

CA Identity Manager™

관리 안내서

12.6.4

도움말 시스템 및 전자적으로 배포된 매체를 포함하는 본 문서(이하 "문서")는 최종 사용자에게 정보를 제공하기 위한 것이며, CA는 언제든지 본 문서를 변경 또는 철회할 수 있습니다. 본 문서는 CA의 재산적 정보이며 CA의 사전 서면 동의 없이 본 문서의 전체 혹은 일부를 복사, 전송, 재생, 공개, 수정 또는 복제할 수 없습니다.

CA 소프트웨어의 라이선스를 허여받은 사용자들은 본인 및 그 직원들의 해당 소프트웨어와 관련된 내부적인 사용을 위해 1부의 문서 사본을 만들 수 있습니다. 단, 이 경우 복사본에는 CA 저작권 표시 및 문구 일체가 기재되어야 합니다.

본건 문서의 사본 인쇄 또는 제작 권한은 해당 소프트웨어의 라이선스가 전체 효력을 가지고 유효한 상태를 유지하는 기간으로 제한됩니다. 어떤 사유로 인해 라이선스가 종료되는 경우, 귀하는 서면으로 문서의 전체 또는 일부 복사본이 CA에 반환되거나 파괴되었음을 입증할 책임이 있습니다.

CA는 관련법의 허용 범위 내에서, 상품성에 대한 묵시적 보증, 특정 목적에 대한 적합성 또는 권리 위반 보호를 비롯하여(이에 제한되지 않음) 어떤 종류의 보증 없이 본 문서를 "있는 그대로" 제공합니다. CA는 본 시스템의 사용으로 인해 발생하는 직, 간접 손실이나 손해(수익의 손실, 사업 중단, 영업권 또는 데이터 손실 포함)에 대해서는 (상기 손실이나 손해에 대해 사전에 명시적으로 통지를 받은 경우라 하더라도) 귀하나 제 3자에게 책임을 지지 않습니다.

본건 문서에 언급된 모든 소프트웨어 제품의 사용 조건은 해당 라이선스 계약을 따르며 어떠한 경우에도 이 문서에서 언급된 조건에 의해 라이선스 계약이 수정되지 않습니다.

본 문서는 CA에서 제작되었습니다.

본 시스템은 "제한적 권리"와 함께 제공됩니다. 미합중국 정부에 의한 사용, 복제 또는 공개는 연방조달규정(FAR) 제 12.212 조, 제 52.227-14 조, 제 52.227-19(c)(1)호 - 제(2)호 및 국방연방구매규정(DFARS) 제 252.227-7014(b)(3)호 또는 해당하는 경우 후속 조항에 명시된 제한 사항을 따릅니다.

Copyright © 2014 CA. All rights reserved. 이 문서에서 언급된 모든 상표, 상호, 서비스 표시 및 로고는 각 해당 회사의 소유입니다.

CA Technologies 제품 참조

이 문서는 다음 CA Technologies 제품을 참조합니다 :

- CA CloudMinder™ Identity Management
- CA Directory
- CA Identity Manager™
- CA Identity Governance(이전 명칭 CA GovernanceMinder)
- CA SiteMinder®
- CA User Activity Reporting
- CA AuthMinder™

CA 에 문의

기술 지원팀에 문의

온라인 기술 지원 및 지사 목록, 기본 서비스 시간, 전화 번호에 대해서는 <http://www.ca.com/worldwide> 에서 기술 지원팀에 문의하십시오.

목차

제 1 장: 역할 계획

17

역할 결정	17
역할의 용도	18
추가 관리자 만들기	19
ID 또는 액세스 관리 역할	20
위임된 관리	20
역할 관리자 지정	21
위임 단계	22
위임 예제	23
역할 성격	24
역할 프로필	24
역할에 대한 태스크	24
계정 템플릿	25
구성원, 관리자 및 소유자 규칙	25
범위 규칙	27
규칙에 대한 일반 지침	30
추가 및 제거 동작	32
구성원 정책	33
관리자 정책	33
역할 계획 검사 목록	34

제 2 장: 관리자 역할

37

관리자 역할 및 관리자 태스크	37
관리자 역할 및 Identity Manager 환경	38
관리자 역할 및 사용자 콘솔	38
관리자 역할 만들기	39
관리자 역할 만들기 시작	39
관리자 역할 프로필 정의	39
역할의 관리자 태스크 선택	40
관리자 역할의 구성원 정책 정의	41
관리자 역할의 관리자 정책 정의	42
관리자 역할의 소유자 규칙 정의	43
관리자 역할 확인	43
사용자가 자신에게 역할을 할당할 수 있도록 허용	44

제 3 장: 관리자 태스크

47

관리자 작업 계획	47
관리자 작업 예제	49
관리자 작업 사용 옵션	51
기본 관리자 작업	52
사용자 지정 관리자 태스크를 만드는 방법	53
작업 프로필 정의	54
관리자 태스크 프로필 탭	55
태스크 구성 속성	59
작업 범위 정의	59
검색 화면 구성	61
작업의 탭 선택	70
계정 탭	71
일정 탭	73
작업의 필드 보기	74
역할 사용 보기	75
이벤트에 대한 워크플로 프로세스 할당	75
Active Directory 사용자 저장소 관리	75
sAMAccountName 특성	75
그룹 유형 및 범위	76
응용 프로그램 기능에 대한 외부 작업	77
외부 탭	78
외부 URL 탭	79
고급 태스크 구성 요소	80
비즈니스 로직 작업 처리기 만들기	80
관리자 태스크 및 이벤트	82
기본 및 보조 이벤트	83
태스크에 대한 이벤트 보기	83
수정되지 않은 프로필에 대해 생성된 이벤트	84
관리자 작업 처리	84
동기식 단계 처리	85
비동기식 단계 처리	86
관리자 태스크 이미지	88

제 4 장: 사용자

89

사용자 만들기	89
사용자 프로필 만들기	91
사용자에게 그룹 할당	92

사용자에게 역할 할당	93
사용자에게 서비스 할당	94
사용자가 자체 등록할 수 있도록 허용	94
자체 서비스 태스크	96
자체 서비스 태스크에 액세스	97
회사 웹 사이트에 자체 서비스 링크 포함	98
여러 개의 자체 서비스 작업 구성	100
자체 관리자 역할에 대한 액세스 제한	103

제 5 장: 암호 관리 105

Identity Manager 의 암호 관리	105
암호 정책 개요	106
암호 정책 만들기	107
추가 암호 정책 사용	107
사용자 집합에 암호 정책 적용	108
암호 만료 구성	110
암호 조합 구성	114
정규식 지정	116
암호 제한 설정	118
고급 암호 옵션 구성	122
암호 정책 관리	123
암호 정책 및 관계형 데이터베이스	123
CA CA Identity Manager 및 Siteminder 통합 암호 조건	123
암호 재설정 또는 계정 잠금 해제	124
자격 증명 공급자 설치	124
자격 증명 공급자 구성	124
자격 증명 공급자 레지스트리 설정	127
Cube 브라우저 레지스트리 설정	128
"Powered By" 메시지 사용자 지정	130
Windows 로그인에 대한 암호 재설정	131
자격 증명 공급자 자동 설치	131

제 6 장: 끝점의 암호 동기화 135

Windows 에서 암호 동기화	135
UNIX 및 Linux 에서 암호 동기화	145
OS400 에서 암호 동기화	160

제 7 장: 그룹 169

정적 그룹 만들기	169
동적 그룹 만들기	170
동적 그룹 쿼리 매개 변수	171
중첩된 그룹 만들기	173
정적, 동적 및 중첩된 그룹 예	175
그룹 관리자	176

제 8 장: 관리 끝점 계정 179

관리 끝점 통합	180
역할 정의 파일 가져오기	181
상관 관계 규칙 만들기	181
환경에 끝점 추가	185
탐색 및 상관 관계 지정 정의 만들기	185
끝점 탐색 및 상관 관계 지정	187
사용자, 계정 및 역할 동기화	188
사용자를 역할과 동기화	190
사용자를 계정 템플릿과 동기화	191
끝점 계정을 계정 템플릿과 동기화	192
끝점 계정과 리버스 동기화	196
리버스 동기화의 작동 방식	197
끝점 특성 매핑	197
리버스 동기화 정책	200
리버스 동기화를 위한 승인 태스크 만들기	204
리버스 동기화 실행	206
끝점의 사용자 지정 특성 확장	207
계정 태스크	209
끝점 계정 보기 또는 수정	209
프로비저닝된 계정 만들기	210
예외 계정 만들기	211
고아 계정 할당	211
시스템 계정 할당	212
계정 이동 태스크 화면	213
끝점 계정 삭제	213
끝점 계정에 대한 암호 변경	214
여러 계정에서 동작 수행	214
고급 계정 오퍼레이션	215
계정에 대한 전역 사용자 변경	215

자동 탐색이 동작하는 방식	216
계정을 삭제합니다.....	217
"삭제 보류"를 사용합니다.....	218
삭제된 계정 다시 만들기	218

제 9 장: 프로비저닝 역할 219

프로비저닝 역할 및 계정 템플릿	219
계정을 할당하기 위한 역할 만들기	220
계정 템플릿 만들기	222
프로비저닝 역할 만들기	223
역할 및 템플릿 태스크	224
프로비저닝 역할 가져오기	224
프로비저닝 역할에 대한 새 소유자 할당	225
프로비저닝 역할에 의해 생성된 계정의 암호.....	225
프로비저닝 역할 이벤트 처리 순서	226
환경에서 중첩된 역할 사용	228
프로비저닝 역할에 역할 포함	229
계정 템플릿의 특성	229
기능 및 초기 특성	230
계정 템플릿의 규칙 문자열	231
특성 값.....	233
고급 규칙 식.....	233
규칙 문자열과 값 결합	234
규칙 하위 문자열.....	234
다중 값 규칙 식	235
명시적 전역 사용자 특성 규칙	237
기본 제공 규칙 함수	238
프로비저닝 역할 성능	240
JAM 개체 캐시	241
세션 풀링.....	242
기존 환경에 대한 프로비저닝 태스크	242

제 10 장: 관리되는 서비스(기본 액세스 요청) 243

서비스 만들기	244
서비스 만들기 이해	246
서비스 만들기 시작.....	247
서비스 프로필 정의.....	247
서비스에 대한 관리자 정책 정의	250

서비스에 대한 소유자 규칙 정의	251
서비스에 대한 필수 조건 정의	251
서비스 갱신에 대한 전자 메일 알림 구성	252
이행 및 해지 동작 이해	253
서비스에 대한 이행 및 해지 동작 정의	253
사용자에게 서비스 할당	255
서비스 할당 확인	256
사용자에게 서비스 제공	256
사용자에게 서비스 할당	258
서비스 할당 확인	259
서비스 수정	260
액세스 요청 및 보기에 검색 추가	261
서비스 삭제	262
서비스 구성원 확인 및 제거	263
서비스 삭제	263
서비스에 대한 액세스 갱신	264

제 11 장: 동기화 267

서버 사이에서 사용자 동기화	267
인바운드 동기화	267
인바운드 동기화에 대한 장애 조치	267
아웃바운드 동기화	267
암호 동기화 사용	270
사용자 생성 또는 수정 태스크에서 사용자 동기화	270
동기화 태스크	272
사용자가 동기화되지 않는 이유	273
사용자 동기화	274
계정 템플릿 동기화	277
계정 동기화	281

제 12 장: 워크플로 283

워크플로 개요	283
WorkPoint 프로세스 다이어그램	284
워크플로 및 전자 메일 통보	285
WorkPoint 설명서	285
워크플로 제어 방법	286
워크플로 제어 - 템플릿 방법 사용	287
사전 요구 사항: 워크플로를 사용하도록 설정	288

워크플로 제어 - 템플릿 방법 아래에 관리자 태스크 배치	288
태스크 또는 이벤트 기반 워크플로	289
프로세스 템플릿의 유형	296
참여자 해결 프로그램의 유형	300
워크플로 프로세스의 전자 메일 정책 설정	305
워크플로 예: 사용자 만들기	305
WorkPoint 방법을 사용하는 방법	308
WorkPoint 관리 도구 구성	309
WorkPoint 프로세스	314
워크플로 활동	320
참여자 해결 프로그램: WorkPoint 방법	323
WorkPoint Designer 의 프로세스	334
작업 및 프로세스 인스턴스	337
워크플로 활동 수행	339
워크플로 서버에서 활동 완료	341
Workpoint 작업 보기	342
기존 승인 탭에 작업 보기 탭 추가	342
승인 태스크에서 작업 보기 탭 보기	343
EventLevel 워크플로의 워크플로 작업 보기	344
태스크 수준 워크플로에 대한 워크플로 작업 보기	344
정책 기반 워크플로	345
기본 워크플로 프로세스	346
규칙 개체	346
규칙 평가	347
정책 순서	349
정책 설명	351
승인 화면에서 변경된 특성 강조 표시	352
승인 정책 및 다중값 특성	353
워크플로 승인 화면에서 특성이 변경된 항목으로 강조 표시됨	354
정책 예	354
이벤트에 대한 정책 기반 워크플로를 구성하는 방법	357
태스크에 대한 정책 기반 워크플로를 구성하는 방법	358
승인 정책을 구성하는 방법	359
정책 기반 워크플로 상태	360
전역 이벤트 수준 정책 기반 워크플로 매핑	361
온라인 요청	365
온라인 요청 작업	365
온라인 요청 프로세스	367
온라인 요청 기록	368
온라인 요청 사용	368

워크플로 동작 단추	369
승인 작업의 워크플로 단추	370
CA Identity Manager 의 단추 구성	370
워크플로 동작 단추 추가	371
작업 목록 및 작업 항목	374
작업 목록 표시	375
작업 항목 보류	376
작업 항목 위임	377
작업 항목 재할당	383
작업 항목에 대한 대량 오퍼레이션	386

제 13 장: 전자 메일 알림 389

CA CA Identity Manager 의 전자 메일 알림	390
전자 메일 알림 방식을 선택하는 방법	391
SMTP 설정 구성	393
JBoss 에서 SMTP 설정 구성	393
WebLogic 에서 SMTP 설정 구성	394
WebSphere 에서 SMTP 설정 구성	395
전자 메일 알림 정책을 만드는 방법	396
전자 메일 알림 프로필 탭	397
보낼 조건 탭	398
받는 사람 탭	400
콘텐츠	402
전자 메일 알림 정책 수정	404
전자 메일 알림 정책 비활성화	404
사용 사례: 환영 전자 메일 보내기	405
전자 메일 템플릿을 사용하는 방법	406
전자 메일 알림 사용	407
전자 메일을 보내도록 이벤트 또는 태스크 구성	407
전자 메일 내용	409
전자 메일 템플릿	410
전자 메일 템플릿 만들기	413
사용자 지정 전자 메일 템플릿	414
전자 메일 템플릿 개발	434

제 14 장: 보고 437

구성 개요	437
보고서 프로세스	439

스냅샷 보고서를 실행하는 방법	440
보고서 서버 연결 구성	443
스냅샷 데이터베이스 연결 만들기	444
스냅샷 정의 만들기	445
예제: 사용자 권한 데이터에 대한 스냅샷 정의 만들기	447
스냅샷 관리	448
스냅샷 데이터 캡처	448
스냅샷 정의를 보고서 태스크와 연결	450
끝점 계정을 계정 템플릿과 동기화	451
관리자 태스크 예제	452
보고서 요청	454
보고서 보기	456
비스냅샷 보고서를 실행하는 방법	457
보고서 서버 연결 구성	458
보고서에 대한 연결 만들기	459
연결을 보고서 태스크와 연결	459
보고서 요청	460
보고서 보기	462
보고 옵션 설정	463
사용자 지정 스냅샷 보고서를 만들고 실행하는 방법	464
Crystal Reports 에서 보고서를 만듭니다.	466
보고서 매개 변수 XML 파일 만들기	466
보고서 및 보고서 매개 변수 XML 파일 업로드	471
보고서 태스크 만들기	473
보고서 요청	476
보고서 보기	478
사용자, 계정 및 역할 동기화	479
사용자를 역할과 동기화	481
사용자를 계정 템플릿과 동기화	482
끝점 계정을 계정 템플릿과 동기화	483
문제 해결	487
보고서를 보면 Infoview 로그인 페이지로 리디렉션됨	487
20,000 개를 초과하는 레코드에 대해 사용자 계정 생성	488

제 15 장: 아이덴티티 정책 489

ID 정책	489
ID 정책 세트 계획 워크시트	490
ID 정책 세트 만들기	491
ID 정책 세트 관리	504

사용자와 ID 정책의 동기화 방법.....	504
Identity Manager 환경의 아이덴티티 정책 세트	509
보호 ID 정책	514
보호 ID 정책 위반에 대한 동작.....	515
보호 ID 정책의 작동 방식.....	516
보호 ID 정책에 대한 중요한 참고 사항	517
보호 ID 정책 만들기.....	518
사용 사례: 사용자가 상충되는 역할을 갖지 못하도록 방지.....	519
워크플로 및 보호 ID 정책.....	520
ID 정책과 보호 ID 정책의 결합.....	525

제 16 장: Policy Xpress 527

Policy Xpress 개요.....	527
정책을 만드는 방법	528
프로필.....	529
이벤트.....	533
데이터 요소.....	534
진입 규칙.....	537
동작 규칙.....	538
고급	543

제 17 장: CA Identity Manager 모바일 응용 프로그램 545

CA Identity Manager 모바일 응용 프로그램 아키텍처	546
구현 프로세스 작동 방식	550
응용 프로그램 구성이 작동하는 방법	552
사용자 등록이 작동하는 방법	552
모바일 응용 프로그램을 지원하도록 CA Identity Manager 를 구성하는 방법.....	552
응답 특성 구성.....	553
관리자 태스크 가져오기.....	557
웹 서비스 구성 만들기	558
등록 전자 메일 수정	561
모바일 앱을 지원하도록 SiteMinder 를 구성하는 방법.....	562
모바일 앱 구성	564
추가 속성 구성	567
모바일 앱 다운로드	569
모바일 응용 프로그램 문제 해결	570

제 18 장: CA 사용자 활동 보고 통합 573

CA UAR 기능	573
CA UAR 구성 요소	573
통합 제한 사항	574
CA UAR 을 CA Identity Manager 와 통합하는 방법	574
추가 CA Enterprise Log Manager 보고서 또는 쿼리를 CA Identity Manager 와 통합.....	586
엔터프라이즈 로그 매니저 뷰어 탭 구성	587

제 19 장: 액세스 역할 591

액세스 역할이 권한을 관리하는 방법	592
예: 간접 프로필 특성 수정	592
액세스 역할 만들기	593
액세스 역할 만들기 시작	593
액세스 역할의 프로필 정의	594
액세스 역할의 구성원 정책 정의	594
액세스 역할의 관리자 정책 정의	595
액세스 역할의 소유자 규칙 정의	595

제 20 장: 시스템 작업 597

기본 시스템 작업	597
피더 파일을 사용한 사용자 추가 방법.....	599
대량 로더 고려 사항	600
피더 파일 만들기	603
로더 레코드 정보 탭	604
로더 동작 매핑 탭	605
로더 알림 정보 탭	606
대량 로더 태스크 변경 사항 승인	606
대량 로더 태스크에 대한 전자 메일 알림 구성	607
Bulk Loader 태스크 예약	608
대량 로더의 구문 분석기 파일 수정	608
Bulk Loader 를 위한 웹 서비스 지원	609
JDBC 연결 관리	610
JDBC 연결 만들기	610
논리적 특성 처리기	610
논리적 특성 처리기 만들기	611
논리적 특성 처리기 복사	612
ForgottenPasswordHandler 논리적 특성 처리기 만들기	612
논리적 특성 처리기 삭제	613

논리적 특성 처리기 수정	613
논리적 특성 처리기 보기	614
선택란 데이터	614
상관 관계 특성 구성 태스크 화면	615
이벤트에 대한 전역 정책 기반 워크플로 구성 태스크 화면	616
CA Identity Manager 의 태스크 상태	617
CA Identity Manager 가 태스크 상태를 확인하는 방법	618
제출된 태스크 보기	619
사용자 기록 탭	630
제출된 태스크 정리	636
되풀이 탭	637
제출된 태스크 정리 탭	640
되풀이 태스크 삭제	641
엔터프라이즈 로그 매니저 연결 구성	642
엔터프라이즈 로그 매니저 연결 삭제	643
비밀 키 관리	644

제 21 장: 태스크 지속 645

자동화된 태스크 지속 가비지 수집 및 아카이브	645
되풀이 탭	646
제출된 태스크 정리 탭	648
지금 작업 실행	649
새 작업 예약	649
기존 작업 수정	650
되풀이 태스크 삭제	650
태스크 지속 데이터베이스를 마이그레이션하는 방법	651
tpmigration125.properties 파일 업데이트	652
JAVA_HOME 변수 설정	652
runmigration 도구 실행	653

제 1 장: 역할 계획

역할을 계획하려면 비즈니스 또는 조직에서 필요로 하는 역할 유형과 사용자 및 응용 프로그램 액세스의 관리를 위임하는 방법을 결정해야 합니다. 이러한 결정을 기준으로 각 역할의 성격을 결정합니다.

역할을 효과적으로 사용하려면 사용자의 필요성 및 관리자 책임에 대한 다음과 같은 질문을 고려해 보십시오.

- 어떤 부서 및 조직에 관리할 사용자가 있습니까?
- 사용자에게 관리 계정에서 어떤 추가 계정이 필요합니까?
- 어떤 사용자가 다른 사용자의 관리자가 되어야 합니까?
- 누가 관리자를 관리해야 합니까?
- 각 역할에서 어떤 관리자 태스크 및 액세스 태스크가 필요합니까?
- 누가 역할 및 태스크를 만듭니까?
- 역할을 어떻게 사용하여 작업을 위임할 수 있습니까?

마지막 질문은 사용자 관리 및 응용 프로그램 액세스 권한 부여 작업을 공유하는 것과 관련됩니다. 위임 모델에 대한 자세한 내용은 위임된 관리를 참조하십시오.

이러한 질문에 대한 답을 기초로 얼마나 많은 어떤 유형의 역할이 필요한지 결정할 수 있습니다.

이 섹션은 다음 항목을 포함하고 있습니다.

[역할 결정](#) (페이지 17)

[역할의 용도](#) (페이지 18)

[추가 관리자 만들기](#) (페이지 19)

[역할 성격](#) (페이지 24)

[역할 계획 검사 목록](#) (페이지 34)

역할 결정

다음 절은 역할 결정에 도움을 주기 위한 정보를 설명합니다.

역할의 용도

역할을 효과적으로 사용하려면 사용자의 필요성 및 관리자 책임에 대한 다음과 같은 질문을 고려해 보십시오.

- 어떤 부서 및 조직에 관리할 사용자가 있습니까?
- 사용자에게 관리 계정에서 어떤 추가 계정이 필요합니까?
- 어떤 사용자가 다른 사용자의 관리자가 되어야 합니까?
- 누가 관리자를 관리해야 합니까?
- 각 역할에서 어떤 관리자 태스크 및 액세스 태스크가 필요합니까?
- 누가 역할 및 태스크를 만듭니까?
- 역할을 어떻게 사용하여 작업을 위임할 수 있습니까?

마지막 질문은 사용자 관리 및 응용 프로그램 액세스 권한 부여 작업을 공유하는 것과 관련됩니다. 위임 모델에 대한 자세한 내용은 위임된 관리를 참조하십시오.

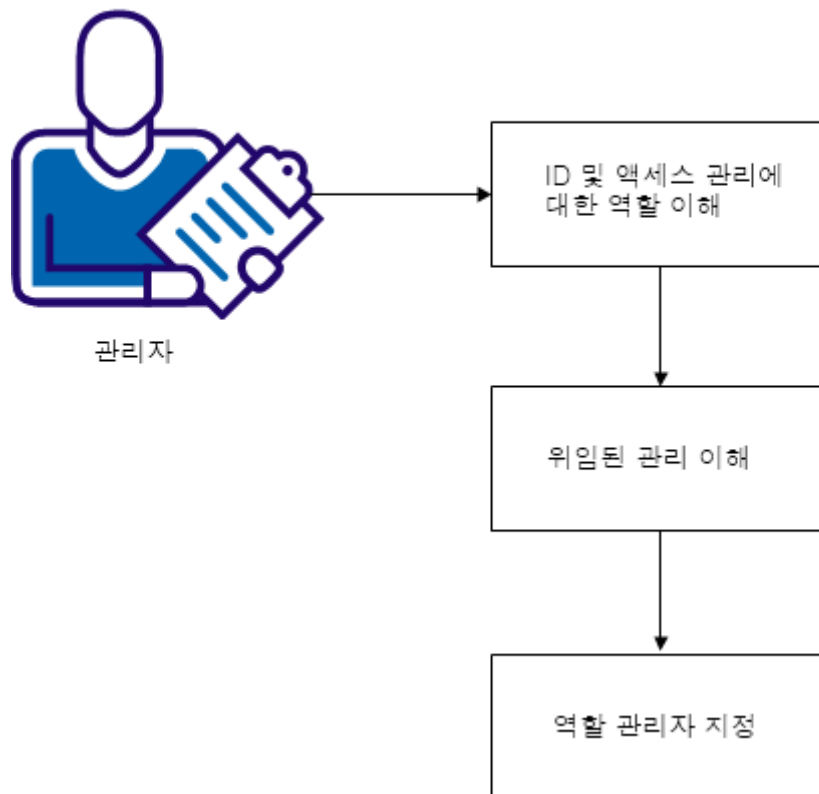
이러한 질문에 대한 답을 기초로 얼마나 많은 어떤 유형의 역할이 필요한지 결정할 수 있습니다.

추가 관리자 만들기

단독으로 시스템의 사용자에게 모든 역할을 부여하는 일을 수행할 수 있지만 추가 관리자를 지정하여 사용자 역할을 부여하는 일을 분담할 수도 있습니다. 이 방법을 *위임된 관리*라고 합니다.

다음 다이어그램에서는 추가 관리자를 만들기 위해 이해해야 할 정보와 수행해야 할 단계를 보여 줍니다.

추가 관리자 만들기



다음 항목에서는 추가 관리자를 만드는 방법을 설명합니다.

- [ID 또는 액세스 관리 역할](#) (페이지 20)
- [위임된 관리](#) (페이지 20)
- [역할 관리자 지정](#) (페이지 21)

ID 또는 액세스 관리 역할

사용자 ID 관리와 다른 계정에 대한 사용자 액세스 관리를 사용하도록 설정하기 위해 CA CloudMinder 는 두 가지 역할을 제공합니다. 관리자 역할이 부여된 사용자는 사용자 암호나 그룹 구성원 자격을 수정하는 것과 같이 사용자를 관리할 수 있습니다. 관리자 역할에는 사용자 콘솔에 나타나는 태스크가 포함될 수도 있습니다. 프로비저닝 역할이 부여된 사용자는 전자 메일 시스템과 같은 다른 비즈니스 응용 프로그램에 액세스할 수 있습니다.

역할에 대한 추가 정보가 다음 표에 나와 있습니다.

역할 유형	목적
관리자 역할	사용자 관리 태스크와 같이 해당 역할이 부여된 사용자가 CA CloudMinder 에서 수행할 수 있는 관리자 태스크를 포함하고 있습니다.
프로비저닝 역할	전자 메일 시스템과 같이 관리 끝점에 있는 계정을 정의하는 계정 템플릿을 포함하고 있습니다. 또한 계정 템플릿은 사용자 특성이 해당 계정에 매핑되는 방법을 정의합니다.
액세스 역할	액세스 역할은 CA Identity Manager 또는 다른 응용 프로그램에서 권한을 제공하는 추가적인 방법을 제공합니다. 예를 들어 액세스 역할을 사용하여 다음 작업을 수행할 수 있습니다. ■ 사용자 특성에 대한 간접 액세스를 제공합니다. ■ 복합 식을 만듭니다. ■ 다른 응용 프로그램이 권한을 결정하는 데 사용할 수 있는 프로필 특성을 설정합니다.

위임된 관리

위임된 관리는 역할을 사용하여 사용자를 관리하고 응용 프로그램 액세스 권한을 부여하는 일을 공유하는 것입니다.

시스템의 각 역할에 대해 사용자는 다음 직능을 하나 이상 수행할 수 있습니다.

직능	정의
역할 소유자	역할을 수정합니다.
역할 관리자	사용자와 다른 역할 관리자에게 역할을 할당합니다.
역할 구성원	역할을 사용하여 관리자 또는 액세스 태스크를 수행하거나 끝점 계정을 사용합니다.

이러한 직능을 사용자 간에 나누어 역할을 관리하는 일을 분담할 수 있습니다. 예를 들어 하위 관리자는 역할 구성원 자격을 관리하고 상위 관리자는 역할을 수정하도록 할 수 있습니다.

다음과 같은 방법으로 위임된 관리를 구현할 수 있습니다.

- 사용자를 지정된 역할의 관리자로 직접 지정합니다.
- 역할의 *관리자 규칙*을 구성합니다. 관리자 규칙은 역할의 관리자가 될 수 있는 사용자를 정의합니다. 사용자가 규칙에서 지정한 조건을 충족하면 추가 관리자가 자동으로 생성됩니다.

참고: 역할을 수정할 수 있는 권한을 가진 관리자만 해당 역할의 관리자 규칙을 구성할 수 있습니다. 일반적으로 시스템 관리자가 이 활동을 수행합니다. 역할의 관리를 자동으로 위임하는 관리자 규칙을 구성하려면 온라인 도움말의 "Reference Information"(참조 정보) 섹션에 있는 "Admin Roles"(관리자 역할) 섹션을 참조하십시오.

역할 관리자 지정

사용자를 역할의 관리자로 지정할 수 있습니다. 그러면 관리자가 다른 사용자에게 역할을 할당할 수 있습니다.

다음 단계를 수행하십시오.

1. 역할 관리 태스크를 가진 사용자로 사용자 콘솔에 로그인합니다.
2. "태스크", "역할 및 태스크"를 선택합니다.
3. 다음 태스크 중 하나를 선택합니다.
 - 관리자 역할, 관리자 역할 구성원/관리자 수정
 - 프로비저닝 역할, 프로비저닝 역할 구성원/관리자 수정
 - 액세스 역할, 액세스 역할 구성원/관리자 수정

검색 화면이 나타납니다.

4. 사용자에게 할당할 역할을 선택합니다.
5. "관리자" 탭을 클릭합니다.

현재 역할 관리자 목록이 나타납니다.

6. "사용자 추가"를 클릭합니다.

검색 화면이 나타납니다.

7. 관리자로 추가할 사용자를 검색하고 "선택"을 클릭합니다.

업데이트된 역할 관리자 목록이 나타납니다.

8. 제출을 클릭합니다.

사용자가 역할의 관리자가 됩니다. 이 단계에서는 프로비저닝 역할의 관리를 위임하는 프로세스를 수행합니다. 이제 관리자가 다른 사용자에게 역할을 할당하고 연결된 끝점 계정에 대한 액세스 권한을 부여할 수 있습니다.

위임 단계

역할의 용도를 기준으로 역할의 사용에 대해 결정한 다음에는 다음과 같이 위임된 관리가 수행됩니다.

1. 관리자는 누가 역할 소유자, 관리자, 구성원인지에 대한 규칙을 사용하여 역할을 만듭니다.
2. 역할 소유자는 변경이 필요할 때 역할을 수정합니다.

3. 역할 관리자:

- 관리자에게 역할을 추가로 할당합니다(선택 사항).
- 구성원에게 역할을 추가로 할당합니다(선택 사항).

일부 사용자는 역할에 정의된 규칙을 충족시킴으로써 이미 역할 관리자 또는 구성원이 되어 있습니다.

4. 역할 구성원이 역할을 사용합니다.

- 관리자 역할 구성원이 **Identity Manager** 환경에서 사용자와 다른 개체를 관리합니다.
- 액세스 역할 구성원이 비즈니스 응용 프로그램에서 직능을 수행합니다.
- 프로비저닝 역할 구성원이 역할의 정책에 의해 정의된 계정을 사용합니다.

위임 예제

누가 구성원 또는 관리자가 될 수 있는지에 대한 규칙을 사용하여 역할을 만들 수 있습니다. 그런 다음 다른 사용자(규칙을 이미 충족시키지 않은 사용자)가 역할 구성원 또는 관리자가 될 수 있도록 역할을 할당할 수 있습니다.

최종 사용자의 비즈니스 응용 프로그램 권한을 관리하는 관리자의 다음 예제를 참고하십시오.

- **Jeff** 는 **Accountant** 역할의 역할 소유자이므로 이 역할을 변경해야 하는 경우 **Jeff** 는 역할을 수정합니다.
- **David** 와 **Lisa** 는 이 역할의 역할 관리자입니다. 이들은 관련 사용자를 역할 구성원으로서 할당합니다.
- 다른 사용자들은 역할 구성원으로서 할당되지 않은 역할 구성원입니다. 대신, 이들은 역할 구성원이 되기 위한 규칙을 충족시킵니다.

이 역할 구성원들은 **Accountant** 역할을 사용하여 구매 주문서를 발행하고 재무 응용 프로그램에서 기타 태스크를 수행합니다.

규칙 및 역할의 기타 성격에 대한 자세한 내용은 역할 성격 절에 설명되어 있습니다.

역할 성격

역할을 만들 때는 다음 표에 설명된 것처럼 성격을 정의합니다.

성격	정의
역할 프로필	역할의 일반 성격입니다.
태스크	관리자 역할의 태스크입니다.
계정 템플릿	프로비저닝 역할에 대해 관리 끝점에서 계정을 정의하는 템플릿입니다.
구성원 규칙, 구성원 정책	구성원 규칙은 사용자가 액세스 또는 관리자 역할 구성원이 되기 위한 조건을 정의합니다. 구성원 정책은 구성원 규칙과 범위 규칙을 결합합니다. 참고: 프로비저닝 역할에는 구성원 규칙과 정책이 없습니다. 사용자를 구성원으로 만들려면 "프로비저닝 역할 구성원/관리자 수정"을 사용합니다.
관리자 규칙, 관리자 정책	■ 관리자 규칙은 사용자가 역할 관리자가 되기 위한 조건을 정의합니다. ■ 관리자 정책은 관리자 규칙을 범위 규칙 및 규칙 할당을 위한 관리자 권한과 결합합니다.
소유자 규칙	사용자가 역할 소유자가 되기 위한 조건입니다.
범위 규칙	역할에 의해 관리될 수 있는 개체에 대한 제한입니다.
동작 추가, 동작 제거	사용자가 역할 구성원 또는 관리자로서 추가 또는 제거될 때 사용자 프로필의 변경 사항입니다.

역할 프로필

역할 프로필은 역할의 이름과 설명, 역할이 사용되는지 여부를 나타냅니다. 사용되는 경우 역할은 만든 즉시 사용할 수 있습니다.

역할에 대한 태스크

관리자 역할의 경우, 하나 이상의 범주로부터 하나 이상의 관리자 태스크(외부 태스크를 포함)를 선택할 수 있습니다.

계정 템플릿

각 프로비저닝 역할은 계정 템플릿을 포함하고 있습니다. 이 템플릿은 관리 끝점에 있는 계정을 정의합니다. 예를 들어, **Exchange** 계정에 대한 끝점은 사서함의 크기를 정의할 수 있습니다. 이 계정 템플릿은 또한 계정에 사용자 특성이 매핑되는 방법을 정의합니다.

각 끝점 유형에 대해 하나 이상의 끝점을 선택할 수 있습니다. 역할이 할당된 사용자는 끝점에서 계정을 받습니다.

구성원, 관리자 및 소유자 규칙

각 역할에는 해당 역할의 구성원, 관리자 또는 소유자일 수 있는 사람에 대한 규칙이 포함되어 있습니다. 따라서 사용자는 하나 또는 여러 역할의 구성원이거나 역할이 없을 수 있습니다.

구성원, 관리자 및 소유자 규칙은 다음 표의 조건을 사용합니다.

규칙 조건	예제	규칙 구문
사용자가 하나의 특성값과 일치해야 합니다.	직책이 선임으로 시작하는 사용자	조건: <사용자-필터>
사용자가 여러 특성값과 일치해야 합니다.	직책=관리자 및 지역=동부인 사용자	조건: <사용자-필터>
사용자가 명명된 조직에 속해야 합니다.	영업 및 하위 조직 내 사용자	다음에 속함: <조직-규칙>
사용자가 조직의 특성에 의해 지정된 조건을 충족하는 조직에 속해야 합니다.	비즈니스 유형=금 또는 백금인 조직 내 사용자	조직 내 조건: <조직-필터>
사용자가 특정 조직에 속하고 특정 사용자 특성과 일치해야 합니다.	직책=관리자 및 지역=동부이고 영업 또는 마케팅 조직 내 사용자	조건: <사용자-필터> 및 다음에 속해 있는 사람: <조직-규칙>

규칙 조건	예제	규칙 구문
사용자가 특정 그룹에 속해야 합니다.	401K 그룹의 구성원인 사용자	다음의 구성원인 사람: 그룹 <그룹>
사용자가 역할의 구성원이어야 합니다.	헬프 데스크 역할의 구성원인 사용자	다음의 구성원인 사람: <역할-규칙>
사용자가 역할의 관리자여야 합니다.	영업 관리자 역할의 관리자인 사용자	다음의 관리자인 사람: <역할-규칙>
사용자가 역할의 소유자여야 합니다.	사용자 관리자 역할의 소유자인 사용자	다음의 소유자인 사람: <역할-규칙>
사용자가 그룹의 특성에 의해 지정된 조건을 충족하는 그룹에 속해야 합니다.	소유자=CIO 인 그룹의 구성원인 사용자	다음의 구성원인 사람: 그룹 <그룹-필터>
사용자가 LDAP 쿼리를 기반으로 조건을 충족해야 합니다.	Identity Manager 사용자 콘솔에서 만든 쿼리가 충분하지 않은 경우에 LDAP 디렉터리를 사용합니다.	<LDAP-쿼리> 쿼리에 의해 반환된 사용자

일부 규칙에서는 값을 다중값 특성과 비교해야 할 수도 있습니다. 규칙을 적용하려면 다중값 특성의 값이 하나 이상 이 규칙을 충족해야 합니다. 예를 들어, 규칙이 특성 A 가 1 과 같음이고 사용자 X 에 대한 특성 A 값이 1, 2, 3 이면 사용자 X 는 조건을 충족합니다.

역할을 만드는 사용자가 역할을 수정하지 못할 수도 있습니다. 역할을 수정하기 위해서는 해당 사용자가 소유자 규칙의 조건을 충족해야 합니다.

참고: 대규모 구현일 경우 구성원, 관리자 및 소유자 규칙을 평가하는 데 오랜 시간이 걸릴 수 있습니다. 메모리 내 평가 옵션을 사용하여 사용자 특성이 포함된 규칙에 대한 평가 시간을 줄일 수 있습니다. 자세한 내용은 *Configuration Guide*(구성 안내서)를 참조하십시오.

범위 규칙

구성원 및 관리자 규칙을 범위 규칙과 결합합니다. *범위 규칙*은 역할이 사용될 수 있는 개체를 제한합니다.

- 역할 구성원의 경우, 범위 규칙은 이 역할을 사용하여 관리할 수 있는 개체를 제어합니다.
- 역할 관리자의 경우, 범위 규칙은 역할 구성원 및 관리자가 될 수 있는 사용자를 제어합니다.

