 네트워크를 검색하고 동료와 협업 관계 유지

Informatica 기술 자료

Informatica 기술 자료를 사용하여 사용 방법 문서, 모범 사례, 비디오 자습서, 자주 묻는 질문에 대한 답변 등 제품 리소스를 확인할 수 있습니다.

기술 자료를 검색하려면 <https://search.informatica.com>을 방문하십시오. 기술 자료에 대한 질문, 의견 또는 아이디어가 있는 경우 KB_Feedback@informatica.com을 통해 Informatica 기술 자료 팀에 문의해 주시기 바랍니다.

Informatica 설명서

Informatica 설명서 포털에서 확장된 설명서 라이브러리를 탐색하여 현재 및 최근 제품 릴리스를 확인할 수 있습니다. 설명서 포털을 탐색하려면 <https://docs.informatica.com>을 방문하십시오.

제품 설명서에 대한 질문, 의견 또는 아이디어가 있는 경우 infa_documentation@informatica.com에서 Informatica 설명서 팀에 문의해 주시기 바랍니다.

Informatica Product Availability Matrix

PAM(Product Availability Matrix)은 제품 릴리스에서 지원하는 운영 체제 버전, 데이터베이스 및 데이터 소스 유형과 대상을 나타냅니다.

<https://network.informatica.com/community/informatica-network/product-availability-matrices>에서 Informatica PAM을 찾을 수 있습니다.

Informatica Velocity

Informatica Velocity는 수백 가지 데이터 관리 프로젝트의 실제 경험을 토대로 Informatica 전문 서비스업에서 개발한 팁과 모범 사례 모음입니다. Informatica Velocity는 전 세계의 조직과 협력하여 성공적인 데이터 관리 솔루션을 계획, 개발, 배포 및 유지 관리하는 Informatica 컨설턴트의 포괄적인 지식을 보여줍니다.

Informatica Velocity 리소스는 <http://velocity.informatica.com>에서 확인할 수 있습니다. Informatica Velocity에 대한 질문, 주석 또는 아이디어가 있으시면 Informatica 전문 서비스업(ips@informatica.com)에 문의하십시오.

Informatica Marketplace

Informatica Marketplace는 Informatica 구현을 확대 및 개선하기 위한 솔루션을 찾을 수 있는 포럼입니다.

Marketplace에서 Informatica 개발자와 파트너가 제공하는 수백 개의 솔루션을 활용하여 생산성을 향상시키고 프로젝트의 구현에 걸리는 시간을 줄일 수 있습니다. <https://marketplace.informatica.com>에서 Informatica Marketplace를 찾을 수 있습니다.

Informatica 글로벌 고객 지원 센터

전화 또는 Informatica Network를 통해 글로벌 지원 센터에 문의할 수 있습니다.

해당 지역의 Informatica 글로벌 고객 지원 전화 번호는 Informatica 웹 사이트 (<https://www.informatica.com/services-and-training/customer-success-services/contact-us.html>)를 방문하여 찾을 수 있습니다.

Informatica Network에서 온라인 지원 리소스를 찾으려면 <https://network.informatica.com>을 방문하고 eSupport 옵션을 선택하십시오.

제 1 장

MDM Hub 보안 소개

이 장에 포함된 항목:

- [MDM Hub 보안 개요 , 9](#)
- [MDM Hub 콘솔, 10](#)
- [Dynamic Data Masking , 10](#)
- [보안 액세스 관리자 , 11](#)
- [인증, 11](#)
- [권한 부여, 12](#)
- [보안 리소스 및 권한, 12](#)
- [역할, 13](#)
- [보안 구현 시나리오, 13](#)

MDM Hub 보안 개요

MDM Hub은 무단 액세스 및 변조로부터 데이터를 안전하게 지켜 개인 정보 및 데이터 무결성을 보호합니다.

Hub 콘솔의 보안 액세스 관리자를 사용하여 MDM Hub 리소스를 보호하고 사용자 인증 및 권한 부여를 비롯한 작업 보안 정책을 적용할 수 있습니다.

Dynamic Data Masking을 사용하여 중요한 정보에 대한 액세스를 차단할 수 있습니다. 예를 들어 Dynamic Data Masking을 사용하여 관리자 권한이 없는 모든 사용자가 신용 카드 번호를 보지 못하도록 숨길 수 있습니다.

여러 가지 방법으로 MDM Hub 구현에서 보안을 구성할 수 있습니다. 타사 보안 공급자를 사용하여 조직의 특정 보안 요소를 처리하거나 MDM Hub을 구성하여 보안의 모든 면을 관리할 수 있습니다. 서비스 통합 프레임워크 (SIF)를 사용한 보안 구성에 대한 자세한 내용은 *Multidomain MDM 서비스 통합 프레임워크 가이드*를 참조하십시오.

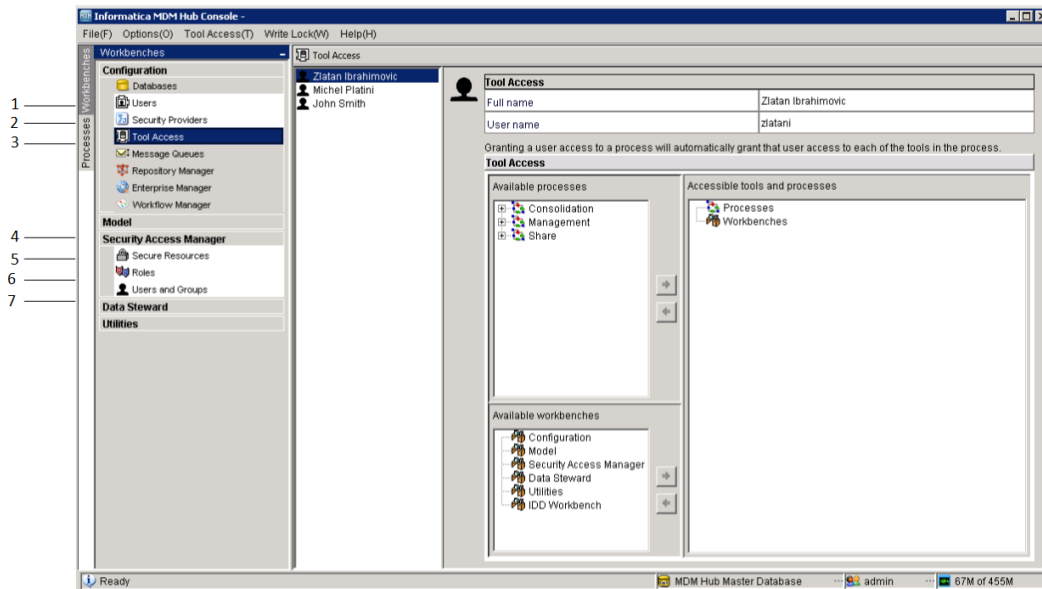
중요: Multidomain MDM 보안을 시작하기 전에 응용 프로그램 서버 및 캐싱 장치가 안전한지 확인하십시오.

MDM Hub 콘솔

Hub 콘솔을 사용하여 MDM Hub에서 보안을 구성합니다.

구성 작업 영역의 도구 액세스 도구를 사용하면 Hub 콘솔 도구에 대한 액세스 권한을 제어할 수 있습니다. 예를 들어 도구 액세스 도구를 사용하여 데이터 관리자 및 병합 관리자 도구를 제외한 모든 Hub 콘솔 도구에 대한 데이터 스튜어드의 액세스를 거부할 수 있습니다.

다음 이미지는 Hub 콘솔 인터페이스를 보여 줍니다.



1. 사용자 도구
2. 보안 공급자 도구
3. 도구 액세스 도구
4. 보안 액세스 관리자
5. 보안 리소스 도구
6. 역할 도구
7. 사용자 및 그룹 도구

Dynamic Data Masking

Informatica Dynamic Data Masking은 데이터 보안 제품으로서, 중요한 정보에 대한 무단 액세스를 방지하도록 클라이언트와 데이터베이스 사이에서 작동합니다. Dynamic Data Masking은 데이터베이스에 전송된 요청을 가로채서 이 요청이 다시 클라이언트에 전송되기 전에 데이터를 마스킹하도록 해당 요청에 데이터 마스킹 규칙을 적용합니다.

Dynamic Data Masking을 사용하여 MDM Hub에서 관리하는 프로덕션 및 비프로덕션 데이터베이스에 저장된 중요한 데이터에 대한 액세스를 마스킹하거나 방지할 수 있습니다. 연결 규칙을 설정하여 들어오는 요청을 식별하고 보안 규칙을 설정하여 데이터를 마스킹할 방법을 정의합니다. Dynamic Data Masking은 MDM Hub에서 들어오는 데이터베이스 요청을 모니터링하고 데이터베이스에 이 요청이 전송되기 전에 데이터베이스 요청을 수

정합니다. 데이터베이스는 수정된 요청을 처리하고 마스킹된 결과를 Dynamic Data Masking에 반환합니다. 그러면 Dynamic Data Masking은 결과를 MDM Hub으로 보냅니다.

Dynamic Data Masking을 사용하여 특정 유형의 데이터베이스 요청에 대해 데이터를 마스킹하거나 조직 내 특정 그룹의 데이터에 대한 액세스를 제한할 수 있습니다. 예를 들어 지원 팀 멤버로부터 데이터베이스 요청이 들어오면 신용 카드 번호에 마스킹 기능을 적용하는 규칙을 생성할 수 있습니다. Dynamic Data Masking이 데이터를 다시 MDM Hub으로 보내면 지원 팀 멤버에게는 실제 신용 카드 번호 대신 마스킹된 번호가 표시됩니다.

참고: MDM Hub에서 Dynamic Data Masking을 사용하려면 Dynamic Data Masking 9.6.0 및 긴급 버그 픽스 14590이 설치되어 있어야 합니다. Dynamic Data Masking 이전 버전은 MDM Hub과 호환되지 않습니다.

Dynamic Data Masking에 대한 자세한 내용은 Dynamic Data Masking 설명서를 참조하십시오.

보안 액세스 관리자

보안 액세스 관리자는 MDM Hub을 위한 보안 모듈입니다. 보안 액세스 관리자는 MDM Hub 리소스를 무단 액세스로부터 보호합니다.

보안 액세스 관리자는 MDM Hub 구현에서 조직에 대한 보안 정책을 적용합니다. 보안 액세스 관리자는 보안 구성에 따라 사용자 인증 및 권한 부여를 관리합니다.

참고: 보안 액세스 관리자를 사용하여 타사 응용 프로그램의 MDM Hub 리소스에 대한 사용자 액세스 권한을 구성할 수 있습니다. 그러나 보안 액세스 관리자를 통해 Hub 콘솔 도구 및 리소스에 대한 보안은 구성할 수 없습니다. Hub 콘솔은 사용자를 인증하고 별도의 보안 메커니즘을 통해 사용자에게 Hub 콘솔 도구 및 리소스에 대한 액세스 권한을 부여합니다.

인증

인증은 사용자의 ID를 확인하는 프로세스입니다.

MDM Hub은 사용자 이름 및 암호와 같은 제공된 자격 증명이나 보안 페이로드의 원시 이진 데이터에 따라 사용자를 인증합니다.

MDM Hub은 다음 인증 유형을 사용합니다.

내부

MDM Hub 내에서 사용자를 인증하며 여기에서 사용자는 사용자 이름과 암호로 로그인합니다.

외부 디렉터리

LDAP 사용 디렉터리 서버, Microsoft Active Directory 및 Kerberos에 대한 기본 지원을 사용하여 외부 사용자 디렉터리를 통해 사용자를 인증합니다.

외부 인증 공급자

타사 인증 공급자를 통해 사용자를 인증합니다.

MDM Hub 구현에서는 각 유형의 인증을 단독으로 사용하거나 조합하여 사용할 수 있습니다. 사용하는 인증 유형은 보안 구성 방식에 따라 달라집니다.

권한 부여

권한 부여는 사용자에게 요청된 MDM Hub 리소스에 액세스할 수 있는 권한이 있는지 확인하는 프로세스입니다.

MDM Hub에서는 다음과 같이 내부 및 외부 인증을 사용할 수 있습니다.

내부

MDM Hub을 통해 권한을 부여합니다. MDM Hub은 사용자 계정에 할당된 모든 역할과 연결되어 있는 권한을 검사하여 보안 리소스에 대한 액세스 가능 여부를 결정합니다.

외부

타사 권한 부여 공급자를 통해 권한을 부여합니다.

MDM Hub을 권한 부여 유형 중 하나를 사용하도록 구성할 수도 있고, 두 가지 권한 부여 유형을 모두 사용하도록 구성할 수도 있습니다.

보안 리소스 및 권한

여러 MDM Hub 리소스를 보안 리소스로 구성할 수 있습니다.

다음 리소스를 구성할 수 있습니다.

- 기본 개체
- 매핑
- 패키지
- 정리 함수
- 일치 규칙 집합
- 메타데이터
- 프로필
- 사용자 테이블

권한에 따라 MDM Hub 리소스에 대한 액세스 권한을 부여할 수 있습니다. MDM Hub은 다음 권한을 할당할 수 있습니다.

- 읽기
- 생성
- 업데이트
- 병합
- 실행
- 삭제

리소스는 개인 또는 보안 중 하나일 수 있습니다. 기본적으로 리소스는 보호입니다. MDM Hub은 보안 리소스에 만 권한을 부여할 수 있습니다.

MDM Hub에서 보안을 구성하는 경우 다음 사항을 고려합니다.

- 특정 리소스가 보안 리소스로 구성됩니다.
- 특정 역할이 하나 이상의 보안 리소스에 액세스할 수 있도록 구성됩니다.

- 각 보안 리소스를 특정 권한(읽기 또는 쓰기 등)으로 구성할 수 있습니다. 이렇게 하면 보안 리소스에 대해 해당 역할이 가지는 액세스 권한을 정의할 수 있습니다.

서비스 통합 프레임워크 요청을 실행하려면 로그인된 사용자가 요청과 관련된 리소스에 액세스하는 데 필요한 권한이 포함된 역할을 가지고 있어야 합니다.

역할

역할은 보안 **MDM Hub** 리소스에 액세스하는 데 사용되는 권한 집합을 나타냅니다. 사용자가 권한을 얻을 수 있도록 해당 사용자에게 역할을 할당합니다.

보안 액세스 관리자 작업 영역의 역할 도구를 사용하여 사용자 및 사용자 그룹에 역할을 할당할 수 있습니다. 사용자 또는 사용자 그룹에 할당된 역할은 사용자 또는 사용자 그룹의 리소스 권한을 결정합니다. 사용자에게 바로 권한을 할당할 수는 없습니다.

보안 액세스 관리자는 외부 응용 프로그램 사용자에게서 온 요청에 대해 리소스 권한 부여를 적용합니다. **MDM Hub** 리소스에 액세스하기 위해 **Hub** 콘솔을 사용하는 관리자 및 데이터 스튜어드는 같은 정도로 리소스 권한의 영향을 받지 않습니다.

보안 구현 시나리오

여러 가지 방법으로 **MDM Hub** 구현에서 보안을 구성할 수 있습니다.

정책 결정 지점은 런타임 시 사용자의 ID를 결정하는 특정 보안 검사점입니다. 이를 인증이라고 합니다. 정책 결정 지점은 사용자가 액세스할 수 있는 **MDM Hub** 리소스도 확인합니다. 이를 권한 부여라고 합니다. 정책 결정 지점을 **MDM Hub**에서 내부적으로 처리할지, 아니면 타사 보안 공급자 또는 기타 보안 서비스를 통해 외부적으로 처리할지는 **MDM Hub** 구현에 따라 달라집니다.

다음 시나리오는 **MDM Hub** 구현에서 보안을 구성할 수 있는 최상위 방법에 대한 예입니다.

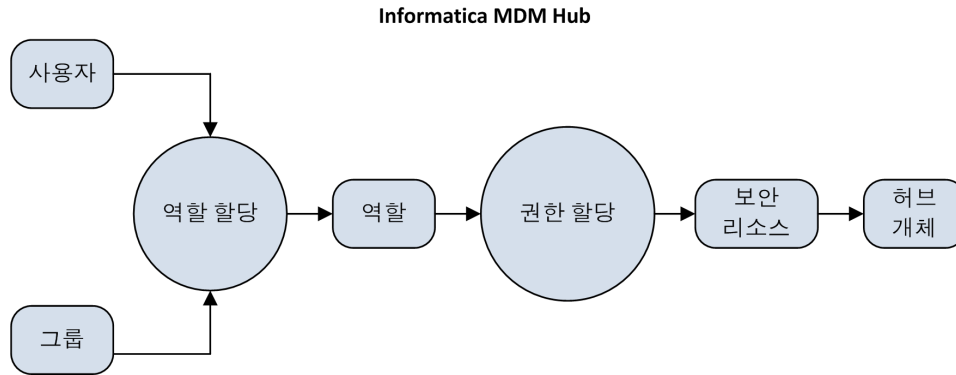
- 내부 전용 정책 결정 지점
- 외부 사용자 디렉터리
- 역할 기반의 중앙 집중식 정책 결정 지점
- 종합적인 중앙 집중식 정책 결정 지점

참고: **MDM Hub**는 외부 보안 공급자의 리소스 권한에 대한 변경 사항을 반영하지 않습니다. 외부 보안 공급자를 사용하여 리소스 권한을 변경할 경우 다른 방법을 사용하여 **MDM Hub**와 변경 사항을 동기화하십시오.

내부 정책 결정 지점

MDM Hub은 모든 정책 결정을 내부적으로 처리합니다.

다음 이미지는 MDM Hub이 모든 정책 결정을 내부적으로 처리하는 보안 배포를 보여 줍니다.



이 시나리오에서 MDM Hub은 Hub 콘솔을 통해 사용자, 그룹, 역할, 권한 및 리소스가 구성되는 방식을 기반으로 하여 모든 정책을 결정합니다.