범위는 태스크의 기본 개체에 적용됩니다. 예를 들어, 사용자가 "사용자 만들기" 태스크의 기본 개체입니다. 하지만 그룹이 보조 개체이므로 범위가 해당 사용자의 그룹에 적용되지 않습니다.

대부분의 개체 유형에 대해 다음 테이블에 범위 규칙의 유형을 지정할 수 있습니다.

규칙 조건	예	규칙 구문
모두	Role members can manage all objects	All
개체가 하나 이상의 특성 값과 일치해야 합니다.	Users where title starts with senior	where <filter>

필터 옵션을 선택할 때 CA Identity Manager 는 두 가지 유형의 필터를 표시합니다.

<attribute> <comparator><value>

개체 프로필의 특성이 특정 값과 일치해야 합니다.

<attribute> <comparator> admin's <user-attribute>

개체 프로필의 특성이 관리자의 프로필에 있는 특성과 일치해야 합니다.

예: Users where manager = admin's UserID.

다음 표에 설명된 추가 옵션은 사용자, 그룹, 조직 개체에 사용할 수 있습니다.

참고: 다음 사용자 범위 규칙은 예제입니다. 관리자 및 관리자가 관리할 수 있는 사용자 사이의 다른 관계를 처리하기 위한 다른 규칙을 만들 수 있습니다.

규칙 조건	예	규칙 구문
사용자가 하나의 특성 값과 일치해야 합니다.	Users where member of group sales or cell phone does not equal null	where <user-filter>
사용자가 여러 특성 값과 일치해야 합니다.	Users where title=manager and locality=USA	where <user-filter>
사용자가 명명된 조직에 속해야 합니다.	Users in organization Australia or New Zealand 참고: 조직 범위 규칙은 규칙을 충족하는 조직의 하위 조직에 적용됩니다. 예를 들어, 조직 규칙이 "in Organization1"인 경우 범위 규칙은 Organization1.1 및 Organization1.2 에 적용되지만 Organization1 에 적용되지 않습니다.	in <org-rule>

규칙 조건	예	규칙 구문
사용자가 조직의 특성에 의해 지정된 조건을 충족하는 조직에 속해야 합니다.	Users in organizations where Business Type=gold or platinum	in organizations where <org-filter>
사용자가 특정 조직에 속하고 특정 사용자 특성과 일치해야 합니다.	Users where title=manager and locality=east and who are in organization sales or organization marketing	조건: <사용자-필터> 및 다음에 속해 있는 사람: <조직-규칙>
사용자 프로필의 특성이 관리자 프로필의 특성과 일치해야 합니다.	Users where manager = admin's UserID	where <user-attribute> <comparator> admin's <user-attribute> 참고: 다중값 특성에 같지 않음 비교 연산자를 사용하지 마십시오.
사용자가 관리자로서 동일한 조직에 있습니다.	Users in the organization where Jeff (the administrator) is a member	admin's organization
사용자가 관리자의 특성에 나열된 조직에 있습니다.	Users in sales or marketing	organization that is a value in admin's <admin-attr>

참고: 다음 그룹 범위 규칙은 단지 예제일 뿐입니다. 관리자 및 관리자가 관리할 수 있는 그룹 사이의 다른 관계를 처리하기 위한 다른 규칙을 만들 수 있습니다.

규칙 조건	예	규칙 구문
그룹이 하나의 특성과 일치해야 합니다.	Group name where Group name = 401K	where <group-filter>
그룹이 명명된 조직에 속해야 합니다.	Groups in organization accounting and lower	in <org-rule>

규칙 조건	예	규칙 구문
그룹이 하나의 특성 값에 일치하고 명명된 조직에 속해야 합니다.	Groups where BusinessType = finance and who are in organization sales and lower	where <group-filter> and who are in <org-rule>
그룹이 관리자의 특성에 나열되어 있어야 합니다.	Groups where Description = Engineering	where <group-attribute> <comparator> admin's <user-attribute> 참고: 다중값 특성에 같지 않음 비교 연산자를 사용하지 마십시오.

참고: 다음 조직 범위 규칙은 단지 예제일 뿐입니다. 관리자 및 관리자가 관리할 수 있는 조직 사이의 다른 관계를 처리하기 위한 다른 규칙을 만들 수 있습니다.

규칙 조건	예	규칙 구문
조직이 하나의 특성 값과 일치해야 합니다.	organizations where org Name=finance	where <org-filter>
조직이 명명된 조직에 속해야 합니다.	organizations in finance and lower	in <org-rule>
조직이 하나의 특성 값과 일치하고 명명된 조직에 속해야 합니다.	organizations where org Name=finance and are in finance and lower	where <org-filter> and are in <org-filter>

규칙에 대한 일반 지침

만드는 규칙 유형에 관계없이 Identity Manager 가 이러한 유형을 처리하는 방식을 알고 있어야 합니다.

연산자의 평가

역할에 대한 규칙을 만들 때는 `>=`, `<=`, `<`, `>` 연산자를 포함할 수 있습니다. 하지만 이러한 연산자는 LDAP 디렉터리 또는 관계형 데이터베이스에서 문자열로 평가됩니다. 대부분의 사용자 저장소는 사전순으로 문자열을 비교합니다. 따라서 가령 500 과 1100 을 비교할 때 5 가 1 보다 크므로 사용자 저장소가 500 이 더 크다고 결정할 수 있습니다.

사용자 저장소에서 문자열이 비교되는 방식을 변경할 수도 있습니다. 자세한 내용은 LDAP 디렉터리 서비스 또는 관계형 데이터베이스 소프트웨어에 대한 설명서를 참조하십시오.

CA Identity Manager 는 OR 문을 먼저 처리한 다음 AND 문을 처리합니다. 다음 예제를 참조하십시오.

```
where(company=CA and city=Boston or city=Framingham)
```

이 예에서 CA Identity Manager 는 (Boston or Framingham)을 먼저 처리한 다음 company=CA 와의 논리적 AND 를 수행합니다.

규칙의 대소문자 구분

관리자 또는 액세스 역할을 만들 때 사용자 저장소에 따라 이 규칙을 평가할 때 대소문자를 구분하거나 구분하지 않을 수 있습니다.

하지만 생성 또는 수정 오퍼레이션의 끝에서 사용자 저장소에 변경 사항을 커밋하기 전에 규칙이 내부적으로 대소문자를 구분하지 않고 평가됩니다. 예를 들어, 규칙에 `title=manager` 인 조건이 있는 경우 규칙은 `title` 값이 `manager` 또는 `Manager` 인 사용자 저장소 개체와 일치합니다.

추가 및 제거 동작

관리자가 역할을 부여하거나 해지할 때 Identity Manager 가 역할의 멤버십을 올바르게 관리하려면 추가 및 제거 동작을 지정해야 합니다.

- 사용자가 역할의 구성원 규칙 중 하나에 포함된 조건을 충족하도록 "추가 동작"을 사용해야 합니다. 예를 들어, 사용자 매니저 역할에 대한 구성원 규칙이 역할 구성원은 관리자 역할 특성의 값이 "사용자 매니저"라고 지정하는 경우 "추가 동작"은 관리자 역할 특성에 "사용자 매니저"를 추가해야 합니다.
- "제거 동작"은 규칙이 해지될 경우 해당 사용자가 더 이상 구성원 규칙과 일치하지 않도록 사용자의 프로필을 변경해야 합니다.

각 역할에는 두 개의 추가 동작과 두 개의 제거 동작이 있습니다.

관리자가 역할의 구성을 추가 및 제거할 수 있는 경우 추가 또는 제거 동작을 정의합니다. 그렇지 않은 경우, 구성원 규칙을 충족함으로써(예를 들어, RoleAdmins 그룹에 속함으로써) 사용자는 해당 역할을 갖습니다. 예:

- 역할 A 는 관리자가 할당할 수 있으므로 추가 또는 제거 동작이 정의됩니다.
- 역할 B 는 그룹 "finance"의 모든 구성원이 역할을 갖는 규칙이 있습니다. 이 역할은 할당될 수 없으므로 추가 또는 제거 동작이 없습니다.

추가 및 제거 동작을 정의할 때는 관리자 역할 특성을 사용하는 것을 고려하십시오. Identity Manager 는 이 특성을 사용하여 사용자의 여러 역할을 저장할 수 있습니다. 예를 들어, 사용자가 '직원' 역할의 구성원으로 추가될 때 사용자의 '관리자 역할' 특성에 '직원'을 추가하는 추가 동작을 구성할 수 있습니다. 관리자가 '자체 관리자' 및 '사용자 매니저' 역할이 이미 있는 매니저에게 '직원' 역할을 할당하는 경우 이 매니저의 '관리자 역할' 특성은 다음 값을 포함하게 됩니다: 자체 관리자, 사용자 매니저, 직원

관리자 역할 특성을 사용하려면 %ADMIN_ROLE_CONSTRAINT% 일반 특성이 사용자 프로필에서 다중 값이 있는 특성에 매핑되어야 합니다. 자세한 내용은 *CA Identity Manager Configuration Guide*(CA Identity Manager 구성 안내서)를 참조하십시오.

중요! 추가 동작을 정의할 때는 정의 중인 역할을 참조하는 규칙을 설정하지 마십시오. 예를 들어, 역할 A 의 구성원이 됨으로써 역할 A 의 구성원이 되는 추가 동작을 정의하지 마십시오. 이렇게 하면 재귀 오류가 발생하여 정책 서버를 다시 시작해야 합니다.

구성원 정책

구성원 정책은 사용자가 구성원 규칙을 충족하는 경우 해당 사용자가 이 정책에 정의된 범위를 가짐을 나타냅니다. 다음 그룹은 두 개의 구성원 정책이 있는 역할을 보여 줍니다.

- 첫 번째 정책은 역할 구성원에 매니저 Jones 가 있으면 이 구성원이 Sales Office 의 사용자에게 이 역할을 사용하고 401k 그룹의 구성원으로서 이들을 관리할 수 있음을 나타냅니다.
- 두 번째 정책은 역할 구성원이 Bend 시에 위치한 경우 이 역할 구성원이 Oregon 주의 사용자에게 이 역할을 사용하고 Group Admin 이 Smith 인 그룹의 구성원으로서 이들을 관리할 수 있음을 나타냅니다.

Member Policies

	Member Rule	User Scope Rule	Group Scope Rule
▶	where (Manager = "Jones")	where (Office = "Sales")	where (Group Name = "401K")
▶	where (City = "Bend")	where (State = "OR")	where (Group Admin = "Smith")

관리자 정책

관리자 정책은 사용자가 관리자 규칙을 충족하는 경우 해당 사용자가 이 정책에 정의된 사용자 범위 및 관리자 권한을 가짐을 나타냅니다. 사용자 범위는 역할이 사용되는 곳을 정의합니다. 관리자 권한은 역할 관리자가 구성원을 관리할 수 있는지 또는 역할의 관리자를 관리할 수 있는지 여부를 결정합니다.

다음 그림은 다음과 같이 정의된 두 개의 관리자 정책을 갖는 역할을 보여줍니다.

- 첫 번째 정책의 경우, IT Admin 은 Boston 시에 위치한 사용자에게 대해 역할 구성원 및 관리자를 추가 및 제거할 수 있습니다.
- 두 번째 정책의 경우, Sales 의 관리자는 Ohio 주에 위치한 구성원을 추가 및 제거할 수 있습니다.

Admin Policies

	Admin Rule	User Scope Rule	Manage Members	Manage Administrators	
▶	where (Employee Type = "IT Admin")	where (City = "Boston")	☒	☒	⊖
▶	where (Office = "Sales")	where (State = "Ohio")	☒	☒	⊖

역할 계획 검사 목록

역할을 만들기 전에 역할 성격에 대한 다음 검사 목록을 사용하십시오.

역할 성격	자세한 내용
역할 프로필	역할의 이름과 설명을 정의하고 "사용" 상태로 설정합니다.
작업	관리자 또는 액세스 태스크를 포함합니다.
계정 템플릿	끝점에 있는 계정을 정의하는 계정 템플릿을 포함합니다(프로비저닝 역할만).
구성원 정책	각 구성원 정책에 대해 다음과 같이 정의합니다. ■ 구성원 규칙 -- 역할을 사용할 수 있는 사용자 ■ 범위 규칙 -- 역할 구성원이 관리할 수 있는 개체 ■ 추가 동작 -- 구성원이 되는 사용자의 프로필에 대한 영향 ■ 제거 동작 -- 구성원에서 제거되는 사용자의 프로필에 대한 영향

역할 성격	자세한 내용
관리자 정책	각 관리자 정책에 대해: ■ 관리자 규칙 -- 구성원 또는 관리자로서 사용자를 관리할 수 있는 사용자 ■ 범위 규칙 -- 구성원 또는 관리자로서 관리하는 관리자가 될 수 있는 사용자 ■ 추가 동작 -- 관리자가 되는 사용자의 프로필에 대한 영향 ■ 제거 동작 -- 관리자에서 제거되는 사용자의 프로필에 대한 영향
소유자 규칙	역할을 수정할 수 있는 사용자를 정의합니다.

제 2 장: 관리자 역할

이 섹션은 다음 항목을 포함하고 있습니다.

[관리자 역할 및 관리자 태스크](#) (페이지 37)

[관리자 역할 만들기](#) (페이지 39)

[관리자 역할 확인](#) (페이지 43)

[사용자가 자신에게 역할을 할당할 수 있도록 허용](#) (페이지 44)

관리자 역할 및 관리자 태스크

개별 비즈니스 요구 사항을 기반으로 개체 관리 태스크가 포함된 역할을 만듭니다. 예를 들어, 사용자를 관리하는 태스크가 포함된 역할을 몇 개 만들고 만든 역할을 관리하는 태스크가 포함되는 다른 역할을 만들 수 있습니다.

또는 다음 작업이 포함된 별도의 역할을 만들 수도 있습니다.

- 관리자가 사용자를 관리하는 태스크
- 관리자를 관리하는 태스크
- 관리자 역할을 관리하는 태스크
- 액세스 역할을 관리하는 태스크

참고: CA Identity Manager 와 함께 제공된 기본 관리자 역할을 사용할 수도 있습니다. 이러한 역할은 앞의 목록과 유사한 범주로 그룹화된 태스크를 가집니다.

관리자 역할 및 Identity Manager 환경

Identity Manager 환경에 로그인하면 사용자 계정에 하나 이상의 관리자 역할이 있습니다. 각 관리자 역할에는 "사용자 만들기"와 같이 해당 Identity Manager 환경에서 사용하는 작업이 포함되어 있습니다.

예를 들어, 중앙 Identity Manager 환경에서 관리자 역할인 *헬프 태스크*에는 암호 재설정 작업이 있습니다. 이 역할에는 사용자가 IT 직원이어야 한다는 구성원 규칙이 있습니다. IT 직원이 중앙 Identity Manager 환경에 로그인하면 *헬프 태스크* 역할을 갖게 되며, 해당 Identity Manager 환경에서 사용자 암호를 재설정할 수 있습니다.

관리자 역할 및 사용자 콘솔

Identity Manager 환경은 사용자 콘솔을 통해 표시됩니다. 다음 표와 같이 할당된 관리자 역할에 따라 콘솔에 표시되는 내용이 결정됩니다.

할당된 역할	사용자 콘솔의 형식
시스템 관리자 역할	모든 개체의 범주 목록 및 이러한 개체 관리를 위한 모든 기본 관리자 태스크
둘 이상의 개체 유형을 관리하는 역할	관리할 수 있는 각 개체 유형에 대해 하나의 항목이 포함된 범주 목록
한 개의 개체 유형만 관리하는 역할(예: 사용자)	범주 목록 없이 해당 개체에 대한 태스크(예: 사용자 수정)
승인 역할	작업 목록 화면 관리자에게 승인 보류 중인 태스크가 있는 경우(예를 들어, 자체 등록 사용자에게 승인이 필요한 경우)에 나타납니다.

둘 이상의 개체를 관리할 수 있는 경우에는 범주 목록이 표시되고 사용자, 그룹과 같이 수정할 수 있는 개체가 화면 맨 위에 탭으로 표시됩니다. 할당된 역할의 태스크를 보려면 탭을 선택하십시오.

참고: 인터넷 브라우저에서 CSS(Cascading Style Sheets)를 지원하지 않는 경우 사용자 콘솔은 다른 형식을 사용합니다. 이 형식을 제어하려면 *Configuration Guide*(구성 안내서)를 참조하십시오.

관리자 역할 만들기

역할 요구 사항을 알면 관리자 역할을 만들 수 있습니다. 이러한 요구 사항은 이 역할을 사용할 사람, 이 역할이 관리할 개체 및 관리할 개체가 있는 환경과 관련이 있습니다.

관리자 역할 만들기 시작

사용자 콘솔에서 관리자 역할을 만듭니다.

관리자 역할을 만들려면

1. 관리자 역할을 만드는 태스크가 포함된 역할을 가진 CA Identity Manager 계정에 로그인합니다.

예를 들어, 환경의 첫 번째 사용자는 시스템 관리자 역할을 가지며, 이 역할에는 관리자 역할 만들기 태스크가 포함되어 있습니다.

2. "역할", "태스크", "관리자 역할", "관리자 역할 만들기"를 선택합니다.
3. 역할을 만들지 또는 복사할지 여부를 결정합니다.
관리자 역할 정의를 시작하는 "프로필" 탭이 나타납니다.
4. 관리자 역할 프로필을 정의합니다.

관리자 역할 프로필 정의

"프로필" 탭에서 역할의 기본 특징을 정의합니다.

프로필을 정의하려면

1. 이름과 설명을 입력하고, 역할에 대해 정의된 다른 사용자 지정 특성을 완료합니다.

참고: "프로필" 탭에서 관리자 역할에 대한 추가 정보를 지정하는 사용자 지정 특성을 지정할 수 있습니다. 이 추가 정보를 사용하여 수많은 역할을 포함하는 환경에서 역할을 쉽게 검색할 수 있습니다.

2. 역할을 만드는 즉시 사용할 수 있게 하려면 "사용"을 선택합니다.
3. [역할의 관리자 작업을 선택하십시오](#) (페이지 40).

역할의 관리자 태스크 선택

"태스크" 탭에서 역할에 포함할 관리자 태스크를 선택합니다. 서로 다른 범주의 태스크를 포함하거나 다른 역할에서 사용된 태스크를 복사할 수 있습니다.

관리자 태스크를 선택하려면

1. "범주별 필터링" 필드에서 범주를 선택합니다.
사용 가능한 태스크 범주 목록을 보려면 아래쪽 화살표 아이콘을 클릭합니다.
2. "태스크 추가" 필드에서 역할에 포함할 태스크를 선택합니다.
CA CA Identity Manager 가 태스크를 역할의 태스크 목록에 추가합니다.
3. 1 단계와 2 단계를 반복하여 태스크를 추가합니다.
4. 해당 태스크에 대한 빼기 부호() 아이콘을 클릭하여 역할에서 태스크를 제거합니다.
5. [관리자 역할의 구성원 정책을 정의합니다](#) (페이지 41).

관리자 역할의 구성원 정책 정의

"구성원" 탭에서 역할 구성원이 될 수 있는 사람을 결정하는 구성원 정책을 만듭니다.

구성원 정책을 정의하려면

1. "추가"를 클릭하여 구성원 정책을 정의합니다. 구성원 정책에는 다음 규칙이 포함되어 있습니다.

- 사용자가 역할 구성원이 되기 위한 요구 사항을 정의하는 구성원 규칙

참고: 다음 연산자는 구성원 규칙의 숫자를 문자로 처리합니다.

- 보다 작음(<)
- 작거나 같음(<=)
- 보다 큼(>)
- 크거나 같음(>=)

예를 들어, '10'은 '1' 뒤와 '2' 앞에 옵니다.

- 역할의 작업에서 사용할 수 있는 주 개체와 보조 개체를 제한하는 범위 규칙

예를 들어, 사용자를 그룹에 할당하여 사용자를 수정하는 작업이 역할에 포함되어 있으면 사용자 범위 규칙은 찾을 수 있는 사용자(주 개체)를 제한하고, 그룹 범위 규칙은 할당할 수 있는 그룹(보조 개체)을 제한합니다.

참고: 적어도 하나의 범위 질문에 대답을 입력해야 합니다. 범위 규칙은 역할의 작업에서 사용할 수 있는 주 개체와 보조 개체를 제한합니다. 예를 들어, 사용자를 그룹에 할당하여 사용자를 수정하는 작업이 역할에 포함되어 있으면 사용자 범위 규칙은 찾을 수 있는 사용자(주 개체)를 제한하고, 그룹 범위 규칙은 할당할 수 있는 그룹(보조 개체)을 제한합니다.

2. 구성원 정책이 "구성원" 탭에 나타나는지 확인합니다.
 - 정책을 편집하려면 왼쪽에 있는 오른쪽 화살표 기호를 클릭합니다.
 - 정책을 제거하려면 빼기 기호 아이콘을 클릭합니다.
3. "구성원" 탭에서, 사용자가 구성원 규칙을 충족해야만 구성원이 되는 경우가 아니면 "관리자가 이 역할의 구성원을 추가하거나 제거할 수 있습니다." 확인란을 선택합니다.

이 기능을 사용하도록 설정하면 화면이 확장됩니다.

4. 확장된 화면 영역에서 사용자가 역할 구성원으로 추가되거나 제거되는 경우에 대한 추가 동작 및 제거 동작을 정의합니다.

중요! 추가 동작을 정의하는 경우 정의하는 역할을 참조하는 규칙을 설정하지 마십시오. 예를 들어, 역할 A의 구성원이 됨으로써 역할 A의 구성원이 되도록 하는 추가 동작을 정의하지 마십시오. 이렇게 하면 오류가 발생할 수 있습니다.

5. [관리자 역할의 관리자 정책을 정의합니다](#) (페이지 42).

관리자 역할의 관리자 정책 정의

"관리자" 탭에서 사용자를 이 역할의 구성원 및 관리자로 추가하거나 제거할 수 있는 사람을 정의합니다.

관리자 정책을 정의하려면

1. "관리자 관리" 옵션을 사용할 수 있게 하려는 경우 "관리자가 이 역할의 관리자를 추가하거나 제거할 수 있습니다." 확인란을 선택합니다.

이 기능을 사용하도록 설정하면 화면이 확장됩니다.

2. 확장 영역에서 사용자가 역할 관리자로 추가되거나 제거되는 경우에 대한 추가 동작 및 제거 동작을 정의합니다.
3. 관리자 및 범위 규칙과 적어도 하나의 관리자 권한(구성원 관리 또는 관리자 관리)이 포함된 관리자 정책을 정의합니다.

참고: 규칙을 충족하는 관리자에 대해 다른 규칙과 다른 권한을 사용하는 관리자 정책을 여러 개 추가할 수 있습니다.

4. 정책을 편집하려면 왼쪽에 있는 화살표 기호를 클릭합니다. 정책을 제거하려면 빼기 기호 아이콘을 클릭합니다.
5. [관리자 역할의 소유자 규칙을 정의합니다](#) (페이지 43).

관리자 역할의 소유자 규칙 정의

"소유자" 탭에서 역할의 소유자, 즉 역할을 수정할 수 있는 사용자가 될 수 있는 사람에 대한 규칙을 정의합니다.

소유자 규칙을 정의하려면

1. 역할을 수정할 수 있는 사용자를 결정하는 소유자 규칙을 정의합니다.
2. "제출"을 클릭합니다.

작업이 제출되었음을 나타내는 메시지가 표시됩니다. 사용자가 역할을 사용할 수 있기 전에 일시적인 지연이 발생할 수도 있습니다.

이 역할을 만들 때 "사용"을 선택한 경우 역할을 사용할 수 있습니다. 사용자가 구성원 규칙의 조건을 충족하면 이제 Identity Manager 환경에 로그인하여 해당 역할의 작업을 사용할 수 있습니다.

관리자 역할 확인

역할이 만들어졌는지 확인하려면 "관리자 역할", "관리자 역할 보기", 역할 이름을 차례로 선택합니다.

또는 "시스템", "제출한 작업 보기"를 선택하여 역할 만들기 작업이 완료되었는지 확인할 수 있습니다.

사용자가 자신에게 역할을 할당할 수 있도록 허용

사용자는 자신에게 특정 역할을 할당할 수 있습니다. 예를 들어, 사용자에게 위임 관리자 역할 등록을 허용하여 한 사용자의 작업 항목을 다른 사용자에게 위임하게 할 수 있습니다.

사용자가 자신에게 할당할 수 있는 역할을 제어하려면 "역할 자체 관리자" 태스크의 조건을 구성합니다.

다음 단계를 수행하십시오.

1. "역할 자체 관리자" 태스크를 다음과 같이 수정합니다.
 - a. "역할 및 태스크", "관리자 태스크 수정"을 차례로 선택하고 "역할 자체 관리자" 태스크를 검색합니다.
 - b. "탭" 탭을 선택합니다.
CA Identity Manager 가 태스크에 적용되는 탭 목록을 표시합니다.
 - c. 편집하려면 "역할 자체 관리자" 탭 옆에 있는 오른쪽 화살표 아이콘을 선택합니다.

- d. 다음 필드를 작성하십시오.

다음 규칙을 충족시키는 관리자 역할만 표시

CA Identity Manager 가 사용자가 자신에게 할당할 수 있도록 허용할 역할을 결정하는 데 사용할 조건을 지정합니다.

다른 규칙을 추가하려면 더하기(+) 아이콘을 클릭합니다.

관리자 역할 관리자로 사용될 사용자

사용자가 자신에게 할당할 수 있는 역할의 관리자를 지정합니다.

사용자가 자신에게 할당할 수 있는 역할은 이 필드에서 관리자로 선택한 사용자를 포함해야 하며 "다음 규칙을 충족시키는 관리자 역할만 표시" 필드에서 지정한 조건을 충족해야 합니다.

목록 화면

사용자가 자신에게 역할을 할당하기 위해 선택할 수 있는 역할 목록의 열과 형식을 지정합니다.

- e. "확인", "제출"을 차례로 클릭합니다.

2. 역할에 "역할 자체 관리자" 태스크를 추가하고 이 기능이 있어야 하는 사용자에게 해당 역할을 할당합니다.

제 3 장: 관리자 태스크

이 섹션은 다음 항목을 포함하고 있습니다.

- [관리자 작업 계획](#) (페이지 47)
- [관리자 작업 사용 옵션](#) (페이지 51)
- [기본 관리자 작업](#) (페이지 52)
- [사용자 지정 관리자 태스크를 만드는 방법](#) (페이지 53)
- [작업 프로필 정의](#) (페이지 54)
- [작업 범위 정의](#) (페이지 59)
- [작업의 탭 선택](#) (페이지 70)
- [작업의 필드 보기](#) (페이지 74)
- [역할 사용 보기](#) (페이지 75)
- [이벤트에 대한 워크플로 프로세스 할당](#) (페이지 75)
- [Active Directory 사용자 저장소 관리](#) (페이지 75)
- [응용 프로그램 기능에 대한 외부 작업](#) (페이지 77)
- [고급 태스크 구성 요소](#) (페이지 80)
- [관리자 태스크 및 이벤트](#) (페이지 82)
- [관리자 작업 처리](#) (페이지 84)
- [관리자 태스크 이미지](#) (페이지 88)

관리자 작업 계획

관리자 역할은 세부적인 개체 관리 기능을 나타내는 관리자 작업으로 구성됩니다. 예를 들어, 다음과 같은 관리자 작업을 사용하여 사용자 개체를 관리할 수 있습니다.

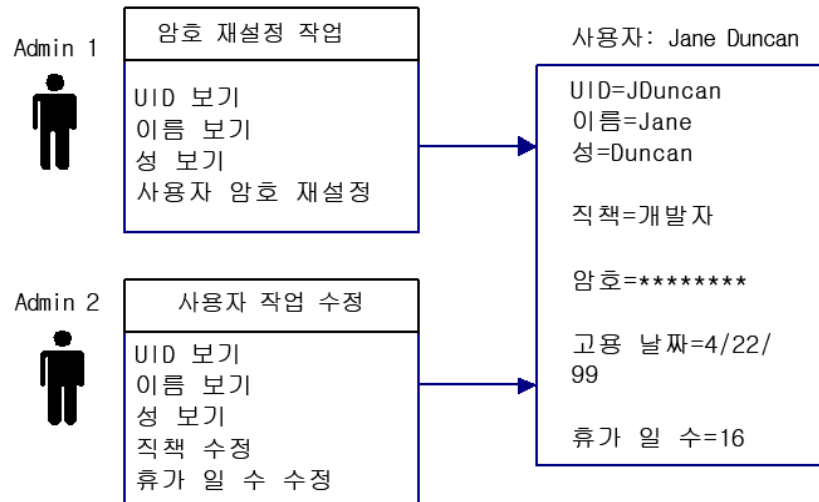
- 사용자 만들기
- 사용자 보기
- 사용자 수정
- 사용자 암호 재설정

정확한 요구 사항에 맞게 각 작업을 만들거나 수정합니다. 그런 다음 적절한 관리자 작업을 관리자 역할로 결합하여 관리자에게 할당합니다. 이러한 역할을 통해 관리자는 개체 관리에 필요한 권한을 갖습니다.

관리자 작업 만들기를 계획하려면 관리해야 하는 개체(사용자, 그룹, 조직, 역할 또는 작업) 및 이러한 작업을 사용할 관리자를 결정합니다. 예:

- 헬프 데스크 관리자는 사용자를 관리하기 위해 사용자 ID 나 직함 등의 사용자 특성을 관리하는 작업이 필요합니다.
- 다른 관리자는 응용 프로그램에 대한 사용자 액세스를 관리하기 위해 사용자를 액세스 역할의 구성원으로 만드는 작업이 필요합니다.
- 상위 관리자는 헬프 데스크 관리자가 사용하는 역할을 관리하기 위해 관리자 역할을 관리하는 작업이 필요합니다.

관리자에 따라 다른 특성을 관리하도록 사용자 등의 단일 개체 유형에 대해 작업을 만들 수 있습니다. 예를 들어, 다음 그림에서는 두 관리자가 관리하는 사용자를 보여 줍니다.



- Admin 1에는 사용자 암호 재설정 작업이 있으므로 관리자가 직원의 사용자 ID 와 이름을 보고 암호를 재설정할 수 있습니다.
- Admin 2는 사용자 수정 작업이 있으므로 관리자가 직원의 사용자 ID 와 이름을 보거나 직함과 휴가 기간을 수정할 수 있습니다.

관리자 작업 예제

관리자 작업을 만드는 경우 다음을 비롯하여 작업 화면의 콘텐츠와 레이아웃을 정의합니다.

- 작업 이름
- 작업이 나타나는 범주
- 작업에 사용할 탭 및 필드와 필드 표시 속성
- 관리자가 검색 쿼리에 사용할 수 있는 필드 및 검색 결과에 표시되는 필드

작업의 요소를 이해하려면 사용자 수정 작업을 확인합니다. 이 경우 "사용자"는 범주, "사용자 관리"는 하위 범주, "사용자 수정"은 태스크입니다. 작업을 만들 때 범주와 작업 이름을 만듭니다.



"사용자 수정"을 선택하면 검색 화면이 나타납니다. *검색 화면*에서는 보거나 수정할 개체를 찾는 데 사용할 수 있는 옵션을 제공합니다. 각 옵션을 *필터*라고 하며, 검색에서 찾는 개체를 제한합니다.

검색 화면에서 데이터를 입력하면 탭이 있는 화면이 나타납니다. 예를 들어, 다음 그림에서는 "사용자 수정" 작업에 대한 탭을 보여 줍니다. "프로필" 탭이 첫 번째로 나타나 사용자 특성이 표시되고, 나머지 탭은 사용자의 역할 및 그룹 권한이 표시됩니다.

만든 작업에 대해 포함할 탭을 결정하고 탭 순서와 콘텐츠를 지정합니다.

사용자 수정: SuperAdmin

[프로필](#)
[액세스 역할](#)
[관리자 역할](#)
[프로비저닝 역할](#)
[그룹](#)

• = 필수

조직

사용자 ID

사용 ☒

•이름(성 제외)

•성(이름)

•전체 이름

전자 메일

예를 들어, "사용자 수정" 작업을 템플릿으로 사용하여 다음을 변경한 "계약자 수정" 작업을 만들 수 있습니다.

- 프로필 탭의 필드
- 작업에 포함할 탭 및 해당 콘텐츠
- 작업이 나타나는 범주

새 범주인 계약자 아래에 이 작업을 만들 수도 있습니다.

다음 계정으로 로그인함: SuperAdmin (로그아웃)

[홈](#)
[계약자](#)
[사용자](#)

▼ 작업

▶ 계약자 관리
 계약자 수정

"계약자 수정" 작업에는 "사용자 수정" 작업의 "프로필" 탭에 있는 필드 중 일부와 계약 시작 날짜, 계약자 회사 등의 다른 필드가 포함되어 있습니다. 관리자는 계약자 이름, 회사 및 시작 날짜를 기준으로 계약자를 검색할 수 있습니다.

계약자 수정: *jhansen*

프로필	그룹	계약자 역할
사용자 ID <i>jhansen</i> 사용 ☒ 이름 Julia 성 Hansen 전자 메일 jhansen@wxyz.com 시작 날짜 2008. 5. 11  회사		

새 작업에는 또한 계약자의 역할을 추가할 수 있는 "계약자 역할" 탭이 포함되어 있습니다.

관리자 작업 사용 옵션

Identity Manager에서는 관리자 작업을 사용하는 다음 두 가지 방법을 제공합니다.

■ 작업 선택

범주와 작업을 선택한 다음 작업이 적용되는 개체를 검색합니다.

예를 들어, 사용자 프로필을 수정하려면 "사용자" 범주를 선택한 다음 "사용자 수정" 작업을 선택합니다. 수정할 사용자를 검색합니다.

■ 개체 선택

사용자 관리나 그룹 관리 등의 "관리" 작업을 사용하여 개체를 검색합니다. 개체를 선택하면 해당 개체를 관리하는 데 사용할 수 있는 작업 목록을 표시할 수 있습니다. 이 방법을 *개체-작업 탐색*이라고 합니다.

예를 들어, 이 방법으로 사용자를 수정하려면 "사용자" 범주를 선택한 다음 "사용자 관리" 작업을 선택합니다. 관리할 사용자를 검색하여 선택합니다. 검색 결과에서 아이콘을 클릭하여 선택한 사용자를 관리하는 데 사용할 수 있는 작업 목록을 표시합니다. 이 목록에서 "사용자 수정"이나 다른 적절한 작업을 선택할 수 있습니다.

관리 작업이 아닌 작업에 작업 목록을 구성할 수도 있습니다. 예를 들어, "멤버십" 탭에 작업 목록을 추가할 수 있습니다. 이 경우 "멤버십" 탭에 표시된 각 구성원이 작업 목록을 사용할 수 있습니다.

참고: 현재 관리자가 사용할 수 있는 작업만 개체에 대한 작업 목록에 나타납니다.

기본 관리자 작업

CA Identity Manager에는 다양한 기본 관리자 태스크와 역할이 포함되며, 이러한 태스크와 역할은 역할 정의 파일을 관리 콘솔로 가져오는 방식으로 CA Identity Manager에 추가됩니다. 관리 콘솔에서 환경을 만들고 기본 역할 만들기를 선택하면 CA Identity Manager에서 자동으로 역할 정의 파일을 가져옵니다.

참고: 특정 끝점 유형을 위한 계정 관리와 같은 일부 기능을 지원하기 위해 추가 역할 정의 파일을 가져와서 필요한 역할과 태스크를 만들어야 할 수도 있습니다.

대부분의 경우 기본 태스크를 설치된 대로 사용할 수 있습니다. 그러나 "사용자 만들기", "사용자 수정", "사용자 보기"와 같은 기본 사용자 태스크의 "프로필" 탭을 수정해야 할 수도 있습니다. "프로필" 탭에는 디렉터리 구성 파일에서 사용자 개체에 대해 정의된 모든 필드가 포함됩니다. 이 탭에 표시되는 필드의 수를 제한하거나 필드 표시 속성을 변경할 수 있습니다.

참고: 기본 태스크를 직접 수정하는 대신 수정할 기본 태스크의 사본을 만드는 것이 좋습니다.

사용자 지정 관리자 태스크를 만드는 방법

관리자 작업은 사용자가 Identity Manager 에서 수행할 수 있는 관리자 기능입니다. 관리자 작업의 예로 "사용자 만들기", "그룹 수정", "역할 멤버십 보기" 등이 있습니다.

CA Identity Manager 에는 비즈니스 필요에 맞게 수정할 수 있는 기본 관리자 태스크가 있습니다.

사용자 지정 관리자 태스크를 만드는 경우 다음 단계를 완료하십시오.

참고: [Active Directory 선행 조건](#) (페이지 75) 섹션에는 CA Identity Manager 가 Active Directory 사용자 저장소를 관리하는 경우의 추가 고려 사항이 포함되어 있습니다.

1. CA Identity Manager 사용자 콘솔에서 "역할 및 태스크", "관리자 태스크", "관리자 태스크 만들기"를 선택합니다.

CA Identity Manager 가 새 작업을 만들 것인지 또는 기존 작업을 기반으로 작업을 만들 것인지를 묻습니다.

예를 들어, 새 작업의 기반으로 "사용자 수정" 작업을 선택합니다.

2. "기존 태스크 사본 만들기"를 선택하고 복사할 태스크를 검색합니다.

참고: 기본 태스크를 직접 수정하지 않고 기본 태스크의 사본을 수정하는 것이 좋습니다.

3. "확인"을 선택하면 다음 6 개의 탭이 있는 화면이 표시됩니다.

탭	용도	참조 항목
프로필	만드는 작업의 프로필 정의	작업 프로필 정의 (페이지 54)
검색	작업에서 관리하는 개체 범위 제한	작업 범위 정의 (페이지 59)
탭	작업의 탭 선택 및 디자인	작업의 탭 선택 (페이지 70)
필드	모든 탭에서 사용되는 필드 표시	작업의 필드 보기 (페이지 74)

탭	용도	참조 항목
이벤트	CA Identity Manager 환경 및 작업에서 워크플로를 사용하는 경우 각 이벤트에 대한 워크플로 프로세스 선택	이벤트에 대한 워크플로 프로세스 할당 (페이지 75)
역할 사용	보거나 수정 중인 태스크가 포함된 역할이 표시됩니다.	역할 사용 보기 (페이지 75)

참고: 사용자 지정 관리자 태스크에 대한 자세한 내용은 *User Console Design Guide*(사용자 콘솔 디자인 안내서)를 참조하십시오.

작업 프로파일 정의

"프로파일" 탭에는 작업에 대한 일반 설정이 포함되어 있습니다.

작업의 프로파일을 정의하려면

1. 작업의 개체 유형(주 개체라고 함) 및 해당 개체에 대해 수행할 동작을 선택합니다.
2. 필수 필드에 데이터를 입력하고 작업에 필요한 경우 해당 확인란을 선택합니다.

참고: 프로파일 설정이 기존 작업과 유사한 작업을 만드는 경우 "다른 작업에서 프로파일 복사"를 클릭합니다. 이 옵션은 만드는 작업의 프로파일 설정을 선택한 기존 작업의 프로파일 설정으로 채웁니다. 새 작업의 이름과 설명을 추가합니다.

3. (선택 사항) 비즈니스 로직 작업 처리기를 작업과 연결합니다.
4. 이 탭을 완료한 경우 다음 단계인 [작업 범위 정의](#) (페이지 59)에서 계속합니다.

관리자 태스크 프로필 탭

"관리자 태스크 프로필" 탭에서 관리자 태스크에 대한 일반 설정을 정의할 수 있습니다.

이 탭에는 다음과 같은 필드가 있습니다.

- **이름**

태스크의 이름을 정의합니다.

- **태그**

태스크의 고유한 식별자를 정의합니다. URL, 웹 서비스 또는 속성 파일에서 사용됩니다. 태그에는 ASCII 문자(a-z, A-Z), 숫자(0-9) 또는 밑줄 문자를 사용할 수 있으며 문자나 밑줄로 시작해야 합니다.

- **설명**

태스크의 목적에 대한 선택적 참고 사항을 지정합니다.

- **작업 순서**

작업의 표시 순서를 지정합니다. 순서를 지정하지 않으면 작업이 사전순으로 표시됩니다.

- **범주**

작업의 범주를 지정합니다. 범주는 화면 맨 위에 탭으로 표시됩니다.

- **범주 순서**

범주 탭이 나타나는 순서를 지정합니다. 예를 들어, 범주 순서를 3 으로 설정하면 지정한 범주가 세 번째 탭으로 나타납니다.

- **범주 2**

범주 탭 목록 아래에 링크로 나타나는 두 번째 수준 범주를 지정합니다. 두 번째 수준 범주는 첫 번째 수준 범주의 탭이 선택된 경우에만 나타납니다. 예를 들어, 첫 번째 수준 범주가 "직원"이고 두 번째 수준 범주가 "직원 관리"인 작업을 만든 경우 "직원" 탭을 선택한 후에만 "직원 관리" 범주가 나타납니다.

- **범주 2 순서**

주 범주에 두 번째 수준 범주가 둘 이상 있는 경우 두 번째 수준 범주가 나타나는 순서를 지정합니다.

- **범주 3**

왼쪽 탐색 창에 나타나는 세 번째 수준 범주를 지정합니다. 작업은 세 번째 수준 범주 아래에 표시됩니다. 예를 들어, 기본 환경에서 "시스템 관리자" 또는 "사용자 관리자" 역할의 사용자가 "사용자" 탭을 선택하면 세 번째 수준 범주인 "사용자 관리"가 표시됩니다.

- **범주 3 순서**

세 번째 수준 범주가 나타나는 순서를 지정합니다.

- **기본 개체**

태스크가 수행되는 개체를 지정합니다.

- **동작**

개체에 대해 수행할 작업을 지정합니다.

- **사용자 동기화**

태스크에서 사용자를 ID 정책과 동기화하는지 여부를 지정합니다. 다음 옵션 중 하나를 선택할 수 있습니다.

- **끄기(기본값)**

이 태스크에서 사용자 동기화를 트리거하지 않도록 지정합니다.

- **태스크 완료 시**

태스크의 모든 이벤트가 완료된 후 CA CA Identity Manager 가 사용자 동기화 프로세스를 시작하도록 지정합니다. 이 설정은 "사용자 만들기", "사용자 수정" 및 "사용자 삭제" 태스크의 기본 동기화 옵션입니다. 다른 모든 태스크의 기본 설정은 "끄기"입니다.

참고: 여러 이벤트가 포함된 태스크에 대해 "태스크 완료 시" 옵션을 선택하면 태스크의 모든 이벤트가 완료될 때까지 CA CA Identity Manager 에서 사용자를 동기화하지 않습니다. 워크플로 승인이 필요한 이벤트가 하나 이상 있는 경우 모든 이벤트가 완료되는 데 며칠이 걸릴 수 있습니다. 모든 이벤트가 완료될 때까지 CA CA Identity Manager 에서 ID 정책을 적용하기 위해 대기하지 않도록 하려면 "모든 이벤트 발생 시" 옵션을 선택하십시오.

- 모든 이벤트 발생 시

태스크의 각 이벤트가 완료될 때 CA CA Identity Manager 가 [사용자 동기화 프로세스](#) (페이지 504)를 시작하도록 지정합니다.

동일한 사용자에게 대해 주 이벤트와 보조 이벤트가 있는 태스크의 경우 사용자 동기화를 "모든 이벤트 발생 시"로 설정하면 "태스크 완료 시" 옵션을 선택한 경우보다 더 많은 ID 정책이 사용자에게 적용될 수 있습니다.

- 계정 동기화

프로비저닝이 사용되는 경우 프로비저닝 서버에 있는 계정을 동기화합니다.

- 끄기(기본값)

이 태스크에서 계정 동기화를 트리거하지 않도록 지정합니다.

- 태스크 완료 시

태스크의 모든 이벤트가 완료된 후 CA CA Identity Manager 가 계정 동기화 프로세스를 시작하도록 지정합니다.

- 모든 이벤트 발생 시

태스크의 각 이벤트가 완료될 때 CA CA Identity Manager 가 계정 동기화 프로세스를 시작하도록 지정합니다.

참고: 최상의 성능을 얻으려면 "태스크 완료 시"를 선택하십시오. 그러나 여러 이벤트가 포함된 태스크에 대해 "태스크 완료 시" 옵션을 선택하면 태스크의 모든 이벤트가 완료될 때까지 CA CA Identity Manager 가 계정을 동기화하지 않습니다. 워크플로 승인이 필요한 이벤트가 하나 이상 있는 경우 모든 이벤트가 완료되는 데 며칠이 걸릴 수 있습니다. 모든 이벤트가 완료될 때까지 CA CA Identity Manager 가 계정 동기화를 대기하지 않으려면 "모든 이벤트 발생 시" 옵션을 선택하십시오.

- 메뉴에서 숨기기

태스크가 메뉴에 표시되지 않도록 합니다. URL 이나 다른 태스크에 의해서만 태스크가 호출되는 경우 이 컨트롤을 사용하도록 설정하십시오.

- 공용 태스크

CA CA Identity Manager 에 로그인하지 않은 사용자가 태스크를 사용할 수 있게 합니다. 기본 공용 태스크는 잊어버린 암호 및 자체 등록입니다.

- **감사 사용**

태스크에 대한 정보를 감사 데이터베이스에 기록합니다. 감사 정보를 사용하여 보고서를 생성할 수 있습니다. *Configuration Guide*(구성 안내서)를 참조하십시오.

- **워크플로 사용**

워크플로 엔진이 설치되어 있는 경우 태스크와 연결된 CA CA Identity Manager 이벤트에서 워크플로 프로세스를 트리거할 수 있게 합니다. 예를 들어, "그룹 삭제" 태스크와 연결된 이벤트에서 승인 단계가 포함된 워크플로 프로세스를 트리거할 수 있습니다.

- **웹 서비스 사용**

관리 콘솔에서 WSDL(Web Services Description Language) 출력을 생성할 수 있는 태스크로 표시합니다. 원격 태스크 제출을 사용하려는 경우 이 컨트롤을 사용하도록 설정하십시오. 자세한 내용은 *Programming Guide for Java*(Java 프로그래밍 안내서)를 참조하십시오.

- **워크플로 프로세스**

태스크 수준 워크플로에 대한 구성을 활성화합니다. 정책 기반 또는 정책 기반이 아닌 워크플로를 구성하려면 연필 아이콘을 클릭하십시오.

- **작업 우선 순위**

CA CA Identity Manager 가 태스크를 실행하는 순서를 결정합니다. "높음" 우선 순위의 태스크가 "중간" 또는 "낮음" 우선 순위의 태스크보다 먼저 실행됩니다. 태스크의 기본 우선 순위는 "중간"입니다.

참고: "제출한 태스크 보기" 태스크를 사용하여 특정 우선 순위의 태스크를 검색하고 해당 상태를 표시할 수 있습니다.

- **비즈니스 로직 태스크 처리기**

[비즈니스 로직 태스크 처리기](#) (페이지 80)를 태스크와 연결합니다.

- **워크플로 동작 단추**

워크플로 승인 태스크에 사용자 지정 동작 단추를 추가합니다.

- **다른 태스크에서 프로파일 복사**

다른 태스크의 "프로파일" 탭에서 데이터를 복사합니다.

예를 들어, "사용자 수정" 태스크의 "프로파일" 탭 설정을 복사한 다음 이름과 설명을 추가할 수 있습니다.

태스크 구성 속성

태스크 구성 속성은 태스크에 대한 표시 속성과 몇 가지 동작을 제어합니다.

태스크 아이콘 경로

태스크 목록에서 이 태스크의 아이콘으로 사용할 그래픽의 URL 을 지정합니다.

태스크 아이콘 미리 보기

태스크의 아이콘을 태스크 목록에 나타나는 것처럼 표시합니다.

태스크 탐색 안 함

이 옵션을 선택한 경우 사용자가 태스크를 선택하면 최상위 탐색 및 태스크 목록이 숨겨집니다. 이렇게 하면 사용자가 필요한 동작을 완료하거나 태스크를 취소하지 않는 한 현재 태스크 이외의 항목을 탐색할 수 없게 됩니다.

대상 창

이 필드에서 값을 제공하면 CA Identity Manager 가 새 브라우저 창에서 이 태스크를 엽니다. 이 필드를 사용하여 외부 태스크에 대해 새 브라우저 창을 열어 사용자를 다른 웹 사이트로 리디렉션할 수 있습니다.

창에 아무 이름이나 지정할 수 있습니다.

참고: CA Identity Manager 관리자 태스크를 별도의 브라우저 창에서 여는 용도로는 이 필드를 사용하지 마십시오. CA Identity Manager 는 단일 CA Identity Manager 사용자 세션에 대해 여러 개의 브라우저 창을 지원하지 않습니다.

작업 범위 정의

"검색" 탭에서 작업에 사용할 수 있는 개체를 제한하는 작업 범위를 정의합니다. 예를 들어, 작업의 개체가 사용자이면 범위를 계약자인 사용자로 정의할 수 있습니다.

참고: 작업에 주 개체가 없거나 동작이 자체 수정, 자체 보기 또는 승인인 경우에는 "검색" 탭이 나타나지 않습니다.

"검색" 탭에서 다음 설정을 구성합니다.

검색 화면

검색 화면에서는 필터를 기반으로 작업 범위를 제한합니다.
"찾아보기"를 클릭하여 사용 가능한 검색 화면 옵션을 봅니다.

참고: [고유한 검색 화면](#) (페이지 61)을 만들 수도 있습니다. 기존 검색 화면의 수정된 버전을 만들려면 검색 화면을 선택하고 "복사"를 클릭합니다. 그런 다음 원래 검색 화면 정의를 변경하지 않고 검색 화면을 수정할 수 있습니다. 검색 화면을 만들려면 "새로 만들기"를 클릭하십시오.

검색 옵션

검색 옵션은 개체가 역할이나 그룹인 경우에만 나타납니다.

- 첫 번째 옵션은 검색 화면에서 정의된 필드를 기반으로 검색을 제한합니다. 이러한 제한 내에서 검색은 관리자 범위에 있는 모든 그룹 또는 역할을 찾습니다.
- 다른 옵션은 표시된 대로 검색을 제한합니다.

다음은 주의하십시오.

- 기본적으로 그룹 검색 화면은 필터링을 지원합니다. 즉, 관리자가 조건을 지정하여 그룹 검색 범위를 제한할 수 있습니다. 필터링 기능을 제거하려면 검색 쿼리에 포함할 필드가 포함되지 않은 검색 화면을 만드십시오.
- 개체가 역할일 때 "검색" 탭에 표시되는 *필터링 지원 안됨*을 선택하면 태스크에서 선택한 옵션의 조건을 충족하는 모든 역할이 표시됩니다. 검색 화면에서 구성된 검색 필드는 무시됩니다.

수정된 개체는 관리자의 범위 내에 있어야 합니다.

이 확인란을 선택하면 태스크 변경으로 인해 주 개체에 대한 관리자의 범위가 손실될 경우 CA CA Identity Manager 에서 오류를 표시합니다. 예를 들어, 관리자는 "사용자 수정"을 사용하여 사용자의 "직원 유형" 특성을 "관리자"로 변경할 수 있습니다. 이 변경으로 인해 사용자가 관리자의 범위에서 벗어날 수 있습니다.

검색 화면 구성

검색 화면을 구성하여 태스크의 범위를 제한하고 사용자가 검색할 수 있는 필드를 제어합니다. 검색 화면은 다음 두 가지 개체 유형에 적용됩니다.

- **기본 개체**- 태스크에 의해 수정되거나 검토될 개체입니다.
- **보조 개체**- 기본 개체와 관련된 개체입니다.

예를 들어, 사용자 만들기 태스크에 그룹 탭을 포함하는 경우 사용자는 주 개체이고 그룹은 보조 개체입니다. 그룹 탭에는 그룹에 대한 검색 화면이 필요합니다.

참고: 검색 화면을 구성한 후 주 개체나 보조 개체를 검색할 모든 태스크에 사용할 수 있습니다.

검색 필터

검색 필터는 검색에서 반환되는 개체를 제한합니다. 예를 들어, 개체가 사용자인 경우 계약자만 검색하도록 제한할 수 있습니다. 직원 유형이 계약자인 사용자를 찾도록 필터를 구성할 수 있습니다.

다음과 같은 검색 필드를 구성할 수 있습니다.

다음 규칙을 충족시키는 개체만 표시

사용자 정의된 필터와 결합하여 검색을 제한할 추가 조건을 정의합니다.

이 필드를 사용할 때 다음 사항에 주의하십시오.

- 프로비저닝 역할 검색의 제한 때문에 이러한 조건은 사용자가 입력한 동일한 이름의 필터 필드보다 우선 순위가 높습니다.
- 이 필드를 구성할 때 사용되는 특성을 검색 화면에서 사용할 수 있는 검색 필드로 추가하지 마십시오.

예를 들어 "사용" 특성이 "예"로 설정된 역할만 표시하도록 검색 화면을 구성할 경우 사용자가 검색 기준에서 지정할 수 있는 특성 목록에서 "사용" 특성을 제거하십시오.

이 특성을 제거하지 않으면 사용자가 입력한 기준이 무시됩니다.

기본 검색 필터

관리자가 검색 화면을 사용할 때 기본적으로 표시되는 필터를 정의합니다. 예를 들어, "계약자 수정" 태스크에 대해 검색 화면을 구성 중이고 관리자가 일반적으로 계약자 회사의 이름을 기반으로 계약자를 검색할 것을 알고 있으면 기본 필터를 계약 회사 = *로 설정할 수 있습니다. 관리자는 다른 검색 조건을 지정하여 기본 필터를 무시할 수 있습니다. 기본 필터를 설정하면 관리자가 검색을 시작하기 전에 필터를 지정하지 않을 경우에 반환되는 결과 수가 제한되어 성능이 향상됩니다.

다중 선택 태스크에 사용될 경우에 모든 검색 결과 자동 선택

모든 검색 결과가 기본적으로 선택되도록 지정합니다. 이 확인란을 선택하면 검색 결과 목록의 모든 개체 이름 옆에 확인란이 선택된 상태로 표시됩니다.

자동 검색 수행

검색 필드가 검색 결과와 함께 표시되도록 지정합니다.

단일 검색 결과만 있을 경우의 태스크 대상 자동 설정

검색 필터와 일치하는 개체가 하나뿐일 경우 자동으로 태스크의 주 개체를 설정합니다.

예를 들어, "사용자 수정" 태스크와 연결된 사용자 검색 화면에 대해 이 옵션이 선택되어 있다고 가정합니다. 관리자가 "사용자 수정" 태스크를 열고 한 사용자만 반환하는 검색 필터를 입력하면 CA CA Identity Manager 는 해당 사용자에 대한 "사용자 수정" 태스크를 엽니다. 관리자가 "사용자 수정" 태스크를 열기 위해 해당 사용자를 선택할 필요가 없습니다.

참고: 이 설정을 적용하려면 "자동 검색 수행"도 선택되어야 합니다.

검색 필터 저장

현재 세션의 사용자에 대해 태스크의 검색 필터가 저장되도록 지정합니다. 다음에 사용자가 태스크에서 검색하는 경우 저장된 검색 필터가 표시됩니다.

참고: CA CA Identity Manager 는 사용자 세션 기간에 대한 검색 필터를 저장합니다. 사용자가 로그 아웃하면 검색 필터는 삭제됩니다.

조직에서 검색

검색 화면에 조직 필터를 표시합니다. 이 확인란을 선택하면 관리자는 CA CA Identity Manager 가 개체를 검색하는 조직을 제한하는 필터를 지정할 수 있습니다. "조직 검색" 필드에서 검색 화면 정의를 지정하여 조직 검색 필터의 기본값을 지정할 수 있습니다.

검색 조직 저장

검색에 대해 조직이 설정된 경우 태스크의 조직을 저장하도록 지정합니다. 다음에 사용자가 태스크에서 검색하는 경우 조직이 표시됩니다.

조직 검색

CA CA Identity Manager 가 관리자의 조직 검색을 허용하기 위해 사용하는 검색 화면을 지정합니다.

기본 조직 검색 범위

관리자가 검색 화면을 사용할 때 나타나는 기본 조직 검색 범위를 지정합니다. 검색 범위는 검색에 포함된 조직 트리의 수준을 결정합니다. 관리자는 검색 화면에서 다른 검색 기준을 지정하여 기본 조직 검색 범위를 다시 정의할 수 있습니다.

예를 들어, 조직 트리의 다양한 수준에서 계약자 정보를 저장하는 환경에서 사용자 지정 "계약자 수정" 태스크에 대한 검색 화면을 구성할 경우 기본 조직 검색 범위를 "및 낮음"으로 설정할 수 있습니다.

단일 정규식 검색

검색 화면에 나타나는 검색 필터 유형을 정의합니다. 이 확인란을 선택하면 사용자가 <특성><비교 연산자><값>과 같이 단일 검색 필터를 지정할 수 있습니다. 이 확인란을 선택 취소하면 사용자가 여러 검색 필터를 지정할 수 있습니다. 예를 들어, <특성 1><비교 연산자><값 1> AND <특성 2><비교 연산자> <값 2>와 같이 지정합니다. 모든 필터의 조건에 맞는 개체가 검색 결과로 반환됩니다. 앞의 예에서는 <값 1> 및 <값 2>가 포함된 개체가 검색 결과로 반환됩니다.

등호 전용 검색

관리자가 등호가 아닌 다른 검색 연산자를 사용하지 못하게 합니다.

결과 수 표시

일치하는 검색 결과 수를 표시합니다. 이 확인란을 선택하면 모든 검색에서 "X 개의 결과가 있습니다." 메시지를 반환합니다.

태스크 단추 추가: <태스크 이름>

검색 화면에 다른 태스크에 대한 링크를 추가합니다. 링크는 단추로 표시됩니다.

이 필드는 일반적으로 개체-태스크 탐색에 대해 구성된 검색 화면에 "만들기" 태스크를 추가하는 데 사용됩니다.

선택적 레이블

앞의 필드에서 선택한 태스크의 레이블을 지정합니다. 이 레이블은 태스크의 단추에 나타납니다.

다중 삭제 단추 추가: <태스크 이름>

관리자가 삭제할 여러 개체를 선택할 수 있는 태스크에 대한 링크를 추가합니다. 링크는 단추로 표시됩니다.

이 필드는 일반적으로 개체-태스크 탐색에 사용됩니다.

검색 필드 및 검색 결과

검색 화면의 다른 부분에서 관리자가 검색 쿼리에 사용할 수 있는 필드와 검색 결과에 표시할 필드를 선택합니다.

사용자가 검색을 수행할 필드 선택

관리자가 검색 쿼리를 만드는 데 사용할 수 있는 필드를 선택합니다.

다른 필드를 추가하려면 검색 필드 테이블 아래의 목록 상자에서 필드를 선택합니다.

필드를 선택한 후 필드 오른쪽의 위쪽 및 아래쪽 화살표 아이콘을 사용하여 필드가 표시되는 순서를 변경할 수 있습니다.

참고: 관리자가 검색할 수 있는 필드를 지정하지 않으면 CA CA Identity Manager 에서 자동으로 검색을 시작합니다.

검색 결과에 나타난 필드 선택

CA Identity Manager 에서 검색 결과에 표시하는 필드를 선택합니다.
검색 쿼리에서 사용할 수 없는 필드를 선택할 수 있습니다.

다른 필드를 추가하려면 검색 필드 테이블 아래의 목록 상자에서 필드를 선택합니다.

스타일

검색 결과에 표시할 필드를 선택하는 경우 다음 스타일 옵션 중 하나를 선택할 수 있습니다.

- **부울 표시 이름**

true 인 모든 결과에 대해 필드 이름이 표시됩니다. 예를 들어, 사용자의 계정 상태를 나타내는 특성 이름으로 "사용"을 입력하면 모든 활성 사용자 계정의 검색 결과에 "사용"이 나타납니다.

- **확인 표시**

특성 값을 기반으로 선택된 확인 표시로 값이 표시됩니다. 예를 들어, 확인 표시 스타일을 선택하여 사용자 계정의 "사용/사용 정지됨" 상태를 나타내는 경우 CA CA Identity Manager 가 모든 활성 계정에 대해 선택된 확인 표시를 표시합니다.

- **다중값 문자열**

다중값 특성의 값을 개별 줄에 표시합니다. 값은 사전순으로 표시됩니다.

- **읽기 전용 확인란**

값을 읽기 전용 확인란으로 표시합니다.

- **문자열**

값을 텍스트 문자열로 표시합니다.

■ 태스크

필드에 태스크 목록을 추가합니다. 사용자는 화살표 아이콘을 클릭하여 검색 필드와 연결된 개체에서 수행할 수 있는 태스크 목록을 확인합니다. 예를 들어, 검색 결과의 "성" 필드에 태스크 목록을 추가하면 사용자는 해당 필드의 화살표 아이콘을 클릭하여 선택한 사용자에 대해 수행할 수 있는 태스크 목록을 볼 수 있습니다.

이 설정은 태스크에 대한 링크로 표시되는 특성 값을 만드는 데도 사용할 수 있습니다.

태스크 스타일을 선택하면 "스타일" 열 옆에 오른쪽 화살표 아이콘이 나타납니다. 화살표를 클릭하여 "필드 속성" 대화 상자를 엽니다. 이 대화 상자를 사용하여 태스크 목록을 구성할 수 있습니다.

■ 작업 목록

사용자가 검색 및 목록 화면에서 개체에 수행할 수 있는 다른 태스크를 추가합니다. 예를 들어 "사용자 수정" 태스크에서 검색 화면을 구성하여 검색에서 반환된 사용자 목록에서 사용자를 비활성화하는 등의 작업을 수행할 수 있도록 만들 수 있습니다.

이 옵션을 선택하면 사용자가 태스크에 액세스할 때 아이콘을 클릭할지 아니면 텍스트 링크를 클릭할지 결정할 수 있습니다.

■ 태스크 메뉴

태스크 목록 스타일과 유사하게 다른 태스크를 팝업 메뉴 항목으로 추가합니다.

이 옵션을 선택하면 검색 또는 목록 화면에서 각 개체 옆에 "동작" 단추가 나타납니다. 사용자가 "동작" 단추를 클릭하면 해당 개체에 대해 수행할 수 있는 태스크 목록이 표시됩니다.

참고: "태스크 목록" 및 "태스크 메뉴" 스타일 옵션을 확인하려면 검색 결과 테이블에 필드를 추가할 때 "(구분 기호)"를 선택합니다. 검색 및 목록 화면에 다른 태스크를 추가하는 방법에 대한 자세한 내용은 *User Console Design Guide*(사용자 콘솔 디자인 안내서)를 참조하십시오.

정렬 가능함

관리자가 필드를 기준으로 검색 결과를 정렬할 수 있게 하려면 이 확인란을 선택합니다.

검색 결과의 기본 정렬 순서 설정

검색 결과가 표시되는 순서를 지정합니다. 검색 결과는 처음에 목록의 첫 번째 필드를 기준으로 정렬된 다음 표시되는 순서대로 각 추가 필드를 기준으로 정렬됩니다. 내림차순으로 결과를 정렬하려면 "내림차순" 확인란을 선택합니다.

필드 이름 필드가 변경된 개체 선택

사용자가 "선택" 단추를 클릭하면 지정된 필드가 변경된 개체가 선택되도록 지정합니다.

페이지당 N 개 결과 반환

페이지당 표시할 결과 수를 선택합니다. 검색 결과가 지정한 개수를 초과하면 CA Identity Manager 에서 각 결과 페이지에 대한 링크를 표시합니다.

검색 화면에 대한 사용자 정의 도움말

검색 화면에 사용자 지정 텍스트를 추가하려는 경우 해당 HTML 텍스트 상자에서 텍스트를 정의할 수 있습니다. 다음 영역에 텍스트를 추가할 수 있습니다.

- 페이지 시작 또는 끝
- 만들기 전 또는 후
- 결과 앞 또는 뒤

검색 화면 유형

Identity Manager 에는 미리 구성된 검색 화면이 포함되어 있습니다.

액세스 역할 검색 화면

"액세스 역할 검색 화면"을 사용하여 특정 조건에 맞는 액세스 역할을 찾도록 검색 필터를 구성할 수 있습니다.

액세스 작업 검색 화면

"액세스 작업 검색 화면"을 사용하여 특정 조건에 맞는 액세스 작업을 찾도록 검색 필터를 구성할 수 있습니다. 이 검색 화면은 보거나 수정할 액세스 작업을 찾거나 액세스 역할에 작업을 추가하는 데 사용됩니다.

관리자 역할 검색 화면

"관리자 역할 검색 화면"을 사용하여 특정 조건에 맞는 관리자 역할을 찾도록 검색 필터를 구성할 수 있습니다.

관리자 작업 검색 화면

"관리자 작업 검색 화면"을 사용하여 특정 조건에 맞는 관리자 작업을 찾도록 검색 필터를 구성할 수 있습니다. 이 검색 화면은 보거나 수정할 관리자 작업을 찾거나 관리자 역할에 작업을 추가하는 데 사용됩니다.

승인 검색 화면

"승인 검색 화면"을 사용하면 승인 작업의 맨 위에 나타나는 표시를 구성할 수 있습니다.

인증 시작 사용자 검색 화면

"인증 시작 사용자 검색 화면"을 사용하여 인증 필요로 설정할 사용자를 찾도록 검색 필터를 구성할 수 있습니다. 선택한 사용자의 인증 상태가 인증 필요로 설정됩니다.

사용자 인증 검색 화면

"사용자 인증 검색 화면"을 사용하여 인증이 필요한 사용자를 찾도록 검색 필터를 구성할 수 있습니다.

위임 검색 화면

"위임 검색 화면"을 사용하여 위임으로 추가할 다른 사용자를 찾도록 검색 필터를 구성할 수 있습니다. 위임은 워크플로 작업 항목을 보고 해결할 권한을 일시적으로 부여할 수 있는 다른 사용자입니다.

사용자 사용 허용/사용 중지 검색 화면

"사용자 사용 허용/사용 중지 검색 화면"을 사용하여 특정 조건에 맞는 사용자의 사용을 허용/중지할 수 있습니다.

인증 종료 사용자 검색 화면

"인증 종료 사용자 검색 화면"을 사용하여 인증 주기를 완료해야 하는 사용자를 식별하도록 검색 필터를 구성할 수 있습니다.

최종 사용자 사용권 계약서 검색 화면

"최종 사용자 사용권 계약서 검색 화면"을 사용하여 아이덴티티 기반 응용 프로그램과 관련된 페이지를 사용하여 자체 등록 작업을 구성할 수 있습니다.

탐색 및 상관 관계 지정 검색

"탐색 및 상관 관계 지정 검색 화면"을 사용하여 특정 조건에 맞는 탐색 및 상관 관계 지정 정의에 대해 검색 필터를 구성할 수 있습니다.

피더 파일 업로드 검색

"피더 파일 업로드 검색 화면"을 사용하여 업로드할 피더 파일을 찾아볼 수 있습니다. 피더 파일은 관리된 많은 개체에서 수행되는 반복 동작을 자동화하는 데 사용됩니다.

잊어버린 암호 검색 화면/잊어버린 사용자 ID 검색 화면

"잊어버린 암호 검색 화면"을 사용하여 아이디를 확인하는 정보를 사용자에게 요청하도록 잊어버린 암호 작업을 구성할 수 있습니다.

그룹 검색 화면

"그룹 검색 화면"을 사용하여 금융 조직 내의 그룹과 같은 그룹에 대해 검색 필터를 구성할 수 있습니다.

아이덴티티 정책 세트 검색 화면

"아이덴티티 정책 세트 검색 화면"을 사용하여 특정 조건에 맞는 아이덴티티 정책 세트를 찾도록 검색 필터를 구성할 수 있습니다.

논리적 특성 처리기 검색 화면

"논리적 특성 처리기 검색 화면"을 사용하여 논리적 특성 처리기를 찾도록 검색 필터를 구성할 수 있습니다. 이 검색 화면은 논리적 특성 처리기를 찾아 해당 구성을 보거나 수정하는 데 사용됩니다.

보고서 관리 검색 화면

"보고서 관리 검색 화면"을 사용하여 보거나 삭제할 보고서를 찾도록 검색 필터를 구성할 수 있습니다.

인증되지 않은 사용자 검색 화면

"인증되지 않은 사용자 검색 화면"을 사용하여 인증 기간이 끝날 때까지 인증되지 않은 사용자를 찾도록 검색 필터를 구성할 수 있습니다.

조직 검색 화면

"조직 검색 화면"을 사용하여 조직 선택을 특정 하위 조직으로 제한하도록 검색 필터를 구성할 수 있습니다.

프로비저닝 역할 검색 화면

"프로비저닝 역할 검색 화면"을 사용하여 프로비저닝 역할을 검색하도록 검색 필터를 구성할 수 있습니다.

계정 템플릿 검색 화면

"계정 템플릿 검색 화면"을 사용하여 계정 템플릿을 검색하도록 검색 필터를 구성할 수 있습니다.

암호 정책 검색 화면

"암호 정책 검색 화면"을 사용하여 특정 조건에 맞는 암호 정책을 찾도록 검색 필터를 구성할 수 있습니다.

스냅샷 정의 검색 화면

"스냅샷 정의 검색 화면"을 사용하여 보거나 수정 또는 삭제할 스냅샷 정의를 찾도록 검색 필터를 구성할 수 있습니다.

표준 검색 화면

"표준 검색 화면"을 사용하여 사용자 지정 관리 개체를 찾도록 필터를 구성할 수 있습니다.

사용자 검색 화면

"사용자 검색 화면"을 사용하여 특정 조건에 맞는 사용자를 찾도록 검색 필터를 구성할 수 있습니다. 예를 들어, 계약자인 사용자를 검색할 수 있습니다.

"검색" 탭을 완료한 후 태스크의 탭을 선택합니다.

작업의 탭 선택

"탭" 탭에서 탭의 이름을 지정하고 구성합니다. 각 탭은 작업에 포함되는 필드 세트입니다. 기본 탭을 포함하거나 새 탭을 만들 수 있습니다. 예를 들어, "사용자 수정" 작업에는 다음 탭이 포함되어 있습니다.

- 프로필
- 액세스 역할
- 관리자 역할

- 그룹
- 작업 항목 위임

탭의 정의를 편집하려면 탭 이름 옆에 있는 편집 아이콘()을 클릭합니다.

계정 탭

"계정" 탭에는 프로비저닝 역할이 할당된 사용자의 관리된 끝점에 있는 계정이 표시됩니다. 일반적으로 이 탭은 사용자를 보거나 수정할 수 있는 태스크에 추가됩니다.

계정 정보
 지금 동작을 수행할 계정 이름을 클릭하십시오.

선택	이름	끝점 유형	끝점	일시 중지됨	잠김
☒	 ken.davis	WindowNT	iamfw	활동적인	잠금 해제

계정 만들기

선택한 계정에 대한 동작

계정 새로 고침
 일시 중지
 다시 시작
 잠금 해제
 암호 변경
 할당 취소
 할당
 삭제

"사용자 수정" 태스크에 "계정" 탭을 추가하면 관리자가 사용자 계정에서 다른 태스크를 수행할 수 있습니다. 예:

- 계정 일시 중지 또는 다시 시작
- 잘못된 액세스나 부적절한 액세스로 인해 자동으로 잠긴 계정을 잠금 해제합니다. 예를 들어, 사용자가 Identity Manager 암호 정책에 설정된 허용 가능한 실패한 로그인 횟수를 초과하면 계정이 잠길 수 있습니다.
- 하나 이상의 계정에서 사용자 암호를 변경합니다.
- 사용자에게 계정을 할당하거나 할당 취소합니다.

"계정" 탭에 제공할 수 있는 다른 옵션에 대한 자세한 내용은 "계정 구성" 탭에 대한 사용자 콘솔 도움말을 참조하십시오.

계정 탭 사용의 선행 조건

"계정" 탭을 사용하려면 프로비저닝 지원을 사용하여 Identity Manager 를 구성해야 하며, Identity Manager 환경에 프로비저닝 디렉터리가 포함되어 있어야 합니다.

참고: 환경에 대해 프로비저닝 지원을 구성하려면 *Configuration Guide*(구성 안내서)를 참조하십시오.

계정 탭의 필드

"계정" 탭에는 끝점 시스템에 있는 사용자 계정에 대한 상세 정보가 표시됩니다.

중요한 몇 개의 필드는 다음과 같습니다.

- 이름 - 계정의 로그인 이름, 전자 메일 이름 또는 기타 이름입니다.
- 끝점 유형 - 계정과 연결된 끝점 유형(예: LDAP 디렉터리)입니다.
- 끝점 - 계정과 연결된 특정 끝점입니다.
- 일시 중지됨—3 개 상태 중 하나입니다.
 - 계정이 활성화되면 "활성" 상태가 표시됩니다.
 - 계정이 비활성화되면 "일시 중지됨" 상태가 표시됩니다.
 - 계정을 다시 시작하거나 일시 중지할 수 없으면 "활성화 보류(수동)" 상태가 표시됩니다. 계정을 다시 시작하거나 일시 중지하려면 끝점 시스템에 로그인해야 합니다.
 - 끝점과 통신이 없어 상태를 검색할 수 없는 경우 '사용할 수 없음'으로 표시됩니다.
- 잠금—계정이 잠긴 경우 표시됩니다. 사용자가 잘못된 암호로 여러 번 계정에 로그인을 시도하면 잠금이 발생합니다. 끝점과 통신이 없어 상태를 검색할 수 없는 경우 '사용할 수 없음'으로 표시됩니다.

계정 탭의 추가 기능

사용자를 수정하는 태스크에 "계정" 탭이 포함되어 있으면 관리자는 해당 태스크를 사용하여 사용자 계정에서 기능을 수행할 수 있습니다. 사용 가능한 기능은 탭 구성에 의해 결정됩니다.

"계정" 탭을 포함하는 태스크에서 "관리자 태스크 수정"을 사용하여 사용 가능한 기능을 선택할 수 있습니다. "계정" 탭을 편집하여 탭에서 "계정 할당" 및 "계정 할당 취소"와 같은 기능을 사용할 수 있는지 여부를 결정합니다.

자세한 내용은 계정 구성에 대한 온라인 도움말을 참조하십시오.

일정 탭

일정을 사용하여 이후 날짜의 작업 실행을 자동화할 수 있습니다. 워크플로와 연결된 작업을 예약하면 **CA Identity Manager** 에서 해당 워크플로에 정의된 대로 모든 작업을 실행합니다. "제출한 작업 보기" 페이지에서 예약된 작업의 상태를 볼 수 있습니다.

"제출한 태스크 보기" 페이지를 통해 **CA Identity Manager** 에서 실행하지 않은 예약된 태스크를 취소할 수 있습니다.

참고: 예약된 태스크가 취소되고 해당 태스크를 다시 제출하면 태스크는 예약된 실행 시간에 상관없이 즉시 실행됩니다.

CA Identity Manager 는 특수 탭으로 스케줄러를 제공합니다. 스케줄러에 액세스하려면 "일정" 탭을 사용하여 작업을 구성해야 합니다.

관리자 작업에 일정 탭 추가

CA Identity Manager 를 사용하면 특정 날짜와 시간에 실행되도록 작업을 예약할 수 있습니다. 작업을 예약하려면 관리자 작업에 "일정" 탭을 추가해야 합니다.

참고: **CA Identity Manager** 의 모든 관리자 작업에 "일정" 탭을 추가할 수 있는 것은 아닙니다. 작업을 예약할 수 없으면 "관리자 작업 수정" 화면에서 일정 탭을 사용할 수 없습니다.

관리자 작업에 일정 탭을 추가하려면

1. "역할 및 태스크", "관리자 태스크", "관리자 태스크 수정"을 클릭합니다.
"관리자 태스크 선택" 페이지가 나타납니다.
2. "위치" 필드에서 "이름" 또는 "범주"를 선택하고 검색할 문자열을 입력한 다음 "검색"을 클릭합니다.
CA Identity Manager 에서 검색 조건에 맞는 관리자 태스크가 표시됩니다.
3. 관리자 태스크를 선택하고 "선택"을 클릭합니다.
CA Identity Manager 에서 선택한 관리자 작업에 대한 작업 상세 정보를 표시합니다.
4. "탭"을 클릭합니다.
선택한 관리자 작업에 대해 구성된 탭이 표시됩니다.
5. "이 작업에 어떤 탭이 나타나야 합니까?" 드롭다운에서 "일정"을 선택하고  를 클릭합니다.
선택한 관리자 작업에 표시될 탭 목록에 "일정" 탭이 추가됩니다.
6. 제출을 클릭합니다.
선택한 관리자 작업에 "일정" 탭이 추가됩니다.

작업의 필드 보기

"필드" 탭에서 이 작업에 적용되는 필드를 확인합니다. 이 필드는 이 작업의 탭에서 만든 필드입니다. 사용되는 필드를 변경하려면 "탭" 탭으로 돌아가 변경해야 하는 탭을 선택합니다.

이 탭을 완료한 후 다음 단계인 [이벤트에 대한 워크플로 프로세스 할당](#) (페이지 75)으로 계속 진행합니다.

하지만 이 Identity Manager 환경에서 워크플로를 사용하지 않는 경우 지금 "제출"을 클릭할 수 있습니다. 작업이 성공했는지 여부를 나타내는 메시지가 표시됩니다. 성공한 경우 역할 구성원이 작업 사용을 시작할 수 있도록 역할에 작업을 추가할 수 있습니다.

역할 사용 보기

"역할 사용" 탭에서 보거나 수정 중인 태스크를 포함하는 역할을 봅니다.

역할 소유자는 태스크를 역할에 추가하거나 역할에서 제거할 수 있습니다.

참고: 기본 관리자 역할은 기본적으로 CA Identity Manager 와 함께 설치된 관리자 역할의 태스크 목록을 제공합니다.

이벤트에 대한 워크플로 프로세스 할당

이 Identity Manager 환경에 대해 워크플로를 사용하도록 설정한 경우 "이벤트" 탭을 사용하여 작업이 시작하는 각 이벤트에 대한 워크플로 프로세스를 선택합니다. 선택한 워크플로 프로세스는 Identity Manager 관리 콘솔에서 기본적으로 선택된 워크플로 프로세스를 무시합니다.

기본 워크플로 매핑에 대한 자세한 내용은 *Configuration Guide*(구성 안내서)의 고급 설정 장을 참조하십시오.