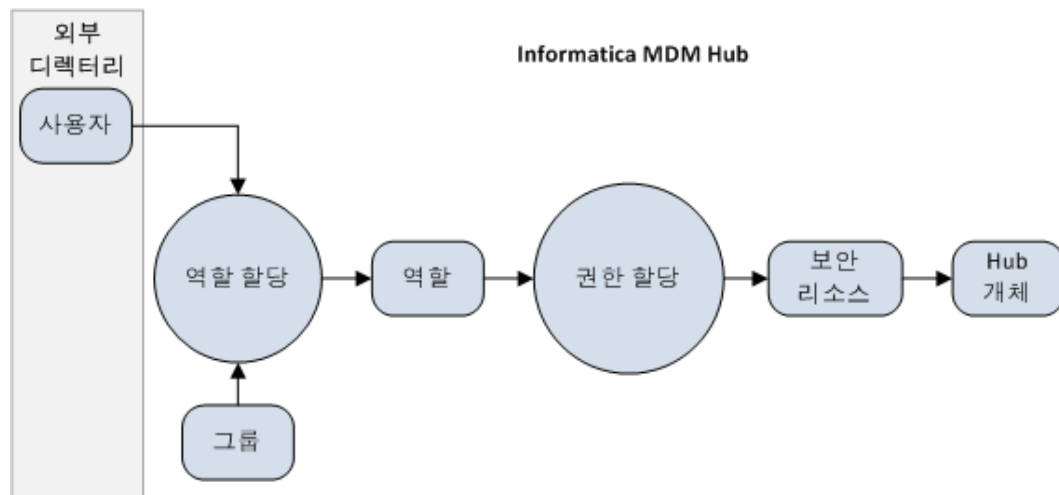
외부 사용자 디렉터리

MDM Hub은 외부 사용자 디렉터리와 통합될 수 있습니다.

외부 사용자 디렉터리에서 유지 관리되는 사용자 또는 사용자 그룹은 MDM Hub에도 등록되어 있어야 합니다. 등록을 해야 MDM Hub이 이러한 사용자 및 그룹에 역할 및 관련 권한을 할당할 수 있습니다.

외부 디렉터리의 사용자를 MDM Hub의 그룹에 할당합니다. LDAP(Lightweight Directory Access Protocol)를 통해 관계를 유지 관리해야 하는 경우에도 MDM Hub의 사용자와 그룹 간 관계를 유지 관리해야 합니다.

다음 이미지는 사용자가 외부 디렉터리에서 관리되지만 그룹, 역할 할당 및 권한 할당은 MDM Hub에서 관리되는 보안 배포를 보여 줍니다.

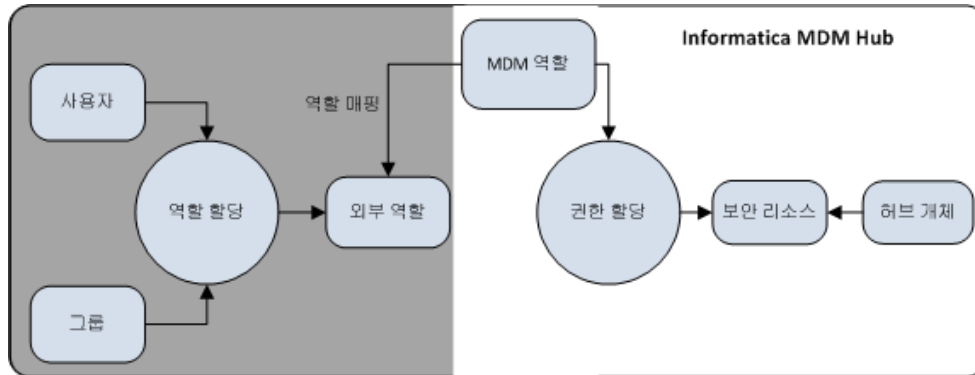


이 시나리오에서는 외부 사용자 디렉터리에서 사용자 계정, 그룹 및 사용자 프로필을 관리합니다. 외부 사용자 디렉터리에서는 사용자를 인증하고 그룹 멤버 자격 및 사용자 프로필에 대한 정보를 MDM Hub에 제공할 수 있습니다.

역할 기반의 중앙 집중식 정책 결정

MDM Hub은 일부 정책 결정을 내부에서 처리하고 외부 역할 할당을 받을 수 있습니다.

다음 이미지는 사용자 계정, 그룹 및 사용자 프로필과 함께, 역할 할당이 MDM Hub 외부에서 발생하는 보안 배포를 보여 줍니다.

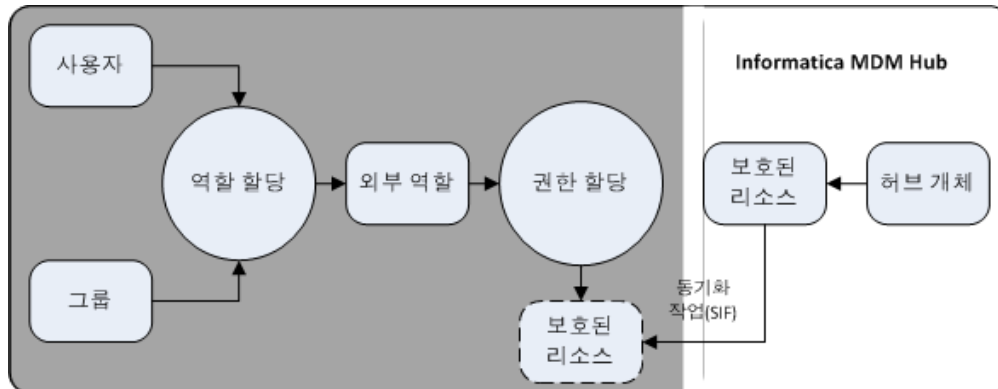


이 시나리오에서는 외부 역할이 MDM Hub 역할에 명시적으로 매핑됩니다.

종합적인 중앙 집중식 정책 결정

MDM Hub은 보호된 리소스를 내부에서 제어하면서도 외부 디렉터리에서 할당된 역할 및 권한을 허용할 수 있습니다.

다음 이미지는 MDM Hub 외부에서 역할 정의 및 권한 할당이 수행되는 보안 배포를 보여 줍니다. 또한 이 그림은 사용자 계정, 그룹, 사용자 프로필 및 역할 할당이 MDM Hub 외부에서 수행된다는 것을 보여 줍니다.



이 시나리오에서 MDM Hub은 단순히 외부 프록시를 사용하여 보호되는 리소스를 표시합니다. 이러한 리소스는 서비스 통합 프레임워크 요청을 통해 내부에서 보호되는 리소스와 동기화됩니다. 모든 정책 결정은 MDM Hub 외부에서 이루어집니다.

보안 시나리오를 위한 태스크 구성

다음 표에서는 각 보안 구현 시나리오와 관련된 보안 구성 태스크를 보여 줍니다. 셀에 "예"가 표시되어 있으면 관련 태스크가 MDM Hub 내에서 발생합니다. 셀에 "아니요"가 표시되어 있으면 관련 태스크가 MDM Hub 외부에서 발생합니다.

서비스/태스크	내부 정책 결정 지점	외부 사용자 디렉터리	RoleNobased 중앙 집중식 정책 결정 지점	종합적인 중앙 집중식 정책 결정 지점
MDM Hub 사용자 구성	예	예	아니요	아니요
외부 인증 사용	아니요	예	아니요	아니요
현재 연산 참조 저장소 데이터베이스에 사용자 할당	예	예	아니요	아니요
글로벌 암호 정책 관리	예	아니요	아니요	아니요
사용자 그룹 구성	예	예	아니요	아니요
MDM Hub 리소스 보호	예	예	예	예
MDM Hub 리소스의 상태 설정	예	예	예	예
역할 구성	예	예	예	아니요
외부 역할에 내부 역할 매핑	아니요	아니요	예	아니요
역할에 리소스 권한 할당	예	예	예	아니요
보안 공급자 관리	아니요	예	예	예
사용자 및 사용자 그룹에 역할 할당	예	예	아니요	아니요

참고: 타사 보안 공급자를 사용하여 MDM Hub 구현의 보안 부분을 처리하는 경우에는 보안 공급자의 구성 지침을 참조하십시오.

기본 관리자 비활성화

기본 관리자 계정을 비활성화하여 보안 목적으로 외부 인증을 차단할 수 있습니다. 이렇게 하면 외부 사용자가 이 계정을 사용하여 MDM 시스템에 액세스할 수 없게 됩니다. MDM Hub에서 비기본 관리자를 생성하고 구성해야 합니다.

1. MDM Hub에서 관리자를 생성합니다. **사용자 > 사용자 추가 > 새로 만들기**로 이동하고, 이 새 사용자 계정을 생성한 다음 **관리자 활성화** 확인란을 선택합니다.
2. 등록된 ORS에 사용자를 할당합니다. 여러 ORS에 할당하려는 경우 **대상 데이터베이스** 탭을 사용합니다.
3. 기본 관리자 계정을 비활성화하려면 MDM Hub 마스터 데이터베이스에 연결하고 다음 명령을 실행합니다.

```
update c_repos_user set user_enabled_ind = 0 where rowid_user = 'INST.0 ' ;
commit;
```


4. ActiveVOS 콘솔의 **ID 서비스**에서 사용할 수 있도록 이 사용자를 할당합니다.
 - a. <MDM Hub 설치 디렉터리>/hub/server/bin 폴더로 이동합니다.
 - b. build.properties 파일을 엽니다.
 - c. 생성한 사용자 이름에 대한 다음 속성을 추가합니다. mdm.identity.user=<사용자 이름>.
 - d. 파일을 저장합니다.
5. 명령 프롬프트를 열고 다음 스크립트를 실행합니다.
 - Windows의 경우. <MDM Hub 설치 디렉터리>\hub\server\postInstallSetup.bat
 - UNIX의 경우. <MDM Hub 설치 디렉터리>/hub/server/postInstallSetup.sh
6. 응용 프로그램 서버를 다시 시작합니다.
7. ActiveVOS 콘솔에 로그인하고 **ID 서비스**에 추가된 이 새 사용자의 암호를 업데이트합니다.
 - a. **관리** 탭에서 **서비스 구성 > ID 서비스**로 이동합니다.
 - b. **연결** 탭의 **연결 설정** 섹션에서 새 암호를 지정하고 확인합니다.
 - c. **업데이트**를 클릭합니다.

HotFix를 설치하는 경우 mdm.identity.user=<사용자 이름> 설정이 build.properties 파일에서 자동으로 제거됩니다. 이 속성을 수동으로 추가해야 합니다. build.properties 파일을 열고 속성을 추가한 다음 파일을 저장합니다. postInstallSetup 스크립트를 실행합니다. 응용 프로그램 서버를 다시 시작합니다.

제 2 장

리소스

이 장에 포함된 항목:

- [리소스 개요, 18](#)
- [보안 및 개인 리소스, 19](#)
- [리소스 그룹, 19](#)
- [보안 리소스 도구, 20](#)
- [보안 리소스 구성, 20](#)
- [리소스 그룹 구성, 21](#)
- [Data Director 비즈니스 항목 서비스에 대한 보안 구성, 23](#)

리소스 개요

Hub 콘솔에서는 외부 응용 프로그램에 MDM Hub 리소스를 표시하거나 숨길 수 있습니다.

보안 리소스는 역할 도구에 표시되는 보호된 MDM Hub 리소스로서, 특정 권한을 가진 역할에 리소스를 추가할 수 있습니다. 리소스 그룹은 권한 할당을 간소화하는 보안 리소스 컬렉션입니다. 보안 리소스 도구를 사용하여 리소스 그룹을 정의하고 리소스 계층을 생성할 수 있습니다.

다음 MDM Hub 리소스를 보안 리소스로 구성할 수 있습니다.

기본 개체

사용자가 모든 보안 기본 개체, 열 및 콘텐츠 메타데이터에 액세스할 수 있습니다.

정리 함수

사용자가 모든 보안 정리 함수를 실행할 수 있습니다.

계층 관리자 프로필

사용자가 모든 보안 계층 관리자 프로필에 액세스할 수 있습니다.

비즈니스 항목 서비스

사용자가 모든 보안 비즈니스 항목 서비스에 액세스할 수 있습니다.

매핑

사용자가 모든 보안 매핑 및 해당 열에 액세스할 수 있습니다.

패키지

사용자가 모든 보안 패키지 및 해당 열에 액세스할 수 있습니다.

원격 패키지

사용자가 모든 보안 원격 패키지에 액세스할 수 있습니다.

일괄 그룹은 기본적으로 보호됩니다. 일괄 그룹의 상태를 개인으로 변경할 수는 없습니다. 일괄 그룹에는 읽기 및 실행 권한이 있습니다.

또한 Hub 콘솔을 사용하여 메타데이터, 일치 규칙 집합, 감사 테이블 및 사용자 테이블을 포함하여 SIF 요청을 통해 액세스할 수 있는 다른 리소스를 보호할 수 있습니다.

참고: Informatica Data Director를 사용하는 경우 HTTP 메서드 GET 또는 POST를 사용하여 Hub 서버에 액세스할 수 있습니다. DELETE 또는 PUT 등 기타 HTTP 메서드는 HTTP 오류를 반환합니다.

보안 및 개인 리소스

보호된 MDM Hub 리소스를 보안 또는 개인 중 하나로 구성할 수 있습니다.

보안

역할 도구에 이 MDM Hub 리소스를 표시합니다. 이를 통해 특정 권한을 가진 역할에 리소스를 추가할 수 있습니다. 사용자에게 특정 역할을 할당하면 사용자는 SIF 요청을 사용하여 해당 역할에 연결된 권한에 따라 보안 리소스에 액세스할 수 있습니다. 기본적으로 MDM Hub는 기본 개체와 같은 새 리소스를 보안으로 지정합니다.

개인

역할 도구에서 MDM Hub 리소스를 숨깁니다. SIF 요청에서 리소스에 액세스하지 못하도록 합니다.

리소스는 외부 응용 프로그램에서 SIF 요청을 사용하여 MDM Hub 리소스에 액세스하기 전에 보호되어야 합니다.

특정 MDM Hub 리소스를 외부 응용 프로그램에 표시하고 싶지 않은 경우가 있습니다. 예를 들어 MDM Hub 구현에 일괄 작업에서만 사용되고 SIF 요청에서는 사용되지 않는 매핑이나 패키지가 있을 수도 있습니다. 이러한 리소스는 개인으로 설정할 수 있습니다.

참고: MDM Hub는 패키지 열을 보안 리소스로 간주하지 않습니다. 패키지 열은 상위 기본 개체 열의 보안 상태와 권한을 상속합니다. 시스템 테이블 열을 기준으로 하는 패키지 열의 경우 기본적으로 액세스할 수 있으므로 이 열에는 보안을 설정할 필요가 없습니다.

리소스 그룹

리소스 그룹은 보안 리소스의 논리적 컬렉션입니다.

보안 리소스 도구를 사용하여 리소스 그룹을 정의하면 관련 리소스를 이 그룹에 할당할 수 있습니다. 리소스 그룹은 권한 할당을 간소화하므로, 여러 리소스에 권한을 할당하고 역할에 리소스 그룹을 할당할 수 있습니다.

관리를 간소화하려면 다음 종류의 리소스 그룹 생성을 고려하십시오.

- 모든 보안 리소스를 포함하는 ALL_RESOURCES 리소스 그룹을 정의합니다. 이 리소스 그룹을 사용하여 최소한의 권한을 전역적으로 설정할 수 있습니다.
- 해당 리소스 종류에 최소한의 권한을 설정할 수 있도록 리소스 유형별로 리소스 그룹을 정의합니다.
- TRAINING_RESOURCES와 같은 기능 영역별로 리소스 그룹을 정의합니다.
- 권한이 비슷한 여러 역할을 할당할 수 있는 다용도 리소스 그룹을 정의합니다.

리소스 그룹 계층

리소스 그룹에는 해당 리소스 그룹이 속한 리소스 그룹을 제외한 다른 리소스 그룹도 포함될 수 있습니다. 즉, 리소스 그룹의 계층을 작성하고 대규모 리소스 컬렉션 관리를 간소화할 수 있습니다.

보안 리소스

보안 리소스만 리소스 그룹에 속할 수 있습니다. 개인 리소스는 리소스 그룹에 속할 수 없습니다.

리소스 상태를 개인으로 변경하면 MDM Hub은 리소스가 속한 모든 리소스 그룹에서 리소스를 제거합니다. 리소스 상태를 보안으로 설정하면 MDM Hub은 적절한 리소스 그룹에 해당 리소스를 추가합니다.

보안 리소스 도구

Hub 콘솔의 보안 리소스 도구를 사용하여 MDM Hub의 모든 리소스 상태를 보안 또는 개인으로 설정하는 등, MDM Hub 리소스에 대한 보안을 세부적으로 관리합니다. 리소스 그룹을 사용하여 리소스 계층을 구성할 수도 있습니다.

보안 리소스 도구에는 다음 탭이 포함되어 있습니다.

리소스

개별 MDM Hub 리소스의 상태를 보안 또는 개인으로 설정하는 데 사용됩니다. MDM Hub에는 리소스 간 관계를 보여 주는 계층으로 해당 리소스가 표시됩니다. 글로벌 리소스는 계층 최상위에 표시됩니다.

리소스 그룹

리소스 그룹을 구성하는 데 사용됩니다.

보안 리소스 도구를 사용하여 역할 도구와 SIF 요청에 리소스를 표시하거나 숨길 수 있습니다. 이 도구를 사용하면 연산 참조 저장소에 연결해야 합니다.

보안 리소스 구성

MDM Hub 리소스를 찾고 구성하려면 보안 리소스 도구의 리소스 탭을 사용합니다.

MDM Hub 리소스의 상태 설정

모든 MDM Hub 리소스에 대해 리소스 상태를 보안 또는 개인으로 구성할 수 있습니다.

참고: 이 상태 설정은 보안 리소스만 포함하는 리소스 그룹이나 글로벌 리소스에는 적용되지 않습니다.

1. 보안 리소스 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. 리소스 탭에서 리소스 트리를 탐색하여 구성할 리소스를 찾습니다.
4. 리소스 이름을 두 번 클릭하여 보안 또는 개인 간에 전환합니다. 한 번에 여러 리소스 상태를 변경하려면 5단계와 6단계를 수행합니다.
5. 상태를 변경해야 하는 리소스를 선택합니다. 원하는 경우 여러 개의 리소스를 선택할 수 있습니다.
6. 선택한 리소스의 상태를 업데이트합니다.

- **보안** 단추를 클릭하면 선택한 리소스의 상태를 보안으로 변경할 수 있습니다.
 - **개인** 단추를 클릭하면 선택한 리소스의 상태를 개인으로 변경할 수 있습니다.
7. **저장** 단추를 클릭하여 변경 내용을 저장합니다.

리소스 필터링

MDM Hub 리소스의 컬렉션 상태 변경을 간소화하기 위해 변경할 리소스만 표시하는 필터를 지정할 수 있습니다.

1. 보안 리소스 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. **리소스 필터링** 단추를 클릭합니다.
보안 리소스 도구에 리소스 필터 대화 상자가 표시됩니다.
4. 리소스 유형을 선택합니다.
 - 필터에 포함하려는 리소스 유형을 선택합니다.
 - 필터에서 제외하려는 리소스 유형을 지웁니다.
5. **확인**을 클릭합니다.
보안 리소스 도구에 필터링된 리소스 트리가 표시됩니다.

리소스 그룹 구성

보안 리소스 도구를 사용하여 리소스 그룹을 정의하고 리소스 계층을 생성할 수 있습니다. 그런 다음 역할 도구를 사용하여 단일 작업의 여러 리소스에 권한을 할당할 수 있습니다.

보안 리소스 도구에서는 현재 리소스 그룹에 직접적으로 속하는 리소스와 간접적으로 속하는 리소스가 시각적으로 구분됩니다. 리소스 그룹에 명시적으로 추가된 리소스는 직접 멤버 자격을 가지고 있습니다. 리소스 그룹에 추가된 리소스 그룹에 속한 리소스는 간접 멤버 자격을 가지고 있습니다.

예를 들어 다음 두 개의 리소스 그룹이 있다고 가정해 봅니다.

- 리소스 그룹 A에는 **Consumer** 기본 개체가 있습니다. 즉, 이 **Consumer** 기본 개체는 리소스 그룹 A의 직접 멤버입니다.
- 리소스 그룹 B에는 **Address** 기본 개체가 있습니다.
- 리소스 그룹 A에 리소스 그룹 B가 포함됩니다. 즉, **Address** 기본 개체가 리소스 그룹 A의 간접 멤버입니다.

이 예에서 리소스 그룹 A를 편집하면 주소 기본 개체를 사용할 수 없습니다. 주소 기본 개체를 편집하려면 리소스 그룹 B를 편집해야 합니다.

리소스 그룹 추가

보안 리소스 도구를 사용하여 리소스 목록에 리소스 그룹을 추가합니다.

1. 보안 리소스 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. **리소스 그룹** 탭을 클릭합니다.

보안 리소스 도구에 리소스 그룹 탭이 표시됩니다.

4. **추가** 단추를 클릭합니다.

보안 리소스에 리소스 그룹에 리소스 추가 대화 상자가 표시됩니다.

5. 리소스 그룹의 고유한 설명 이름을 입력합니다.

6. 더하기 기호(+를 클릭하여 리소스 계층을 필요한 대로 확장합니다.

각 리소스에는 해당 리소스가 리소스 그룹의 멤버인지 여부를 나타내는 확인란이 있습니다. 상위를 선택하면 하위도 모두 선택됩니다. 예를 들어 트리에서 기본 개체 항목을 선택하면 모든 기본 개체 및 하위 리소스가 선택됩니다.

7. 이 리소스 그룹에 할당할 리소스를 선택합니다.

8. **확인**을 클릭합니다.

리소스 그룹 노드에 새 리소스가 추가됩니다.

리소스 그룹 편집 및 삭제

보안 리소스 도구를 사용하여 리소스 그룹을 편집 또는 삭제할 수 있습니다.

1. 보안 리소스 도구를 시작합니다.

2. 쓰기 잠금을 획득합니다.

3. **리소스 그룹** 탭을 클릭합니다.

4. 속성을 편집하거나 삭제할 리소스 그룹을 선택합니다.

- **편집** 단추를 클릭하여 리소스 그룹을 편집합니다.
- **제거** 단추를 클릭하여 리소스 그룹을 제거합니다.

보안 리소스 도구에 리소스 그룹에 리소스 할당 대화 상자가 표시됩니다. 또는 보안 리소스 도구의 리소스 그룹 노드에서 삭제된 리소스가 제거됩니다.

5. 리소스 그룹 이름을 편집합니다.

6. 더하기(+) 기호를 클릭하여 리소스 계층을 확장합니다.

7. **이 리소스 그룹에 대해 선택된 리소스만 표시** 확인란을 선택합니다.

8. 이 리소스 그룹에 할당할 리소스를 선택합니다.

9. 이 리소스 그룹에서 제거할 리소스를 지웁니다.

10. **확인**을 클릭합니다.

리소스 목록 새로 고침

리소스를 추가하면 리소스 목록을 새로 고쳐서 업데이트할 수 있습니다.

리소스 목록을 새로 고치려면 보안 리소스 메뉴에서 **새로 고침**을 선택합니다.

보안 리소스 도구가 리소스 목록을 업데이트합니다.

기타 보안 변경 내용 새로 고침

다른 모든 보안 변경 내용에 대해 새로 고침 간격을 변경할 수도 있습니다.

보안 변경 내용의 새로 고침 빈도를 설정하려면 `cmxserver.properties` 파일에서 다음 매개 변수를 설정합니다.

`cmx.server.sam.cache.resources.refresh_interval`

참고: 기본 새로 고침 간격은 5클록 틱(1클록 틱/60,000밀리초의 속도)이며 이는 5분에 해당합니다.

Data Director 비즈니스 항목 서비스에 대한 보안 구성

비즈니스 항목 서비스는 보안 리소스이며, 권한을 가진 사용자 역할만 Data Director의 비즈니스 항목 서비스에 액세스할 수 있습니다.

MDM Hub 콘솔에서 다음 비즈니스 항목 서비스 리소스를 구성할 수 있습니다.

- 찾기-교체
- 파일 가져오기
- 임시 일치

비즈니스 항목 서비스를 보안 리소스로 구성하려면 보안 리소스 도구를 사용해야 합니다. 그런 다음 역할 도구를 사용하여 사용자 역할에 권한을 할당할 수 있습니다.

비즈니스 항목 서비스를 보안 리소스로 구성

보안 액세스 관리자 작업 영역에서 보안 리소스 도구를 사용하여 필수 리소스를 보안 리소스로 구성합니다.

1. 보안 리소스 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. 리소스 탭을 클릭합니다.
4. 리소스 트리로 이동한 후 **비즈니스 항목 서비스**를 확장합니다.
5. 리소스 이름을 두 번 클릭하여 보안 또는 개인 간에 전환합니다.
 - a. **보안** 단추를 클릭하면 선택한 리소스의 상태를 보안으로 변경할 수 있습니다.
 - b. **개인** 단추를 클릭하면 선택한 리소스의 상태를 개인으로 변경할 수 있습니다.
6. **저장**을 클릭합니다.

비즈니스 항목 서비스에 역할 권한 할당

보안 액세스 관리자 작업 영역에서 역할 도구를 사용하여 비즈니스 항목 서비스 권한을 사용자 역할에 할당합니다.

1. 역할 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. 역할 목록을 스크롤하여 필요한 역할을 선택합니다.
4. 리소스 권한 탭을 클릭합니다.
5. 리소스 트리로 이동한 후 **비즈니스 항목 서비스**를 확장합니다.
6. 각 비즈니스 항목 서비스 리소스에 대한 **실행** 권한을 선택합니다.
7. **저장**을 클릭합니다.

제 3 장

역할

이 장에 포함된 항목:

- [역할 개요, 24](#)
- [역할 구성, 24](#)
- [권한, 25](#)
- [내부 역할 및 외부 역할, 26](#)

역할 개요

역할은 사용자 또는 그룹에 할당하는 권한의 컬렉션입니다. 역할은 보안 MDM Hub 리소스에 액세스하는 데 사용되는 권한 집합을 나타냅니다.

사용자가 MDM Hub의 보안 리소스를 보거나 조작할 수 있으려면 이러한 사용자에게 리소스에 액세스할 수 있는 권한을 부여하는 역할이 할당되어 있어야 합니다. 역할을 통해 사용자가 액세스할 수 있는 대상과 사용자가 MDM Hub에서 수행할 수 있는 태스크가 결정됩니다.

MDM Hub 역할은 매우 세부적이고 유연하므로, 관리자는 조직의 보안 정책에 따라 복잡한 보안 조치를 구현할 수 있습니다. 관리자와 같은 일부 사용자는 모든 대상에 액세스할 수 있는 단일 역할을 할당받을 수도 있습니다. 데이터 스튜어드와 같은 다른 사용자는 명시적으로 권한이 제한된 역할을 할당받을 수도 있습니다.

역할에 다른 역할을 할당할 수도 있습니다. 이 경우에는 할당된 역할에 구성된 액세스 권한이 상속됩니다. 권한은 가산적입니다. 다시 말해, 역할을 결합하면 해당 역할의 권한도 결합됩니다. 예를 들어 역할 A에는 주소 기본 개체에 대한 읽기 권한이 있고 역할 B에는 이 기본 개체에 대한 생성 및 업데이트 권한이 있다고 가정해 보겠습니다. 사용자 계정에 역할 A와 역할 B가 할당되면 이 사용자 계정은 주소 기본 개체에 대한 읽기, 생성, 업데이트 권한을 모두 갖게 됩니다. 사용자 계정은 해당 사용자 계정이 할당된 모든 역할에 구성된 권한을 상속합니다.

역할 구성

MDM Hub에서 역할을 생성, 편집 및 삭제할 수 있습니다.

참고: 외부적으로 사용자에게 권한이 부여되는 종합적인 중앙 집중식 보안 배포를 사용하는 경우에는 역할을 구성하지 않아도 됩니다.

리소스 권한은 사용자가 작업을 수행하는 데 필요한 액세스 범위에 따라 다릅니다. 관리자에게 있어 모범 사례는 권한 최소화 원칙을 따르는 것입니다. 사용자에게 작업을 수행하는 데 필요한 최저 수준의 권한을 할당합니다.

역할 추가

역할을 구성하고 MDM Hub 리소스에 대한 액세스 권한을 할당하려면 보안 액세스 관리자 작업 영역에서 역할 도구를 사용합니다.

팁: 역할 이름에 공백을 사용하지 마십시오. 공백을 사용하면 MDM Hub가 ActiveVOS와 통신할 때 오류가 발생할 수 있습니다.

1. 역할 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. 탐색 창에서 아무 곳이나 가리키고 마우스 오른쪽 단추를 클릭한 후 **역할 추가**를 선택합니다.
역할 도구에 역할 추가 대화 상자가 표시됩니다.
4. 역할 이름을 입력합니다.
5. 역할의 선택적 설명을 입력합니다.
6. 역할의 외부 이름 내지는 별칭을 입력합니다.
7. **확인**을 클릭합니다.
새 역할이 역할 목록에 나타납니다.

역할 편집 및 삭제

기존 역할을 편집 또는 삭제하려면 보안 액세스 관리자 작업 영역에서 역할 도구를 사용합니다.

1. 역할 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. 역할 목록을 스크롤하여 편집할 역할을 선택합니다.
 - 편집할 각 속성에서 옆에 있는 **편집** 단추를 클릭하고 새 값을 지정합니다.
 - 탐색 창에서 아무 곳이나 가리키고 마우스 오른쪽 단추를 클릭한 후 **역할 삭제**를 선택한 후, 확인 메시지가 표시되면 **예**를 클릭합니다.
4. **저장** 단추를 클릭하여 변경 내용을 저장합니다.

권한

MDM Hub 내부 권한 부여를 사용하여 역할에 권한을 할당할 수 있습니다.

역할에 다음 권한을 할당할 수 있습니다.

읽기

사용자가 데이터를 볼 수는 있지만 변경할 수는 없습니다.

생성

사용자가 Hub 저장소에서 데이터 레코드를 생성할 수 있습니다.

업데이트

사용자가 Hub 저장소에서 데이터 레코드를 업데이트할 수 있습니다.

삭제

사용자가 Hub 저장소에서 데이터 레코드를 삭제할 수 있습니다.

병합

사용자가 데이터를 병합 및 병합 해제할 수 있습니다.

실행

사용자가 정리 함수 및 일괄 그룹을 실행할 수 있습니다.

권한은 MDM Hub 리소스에 대해 외부 응용 프로그램 사용자가 갖는 액세스 권한을 결정합니다. 예를 들어 특정 패키지에 대해 읽기, 생성, 업데이트 및 병합 권한을 갖도록 역할을 구성할 수 있습니다.

참고: 각 권한은 고유하며 명시적으로 할당되어야 합니다. 권한은 다른 권한을 집계하지 않습니다. 예를 들어 사용자가 어떤 리소스에 대한 업데이트 액세스 권한을 갖고 있다고 해서 해당 리소스에 대한 읽기 권한도 가진다고 할 수는 없습니다. 두 권한은 개별적으로 할당되어야 합니다.

Hub 콘솔을 사용하는 경우 설정이 Hub 콘솔 사용에 여전히 영향을 미치더라도 권한은 적용되지 않습니다. 예를 들어 데이터 스튜어드는 읽기 권한을 가진 패키지 이외에는 병합 관리자 및 데이터 관리자의 어떠한 패키지도 볼 수 없습니다. 데이터 스튜어드가 특정 패키지의 데이터를 편집하고 변경 사항을 저장하려면 데이터 스튜어드에 해당 패키지에 대한 업데이트 및 생성 권한이 있어야 합니다.

데이터 스튜어드에게 업데이트 또는 생성 권한이 없으면 데이터 관리자에서 어떤 데이터도 변경할 수 없습니다. 유사하게, 병합 관리자를 사용하여 레코드를 병합 또는 병합 해제하려면 데이터 스튜어드에 병합 권한이 있어야 합니다. 병합 관리자 및 데이터 관리자 도구에 대한 자세한 내용을 알아보려면 *Multidomain MDM 데이터 스튜어드 가이드*를 참조하십시오.

내부 역할 및 외부 역할

역할 기반의 중앙 집중식 보안 구현에서는 MDM Hub와 별도로 관리되는 외부 역할과 MDM Hub 내부 역할 간에 매핑을 생성해야 합니다.

외부 역할 이름은 MDM Hub 환경에서 사용되는 내부 역할 이름과 다를 수도 있습니다.

구성 세부 내용은 보안 공급자의 역할 매핑 구현에 따라 달라집니다. 구성 파일에서 역할을 매핑합니다. 두 개 이상의 내부 역할에 한 개의 외부 역할을 매핑할 수 있습니다.

참고: 매핑이 XML로 생성될 경우도 있지만 미리 정의된 구성 파일 형식은 없습니다. XML 파일이 아닐 수도 있고 아예 파일이 아닐 수도 있습니다. 매핑은 사용자 지정 사용자 프로필 또는 인증 공급자 구현의 일부입니다. 매핑은 사용자 프로필 개체 역할 목록을 내부 역할 ID로 채우는 데 그 목적이 있습니다.

역할에 리소스 권한 할당

보안 액세스 관리자 작업 영역에서 역할 도구를 사용하여 역할에 대한 리소스 권한을 할당 및 편집할 수 있습니다.

1. 역할 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. 역할 목록을 스크롤하고 리소스 권한을 할당할 역할을 선택합니다.
4. **리소스 권한** 탭을 클릭합니다.
5. 리소스 계층을 확장하여 이 역할에 대해 구성할 보안 리소스를 표시합니다.
6. 구성할 각 리소스에 대해 다음을 수행합니다.
 - 이 역할에 부여할 권한을 모두 선택합니다.
 - 이 역할에서 제거할 권한을 모두 지웁니다.

7. **저장** 단추를 클릭하여 변경 내용을 저장합니다.

다른 역할에 역할 할당

역할은 해당 역할이 이미 속해 있는 역할을 제외하고 다른 역할도 상속할 수 있습니다. 예를 들어 역할 **A**에 역할 **B**를 할당하면 역할 **A**는 역할 **B**의 액세스 권한을 상속합니다.

1. 역할 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. 역할 목록을 스크롤하고 다른 역할을 할당할 역할을 선택합니다.
4. **역할** 탭을 클릭합니다.
역할 도구에 선택한 역할에 할당할 수 있는 역할이 모두 표시됩니다.
5. 선택한 역할에 할당할 역할을 모두 선택합니다.
6. 이 역할에서 제거할 역할을 모두 지웁니다.
7. **저장** 단추를 클릭하여 변경 내용을 저장합니다.

역할에 대한 리소스 권한 보고서 생성

특정 역할에 부여된 리소스 권한을 설명하는 보고서를 생성할 수 있습니다.

1. 역할 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. 역할 목록을 스크롤하여 보고서를 생성할 역할을 선택합니다.
4. **보고서** 탭을 클릭합니다.
5. **생성**을 클릭합니다.

역할 도구에서 보고서가 생성되어 보고서 탭에 표시됩니다.

생성된 보고서를 HTML 파일로 저장

1. **저장**을 클릭합니다.
역할 도구에 저장된 보고서에 대한 대상 위치를 지정하라는 메시지가 표시됩니다.
2. 대상 위치로 이동합니다.
3. **저장**을 클릭합니다.

보안 액세스 관리자가 다음 이름 지정 규칙을 사용하여 보고서를 저장합니다.

`<ORS_Name>-<Role_Name>-RolePrivilegeReport.html`

여기서

- **ORS_Name**은 대상 데이터베이스의 이름입니다.
- **Role_Name**은 생성된 보고서에 연결된 역할입니다.

역할 도구는 현재 보고서를 대상 위치에 **HTML** 파일로 저장합니다. 그러면 이후에 브라우저에 이 보고서를 표시할 수 있습니다.

제 4 장

사용자 및 사용자 그룹

이 장에 포함된 항목:

- [사용자 및 사용자 그룹 개요, 28](#)
- [사용자 구성, 28](#)
- [암호 정책 구성, 31](#)
- [JDBC 데이터 소스 보안 구성, 33](#)
- [사용자 그룹 구성, 35](#)
- [역할과 사용자 및 사용자 그룹 간의 연결, 37](#)

사용자 및 사용자 그룹 개요

MDM Hub 사용자는 MDM Hub 리소스에 액세스할 수 있는 개인입니다.

사용자 계정은 Hub 저장소의 마스터 데이터베이스에 정의되어 있습니다. MDM Hub 사용자 소개는 *Multidomain MDM 개요 가이드*를 참조하십시오.

사용자 계정은 할당된 역할을 사용하여 MDM Hub 리소스에 대한 액세스 권한을 받으며 각 역할에 구성된 권한을 상속합니다.

구성 작업 영역의 사용자 도구를 사용하여 MDM Hub 사용자의 사용자 계정을 구성하고, 암호를 변경하고, 외부 인증을 활성화할 수 있습니다. *Multidomain MDM 서비스 통합 프레임워크 가이드*에 설명된 대로, 적절한 권한이 부여된 외부 응용 프로그램에서도 SIF 요청을 사용하여 사용자 계정을 등록할 수 있습니다.