이 작업의 만들기를 완료하려면 "제출"을 클릭합니다. 작업이 성공했는지 여부를 나타내는 메시지가 표시됩니다. 성공한 경우 역할 구성원이 작업 사용을 시작할 수 있도록 역할에 작업을 추가할 수 있습니다.

Active Directory 사용자 저장소 관리

Active Directory 가 사용자 저장소인 경우 관리자 태스크를 만들기 전에 일부 Active Directory 기능을 구성해야 할 수 있습니다.

sAMAccountName 특성

sAMAccountName 특성은 사용자와 그룹에 적용됩니다. 이 특성은 필수이며, 사용자와 그룹을 만드는 데 사용된 작업 화면에 포함되어 있어야 합니다.

참고: 사용자를 만들 때 sAMAccountName 특성 값은 20 자를 초과할 수 없습니다. 그룹에는 이 제한이 적용되지 않습니다.

사용자나 그룹을 만들 때 자동으로 고유한 sAMAccountName 을 생성하는 사용자 지정 논리적 특성 처리기를 작성할 수 있습니다. 이 경우 "사용자 만들기" 및 "그룹 만들기" 화면에서 sAMAccountName 특성을 숨김 필드로 포함할 수 있습니다.

자세한 내용은 *Programming Guide for Java*(Java 프로그래밍 안내서)의 논리적 특성 장을 참조하십시오.

그룹 유형 및 범위

Active Directory에는 다음 두 가지 유형의 그룹이 있습니다.

- 보안 - 리소스 및 개체에 대한 사용 권한을 정의하는 ACL(액세스 제어 목록)에 표시됩니다.
- 배포 - 사용자 및 그룹과 같은 개체를 그룹화하는 데 사용됩니다. 배포 그룹을 사용하여 Active Directory에서 권한을 부여할 수는 없습니다.

각 그룹 유형에는 다음을 결정하는 범위가 있습니다.

- 구성원 위치 - 잠재적 구성원이 있을 수 있는 위치
- 사용 권한 - 그룹을 액세스 권한에 사용할 수 있는 위치(그룹이 보안 그룹인 경우)
- 기타 그룹의 그룹 멤버십 - 그룹이 속할 수 있는 그룹의 위치

각 그룹 유형에는 다음 범위 중 하나가 포함될 수 있습니다.

범위	구성원 위치	권한	기타 그룹의 그룹 멤버십
Universal	그룹 구성원은 Universal 그룹, Global 그룹 및 포리스트에 있는 도메인의 사용자일 수 있습니다.	포리스트의 도메인에서 액세스 권한을 부여하는 데 사용할 수 있습니다.	포리스트의 도메인에 있는 Domain Local 및 Universal 그룹의 구성원일 수 있습니다.

범위	구성원 위치	권한	기타 그룹의 그룹 멤버쉽
Global	그룹 구성원은 Global 그룹 및 그룹과 동일한 도메인에 있는 사용자일 수 있습니다.	포리스트의 도메인에서 액세스 권한을 부여하는 데 사용할 수 있습니다.	포리스트의 도메인에 있는 Global , Domain Local 및 Universal 그룹의 구성원일 수 있습니다.
Domain Local	그룹 구성원은 Universal 그룹, Global 그룹 및 포리스트에 있는 도메인의 사용자일 수 있습니다. 구성원은 동일한 도메인의 Domain Local 그룹일 수도 있습니다.	그룹이 있는 도메인에 대한 액세스 권한을 부여하는 데에만 사용할 수 있습니다.	도메인 내 기타 Domain Local 그룹의 구성원일 수만 있습니다.

그룹 유형과 범위는 필수 특성이 아닙니다. 하지만 그룹 유형과 범위를 지정하지 않으면 **Active Directory** 에서 전역 범위의 보안 그룹을 만듭니다.

다른 유형의 그룹을 만들려면 사용자 지정 논리적 특성 처리기를 만들 수 있습니다. 자세한 내용은 *Programming Guide for Java*(Java 프로그래밍 안내서)의 논리적 특성에 대한 장을 참조하십시오.

이러한 **Active Directory** 기능을 구성한 후 다음 단계인 관리자 작업 만들기로 계속 진행합니다.

응용 프로그램 기능에 대한 외부 작업

외부 태스크에서는 다음을 수행합니다.

- 관리자가 사용자 콘솔에서 **CA Identity Manager** 와 다른 응용 프로그램의 기능을 수행할 수 있도록 허용합니다.
- 선택적으로 응용 프로그램에 정보를 전달하여 사용자, 그룹 또는 조직별 작업을 생성합니다.

예를 들어, 외부 작업은 구입 주문을 생성하는 응용 프로그램에 조직에 대한 정보를 전달할 수 있습니다. 태스크를 수행하는 관리자는 사용자 콘솔에서 조직에 대한 구매 주문을 볼 수 있습니다.

응용 프로그램을 새 브라우저 창에서 열거나 **CA Identity Manager** 관리자 태스크에서 탭으로 표시하여 외부 태스크를 볼 수 있습니다.

외부 작업에는 두 개의 탭을 사용할 수 있습니다. 두 탭은 동일한 방식으로 구성할 수 있지만 다르게 동작합니다.

- "외부" 탭은 시각적 탭이므로 작업이 URL의 콘텐츠를 탭 내에 표시합니다.
- "외부 URL"은 비시각적 탭이므로 작업이 입력된 URL로 리디렉션됩니다.

외부 탭

만들기, 보기 또는 수정 태스크에 외부 탭을 추가하여 해당 태스크를 외부 태스크로 전환할 수 있습니다. 예를 들어, "사용자 만들기" 태스크에 외부 탭을 추가하면 탭이 해당 태스크에 나타납니다.

외부 탭의 경우:

- 외부 태스크에 대해 이벤트가 생성되지 않습니다.
- 선택적으로 관리 개체를 사용할 수 있습니다.
- "외부 URL" 필드에서 응용 프로그램의 주소를 다음과 같은 형식으로 지정할 수 있습니다.
 - 정규화된 도메인 이름을 포함하는 전체 주소(예:
`http://server1.mycompany.org/report/viewUserReport`)
 - 상대 경로(예:
`/report/viewUserReport`)상대 경로를 지정하면 **CA Identity Manager**가 자동으로 **CA Identity Manager**가 설치된 서버의 정규화된 도메인 이름을 추가합니다.
- "프로필" 탭에서 특성이 응용 프로그램에 전달되도록 구성합니다.
- URL에 관리자 고유 이름 또는 태스크 이름을 포함하거나 제외할 수 있습니다.

외부 URL 탭

"사용자 보기"와 같은 보기 태스크에 외부 URL 탭을 추가할 수 있습니다. "사용자 보기" 태스크를 사용하면 URL 로 식별된 웹 사이트로 리디렉션됩니다. 그 외의 다른 탭은 표시되지 않습니다.

외부 URL 탭의 경우:

- 외부 URL 탭은 태스크의 유일한 탭이어야 합니다. 동일한 태스크에 연결된 다른 탭이 있는 경우 외부 탭을 클릭해도 지정된 URL 로 사용자가 리디렉션되지 않습니다.
- 태스크는 감사 대상일 수 있는 이벤트를 생성할 수 있습니다.
- "외부 URL" 필드에서 응용 프로그램의 주소를 다음과 같은 형식으로 지정할 수 있습니다.
 - 정규화된 도메인 이름을 포함하는 전체 주소(예:
`http://server1.mycompany.org/report/viewUserReport`)
 - 상대 경로(예:
`/report/viewUserReport`)
상대 경로를 지정하면 CA Identity Manager 가 자동으로 CA Identity Manager 가 설치된 서버의 정규화된 도메인 이름을 추가합니다.
- 선택적으로 관리 개체를 사용할 수 있습니다.
- URL 로 전달되는 특성을 구성할 수 있습니다.
시작하려는 응용 프로그램의 URL 을 제공하고 응용 프로그램에 전달하려는 특성을 포함합니다.
- URL 에 관리자 고유 이름 또는 태스크 이름을 포함하거나 제외할 수 있습니다.

고급 태스크 구성 요소

고급 태스크 구성 요소를 사용하면 태스크 처리를 사용자 지정할 수 있습니다.

- 태스크 수준 유효성 검사는 태스크의 다른 특성을 사용하여 특성 값의 유효성을 검사합니다. 예를 들어, 사용자가 제공한 전화 번호의 지역 번호가 사용자의 구/군/시 및 시도에 적합한지 확인할 수 있습니다.
- [비즈니스 로직 태스크 처리기](#) (페이지 80)는 CA Identity Manager 태스크가 처리되도록 제출되기 전에 먼저 사용자 지정 비즈니스 로직을 실행합니다. 일반적으로 사용자 지정 비즈니스 로직은 데이터의 유효성을 검사합니다. 예를 들어, 비즈니스 로직 태스크 처리기는 CA Identity Manager 가 그룹에 새 구성원을 추가하기 전에 그룹의 구성원 자격 제한을 검사할 수 있습니다. 그룹 구성원 자격 제한에 도달하는 경우 새 구성원을 추가할 수 없음을 그룹 관리자에게 알리는 메시지가 표시됩니다.

비즈니스 로직 작업 처리기 만들기

다음과 같이 비즈니스 로직 작업 처리기의 정규화된 클래스 이름을 정의합니다.

1. 관리자 작업을 만들거나 수정합니다.
2. "관리자 프로필" 탭에서 "비즈니스 로직 작업 처리기"를 클릭합니다.
"비즈니스 로직 작업 처리기" 화면이 나타납니다. 이 화면에는 작업에 할당된 기존 비즈니스 로직 작업 처리기가 표시됩니다. Identity Manager 는 목록에 표시되는 순서대로 처리기를 실행합니다.
3. "추가"를 클릭합니다.
"비즈니스 로직 작업 처리기 상세 정보" 화면이 나타납니다.

"비즈니스 로직 작업 처리기 상세 정보" 화면을 사용하여 작업에 할당할 비즈니스 로직 작업 처리기에 대해 다음 정보를 정의할 수 있습니다.

이름

비즈니스 로직 작업 처리기에 할당할 이름입니다.

설명

"비즈니스 로직 작업 처리기의 선택적 설명입니다.

자바 클래스

비즈니스 로직 작업 처리기가 자바로 구현된 경우 정규화된 비즈니스 로직 작업 처리기 클래스 이름입니다. 예를 들면 다음과 같습니다.

`com.mycompany.MyJavaBLTH`

Identity Manager 에서 클래스 파일은 사용자 지정 자바 클래스 파일용 루트 디렉터리에 있어야 합니다. 자바 클래스 파일 배포에 대한 자세한 내용은 *Programming Guide for Java*(Java 프로그래밍 안내서)를 참조하십시오.

자바스크립트 파일 이름

비즈니스 로직 작업 처리기가 자바스크립트로 구현되었으며 자바스크립트가 파일에 포함된 경우 이 필드에 파일 이름을 지정합니다. 예를 들어, 여러 작업 화면에서 비즈니스 로직 작업 처리기를 사용하는 경우 자바스크립트를 파일에 포함할 수도 있습니다.

Identity Manager 에서 이 파일은 사용자 지정 자바스크립트 파일용 루트 디렉터리에 있어야 합니다. 자바스크립트 파일 배포에 대한 자세한 내용은 *Programming Guide for Java*(Java 프로그래밍 안내서)를 참조하십시오.

루트의 하위 디렉터리에 파일을 저장하는 경우 자바스크립트 파일 이름을 지정할 때 하위 디렉터리 이름을 포함합니다. 예를 들면 다음과 같습니다.

`JavaScriptSubDir\MyJavaScriptBLTH.js`

슬래시는 자바스크립트 파일이 배포되는 플랫폼에 적합해야 합니다.

자바스크립트

파일 대신 이 필드에 전체 자바스크립트 코드를 입력하여 자바스크립트 비즈니스 로직 작업 처리기를 구현할 수 있습니다. 예를 들어, 스크립트가 매우 짧거나 다른 작업 화면에서 사용되지 않는 경우 자바스크립트를 이 필드에 포함할 수도 있습니다.

속성 및 값

자바 구현에서 이러한 필드는 처리기의 비즈니스 로직에 필요한 방식으로 사용하기 위해 자바 비즈니스 로직 작업 처리기의 `init()` 메서드로 전달되는 데이터의 선택적 이름/값 쌍입니다.

사용자 정의 속성을 추가하려면 속성 이름과 값을 지정한 다음 "추가"를 클릭합니다.

참고: 자바스크립트 비즈니스 로직 작업 처리기를 추가하는 경우 처리기가 로드되도록 응용 프로그램 서버를 다시 시작합니다.

관리자 태스크 및 이벤트

관리자 태스크에는 **CA Identity Manager** 에서 태스크를 완료하기 위해 수행하는 동작인 *이벤트*가 포함되어 있습니다. 한 태스크에 여러 이벤트가 포함될 수도 있습니다. 예를 들어 "사용자 만들기" 태스크에는 사용자 프로필을 만들고 사용자를 그룹에 추가하며 역할을 할당하는 이벤트가 포함될 수 있습니다.

CA Identity Manager 는 이벤트를 감사하고, 이벤트와 연관된 고객별 비즈니스 규칙을 적용하며, 이벤트가 워크플로 프로세스에 매핑된 경우 이벤트에 대한 승인을 요구합니다.

태스크에 대해 여러 이벤트가 생성되고 이벤트가 워크플로 프로세스에 매핑되어 있는 경우 **CA Identity Manager** 가 태스크를 완료하려면 먼저 모든 워크플로 프로세스를 완료해야 합니다.

기본 및 보조 이벤트

일반적으로 이벤트는 다른 이벤트에 독립적입니다. 그러나 일부 태스크는 기본 이벤트 및 하나 이상의 보조 이벤트와 연결되어 있습니다.

- 기본 이벤트가 실패하면 모든 보조 이벤트가 자동으로 거부됩니다. 예를 들어, `CreateUserEvent` 가 실패하면 사용자에게 대해 `AddToGroupEvent` 가 발생할 필요가 없습니다. 또한 연결된 태스크가 취소됩니다.
- 보조 이벤트가 실패해도 태스크에 대해 실행된 다른 이벤트나 태스크 자체의 실행에는 영향을 주지 않습니다. 예를 들어, 사용자 만들기 태스크에서 `AddToGroupEvent` 를 거부하여 새 사용자를 특정 그룹에 추가하지 않을 수 있습니다. 사용자는 계속 생성되고(`CreateUserEvent`) 프로비저닝 역할에 할당될(`AssignProvisioningRoleEvent`) 수 있으며 다른 그룹에 추가될 수도 있습니다.

태스크에 대한 이벤트 보기

CA Identity Manager 사용자 콘솔에서 태스크와 연결된 이벤트를 볼 수 있습니다.

태스크에 대한 이벤트를 보려면

1. 사용자 콘솔에서 "역할 및 태스크"와 "관리자 태스크 보기"를 선택합니다.
2. 해당 태스크를 검색하여 선택합니다.
3. "이벤트" 탭을 선택합니다.
현재 태스크와 연관된 이벤트가 표시됩니다.

수정되지 않은 프로필에 대해 생성된 이벤트

사용자, 그룹, 조직 개체는 각각 사용자 디렉터리에 저장된 일련의 물리적 특성을 포함하고 있습니다. 이러한 개체 중 하나의 물리적 특성이 프로필 탭에서 변경된 경우 Identity Manager 는 사용자가 태스크를 제출한 이후에 "수정..." 이벤트를 생성합니다. 예를 들어, 제목 특성이 "사용자 프로필" 탭에서 변경된 경우 Identity Manager 는 ModifyUserEvent 이벤트를 생성합니다.

사용자, 그룹, 조직 개체가 프로필 탭에 나타나지만 물리적 특성이 사용자가 "제출"을 클릭할 때 변경된 경우 Identity Manager 는 "수정..." 이벤트를 생성하지 않습니다. 대신, 다음과 같이 해당 "보기..." 이벤트가 생성됩니다.

- ViewUserEvent 가 ModifyUserEvent 대신 생성됩니다.
- ViewGroupEvent 가 ModifyGroupEvent 대신 생성됩니다.
- ViewOrganizationEvent 가 ModifyOrganizationEvent 대신 생성됩니다.

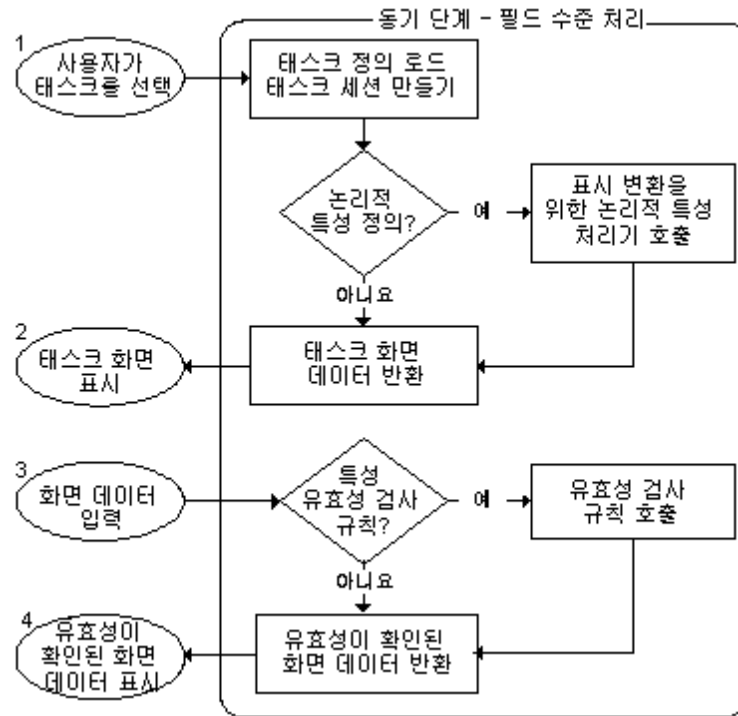
관리자 작업 처리

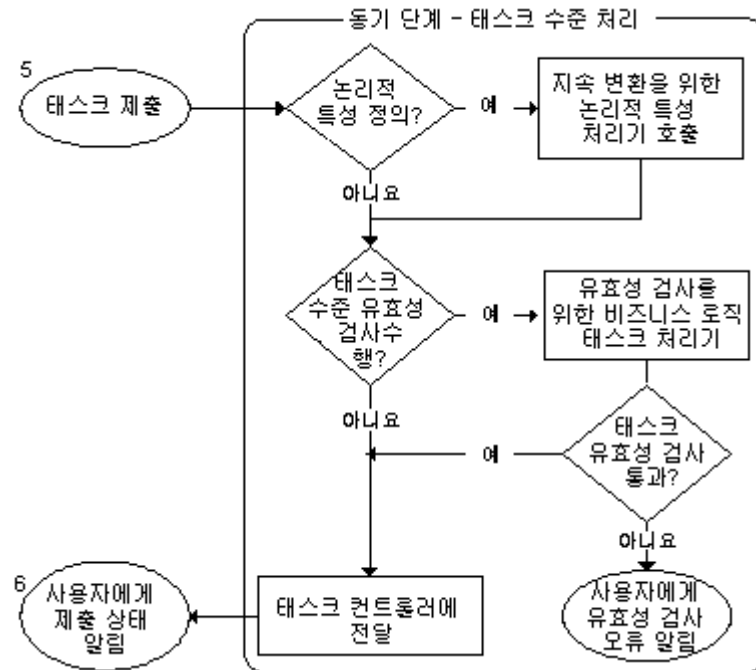
작업 처리 시간은 필요한 단계에 따라 달라집니다. 처리를 위해 작업이 제출되면 CA Identity Manager 가 다음 단계를 수행합니다.

1. CA Identity Manager 가 제출되는 데이터의 유효성을 검사합니다.
이것을 동기식 단계라고 합니다.
2. 작업에 승인이 필요한 경우 CA Identity Manager 가 작업을 워크플로 엔진으로 보냅니다.
 - a. 워크플로 엔진에서 승인자를 결정하고 승인자 작업 목록에 승인 작업을 배치합니다.
 - b. 선택적으로 CA Identity Manager 가 보류 중인 작업 항목의 승인자를 알리는 전자 메일을 보냅니다.
 - c. 승인자가 다른 승인자의 작업 목록에서 항목을 제거하는 작업 항목을 보류하고 항목을 승인하거나 거부합니다.
 - d. 선택적으로 CA Identity Manager 가 관련된 사용자에게 작업 상태를 알리는 전자 메일을 보냅니다.이것을 비동기식 단계라고 합니다.
3. 작업이 거부되지 않은 경우 CA Identity Manager 가 작업을 수행합니다.

동기식 단계 처리

동기식 단계 중 Identity Manager 는 사용자가 태스크 화면에서 입력하는 데이터를 변환 및 검증할 수 있고 데이터를 처리하기 위해 제출하기 전에 해당 데이터에 대해 비즈니스 로직을 강제 실행할 수 있습니다. 다음 다이어그램은 이 단계 중 발생하는 동작에 대한 전체 설명을 제공합니다.

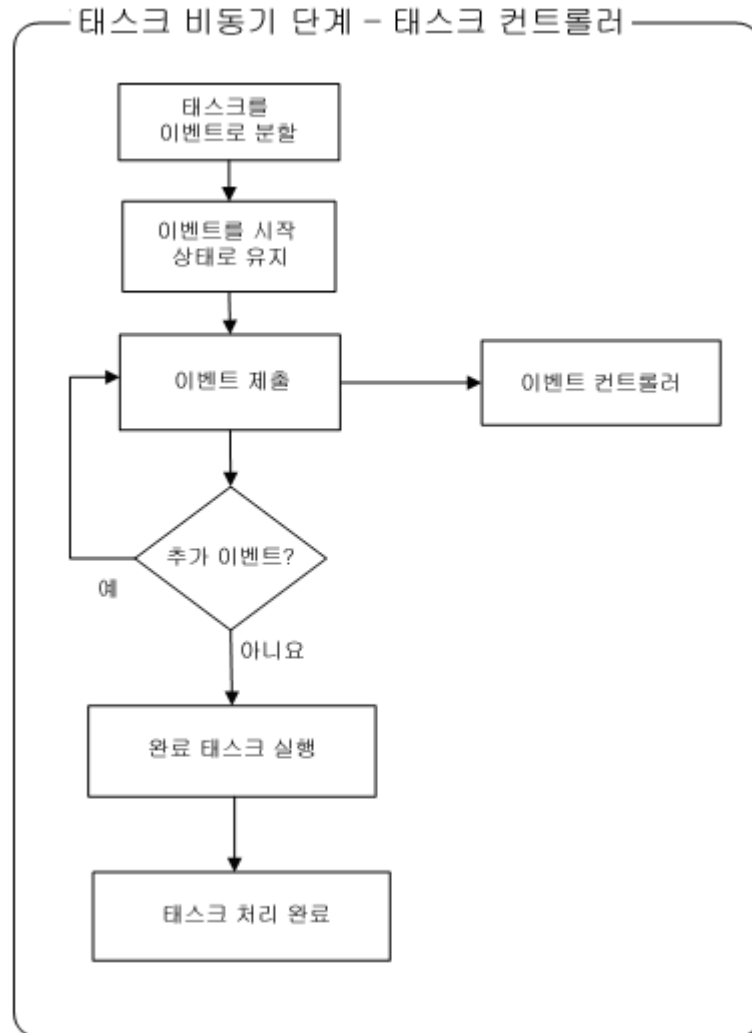




비동기식 단계 처리

동기식 단계를 완료하면 태스크는 비동기식 실행 단계로 들어갑니다. 이 단계에서 태스크는 하나 이상의 이벤트를 생성합니다. 이 이벤트는 사용자 프로필 만들거나 그룹에 사용자 추가와 같이 사용자가 정의했거나 감사 로그에 정보 기록과 같은 시스템에서 생성했을 수 있습니다.

Identity Manager 서버의 구성 요소인 태스크 컨트롤러는 다음 그림과 같이 태스크 및 태스크 이벤트의 수명 주기를 책임집니다.



대부분의 이벤트에 대해 수명 주기, 실행 및 작업은 다른 이벤트와 독립적입니다. 만들기 태스크를 수행하려면 보조 이벤트 전에 기본 개체의 만들기 이벤트를 실행해야 합니다.

일반적으로 이벤트는 다음 상태로 전환됩니다.

- 시작
- 보류
- 승인됨
- 실행
- 완료함
- 게시

참고: Identity Manager 는 특정 이벤트 또는 이벤트 그룹을 "수신하는" **EventListeners** 라는 후크를 제공합니다. 이벤트가 발생할 때 이벤트 수신기가 이벤트 및 현재 이벤트 상태에 적합한 사용자 지정 비즈니스 로직을 수행합니다. 이벤트 수신기 API 를 사용하여 사용자 지정 이벤트 수신기를 작성할 수 있습니다. 자세한 내용은 *Programming Guide for Java*(Java 프로그래밍 안내서)를 참조하십시오.

관리자 태스크 이미지

홈 페이지에서 추가한 관리자 태스크에 사용할 이미지를 만들 수 있습니다.

제 4 장: 사용자

이 섹션은 다음 항목을 포함하고 있습니다.

[사용자 만들기](#) (페이지 89)

[사용자가 자체 등록할 수 있도록 허용](#) (페이지 94)

사용자 만들기

사용자 프로필을 통해 관리자는 사용자 정보를 관리하고 권한, 응용 프로그램 및 서비스 액세스를 관리하며 사용자에게 자신의 계정과 서비스에 대한 자체 관리 권한을 부여할 수 있습니다. 사용자 프로필 만들기는 시스템 관리자의 일반 태스크입니다.

사용자 만들기 및 구성을 수행하는 경우 다음 사용자 계정 요소를 고려하십시오.

자체 서비스 태스크: 사용자 프로필은 기본적으로 사용자에게 특정 자체 서비스 태스크(예: 암호 및 프로필 정보 변경)에 대한 액세스 권한을 부여하도록 구성되어 있습니다. 적절한 태스크가 있는 시스템 관리자는 기본적으로 사용자에게 부여되어 있는 자체 서비스 태스크를 수정할 수 있습니다.

그룹: 그룹은 역할 관리를 간소화합니다. 예를 들어 적절한 태스크가 있는 시스템 관리자는 그룹 구성원으로 추가된 사용자에게 자동으로 할당할 시스템의 역할을 여러 개 구성할 수 있습니다.

관리자 역할: 관리자 역할은 사용자가 사용자 콘솔에서 수행할 수 있는 태스크를 정의합니다. 예를 들어 주소, 직책 등의 사용자 계정 정보를 사용자가 수정할 수 있도록 허용하는 태스크를 정의할 수 있습니다. 한 사용자가 다른 사용자에게 그룹 구성원 자격을 부여하는 등 태스크를 관리할 수 있는 다른 태스크도 정의할 수 있습니다. 사용자에게 관리자 역할을 할당하면 해당 사용자가 역할과 관련된 태스크를 수행할 수 있습니다.

끝점 계정 및 프로비저닝 역할: 다른 시스템에 존재하는 계정은 끝점 계정으로 명명됩니다. 프로비저닝 역할을 통해 끝점에 있는 계정을 CA CloudMinder 사용자에게 할당할 수 있습니다. 예를 들어 사용자에게 전자 메일용 Exchange 계정, 데이터베이스 액세스용 Oracle 계정 및 Windows 시스템용 Active Directory 계정이 필요한 경우를 생각해 봅시다. 이 경우 사용자에게 프로비저닝 역할을 할당하면 해당 사용자는 프로비저닝 역할이 지정하는 끝점 계정을 받습니다.

액세스 역할: 액세스 역할은 CA Identity Manager 나 다른 응용 프로그램에서 권한을 제공하는 방법을 추가로 제공합니다. 예를 들어 액세스 역할을 사용하여 다음을 수행할 수 있습니다.

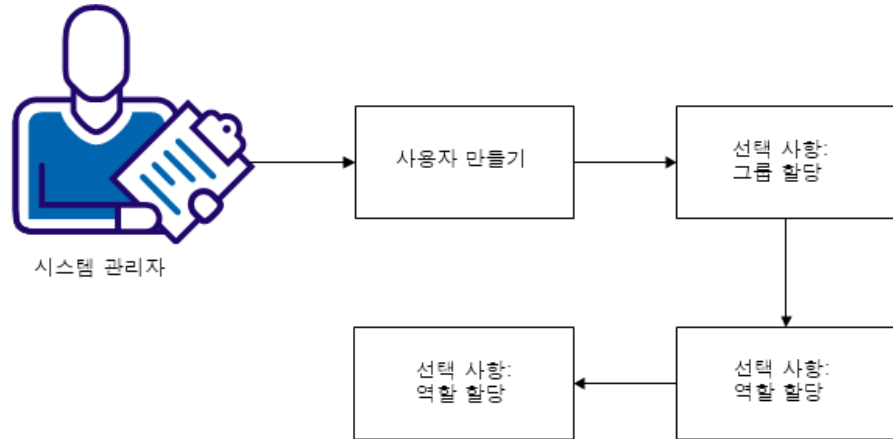
- 사용자 특성에 대한 간접 액세스 제공
- 복합 식 만들기
- 다른 응용 프로그램에서 권한을 결정하는 데 사용되는 사용자 프로필의 특성 설정

서비스: 서비스를 사용하면 선택한 사용자 태스크, 역할, 그룹 및 특성을 단일 패키지로 결합할 수 있습니다. 이 권한 패키지를 하나의 집합으로 관리할 수 있습니다. 예를 들어 새 "영업" 직원 모두에게 태스크, 특정 끝점 시스템의 계정 및 해당 직원의 사용자 계정 프로필에 추가된 정보의 정의된 집합에 대한 액세스가 필요한 경우를 생각해 봅시다. 이 경우 사용자에게 서비스를 할당하면 해당 사용자는 서비스가 지정하는 역할, 태스크, 그룹 및 계정 특성의 전체 집합을 받습니다.

암호 정책: 암호 정책은 암호 만료, 조합 및 사용을 제어하는 규칙과 제한을 강제 적용하여 사용자 암호를 관리합니다. 시스템 관리자가 환경에 대한 암호 정책을 만든 경우 해당 정책은 하나 이상의 암호 정책 규칙과 일치하는 새 사용자에게 자동으로 적용됩니다. 적절한 태스크가 있는 시스템 관리자는 암호 정책을 수정할 수 있습니다.

다음 다이어그램에서는 사용자 만들기 및 구성을 수행할 때 이해해야 할 정보와 수행해야 할 단계를 보여 줍니다.

사용자 만들기 및 구성



다음 항목에서는 사용자 만들기에 대해 자세히 설명하고 사용자를 구성하는 방법에 대해서도 설명합니다.

1. [사용자 만들기](#) (페이지 91)
2. [그룹 할당](#) (페이지 92)(필요한 경우)
3. [사용자에게 역할 할당](#) (페이지 93)(필요한 경우)
4. [서비스 할당](#) (페이지 94) (필요한 경우)

사용자 프로필 만들기

사용자 프로필을 만들려면 이 절차를 사용하십시오. "사용자 만들기" 태스크를 구성하는 방법에 따라 이 태스크를 사용하여 추가 프로필 요소를 정의할 수도 있습니다. 사용자를 그룹에 추가하거나 관리자 또는 프로비저닝 역할의 구성원으로 만들 수 있습니다.

다음 단계를 수행하십시오.

1. 사용자 관리 태스크가 있는 사용자로 사용자 콘솔에 로그인합니다.
기본 "사용자 매니저" 역할이 있으면 적절한 태스크가 부여됩니다.
2. "태스크", "사용자", "사용자 관리", "사용자 만들기"를 차례로 선택합니다.
"사용자 만들기" 태스크가 열립니다.
3. 필요에 따라 사용자 프로필 정보 필드를 작성합니다.
4. "다음"을 클릭합니다.
5. 해당되는 경우 태스크의 다른 탭에 있는 필드를 작성합니다.
예를 들어 해당 옵션을 사용할 수 있는 경우 그룹에 사용자를 추가하거나 사용자에게 관리자 역할, 프로비저닝 역할 또는 서비스를 할당합니다.
6. "마침"을 클릭합니다.
사용자가 만들어집니다.

사용자에게 그룹 할당

사용자를 그룹의 구성원으로 만들 수 있습니다.

다음 단계를 수행하십시오.

1. 사용자 관리 태스크가 있는 사용자로 사용자 콘솔에 로그인합니다.
2. "태스크", "그룹", "그룹 구성원 수정"을 차례로 선택합니다.
관리할 수 있는 그룹 목록이 나타납니다.
3. 그룹을 선택하고 "선택"을 클릭합니다.
그룹에 할당된 사용자 목록이 나타납니다.
4. "사용자 추가"를 클릭합니다.
5. 그룹에 할당할 사용자를 검색합니다.
관리 권한이 있는 사용자를 모두 나열하는 목록을 표시하려면 검색 조건을 수정하지 않고 "검색"을 클릭합니다.

6. 사용자를 선택하고 "선택"을 클릭합니다.
그룹에 할당된 사용자 목록이 업데이트되어 나타납니다.
7. "제출"을 클릭합니다.
지정된 사용자가 그룹의 구성원이 됩니다.

사용자에게 역할 할당

개별 사용자에게 프로비저닝 역할을 할당할 수 있습니다.

다음 단계를 수행하십시오.

1. "프로비저닝 역할 구성원/관리자 수정" 태스크가 있는 사용자로 사용자 콘솔에 로그인합니다.
2. "역할 및 태스크"를 선택합니다.
3. 다음 태스크 중 하나를 선택합니다.
 - 관리자 역할, 관리자 역할 구성원/관리자 수정
 - 프로비저닝 역할, 프로비저닝 역할 구성원/관리자 수정
 - 액세스 역할, 액세스 역할 구성원/관리자 수정

검색 화면이 나타납니다.
4. 사용자에게 할당할 역할을 선택합니다.
"구성원 자격" 탭이 나타납니다.
5. "사용자 추가"를 클릭합니다.
6. 역할에 할당할 사용자를 검색합니다.
관리 태스크가 있는 사용자를 모두 나열하는 목록을 표시하려면 검색 조건을 수정하지 않고 "검색"을 클릭합니다.
7. 사용자를 선택하고 "선택"을 클릭합니다.
8. "제출"을 클릭합니다.
지정된 역할이 사용자에게 할당됩니다.

사용자에게 서비스 할당

개별 사용자에게 서비스를 직접 할당할 수 있습니다. 이 사용자는 서비스의 구성원이 됩니다.

다음 단계를 수행하십시오.

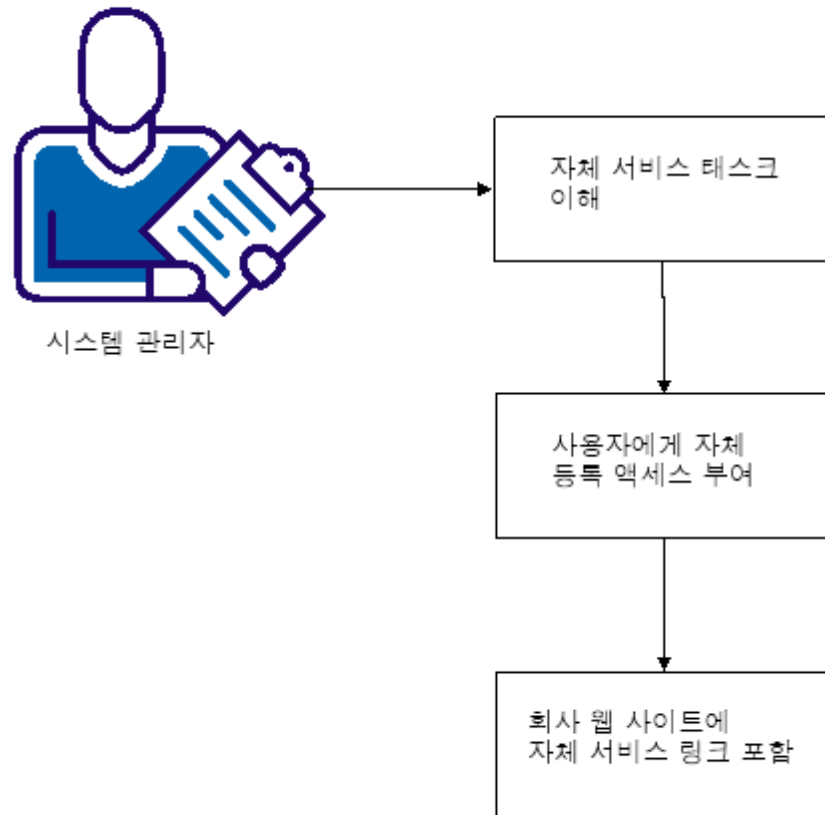
1. "서비스", "액세스 요청 및 보기"로 이동합니다.
관리할 수 있는 서비스 목록이 나타납니다.
2. 사용자에게 할당할 서비스를 선택하고 "선택"을 클릭합니다.
서비스에 할당된 사용자 목록이 나타납니다.
3. "액세스 요청"을 클릭합니다.
4. 서비스를 할당할 사용자를 검색합니다.
관리 권한이 있는 사용자를 모두 나열하는 목록을 표시하려면 검색 조건을 수정하지 않고 "검색"을 클릭합니다.
5. 사용자를 선택하고 "선택"을 클릭합니다.
서비스에 할당된 사용자 목록이 업데이트되어 나타납니다.
6. "변경 내용 저장"을 클릭합니다.
사용자가 지정된 서비스를 받습니다. 이 사용자는 서비스에 추가한 모든 응용 프로그램, 역할, 그룹, 특성을 받습니다.

사용자가 자체 등록할 수 있도록 허용

자체 서비스 태스크를 통해 사용자가 자신의 환경을 관리할 수 있습니다. "자체 등록" 태스크를 통해 사용자가 공용 사용자 콘솔에서 자신의 사용자 계정과 프로필을 만들 수 있습니다. 예를 들어 Bentley Cola의 경우 Bentley Cola 회사 웹 사이트에 포함된 링크를 통해 새 직원과 고객이 자신의 사용자 계정과 프로필을 만들 수 있습니다.

다음 다이어그램에서는 사용자가 자체 등록할 수 있도록 허용할 때 이해해야 할 정보와 수행해야 할 단계를 보여 줍니다.

사용자에게 자체 등록 허용



다음 항목에서는 사용자에게 자체 등록 액세스를 부여하는 방법에 대해 자세히 설명합니다.

1. [자체 서비스 태스크 이해](#) (페이지 96)
2. [사용자에게 자체 등록 액세스 부여](#) (페이지 97)
3. [회사 웹 사이트에 자체 서비스 링크 포함](#) (페이지 98)

자체 서비스 태스크

자체 서비스 태스크는 사용자가 자신의 프로필을 관리하기 위해 대개 사용자 콘솔을 통해 수행할 수 있는 태스크입니다. 사용자 계정은 기본적으로 사용자에게 암호 및 프로필 정보 변경 등의 특정 자체 서비스 태스크에 대한 액세스 권한을 부여하도록 구성되어 있습니다. 적절한 권한이 있는 시스템 관리자는 사용자에게 기본적으로 부여되는 자체 서비스 태스크를 수정할 수 있습니다.

자체 서비스 태스크는 다음 두 가지 유형으로 나뉘어집니다.

- 공용 태스크 - 사용자가 로그인 자격 증명을 제공하지 않고 액세스할 수 있는 태스크입니다. 공용 태스크의 예로 자체 등록, 잊어버린 암호 및 잊어버린 사용자 ID 태스크가 있습니다.
- 보호된 태스크 - 사용자가 유효한 자격 증명을 제공하는 태스크입니다. 예를 들어, 암호 또는 프로필 정보 변경 태스크가 포함됩니다.