사용자 구성

MDM Hub에서 사용자를 생성, 편집 및 삭제할 수 있습니다.

보안을 배포한 방식에 따라 MDM Hub 구현에서 마스터 데이터베이스에 사용자를 추가해야 할 수도 있습니다.

다음 시나리오에서는 마스터 데이터베이스에서 사용자를 구성해야 합니다.

- MDM Hub에서 내부 권한 부여를 사용하고 있습니다.
- MDM Hub를 통해 외부 권한 부여를 사용하고 있습니다.
- 여러 사용자가 다른 계정을 사용하여 Hub 콘솔에 액세스합니다.

동일한 사용자가 마스터 데이터베이스와 연결된 두 개 이상의 연산 참조 저장소에 액세스하더라도 한 번만 사용자를 정의해야 합니다.

MDM Hub 리소스에 대한 사용자 액세스

관리자와 데이터 스튜어드를 포함하여 사용자는 아래 방법으로 MDM Hub 리소스에 액세스할 수 있습니다.

MDM 응용 프로그램

사용자는 Hub 콘솔에 로그인하고 액세스 권한이 있는 도구를 사용하여 MDM Hub와 상호 작용할 수 있습니다. 또한 IDD 또는 프로비저닝 도구를 사용하여 기본 개체 및 비즈니스 엔터티의 데이터에 액세스할 수 있습니다.

타사 응용 프로그램

사용자는 SIF 클래스 기반의 타사 응용 프로그램을 사용하여 간접적으로 MDM Hub 데이터와 상호 작용할 수 있습니다. 이 사용자는 절대 Hub 콘솔에 로그인하지 않고 SIF 클래스를 호출할 수 있는 응용 프로그램을 사용하여 MDM Hub에 로그인합니다. 이와 같은 사용자를 외부 응용 프로그램 사용자라고 합니다. 개발자가 호출할 수 있는 SIF 요청 종류에 대한 자세한 내용은 *Multidomain MDM 서비스 통합 프레임워크 가이드*를 참조하십시오.

사용자 계정 추가

보안 액세스 관리자 작업 영역의 사용자 도구를 사용하여 MDM Hub에 사용자 계정을 추가합니다.

1. 사용자 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. **사용자** 탭을 클릭합니다.
4. **사용자 추가** 단추를 클릭합니다.

사용자 도구에 **사용자 추가** 대화 상자가 표시됩니다.

5. 사용자의 이름, 중간 이름 및 성을 입력합니다.
6. 사용자의 사용자 이름을 입력합니다.
참고: 사용자 이름은 대/소문자를 구분하지 않으며 소문자로 저장됩니다.
7. 사용자의 유효한 전자 메일 주소를 입력합니다. MDM Hub에서 이 사용자 계정의 암호를 이 전자 메일 주소로 전송합니다.
8. 사용자의 기본 데이터베이스를 입력합니다. 이는 사용자가 Hub 콘솔에 로그인할 때 기본적으로 선택되어 있는 데이터베이스입니다.
9. 사용자 계정이 응용 프로그램용인 경우 **응용 프로그램 사용자** 확인란을 선택합니다.

참고: 응용 프로그램 사용자는 사용자를 대신하여 트러스트된 응용 프로그램에서 생성한 요청의 인증서 기반 인증에 사용됩니다.

10. 사용자의 암호를 입력하고 확인합니다.
11. 인증 유형을 선택합니다.
 - MDM Hub 구현에서 타사 보안 공급자를 통해 인증을 사용하는 경우 **외부 인증 사용** 확인란을 선택합니다.
 - MDM Hub의 내부 인증을 사용하려면 **외부 인증 사용** 확인란을 선택 취소합니다.
12. 사용자의 공용 인증서를 찾습니다. 이 인증서는 MDM Hub에서 사용자 요청에 대한 인증용으로 사용할 수 있습니다.

참고: 사용자 계정이 응용 프로그램 사용자용인 경우 인증서를 선택해야 합니다.

13. **확인**을 클릭합니다.

사용자 도구의 **사용자** 탭에 있는 사용자 목록에 새 사용자가 추가됩니다.

사용자 계정 편집 및 삭제

보안 액세스 관리자 작업 영역의 사용자 도구를 사용하여 사용자 계정을 편집하거나 제거할 수 있습니다.

1. 사용자 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. **사용자** 탭을 클릭합니다.
4. 사용자를 삭제하려면 제거할 사용자 계정을 선택합니다.
5. **삭제** 단추를 클릭합니다.
사용자 도구에 삭제를 확인하는 메시지가 나타납니다.
6. **예**를 클릭하여 삭제를 확인합니다.
사용자 도구의 사용자 목록에서 삭제된 사용자 계정이 제거됩니다.
7. 사용자를 편집하려면 구성할 사용자 계정을 선택합니다.
8. 이름을 변경하려면 셀을 두 번 클릭하고 다른 이름을 입력합니다.
9. 원하는 경우 다른 로그인 데이터베이스와 서버를 선택합니다.
10. **관리자** 확인란을 선택하여 이 사용자에게 관리자 액세스 권한을 부여합니다. 그러면 사용자가 모든 Hub 콘솔 도구 및 모든 데이터베이스에 액세스할 수 있습니다.
11. **활성화** 확인란을 선택하여 이 사용자 계정을 활성화하고 이 사용자가 로그인하도록 허용합니다.
참고: 사용자에게 대해 외부 인증을 사용하는 경우 Hub 콘솔을 통해 사용자 계정을 비활성화할 수 없습니다.
12. **저장** 단추를 클릭합니다.
사용자 계정에 대한 변경 내용이 사용자 도구에 저장됩니다.

보충 사용자 정보 편집

MDM Hub을 사용하여 각 사용자에게 대한 보충 정보(전자 메일 주소 또는 전화 번호 등)를 관리할 수 있습니다. MDM Hub에는 이러한 정보를 입력하라는 메시지가 표시되지 않으며 MDM Hub은 이러한 정보를 특별한 방식으로 사용하지도 않습니다.

참고: Hub 콘솔에서 **admin** 사용자의 전자 메일 주소를 변경할 수 없습니다. **admin** 사용자의 전자 메일 주소를 변경하려면 CMX_SYSTEM 스키마의 C_REPOS_USER 테이블에서 **admin** 사용자 항목을 직접 업데이트합니다.

1. 사용자 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. **사용자** 탭을 클릭합니다.
4. 속성을 편집하려는 사용자를 선택합니다.
5. **편집** 단추를 클릭합니다.
사용자 도구에 **사용자 편집** 대화 상자가 표시됩니다.
6. 직위, 전자 메일 주소 또는 로그인 메시지와 같은 사용자에게 대한 속성을 모두 지정합니다. 로그인 메시지는 이 사용자가 로그인한 후 Hub 콘솔에 표시되는 메시지입니다.
7. **확인**을 클릭합니다.
8. **저장** 단추를 클릭하여 변경 내용을 저장합니다.

사용자 계정의 암호 설정 변경

사용자에 대한 암호 설정을 변경할 수 있습니다. 최신 암호와 암호를 변경한 사용자에 대한 최신 정보가 유지 관리됩니다. 암호 기록은 사용할 수 없습니다.

1. 사용자 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. **사용자** 탭을 클릭합니다.
4. 암호를 변경할 사용자를 선택합니다.
5. **암호 변경** 단추를 클릭합니다.

사용자 도구에 선택한 사용자에 대한 **암호 변경** 대화 상자가 표시됩니다.

6. 새 암호를 지정하고 확인합니다.
7. 인증 유형을 선택합니다.
 - MDM Hub 구현에서 타사 보안 공급자를 통해 인증을 사용하는 경우 **외부 인증 사용** 확인란을 선택합니다.
 - MDM Hub의 내부 인증을 사용하려면 **외부 인증 사용** 확인란을 선택 취소합니다.
8. **확인**을 클릭합니다.

연산 참조 저장소에 대한 사용자 액세스 권한 구성

연산 참조 저장소 데이터베이스에 대한 사용자 액세스 권한을 구성할 수 있습니다.

1. 사용자 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. **대상 데이터베이스** 탭을 클릭합니다.

사용자 도구에 대상 데이터베이스 탭이 표시됩니다.
4. 각 데이터베이스 노드를 확장하여 해당 데이터베이스에 액세스할 수 있는 사용자를 표시합니다.
5. 데이터베이스에 대한 사용자 할당을 변경하려면 데이터베이스 이름을 마우스 오른쪽 단추로 클릭하고 **사용자 할당**을 선택합니다.

사용자 도구에 **데이터베이스에 사용자 할당** 대화 상자가 표시됩니다.
6. 선택한 데이터베이스에 할당할 사용자의 이름을 모두 선택합니다.
7. 선택한 데이터베이스에 할당하지 않을 사용자의 이름을 모두 지웁니다.
8. **확인**을 클릭합니다.

암호 정책 구성

모든 사용자에 대한 글로벌 암호 정책을 정의할 수 있습니다. 개별 사용자에 대해 글로벌 암호 정책보다 우선 적용되는 개인 암호 정책을 구성합니다. 모든 암호는 대/소문자를 구분합니다.

참고: 보안이 활성화된 JBoss 응용 프로그램 서버에서 MDM Hub을 배포하는 경우 설정한 암호가 JBoss 암호 정책을 준수하는지 확인해야 합니다. 암호는 MDM Hub 글로벌 암호 정책도 준수해야 합니다. 이는 Hub 콘솔과 JBoss의 암호가 일치해야 하기 때문에 중요합니다.

암호 정책 설정

MDM Hub 사용자에게 대한 암호 정책 설정을 지정할 수 있습니다.

MDM Hub를 사용하면 사용자에게 대해 다음과 같은 개인 암호 정책을 설정할 수 있습니다.

암호 길이

암호의 최소 및 최대 문자 길이입니다.

암호 만료

암호 만료 여부와 암호가 유효한 기간(일)을 지정합니다.

암호의 만료 기간을 설정하려면 **암호 사용 가능 기간** 확인란을 선택합니다. 만료되지 않는 암호를 설정하려면 **암호 사용 가능 기간** 확인란을 선택 취소합니다.

암호 사용 가능 기간 확인란을 선택하는 경우 암호가 만료되어야 하는 일 수를 지정합니다. 설정할 수 있는 최소 암호 만료 기간은 10입니다.

로그인 설정

허용되는 유예 로그인 횟수 및 최대 로그인 실패 횟수입니다.

암호 기록

암호를 재사용할 수 있는 횟수입니다.

암호 요구 사항

암호 패턴을 적용하려면 **암호 패턴 유효성 검사**가 **활성화됨** 확인란을 선택합니다. 암호 패턴에 다음 조건을 지정할 수 있습니다.

- 최소 고유 문자 수
- 암호가 다음 문자로 시작해야 함
- 암호에 다음 문자가 포함되어야 함
- 암호가 다음 문자로 끝나야 함

글로벌 암호 정책 관리

글로벌 암호 정책은 개인 암호 정책이 지정되어 있지 않은 사용자에게 적용됩니다.

1. **사용자** 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. **글로벌 암호 정책** 탭을 클릭합니다.
[글로벌 암호 정책] 창이 나타납니다.
4. 암호 정책 설정을 지정합니다.
5. **확인**을 클릭합니다.
6. **저장** 단추를 클릭하여 글로벌 설정을 저장합니다.

개인 암호 정책 관리

모든 사용자의 글로벌 암호 정책을 재정의하는 개인 암호 정책을 지정할 수 있습니다.

참고: 암호 정책 관리에 대한 모범 사례는 대부분의 사용자 암호를 여러 개의 개인 정책이 아닌, 글로벌 정책으로 관리하는 것입니다.

1. 사용자 도구를 시작합니다.

2. 쓰기 잠금을 획득합니다.
3. **사용자** 탭을 클릭합니다.
4. 개인 암호 정책을 설정할 사용자를 선택합니다.
5. **암호 정책 관리** 단추를 클릭합니다.
선택한 사용자에 대한 **개인 암호 정책** 창이 나타납니다.
6. **개인 암호 정책 활성화** 옵션을 선택합니다.
7. 사용자에 대한 암호 정책 설정을 지정합니다.
8. **확인**을 클릭합니다.
9. **저장** 단추를 클릭하여 변경 내용을 저장합니다.

JDBC 데이터 소스 보안 구성

JDBC 데이터 소스에서 응용 프로그램 서버 보안을 사용하는 경우 MDM Hub 구현 시 `cmxserver.properties` 파일에서 설정을 구성해야 합니다.

JDBC 데이터 소스를 위한 응용 프로그램 서버의 사용자 이름 및 암호를 `cmxserver.properties` 파일에 저장해야 합니다. 암호는 일반 텍스트로 나타날 수 없습니다. 암호를 `cmxserver.properties` 파일에 저장하기 전에 암호를 암호화해야 합니다.

보안 JDBC 데이터 소스에 대한 자세한 내용은 응용 프로그램 서버 설명서를 참조하십시오.

보안 JDBC 데이터 소스에 대한 사용자 이름 및 암호

`cmxserver.properties` 파일에서 보안 JDBC 데이터 소스에 대한 사용자 이름과 암호를 구성하려면 다음 매개 변수를 사용합니다.

```
databaseId.username=username
databaseId.password=encryptedPassword
```

여기서 `databaseId`는 JDBC 데이터 소스의 고유 식별자입니다.

Oracle SID 연결 유형에 대한 데이터베이스 ID

Oracle SID 연결 유형의 경우 `databaseId`는 다음과 같은 문자열로 구성됩니다.

<데이터베이스 호스트 이름>-<Oracle SID>-<스키마 이름>

예를 들어 설정이 다음과 같은 경우

- <데이터베이스 호스트 이름> = localhost
- <Oracle SID> = MDMHUB
- <스키마 이름> = Test_ORS

사용자 이름 및 암호 속성은 다음과 같습니다.

```
localhost-MDMHUB-Test_ORS.username=weblogic
localhost-MDMHUB-Test_ORS.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

Oracle 서비스 연결 유형에 대한 데이터베이스 ID

Oracle 서비스 연결 유형의 경우 **databaseId**는 다음과 같은 문자열로 구성됩니다.

<서비스 이름>-<스키마 이름>

예를 들어 설정이 다음과 같은 경우

- <서비스 이름> = MDM_Service
- <스키마 이름> = Test_ORS

사용자 이름 및 암호 속성은 다음과 같습니다.

```
MDM_Service-Test_ORS.username=weblogic
MDM_Service-Test_ORS.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

IBM Db2 연결 유형에 대한 데이터베이스 ID

IBM Db2 연결 유형의 경우 **databaseId**는 다음과 같은 문자열로 구성됩니다.

<데이터베이스 호스트 이름>-<데이터베이스 이름>-<스키마 이름>

예를 들어 설정이 다음과 같은 경우

- <데이터베이스 호스트 이름> = localhost
- <데이터베이스 이름> = dsui2
- <스키마 이름> = DS_UI2

사용자 이름 및 암호 속성은 다음과 같습니다.

```
localhost-dsui2-DS_UI2.username=weblogic
localhost-dsui2-DS_UI2.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

Microsoft SQL Server 연결 유형에 대한 데이터베이스 ID

Microsoft SQL Server 연결 유형의 경우 **databaseId**는 다음과 같은 문자열로 구성됩니다.

<데이터베이스 호스트 이름>-<데이터베이스 이름>

예를 들어 설정이 다음과 같은 경우

- <데이터베이스 호스트 이름> = localhost
- <데이터베이스 이름> = ds_ui1

사용자 이름 및 암호 속성은 다음과 같습니다.

```
localhost-ds_ui1.username=weblogic
localhost-ds_ui1.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

마스터 데이터베이스의 데이터베이스 ID

마스터 데이터베이스에 액세스하는 JDBC 데이터 소스를 보호하려는 경우 **databaseId**는 CMX_SYSTEM입니다.
이 경우 속성은 다음과 같습니다.

```
CMX_SYSTEM.username=weblogic
CMX_SYSTEM.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

암호 암호화

데이터베이스 스키마의 암호화된 암호를 생성하려면 다음 명령을 사용합니다.