다음 표에는 기본 자체 서비스 태스크가 나열되어 있습니다.

태스크 유형	태스크
공용 태스크	■ 자체 등록 - 사용자가 회사 웹 사이트에서 등록할 수 있게 합니다. ■ 잊어버린 암호 다시 설정 - 사용자가 잊어버린 암호를 다시 설정할 수 있게 합니다. ■ 잊어버린 암호 - 사용자가 CA Identity Manager 에 로그인하는 데 사용할 수 있는 임시 암호를 표시합니다. 사용자가 로그인하면 새 암호를 입력하라는 메시지가 표시됩니다. ■ 잊어버린 사용자 ID - 잊어버린 사용자 ID 를 검색하거나 다시 설정합니다.

태스크 유형	태스크
보호된 태스크	■ 액세스 요청 및 보기 - 사용자가 서비스 액세스를 요청 및 제거할 수 있게 합니다. ■ 내 암호 변경 - 사용자가 자신의 암호를 다시 설정할 수 있게 합니다. ■ 내 프로필 수정 - 주소, 전화 번호와 같은 프로필 정보를 유지 관리합니다. ■ 내 그룹 수정 - 사용자가 그룹에 등록할 수 있게 합니다. ■ 내 역할 보기 - 사용자의 역할이 표시됩니다. ■ 내 제출된 태스크 보기 - 사용자가 시작한 CA Identity Manager 태스크를 표시합니다.

자체 서비스 태스크에 액세스

환경에 대한 자체 서비스 태스크를 구성한 후 회사 웹 사이트에 해당 태스크의 URL 을 추가할 수 있습니다.

자체 서비스 태스크의 URL 형식은 다음과 같습니다.

`https://domain/iam/im/public_alias/ui7/index.jsp?task.tag=task_tag`

설명:

- *domain* 은 CA CloudMinder 를 실행 중인 환경에 있는 웹 서버의 정규화된 도메인 이름입니다.
- *public_alias* 는 환경의 공용 별칭입니다. 시스템 관리자는 환경이 생성될 때 공용 별칭을 정의합니다.
- *task_tag* 는 태스크의 고유한 식별자입니다.

"잊어버린 암호 다시 설정" 기본 태스크의 태스크 태그는 다음과 같습니다.

ForgottenPasswordReset

https://domain/iam/im/public_alias/ui7/index.jsp?task.tag=ForgottenPasswordReset

"잊어버린 사용자 ID" 기본 태스크의 태스크 태그는

ForgottenUserID 입니다.

https://domain/iam/im/public_alias/ui7/index.jsp?task.tag=ForgottenUserID

회사 웹 사이트에 자체 서비스 링크 포함

회사 웹 사이트에서 공용 자체 서비스 태스크에 액세스할 수 있도록 임의 웹 페이지로의 링크를 추가할 수 있습니다. 사용자가 링크를 클릭하면 태스크 화면이 열립니다. 사용자가 태스크를 완료하면 사용자는 기본적으로 사용자 콘솔로 리디렉션됩니다.

사용자가 리디렉션되는 페이지를 변경하려면 다음과 같이 링크와 연결된 URL 에 task.RedirectURL 태그를 추가할 수 있습니다.

```
<A  
href="http://domain/iam/im/public_alias/ui7/index.jsp?task.tag=tasktag&  
task.RedirectURL=http://domain/redirect_URL">link text</A>
```

domain

CA Identity Manager 를 실행 중인 환경에 있는 웹 서버의 정규화된 도메인 이름입니다.

public_alias

공용 태스크에 액세스하기 위해 URL 에 추가된 고유 문자열입니다.

공용 태스크는 자체 등록 또는 잊어버린 암호 태스크와 같은 자체 서비스 태스크입니다. 사용자가 공용 태스크에 액세스하기 위해 로그인할 필요가 없습니다.

참고: 공용 태스크 및 별칭에 대한 자세한 내용은 *Configuration Guide(구성 안내서)*를 참조하십시오.

tasktag

태스크의 고유한 식별자입니다. 태스크 태그를 확인하려면 "관리자 태스크 수정"을 사용하여 태스크의 프로필을 보십시오.

redirect_URL

사용자가 태스크를 제출한 후 리디렉션되는 URL 입니다.

예를 들어 사용자가 자체 등록한 후에 시작 페이지로 리디렉션되도록 할 수 있습니다.

link text

대상 URL 에 액세스하기 위해 사용자가 클릭하는 텍스트입니다.

예를 들어 회사는 사용자가 잊어버린 암호를 다시 설정한 다음 시작 페이지로 리디렉션되는 링크를 추가할 수 있습니다.

다음 HTML 은 링크 텍스트의 예를 나타냅니다.

```
<A href="http://myserver.mycompany.org/iam/im/Employees/ui7/index.jsp?task.tag=ForgottenPasswordReset&task.RedirectURL=http://myserver.mycompany.org/welcome.html">Reset My Password</A>
```

사용자들이 자체 서비스 태스크를 액세스한 페이지로 사용자를 돌려보내려면 다음과 같이 task.RedirectURL 태스크의 값으로 RefererURL 을 지정하십시오.

```
<A href="http://domain/iam/im/public_alias/ui7/index.jsp?task.tag=tasktag&task.RedirectURL=RefererURL">
```

여러 개의 자체 서비스 작업 구성

서로 다른 사용자 유형에 대해 여러 개의 자체 서비스 작업을 만들 수 있습니다. 예를 들어, 새 직원을 등록하는 작업과 고객을 등록하는 작업을 만들 수 있습니다. 여러 개의 자체 등록 작업을 사용하여 다음을 수행할 수 있습니다.

- 서로 다른 정보 수집
- 서로 다른 조직의 사용자 등록
- 등록 후 사용자를 서로 다른 로그아웃 페이지로 리디렉션
- 서로 다른 브랜딩 사용

다음 그림에서는 각각 새 직원과 고객의 자체 등록 작업을 보여 줍니다.

직원의 자기 등록

• = 필수

MyCompany.com에 오신 것을 환영합니다! 주셔서 감사합니다 우리 팀에 합류.

•이름(성 제외)

•성(이름)

•암호 선택

•암호 다시 입력

보안 질문 1

 대답 1

전자 메일

고객 자가 등록

• = 필수

MyCompany.Com에 대한 관심에 감사드립니다. 저희 제품에 대한 정보를 받아보시려면
다음 자료를 제공해 주십시오:

•이름(성 제외)

•성(이름)

회사

제목

•암호 선택

•암호 다시 입력

보안 질문 1

대답 1

전자 메일

동일한 유형의 자체 서비스 작업을 여러 개 구성하려면 작업을 만들 때
고유한 태그를 지정합니다. "태그" 필드는 작업의 "프로필 구성" 화면에
있습니다.

태스크에 액세스하기 위한 링크를 웹 사이트에 추가하는 경우 태스크
태그를 추가하여 고유한 URL 을 만듭니다.

예를 들어, 다음과 같이 두 개의 작업을 만들 수 있습니다.

작업	태그	URL
새 직원으로 등록	selfregistration_e mployee	http://domain/iam/im/alias/index.jsp? task.tag=SelfRegistration_employee

작업	태그	URL
고객으로 등록	selfregistration_customer	http://domain/iam/im/alias/index.jsp?task.tag=SelfRegistration_customer

자체 관리자 역할에 대한 액세스 제한

사용자가 프로필 정보를 관리하고 해당 역할 및 제출한 태스크를 볼 수 있게 하는 자체 관리자 역할이 기본적으로 모든 사용자에게 할당됩니다.

사용자의 하위 세트에 자체 관리자 역할을 제공하려면 기존 구성원 정책을 삭제하고 관리자 역할의 구성원 정책 정의에 설명된 대로 새 정책을 만듭니다.

제 5 장: 암호 관리

이 섹션은 다음 항목을 포함하고 있습니다.

[Identity Manager 의 암호 관리](#) (페이지 105)

[암호 정책 개요](#) (페이지 106)

[암호 정책 만들기](#) (페이지 107)

[암호 정책 관리](#) (페이지 123)

[암호 정책 및 관계형 데이터베이스](#) (페이지 123)

[CA CA Identity Manager 및 Siteminder 통합 암호 조건](#) (페이지 123)

[암호 재설정 또는 계정 잠금 해제](#) (페이지 124)

[끝점의 암호 동기화](#) (페이지 135)

Identity Manager 의 암호 관리

Identity Manager 에는 사용자 암호를 관리하기 위한 여러 기능이 포함되어 있습니다.

- 암호 정책 - 이 정책은 암호 만료, 컴퍼지션 및 사용을 제어하는 규칙과 제한을 적용하여 사용자 암호를 관리합니다.
- 암호 관리자 - "암호 관리자" 역할을 가진 관리자는 사용자가 헬프 데스크에 문의할 때 암호를 재설정할 수 있습니다.
- 자체 서비스 암호 관리 - Identity Manager 에는 사용자가 자신의 암호를 관리할 수 있게 하는 여러 개의 자체 서비스 작업이 포함되어 있습니다. 이러한 작업의 예는 다음과 같습니다.
 - 자체 등록 - 사용자가 회사 웹 사이트에서 등록할 때 암호를 지정합니다.
 - 내 암호 변경 - IT 또는 헬프 데스크 직원의 도움 없이 사용자가 자신의 암호를 수정할 수 있습니다.
 - 잊어버린 암호 - Identity Manager 가 아이덴티티를 확인한 후 사용자가 잊어버린 암호를 재설정하거나 검색할 수 있습니다.
 - 암호 재설정 또는 계정 잠금 해제--잊어버린 암호를 재설정 또는 검색하거나 Identity Manager 를 액세스하는 시스템의 Windows 계정을 잠금 해제할 수 있습니다.
 - 잊어버린 사용자 ID - Identity Manager 가 아이덴티티를 확인한 후 사용자가 잊어버린 사용자 ID 를 검색할 수 있습니다.

- 끝점 계정의 암호 동기화 - 암호 변경이 Identity Manager, 프로비저닝 서버 및 대상 시스템에서 동기화됩니다. 새 암호는 Identity Manager 암호 정책과 비교하여 확인됩니다.

암호 정책 개요

암호 정책은 규칙 및 제한 집합입니다. 이러한 규칙은 암호 생성과 만료를 지정합니다. CA Identity Manager 환경에서 구성하는 암호 정책은 해당 환경과 관련된 사용자 저장소에 적용됩니다. 사용자 디렉터리가 여러 환경과 관련된 경우 한 환경에서 정의한 암호 정책이 다른 환경에서도 적용될 수 있습니다.

암호 정책에서 다음과 같은 설정을 구성할 수 있습니다.

참고: 이러한 설정 중 일부를 사용하려면 특정 특성에 대한 사용자 디렉터리 매핑이 필요합니다. [추가 암호 정책 사용](#) (페이지 107)을 참조하십시오.

- 특정 사용자 집합에 암호 적용
- 암호 만료 - 암호가 만료되게 한 이벤트(예: 경과한 일수 또는 실패한 로그인 시도 횟수)를 정의합니다. 암호가 만료되면 사용자 계정을 사용할 수 없습니다.
- 암호 컴퍼지션 - 새 암호의 콘텐츠 요구 사항을 지정합니다. 예를 들어, 사용자가 8 자 이상이고 숫자와 문자를 포함하는 암호를 만들어야 하는 설정을 구성할 수 있습니다.
- 정규식 - 유효한 암호의 형식을 결정하는 표현식을 제공합니다. 암호가 해당 형식과 일치하는지 여부를 지정할 수 있습니다. 여러 정규식을 지정할 수도 있습니다.
- 암호 제한 - 암호 재사용에 대한 제한을 설정합니다. 예를 들어, 사용자가 암호를 재사용하려면 90 일 동안 기다려야 합니다.
- 고급 암호 옵션 - CA Identity Manager 가 암호를 처리하기 전에 수행해야 하는 동작(예: 암호를 소문자로 만들기)을 지정합니다. 여러 암호 정책이 적용되는 경우 암호 정책의 우선 순위를 지정할 수도 있습니다.

SiteMinder 사용자는 SiteMinder 관리자 사용자 인터페이스에서 암호 정책을 구성할 수도 있습니다. 이러한 정책은 CA Identity Manager 사용자 콘솔에 나타납니다.

참고: CA Identity Manager 가 SiteMinder 와 통합된 경우 SiteMinder 가 모든 암호 정책을 강제 적용합니다.

암호 정책 만들기

CA Identity Manager 사용자 콘솔을 통해 암호 정책을 만듭니다.

참고: 일부 암호 정책 옵션을 사용하려면 잘 알려진 특정 특성을 매핑해야 합니다. [추가 암호 정책 사용](#) (페이지 107)을 참조하십시오.

다음 단계를 수행하십시오.

1. "사용자 콘솔"에서 다음 중 하나를 선택합니다.
 - "정책", "암호 정책 관리", "암호 정책 만들기"
 - "태스크", "정책", "암호 정책 관리", "암호 정책 만들기"
2. 암호 정책의 고유한 이름과 선택적 설명을 입력합니다.
3. 구현에 가장 적합하도록 다음 암호 정책 설정을 구성합니다.
 - [사용자 집합에 암호 정책 적용](#) (페이지 108)
 - [암호 만료 구성](#) (페이지 110)
 - [암호 조합 구성](#) (페이지 114)
 - [정규식 지정](#) (페이지 116)
 - [암호 제한 설정](#) (페이지 118)
 - [고급 암호 옵션 구성](#) (페이지 122)

추가 암호 정책 사용

CA Identity Manager 를 사용하면 암호 만료, 조합 및 사용을 강제 적용하여 사용자 암호를 관리하는 기본 암호 정책을 만들 수 있습니다. 다음 암호 규칙과 제한을 추가로 정의할 수도 있습니다.

- 암호 만료:
 - 실패한 로그인 추적 또는 성공한 로그인 추적
 - 로그인 인증
 - 변경하지 않으면 암호가 만료됨

- 암호 미사용
- 잘못된 암호
- 여러 정규식
- 암호 제한:
 - 재사용하기 전 최소 일수
 - 다시 사용하기까지 남은 최소 암호 수
 - 마지막 암호와의 차이(백분율)
 - 차이점을 확인할 때 시퀀스 무시

다음 단계를 수행하십시오.

1. 관리 콘솔에서 "디렉터리", <디렉터리 이름>, "사용자"로 이동합니다.
2. %PASSWORD DATA% 및 %ENABLED STATES% -> 'STATE'가 물리적 특성에 매핑되었는지 확인합니다.
3. 이러한 특성은 기본적으로 샘플 `directory.xml` 파일에서 매핑됩니다. 이러한 특성이 매핑되지 않은 경우 *CA Identity Manager Configuration Guide*(CA Identity Manager 구성 안내서)에서 추가 정보를 참조하십시오.

사용자 집합에 암호 정책 적용

암호 정책이 적용되는 사용자 집합을 결정하는 규칙을 지정할 수 있습니다. 이 기능을 사용하면 일반 직원에 대해 하나의 암호 정책을 사용하고 고급 관리자에 대해 보다 엄격한 정책을 사용할 수 있습니다.

다음 단계를 수행하십시오.

1. 사용자 콘솔에서 암호 정책을 만들거나 수정합니다.
2. "디렉터리 필터" 필드에서 구성할 필터 유형을 선택합니다.

각 필터 유형에 대한 설명은 다음 표를 참조하십시오.

참고: 암호 정책이 적용되는 사용자 저장소 유형에 따라 "디렉터리 필터" 목록 상자에 대한 옵션이 결정됩니다. CA Identity Manager 가 SiteMinder 와 통합된 경우 일부 필터 유형은 관계형 데이터베이스와 CA Directory 사용자 저장소에 사용할 수 없습니다.

3. 특성과 연산자를 선택하고 값을 입력하여 조건을 지정합니다.
4. 다른 규칙을 추가하려면 더하기 부호를 클릭합니다.

다음 표에서는 디렉터리 필터 유형에 대한 옵션을 설명하고 각 필터 유형의 예를 제공합니다. 다음 예에서 "=" 왼쪽에 있는 특성은 사용자 디렉터리 정의 영역에서 미리 지정한 것과 같습니다. "만들기" 유형 사용자 태스크의 경우 디렉터리 필터가 구성된 암호 정책은 다음 조건을 모두 충족하는 경우에만 적용됩니다.

- CA Identity Manager 가 SiteMinder 와 통합되지 않았습니다.
- 디렉터리 필터 유형이 "사용자", "그룹", "그룹 필터" 또는 "그룹 검색"이 아닙니다.

필터 유형	용도	예
조직 내	조직을 탐색하고 선택합니다.	
그룹 내	그룹을 탐색하고 선택합니다.	
사용자	단일 사용자를 탐색하고 선택합니다.	
사용자 필터 (SiteMinder 와 통합된 경우 관계형 데이터베이스에 사용할 수 없음)	사용자에 대한 필터 지정	직원 유형 = 계약자 부서 = 보안
사용자 검색 표현식	사용자에 대한 검색 쿼리를 입력합니다.	uid=jsmith(LDAP 의 경우) TBLUSERS.ID = jsmith(관계형 데이터베이스의 경우)
그룹 필터 (SiteMinder 와 통합된 경우 관계형 데이터베이스에 사용할 수 없음)	그룹에 대한 필터를 지정합니다.	자체 구독 = *
그룹 검색 표현식	그룹에 대한 검색 쿼리를 입력합니다.	cn=Sales(LDAP 의 경우) TBLGROUPS.NAME=GroupA(관계형 데이터베이스의 경우)

필터 유형	용도	예
조직 필터 (SiteMinder 와 통합된 경우 관계형 데이터베이스에 사용할 수 없음)	조직에 대한 필터를 지정합니다.	조직 이름 = *Marketing
조직 검색 표현식	조직에 대한 검색 쿼리를 입력합니다.	ou=Boston(LDAP 의 경우) TBLORGANIZATIONS.NAME= Boston(관계형 데이터베이스의 경우)
검색	필터 유형에 대한 기타 옵션에 포함되지 않은 쿼리를 지정합니다.	(&(uid=*smith)(ou=Boston))

암호 만료 구성

사용자 액세스 관리를 돕기 위해 여러 번 실패한 로그인 시도, 장시간 계정 미사용 등의 이벤트를 정의할 수 있습니다. 이러한 이벤트가 발생하면 **CA Identity Manager** 는 이벤트 발생을 초래한 사용자 계정을 사용하지 않도록 설정합니다. **CA Identity Manager** 가 **SiteMinder** 와 통합된 경우에는 리디렉션을 지정할 수 있습니다.

참고: 이러한 설정을 사용하려면 추가 구성이 필요합니다. [추가 암호 정책 사용](#) (페이지 107)을 참조하십시오.

다음 암호 만료 설정을 구성할 수 있습니다.

- "실패한 로그인 추적"/"성공한 로그인 추적" 확인란
- "로그인 인증 추적 실패" 확인란
- "변경하지 않으면 암호가 만료됨" 설정
- "암호가 장시간 미사용으로 만료되었습니다" 설정
- "잘못된 암호" 설정

"실패한 로그인 추적"/"성공한 로그인 추적" 확인란

이 확인란은 마지막 로그인 시도 시간을 포함하여 사용자 로그인 시도 추적을 사용하거나 사용하지 않도록 설정합니다. 이 확인란을 사용하도록 설정하면 로그인 정보가 사용자 저장소의 암호 데이터 특성에 기록됩니다.

참고: 이 설정을 사용하려면 추가 구성이 필요합니다. [추가 암호 정책 사용](#) (페이지 107)을 참조하십시오.

"실패한 로그인 추적" 확인란을 사용하도록 설정하면 "잘못된 암호" 섹션과 "로그인 인증 추적 실패" 확인란이 활성화됩니다. "성공한 로그인 추적" 확인란을 사용하도록 설정하면 "암호가 장시간 미사용으로 만료되었습니다" 섹션과 "로그인 인증 추적 실패" 확인란이 활성화됩니다.

여러 암호 정책이 있는 경우에는 해당되는 암호 정책 모두에서 로그인 정보를 사용하지 않도록 설정해야 합니다. 그러지 않으면 로그인 정보 추적을 사용하도록 설정한 단일 정책으로 인해 암호 정책이 잘못 작동할 수 있습니다.

"로그인 인증 추적 실패" 확인란

이 확인란을 선택하면 사용자 추적 실패 시 로그인이 허용됩니다. 기본적으로 이 확인란은 사용하지 않도록 설정되어 있습니다. 로그인 추적을 사용하지 않도록 설정하면 사용자가 로그인할 수 없습니다.

이 확인란을 선택하는 경우에는 "실패한 로그인 추적" 또는 "성공한 로그인 추적" 확인란도 선택해야 합니다.

참고: 이 설정을 사용하려면 추가 구성이 필요합니다. [추가 암호 정책 사용](#) (페이지 107)을 참조하십시오.

"변경하지 않으면 암호가 만료됨" 설정

"변경하지 않으면 암호가 만료됨" 필드에서는 만료된 암호에 대한 동작을 구성할 수 있습니다. 선택적으로 사용자에게 만료될 암호에 대한 경고를 얼마나 미리 표시할지 지정할 수 있습니다.

참고: 이 설정을 사용하려면 추가 구성이 필요합니다. [추가 암호 정책 사용](#) (페이지 107)을 참조하십시오.

다음 필드를 구성할 수 있습니다.

다음 이후: <숫자>일

암호가 만료된 후 CA Identity Manager 가 사용자를 비활성화하거나 암호를 강제 변경할 때까지 기다리는 기간(일)을 결정합니다.

참고: 지정된 기간이 경과한 후 사용자가 로그인하려고 시도해야 사용자 계정이 사용하지 않도록 설정됩니다.

사용자 사용 중지

이 라디오 단추를 선택하면 암호 만료 시 사용자가 비활성화됩니다. 비활성화된 사용자는 다음을 통해 활성화할 수 있습니다.

- 사용자 콘솔의 "사용자 활성화/비활성화" 태스크. 기본 "시스템 매니저", "조직 매니저" 및 "보안 매니저" 역할에 "사용자 활성화/비활성화" 태스크가 포함되어 있습니다.
- SiteMinder 관리 사용자 인터페이스

참고: 자세한 내용은 *CA SiteMinder Policy Server Administration Guide*(CA SiteMinder 정책 서버 관리 설명서)를 참조하십시오.

암호 강제 변경

이 라디오 단추를 선택하면 다음에 사용자가 로그인하려고 시도할 때 암호가 강제 변경됩니다.

다음에 대해 만료 경고 통보: <숫자>일

사용자에게 만료될 암호에 대한 알림을 미리 표시할 기간(일)을 입력합니다.

"암호가 장시간 미사용으로 만료되었습니다" 설정

"암호가 장시간 미사용으로 만료되었습니다" 설정을 사용하여 사용자 로그인 시도 간격(시간)을 지정할 수 있습니다. 이 시간이 경과하면 사용자 계정이 비활성 상태로 간주됩니다. 이 섹션을 사용하여 계정이 비활성 상태로 간주된 사용자가 로그인할 수 있는 권한을 가지고 있을 때의 동작을 지정할 수도 있습니다.

"암호가 장시간 미사용으로 만료되었습니다" 섹션의 설정을 구성하려면 "Track login details"(로그인 정보 추적) 확인란을 사용하도록 설정해야 합니다.

참고: 이 설정을 사용하려면 추가 구성이 필요합니다. [추가 암호 정책 사용](#) (페이지 107)을 참조하십시오.

"암호가 장시간 미사용으로 만료되었습니다" 섹션에는 다음 설정이 포함되어 있습니다.

- 다음 이후: <숫자>일 - 암호가 만료되기 전의 미사용 기간(일)을 결정합니다.
- 사용자 사용 안 함 - 장시간 미사용으로 인해 암호가 만료되어 사용자 계정이 사용되지 않도록 설정된 경우 사용자를 비활성화합니다. 이 경우 비활성화된 사용자는 "사용자 활성화/비활성화" 태스크를 사용하여 활성화해야 합니다.
- 암호 강제 변경 - 장시간 미사용으로 인해 암호가 만료된 경우 암호를 강제 변경합니다. 사용자는 다음에 로그인하려고 시도할 때 암호를 변경합니다.

"잘못된 암호" 설정

"잘못된 암호" 설정 섹션에서는 사용자 계정을 사용하지 않도록 설정할 때까지 허용되는 실패한 로그인 횟수를 지정할 수 있습니다. 사용자가 다시 로그인을 시도할 수 있도록 허용할 때까지 계정이 사용되지 않도록 설정하는 기간을 지정할 수도 있습니다. 이 섹션은 "실패한 로그인 추적" 확인란을 선택한 경우에만 적용됩니다.

참고: 이 설정을 사용하려면 추가 구성이 필요합니다. [추가 암호 정책 사용](#) (페이지 107)을 참조하십시오.

"잘못된 암호" 섹션에는 다음 필드가 포함되어 있습니다.

다음 이후 계정 사용 정지: <숫자>회 잘못된 암호 연속 사용

이 설정에 따라 사용자가 수행할 수 있는 실패한 로그인 연속 시도 횟수가 결정됩니다. 실패한 시도 횟수를 제한하면 올바른 암호를 찾을 때까지 반복적으로 암호를 입력하여 리소스에 액세스하도록 설계된 프로그램으로부터 보호됩니다. 지정된 시도 횟수가 지났는데도 사용자가 올바르게 로그인하지 못하면 **CA Identity Manager** 는 해당 계정이 사용되지 않도록 설정합니다. 관리자가 계정을 다시 사용하도록 설정해야 합니다.

다음 이후: <숫자>분

이 설정에 따라 사용자가 다른 로그인 시도를 하거나 해당 계정이 다시 사용되도록 설정될 때까지 기다리는 기간이 결정됩니다. 사용자가 또 다른 잘못된 암호를 입력하면 **CA Identity Manager** 는 다시 계정이 사용되지 않도록 설정합니다. 사용자는 지정된 시간만큼 기다렸다가 다시 시도해야 합니다.

단일 로그인 시도 허용

이 설정은 사용자가 잘못된 암호를 입력한 후 한 번 더 로그인하려고 시도할 때까지 걸리는 기간(분)을 지정합니다.

계정 다시 사용

이 설정은 지정된 기간(분)이 경과한 후 계정을 다시 사용하도록 설정합니다.

암호 조합 구성

새로 만든 암호의 문자 조합을 결정하는 규칙을 지정할 수 있습니다. 문자 요구 사항에 대한 값을 결정할 때 최대 암호 길이를 고려해야 합니다. 총 문자 및 숫자 수가 최대 암호 길이를 초과하면 모든 암호가 거부됩니다. 예를 들어 "문자"와 "숫자"를 모두 6 으로 설정한 경우 모든 암호에는 적어도 12 자(문자 6 자 및 숫자 6 자)가 포함됩니다. 이 경우 최대 암호 길이가 8 자이면 모든 암호가 거부됩니다.

암호 조합 설정에는 다음이 포함됩니다.

최소 암호 길이

사용자 암호의 최소 길이를 지정합니다.

최대 암호 길이

사용자 암호의 최대 길이를 지정합니다.

최대 반복 문자

암호에 연속적으로 나타날 수 있는 동일한 문자의 최대 수를 결정합니다.

예를 들어, 이 값을 3 으로 설정하면 암호에 "aaaa"를 사용할 수 없습니다. 하지만 "aaa"는 암호 내에 사용할 수 있습니다. 이 값을 설정하면 사용자가 단일 문자로 된 암호를 입력할 수 없게 됩니다.

대문자

대문자를 허용할지 여부와 허용하는 경우 암호에 포함되어야 하는 최소 개수를 지정합니다.

소문자

소문자를 허용할지 여부와 허용하는 경우 암호에 포함되어야 하는 최소 개수를 지정합니다.

문자

문자를 허용할지 여부와 허용하는 경우 암호에 포함되어야 하는 최소 개수를 지정합니다.

참고: 대문자 또는 소문자를 허용하는 경우 "문자" 확인란이 자동으로 선택됩니다.

숫자

숫자를 허용할지 여부와 허용하는 경우 암호에 포함되어야 하는 최소 개수를 지정합니다.

문자 또는 숫자

문자 또는 숫자를 허용할지 여부와 허용하는 경우 암호에 포함되어야 하는 최소 개수를 지정합니다. "숫자"와 함께 이 설정을 지정하면 문자가 두 요구 사항을 모두 충족할 수 있습니다. 예를 들어, 이 설정과 "숫자"를 4 로 설정하면 암호 "1234"는 유효한 암호입니다.

참고: 대문자나 소문자 또는 숫자를 허용하는 경우 "문자 또는 숫자" 확인란이 자동으로 선택됩니다.

문장 부호

문장 부호를 허용할지 여부와 허용하는 경우 암호에 포함될 수 있는 최소 개수를 지정합니다. 문장 부호는 마침표, 쉼표, 느낌표, 슬래시, 대시, 하이픈입니다.

인쇄할 수 없는 문자

인쇄할 수 없는 문자를 허용할지 여부와 허용하는 경우 암호에 포함해야 하는 최소 문자 수를 지정합니다. 이러한 문자는 컴퓨터 화면에 표시할 수 없습니다.

참고: 특정 브라우저에서는 인쇄할 수 없는 문자를 지원하지 않습니다.

영숫자 아님

문장 부호 및 다른 기호("@", "\$" 및 "*")와 같은 영숫자가 아닌 문자를 허용할지 여부와 허용하는 경우 암호에 포함될 수 있는 최소 개수를 지정합니다. 인쇄할 수 없는 문자도 포함됩니다. 또한 인쇄할 수 없는 문자는 문장 부호 및 인쇄할 수 없는 문자 요구 사항을 충족합니다.

정규식 지정

암호 정규식을 사용하면 각 암호와 일치하거나 일치하지 않는 문자열 일치를 유효한 것으로 만들기 위한 정규식 텍스트 패턴을 지정할 수 있습니다. 이 테스트는 첫 번째 문자는 숫자이고 마지막 문자는 숫자가 아니어야 하는 등의 경우에 유용할 수 있습니다.

단일 암호 정책에 대해 여러 식을 구성합니다. 여러 식을 만들면 허용 가능한 암호가 모든 지정된 식과 일치합니다.

다음 단계를 수행하십시오.

1. "이름" 필드에 식에 대한 설명 태그(공백 없음)를 입력합니다.
2. "정규식 구문"에 설명된 구문을 사용하여 "일치해야 함" 필드에 정규식을 입력합니다.
3. 암호가 정규식과 일치하지 않는 경우에는 "일치하지 않아야 함" 열의 확인란을 선택합니다.

참고: 더하기(+) 기호를 클릭하고 식을 추가하여 여러 식을 지정할 수 있습니다.

예: Name: MustStartAlpha

Expression: [a-zA-Z]*라는 정규식 정의를 사용하여 모든 암호가 대문자 또는 소문자로 시작하도록 지정할 수 있습니다.

정규식 구문

이 섹션에서는 암호 일치를 위한 정규식을 구성하는 데 사용하는 구문을 설명합니다. 이 구문은 영역을 지정할 때 리소스 일치에 대해 지원되는 정규식 구문과 일치합니다.

문자	결과
\	메타 문자(예: '*')를 나타내는 데 사용됩니다.
\\	단일 '\' 문자와 일치
(A)	하위 표현식 그룹화(패턴 평가 순서에 영향을 줌)
[abc]	단순한 문자 클래스(대괄호 내의 모든 문자가 대상 문자와 일치함)
[a-zA-Z]	범위가 있는 문자 클래스(대괄호 내의 모든 문자 범위가 대상 문자와 일치함)
[^abc]	부정 문자 클래스
.	새 줄이 아닌 모든 문자와 일치

문자	결과
^	줄의 시작 부분에서만 일치
\$	줄의 끝 부분에서만 일치
A*	A 와 0 번 이상 일치(확장)
A+	A 와 1 번 이상 일치(확장)
A?	A 와 1 번 또는 0 번 일치(확장)
A*?	A 와 0 번 이상 일치(축소)
A+?	A 와 1 번 이상 일치(축소)
A??	A 와 0 번 또는 1 번 일치(축소)
AB	순서대로 A 및 B 와 일치
A B	A 또는 B 와 일치
\1	첫 번째 괄호 안의 하위 표현식에 대한 후참조
\n	n 번째 괄호 안의 하위 표현식에 대한 후참조

모든 종료 연산자(+, *, ?)는 기본적으로 확장이므로 전체 일치가 실패하지 않고 가능한 한 많은 문자열 요소와 일치합니다. 종료를 축소(확장 아님)로 설정하려는 경우 뒤에 '?'만 추가하면 됩니다. 축소 종료는 일치 항목을 찾을 때 가능한 한 적은 문자열 요소와 일치합니다.

암호 제한 설정

암호 사용에 대한 제한을 설정할 수 있습니다. 제한에는 사용자가 암호를 다시 사용할 때까지 기다려야 하는 기간뿐 아니라 새 암호를 이전에 선택한 암호와 얼마나 다르게 설정해야 하는지도 포함됩니다. 사용자가 보안 위험 요소이거나 개인 정보를 포함한다고 판단되는 단어를 지정하지 못하게 할 수도 있습니다.

참고: 이 설정을 사용하려면 추가 구성이 필요합니다. [추가 암호 정책 사용](#) (페이지 107)을 참조하십시오.

"제한" 섹션에는 다음 필드가 포함되어 있습니다.

다시 사용할 수 있기까지 남은 최소 기간(일)

사용자가 암호를 다시 사용할 수 있을 때까지 기다려야 하는 기간(일)을 결정합니다.

다시 사용하기까지 남은 최소 암호 수

한 암호를 다시 사용할 수 있을 때까지 사용해야 하는 암호 수를 결정합니다.

참고: 기간과 암호 수를 지정하면 두 조건을 모두 충족해야 암호를 다시 사용할 수 있습니다. 예를 들어 사용자가 한 암호를 다시 사용할 때까지 365 일을 기다리면서 12 개의 암호를 지정하도록 요구하는 암호 정책을 구성할 수 있습니다. 1 년이 경과했는데도 6 개의 암호만 사용된 경우 사용자는 다른 암호 6 개를 마저 사용해야 첫 번째 암호를 다시 사용할 수 있습니다.

지난 암호와의 차이(백분율)

새 암호에 포함되어야 하는 문자의 백분율을 지정합니다. 값을 100 으로 설정할 수 있습니다. 이 경우 새 암호에는 이전 암호에 있는 문자가 포함될 수 없습니다.

차이점을 확인할 때 시퀀스 무시

백분율을 확인할 때 암호에 있는 문자의 위치를 무시합니다.

예를 들어 초기 암호가 **BASEBALL12** 인 경우 "차이점을 확인할 때 시퀀스 무시" 확인란을 선택하면 **12BASEBALL** 이 허용되지 않습니다. 이 확인란을 선택 해제한 경우 **12BASEBALL** 은 각 문자가 서로 다른 위치에 나타나기 때문에 허용 가능한 암호입니다.

보안을 강화하기 위해 "차이점을 확인할 때 시퀀스 무시" 확인란이 선택되어 있습니다.

암호	차이(백분율)	시퀀스 무시	허용됨
BASEBALL12(이전)	0	선택됨	Y
12BASEBALL		선택 해제됨	Y

암호	차이(백분율)	시퀀스 무시	허용됨
BASEBALL12(이전)	100	선택됨	N
12BASEBALL		선택 해제됨	Y
BASEBALL12(이전)	0	선택됨	Y
12SOFTBALL		선택 해제됨	Y
BASEBALL12(이전)	90	선택됨	N
12SOFTBALL		선택 해제됨	Y
BASEBALL12(이전)	100	선택됨	N
12SOFTBALL		선택 해제됨	N

프로필 특성

"일치 길이" 필드를 구성하면 사용자가 개인 정보를 암호에 사용하지 못하게 됩니다. "일치 길이" 필드는 암호 정책이 디렉터리 항목에 있는 특성과 비교하는 최소 시퀀스 길이를 결정합니다. 예를 들어 이 값을 4 로 설정한 경우 CA Identity Manager 는 암호에 사용자 프로필 특성의 마지막 4 개 문자(예: 성 또는 전화 번호)가 포함되어 있지 않은지 확인합니다.

사전

암호에 사용할 수 없는 문자열 목록을 지정합니다.

참고: 사전 항목의 마지막 줄 뒤에 캐리지 리턴이 옵니다.

"사전" 설정에는 다음 필드가 포함되어 있습니다.

- 경로 - 사전 파일의 전체 경로와 이름을 포함합니다.
- 일치 길이 - 사전 파일에 있는 값과 비교되는 문자열의 길이를 제어합니다. 비교할 때 문자열의 대소문자가 무시됩니다. "일치 길이" 필드를 비워 두거나 0 으로 설정할 수 있습니다. 이러한 경우 사전에 있는 문자열과 정확히 일치하는 암호만 거부됩니다. 일치 길이가 0 보다 큰 경우에는 다음 조건을 충족하는 항목이 거부됩니다.
 - 암호에 사전 항목과 동일한 일련의 문자로 시작하는 하위 문자열이 포함되어 있습니다.
 - 연속 일치 문자 수가 "일치 길이" 필드에서 지정한 수보다 크거나 같습니다.

예를 들어 다음 항목을 포함하는 사전 파일을 생각해 봅시다.

- lion
- tiger
- bear

"일치 길이" 필드를 4 로 설정한 경우 다음 동작이 발생합니다.

"TeddyBear"는 Bear 가 사전 파일에 있는 bear 항목과 일치하기 때문에 거부됩니다.

"prestige"는 "tige"가 사전 파일에 있는 tiger 항목의 처음 4 개 문자와 일치하기 때문에 거부됩니다.

"Geiger Counter"는 "iger"에 사전 파일에 있는 tiger 항목의 첫 번째 문자가 포함되어 있지 않기 때문에 허용됩니다.

고급 암호 옵션 구성

고급 암호 정책 옵션을 사용하여 유효성 검사 및 저장 전에 제출된 암호의 사전 처리를 구성할 수 있습니다. 또한 이렇게 하면 정책에 우선 순위를 할당할 수 있으므로 동일한 사용자 디렉터리 또는 네임스페이스에 적용되는 여러 암호 정책의 예측 가능한 평가가 가능해집니다.

대소문자 구분 안 함 | 대문자 강제 사용 | 소문자 강제 사용

처리 및 저장 전에 암호를 강제로 대문자 또는 소문자로 변경할지 여부를 결정합니다. "대문자 사용 강제" 또는 "소문자 사용 강제" 라디오 단추를 클릭하여 대소문자 구분 옵션을 선택합니다. 그렇지 않으면 "대소문자 구분 안 함" 라디오 단추(기본값)가 선택되었는지 확인합니다.

중요! 지정한 대소문자 강제 적용 옵션과 정의한 대소문자 관련 조합 요구 사항이 일치하는지 확인하십시오.

선행 공백 제거

처리 전에 암호에서 선행 공백을 제거하려면 선택합니다.

후행 공백 제거

처리 전에 암호에서 후행 공백을 제거하려면 선택합니다.

포함된 공백 제거

처리 전에 포함된 공백을 모두 제거하려면 선택합니다.