```
C:\>java -cp siperian-common.jar com.siperian.common.security.Blowfish password
Plaintext Password: password
Encrypted Password: 9C03B113CD8E4BBFD236C56D5FEA56EB
```

사용자 그룹 구성

사용자 그룹은 사용자 계정의 논리적 컬렉션입니다.

사용자 그룹을 사용하면 보안 관리가 간소화됩니다. 예를 들어 외부 응용 프로그램 사용자를 하나의 사용자 그룹으로 결합한 다음 보안 역할을 각 개별 사용자 대신 이러한 사용자 그룹에 부여할 수 있습니다. 사용자 그룹에는 사용자뿐 아니라 다른 사용자 그룹도 포함될 수 있습니다.

보안 액세스 관리자 작업 영역의 사용자 및 그룹 도구에 있는 그룹 탭을 사용하여 사용자 그룹을 구성합니다.

사용자 및 그룹 도구 시작

Hub 콘솔에서 사용자 및 그룹 도구를 시작합니다.

1. Hub 콘솔에서 연산 참조 저장소에 연결합니다(아직 연결하지 않은 경우).
2. 보안 액세스 관리자 작업 영역을 확장한 후 **사용자 및 그룹**을 클릭합니다.

Hub 콘솔에 사용자 및 그룹 도구가 표시됩니다.

사용자 및 그룹 도구에는 다음과 같은 탭이 포함됩니다.

그룹

사용자 그룹을 정의하고 사용자 그룹에 사용자를 할당하는 데 사용됩니다.

데이터베이스에 할당된 사용자

사용자 계정과 데이터베이스를 연결하는 데 사용됩니다.

역할에 사용자/그룹 할당

사용자 및 사용자 그룹을 역할과 연결하는 데 사용됩니다.

사용자/그룹에 역할 할당

역할을 사용자 및 사용자 그룹과 연결하는 데 사용됩니다.

사용자 그룹 추가

보안 액세스 관리자 작업 영역의 사용자 및 그룹 도구를 사용하여 사용자 그룹을 추가할 수 있습니다.

1. 사용자 및 그룹 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. **그룹** 탭을 클릭합니다.
4. **추가** 단추를 클릭합니다.
사용자 및 그룹 도구에 **사용자 그룹 추가** 대화 상자가 표시됩니다.
5. 사용자 그룹의 설명 이름을 입력합니다.
6. 필요한 경우 사용자 그룹에 대한 설명을 입력합니다.

7. **확인**을 클릭합니다.

사용자 및 그룹 도구의 목록에 새 사용자 그룹이 추가됩니다.

사용자 그룹 편집 및 삭제

사용자 및 그룹 도구를 사용하여 사용자 그룹을 편집하거나 제거할 수도 있습니다.

1. 사용자 및 그룹 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. **그룹** 탭을 클릭합니다.
4. 사용자 그룹 목록을 스크롤하여 편집할 사용자 그룹을 선택합니다.
5. 사용자 그룹을 제거하려면 **삭제** 단추를 클릭합니다.
사용자 및 그룹 도구에 삭제를 확인하는 메시지가 나타납니다.
6. **예**를 클릭합니다.
사용자 및 그룹 도구의 목록에서 삭제된 사용자 그룹이 제거됩니다.
7. 사용자 그룹을 편집하려면 편집할 각 속성 옆에 있는 **편집** 단추를 클릭하고 새 값을 지정합니다.
8. **저장** 단추를 클릭하여 변경 내용을 저장합니다.

사용자 그룹에 사용자 및 사용자 그룹 할당

사용자 그룹에 멤버를 할당하려면 다음을 수행합니다.

1. 사용자 및 그룹 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. **그룹** 탭을 클릭합니다.
4. 사용자 그룹 목록을 스크롤하여 편집할 사용자 그룹을 선택합니다.
5. 방금 생성한 사용자 그룹을 마우스 오른쪽 단추로 클릭하고 **사용자 및 그룹 할당**을 선택합니다.
사용자 및 그룹 도구에 **사용자 그룹에 할당** 대화 상자가 표시됩니다.
6. 선택한 사용자 그룹에 할당할 사용자 및 사용자 그룹의 이름을 모두 선택합니다.
7. 선택한 사용자 그룹에 할당하지 않을 사용자 및 사용자 그룹의 이름을 모두 지웁니다.
8. **확인**을 클릭합니다.

현재 ORS 데이터베이스에 사용자 할당

현재 연산 참조 저장소 데이터베이스에 사용자를 할당하려면

1. 사용자 및 그룹 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. **데이터베이스에 할당된 사용자** 탭을 클릭합니다.
4. **데이터베이스에 사용자 할당** 단추를 클릭하여 사용자를 연산 참조 저장소 데이터베이스에 할당합니다.
사용자 및 그룹 도구에 **데이터베이스에 사용자 할당** 대화 상자가 표시됩니다.
5. 선택한 연산 참조 저장소 데이터베이스에 할당할 사용자의 이름을 모두 선택합니다.
6. 선택한 연산 참조 저장소 데이터베이스에 할당하지 않을 사용자의 이름을 모두 지웁니다.
7. **확인**을 클릭합니다.

역할과 사용자 및 사용자 그룹 간의 연결

역할을 사용자 및 사용자 그룹과 연결할 수 있습니다. **사용자 및 그룹** 도구를 사용하여 다음과 같은 방법으로 역할을 사용자와 연결할 수 있습니다.

- 역할에 사용자 및 사용자 그룹을 할당합니다.
- 사용자와 사용자 그룹에 역할을 할당합니다.

구현에 가장 적절한 방법을 선택하십시오.

역할에 사용자 및 사용자 그룹 할당

역할에 사용자 및 사용자 그룹을 할당하려면

1. 사용자 및 그룹 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. **역할에 사용자/그룹 할당** 탭을 클릭합니다.
4. 사용자 및 사용자 그룹을 할당할 역할을 선택합니다.
5. **편집** 단추를 클릭합니다.
사용자 및 그룹 도구에 **역할에 사용자 할당** 대화 상자가 표시됩니다.
6. 선택한 역할에 할당할 사용자 및 사용자 그룹의 이름을 모두 선택합니다.
7. 선택한 역할에 할당하지 않을 사용자 및 사용자 그룹의 이름을 모두 지웁니다.
8. **확인**을 클릭합니다.

사용자 및 사용자 그룹에 역할 할당

사용자 및 사용자 그룹에 역할을 할당하려면

1. 사용자 및 그룹 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. **사용자/그룹에 역할 할당** 탭을 클릭합니다.
4. 역할을 할당할 사용자 또는 사용자 그룹을 선택합니다.
5. **편집** 단추를 클릭합니다.
사용자 및 그룹 도구에 **사용자에게 역할 할당** 대화 상자가 표시됩니다.
6. 선택한 사용자 또는 사용자 그룹에 할당할 역할을 선택합니다.
7. 선택한 사용자 또는 사용자 그룹에 할당하지 않을 역할을 지웁니다.
8. **확인**을 클릭합니다.

제 5 장

보안 공급자

이 장에 포함된 항목:

- [보안 공급자 개요, 38](#)
- [보안 공급자 관리, 38](#)
- [공급자 파일 관리, 39](#)
- [보안 공급자 설정, 40](#)
- [공급자 속성, 41](#)
- [사용자 지정 공급자, 42](#)
- [외부 인증, 43](#)

보안 공급자 개요

보안 공급자는 타사 응용 프로그램으로서, MDM Hub에 액세스하는 사용자에게 대한 인증 및 권한 부여와 같은 보안 서비스를 제공합니다. 보안 공급자는 일부 MDM Hub 보안 배포 시나리오에서 사용됩니다.

공급자 파일에는 보안 공급자의 프로필 정보가 포함되어 있습니다. 다른 타사 보안 공급자를 사용하려면 보안 공급자 도구를 사용하여 MDM Hub에 공급자 파일을 업로드합니다. 또한 보안 공급자 도구를 사용하여 공급자 목록에서 보안 공급자를 수정, 삭제, 활성화 또는 비활성화할 수도 있습니다.

MDM Hub은 기본적인 내부 보안 공급자 집합과 함께 제공됩니다. 또한 타사 보안 공급자를 추가할 수도 있습니다. 내부 보안 공급자를 제거할 수는 없습니다.

보안 공급자 관리

Hub 콘솔의 구성 작업 영역에 있는 보안 공급자 도구를 통해 MDM Hub 구현에서 보안 공급자를 관리할 수 있습니다.

MDM Hub 내부의 기본 선택 또는 사용자 지정 추가 공급자 선택에서 보안 공급자를 추가할 수 있습니다. 내부 보안 공급자를 제거할 수는 없습니다.

MDM Hub은 다음 보안 공급자 유형을 지원합니다.

인증 공급자

사용자 ID의 유효성을 검사하여 사용자를 인증합니다. MDM Hub에 해당 사용자가 인증된 사용자인지 알려 줍니다. 이 보안 공급자 유형은 사용자가 특정 MDM Hub 리소스에 액세스하는 데 필요한 권한을 가지고 있는지 여부를 확인하지 않습니다.

권한 부여 공급자

MDM Hub에 사용자가 특정 MDM Hub 리소스에 액세스하는 데 필요한 권한을 가지고 있는지 알려 줍니다.

사용자 프로필 공급자

사용자 관련 특성과 사용자가 속해 있는 역할 등 개별 사용자에 대한 정보를 MDM Hub에 알려 줍니다.

내부 공급자는 인증, 권한 부여 및 사용자 프로필 서비스에 대한 내부 MDM Hub 구현을 나타냅니다.

MDM Hub 기본 공급자 중 일부는 슈퍼 공급자입니다. 슈퍼 공급자는 인증 및 권한 부여 요청에 항상 긍정적인 응답을 반환합니다. 사용자, 역할 및 권한을 구성하지 않으려면 배포 환경의 슈퍼 공급자를 사용합니다. 슈퍼 공급자는 또한 보안이 성능 향상을 위한 SIF 요청 최상위에서 계층으로 제공되는 프로덕션 환경에서도 유용할 수 있습니다.

공급자 파일 관리

공급자 파일에는 보안 공급자의 프로필 정보가 포함되어 있습니다.

고유한 타사 보안 공급자를 사용하려면 보안 공급자 도구를 통해 명시적으로 등록해야 합니다. 보안 공급자를 등록하려면 등록에 필요한 프로필 정보가 포함된 공급자 파일을 업로드합니다.

공급자 파일은 다음 데이터가 포함된 JAR 파일입니다.

- 하나 이상의 외부 보안 공급자를 설명하는 매니페스트. 각 보안 공급자에는 다음 설정이 있습니다.
 - 공급자 이름
 - 공급자 설명
 - 공급자 유형
 - 공급자 팩터리 클래스 이름
 - 공급자에 대한 구성 세부 정보를 지정하는 속성. 이는 이름-값 쌍, 즉 속성 이름과 기본값의 목록일 수 있습니다.
- 공급자 구현 및 필요한 모든 타사 라이브러리.

Informatica 리소스 키트는 Hub 서버에서 공급자 파일에 대한 샘플 구현을 복사합니다. 샘플 공급자 파일에 대한 자세한 내용은 *Multidomain MDM 리소스 키트 가이드*를 참조하십시오.

공급자 파일 업로드

공급자 파일을 업로드하여 공급자 정보를 추가하거나 업데이트합니다.

1. 보안 공급자 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. 왼쪽 탐색 창에서 "공급자 파일"을 마우스 오른쪽 단추로 클릭하고 **공급자 파일 업로드**를 선택합니다.
이 공급자에 대한 JAR 파일을 선택하라는 메시지가 표시됩니다.
4. 파일 시스템을 필요한 대로 탐색하고 업로드하려는 JAR 파일을 선택하여 JAR 파일을 지정합니다.
5. **열기**를 클릭합니다.

보안 공급자 도구가 선택한 파일을 검사하여 유효한 공급자 파일인지 여부를 확인합니다.

6. 업로드하는 공급자 파일의 이름이 기존 공급자 파일의 이름과 동일하면 보안 공급자 도구에 기존 공급자 파일을 덮어쓸지 묻는 메시지가 나타납니다. **예**를 클릭하여 확인합니다.

보안 공급자 도구는 공급자 목록을 추가적인 공급자 정보로 채웁니다. 공급자 파일을 업로드하면 파일 시스템에서 원본 파일을 제거할 수 있습니다.

공급자 파일 삭제

공급자 파일은 해당 보안 공급자를 더 이상 사용하지 않을 경우 삭제할 수 있습니다.

1. 보안 공급자 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. 왼쪽 탐색 창에서 삭제하려는 공급자 파일을 마우스 오른쪽 단추로 클릭한 다음 **공급자 파일 삭제**를 선택합니다.

삭제를 확인하는 메시지가 나타납니다.

4. **예**를 클릭합니다.

보안 공급자 도구의 목록에서 삭제된 공급자 파일이 제거됩니다.

참고: MDM Hub과 함께 제공되는 내부 공급자 파일은 삭제할 수 없습니다.

보안 공급자 설정

보안 공급자 도구에 등록된 공급자 목록이 표시됩니다.

등록된 공급자 목록은 공급자 유형별로 정렬됩니다. 또한 공급자 목록의 공급자 순서는 공급자가 호출되는 순서를 나타냅니다. 사용자는 공급자 목록에 있는 하나 이상의 공급자로부터 인증을 받아야 합니다.

예를 들어 로그인하여 사용자 이름 및 암호를 제공하려고 하면 MDM Hub은 인증 목록에 있는 각 인증 공급자에 로그인 자격 증명을 제출합니다. MDM Hub은 목록을 통해 순차적으로 진행합니다. 목록의 공급자 중 하나에서 인증이 성공하면 MDM Hub이 사용자를 인증한 것입니다. 사용 가능한 모든 인증 공급자에서 인증이 실패한 경우에는 사용자가 인증되지 않은 것입니다.

보안 공급자 설정 변경

보안 공급자의 설정을 변경하려면 다음 단계를 수행합니다.

1. 보안 공급자 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. 수정할 보안 공급자를 선택합니다.
4. 속성 패널에서 편집할 설정 옆의 **편집** 단추를 클릭합니다.
5. **저장** 단추를 클릭하여 변경 내용을 저장합니다.

보안 공급자 활성화 및 비활성화

1. 쓰기 잠금을 획득합니다.
2. 활성화 또는 비활성화하려는 보안 공급자를 선택합니다.

- 비활성화된 보안 공급자를 활성화하려면 **활성화됨** 확인란을 선택합니다.
- 보안 공급자를 비활성화하려면 **활성화됨** 확인란을 선택 취소합니다.

비활성화하면 공급자 이름이 사용할 수 없는 상태가 되고 공급자 목록의 끝으로 이동합니다. 공급자 목록에서 비활성화된 공급자를 다시 정렬할 수 없습니다.

3. **저장** 단추를 클릭하여 변경 내용을 저장합니다.

처리 순서에서 보안 공급자 이동

MDM Hub은 공급자 목록에 나타난 순서대로 보안 공급자를 처리합니다. 보안 공급자가 나타나는 순서를 다시 정렬할 수 있습니다.

1. 보안 공급자 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. 공급자를 위로 이동하려면 이동할 공급자를 마우스 오른쪽 단추로 클릭하고 **공급자 위로 이동**을 선택합니다.

보안 공급자 도구가 공급자를 공급자 목록에서 이전 항목 앞으로 옮긴 다음 탐색 창을 새로 고칩니다.

4. 공급자를 아래로 이동하려면 이동할 공급자를 마우스 오른쪽 단추로 클릭하고 **공급자 아래로 이동**을 선택합니다.

보안 공급자 도구가 공급자를 공급자 목록에서 이전 항목 아래로 옮긴 다음 탐색 창을 새로 고칩니다.

공급자 속성

공급자 패널에는 다음과 같은 필드가 포함됩니다.

이름

이 보안 공급자의 이름입니다.

설명

이 보안 공급자의 설명입니다.

공급자 유형

보안 공급자 유형입니다. 유형은 다음 값 중 하나일 수 있습니다.

- 인증
- 권한 부여
- 사용자 프로필

공급자 파일

이 보안 공급자와 연결된 공급자 파일의 이름입니다. 즉 내부 공급자의 경우 **내부 공급자**입니다.

활성화

이 보안 공급자의 활성화 여부를 나타냅니다. 활성화된 보안 공급자는 선택되어 있습니다. 비활성화된 보안 공급자는 선택되어 있지 않습니다. 내부 공급자는 비활성화할 수 없습니다.

속성

이 보안 공급자의 추가 속성(보안 공급자에서 정의한 경우)입니다. 각 속성은 이름-값 쌍입니다. 보안 공급자는 여기에서 지정할 수 있는 고유한 속성을 필요로 하거나 허용할 수 있습니다.

공급자 속성 추가

공급자 속성을 추가하려면 다음 단계를 수행합니다.

1. 보안 공급자 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. 탐색 창에서 속성을 추가할 인증 공급자를 선택합니다.
4. **추가** 단추를 클릭합니다.
보안 공급자 도구에 공급자 속성 추가 대화 상자가 표시됩니다.
5. 속성의 이름을 지정합니다.
6. 이 속성에 할당할 값을 지정합니다.
7. **확인**을 클릭합니다.

공급자 속성 편집

기존 공급자 속성을 편집하려면 다음 단계를 수행합니다.

1. 보안 공급자 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. 탐색 창에서 속성을 편집할 인증 공급자를 선택합니다.
4. 편집할 각 속성에 대해 옆에 있는 **편집** 단추를 클릭하고 새 값을 지정합니다.
5. **저장** 단추를 클릭하여 변경 내용을 저장합니다.

사용자 지정 공급자

공급자 파일을 구성하는 JAR 또는 ZIP 파일에 사용자 지정 공급자 클래스를 패키징할 수 있습니다.

`providers.properties` 파일에서 사용자 지정 공급자 설정을 지정합니다. 그런 다음 `META-INF` 디렉터리의 JAR 파일 내에 파일을 배치합니다. 그러면 이 설정은 로더에 의해 **Hub** 콘솔에 표시되는 대상으로 변환됩니다.

`provider.properties` 파일에는 다음 요소가 있습니다.

ProviderList

포함된 공급자 이름의 쉼표로 구분된 목록입니다.

File-Description

패키지에 대한 설명입니다.

XXX-Provider-Name

공급자 *XXX*의 표시 이름입니다.

XXX-Provider-Description

공급자 *XXX*에 대한 설명입니다.

XXX-Provider-Type

공급자 *XXX*의 유형입니다. 가능한 값은 `USER_PROFILE_PROVIDER`, `JAAS_LOGIN_MODULE` 및 `AUTHORIZATION_PROVIDER`입니다.

XXX-Provider-Factory-Class-Name

공급자의 구현 클래스로서, 동일한 JAR 또는 ZIP 파일에도 있습니다.

XXX-Provider-Properties

공급자 속성을 정의하는 쉼표로 구분된 이름/값 쌍의 목록입니다.

참고: 공급자 보관 파일에는 사용자 지정 공급자가 제대로 기능하는 데 필요한 모든 클래스뿐만 아니라 필수 리소스도 포함되어 있어야 합니다. 이러한 리소스는 구현 환경에 따라 다릅니다.

샘플 providers.properties 파일

참고: XXX-Provider-Properties를 제외한 모든 설정이 필수입니다.