참고: 일부 사용자 디렉터리 구현에서는 사용자 암호가 담긴 특성 값을 저장하기 전에 해당 특성 값에서 선행 또는 후행 공백을 자동으로 제거합니다. 암호 정책에서 지정한 설정이 적용되지 않습니다.

평가 우선 순위

암호 정책의 평가 우선 순위를 지정합니다. 값의 범위는 0(기본값)에서 999 사이입니다. 적용 가능한 정책은 내림차순으로 평가됩니다. 즉, 999 가 맨 먼저 평가된 다음 0 이 맨 마지막으로 평가됩니다.

낮은 우선 순위의 암호 정책 적용

낮은 우선 순위의 암호 정책이 이 암호 정책 뒤에 적용되는지 여부를 결정합니다.

암호 정책 관리

적절한 권한이 있는 관리자는 "암호 정책 보기", "암호 정책 수정", "암호 정책 만들기" 및 "암호 정책 삭제" 태스크를 사용하여 암호 정책을 관리할 수 있습니다. 기본적으로 이러한 태스크는 "정책" 범주에 나타납니다.

해당 태스크 중 하나에 액세스하면 CA Identity Manager 가 현재 CA Identity Manager 환경과 관련된 사용자 저장소에 적용되는 암호 정책 목록을 표시합니다. CA Identity Manager 가 SiteMinder 와 통합된 경우 "암호 서비스"를 사용하여 SiteMinder 관리 사용자 인터페이스에서 만든 암호 정책이 목록에 포함될 수도 있습니다. CA Identity Manager 또는 SiteMinder 에서 만든 암호 정책을 관리할 수 있습니다.

암호 정책 및 관계형 데이터베이스

관계형 데이터베이스에 적용되는 암호 정책을 구성하는 경우 다음 형식을 사용하여 SiteMinder 사용자 디렉터리에 대해 "암호 데이터" 특성을 구성해야 합니다.

tablename.columnname

실행 중에 구문 문제를 방지하려면 이 필드가 주 테이블에 있는 것이 좋습니다.

CA CA Identity Manager 및 Siteminder 통합 암호 조건

CA CA Identity Manager 가 SiteMinder 와 통합되고 Siteminder 의 암호 처리 기능을 사용하는 경우 암호 정책은 Siteminder 정책 저장소에서 얻게 됩니다. 이 경우 Siteminder 의 암호 조건을 충족하는 암호를 구성하십시오. 다음 문장 부호가 Siteminder 의 암호 조건을 충족하는 문장 부호입니다.

'*, '(', '\', ',', '@', '!', ':", ':", '#', '_', '-', '.', '!', '&', '?', ')', '(', '{', '}', '*', '!', '/', " "

중요: CA CA Identity Manager 는 암호 내의 문장 부호 사용에 대해 어떠한 제한도 적용하지 않습니다. 하지만 Siteminder 암호 기능을 사용하는 경우에는 Siteminder 제한을 충족하는 암호를 구성하는 것이 좋습니다.

암호 재설정 또는 계정 잠금 해제

사용자가 Windows 시스템에서 본인의 암호를 잊어버리는 경우 Windows 로그인 화면에서 사용자에게 물어보도록 자체 서비스를 구성할 수 있습니다. Windows VISTA 및 Windows 7 시스템의 경우 자격 증명 공급자를 설치하여 이 기능을 사용할 수 있습니다.

이 기능을 사용하면 Cube 웹 브라우저를 통해 사용자가 자체 서비스에 로그인되고, 여기에 암호 변경 요청 페이지가 표시됩니다. 이 페이지에 입력한 후에 사용자는 "돌아가기"를 클릭하여 Windows 로그인 화면으로 돌아갑니다.

자격 증명 공급자 설치

다음 단계를 수행하십시오.

1. CA Identity Manager 프로비저닝 구성 요소 다운로드 또는 기타 설치 미디어를 찾습니다.

2. "에이전트"에서 설치 관리자를 실행합니다.

참고: 64 비트 운영 체제에 자격 증명 공급자를 설치하는 경우에는 이 소프트웨어의 64 비트 버전을 선택하십시오.

3. 마법사 프롬프트에 따라 질문에 대답합니다.
4. 64 비트 운영 체제에 자격 증명 공급자를 설치한 경우 [Microsoft Visual C++ 2008 SP1\(64 비트\)](#) 을 다운로드합니다.
5. 설치가 완료되면 자격 증명 공급자를 구성합니다.

자격 증명 공급자 구성

구성 도구를 사용하여 자격 증명 공급자가 설치된 시스템을 구성할 수 있습니다.

자격 증명 공급자를 구성하려면

1. Windows 탐색기에서 자격 증명 공급자를 설치한 디렉터리로 이동합니다. 예를 들면 다음과 같습니다.

C:\Program Files\CA\Identity Manager\Credential Provider

2. 다음 실행 파일을 두 번 클릭합니다.

CAIMCredProvConfig.exe

3. 기본값으로 첫 번째 자격 증명 공급자를 선택합니다.

Microsoft 암호 자격 증명 공급자 등과 같은 두 번째 자격 증명 공급자가 사용 중인 경우 로그인 화면에 이 설정이 표시되지 않을 수 있습니다. 두 공급자 모두 기본 공급자가 되려고 시도하면 로그인 화면이 기본 공급자를 선택합니다.

4. 기본 자격 증명 공급자를 비활성화합니다.
5. 다음과 같이 "자격 증명 공급자 설정" 필드를 채웁니다.

Link1 URL

사용자가 "암호 분실" 링크를 클릭하면 사용되는 URL 입니다. 이 링크는 암호 재설정을 위한 웹 인터페이스 URL 이어야 합니다.

다음은 샘플 링크입니다.

```
http://eastern.local:8080/iam/im/environment/cal2/index.jsp?
task.tag=forgottenpassword&facesViewId=/app/page/screen/
fp_identify_user.jsp&action.forgottenpassword.identify=1&USER_ID=%username%
e%
```

이 URL 의 경우 해당 환경에서 자체 등록이 작동 중이어야 합니다. 또한 CA Identity Manager 환경의 자체 서비스 URL 이 자격 증명 공급자를 설치하는 시스템에서 작동되는지 확인하십시오. 여기서 %username%는 로그인 대화 상자의 사용자 이름 필드의 값으로 대체됩니다.

Link2 URL

사용자가 "계정 잠금 해제" 링크를 클릭하면 사용되는 URL 입니다. 이 링크는 사용자가 계정을 잠금 해제할 수 있게 해 주는 웹 인터페이스 URL 이어야 합니다. 여기서 %username%는 로그인 대화 상자의 사용자 이름 필드의 값으로 대체됩니다.

Link3 URL

사용자가 "새 계정" 링크를 클릭하면 사용되는 URL 입니다. 이 링크는 사용자가 계정을 만들 수 있도록 허용하는 웹 인터페이스 URL 이어야 합니다. %username% 태그는 URL 에 포함되지 않습니다.

사용자 지정 제목 사용

제목 표시줄 또는 자격 증명 공급자의 돌아가기 대화 상자에 표시되는 "Powered by ..." 문자열을 대체하는 사용자 지정된 문자열입니다. 이 문자열의 위치는 "섹션 508 규정 준수" 설정에 기초합니다.

도메인

프로비저닝 도메인 이름입니다.

섹션 508 규정 준수(메뉴의 "돌아가기" 사용)

메뉴의 "돌아가기" 기능을 활성화합니다. 이 옵션을 선택하지 않으면 "돌아가기" 대화 상자가 사용됩니다.

모든 대화 상자 비활성화

보안 브라우저에서 팝업, 오류, 인쇄, 저장 대화 상자 등과 같은 새 대화 상자 창이 표시되지 않도록 방지합니다. *모든 대화 상자 비활성화*는 시스템 보안을 개선하기 위해 활성화되어 있지만 문제 해결 목적으로 비활성화할 수 있습니다.

6. 다음과 같이 "보안 브라우저 설정" 필드를 채웁니다.

허용 목록

액세스가 항상 허용되어야 하는 URL 과 일치하는 정규식 패턴입니다.

거부 목록

액세스가 항상 거부되어야 하는 URL 과 일치하는 정규식 패턴입니다.

7. (선택 사항) "내보내기"를 클릭하여 설정을 다른 시스템으로 내보냅니다.
8. "확인"을 클릭하여 설정을 저장합니다.
9. 시스템을 다시 시작합니다.

자격 증명 공급자 레지스트리 설정

자격 증명 공급자 구성 도구를 사용하지 않기로 선택한 경우 다음 키에서 Windows 레지스트리 설정을 편집할 수 있습니다.

[HKEY_LOCAL_MACHINE\SOFTWARE\CA\CAIMCredentialProvider]

link1_cmd

이 링크는 사용자가 링크 1 을 클릭할 때 이동할 URL 입니다.

link2_cmd

이 링크는 사용자가 링크 2 을 클릭할 때 이동할 URL 입니다. 예를 들어, 계정 잠금을 해제하기 위한 웹 사이트로 연결되는 링크를 추가할 수 있습니다.

link2_cmd 가 비어 있으면 link1_cmd 만 "로그온" 대화 상자 창에 나타납니다.

link3_cmd

이 링크는 사용자가 계정을 만들 수 있도록 허용하는 웹 인터페이스 URL 을 로드합니다.

comp508

메뉴의 "돌아가기" 기능을 활성화합니다. 이 옵션을 선택하지 않으면 "돌아가기" 대화 상자가 사용됩니다.

domain

프로비저닝 도메인 이름입니다.

langdir

지역화된 언어 DLL 의 위치입니다.

disablepwdcp

"Microsoft 암호 자격 증명 공급자 사용 안 함" 옵션입니다. 1 은 사용 안 함입니다. 0 은 사용입니다.

CredentialProviderInstallPath

자격 증명 공급자가 설치되는 전체 디렉터리 경로입니다.

configdir

자격 증명 공급자가 설치되는 전체 디렉터리 경로입니다.

selectdefaultcredential

기본 옵션으로 첫 번째 자격 증명 공급자를 선택합니다. Yes 는 활성화입니다. No 는 비활성화입니다.

Cube 브라우저 레지스트리 설정

Cube 보안 브라우저 구성 요소에는 동작을 제어하는 일부 레지스트리 값이 있습니다. 이러한 설정은 다음 레지스트리 키에 있습니다.

[HKEY_LOCAL_MACHINE\SOFTWARE\CA\Cube]

Type

REG_SZ(String)

404

시작할 때 컴퓨터가 CA Identity Manager 에 연결할 수 없는 경우 표시되는 표준 HTML 문서의 경로입니다.

default

Link1 명령 및 Link2 명령에 포함된 URL 이 없는 경우 이동할 기본 페이지입니다.

allow

명시적 허용 ACL. 항상 허용되는 패턴 일치 URL 에 대한 정규식입니다. 자세한 내용은 [Cube 액세스 제어 목록](#) (페이지 129)을 참조하십시오.

close

보안 브라우저를 닫고 사용자를 자격 증명 공급자 암호 잊음 대화 상자로 돌려보냅니다.

deny

명시적 거부 ACL. 액세스가 항상 거부되어야 하는 패턴 일치 URL 에 대한 정규식입니다. 자세한 내용은 [Cube 액세스 제어 목록](#) (페이지 129)을 참조하십시오.

langdir

지역화된 언어 DLL 의 위치입니다.

rejectinvalidcerts

자격 증명 공급자에서 유효한 SSL 인증서만 수락할지 여부를 제어합니다. **no** 로 설정하면 만료되거나 유효하지 않은 SSL 인증서가 허용됩니다.

이 키의 유효한 값은 **yes** 및 **no** 입니다.

unreachable

Cube 에 연결 문제가 발생할 경우 URL 로 리디렉션합니다.

샘플 값: file:///C:\unreachable.html

usecustomtitle

자격 증명 공급자에 대한 사용자 지정 제목을 활성화합니다.

customtitle

자격 증명 공급자에 나타내려는 제목입니다.

큐브 액세스 제어 목록

큐브 ACL 은 선택한 URL 로 이동할 권한을 명시적으로 허용 또는 거부하는 정규식 패턴입니다. ACL 은 다음과 같은 순서로 평가됩니다.

1. 허용(첫 번째로 사용 권한이 자동으로 허용됨)
2. 거부(두 번째로 거부된 URL 이 확인됨)

액세스 제어 목록 예제

"allow"=".pdf"

모든 PDF 문서가 표시되도록 허용합니다.

"deny"=".doc|.xls"

Microsoft Word 및 Excel 문서에 대한 액세스를 거부합니다.

"Powered By" 메시지 사용자 지정

자격 증명 공급자의 "돌아가기" 대화 상자 또는 "돌아가기" 메뉴 옵션에서 "Powered by..." 메시지를 볼 수 있습니다. 이 메시지는 편집하거나 제거할 수 있습니다.

"Powered By"(제공:) 메시지를 사용자 지정하려면

1. <http://www.resedit.net> 에서 무료 리소스 편집기인 ResEdit 를 다운로드합니다.
2. ResEdit 를 시작합니다.
3. languages 폴더에서 1033.dll 파일을 편집합니다.
4. 문자열 테이블을 두 번 클릭합니다.
5. 이 메시지에 대한 영어 버전의 리소스인 리소스 ID 135 를 제거하거나 수정합니다.

Windows 로그인에 대한 암호 재설정

Windows 시스템에 자격 증명 공급자가 설치되면 표준 Microsoft Windows 로그인 대화 상자에 "암호를 잊으셨습니까?" 링크가 표시됩니다. 이 링크를 사용하여 암호를 재설정하거나 쉽게 기억할 수 있는 힌트를 볼 수 있습니다.

Windows 로그인에 대한 암호를 재설정하려면

1. "Windows 보안" 대화 상자에서 "로그인"을 클릭합니다. "Windows 로그인" 대화 상자가 표시됩니다.
2. 올바른 사용자 이름을 입력합니다.
3. "암호를 잊으셨습니까?"를 클릭합니다.

CA Identity Manager 암호 힌트 페이지가 표시됩니다.

암호가 생각난 경우 로그인 대화 상자로 돌아가 계속하십시오. 암호가 생각나지 않으면 4 단계를 수행하여 CA Identity Manager 자체 서비스의 인증을 받으십시오.

4. 인증 질문에 대한 답을 입력합니다.

참고: 모든 질문에 대한 올바른 답을 입력하지 못한 경우 "요청"을 클릭하여 관리자가 암호를 재설정할 수 있도록 하십시오.

그러면 다음 화면에 암호 변경 메시지가 표시됩니다.

자격 증명 공급자 자동 설치

자격 증명 공급자는 자동 설치 모드를 지원합니다. 다음 6 개 속성이 지원됩니다.

LINK1

레지스트리에서 SOFTWARE\CA\CAIMCredentialProvider\link1_cmd 를 참조합니다.

LINK2

레지스트리에서 SOFTWARE\CA\CAIMCredentialProvider\link2_cmd 를 참조합니다.

LINK3

레지스트리에서 SOFTWARE\CA\CAIMCredentialProvider\link3_cmd 를 참조합니다.

DOMAIN

레지스트리에서 SOFTWARE\CA\CAIMCredentialProvider\domain 을 참조합니다.

COMP508

레지스트리에서 SOFTWARE\CA\CAIMCredentialProvider\comp508 을 참조합니다.

USECUSTOMTITLE

레지스트리에서 SOFTWARE\CA\Cube\usecustomtitle 을 참조합니다.

CUSTOMTITLE

레지스트리에서 SOFTWARE\CA\Cube\customtitle 을 참조합니다.

REJECTINVALIDCERTS

레지스트리에서
SOFTWARE\ComputerAssociates\Cube\rejectinvalidcerts 를 참조합니다.

UNREACHABLE

연결할 수 없는 페이지의 위치를 나타냅니다.

이러한 속성 값을 설정하는 구문은 다음과 같습니다.

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR="C:\Program Files\CA\Identity
Manager\Credential Provider\" LINK1="\<url>" LINK2="\<url>" LINK3="\<url>"
COMP508="\yes\" REJECTINVALIDCERTS="\yes\" USECUSTOMTITLE="\yes\"
CUSTOMTITLE="custom cp title\""
```

또는

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR="C:\Program Files\CA\Identity
Manager\Credential Provider\" LINK1="\<url>" LINK2="\<url>" LINK3="\<url>"
COMP508="\yes\" USECUSTOMTITLE="\yes\" CUSTOMTITLE="custom cp title\"
SELECTDEFAULTCREDENTIAL="\yes\" UNREACHABLE="\<url>\""
```

또는

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR="C:\Program Files\CA\Identity
Manager\Credential Provider\"
LINK1="\<url>" LINK2="\<url>" LINK3="\<url>" COMP508="\yes\"
USECUSTOMTITLE="\yes\" CUSTOMTITLE="custom cp title\"
SELECTDEFAULTCREDENTIAL="\yes\" UNREACHABLE="file:///[INSTALLDIR]<file
name>" CUBE_ALLOW="\\" CUBE_DENY="\\""
```

[INSTALLDIR]

INSTALLDIR 속성 값을 나타냅니다.

<url>

계정 잠금 해제 또는 암호 분실 링크에 대한 URL 을 지정합니다.

<file name>

연결할 수 없는 파일의 이름을 정의합니다.

CUBE_ALLOW

Cube 에서 URL 호출 허용을 참조합니다.

CUBE_DENY

Cube 에서 URL 호출 제한을 참조합니다.

제 6 장: 끝점의 암호 동기화

CA Identity Manager 가 지원하는 특정 끝점에 암호 동기화 에이전트를 설치할 수 있습니다. 그러면 에이전트가 끝점에서 암호 변경 요청을 가로채고 변경 내용을 프로비저닝 서버로 제출합니다.

이 섹션은 다음 항목을 포함하고 있습니다.

[Windows 에서 암호 동기화](#) (페이지 135)

[UNIX 및 Linux 에서 암호 동기화](#) (페이지 145)

[OS400 에서 암호 동기화](#) (페이지 160)

Windows 에서 암호 동기화

CA Identity Manager 는 기본 Windows 계정의 암호 변경 내용을 가로채고 새 암호를 사용자 및 해당 사용자에게 속한 모든 계정으로 전파할 수 있습니다.

암호 동기화 에이전트가 암호 변경 시도를 감지하면 요청을 가로채어 프로비저닝 서버로 전송합니다. 그러면 프로비저닝 서버가 새 암호를 사용자 및 해당 사용자와 연결된 다른 계정으로 전파합니다.

암호 동기화에 대한 요구 사항은 다음과 같습니다.

- 암호 변경 내용을 가로채는 시스템에 암호 동기화 에이전트를 설치해야 합니다.
- 시스템은 획득한 끝점으로서 관리되어야 합니다.
- 획득한 "끝점 설정" 탭에서 "암호 동기화 에이전트가 설치되어 있음" 확인란을 선택해야 합니다.
- 관리 시스템의 계정을 탐색하여 CA Identity Manager 사용자와의 상관 관계를 지정해야 합니다.
- 환경이 끝점 계정으로부터 수신되는 암호 변경 내용을 허용해야 합니다. 관리 콘솔에 대한 액세스 권한이 있는 관리자가 이 기능을 사용하도록 설정합니다.

중요! 하나의 암호가 모든 시스템에 적용되도록 암호 규칙을 주의하여 구성하십시오. 예를 들어 Windows 암호는 12 자여야 하는 경우 최대 10 자의 암호를 허용하는 모든 시스템은 동기화 중 변경을 거부합니다.

CA Identity Manager 서버는 끝점의 암호 제한 사항에 대해 알지 못합니다. 끝점 계정을 사용하여 작업할 때는 암호 정책이 끝점의 암호 정책보다 더 엄격해야 합니다.

암호 동기화 에이전트를 설치하려면

전역 사용자가 로그인하는 임의의 관리되는 Windows 컴퓨터에 암호 동기화 에이전트를 설치할 수 있습니다. 에이전트는 이러한 컴퓨터에서 백그라운드로 실행됩니다.

설치 프로그램 실행

다음 요구 사항에 주의하십시오.

- 프로비저닝 서버는 에이전트를 설치할 시스템을 관리해야 합니다.
- 암호 변경에 대한 관리자 역할을 할 사용자를 만드십시오. 제안된 이름은 etapwsad 입니다. 이 사용자는 PasswordAdministrator 프로필을 가지고 있어야 합니다.
- 설치 미디어에는 32 비트 Windows 용과 64 비트 Windows 용의 두 가지 Windows 암호 동기화 에이전트가 있습니다. 32 비트 암호 동기화 에이전트는 64 비트 Windows 에서 지원되지 않습니다. FIPS 는 32 비트 암호 동기화 에이전트에서만 지원됩니다.

다음 단계를 수행하십시오.

1. CA Identity Manager 설치 미디어를 찾습니다.
2. \Agent\PasswordSync 또는 \Agent\PasswordSync-x64 를 찾습니다.
3. setup.exe 를 실행합니다.
4. 다음과 같이 구성 마법사에 응답합니다.
 - a. "호스트 이름" 필드에 프로비저닝 서버 시스템의 이름을 입력합니다.

- b. 프로비저닝 서버 설치에서 기본이 아닌 포트를 사용하는 경우 필요에 따라 포트를 변경합니다.

프로비저닝 서버에 연결하는 데 사용하도록 제안된 LDAP 포트는 20390 입니다.

- c. "도메인 찾기" 단추를 클릭하여 프로비저닝 서버 도메인을 검색합니다.
- d. 프로비저닝 서버 설치가 장애 조치를 위해 구성된 경우 화면에 나타나는 지침을 따라 쉽표로 구분된 서버 목록을 추가합니다.
- e. "다음"을 클릭합니다.
- f. "관리자" 필드에 암호 동기화 에이전트에 대한 기본 전역 사용자 이름으로 `etapwsad` 를 입력합니다. 이 사용자는 `PasswordAdministrator` 프로필을 가지고 있어야 합니다. 이것은 기본적으로 존재하지 않습니다.
- g. "암호 관리자" 필드에 관리자의 암호를 입력합니다.
- h. "다음"을 클릭합니다.
- i. "끝점 유형" 드롭다운 목록에서 에이전트를 설치할 호스트의 끝점 유형을 선택합니다.
- j. "끝점 이름" 드롭다운 목록에서 사용자 콘솔에서 끝점을 만들 때 사용된 끝점 이름을 선택합니다.
- k. "구성"을 클릭합니다.

- 5. 메시지가 표시되면 "마침"을 클릭하여 설치를 완료하고 재부팅합니다.

사용자 콘솔에서 끝점 업데이트

사용자 콘솔에서 끝점을 업데이트하여 에이전트가 설치되었음을 나타내십시오.

다음 단계를 수행하십시오.

1. 사용자 콘솔에 로그인합니다.
2. 에이전트가 설치된 끝점을 검색합니다.
3. "끝점 설정" 탭을 클릭합니다.
4. "암호 동기화 에이전트가 설치되어 있음" 확인란을 선택합니다.

암호 동기화를 허용하도록 환경 설정

암호 동기화 에이전트를 설치한 후에는 끝점에서 수행된 암호 변경 내용을 수신하도록 환경을 설정할 수 있습니다. 이 태스크의 경우 관리자가 해당 변경 내용을 허용하도록 환경을 설정하려면 관리 콘솔과 CA Directory에 대한 액세스 권한이 있어야 합니다.

다음 단계를 수행하십시오.

1. 새 사용자의 경우 다음과 같이 관리 콘솔을 사용합니다.
 - a. 환경을 선택합니다.
 - b. "고급 설정", "프로비저닝"을 차례로 클릭합니다.
 - c. "Enable Password Changes from Endpoint Accounts"(끝점 계정의 암호 변경 사용) 확인란을 선택합니다.
2. 기존 사용자의 경우 CA Directory에서 eTPropagatePassword 특성을 1로 설정합니다.

암호 동기화 에이전트에 대한 대체 서버 구성

암호 동기화 에이전트에 대한 대체 서버를 구성하려면 암호 동기화 에이전트 구성 마법사를 사용하십시오.

암호 동기화 에이전트에 대한 대체 서버를 추가하려면

1. `password_sync_folder\bin`에 있는 PwdSyncConfig.exe를 실행합니다.
2. 다음 구성 정보를 입력합니다.

호스트

기본 프로비저닝 서버 호스트 이름을 지정합니다.

지정한 호스트 이름이 서버 URL 필드에 입력됩니다.

LDAP 포트

시스템이 프로비저닝 서버에 연결할 때 사용하는 포트 번호를 지정합니다.

CA Identity Manager에서 지정한 호스트 및 포트가 서버 URL 필드에 입력됩니다.

3. "도메인 찾기" 단추를 클릭하여 도메인 목록을 가져옵니다.
4. 도메인 드롭다운 상자에서 도메인의 이름을 선택하고 "다음"을 클릭합니다.

5. 다음 형식을 사용하여 서버 URL 필드에 대체 서버의 호스트 이름과 포트를 추가합니다.

`ldaps://primaryhost:20390,ldaps://alternatehost1:20390`

6. "다음"을 클릭합니다.
7. 구성 마법사의 나머지 필드를 완료합니다.

암호 동기화 에이전트가 작동하는 방식

전파 프로세스는 전역 사용자가 사용 가능한 방법으로 Windows 시스템에서 자신의 암호를 변경할 때 시작됩니다. 암호를 입력하면 다음이 발생합니다.

1. Windows 운영 체제가 암호가 암호 정책을 충족하는지 검사합니다. Windows 가 암호를 허용하지 않으면 변경 요청은 거부되고 오류 메시지가 표시되며 동기화를 포함한 이후 작업은 수행되지 않습니다.
2. Windows 시스템이 암호 변경 요청을 CA Identity Manager 암호 동기화 에이전트로 전달하면 에이전트는 암호 품질 검사에 대해 구성되어 있는 경우 암호 품질 검사를 위해 암호를 프로비저닝 서버로 제출합니다. 암호가 CA Identity Manager 품질 규칙을 충족하지 않는 경우 변경 요청은 거부되고 오류 메시지가 표시됩니다. Windows 암호는 변경되지 않은 상태로 남아 있고 동기화는 수행되지 않습니다.
3. 암호가 Windows 와 CA Identity Manager 의 품질 규칙을 모두 충족하는 경우 암호 동기화 에이전트가 전파를 위해 암호를 프로비저닝 서버로 제출합니다.
4. CA Identity Manager 는 전역 사용자 암호를 업데이트하고 새 암호를 전역 사용자와 관련된 새 계정 또는 모든 계정에 전파합니다.

참고: CA Identity Manager 가 요청을 거부하는 경우에도 표시되는 오류 메시지는 Windows 암호 정책에 기반하므로 Windows 및 CA Identity Manager 의 암호 정책은 동일하거나 일관성이 있어야 합니다.

password_update_timeout 구성 매개 변수(eta_pwdsync.conf)는 PSA 가 CA Identity Manager 서버로부터 암호 변경 전파 확인을 기다리는 시간(초)을 지정합니다. 이 시간 동안 PSA 가 확인을 받지 못하면 전파가 성공한 것으로 간주되며 암호 변경 전파가 확인되지 않았음을 나타내는 경고가 로깅(eta_pwdsync.log)됩니다. 이 매개 변수의 최소값은 0(영)으로, 이것은 PSA 가 승인을 기다리지 않음을 의미합니다. 자세한 내용은 프로비저닝 관리자 도움말에서 eta_pwdsync.conf--암호 동기화 구성 에이전트를 참조하십시오.

계정 수준 암호 품질 검사

암호 품질 검사는 관리되는 끝점에서 계정을 만들거나 수정하는 경우, 또는 전역 사용자 암호를 설정하는 경우 수행됩니다. 계정에 대한 암호 품질 검사는 암호에 포함된 문자에 기반한 검사로 제한됩니다. 최근 변경 내역에 기초한 전역 사용자 검사(암호 업데이트 빈도 및 암호 재사용 빈도)는 **CA Identity Manager**가 계정 암호에 대한 모든 암호 변경 사항을 인터셉트하지 않으므로 수행되지 않습니다. 따라서 여기에는 이러한 검사를 수행하기 위한 정확한 암호 변경 내역이 없습니다.

계정 암호 확인은 다음 도메인 구성 매개 변수에 의해 제어됩니다.

- 끝점 유형/계정 암호 검사
- 끝점 유형/빈 계정 암호 검사

각 매개 변수의 값은 관리되는 각 끝점에 대해 수행되어야 하는 검사 수준을 지정합니다. 끝점은 다음과 같은 방식으로 지정될 수 있습니다.

```
ALL
-ALL
<NamespaceName>
-<NamespaceName>
<NamespaceName>:<DirectoryName>
-<NamespaceName>:<DirectoryName>
```

빼기(-) 기호를 포함하는 형식은 매개 변수를 비활성화합니다. 이 기호가 없는 형식은 매개 변수를 활성화합니다. [-]<NamespaceName> 형식은 나타난 끝점 유형의 모든 끝점을 제어하고

[-<NamespaceName>:<DirectoryName> 형식은 개별 끝점을 제어합니다. [-]ALL 형식은 모든 끝점 유형의 모든 끝점을 제어합니다. 두 매개 변수의 기본값은 -ALL 입니다.

이러한 각 매개 변수는 여러 번 지정될 수 있습니다. 여러 값이 동일한 끝점을 지정하는 경우에는 마지막 값이 사용됩니다. 먼저 일반 규칙을 배치한 다음 일반 규칙을 무시하는 특수 규칙을 나중에 배치할 수 있습니다.

"계정 암호 검사" 매개 변수는 전역 사용자 암호 품질 검사와 대등한 검사 기능을 제공합니다. 끝점에 대해 이 매개 변수가 활성화되면 **CA Identity Manager**가 기존 계정에 대한 요청된 변경에서 모든 암호를 검사합니다. 이 검사에는 빈 암호를 설정하려는 시도도 포함됩니다. 계정을 만드는 동안 암호가 제공되지 않으면 암호 품질 검사가 수행되지 않습니다.

"빈 계정 암호 검사"는 암호를 만들 때 추가로 빈 암호를 검사합니다. 암호 프로필이 활성화되어 있고 암호에 하나 이상의 문자를 요구하는 경우 빈 암호를 사용하면 계정이 만들어지지 않습니다. 일부 끝점 유형에서는 암호 없이 계정을 만드는 것이 허용되기 때문에 이 매개 변수는 계정 암호 검사와 분리되어 있습니다.

참고: 제공된 암호가 현재 전역 사용자 암호와 일치하는 경우 동기화된 계정 암호에 대한 계정 암호 품질 검사는 생략됩니다.

암호 품질 시행

암호 동기화 옵션은 기본 시스템(예: Windows NT/ADS)의 암호 변경 요청을 인터셉트하여 CA Identity Manager 서버로 제출합니다. 이 서버는 전역 사용자 암호를 전역 사용자와 관련된 계정 암호와 동기화합니다. 암호 품질 제어를 시행하기 위해 암호 프로필에 대한 두 CA Identity Manager 암호 품질 규칙과 기본 시스템 암호 품질 규칙을 사용할 수 있습니다.

암호 동기화 구성

암호 동기화 에이전트는 설치하는 동안 처음 구성되는데 암호 동기화 구성 마법사를 사용하여 언제든지 재구성될 수 있습니다. 추가 구성이 가능합니다. 예를 들어 `eta_pwdsync.conf` 파일을 사용하여 암호 품질 검사 또는 수정 시간 만료에 대한 설정을 변경할 수 있습니다.

이 파일은 `password_sync_folder\data\` 폴더에 있습니다. 이 구성 파일의 모든 키는 암호 동기화 에이전트를 설치하는 동안 설정됩니다. 따라서 필요한 경우에만 이러한 키를 변경하십시오. 자세한 내용은 이 파일에 있는 텍스트를 참조하십시오.

중요! 예방 조치로 구성 파일을 편집하기 전에 백업을 만드십시오.

[Server] 섹션

키	설명	기본값
host	암호 전파를 관리하는 도메인 서버를 지정합니다.	없음
port	프로비저닝 서버의 LDAP 수신 대기 포트를 지정합니다.	20411

키	설명	기본값
use_tls	TLS/SSL 이 암호 동기화 에이전트와 프로비저닝 서버 간의 통신 보안에 사용되는지 여부를 지정합니다.	예
admin_suffix	암호 동기화 에이전트가 CA Identity Manager 에 로그인하는 데 사용하는 관리 사용자의 도메인 접미사를 지정합니다.	없음
admin	암호 동기화 에이전트가 CA Identity Manager 에 로그인하는 데 사용하는 관리 사용자의 계정 이름을 지정합니다.	없음
password	admin 키에 지정된 계정 이름의 암호를 지정합니다.	없음

[eTaDomain] 섹션

키	설명	기본값
도메인	암호 동기화 에이전트를 설치한 프로비저닝 도메인을 지정합니다.	없음
etrust_suffix	전체 CA Identity Manager 제품에 대한 접미사를 지정합니다.	없음
domain_suffix	프로비저닝 도메인에 대한 도메인 접미사를 지정합니다.	없음
endpoint type	암호 동기화 에이전트를 설치한 끝점 유형을 지정합니다.	없음
endpoint	암호 동기화 에이전트가 암호를 가로채는 끝점을 지정합니다.	없음
endpoint_dn	끝점의 고유 이름을 지정합니다.	없음

키	설명	기본값
container_dn	암호가 변경되고 있는 계정을 포함하는 컨테이너의 고유 이름을 지정합니다.	없음
acct_attribute_name	계정의 특성 이름(예: Windows NT 의 경우 eTN16AccountName)을 지정합니다.	끝점 유형에 따라 다름
acct_object_class	계정의 objectClass 를 지정합니다.	끝점 유형에 따라 다름

[PasswordProfile] 섹션

키	설명	기본값
profile_enabled	암호 프로필 검사 기능이 사용되는지 여부를 지정합니다.	아니요
profile_dn	암호 구성 마법사가 암호 프로필에 대한 DN 을 생성하는지 여부를 지정합니다.	eTPasswordProfileName= Password Profile,eTPasswordProfile ContainerName=Password Profile,eTNamespaceName=CommonObjects,dc=cai,dc=eta

[Timeout] 섹션

키	설명	기본값
search_acct_dn	계정 DN 을 검색할 때의 시간 만료 값을 지정합니다.	120 초
pwd_update	암호를 전파할 때의 시간 만료 값을 지정합니다.	400 초
pwd_quality_check	암호 품질 검사를 수행할 때의 시간 만료 값(초)을 지정합니다.	1

[Logs] 섹션

키	설명	기본값
log_file	암호 동기화 에이전트에서 로깅된 메시지를 포함하는 로그 파일을 지정합니다.	..\Program files\CA\Identity Manager Password Sync Agent
log_level	로깅 수준을 지정합니다. 유효한 값: 1--init 파일 2--암호 업데이트 성공 또는 실패 3--연결 디버깅 4--추적	0, 로깅 없음

장애 조치

프로비저닝 서버가 중단되거나 로드가 심할 경우 암호 동기화 에이전트가 다른 서버로 장애 조치할 수 있습니다. 장애 조치하려면 여러 프로비저닝 서버가 동일한 도메인을 지원하고 에이전트가 해당 서버를 사용해야 합니다.

[대체 서버를 사용하도록 에이전트 구성](#) (페이지 138) 섹션에서 구성 지침을 제공합니다.

로그 메시지 사용

암호 수정이 거부된 이유를 알려면 암호 동기화 에이전트에서 보낸 로그 메시지를 보십시오. 로깅된 모든 메시지는 eta_pwdsync.log 파일에 저장됩니다. 기본적으로 이 파일은 ..\Program files\CA\CA Identity Manager Password Sync Agent 폴더에 있습니다.

PSA 로깅(eta_pwdsync.log 파일로 이동)에는 다음과 같은 메시지가 있습니다.

- 오류 메시지. 항상 로깅됩니다.
- 진단(프로세스 흐름, 추적) 메시지, eta_pwdsync.conf 파일의 logging_enabled=yes|no 매개 변수의 값에 따라 활성화 또는 비활성화됩니다.

문제점을 보다 잘 진단하려면 동일한 기간 동안의 `eta_pwdsync.log` 와 프로비저닝 서버 로그를 검토하십시오.

이전 `log_level` 구성 매개 변수는 더 이상 사용되지 않지만 이전 버전과의 호환성을 위해 남아 있습니다. `log_level=0` 은 `logging_enabled=no` 와 동일하고, `log_level=기타` 는 `logging_enabled=yes` 와 동일합니다. 구성 파일에 이전 매개 변수와 새 매개 변수가 모두 있으면 `logging_enabled=yes|no` 매개 변수의 명시적 설정이 이전 `log_level=숫자` 를 통해 수행된 간접 설정보다 우선 순위가 높습니다.

참고: 사용 가능한 커넥터의 목록은 `eta_pwdsync.log` 에 포함되어 있지만 에이전트는 더 이상 이 정보를 제공하지 않습니다.

설치 확인

암호 동기화 에이전트 설치가 완료된 다음 Windows 시스템에서 암호를 변경하여 계정과 연결된 전역 사용자 암호도 변경되는지 확인하십시오.

UNIX 및 Linux 에서 암호 동기화

CA Identity Manager 는 UNIX 또는 Linux 시스템에서 계정의 암호 변경 내용을 가로챌 다음 해당 변경 내용을 전역 사용자와 연결된 다른 모든 계정으로 전파할 수 있습니다. 외부 보안 시스템에 대해 암호를 인증하는 데 사용되는 구성 요소를 PAM(플러그형 인증 모듈)이라고 합니다. PAM 을 통해 CA Identity Manager 가 외부 보안 시스템에 대해 암호를 인증하므로 전역 사용자는 기존 시스템 암호를 사용하여 CA Identity Manager 에 로그인할 수 있습니다.

UNIX 암호 동기화

UNIX PAM 프레임워크를 통해 암호 변경 이벤트를 감지하는 암호 동기화 모듈이 제공됩니다. UNIX 암호 동기화 모듈이 프로비저닝 서버에 암호 변경을 알리면 프로비저닝 서버가 관련된 전역 사용자를 찾은 다음 해당 변경 내용을 다른 관련 계정으로 자동으로 전파합니다.

PAM 프레임워크를 지원하는 UNIX 운영 체제는 다음과 같습니다.

- PAM 사용이 설정된 Power 플랫폼의 AIX v5.3
- PA-RISC 플랫폼 및 Itanium® 2 플랫폼의 HP-UX v11.00
- Sparc 및 Intel 플랫폼의 Solaris v2.6 이상
- s390 또는 Intel i386 플랫폼의 glibc v2.2 이상이 있는 32 비트 Linux

참고: Linux 플랫폼의 경우 `test_sync` 바이너리가 모든 사용자의 `PATH`에 있어야 하지만 루트 사용자, 소유자만 실행 권한을 가지고 있어야 합니다.

이 바이너리를 모든 사용자의 경로에 추가하려면 다음 명령을 전역 `/etc/bashrc` 파일에 포함하십시오.