```
ProviderList=ProviderOne,ProviderTwo,ProviderThree,ProviderFour
ProviderOne-Provider-Name: Sample Role Based User Profile Provider
ProviderOne-Provider-Description: Sample User Profile Provider for roled-based management
ProviderOne-Provider-Type: USER_PROFILE_PROVIDER
ProviderOne-Provider-Factory-Class-Name:
com.siperian.sam.sample.userprofile.SampleRoleBasedUserProfileProviderFactory
ProviderOne-Provider-Properties: name1=value1,name2=value2
ProviderTwo-Provider-Name: Sample Login Module
ProviderTwo-Provider-Description: Sample Login Module
ProviderTwo-Provider-Type: JAAS_LOGIN_MODULE
ProviderTwo-Provider-Factory-Class-Name: com.siperian.sam.sample.authn.SampleLoginModule
ProviderTwo-Provider-Properties:
ProviderThree-Provider-Name: Sample Role Based Authorization Provider
ProviderThree-Provider-Description: Sample Role Based Authorization Provider
ProviderThree-Provider-Type: AUTHORIZATION_PROVIDER
ProviderThree-Provider-Factory-Class-Name:
com.siperian.sam.sample.authz.SampleAuthorizationProviderFactory
ProviderThree-Provider-Properties:
ProviderFour-Provider-Name: Sample Comprehensive User Profile Provider
ProviderFour-Provider-Description: Sample Comprehensive User Profile Provider
ProviderFour-Provider-Type: USER_PROFILE_PROVIDER
ProviderFour-Provider-Factory-Class-Name:
com.siperian.sam.sample.userprofile.SampleComprehensiveUserProfileProviderFactory
ProviderFour-Provider-Properties:
File-Description=The sample provider files
```

외부 인증

JAAS(Java Authentication and Authorization Service)를 통해 사용자에게 대한 외부 인증을 MDM Hub으로 사용할 수 있습니다.

MDM Hub은 다음과 같은 인증 표준 유형에 대한 템플릿을 제공합니다.

- LDAP(Lightweight Directory Access Protocol)
- Microsoft Active Directory
- Kerberos 프로토콜을 사용하는 네트워크 인증

이와 같은 템플릿에서는 이러한 인증 표준에 필요한 설정(예: 프로토콜, 서버 이름 및 포트)을 제공합니다. 이러한 템플릿을 사용하여 필요한 설정으로 새 로그인 모듈을 추가할 수 있습니다. 이와 같은 인증 표준에 대한 자세한 내용은 해당 공급업체 설명서를 참조하십시오.

로그인 모듈 추가

MDM Hub에서 외부 인증을 설정하려면 로그인 모듈을 생성해야 합니다.

1. 보안 공급자 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. 인증 공급자(로그인 모듈)를 마우스 오른쪽 단추로 클릭하고 **로그인 모듈 추가**를 선택합니다.
로그인 모듈 추가 대화 상자가 표시됩니다.
4. 아래쪽 화살표를 클릭하고 로그인 모듈의 템플릿을 선택합니다.

OpenLDAP-template

LDAP 인증 속성을 기반으로 합니다.

MicrosoftActiveDirectory-template

Active Directory 인증 속성을 기반으로 합니다.

Kerberos-template

Kerberos 인증 속성을 기반으로 합니다.

5. **확인**을 클릭합니다.
보안 공급자 도구의 목록에 새 로그인 모듈이 추가됩니다.
6. 속성 패널에서 편집할 속성 옆의 **편집** 단추를 클릭합니다. 생성할 로그인 모듈 유형에 대한 설정을 지정합니다.
7. **저장** 단추를 클릭하여 변경 내용을 저장합니다.

로그인 모듈 삭제

원하는 경우 로그인 모듈을 삭제할 수 있습니다.

1. 보안 공급자 도구를 시작합니다.
2. 쓰기 잠금을 획득합니다.
3. 탐색 창의 인증 공급자(로그인 모듈) 아래에서 로그인 모듈을 마우스 오른쪽 단추로 클릭하고 **로그인 모듈 삭제**를 선택합니다.
삭제를 확인하는 메시지가 나타납니다.
4. **예**를 클릭합니다.
삭제하는 로그인 모듈이 목록에서 제거되고 왼쪽 탐색 창이 새로 고쳐집니다.

제 6 장

응용 프로그램 수준 보안

이 장에 포함된 항목:

- [응용 프로그램 수준 보안 개요, 45](#)
- [Informatica Data Director, 46](#)
- [프로비저닝 도구, 47](#)
- [ActiveVOS, 47](#)
- [Dynamic Data Masking, 48](#)
- [Linux에서 WebLogic T3S 채널 설정, 50](#)
- [WebSphere 응용 프로그램 서버에서 보안 Siperian 버스 활성화, 51](#)
- [보안 Siperian 버스에 대한 cmxserver.properties 구성, 52](#)

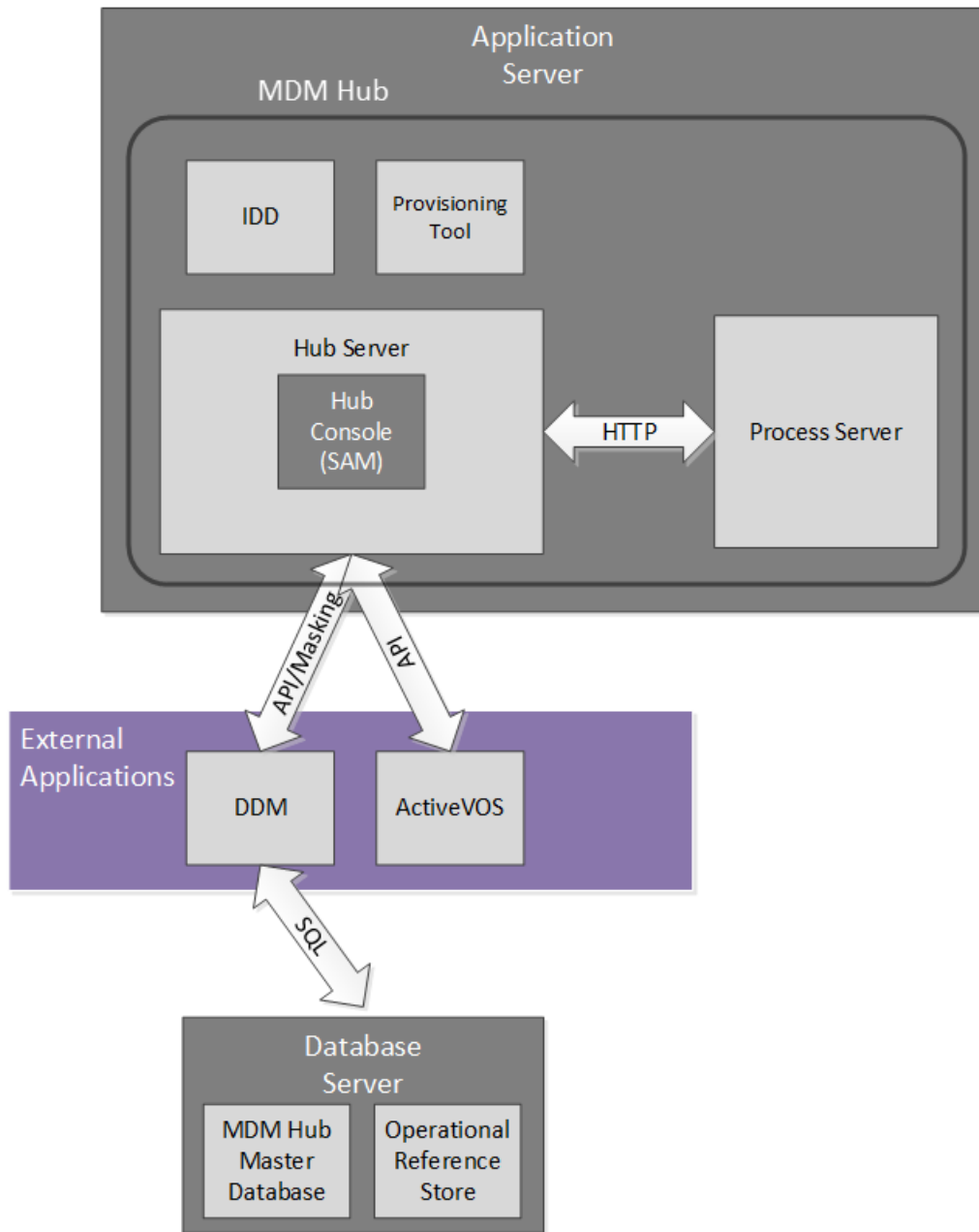
응용 프로그램 수준 보안 개요

SAM(보안 액세스 관리자)은 MDM Hub의 보안 모듈로, 사용자 자격 증명과 역할을 제어합니다. MDM Hub 구현 내의 기타 응용 프로그램과 구성 요소에도 MDM Hub와 안전하게 통신하는 데 필요한 보안 설정이 있습니다. 예를 들어 Informatica Data Director에 대해 데이터 수준의 보안을 구성할 수 있습니다.

Informatica에서는 Informatica 제품을 대상으로 내부 보안 테스트를 수행합니다. 예를 들어 Informatica에서는 업계 표준 검사 응용 프로그램을 통해 제품을 대상으로 SQL 삽입 공격 같은 보안 취약성을 테스트합니다.

SAM과 함께 사용되는 기타 Informatica 보안 응용 프로그램은 MDM Hub 구현에 추가적인 보안 기능을 제공합니다. Informatica DDM(Dynamic Data Masking)은 데이터를 마스킹하여 중요 정보에 대한 무단 액세스를 방지합니다. Informatica MDM 프로비저닝 도구 및 Informatica ActiveVOS는 보안 응용 프로그램은 아니지만 MDM Hub와 안전하게 통신합니다.

다음 이미지는 샘플 MDM Hub 구현 및 구성 요소가 서로 어떻게 연결되어 있는지 보여 줍니다.



Informatica Data Director

Informatica Data Director는 MDM Hub를 위한 웹 기반의 데이터 거버넌스 응용 프로그램입니다. Data Director 응용 프로그램을 구성하면 사용자가 마스터 데이터를 생성하고, 관리하고, 사용하고, 모니터링할 수 있습니다.

Informatica Data Director는 OWASP(Open Web Application Security Project)의 최상위 10가지 보안 권장 사항을 따릅니다. Informatica에서는 IBM Security AppScan을 사용하여 SQL 삽입 공격 같은 보안 취약성을 테스트합니다. HTTP 메서드인 GET 또는 POST는 IDD에서 정보를 검색할 수 있지만 DELETE 또는 PUT 같은 기타 HTTP 메서드는 HTTP 오류를 반환합니다.

Data Director 응용 프로그램을 구성할 때 연산 참조 저장소의 테이블을 비즈니스 항목 또는 제목 영역으로 구성할 수 있습니다. 두 접근 방식 모두 한 단위(예: 모든 고객 관련 데이터)로 처리할 관련 데이터를 그룹화하는 방법을 제공합니다. **Multidomain MDM** 버전 10.1부터는 비즈니스 항목을 조직의 접근 방식으로 사용하는 것이 좋습니다. 비즈니스 항목은 비즈니스 항목 서비스 및 최신 항목 보기를 포함하는 **Entity 360** 프레임워크의 핵심입니다.

Data Director 응용 프로그램은 보안을 위해 연산 참조 저장소에 설정된 사용자 역할 및 리소스 권한을 사용합니다. MDM 관리자는 **Hub** 콘솔에서 보안 액세스 관리자 작업 영역을 사용하여 각 사용자 역할에 대한 리소스 권한을 정의합니다. **Data Director** 응용 프로그램에서 사용자는 사용자 역할에 의해 허용되는 작업을 수행할 수 있습니다.

비즈니스 항목 및 제목 영역에 대한 역할 권한은 서로 다른 방식으로 리소스 권한에서 파생되므로 보안이 조금 다를 수 있습니다. 그러나 두 접근 방식 모두 똑같이 안전합니다. 비즈니스 항목의 보안에 대한 자세한 내용은 *Multidomain MDM 프로비저닝 도구 가이드*를 참조하십시오. 제목 영역의 보안 구성 및 데이터 보안에 대한 자세한 내용은 *Multidomain MDM Data Director 구현 가이드*를 참조하십시오.

프로비저닝 도구

프로비저닝 도구를 사용하여 **ORS**(연산 참조 저장소)에서 정의한 스키마 정보에 따라 비즈니스 항목 모델을 작성합니다. 비즈니스 항목 모델은 **Data Director**에서 **Entity 360** 프레임워크의 기초적인 구성 요소입니다.

비즈니스 항목을 구성하려면 프로비저닝 도구에 먼저 로그인해야 합니다.

구성 파일로 작업하면서 변경 내용은 임시 작업 공간에 저장됩니다. 프로비저닝 도구는 변경 내용을 게시하기 전까지 변경 내용을 적용하지 않습니다. 여러 명의 사용자가 **ORS**의 비즈니스 항목 구성을 동시에 변경하는 경우에는 가장 최근에 게시된 구성을 사용하여 **MDM Hub**가 업데이트됩니다.

프로비저닝 도구는 **Hub** 서버와 동일한 응용 프로그램 서버에서 실행되어야 합니다.

자세한 내용은 *Multidomain MDM 프로비저닝 도구 가이드*를 참조하십시오.

ActiveVOS

Informatica ActiveVOS®는 비즈니스 프로세스 자동화에 도움을 주는 **BPM**(비즈니스 프로세스 관리) 도구입니다. 사용자, 프로세스 및 시스템을 통합하는 프로세스 모델을 생성함으로써 비즈니스의 효율성을 높일 수 있습니다.

ActiveVOS는 업데이트된 레코드가 **BVT**(최선의 진실, **Best Version of the Truth**) 레코드에 제공되기 전에 업데이트된 항목 데이터가 변경 승인 워크플로우를 거치도록 보장합니다. 예를 들어 비즈니스 프로세스에서 고객 데이터에 대한 업데이트가 마스터 데이터가 되기 전에 선임 관리자의 검토 및 승인을 거쳐야 할 수 있습니다.

변경 승인 워크플로우를 지원하기 위해 **MDM Hub** 및 **Data Director**가 **ActiveVOS** 서버와 통합됩니다. 미리 정의된 **MDM** 워크플로우, 태스크 유형 및 역할을 통해 구성 요소가 서로 동기화되도록 할 수 있습니다. 포함된 **ActiveVOS** 서버와 작동하도록 **MDM** 구현을 구성할 수 있습니다. 또는 환경에서 **ActiveVOS**의 독립 실행형 인스턴스를 실행할 수도 있습니다.

포함된 **ActiveVOS**는 **MDM** 및 **ActiveVOS** 양쪽에서 트러스트하는 특정 사용자가 **Data Director** 및 **MDM Hub**에서 보내는 요청을 인증합니다. 이 사용자를 트러스트된 사용자라고 합니다. 시스템 관리자는 트러스트된 사용자의 자격 증명과 역할을 응용 프로그램 서버에서 생성합니다.

ActiveVOS 서버는 **MDM Hub**와 동일한 응용 프로그램 서버에서 실행되어야 합니다. 자세한 내용은 *Multidomain MDM 구성 가이드*를 참조하십시오.

Dynamic Data Masking

Informatica Dynamic Data Masking은 데이터 보안 제품으로서, 중요한 정보에 대한 무단 액세스를 방지하도록 클라이언트와 데이터베이스 사이에서 작동합니다. Dynamic Data Masking은 데이터베이스에 전송된 요청을 가로채서 클라이언트에 요청 결과를 보내기 전에 데이터에 마스크를 적용합니다.

Dynamic Data Masking은 MDM Hub에서 관리하는 데이터베이스에 추가적인 데이터 보안 수준을 제공합니다. Dynamic Data Masking 관리 콘솔을 사용하여 연산 참조 저장소에 대한 Dynamic Data Masking 연결을 구성하고 데이터에 대한 마스크 규칙을 설정합니다. 연산 참조 저장소를 등록할 때 Dynamic Data Masking에 대한 MDM Hub 연결을 구성합니다.

MDM 설치 프로그램은 MDM Hub과 함께 Dynamic Data Masking을 설치하지 않습니다. Dynamic Data Masking은 별도로 설치해야 합니다. Dynamic Data Masking 설치에 대한 자세한 내용은 Dynamic Data Masking 설명서를 참조하십시오.

참고: MDM Hub에서 Dynamic Data Masking을 사용하려면 Dynamic Data Masking 9.6.0 및 긴급 버그 픽스 14590이 설치되어 있어야 합니다. Dynamic Data Masking 이전 버전은 MDM Hub과 호환되지 않습니다.

Dynamic Data Masking과 MDM Hub의 통합

Dynamic Data Masking을 올바르게 설치 및 설정하면 Dynamic Data Masking과 MDM Hub을 통합할 수 있습니다.

다음 단계에서는 통합 프로세스를 설명합니다.

1. Dynamic Data Masking 관리 콘솔에서 Dynamic Data Masking 서비스를 생성합니다. 클라이언트가 데이터베이스에 요청을 보내는 포트 번호와 일치하도록 수신기 포트 번호를 구성합니다.
2. 데이터를 마스크해야 하는 데이터베이스의 데이터베이스 연결 속성을 정의합니다.
3. 연결 규칙을 생성합니다. 마스크해야 하는 데이터베이스 요청을 식별하도록 규칙을 구성합니다. 연결 규칙 집합에 데이터베이스 및 보안 규칙 집합을 할당합니다.
4. 보안 규칙 집합을 생성합니다. MDM Hub에 다시 전송된 데이터의 마스크 규칙을 정의합니다.
5. Hub 콘솔에서 Dynamic Data Masking에 대한 연결을 구성합니다.

연산 참조 저장소에 대한 프로세스를 실행하면 Dynamic Data Masking이 데이터를 MDM Hub으로 반환하기 전에 데이터베이스에 규칙을 적용합니다.

참고: 연산 참조 저장소에 대한 Dynamic Data Masking 연결을 추가하지 않으면 MDM Hub은 정의한 모든 Dynamic Data Masking 규칙을 바이패스합니다.

Dynamic Data Masking 구성 방법에 대한 자세한 내용은 *Informatica Dynamic Data Masking 관리자 가이드*를 참조하십시오.

MDM Hub에 대한 Dynamic Data Masking 모범 사례

추천 모범 사례를 통해 MDM Hub에서 Dynamic Data Masking을 효과적으로 사용할 수 있습니다.

규칙 편집기에서 Dynamic Data Masking 규칙을 생성하는 모범 사례

Dynamic Data Masking은 규칙 편집기에서 규칙을 위에서 아래로 평가합니다. 그렇기 때문에 비마스크 규칙을 생성할 때는 이를 다른 마스크 규칙보다 위에 배치해야 제대로 적용됩니다.

마스크되지 않은 데이터를 사용자가 보도록 허용하는 모범 사례

Dynamic Data Masking은 데이터베이스의 데이터를 마스크하지 않습니다. MDM Hub에서 데이터를 볼 때 데이터가 마스크되어 나타납니다. Dynamic Data Masking에서 Create View 문을 사용하여 사용자에게 마스크되지 않은 데이터를 볼 수 있는 권한을 부여합니다.

사용자를 차단하는 모범 사례

사용자가 마스킹이 적용되는 레코드를 추가하지 못하도록 차단하려면 영향을 받는 기본 개체마다 별도의 규칙을 생성해야 합니다. 텍스트 **Matcher**를 %INSERT%<BO_NAME>%<ROLE NAME>% 및 Block 문 처리 작업으로 정의합니다.

마스킹된 데이터를 사용자가 업데이트하도록 허용하는 모범 사례

기본적으로 **Dynamic Data Masking** 엔진에서 사용자는 마스킹된 데이터가 있는 테이블을 편집할 수 없습니다. **MDM Hub**에서 마스킹된 데이터를 업데이트하려면 **Dynamic Data Masking** 규칙 편집기에서 규칙을 생성하여 마스킹된 열을 사용자가 업데이트하도록 허용하면 됩니다.

MDM_SYSTEM 표시기로 규칙을 생성하는 모범 사례

MDM Hub에서 사용자 **MDM_SYSTEM**은 시스템 호출을 위한 내부 표시기입니다. **MDM_SYSTEM**은 **Hub** 콘솔의 역할 목록에 나타나지 않습니다. **Dynamic Data Masking**은 사용자에게 있는 **MDM Hub** 역할에 따라 마스킹을 적용합니다. 규칙 편집기에서 **Dynamic Data Masking** 규칙을 생성할 때 **MDM_SYSTEM** 표시기 단독 규칙은 생성하지 마십시오. **YouChart of Accounts** 설치 및 구성 가이드는 **MDM_SYSTEM**과 사용자에게 속한 사용자 이름 또는 규칙을 결합해야 합니다. **MDM_SYSTEM** 표시기를 다른 규칙과 결합하여 **Dynamic Data Masking**에서 세분화된 규칙을 생성할 수 있습니다.

연산 참조 저장소를 사용하도록 Dynamic Data Masking 설정

Hub 콘솔을 통해 연산 참조 저장소를 등록할 때 **MDM Hub**에 대한 **Dynamic Data Masking** 연결을 구성합니다.

1. **Hub** 콘솔을 시작합니다.

데이터베이스 변경 대화 상자가 표시됩니다.

2. **MDM Hub** 마스터 데이터베이스를 선택하고 **연결**을 클릭합니다.
3. 구성 작업 영역에서 **데이터베이스** 도구를 시작합니다.
4. 쓰기 잠금을 획득합니다.
5. **데이터베이스 등록** 단추를 클릭합니다.

Informatica MDM Hub 연결 마법사가 표시되어 데이터베이스 유형을 선택하라는 메시지를 표시합니다.

6. 데이터베이스 유형을 선택하고 **다음**을 클릭합니다.
7. 데이터베이스의 연결 속성을 구성합니다.
8. **포트** 필드에서 입력하는 포트는 데이터베이스의 **Dynamic Data Masking** 수신기 포트와 일치해야 합니다.
9. **DDM 연결 URL** 필드에 **Dynamic Data Masking** 서버의 URL을 입력합니다.

10. **마침**을 클릭합니다.

데이터베이스 등록 대화 상자가 표시됩니다.

11. **확인**을 클릭합니다.

MDM Hub이 연산 참조 저장소를 등록합니다.

12. 등록된 연산 참조 저장소를 선택하고 **데이터베이스 연결 테스트** 단추를 클릭하여 데이터베이스 설정을 테스트합니다.

WebSphere를 사용하는 경우 데이터베이스 연결을 테스트하기 전에 **WebSphere**를 다시 시작해야 합니다.

데이터베이스 테스트 대화 상자에 데이터베이스 연결 테스트 결과가 표시됩니다.

13. **확인**을 클릭합니다.

Dynamic Data Masking이 등록된 연산 참조 저장소에 연결됩니다.

Linux에서 WebLogic T3S 채널 설정

WebLogic T3S는 MDM Hub에 대해 설정할 수 있는 SSL 기반 프로토콜입니다.

다음 단계에서는 키 저장소 생성 및 사용 방법, SSL에 대한 서버 인스턴스 구성 방법 및 채널 생성 방법을 알고 있는 것으로 가정합니다. 자세한 내용은 WebLogic 설명서를 참조하십시오.

1. 시작하기 전에 ID 용도로 사용할 키 저장소가 있어야 합니다.
2. WebLogic 관리 콘솔에서 MDM에서 사용할 서버 인스턴스로 이동하고 다음 속성을 사용하여 SSL을 구성합니다.

- ID 및 트러스트 위치 = 키 저장소
- 개인 키 위치 = 사용자 지정 ID 키 저장소
- 개인 키 별칭 = <키 저장소에 정의된 별칭>
- 개인 키 암호 = <키 저장소에 정의된 암호>
- 인증서 위치 = 사용자 지정 ID 키 저장소
- 신뢰할 수 있는 인증 기관 = Java 표준 트러스트 키 저장소

3. 관리자 명령 프롬프트(cmd) 창을 열고 keytool 명령을 사용하여 JDK 및 JRE 디렉터리의 lib/security/cacerts로 키 저장소를 가져옵니다.

다음 샘플 코드는 구문을 보여 줍니다.

```
keytool -import -alias <SSL Private Key Alias> -keystore "<JDK installation directory>/jre/lib/security/cacerts" -file "/data/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/base_domain/servers/<WebLogic server instance>/keystores/wls12c_server.cer" -v
```

```
keytool -import -alias <SSL Private Key Alias> -keystore "<JRE installation directory>/lib/security/cacerts" -file "/data/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/base_domain/servers/<WebLogic server instance>/keystores/wls12c_server.cer" -v
```

참고: keytool 명령과 관련하여 도움이 필요한 경우 Java 설명서를 참조하십시오.

4. <WebLogic 도메인>/bin/startWebLogic.sh 파일로 이동하고 다음 Java 옵션을 설정합니다.
-Doracle.jdbc.J2EE13Compliant=true
5. WebLogic 관리 콘솔에서 SSL 구성과 일치하는 T3S 채널을 생성합니다. 다음 속성을 설정합니다.
 - 이름 = <채널 이름>
 - 프로토콜 = t3s
 - 수신 주소 = <키 저장소에 정의된 호스트 이름>
 - 수신 포트 = <키 저장소에 정의된 포트>
 - 터널링 활성화를 선택합니다.
 - 양방향 SSL을 선택합니다.
 - 서버 개인 키 별칭에 SSL을 구성할 때 지정한 별칭이 표시되는지 확인합니다.
6. 채널을 저장하고 네트워크 채널 목록에 채널이 표시되는지 확인합니다.
7. Informatica Data Director에서 Entity 360 보기를 사용하는 경우 <WebLogic 도메인>/bin/setDomainEnv.sh 파일로 이동하고 다음 MDM 옵션을 설정합니다.
 - e360.mdm.protocol=t3s
 - e360.mdm.host=<T3S 채널 수신 주소>
 - e360.mdm.port=<T3S 채널 수신 포트>
8. WebLogic을 다시 시작합니다.

9. 채널을 ping하여 테스트합니다.

```
java weblogic.Admin -url t3s://<T3S Channel Listen Address>:<T3S Channel Listen Port> -username  
<WebLogic username> -password <WebLogic password> PING
```

10. 이제 HTTPS 및 보안 포트를 사용하여 Hub 콘솔을 시작할 수 있습니다.

```
https://<T3S Channel Listen Address>:<T3S Channel Listen Port>/cmx/
```

WebSphere 응용 프로그램 서버에서 보안 Siperian 버스 활성화

Siperian 버스를 통한 보안 메시지 통신을 활성화하려면 WebSphere 콘솔을 구성한 다음 관련 `cmxserver.properties`를 구성해야 합니다.

1. WebSphere 콘솔을 엽니다.
2. 사용자 및 그룹 탭에서 새 사용자를 구성합니다.
 - a. 사용자 관리를 클릭한 다음 생성을 클릭합니다.
 - b. 새 사용자 생성 페이지에서 새 사용자를 생성하는 데 필요한 정보를 입력합니다. 이 사용자에게 어떤 권한도 할당하지 마십시오.
 - c. 생성을 클릭하여 작업을 완료합니다.
3. 서비스 통합 탭에서 설정을 구성합니다.
 - a. 버스로 이동한 다음 **SiperianBus** 링크를 클릭합니다. 구성 페이지가 표시됩니다.
 - b. 추가 속성 섹션에서 보안을 클릭합니다. 버스 > SiperianBus > 버스 > SiperianBus 버스에 대한 보안 페이지가 나타납니다.
 - c. 일반 속성 섹션에서 버스 보안 활성화 확인란을 선택합니다.
 - d. 권한 부여 정책 섹션에서 버스 커넥터 역할의 사용자 및 그룹을 클릭합니다.
 - e. 새로 만들기를 클릭하고 사용자 라디오 단추를 선택한 다음 다음을 클릭합니다.
 - f. 사용자를 선택하고 다음을 다시 클릭합니다. 요약 페이지가 표시됩니다.
 - g. 마침을 클릭합니다.
 - h. 버스 > SiperianBus > 버스 > SiperianBus 버스에 대한 보안 페이지로 돌아갑니다.
 - i. 관련 항목에서 JAAS -J2C 인증 데이터 링크를 클릭하고 새로 만들기를 클릭합니다.
 - j. 일반 속성 섹션에서 별칭, 사용자 ID 및 암호를 지정합니다. 확인을 클릭합니다.
 - k. 버스 > SiperianBus > SiperianBus 버스에 대한 보안 페이지로 돌아갑니다.
 - l. 일반 속성 섹션의 엔진 간 인증 별칭 목록에서 이 JAAS 별칭을 선택합니다. 확인을 클릭합니다.
4. 리소스 탭에서 설정을 구성합니다.
 - a. JMS > 대기열 연결 팩터리로 이동하고 연결 팩터리 링크를 클릭하여 팩터리를 엽니다. 구성 페이지가 표시됩니다.
 - b. 보안 설정 섹션의 컨테이너 관리 인증 별칭 목록에서 이전에 정의한 JAAS 별칭을 선택합니다. 확인을 클릭합니다.
 - c. JMS > 활성화 사양으로 이동한 다음 SiperianActivation 링크를 클릭합니다. 구성 페이지가 표시됩니다.
 - d. 보안 설정 섹션의 인증 별칭 목록에서 이전에 정의한 JAAS 별칭을 선택합니다. 확인을 클릭합니다.

계속해서 `cmxserver.properties` 파일의 관련 속성을 구성합니다.

보안 Siperian 버스에 대한 cmxserver.properties 구성

보안 Siperian 구성을 완료하려면 관련된 cmxserver.properties를 구성해야 합니다. 그런 다음 암호화된 암호를 생성합니다. 시작하기 전에 WebSphere 응용 프로그램 서버에서 Siperian 버스에 대한 보안을 활성화합니다.

1. MDM Hub에서 cmxserver.properties 파일을 엽니다.

- UNIX의 경우. <infadm 설치 디렉터리>/hub/server/resources
- Windows의 경우. <infadm 설치 디렉터리>\hub\server\resources

2. 다음과 같이 저장할 사용자 이름을 설정합니다.

```
siperian.mrm.jms.xaconnectionfactory.qcf.username=<사용자 이름>
```

3. 다음과 같이 저장할 암호를 설정합니다.

```
siperian.mrm.jms.xaconnectionfactory.qcf.password=<암호>
```

예를 들면 다음과 같습니다.

```
siperian.mrm.jms.xaconnectionfactory.qcf.password=ULRJz88k402EL5yDw2jypuCLaKEYHCwVg8FiNJavdfVvKnC8RFG  
IGE45IeKyQm5C2WJe2pX+ajXj1QeC/j+o7jQmItiaYoyrEMsIRWtVziHg14ZKjYbFNJcwGSC3rpURvPqH  
+WMjaEwdXxcD8p7uZ1pphc7WXkE+VouCR6kRwy0=
```

4. 다음 명령을 실행하여 암호화된 암호를 환경에 생성합니다.

```
java -classpath siperian-api.jar;siperian-common.jar;siperian-server.jar  
com.delos.util.PublicKeyBasedEncryptionHelper <plain text password> <infa home server>
```

예를 들면 다음과 같습니다.