```
export PATH=$PATH:/etc/pam_CA_eta
```

UNIX PAM 작동 방법

다음 프로세스에서는 UNIX PAM 기능을 설명합니다.

1. 다음 이유 중 하나로 UNIX 사용자의 암호를 변경해야 합니다.
 - 사용자의 결정
 - 시스템 설정이나 수동 개입으로 인해 사용자가 암호를 변경해야 합니다.
 - 사용자의 암호가 관리자로 인해 변경됩니다.
2. 새 암호가 PAM 프레임워크의 암호 서비스로 제출됩니다.
3. PAM 프레임워크의 암호 서비스가 PAM 라이브러리를 호출하여 로컬 UNIX 보안 파일을 업데이트합니다.
4. PAM 프레임워크의 암호 서비스가 UNIX 암호 동기화 모듈(`pam_CA_eta`)을 호출하여 프로비저닝 서버에 암호 변경을 알립니다.
5. 프로비저닝 서버가 관련된 전역 사용자 및 해당 전역 사용자와 연결된 모든 계정의 암호를 업데이트합니다.

UNIX 암호 동기화를 사용하기 위한 요구 사항

UNIX 암호 동기화 기능을 사용하기 위한 요구 사항은 다음과 같습니다.

- 암호 변경을 감지할 UNIX 시스템에 UNIX 암호 동기화 에이전트를 설치해야 합니다.
- UNIX 암호 동기화 에이전트가 상주하는 UNIX 시스템에 UNIX 원격 에이전트와 CAM 을 설치해야 합니다.
- 시스템은 획득한 끝점으로서 관리되어야 합니다. "암호 동기화 에이전트가 설치됨" 확인란이 획득한 끝점의 속성에서 선택되어 있어야 합니다.
- 관리 시스템의 계정을 탐색하여 전역 사용자와의 상관 관계를 지정해야 합니다.
- 환경이 끝점 계정으로부터 수신되는 암호 변경 내용을 허용해야 합니다. 관리 콘솔에 대한 액세스 권한이 있는 관리자가 이 기능을 사용하도록 설정합니다.

UNIX PAM 기능 설치

UNIX PAM 을 설치하려면 다음 절차를 수행하십시오.

UNIX PAM 기능을 설치하려면

1. 사용 중인 UNIX 플랫폼에 해당하는 패키지 파일을 선택합니다.

UNIX 운영 체제	패키지 파일 이름
HP-UX v11 PA-RISC	pam_CA_eta-1.1.HPUX.tar.Z
HP-UX Itanium2	pam_CA_eta1.1HPUX-IA64.tar.Z
AIX v5.3 Power	pam_CA_eta-1.1.AIX.tar.Z
Solaris Sparc	pam_CA_eta-1.1.Solaris.tar.Z
Solaris Intel	pam_CA_eta-1.1.SolarisIntel.tar.Z
Linux x86	pam_CA_eta-1.1.Linux.tar.gz
Linux s390	pam_CA_eta-1.1.LinuxS390.tar.gz

2. 바이너리 모드로 FTP 를 사용하거나 바이너리 파일을 지원하는 다른 파일 전송 도구를 사용하여 선택한 패키지 파일을 UNIX 서버의 임시 폴더(/tmp)로 전송합니다. 이때 나타날 수 있는 샘플 전송 세션은 다음과 같습니다.

```
W:\Pam>ftp user01
Connected to user01.company.com.
220 user01 FTP server (Version 1.2.3.4) ready.
User (user01.company.com:(none)): root
331 Password required for root.
Password:
230 User root logged in.
ftp> cd /tmp
250 CWD command successful.
ftp> bin
200 Type set to I.
ftp> put pam_CA_eta-1.1.HPUX.tar.Z
200 PORT command successful.
150 Opening BINARY mode data connection for pam_CA_eta-1.1.HPUX.tar.Z.
226 Transfer complete.
ftp: 117562 bytes sent in 0,09Seconds 1306,24Kbytes/sec.
ftp> quit
```

3. UNIX 서버에서 루트 사용자로 로그인하고 패키지 파일을 추출합니다.

```
# cd /tmp
# zcat pam_CA_eta-1.1.<platform>.tar.Z | tar -xf -
```

Linux 에서 다음 명령을 사용합니다.

```
# tar -xzf pam_CA_eta-1.1.<platform-hardware>.tar.gz
```

4. 구성 및 TLS 파일을 기본 구성 폴더에 복사합니다.

```
# cd pam_CA_eta-1.1
# mv pam_CA_eta /etc
```


5. pam_CA_eta 모듈을 Security 라이브러리 폴더에 복사합니다.

AIX 에서 다음 명령을 사용합니다.

```
# cp -p pam_CA_eta.o /usr/lib/security/
```

HP-UX 에서 다음 명령을 사용합니다.

```
# cp -p libpam_CA_eta.1 /usr/lib/security/
```

HP-UX Itanium2 에서 다음 명령을 사용합니다.

```
# cp -p libpam_CA_eta.1 /usr/lib/security/hpux32
```

Linux i386 또는 s390 에서 다음 명령을 사용합니다.

```
# cp -p pam_CA_eta.so /lib/security/
```

Solaris Sparc 또는 Intel 에서 다음 명령을 사용합니다.

```
# cp -p pam_CA_eta.so /usr/lib/security/
```

6. (선택 사항) 테스트 프로그램을 복사합니다.

```
# cp -p test_* /etc/pam_CA_eta
```

```
# cp -p pam_test* (/usr)/lib/security/
```

추가 정보

[UNIX 암호 동기화 문제 해결](#) (페이지 156)

사용자 콘솔에서 끝점 업데이트

사용자 콘솔에서 끝점을 업데이트하여 에이전트가 설치되었음을 나타내십시오.

다음 단계를 수행하십시오.

1. 사용자 콘솔에 로그인합니다.
2. 에이전트가 설치된 끝점을 검색합니다.
3. "끝점 설정" 탭을 클릭합니다.
4. "암호 동기화 에이전트가 설치되어 있음" 확인란을 선택합니다.

암호 동기화를 허용하도록 환경 설정

암호 동기화 에이전트를 설치한 후에는 끝점에서 수행된 암호 변경 내용을 수신하도록 환경을 설정할 수 있습니다. 이 태스크의 경우 관리자가 해당 변경 내용을 허용하도록 환경을 설정하려면 관리 콘솔과 CA Directory에 대한 액세스 권한이 있어야 합니다.

다음 단계를 수행하십시오.

1. 새 사용자의 경우 다음과 같이 관리 콘솔을 사용합니다.
 - a. 환경을 선택합니다.
 - b. "고급 설정", "프로비저닝"을 차례로 클릭합니다.
 - c. "Enable Password Changes from Endpoint Accounts"(끝점 계정의 암호 변경 사용) 확인란을 선택합니다.
2. 기존 사용자의 경우 CA Directory에서 eTPropagatePassword 특성을 1로 설정합니다.

UNIX 암호 동기화 기능 구성

UNIX 암호 동기화 기능 구성에는 다음 파일에서 매개 변수를 설정하는 작업이 포함됩니다.

- /etc/pam_CA_eta/pam_CA_eta.conf
- /etc/pam.conf

중요! 권한이 높은 사용자의 암호가 pam_CA_eta.conf 구성 파일에 저장되기 때문에 루트 계정을 통해서만 해당 파일을 읽을 수 있어야 합니다. 패키지 파일의 파일 설정에 owner=root 와 mode=500 이 포함되고 cp 명령의 -p 스위치가 설치 중에 해당 설정을 유지합니다.

pam_CA_eta.conf 파일 구성

pam_CA_eta.conf 파일을 구성하려면 다음 절차를 수행하십시오.

pam_CA_eta.conf 파일을 구성하려면

1. /etc/pam_CA_eta 폴더로 이동합니다.
2. pam_CA_eta.conf 파일을 편집합니다. 이 구성 파일에는 자체 설명서가 포함되어 있습니다.

```
#
# CA - CA Identity Manager
#
# pam_CA_eta.conf
#
# Configuration file for the Unix PAM password module "pam_CA_eta"
#

# keyword: server
# description: the CA Identity Manager LDAP server primary and optional alternate
server hostname
# value: a valid hostname and an optional server
# default: no default
server ETA_SERVER ALT_SERVER

#

# keyword: port
# description: the numeric TCP/IP port number of the CA Identity Manager LDAP
server
# value: a valid TCP/IP port number
# default: 20390
# port 20390

# keyword: use-tls
# description: does it use the secured LDAP over TLS protocol ?
# value: yes or no
# default: yes
# use-tls yes
```

```
# keyword: time-limit
# description: the maximum time in seconds to wait for the end of an LDAP operation.
# value: a numeric value of seconds
# default: 300
# time-limit 300

# keyword: remote-server
# description: identifies whether on premise or cloud Identity Manager
#               server is used.
#               Cloud based server is accessed by proxying the requests
#               through the on-premise CS, requiring use of remote-server
#               set to 'yes'.
# value: yes or no
# default: no
# remote-server no

# keyword: size-limit
# description: the maximum number of entries returned by the CA Identity Manager
#               server
# value: a numeric value
# default: 100
# size-limit 100

# keyword: root
# description: the root DN of the CA Identity Manager server
# value: a valid DN string
# default: dc=eta
# root dc=eta

# keyword: domain
# description: the name of the CA Identity Manager domain
# value: a string
# default: im
# domain im

# keyword: user
# description: the CA Identity Manager Global User name used to bind to the CA
#               Identity Manager server
# value: a valid Global User name string
# default: etaadmin
# user etaadmin

# keyword: password
# description: the clear-text password of the "binding" CA Identity Manager Global
#               User
# value: the password of the above Global User
# default: no default
password SECRET
```

```
# keyword: directory-type
# description: the CA Identity Manager Unix Endpoint type of this Unix server
# value: ETC or NIS
# default: ETC
# endpoint-type ETC

# keyword: endpoint-name
# description: the CA Identity Manager Unix Endpoint name of this Unix server
# value: a valid Unix Endpoint name string
# default:
# ETC: the result of the "hostname" command (ie: gethostname() system call)
# NIS: "domain [hostname]" where "domain" is the result of the "domainname" command
# (ie: getdomainname() system call) and "hostname" the result of the "hostname"
# command (ie: gethostname() system call)
# endpoint-name dirname

# keyword: tls-cacert-file
# description: the name of the CA Identity Manager CA certificate file
# value: a valid full path file name
# default: /etc/pam_CA_eta/et2_cacert.pem
# tls-cacert-file /etc/pam_CA_eta/et2_cacert.pem

# keyword: tls-cert-file
# description: the name of the CA Identity Manager client certificate file
# value: a valid full path file name
# default: /etc/pam_CA_eta/eta2_clientcert.pem
# tls-cert-file /etc/pam_CA_eta/eta2_clientcert.pem

# keyword: tls-key-file
# description: the name of the CA Identity Manager client private key file
# value: a valid full path file name
# default: /etc/pam_CA_eta/eta2_clientkey.pem
# tls-key-file /etc/pam_CA_eta/eta2_clientkey.pem

# keyword: tls-random-file
# description: the name of the "pseudo random number generator" seed file
# value: a valid full path file name
# default: /etc/pam_CA_eta/prng_seed
# tls-random-file /etc/pam_CA_eta/prng_seed

# keyword: use-status
# description: this module will exit with a non-zero status code in case of failure.
# value: yes or no
# default: no
# use-status no
```

```
# keyword: verbose
# description: this module will display informational or error messages to the
user.
# value: yes or no
# default: yes
# verbose yes
```

참고: server, domain 및 password 매개 변수는 기본값이 없으며 업데이트해야 합니다.

pam.conf 파일 구성

/etc/pam.conf 파일이 기본 PAM 구성 파일입니다. 이 파일을 편집하여 암호 서비스 스택에 한 줄을 삽입해야 합니다. 일부 Linux 시스템에서는 pam.conf 파일이 /etc/pam.d 로 대체되므로 /etc/pam.d/system-auth 파일을 편집해야 합니다

pam.conf 파일을 구성하려면

1. /etc 디렉터리로 이동하거나, 적절한 Linux 시스템에서 PAM 모듈을 구성하는 경우 /etc/pam.d 디렉터리로 이동합니다.
2. pam.conf 파일을 편집하여 암호 서비스 스택에 암호 동기화 줄을 삽입합니다. 플랫폼별 구성은 다음 예제를 참조하십시오.

```
passwd password required /usr/lib/security/pam_unix.so
```

```
passwd password optional /usr/lib/security/pam_CA_eta.so
```

3. (선택 사항) `pam_CA_eta` 모듈 줄에서 다음 선택적 매개 변수를 추가할 수 있습니다.

config=/path/file

대체 구성 파일의 위치를 나타냅니다.

syslog

오류 및 정보 메시지를 로컬 `syslog` 서비스로 전송합니다.

trace

각 암호 업데이트 오퍼레이션에 대한 추적 파일을 생성합니다. 추적 파일의 이름은 `/tmp/pam_CA_eta-trace.<nnnn>`으로 지정됩니다. 여기서 `<nnnn>`은 암호 프로세스의 PID 번호입니다.

4. 다음 플랫폼별 구성 변경을 구현합니다.

AIX 시스템의 경우 `/etc/pam.conf` 파일의 맨 아래에 다음 줄을 추가합니다.

#

CA Identity Manager Unix Password Synchronization

#

```
login password optional /usr/lib/security/pam_CA_eta.so syslog
passwd password optional /usr/lib/security/pam_CA_eta.so syslog
rlogin password optional /usr/lib/security/pam_CA_eta.so syslog
su password optional /usr/lib/security/pam_CA_eta.so syslog
telnet password optional /usr/lib/security/pam_CA_eta.so syslog
sshd password optional /usr/lib/security/pam_CA_eta.so syslog
OTHER password optional /usr/lib/security/pam_CA_eta.so syslog
```

HP-UX 시스템의 경우 `/etc/pam.conf` 파일의 맨 아래에 다음 줄을 추가합니다.

#

CA Identity Manager Unix Password Synchronization

#

```
login password optional /usr/lib/security/libpam_CA_eta.1 syslog
passwd password optional /usr/lib/security/libpam_CA_eta.1 syslog
dtlogin password optional /usr/lib/security/libpam_CA_eta.1 syslog
dtaction password optional /usr/lib/security/libpam_CA_eta.1 syslog
OTHER password optional /usr/lib/security/libpam_CA_eta.1 syslog
```

HP-UX Itanium2 의 경우 `/etc/pam.conf` 파일의 맨 아래에 다음 줄을 추가합니다.

#

```
# CA Identity Manager Unix Password Synchronization
```

```
#
```

```
login    password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
passwd   password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
dtlogin  password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
dtaction password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
OTHER    password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
```

Sun Solaris 시스템의 경우 기존 pam_unix 줄 뒤에 pam_CA_eta 줄을 추가합니다.

```
#
```

```
# Password management
```

```
#
```

```
other    password required    /usr/lib/security/pam_unix.so.1
other    password optional    /usr/lib/security/pam_CA_eta.so syslog
```

Linux 시스템의 경우 기존 pam_cracklib 줄과 pam_unix 줄 사이에 pam_CA_eta 줄을 추가합니다.

```
password required    /lib/security/pam_cracklib.so retry=3 type=
password optional    /lib/security/pam_CA_eta.so syslog
password sufficient  /lib/security/pam_unix.so nullok use_authok md5 shadow
password required    /lib/security/pam_deny.so
```

5. AIX 시스템의 경우 /etc/security/login.cfg 파일을 편집하여 auth_type = PAM_AUTH 를 설정합니다. 그러면 기본적으로 사용되지 않는 PAM 프레임워크가 사용하도록 설정됩니다. 이 설정은 런타임 설정이므로 시스템을 재부팅하지 않아도 적용됩니다.

UNIX 암호 동기화 문제 해결

syslog 및 추적 메시지를 사용하고 구성, LDAP/TLS 연결, 암호 동기화 및 PAM 프레임워크를 테스트하여 UNIX PAM 기능의 문제를 해결할 수 있습니다.

추가 정보

[syslog 메시지 활성화](#) (페이지 157)

[추적 메시지 활성화](#) (페이지 157)

syslog 메시지 활성화

/etc/pam.conf 파일의 pam_CA_eta 줄에 syslog 매개 변수를 추가하면 pam_CA_eta 모듈이 정보 및 오류 메시지를 생성합니다. 로깅 옵션을 사용 중인 경우 UNIX 관리자는 UNIX 계정의 암호가 변경될 때마다 syslog 파일에서 정보 메시지를 볼 수 있습니다. 이러한 메시지는 기본 문제를 진단하기에 충분한 정보를 제공합니다.

자동 서비스로 실행될 때보다 리소스가 더 많이 필요하지 않으므로 프로덕션 시스템에서 이 옵션을 영구적으로 설정할 수 있습니다.

추적 메시지 활성화

syslog 메시지가 충분한 정보를 제공하지 않는 경우 추적 모드가 더 자세한 정보를 제공할 수 있습니다. 추적 모듈에서는 각 암호 업데이트 오퍼레이션마다 모듈에서 사용되는 대부분의 기능 호출과 해당 기능에서 사용되거나 반환되는 데이터 항목이 포함된 /tmp/pam_CA_eta-trace.<nnnn>이라는 파일이 생성됩니다. 여기서 <nnnn>은 암호 프로세스의 PID 입니다.

루트 계정을 통해서만 추적 파일을 읽을 수 있지만 추적 파일에는 새 일반 텍스트 암호가 포함됩니다. 따라서 프로덕션 시스템에서 이 매개 변수를 영구적으로 사용하면 안 됩니다.

구성 파일 테스트

/etc/pam_CA_eta 디렉터리에 있는 test_config 도구를 사용하여 구성 파일을 확인할 수 있습니다. 우선, 다음과 같이 폴더 구조를 설정하십시오.

1. pam_CA_eta 폴더를 /etc 아래로 이동하십시오.
2. pam_CA_eta-1.1 아래의 모든 항목을 /etc/pam_CA_eta 로 복사하십시오.

샘플 명령줄 항목은 다음과 같습니다.

```
/etc/pam_CA_eta/test_config [config=/path/to/config_file]
```

예제 세션은 다음과 같습니다.

```
./test_config [config=/path/to/config_file]
# ./test_config
./test_config: succeeded
Trace file is /tmp/test_config-trace.1274
```

명령 출력에 표시된 대로 구성 파일 구문 분석의 모든 상세 정보를 포함하는 추적 파일이 생성되었습니다.

CAM 서비스 보기

다음 절차를 수행하여 누가 서비스를 시작했는지 찾을 수 있습니다.

CAM 서비스를 보려면

1. 텔넷 또는 SSH 클라이언트를 사용하여 root 로서 UNIX 컴퓨터에 로그인합니다.
2. 다음 UNIX 명령을 실행합니다.

```
ps -ef | grep cam
```

다음과 유사한 화면이 표시됩니다.

```
root 13822      1 11 11:30:12 ?    0:00 cam
```

```
root 13843 13753  3 11:56:31 pts/5  0:00 grep cam
```

참고: 시스템의 root 사용자가 서비스를 시작하지 않는 경우 서비스는 시작된 것처럼 보이지만 서비스를 사용할 수는 없습니다. CA Identity Manager 는 다음 메시지를 표시합니다: “Permission denied: user must be root”(권한 거부됨: 사용자가 root 여야 합니다.)

LDAP/TLS 연결 테스트

/etc/pam_CA_eta 디렉터리에 있는 `test_ldap` 도구를 통해 구성 파일 매개 변수를 사용하여 프로비저닝 서버에 대한 연결을 확인할 수 있습니다. 샘플 명령줄 항목은 다음과 같습니다.

```
/etc/pam_CA_eta/test_ldap [config=/path/to/config_file]
```

예제 세션은 다음과 같습니다.

```
./test_ldap [config=/path/to/config_file]
# ./test_ldap: succeeded
Trace file is /tmp/test_ldap-trace.1277
```

명령 출력에 표시된 대로 구성 파일 구문 분석과 프로비저닝 서버에 대한 연결의 모든 상세 정보를 포함하는 추적 파일이 생성되었습니다.

암호 동기화 테스트

/etc/pam_CA_eta 폴더에 있는 `test_sync` 도구를 사용하여 프로비저닝 서버가 로컬 계정의 암호 업데이트를 효과적으로 전파하는지 확인할 수 있습니다. 샘플 명령줄 항목은 다음과 같습니다.

```
/etc/pam_CA_eta/test_sync <user> <password> [config=/path/to/config_file]
```

예제 세션은 다음과 같습니다.

```
# /etc/pam_CA_eta/test_sync pam002 newpass1234
CA Identity Manager password synchronization started.
:ETA_S_0245<MGU>, Global User 'pam002' and associated account passwords updated
successfully: (accounts updated: 2, unchanged: 0, failures: 0)
CA Identity Manager password synchronization succeeded.
/etc/pam_CA_eta/test_sync: succeeded
Trace file is /tmp/test_sync-trace.2244
```

명령 출력에 표시된 대로 구성 파일 구문 분석, 프로비저닝 서버에 대한 연결 및 계정 업데이트의 모든 상세 정보를 포함하는 추적 파일이 생성되었습니다.

구성 파일에서 기본 `verbose yes` 매개 변수를 사용하여 상세 모드를 사용하는 경우 이 명령은 암호 전파에 대한 정보 메시지와 잠재적 오류 메시지를 제공합니다.

PAM 프레임워크 테스트

PAM 테스트 라이브러리를 사용하여 PAM 프레임워크가 암호 변경을 올바르게 감지하는지 확인할 수 있습니다.

PAM 프레임워크를 테스트하려면

1. `pam_test` 파일을 `/usr/lib/security(/hpux32)` 폴더에 복사합니다.
2. 매개 변수 없이 `pam_test` 라이브러리에 대한 암호 클래스 줄을 추가합니다.

Solaris 에 대한 예제는 다음과 같습니다.

```
other password optional /usr/lib/security/pam_test
```

3. 테스트 사용자에게 `passwd` 명령을 실행한 다음 `syslog` 파일에서 `pam_test[<pid>]` 태그가 지정된 줄을 검색합니다.

명령 출력에 생성된 추적 파일의 이름이 표시됩니다. 예를 들면 다음과 같습니다.

```
pam_test[1417]: Succeeded, trace file is /tmp/pam_test-trace.1417
```

OS400 에서 암호 동기화

암호 동기화 에이전트를 사용하면 OS/400 끝점 시스템에서 수행된 암호 변경 내용을 CA Identity Manager 가 관리하는 다른 계정으로 전파할 수 있습니다. 암호 동기화 에이전트는 다음과 같이 작동합니다.

1. 에이전트를 OS/400 끝점 시스템에 설치하고 실행합니다.

설치 중에 프로그램이 OS/400 시스템에 등록되므로 사용자가 자신의 암호를 변경하면 에이전트가 암호 변경 내용을 프로비저닝 서버로 전송합니다.

2. 프로비저닝 서버가 암호 변경 내용을 연결된 계정으로 전파합니다.

암호 변경 명령(CHGPWD)이나 암호 변경(QSYCHGPW) API 에서 시작된 암호 변경 내용이 에이전트에 수신됩니다.

3. 에이전트가 PWDSYNCH/LOG 에 있는 로그 파일에 오퍼레이션 성공 또는 실패를 기록합니다.

암호 동기화 에이전트는 다음 플랫폼에서 지원됩니다.

- OS400 V5R2
- OS400 V5R3
- OS400 V5R4

암호 동기화 에이전트를 설치하려면

1. 프로비저닝 구성 요소 설치 미디어를 찾습니다.
2. \Agent 아래 OS/400 에서 암호 동기화 에이전트 설치 관리자를 실행합니다.
3. 화면에 나타나는 지침을 따라 설치를 완료합니다.

참고: "Endpoint Agent Software"(끝점 에이전트 소프트웨어) 링크에 있는 설치 지침은 다음 섹션에 포함되어 있습니다.

OS400 암호 동기화 에이전트 설치

*ADDOBJ 권한이 있어야 합니다. 다음은 에이전트가 암호 변경 알림을 수신하는 데 필요한 사항입니다.

- 시스템 값 QPWDVLDPGM 을 *REGFAC 로 설정해야 합니다.
- WRKREGINF EXITPNT 명령(QIBM_QSY_VLD_PASSWRD)을 사용하여 프로그램을 등록해야 합니다.
- 환경이 끝점 계정으로부터 수신되는 암호 변경 내용을 허용해야 합니다. 관리 콘솔에 대한 액세스 권한이 있는 관리자가 이 기능을 사용하도록 설정합니다.

에이전트는 암호 변경이 수행된 경우에만 시작됩니다. 암호를 변경하려면 CHGPWD 명령을 실행하십시오.

참고: 전역 사용자에게 암호 동기화 대상 플래그가 지정되어야 합니다.

iSeries 에서

1. *ALLOBJ 및 *SECADM 권한이 있는 사용자(예: QSECOFR)로 로그인합니다.
2. PWDSYNCH 라는 사용자를 만듭니다.

CRTUSRPRF USRPRF(PWDSYNCH) PWDEXP(*YES)

참고: 보안 조치로 암호가 만료된 사용자가 생성됩니다.

3. 선택한 라이브러리(예: MYLIB)에 설치 패키지를 저장할 저장 파일을 만듭니다.

```
CRTSAVF MYLIB/PWDSYNCH
```

4. 저장 파일이 있는 Windows 시스템에서 FTP 를 사용하여 저장 파일을 iSeries 로 전송합니다.

```
ftp <hostname>  
바이너리  
cd MYLIB  
put PWDSYNCH.FILE
```

5. iSeries 에서 저장 파일의 프로그램을 추출합니다.

```
RSTLIB SAVLIB(PWDSYNCH) DEV(*SAVF) SAVF(MYLIB/PWDSYNCH)
```

이 명령은 동기화 에이전트를 추출하여 PWDSYNCH 라이브러리에 설치합니다.

6. 설치를 확인합니다.

```
DSPLIB PWDSYNCH
```

다음 개체가 표시됩니다.

개체	유형	특성
PWDSYNCH	*PGM	CLE
CONFIG	*FILE	PF
LOG	*FILE	PF

7. PWDSYNCH 를 암호 유효성 검사 종료 프로그램으로 사용하도록 iSeries 를 설정합니다.

```
CHGSYSVAL SYSVAL(QPWDVLDPGM) VALUE(*REGFAC)  
ADDEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD) FORMAT(VLDP0100) PGMNBR(1)  
PGM(PWDSYNCH/PWDSYNCH) TEXT('eTrust Admin Password Synch Agent')
```

8. iSeries 에서 CA IAM 커넥터 서버에 대한 연결 매개 변수를 지정합니다.

```
EDTF FILE(PWDSYNCH/CONFIG)
```

05400 암호 동기화 에이전트 설치

*ADDOBJ 권한이 있어야 합니다. 다음은 에이전트가 암호 변경 알림을 수신하는 데 필요한 사항입니다.

- 시스템 값 QPWDVLDPGM 을 *REGFAC 로 설정해야 합니다.
- WRKREGINF EXITPNT 명령(QIBM_QSY_VLD_PASSWRD)을 사용하여 프로그램을 등록해야 합니다.
- 환경이 끝점 계정으로부터 수신되는 암호 변경 내용을 허용해야 합니다. 관리 콘솔에 대한 액세스 권한이 있는 관리자가 이 기능을 사용하도록 설정합니다.

에이전트는 암호 변경이 수행된 경우에만 시작됩니다. 암호를 변경하려면 CHGPWD 명령을 실행하십시오.

참고: 전역 사용자에게 암호 동기화 대상 플래그가 지정되어야 합니다.

iSeries 에서

1. *ALLOBJ 및 *SECADM 권한이 있는 사용자(예: QSECOFR)로 로그인합니다.
2. PWDSYNCH 라는 사용자를 만듭니다.

```
CRTUSRPRF USRPRF(PWDSYNCH) PWDEXP(*YES)
```

참고: 보안 조치로 암호가 만료된 사용자가 생성됩니다.

3. 선택한 라이브러리(예: MYLIB)에 설치 패키지를 저장할 저장 파일을 만듭니다.

```
CRTSAVF MYLIB/PWDSYNCH
```

4. 저장 파일이 있는 Windows 시스템에서 FTP 를 사용하여 저장 파일을 iSeries 로 전송합니다.

```
ftp <hostname>
바이너리
cd MYLIB
put PWDSYNCH.FILE
```

5. iSeries 에서 저장 파일의 프로그램을 추출합니다.

```
RSTLIB SAVLIB(PWDSYNCH) DEV(*SAVF) SAVF(MYLIB/PWDSYNCH)
```

이 명령은 동기화 에이전트를 추출하여 PWDSYNCH 라이브러리에 설치합니다.

6. 설치를 확인합니다.

DSPLIB PWDSYNCH

다음 개체가 표시됩니다.

개체	유형	특성
PWDSYNCH	*PGM	CLE
CONFIG	*FILE	PF
LOG	*FILE	PF

7. PWDSYNCH 를 암호 유효성 검사 종료 프로그램으로 사용하도록 iSeries 를 설정합니다.

```
CHGSYSVAL SYSVAL(QPWDVLDPGM) VALUE(*REGFAC)
ADDEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD) FORMAT(VLDP0100) PGMNBR(1)
PGM(PWDSYNCH/PWDSYNCH) TEXT('eTrust Admin Password Synch Agent')
```

8. iSeries 에서 CA IAM CS(CA IAM 커넥터 서버)에 대한 연결 매개 변수를 지정합니다.

```
EDTF FILE(PWDSYNCH/CONFIG)
```

사용자 콘솔에서 끝점 업데이트

사용자 콘솔에서 끝점을 업데이트하여 에이전트가 설치되었음을 나타내십시오.

다음 단계를 수행하십시오.

1. 사용자 콘솔에 로그인합니다.
2. 에이전트가 설치된 끝점을 검색합니다.
3. "끝점 설정" 탭을 클릭합니다.
4. "암호 동기화 에이전트가 설치되어 있음" 확인란을 선택합니다.

암호 동기화를 허용하도록 환경 설정

암호 동기화 에이전트를 설치한 후에는 끝점에서 수행된 암호 변경 내용을 수신하도록 환경을 설정할 수 있습니다. 이 태스크의 경우 관리자가 해당 변경 내용을 허용하도록 환경을 설정하려면 관리 콘솔과 CA Directory에 대한 액세스 권한이 있어야 합니다.

다음 단계를 수행하십시오.

1. 새 사용자의 경우 다음과 같이 관리 콘솔을 사용합니다.
 - a. 환경을 선택합니다.
 - b. "고급 설정", "프로비저닝"을 차례로 클릭합니다.
 - c. "Enable Password Changes from Endpoint Accounts"(끝점 계정의 암호 변경 사용) 확인란을 선택합니다.
2. 기존 사용자의 경우 CA Directory에서 eTPropagatePassword 특성을 1로 설정합니다.

SSL 구성

SSL은 동기화 에이전트와 프로비저닝 서버 간의 통신을 암호화하는 데 사용됩니다. 이는 SSL이 네트워크를 통해 암호를 전송하기 때문에 동기화 에이전트에 중요합니다. SSL을 항상 사용하는 것이 좋습니다.

동기화 에이전트는 SSL과 연결하기 위해 프로비저닝 서버의 인증서를 트러스트해야 합니다. 따라서 인증서를 iSeries 시스템에 설치하고 구성해야 동기화 에이전트가 인증서를 트러스트합니다. 이러한 태스크는 OS/400의 선택적 구성 요소인 Digital Certificate Manager가 수행합니다. Digital Certificate Manager 설치 및 설정에 대해서는 OS/400 설명서를 따르십시오.

프로비저닝 서버 인증서 설치

SSL 을 사용하려면 iSeries 시스템에 다음 운영 체제 구성 요소를 설치해야 합니다.

- 암호화 액세스 공급자 라이선스 프로그램(5722-AC3)
- Digital Certificate Manager(OS/400 의 옵션 34)
- iSeries 용 IBM HTTP Server(5722-DG1)

iSeries 에서

1. 프로비저닝 서버 시스템에서 iSeries 로 프로비저닝 서버 인증서를 업로드합니다. 다음 위치에서 인증서를 찾을 수 있습니다.

```
C:\Program Files\CA\Identity Manager\Provisioning  
Server\Data\TLS\server\et2_cacert.pem
```

2. DCM 에 로그인합니다.

웹 브라우저를 사용하여 <http://<hostname>:2001> 로 이동합니다.

메시지가 표시되면 QSECOFR 로 로그인하고 "Digital Certificate Manager"를 클릭합니다.

3. "Select a Certificate Store"(인증서 저장소 선택)를 클릭하고 *SYSTEM 인증서 저장소를 선택합니다. 이 저장소가 없는 경우 *SYSTEM 이라는 저장소를 만들고 인증서 저장소 암호를 입력하십시오.

4. DCM 을 사용하여 CA 인증서가 될 인증서를 가져옵니다.

"Manage Certificates"(인증서 관리), "Import Certificate"(인증서 가져오기)를 클릭하십시오. "Certificate Authority (CA)"(인증 기관) 옵션을 선택한 다음 프로비저닝 서버 인증서의 파일 이름을 입력하십시오. 이 위치는 1 단계에서 인증서를 업로드한 곳입니다. 인증서에 대해 레이블 "Provisioning Server"를 입력하십시오.

5. CA 인증서를 끝점 *SYSTEM 키 저장소로 가져온 후에는 IBM Directory 클라이언트 QIBM_GLD_DIRSRV_CLIENT 가 *SYSTEM 키 저장소에 액세스할 수 있는지 확인합니다. 그렇지 않으면 PSA 의 SSL 초기화 호출이 실패합니다.

6. "Manage Applications"(응용 프로그램 관리), "Define CA Trust List"(CA 트러스트 목록 정의)를 차례로 열고 "Directory Services Client"(Directory Services 클라이언트)를 선택하여 프로비저닝 서버 인증서를 트러스트하도록 Directory Services 클라이언트 응용 프로그램을 구성합니다.

4 단계에서 올바로 가져온 경우 여기에 프로비저닝 서버 인증서가 나열됩니다.

"Trusted for the Provisioning Server"(프로비저닝 서버에 대해 트러스트됨) 인증서를 클릭한 다음 "확인"을 클릭하십시오.

7. SSL 파일에 대한 PUBLIC 읽기 권한을 지정하고 *SYSTEM 인증서 저장소에 대한 읽기 액세스 권한을 부여합니다.

(/QIBM/userdata/ICSS/Cert/Server/default.kdb)

상위 폴더에 대한 읽기 및 실행 권한을 부여합니다.

(/QIBM/userdata/ICSS/Cert/Server)

참고: 사용자 PWDSYNCH의 권한 수용이 / 파일 시스템에서 작동하지 않으므로 모든 사용자에게 액세스 권한을 부여해야 합니다.

암호 동기화 에이전트 제거

암호 동기화 에이전트를 제거해야 하는 경우 다음 절차를 따르십시오.

암호 유효성 검사 종료 지점에서

1. PWDSYNCH를 제거합니다.

RMVEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD) FORMAT(VLDP0100) PGMNBR(1)

2. 동기화 에이전트 라이브러리를 삭제합니다.

DLTLIB PWDSYNCH

3. 사용자 PWDSYNCH를 삭제합니다.

DLTUSRPRF PWDSYNCH

4. SSL 지침을 따라 DCM에 로그인하고 *SYSTEM 인증서 저장소로 작업하여 프로비저닝 서버 인증서를 제거합니다.

"Manage Certificates"(인증서 관리), "Delete Certificate"(인증서 삭제)를 차례로 클릭하고 'Certificate Authority (CA)'(CA(인증 기관))를 선택합니다.

'프로비저닝 서버' 인증서를 선택하고 "삭제"를 클릭합니다.

OS/400 암호 에이전트 매개 변수가 올바르게 설정되어야 함

작동하려면 "pwd_case_action" 매개 변수의 값이 올바르게 설정되어야 합니다. 올바른 값은 다음을 포함합니다.

- pwd_case_action = pwd_case_unchanged
- pwd_case_action = pwd_to_uppercase
- pwd_case_action = pwd_to_lowercase

pwd_case_action = [잘못된 값]인 경우 암호는 대문자로 강제됩니다.

참고: OS400 PSA 구성 파일에서 pwd_case_action 플래그를 pwd_to_uppercase 또는 pwd_to_lowercase 로 설정하면 제공된 암호가 프로비저닝 서버의 암호 정책 설정을 준수하지 않는 경우 암호가 전역 사용자로 다시 전파되지 않을 수 있습니다. 예를 들어, 일부 암호 정책은 암호 값이 최소 1 개 이상의 대문자 또는 소문자 값을 포함하도록 요구할 수 있습니다.

참고: 암호 동기화 에이전트를 구성할 때 QPWDVLV(암호 수준) 시스템 값에 주의하십시오.

- AS400 시스템에서 QPWDVLV 을 0(기본값)으로 설정한 경우 1~10 자의 대문자로 된 암호가 지원됩니다.
- QPWDVLV 을 2 나 3 으로 설정한 경우에는 1~128 자의 대/소문자로 된 암호가 허용됩니다.

기본적으로 PSA 는 변경되지 않은 암호를 프로비저닝 서버로 전파합니다. 하지만 QPWDVLV 값에 관계없이 "pwd_case_action"을 "pwd_to_uppercase"로 설정하여 대문자로 된 암호를 전파하거나 "pwd_to_lowercase"로 설정하여 소문자로 된 암호를 전파하도록 PSA 를 강제할 수 있습니다.

제 7 장: 그룹

여러 유형의 그룹이나 이러한 유형의 조합을 만들 수 있습니다.

- 정적 그룹--대화식으로 추가된 사용자의 목록
- 동적 그룹--LDAP 쿼리를 충족하는 경우 그룹에 속하는 사용자(사용자 저장소로 LDAP 디렉터리 필요)

참고: "동적 그룹 쿼리" 필드는 이 필드가 그룹에 대한 `directory.xml`에 있는 경우라도 "그룹 만들기" 태스크 또는 기타 그룹 태스크에 포함되지 않습니다. 관련된 프로필 화면을 편집하여 태스크에 "동적 그룹 쿼리" 필드를 포함합니다.

- 중첩된 그룹--다른 그룹을 포함하는 그룹(사용자 저장소로 LDAP 디렉터리 필요)

참고: 사용자가 속한 정적, 동적, 중첩 그룹을 보려면 "사용자" 개체의 "그룹" 탭을 사용하십시오. 이 탭은 기본적으로 "사용자 보기" 및 "사용자 수정" 태스크에 표시됩니다.

이 섹션은 다음 항목을 포함하고 있습니다.

[정적 그룹 만들기](#) (페이지 169)

[동적 그룹 만들기](#) (페이지 170)

[동적 그룹 쿼리 매개 변수](#) (페이지 171)

[중첩된 그룹 만들기](#) (페이지 173)

[정적, 동적 및 중첩된 그룹 예](#) (페이지 175)

[그룹 관리자](#) (페이지 176)

정적 그룹 만들기

사용자 모음을 정적 그룹으로 연결할 수 있습니다. 그룹의 구성원 목록에 개별 사용자를 추가하거나 제거하여 정적 그룹을 관리합니다. 그룹의 구성원 목록을 보려면 "그룹 보기" 및 "그룹 수정" 태스크에 기본적으로 포함되는 "구성원" 탭을 사용합니다.

참고: "구성원" 탭에는 명시적으로 그룹에 추가된 구성원만 표시되고 동적으로 추가된 구성원은 표시되지 않습니다.

정적 그룹을 만들려면

1. 사용자 콘솔에서 "그룹", "그룹 만들기"를 선택합니다.
2. 새 그룹이나 그룹 사본을 만들도록 선택하고 **확인**을 클릭합니다.
3. "프로필" 탭에서 그룹 이름, 그룹 조직, 설명 및 그룹 관리자 이름을 입력합니다.
4. "구성원" 탭을 클릭합니다.
5. "사용자 추가"를 클릭합니다.
6. 포함할 사용자를 검색합니다.
7. 사용자 옆에 확인 표시를 하고 "선택"을 클릭합니다.
8. "제출"을 클릭합니다.

동적 그룹 만들기

사용자를 개별적으로 검색하고 추가할 필요 없이 사용자 콘솔에서 LDAP 필터 쿼리를 정의하여 런타임에 동적으로 그룹 구성원 자격을 결정함으로써 동적 그룹을 만들 수 있습니다.

예를 들어, NeteAuto 의 모든 미국 직원을 나열하는 그룹을 생성하려면 사용자 콘솔의 "동적 그룹 쿼리" 필드에 다음과 유사한 LDAP 검색 필터를 정의할 수 있습니다.