```
java -classpath siperian-api.jar;siperian-common.jar;siperian-server.jar  
com.delos.util.PublicKeyBasedEncryptionHelper admin \<infadm installation directory>\hub\
```

제 7 장

인증서 기반 인증

이 장에 포함된 항목:

- [인증서 기반 인증 개요, 53](#)
- [인증서 기반 인증 및 외부 클라이언트, 53](#)
- [트러스트된 응용 프로그램, 54](#)
- [인증서 및 키 관리, 54](#)

인증서 기반 인증 개요

MDM Hub은 MDM Hub 구성 요소 및 트러스트된 응용 프로그램 간 통신을 보호하기 위해 인증서 기반 인증 메커니즘을 사용합니다. 이 인증 메커니즘은 SIF(서비스 통합 프레임워크) 및 비즈니스 항목 서비스 API에서도 지원됩니다.

기본적으로 인증서 로그인 모듈은 Data Director와 같은 Informatica 응용 프로그램을 트러스트된 응용 프로그램으로 간주합니다. 외부 응용 프로그램에 대해 인증서 기반 인증을 사용하려면 해당 응용 프로그램을 트러스트된 응용 프로그램으로 등록해야 합니다.

트러스트된 응용 프로그램으로 등록된 외부 응용 프로그램은 MDM Hub에 응용 프로그램 이름과 사용자 이름을 연결하여 전달합니다. 예를 들면 IDD/admin과 같습니다. 외부 응용 프로그램은 보안 페이로드도 전달해야 합니다.

인증서 기반 인증 및 외부 클라이언트

SiperianClient API와 같은 MDM Hub 외부 클라이언트는 사용자 이름 및 암호 인증을 사용하여 요청을 전송할 수 있습니다. 하지만 외부 클라이언트도 인증서 기반 인증을 사용할 수 있습니다.

MDM Hub 외부 클라이언트에 대한 인증서 기반 인증을 구성하려면 다음 단계를 수행합니다.

1. Hub 콘솔에서 외부 클라이언트와 연결된 사용자의 공용 인증서를 등록합니다.
2. 외부 클라이언트를 사용하여 요청을 트리거합니다.

트러스트된 응용 프로그램

MDM Hub에서 트러스트된 응용 프로그램에는 **admin** 사용자를 포함하여 모든 정규 MDM Hub 사용자를 대신해 요청을 실행할 수 있는 응용 프로그램 사용자라는 사용자 유형이 있습니다. 트러스트된 응용 프로그램은 MDM Hub 트러스트된 응용 프로그램 프레임워크에 속합니다.

Hub 콘솔을 사용하여 트러스트된 응용 프로그램으로 사용하려는 각 사용자 지정 응용 프로그램을 등록해야 합니다. 기본적으로 MDM Hub는 Data Director 및 ActiveVOS와 같이 MDM Hub 구현에 사용되는 Informatica 응용 프로그램을 트러스트된 응용 프로그램으로 간주합니다.

기본적으로 각 트러스트된 응용 프로그램에는 공용 및 개인 키 집합이 구성되어 있습니다. MDM Hub는 인증서 기반 인증을 통해 트러스트된 응용 프로그램의 요청을 인증합니다.

사용자 지정 응용 프로그램을 트러스트된 응용 프로그램으로 구성하려면 [“사용자 계정 추가” 페이지 29](#)를 참조하십시오.

외부 응용 프로그램을 트러스트된 응용 프로그램으로 추가

MDM Hub 트러스트된 응용 프로그램 프레임워크 외부의 응용 프로그램을 트러스트된 응용 프로그램으로 추가할 수 있습니다.

1. Hub 콘솔에서 외부 응용 프로그램에 해당하는 응용 프로그램 사용자의 사용자 계정을 추가합니다.

참고: 사용자 추가 대화 상자에서 **응용 프로그램 사용자** 확인란을 선택하고 사용자 계정의 이름에는 소문자만 사용해야 합니다.

2. 응용 프로그램 사용자 계정에 공용 인증서를 등록합니다.

3. 외부 응용 프로그램을 사용하여 요청을 트리거합니다.

참고: 인증서 기반 인증을 사용하려면 요청 이름을 <응용 프로그램 이름>/<사용자 이름>으로 설정합니다. <응용 프로그램 이름>은 1단계에 사용된 이름과 같아야 합니다. <사용자 이름>은 요청을 트리거하는 MDM Hub 사용자의 이름입니다.

인증서 및 키 관리

MDM Hub는 인증서 기반 인증을 사용합니다. 보안 위치의 각 사용자에게 대해 인증서 및 개인 키 쌍을 유지 관리해야 합니다.

기본적으로 MDM Hub는 개인 키와 인증서를 다음 위치에 보관합니다.

<MDM Hub 설치 디렉터리>/server/resources/certificates

또한 Multidomain MDM 설치 중에 사용자 지정 인증서 공급자를 구성할 수 있습니다.

사용자 지정 인증서 공급자를 구현하려면 다음 디렉터리에 있는 siperian-server-pkiutil.jar 파일에 PKIUtil.java 인터페이스를 구현해야 합니다.

<MDM Hub 설치 디렉터리>/hub/server/lib/pkiutils

사용자 지정 인증서 공급자를 사용하는 경우 PKIUtil 구현이 사용하는 키 저장소 및 공용 인증서를 유지 관리해야 합니다.

참고: 인증서 공급자를 변경하려면 Informatica 글로벌 고객 지원 센터에 연락하여 보안 구성 유틸리티를 요청하십시오.

관련 항목:

- [“보안 구성 유틸리티” 페이지 55](#)

보안 구성 유틸리티

보안 구성 유틸리티를 사용하여 MDM Hub 구현의 일부 보안 설정을 관리할 수 있습니다.

보안 구성 유틸리티를 사용하여 다음과 같은 태스크를 수행할 수 있습니다.

- 인증에 사용되는 인증서 공급자 변경
- MDM Hub의 사용자 암호 재설정
- 암호 해시에 사용되는 해시 알고리즘 변경
- 해시 알고리즘을 생성하는 데 사용되는 고객 해시 키 변경

참고: 보안 구성 유틸리티를 얻으려면 Informatica 글로벌 고객 지원 센터에 문의하십시오.

제 8 장

암호 해시

이 장에 포함된 항목:

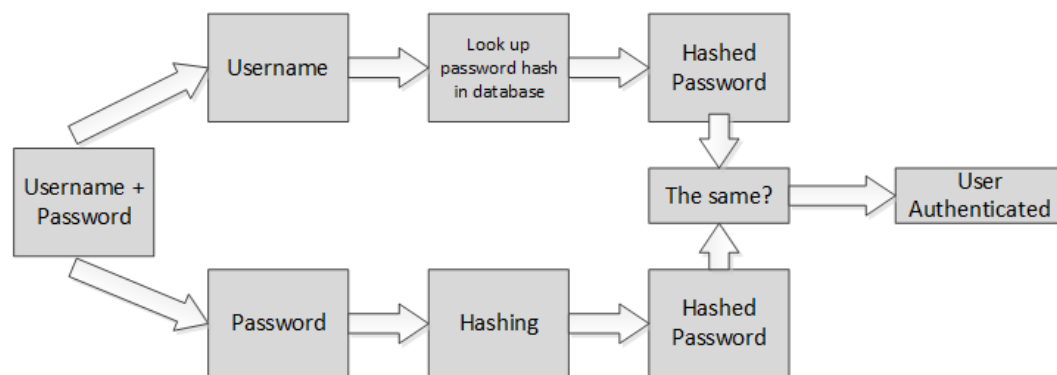
- [암호 해시 개요, 56](#)
- [암호 해시 옵션, 57](#)
- [암호 재설정 프로세스, 57](#)
- [보안 구성 유틸리티, 58](#)
- [문제 해결, 58](#)

암호 해시 개요

암호 해시는 암호화 해시 함수를 통해 암호를 되돌릴 수 없도록 암호화하는 방법입니다. MDM Hub에서는 사용자 암호를 보호하고 암호가 데이터베이스에 일반 텍스트 형태로 저장되지 않도록 하는 암호 해시 방법을 사용합니다. MDM Hub 관리자는 Hub 서버 설치 중에 알고리즘 및 고객 해시 키와 같은 암호 해시 옵션을 구성합니다.

Informatica에서는 해시 알고리즘 변경 또는 MDM Hub 사용자 암호 재설정 등 MDM Hub 구현의 일부 보안 설정을 관리하는 보안 구성 유틸리티를 제공합니다.

다음 이미지는 MDM Hub에서 사용자 암호를 인증하는 방법을 보여 줍니다.



관련 항목:

- [“보안 구성 유틸리티” 페이지 55](#)

암호 해시 옵션

Hub 서버 설치 중에 다음 암호 해시 옵션을 구성합니다.

- 해시 알고리즘의 일부로 사용자 지정 해시 키를 생성할지 여부
- 기본 SHA3 해시 알고리즘을 사용할지 아니면 사용자 지정 해시 알고리즘을 생성할지 여부
- 기본 인증서 공급자를 사용할지 아니면 사용자 지정 인증서 공급자를 사용할지 여부

SHA3 및 사용자 지정 해시 알고리즘 모두 MDM Hub 사용자의 암호를 되돌릴 수 없도록 암호화하고 데이터베이스에 일반 텍스트 형태로 저장되지 않도록 합니다. 사용하는 해시 알고리즘에 상관없이 해당 알고리즘에는 다음 구성 요소가 있습니다.

- 해시 함수
- 솔트 값
- MDM Hub 설치 동안 설정되는 선택적 페퍼 값 또는 해시 키. 이 키를 생성하고 안전하게 저장하는 것은 MDM Hub 관리자의 책임입니다.

페퍼 값을 생성하는 경우 구분자 없이 최대 32개 16진수 문자 시퀀스를 포함하는 키를 사용하는 것이 좋습니다.

중요: 데이터 유출 위험을 피하려면 해시 키의 비밀을 보호하십시오. 해시 키를 도난 당한 경우 모든 암호를 재설정해야 합니다.

암호 해시 알고리즘과 해당 알고리즘의 기본 구현은 Hub 서버 속성에 저장됩니다. Hub 서버 속성에 대한 자세한 내용은 *Multidomain MDM 구성 가이드*를 참조하십시오.

사용자 지정 해시 알고리즘

암호 재설정 프로세스

암호를 잊어버리거나 해시 알고리즘의 비밀 구성 요소 보안이 손상되었을 가능성이 있다고 생각하는 경우 암호를 재설정할 수 있습니다. 암호를 재설정하려면 Informatica 글로벌 고객 지원 센터에 문의하십시오.

암호를 재설정할 경우 임시 암호가 있는 전자 메일을 받게 됩니다. 이 암호를 사용하여 MDM Hub에 로그인한 다음 의미 있는 적절한 암호로 변경합니다. Hub 콘솔이나 Informatica Data Director를 통해 암호를 변경할 수 있습니다.

보안 구성 유틸리티

보안 구성 유틸리티를 사용하여 MDM Hub 구현의 일부 보안 설정을 관리할 수 있습니다.

보안 구성 유틸리티를 사용하여 다음과 같은 태스크를 수행할 수 있습니다.

- 인증에 사용되는 인증서 공급자 변경
- MDM Hub의 사용자 암호 재설정
- 암호 해시에 사용되는 해시 알고리즘 변경
- 해시 알고리즘을 생성하는 데 사용되는 고객 해시 키 변경

참고: 보안 구성 유틸리티를 얻으려면 **Informatica** 글로벌 고객 지원 센터에 문의하십시오.

문제 해결

문제가 발생하면 다음 정보를 사용하여 문제를 해결합니다.

MDM Hub 사용자가 로그인할 수 없음

Hub 서버를 설치한 후에 MDM Hub가 CMX_SYSTEM 스키마를 다시 생성하면 MDM Hub는 해시된 암호를 인식할 수 없습니다. 이로 인해 사용자가 MDM Hub에 로그인할 수 없습니다.

이 문제를 해결하려면 `postInstallSetup` 스크립트를 수동으로 다시 실행합니다. 이 스크립트는 MDM Hub 사용자의 암호가 다시 해시되고 사용자가 로그인할 수 있도록 해줍니다.

`postInstallSetup` 스크립트에 대한 자세한 내용은 *Multidomain MDM 설치 가이드*를 참조하십시오.

부록 A

용어

database: 데이터베이스

Hub 저장소에 구성된 데이터 컬렉션입니다. **Informatica MDM Hub**는 마스터 데이터베이스와 **ORS**(연산 참조 저장소)의 두 가지 데이터베이스 유형을 지원합니다.

Data Manager: 데이터 관리자

자동 병합을 비롯한 모든 병합 결과를 검토하고 필요한 경우 데이터 콘텐츠를 수정하는 데 사용하는 도구입니다. 이 도구는 각 기본 개체 레코드의 데이터 연계에 대한 보기를 제공합니다. 또한 데이터 관리자를 사용하여 이전에 병합한 레코드의 병합을 해제할 수 있으며, 각 통합된 레코드에 대한 다양한 유형의 기록을 볼 수 있습니다.

데이터 관리자 도구를 사용하여 레코드를 검색하고, 레코드의 교차 참조를 확인하고, 레코드 병합을 해제하고, 레코드 연결을 해제하고, 기록 레코드를 확인하고, 새 레코드를 생성하고, 레코드를 편집하고, 트러스트 설정을 재정의할 수 있습니다. 데이터 관리자는 사용자가 정의한 검색 조건과 일치하는 모든 레코드를 표시합니다.

data steward: 데이터 스튜어드

데이터 품질을 일차적으로 책임지는 **Informatica MDM Hub** 사용자입니다. 데이터 스튜어드는 **Hub** 콘솔을 통해 **Informatica MDM Hub**에 액세스하고, **Informatica MDM Hub** 도구를 사용하여 **Hub** 저장소의 개체를 구성합니다.

Dynamic Data Masking

중요한 데이터에 무단으로 액세스하지 못하도록 클라이언트와 데이터베이스 간에 작동하는 데이터 보안 제품입니다. **Dynamic Data Masking**은 데이터베이스에 전송된 요청을 가로채서 이 요청이 다시 클라이언트에게 전송되기 전에 데이터를 마스킹하도록 해당 요청에 데이터 마스킹 규칙을 적용합니다.

hierarchy: 계층

계층 관리자에서 관계 유형의 집합입니다. 이러한 관계 유형은 계층 내 항목의 위치를 기준으로 평가되지 않으며 서로 연관될 필요도 없습니다. 쉽게 분류하고 식별할 수 있도록 함께 그룹화된 관계 유형일 뿐입니다.

Hierarchy Manager

The 계층 관리자 allows users to manage hierarchy data that is associated with the records managed in the MDM Hub. For more information, see the *Multidomain MDM Configuration Guide*.

Hub Console: Hub 콘솔

관리자 및 데이터 스튜어드용 도구 집합으로 구성된 **Informatica MDM Hub** 사용자 인터페이스입니다. 사용자는 각 도구를 사용하여 특정 작업 또는 관련 작업 집합(예: 데이터 모델 작성, 일괄 작업 실행, 데이터 흐름 구성, **Informatica MDM Hub** 리소스에 대한 외부 응용 프로그램 액세스 권한 구성, 기타 시스템 구성 및 운영 태스크)을 수행할 수 있습니다.

Hub Server: Hub 서버

액세스 권한, 보안 및 세션 관리 등 핵심 및 일반 서비스에 사용되는 중간 계층(응용 프로그램 서버)의 런타임 구성 요소입니다.

Hub Store: Hub 저장소

Informatica MDM Hub 구현에서 마스터 데이터베이스와 하나 이상의 ORS(연산 참조 저장소) 데이터베이스를 포함하는 데이터베이스입니다.

Kerberos

비보안 네트워크를 통해 통신하는 노드가 서로 안전한 방법으로 ID를 증명할 수 있도록 하는 컴퓨터 네트워크 인증 프로토콜입니다. MIT(Massachusetts Institute of Technology)에서 이 프로토콜을 개발하여 Kerberos 구현을 무료로 사용할 수 있도록 했습니다.

ORS(연산 참조 저장소)

마스터 데이터와 마스터 데이터에 적용되는 규칙을 포함하는 데이터베이스입니다. 규칙에는 마스터 데이터 처리를 위한 규칙, 마스터 데이터 개체 집합 관리를 위한 규칙 및 MDM Hub가 최선의 진실을 정의할 때 사용하는 처리 규칙 및 보조 논리가 포함됩니다. MDM Hub 구성에는 하나 이상의 연산 참조 저장소가 포함될 수 있습니다. ORS의 기본 이름은 CMX_ORS입니다.

PDP(정책 결정 지점)

사용자 ID를 인증하고 사용자에게 MDM Hub 리소스에 대한 액세스 권한을 부여하는 특정 보안 검사점입니다.

PEP(정책 적용 지점)

인증 및 권한 부여 요청에 대해 런타임 시 보안 정책을 적용하는 특정 보안 확인 지점입니다.

SAM(보안 액세스 관리자)

SAM(보안 액세스 관리자)은 MDM Hub 리소스를 무단 액세스로부터 보호하는 보안 모듈입니다. 런타임 시 SAM은 MDM Hub 구현에 대해 조직의 보안 정책 결정을 적용하며 보안 구성에 따라 사용자 인증 및 액세스 권한 부여를 처리합니다.

개인 리소스

역할 도구에서 숨겨진 Informatica MDM Hub 리소스는 SIF(서비스 통합 프레임워크) 작업을 통해 액세스할 수 없습니다. Hub 콘솔에서 새 리소스를 추가한 경우(예: 새 기본 개체) 이 리소스는 기본적으로 PRIVATE로 설정됩니다.

공급자

[보안 공급자 페이지 61](#)를 참조하십시오.

구성 작업 영역

연산 참조 저장소, 사용자, 보안, 메시지 대기열 및 메타데이터 유효성 검사를 비롯하여 다양한 MDM Hub 개체를 구성하는 데 사용할 수 있는 도구가 포함되어 있습니다.

권한

MDM Hub 리소스에 액세스하는 데 필요한 권한입니다. MDM Hub 내부 권한 부여에서 각 역할에는 다음 권한 중 하나가 할당됩니다.

권한	사용자가 수행 가능한 작업....
읽기	데이터를 봅니다.
CREATE	Hub 저장소에서 데이터 레코드를 생성합니다.
UPDATE	Hub 저장소에서 데이터 레코드를 업데이트합니다.
MERGE	데이터를 병합 및 병합 해제할 수 있습니다.
EXECUTE	정리 함수 및 일괄 그룹을 실행합니다.
삭제	Hub 저장소에서 데이터 레코드를 삭제합니다.

권한은 MDM Hub 리소스에 대해 외부 응용 프로그램 사용자가 갖는 액세스 권한을 결정합니다. 예를 들어 특정 패키지 및 패키지 열에 대해 READ, CREATE, UPDATE 및 MERGE 권한이 포함되도록 역할을 구성할 수 있습니다. 이 권한은 설정이 Hub 콘솔 사용에 어느 정도 영향을 미치더라도 Hub 콘솔을 사용할 때는 적용되지 않습니다.

권한 부여

사용자에게 요청한 Informatica MDM Hub 리소스에 액세스할 수 있는 권한이 있는지 여부를 확인하는 프로세스입니다. Informatica MDM Hub에서는 역할에 리소스 권한이 할당됩니다. 사용자 및 사용자 그룹은 역할에 할당됩니다. 사용자의 리소스 권한은 사용자에게 할당된 역할과 사용자가 속해 있는 사용자 그룹에 할당된 역할에 따라 결정됩니다.

기본 개체

고객 또는 계정과 같은 비즈니스 관련 항목에 대한 정보가 포함된 테이블입니다.

메타데이터

다른 데이터를 설명하는 데 사용되는 데이터입니다. Informatica MDM Hub에서 메타데이터는 관련 구성 설정과 함께 Informatica MDM Hub 구현에 사용된 스키마(데이터 모델)를 설명하는 데 사용됩니다.

보안

Informatica MDM Hub 구현에서 무단 액세스, 무단 변경으로부터 데이터 및 기타 리소스를 보호하여 개인 정보, 기밀성 및 데이터 무결성을 보호하는 기능입니다.

보안 공급자

Informatica MDM Hub에 액세스하는 사용자에게 보안 서비스(인증, 권한 부여 및 사용자 프로필 서비스)를 제공하는 타사 응용 프로그램입니다.

보안 액세스 관리자 작업 영역

사용자, 그룹, 리소스 및 역할을 관리하는 도구를 포함합니다.

보안 페이로드

MDM Hub 작업 요청에 제공된 원시 이진 데이터로, 추가 인증 또는 권한 부여에 필요한 보조 데이터가 포함될 수 있습니다.

쓰기 잠금

Hub 콘솔에서 기본 스키마를 변경하는 데 필요한 잠금입니다. 연산 참조 저장소 보안 도구를 제외하고 데이터 스튜어드 도구가 아닌 모든 도구는 쓰기 잠금을 획득하지 않는 한 읽기 전용 모드에 있습니다. 쓰기 잠금 상태에서는 여러 명의 사용자가 동시에 스키마를 변경할 수 있습니다.

암호 정책

암호 길이, 만료, 로그인 설정, 암호 재사용 및 기타 요구 사항 등을 비롯하여 Informatica MDM Hub 사용자 계정의 암호 특성을 지정합니다. Informatica MDM Hub 구현의 모든 사용자 계정에 대해 글로벌 암호 정책을 정의할 수 있으며, 개별 사용자의 이 설정을 재정의할 수 있습니다.

역할

보안 Informatica MDM Hub 리소스에 액세스하는 데 사용되는 권한 집합을 정의합니다.

인증

사용자 ID가 본인인 주장하는 것과 일치하는지 확인하는 프로세스입니다. Informatica MDM Hub에서 사용자는 제공된 자격 증명(사용자 이름/암호, 보안 페이로드 또는 둘 모두의 조합)을 기반으로 인증됩니다. Informatica MDM Hub에서는 내부 인증 메커니즘을 제공하며 타사 인증 공급자를 사용한 사용자 인증도 지원합니다.

일괄 그룹

개별 일괄 작업(예: 준비, 로드 및 일치 작업)의 컬렉션으로, 단일 명령으로 실행할 수 있습니다. 그룹의 각 일괄 작업은 순차적으로 실행되거나 다른 작업과 병렬로 실행될 수 있습니다.

작업 영역

Hub 콘솔에서 유사한 여러 도구를 그룹화하기 위한 메커니즘입니다. 작업 영역은 관련 도구의 논리적 컬렉션입니다. 예를 들어, 모델 작업 영역에는 스키마, 쿼리, 패키지 및 매핑과 같은 데이터를 모델링하기 위한 도구가 포함되어 있습니다.

패키지

Informatica MDM Hub에서 *패키지*는 하나 이상의 기본 테이블에 대한 공용 뷰입니다. 패키지는 이러한 테이블과 이러한 테이블에 조인된 다른 테이블에 있는 열의 하위 집합을 나타냅니다. 패키지는 쿼리를 기반으로 합니다. 기본 쿼리에서는 테이블 또는 다른 패키지의 레코드 하위 집합을 선택할 수 있습니다.

프로필

계층 관리자에서 HM 사용자가 표시, 편집 또는 추가할 수 있는 필드와 레코드를 설명합니다. 예를 들어 전체 항목 및 관계에 대한 모든 읽기/쓰기 권한을 허용하는 프로필과 추가 또는 편집 작업은 허용하지 않고 읽기만 허용하는 프로필이 있을 수 있습니다.

인덱스

D

Dynamic Data Masking

개요 [10](#)

J

JDBC 데이터 소스

보안, 구성 [33](#)

N

데이터베이스

사용자 액세스 [31](#)

리소스 권한, 역할에 할당 [26](#)

리소스 그룹

추가 [21](#)

편집 [22](#)

문제 해결

암호 해시 [58](#)

보안

JDBC 데이터 소스, 구성 [33](#)

구성 [9](#)

권한 부여 [12](#)

인증 [11](#)

보안 공급자 도구

공급자 파일 [39](#)

보안 공급자 정보 [38](#)

보안 공급자 파일

보안 공급자 파일 정보 [38](#)

삭제 [40](#)

업로드 [39](#)

사용자

ORS(연산 참조 저장소)에 할당 [36](#)

개인 암호 정책 [32](#)

글로벌 암호 정책 [32](#)

데이터베이스 액세스 [31](#)

보충 정보 [30](#)

암호 설정 [31](#)

외부 응용 프로그램 사용자 [29](#)

사용자 그룹

사용자 할당 [36](#)

암호

개인 암호 [32](#)

암호 (계속)

글로벌 암호 정책 [32](#)

암호 정책

개인 암호 정책 [32](#)

글로벌 암호 정책 [32](#)

역할

역할에 리소스 권한 할당 [26](#)

편집 [25](#)

외부 응용 프로그램 사용자 [29](#)

용어 [59](#)

인증

내부 인증 [11](#)

외부 디렉터리 인증 [11](#)

외부 인증 공급자 [11](#)

인증 정보 [11](#)

O

ORS(연산 참조 저장소)

사용자 할당 [36](#)

P

providers.properties 파일

예 [43](#)

S

SAM(보안 액세스 관리자) [11](#)

Siperian 버스 [51](#), [52](#)

└

개인 암호 정책 [32](#)

공급자

사용자 지정 추가 [42](#)

권한 부여

권한 부여 정보 [12](#)

내부 권한 부여 [12](#)

외부 권한 부여 [12](#)

글로벌

암호 정책 [32](#)