```
ldap:///cn=Employees,o=NeteAuto,c=US??sub
```

이 쿼리를 수정하여 미국 내에 없는 직원을 찾을 수도 있습니다.

[정적, 동적 및 중첩된 그룹 예](#) (페이지 175)에서는 정적, 동적 및 중첩된 그룹에서 만들어진 그룹의 예를 보여 줍니다.

관련된 프로필 화면을 편집하여 태스크에 "동적 그룹 쿼리" 필드를 포함합니다. "그룹 만들기" 태스크에는 이 필드가 기본적으로 포함되지 않습니다.

참고: 동적 그룹을 사용하려면 시스템 관리자가 디렉터리 구성 파일(directory.xml)에서 지원을 구성해야 합니다.

- 다음과 같이 "Directory Groups Behavior" 섹션에 GroupTypes 요소를 추가합니다.

```
<GroupTypes type=type>
```

type 은 [NESTED](#) (페이지 173), DYNAMIC, ALL 일 수 있습니다.

GroupTypes 는 대/소문자를 구분합니다.

- 잘 알려진 %DYNAMIC_GROUP_MEMBERSHIP% 특성을 사용자 저장소에 있는 실제 특성에 매핑합니다.

동적 그룹을 만들려면

1. 사용자 콘솔에서 "그룹", "그룹 만들기"를 선택합니다.
2. 새 그룹이나 그룹 사본을 만들도록 선택하고 **확인**을 클릭합니다.
3. "프로필" 탭에서 그룹 이름, 그룹 조직, 설명 및 그룹 관리자 이름을 입력합니다.
4. "동적 그룹 쿼리" 필드에 다음 예와 유사한 LDAP 검색 필터를 입력합니다.

```
ldap:///cn=Employees,o=NeteAuto,c=US??sub?
```

5. "제출"을 클릭합니다.

참고: "그룹 수정" 태스크가 있는 관리자만 그룹의 동적 구성원 자격을 변경할 수 있습니다.

동적 그룹 쿼리 매개 변수

검색에서 다음과 같은 동적 쿼리 매개 변수를 사용할 수 있습니다.

```
ldap:///<검색 기본 DN>??<검색 범위>?<검색 필터>
```

- <검색 기본 DN>은 LDAP 디렉터리에서 검색을 시작하는 지점입니다. 쿼리에 기본 DN 을 지정하지 않으면 그룹의 조직이 기본 DN 이 됩니다.

- <검색 범위>는 검색 범위를 지정하며 다음을 포함합니다.
 - sub - 기본 DN 수준 이하의 항목을 반환합니다.
 - one - URL 에 지정한 기본 DN 보다 한 수준 아래의 항목을 반환합니다. (기본값)
 - base - 검색 옵션으로 base 를 무시하고 대신 one 을 사용합니다.

one 또는 base 를 사용하면 기본 DN 조직의 사용자만 가져옵니다.
sub 를 사용하면 기본 DN 조직 및 트리에서 모든 하위 조직의 사용자를 모두 가져옵니다.
- <검색 필터>는 검색 범위 내의 항목에 적용할 필터입니다. 검색 필터를 입력하는 경우 다음과 같은 표준 LDAP 쿼리 구문을 사용합니다.
(<논리 연산자><비교><비교...>)
- <논리 연산자>는 다음 중 하나입니다.
 - 논리적 OR: |
 - 논리적 AND: &
 - 논리적 NOT: !
- <비교>는 <특성><연산자><값>을 나타냅니다.
예:
(&(city=boston)(state=Massachusetts))
기본 검색 필터는 (objectclass=*)입니다.

동적 쿼리를 만들 때 다음 사항에 주의하십시오.

- "ldap" 접두어는 다음과 같이 소문자여야 합니다.
ldap:///o=MyCorporation??sub?(title=Manger)
- LDAP 서버 호스트 이름이나 포트 번호를 지정할 수 없습니다. 모든 검색은 환경과 관련된 LDAP 디렉터리 내에서 수행됩니다.

다음 표에는 샘플 LDAP 쿼리가 포함되어 있습니다.

설명	쿼리
매니저인 모든 사용자	ldap:///o=MyCorporation??sub?(title=Manger)

설명	쿼리
뉴욕 서부 지사에 있는 모든 매니저	ldap:///o=MyCorporation??one?(&(title=Manager)(roomNumber=NYWest))
휴대폰이 있는 모든 기술자	ldap:///o=MyCorporation??one?(&(employeetype=technician)(mobile=*))
직원 번호가 1000 에서 2000 사이에 있는 모든 직원	ldap:///o=MyCorporation, (& (ou=employee) (employeenumber >=1000) (employeenumber <=2000))
회사에서 6 개월 이상 근무한 모든 헬프 데스크 관리자	ldap:///o=MyCorporation,(& (cn=helpdeskadmin) (DOH => 2004/04/22))
	참고: 이 쿼리를 사용하려면 사용자의 고용 날짜에 대해 DOH 특성을 만들어야 합니다.

참고: > 및 <(보다 큼 및 보다 작음) 비교는 산술적이 아니라 사전순입니다. 이러한 비교 연산자 사용에 대한 자세한 내용은 LDAP 디렉터리 서버 설명서를 참조하십시오.

중첩된 그룹 만들기

사용자 저장소가 LDAP 디렉터리이면 그룹을 다른 그룹의 구성원으로 추가할 수 있습니다. 해당 그룹을 **중첩된 그룹**이라고 합니다.

중첩된 그룹이 포함된 그룹을 **부모 그룹**이라고 합니다. 중첩된 그룹의 구성원은 부모 그룹의 구성원이 됩니다. 하지만 부모 그룹의 구성원은 중첩된 그룹의 구성원이 되지 않습니다.

중첩된 그룹은 한 목록이 다른 목록의 구성원이 될 수 있는 전자 메일 배포 목록과 유사합니다. 중첩된 그룹을 사용하면 그룹과 사용자를 그룹의 구성원으로 추가할 수 있습니다. 그룹을 다른 그룹의 구성원 목록에 중첩하면 중첩된 그룹 구성원을 모두 포함할 수 있습니다.

예를 들어, 회사의 제조, 디자인, 운송 및 회계 사업부에 대해 별도 그룹을 만든 경우 모든 개별 사업부 그룹을 회사 부모 그룹의 구성원으로 중첩하여 전체 회사에 대해 부모 그룹을 만들 수 있습니다. 따라서 중첩된 제조, 디자인, 운송 및 회계 그룹의 모든 변경 사항이 전체 회사의 중첩된 그룹에 자동으로 반영됩니다. 다른 그룹 내에 중첩된 그룹은 동적일 수 있으며 다른 중첩된 그룹을 포함할 수 있습니다.

[정적, 동적 및 중첩된 그룹 예](#) (페이지 175)의 그림은 정적, 동적 및 중첩된 그룹에서 만들어진 부모 그룹을 보여 줍니다.

중첩된 그룹을 만들기 전에 다음을 확인합니다.

- "그룹 구성원 수정" 태스크가 있는 관리자만 사용자 콘솔에 있는 그룹의 정적 구성원 목록에서 중첩된 그룹을 추가하거나 변경할 수 있습니다.
- 적절한 관리자 권한이 있는 사용자만 그룹의 구성원을 수정, 추가 또는 제거할 수 있습니다.

예를 들어, 부모 그룹 A가 중첩된 그룹 B와 C에서 만들어진 경우 그룹 A 관리자는 그룹 A의 구성원만 수정할 수 있고 B와 C의 구성원은 수정할 수 없습니다. 해당 관리자만 그룹 B와 C를 수정할 수 있습니다.

- 중첩 그룹을 사용하려면 시스템 관리자가 디렉터리 구성 파일(directory.xml)에서 중첩 그룹 지원을 구성해야 합니다.
 - 다음과 같이 "Directory Groups Behavior" 섹션에 GroupTypes 요소를 추가합니다.

```
<GroupTypes type=type>
```

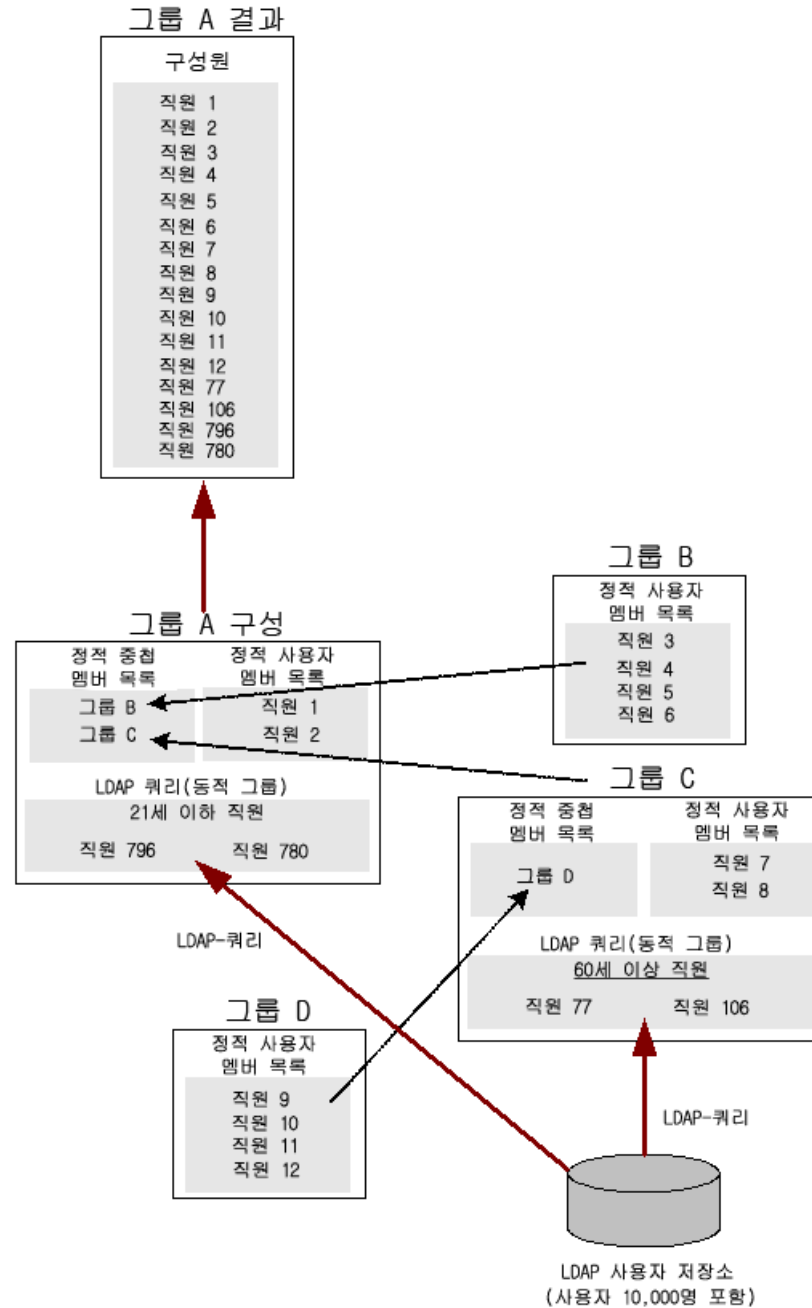

type 은 NESTED, [DYNAMIC](#) (페이지 170), ALL 일 수 있습니다.
GroupTypes 는 대/소문자를 구분합니다.
 - 잘 알려진 %NESTED_GROUP_MEMBERSHIP% 특성을 사용자 저장소에 있는 실제 특성에 매핑합니다.

중첩된 그룹을 만들려면

1. 사용자 콘솔에서 "그룹", "그룹 만들기"를 선택합니다.
2. 새 그룹이나 그룹 사본을 만들도록 선택하고 **확인**을 클릭합니다.
3. "프로필" 탭에서 그룹 이름, 그룹 조직, 설명 및 그룹 관리자 이름을 입력합니다.
4. "구성원" 탭에서 다음을 수행합니다.
 - a. "그룹 추가"를 클릭하여 이 그룹에 중첩된 그룹을 추가합니다.
 - b. 기존 그룹을 검색합니다.
 - c. 그룹 옆에 확인 표시를 하고 "선택"을 클릭합니다.
 - d. "제출"을 클릭합니다.

정적, 동적 및 중첩된 그룹 예

동적, 정적 또는 중첩된 그룹의 조합으로 구성된 복잡한 그룹이 있을 수 있습니다. 다음 그림은 정적, 동적 및 중첩된 그룹에서 만들어진 부모 그룹의 예를 보여 줍니다.



앞의 그림에서 다음을 확인합니다.

- 부모 그룹 A에는 중첩된 그룹 B와 C, 정적 사용자 두 명, 21 살보다 어린 모든 직원을 표시하는 동적 LDAP 쿼리가 포함되어 있습니다.
- 그룹 B는 정적 사용자 4 명으로 구성되어 있습니다.
- 부모 그룹 C에는 중첩된 그룹 D, 정적 사용자 두 명, 나이가 60 살보다 많은 모든 직원을 표시하는 동적 LDAP 쿼리가 포함되어 있습니다.
- 그룹 D에는 정적 사용자 4 명이 포함되어 있습니다.
- 그림 맨 위에는 중첩된 그룹, 동적 쿼리, 그룹 B, C, D의 정적 사용자 구성원 목록에서 얻은 그룹 A 구성원이 표시됩니다.

그룹 관리자

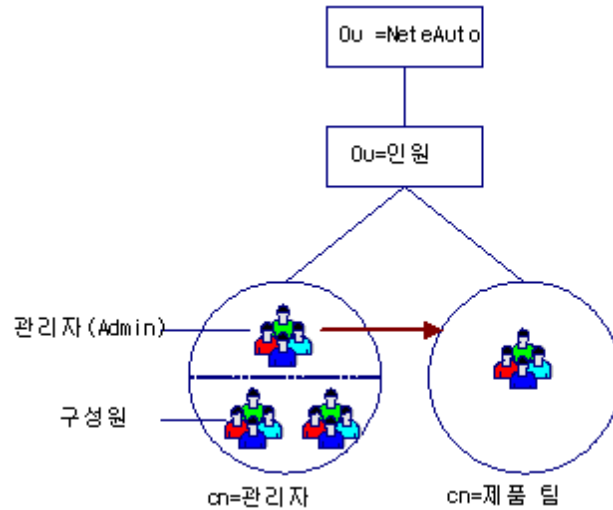
"그룹 만들기" 또는 "그룹 수정"의 "관리자" 탭에서 사용자 또는 그룹을 그룹의 관리자로 지정할 수 있습니다. 참고: 사용자를 그룹 관리자로 할당하는 경우 관리자가 그룹 관리에 적합한 범위가 있는 역할을 가지고 있는지 확인하십시오. 예를 들면 다음과 같습니다.

1. 한 사용자를 그룹의 관리자로 할당하려면 "그룹 수정"을 사용합니다.
2. "그룹" 탭을 사용하여 해당 사용자에게 그룹 관리 태스크(예: 그룹 구성원 수정) 또는 사용자 관리 태스크의 관리자 역할을 할당합니다.
3. 해당 역할이 그룹에 대한 적절한 범위를 갖는지 확인합니다.
 - a. 그룹 관리 태스크를 할당한 역할에 대해 "관리자 역할 보기"를 사용합니다.
 - b. "구성원" 탭에서 다음과 같은 규칙이 있는 정책이 있는지 확인합니다.
 - 그룹 관리자가 충족시키는 구성원 규칙
 - 그룹을 포함하는 범위 규칙
 - 그룹에 추가할 일부 사용자를 포함하는 범위 규칙

참고: 그룹을 다른 그룹의 관리자로 만들려면 시스템 관리자가 디렉터리 구성 파일(directory.xml)에서 그룹 관리자 지원을 구성해야 합니다.

- "Directory AdminGroups Behavior" 섹션에서 AdminGroupTypes type=ALL 을 설정합니다. AdminGroupTypes 는 대/소문자를 구분합니다.
- 잘 알려진 %GROUP_ADMIN_GROUP% 특성을 사용자 저장소에 있는 실제 특성에 매핑합니다.

그룹을 관리자로 할당하는 경우 생성하거나 수정하는 그룹의 관리자만 지정된 그룹의 관리자가 될 수 있습니다. 지정하는 관리자 그룹의 구성원에게는 그룹을 관리할 권한이 없습니다. 다음 그림은 다른 그룹의 관리자인 그룹을 보여 줍니다.



설명:

- "Managers" 그룹은 "Product Teams" 그룹의 관리자입니다.
- "Managers" 그룹의 관리자는 "Product Teams" 그룹을 관리할 수 있습니다. "Managers" 그룹의 구성원은 관리 권한이 없습니다.

제 8 장: 관리 끝점 계정

CA Identity Manager에서는 CA Identity Manager 설치 시 프로비저닝 서버가 설치되는 경우 끝점 시스템의 계정을 관리할 수 있습니다. Exchange, Windows NT 또는 Oracle 계정과 같은 계정을 관리하고 현재 CA Identity Manager와 연결되지 않은 계정인 고아 및 시스템 계정을 관리할 수 있습니다.

이 섹션은 다음 항목을 포함하고 있습니다.

[관리 끝점 통합](#) (페이지 180)

[사용자, 계정 및 역할 동기화](#) (페이지 188)

[끝점 계정과 리버스 동기화](#) (페이지 196)

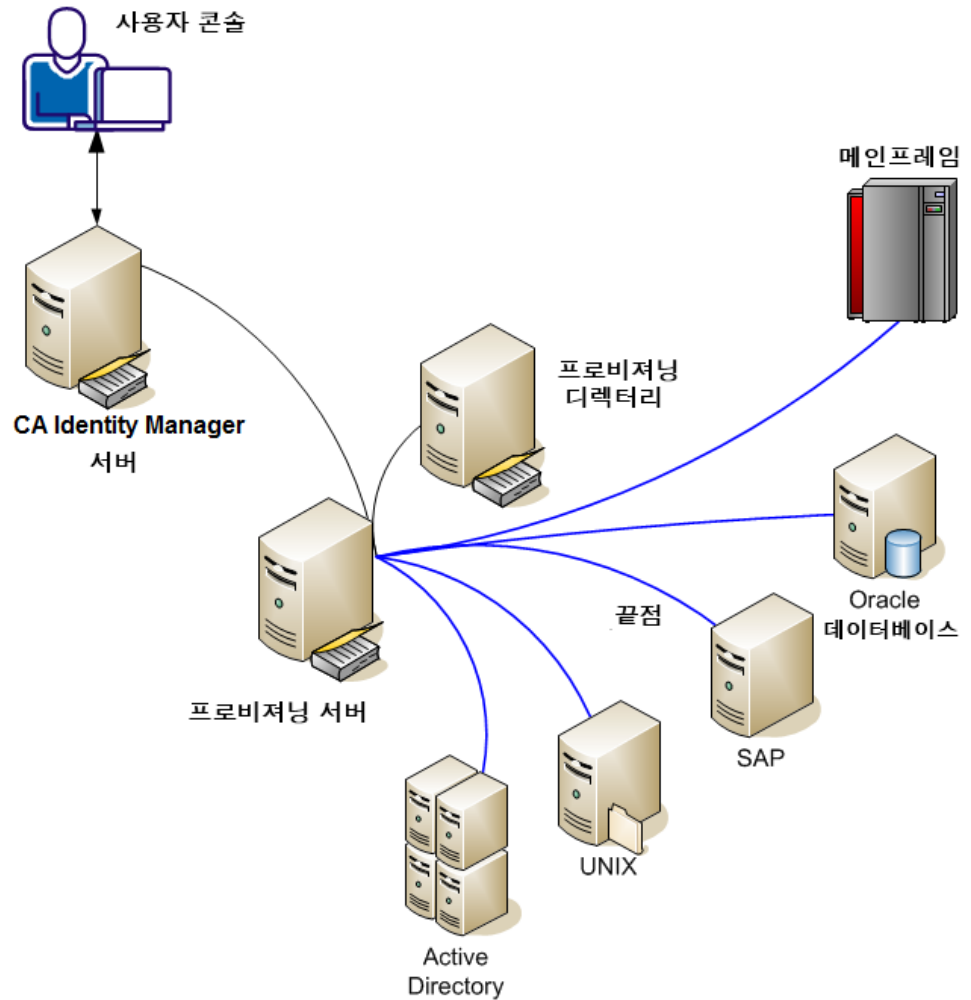
[끝점의 사용자 지정 특성 확장](#) (페이지 207)

[계정 태스크](#) (페이지 209)

[고급 계정 오퍼레이션](#) (페이지 215)

관리 끝점 통합

CA Identity Manager 를 통해 단일 사용자 인터페이스인 사용자 콘솔에서 여러 시스템의 계정을 관리할 수 있습니다. 계정은 관리 끝점 또는 간단히 끝점이라고 하는 시스템에 있습니다. 다음 예에서는 다섯 개의 끝점에서 사용자를 관리합니다.



모든 끝점 조합의 계정을 사용자에게 할당할 수 있습니다. 끝점을 통합하면 CA Identity Manager가 각각의 끝점 계정을 프로비저닝 디렉터리의 사용자와 연결합니다.

다음 절차에서는 사용자 콘솔에서 해당 끝점 계정을 관리할 수 있도록 끝점을 통합하는 방법을 설명합니다.

1. [역할 정의 파일 가져오기](#) (페이지 181)
2. 상관 관계 규칙 만들기
3. 환경에 끝점 추가
4. 탐색 및 상관 관계 지정 정의 만들기
5. 끝점 탐색 및 상관 관계 지정

역할 정의 파일 가져오기

새 끝점에 적용되는 파일에서 역할 정의를 가져옵니다. 이 절차를 수행하려면 관리 콘솔에 액세스해야 합니다.

다음 단계를 수행하십시오.

1. 관리 콘솔에서 "환경"을 클릭합니다.
2. 끝점을 추가하려는 환경을 선택합니다.
3. "역할 및 태스크 설정"을 클릭합니다.
4. "가져오기"를 클릭합니다.
5. "끝점 유형"에서 끝점을 선택합니다.
6. "마침"을 클릭합니다.

현재 창에 가져오기 상태가 나타납니다.

7. "계속"을 클릭하여 종료합니다.
8. 환경을 다시 시작하여 변경 내용을 적용합니다.

상관 관계 규칙 만들기

호스팅 관리자나 "상관 관계 특성 구성" 태스크가 있는 관리자는 사용자가 끝점을 탐색할 때 사용되는 규칙을 만들 수 있습니다. "탐색 및 상관 관계 지정 실행" 태스크는 이러한 규칙을 태스크의 상관 관계 부분에 사용합니다.

상관 관계 규칙은 사용자 콘솔에서 끝점 계정 특성이 사용자 특성에 매핑되는 방법을 결정합니다. 예를 들어 Access Control에는 AccountName이라는 특성이 존재합니다. 이 특성을 사용자 콘솔의 FullName에 매핑하는 규칙을 만들 수 있습니다. 이 규칙에 따라 두 개의 매핑이 하나의 사용자 특성에 적용되는 경우 첫 번째 매개 변수 값이 사용됩니다.

다음 단계를 수행하십시오.

1. 사용자 콘솔에 로그인합니다.
2. "시스템", "프로비저닝 구성", "상관 관계 특성 구성"을 차례로 클릭합니다.
3. "추가"를 클릭합니다.
4. 다음과 같이 상관 관계 규칙을 정의합니다.
 - a. 전역 사용자 특성 목록을 선택합니다.
이 값은 프로비저닝 디렉터리에 나열된 사용자 특성을 참조합니다.
 - b. "특정 계정 특성 설정" 확인란을 사용하도록 설정합니다.
 - c. 끝점 유형을 선택합니다.
 - d. 전역 사용자 특성에 적용되는 계정 특성을 선택합니다.

- e. 선택적으로 "하위 문자열" 필드를 작성합니다.

"하위 문자열 시작" 필드가 비어 있으면 문자열의 시작 부분에서 처리가 시작됩니다. "하위 문자열 끝" 필드가 비어 있으면 문자열의 끝 부분에서 처리가 시작됩니다.

5. "확인"을 클릭합니다.
6. "제출"을 클릭합니다.

참고: 이전에 탐색했다라도 상관 관계 규칙을 변경할 때마다 항상 끝점을 탐색해야 합니다.

상관 관계 규칙의 예

다음 예에서는 Active Directory 끝점에 대한 샘플 설정을 제공합니다.

```
GlobalUserName
FullName=LDAP Namespace:globalFullName
FullName=ActiveDirectory:DisplayName
CustomField01=ActiveDirectory:Telephone
```

다음 동작은 Active Directory 컨테이너에 있는 계정의 상관 관계를 지정하는 동안에 발견된 이전에 상관 관계가 지정되지 않은 계정 각각에 대해 발생합니다.

1. 프로비저닝 서버가 첫 번째 매개 변수 값(GlobalUserName)을 Active Directory 끝점 계정 특성(NT_AccountID)과 비교합니다. 서버는 이름이 해당 계정에 대한 NT_AccountID 특성 값과 일치하는 고유한 전역 사용자를 찾으려고 시도합니다. 고유한 일치 항목이 발견되면 프로비저닝 서버가 계정을 전역 사용자에게 연결합니다. 둘 이상의 일치 항목이 발견되면 프로비저닝 서버가 5 단계를 수행합니다. 일치 항목이 발견되지 않으면 프로비저닝 서버가 다음 단계를 수행합니다.
2. 프로비저닝 서버가 두 번째 매개 변수 값(FullName=LDAP Namespace:globalFullName)을 고려합니다. 이 값은 다른 끝점 유형에 고유하게 적용되므로 건너뛰게 되며 프로비저닝 서버가 다음 단계를 수행합니다.

3. 프로비저닝 서버가 세 번째 매개 변수
값(FullName=ActiveDirectory:DisplayName)을 고려합니다. Active Directory 에 고유하게 적용되므로 이 값이 사용됩니다. 서버는 FullName 이 해당 계정에 대한 DisplayName 특성 값과 일치하는 고유한 전역 사용자를 찾으려고 시도합니다. 고유한 일치 항목이 발견되면 프로비저닝 서버가 계정을 전역 사용자에게 연결합니다. 둘 이상의 일치 항목이 발견되면 프로비저닝 서버가 5 단계를 수행합니다. 일치 항목이 발견되지 않으면 프로비저닝 서버가 4 단계를 수행합니다.
4. 프로비저닝 서버가 최종 매개 변수
값(CustomField01=ActiveDirectory:Telephone)을 고려합니다. 이 값은 Active Directory 에 고유하게 적용되므로 이 값이 사용됩니다. 서버는 사용자 지정 필드 #01 특성이 해당 계정에 대한 Telephone 특성 값과 같은 고유한 전역 사용자를 찾으려고 시도합니다. 시스템 태스크의 전역 속성을 사용하여 사용자 지정 전역 사용자 특성에 부여한 이름은 여기에 표시되지 않습니다. 고유한 일치 항목이 발견되면 프로비저닝 서버가 계정을 전역 사용자에게 연결합니다. 둘 이상의 일치 항목이 발견되면 프로비저닝 서버가 5 단계를 수행합니다. 일치 항목이 발견되지 않으면 프로비저닝 서버가 다음 단계를 수행합니다.
5. 프로비저닝 서버가 계정을 [기본 사용자] 개체에 연결합니다. [기본 사용자] 개체가 존재하지 않으면 서버가 자동으로 이 개체를 생성합니다.

환경에 끝점 추가

끝점을 관리하려는 환경에 해당 끝점을 추가합니다. "끝점 만들기" 태스크가 있는 관리자가 이 절차를 수행할 수 있습니다.

다음 단계를 수행하십시오.

1. "끝점", "끝점 관리", "끝점 만들기"를 선택합니다.
2. 끝점 유형을 선택합니다.
3. 탭을 완료하여 필드를 채웁니다.

필수 필드는 빨간색 원으로 시작합니다.

참고: 끝점 이름에 # 기호를 사용하지 마십시오. 이 문자는 검색되지 않습니다.

4. "제출"을 클릭합니다.

이제 해당 계정을 관리할 수 있도록 [탐색 및 상관 관계 지정 정의](#) (페이지 185)를 만들 준비가 되었습니다.

탐색 및 상관 관계 지정 정의 만들기

끝점에 존재하는 사용자를 추가하려면 해당 끝점에 대한 탐색 및 상관 관계 지정 정의를 만듭니다. "탐색 및 상관 관계 지정 정의 만들기" 태스크가 있는 관리자가 정의를 만들 수 있습니다.

다음 단계를 수행하십시오.

1. 환경에서 "끝점", "탐색 및 상관 관계 지정 정의", "탐색 및 상관 관계 지정 정의 만들기"를 차례로 클릭합니다.
2. "확인"을 클릭하여 새 정의를 시작합니다.
3. 의미 있는 이름으로 탐색 및 상관 관계 지정 이름을 채웁니다.
4. "컨테이너/끝점/탐색 방법 선택"을 클릭하여 끝점을 선택하고 컨테이너가 존재하는 경우 컨테이너도 선택합니다. 큰 끝점의 경우 컨테이너 검색에 시간이 걸릴 수도 있으므로 검색 필터를 사용하여 검색 범위를 좁힐 수 있습니다.
5. 컨테이너에 대한 탐색 방법을 클릭합니다. 탐색 및 상관 관계 지정 프로세스는 선택한 컨테이너와 하위 컨테이너를 포함합니다. 디렉터리 컨테이너의 경우에는 하위 트리의 모든 컨테이너를 포함합니다.

6. "동작 탐색/상관 관계 지정"을 클릭하여 다음 작업을 수행합니다.

- **관리 개체에 대한 디렉터리 탐색** - 끝점에 저장되고 프로비저닝 디렉터리에는 저장되지 않은 개체를 찾습니다.
- **계정과 사용자의 상관 관계 지정** - 탐색 기능에서 검색된 개체와 프로비저닝 디렉터리에 있는 사용자의 상관 관계를 지정합니다. 상관 관계에는 다음 두 가지 옵션이 있습니다.

- **기존 사용자 사용**

각 계정을 이전에 만든 사용자와 일치시키는 [상관 관계 규칙](#) (페이지 181)을 사용하려면 이 옵션을 선택합니다.

사용자가 검색되면 계정과 해당 사용자 간의 상관 관계가 지정됩니다. 여러 사용자가 검색되면 계정과 기본 사용자 간의 상관 관계가 지정됩니다. 사용자를 찾지 못하면 이 옵션은 사용자를 만들고(모든 필수 특성이 알려진 경우) 계정과 해당 사용자 간의 상관 관계를 지정합니다. 그렇지 않으면 계정과 기본 사용자 간의 상관 관계를 지정합니다.

- **필요할 때 사용자 만들기**

기본 끝점에서 계정의 상관 관계를 지정하려면 이 옵션을 사용합니다. 이 옵션은 끝점의 계정에 사용자와 동일한 이름이 지정된다고 가정합니다. 이 옵션에는 상관 관계 일치 알고리즘이 사용되지 않습니다. 대신 각 계정이 동일한 이름을 가진 사용자에 연결됩니다. 사용자가 없으면 새로 만들어집니다. 기본 사용자에는 계정이 연결되지 않습니다.

- **사용자 필드 업데이트** - 개체 필드와 사용자 필드 간에 매핑이 존재하면 사용자 필드가 개체 필드의 데이터로 업데이트됩니다.

전체 이름, 주소 및 전화 번호 같은 선택적 특성이 없이 사용자가 만들어집니다. 끝점을 처음 획득하는 동안 이 옵션을 사용하여 계정 특성 값으로 이러한 사용자 특성을 설정하십시오. 이후의 탐색 및 상관 관계 지정 중에 이 옵션을 사용하여 사용자 특성을 새로 고쳐 CA Identity Manager 이외의 도구에 의한 계정 특성 변경 내용을 적용합니다.

7. "제출"을 클릭합니다.

이제 [탐색 및 상관 관계 지정 실행](#) (페이지 187) 태스크가 있는 관리자가 끝점 통합을 완료합니다.

끝점 탐색 및 상관 관계 지정

호스팅 관리자나 탐색 및 상관 관계 지정 실행 태스크가 있는 다른 관리자가 이 절차를 수행합니다. 태스크의 탐색 단계에서는 끝점의 계정을 식별합니다. 상관 관계 지정 단계에서는 계정을 **CA Identity Manager**의 사용자와 일치시키거나 계정을 만듭니다.

다음 단계를 수행하십시오.

1. 환경에서 "끝점", "탐색 및 상관 관계 지정 실행"을 차례로 클릭합니다.
2. 탐색 및 상관 관계 지정을 즉시 실행하려면 "지금 실행"을 선택하고 탐색 및 상관 관계 지정을 나중에 또는 되풀이 일정에 따라 실행하려면 [새 작업 예약](#) (페이지 449)을 선택합니다.

참고: 이 오퍼레이션을 수행하려면 클라이언트 브라우저가 서버와 동일한 시간대에 있어야 합니다. 예를 들어, 서버 시간이 오전 7 시일 때 클라이언트 시간이 화요일 오후 10 시이면 탐색 및 상관 관계 지정 정의가 작동하지 않습니다.

3. 실행할 탐색 및 상관 관계 지정 정의를 클릭합니다.
4. "제출"을 클릭합니다.

끝점에 있는 사용자 계정이 사용자가 만든 탐색 및 상관 관계 지정 정의를 기반으로 **CA Identity Manager**에 생성되거나 업데이트됩니다.

5. 다음과 같이 태스크가 성공적으로 완료되었는지 확인합니다.
 - a. "시스템", "제출한 태스크 보기"를 차례로 클릭합니다.
 - b. 태스크 이름 필드를 "탐색 및 상관 관계 지정 실행"으로 작성합니다.
 - c. "검색"을 클릭합니다.

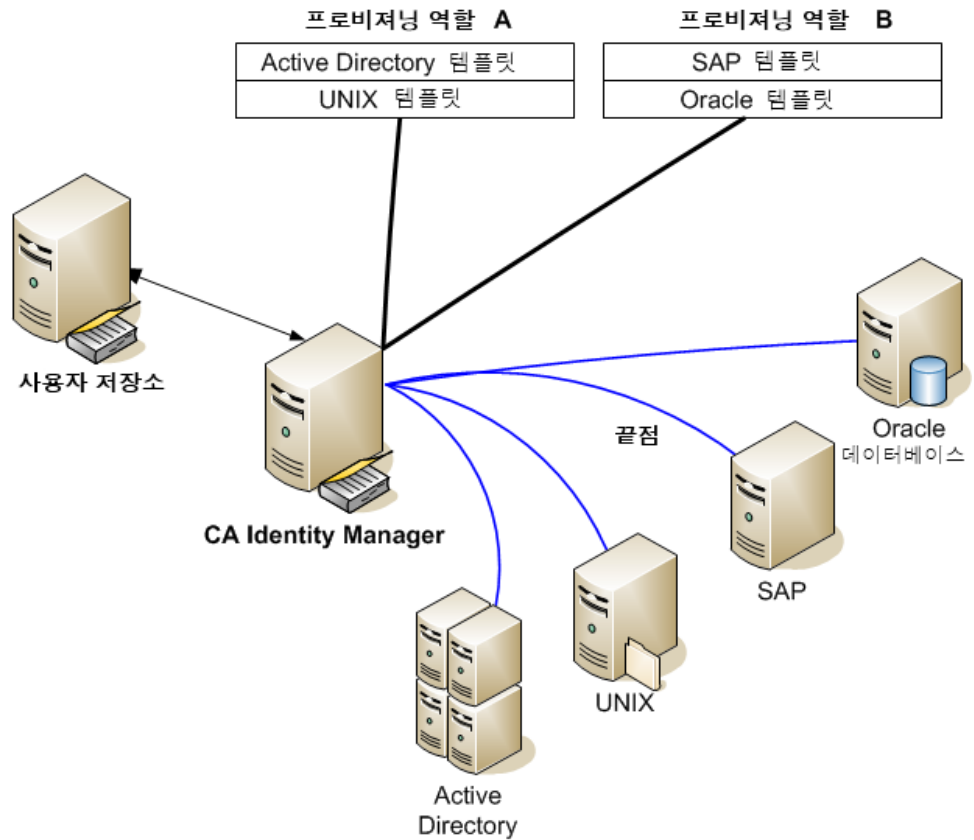
태스크가 성공적으로 완료되었는지 보여 주는 결과가 표시됩니다.

참고: "제출한 태스크 보기"(VST)에서 태스크 상태를 볼 때 "탐색 및 상관 관계 지정" 태스크를 중단할 수 있습니다. 태스크를 중단하면 태스크의 처리가 중단되어 중단할 당시 상태로 태스크가 남아 있게 됩니다. 생성된 알림은 모두 전달되므로 모든 시스템의 동기화가 유지됩니다.

사용자, 계정 및 역할 동기화

여러 끝점과 계정을 단일 사용자 관리 시스템으로 통합하면 동기화가 이루어지지 않을 수 있습니다. 사용자에게 할당된 프로비저닝 역할이나 계정 템플릿이 해당 사용자에 대해 존재하는 실제 계정과 다를 수 있습니다.

예를 들어 두 개의 프로비저닝 역할, 즉 Active Directory 및 UNIX 계정 템플릿이 있는 프로비저닝 역할과 SAP 및 Oracle 템플릿이 있는 프로비저닝 역할이 존재하는 경우를 생각해 봅시다. 사용자 john_smith 에게 Active Directory 및 UNIX 계정 템플릿을 포함하는 프로비저닝 역할 A 가 있지만 해당 사용자가 가지고 있는 계정은 Active Directory 계정뿐입니다. UNIX 계정 템플릿은 사용자에게 할당된 후에 역할에 추가되었을 가능성이 있습니다. 따라서 관리자가 사용자를 현재 역할 정의와 동기화합니다.



다음 상황은 사용자와 프로비저닝 역할이나 계정 템플릿 간의 동기화가 이루어지지 않는 그 밖의 이유입니다.

- 네트워크에서 하드웨어 또는 소프트웨어 문제로 인해 필요한 계정을 만들려는 이전의 시도가 실패하고, 이로 인해 누락된 계정이 발생합니다.
- 프로비저닝 역할 및 계정 템플릿이 변경되고, 이로 인해 불필요하거나 누락된 계정이 발생합니다.
- 계정이 생성된 후 계정 템플릿에 할당되어 계정은 존재하나 계정 템플릿과 동기화되지 않은 계정이 존재합니다.
- 계정이 나중에 생성되도록 지정되었기 때문에 새 계정의 생성이 지연되었습니다.
- 새 끝점이 획득되었습니다. 탐색 및 상관 관계 지정 중에 프로비저닝 서버가 프로비저닝 역할을 사용자에게 자동으로 할당하지 않았습니다. 끝점에서 계정이 필요한 사용자를 나타내도록 역할을 업데이트하십시오. 사용자와의 상관 관계가 지정된 모든 계정은 사용자가 동기화될 때 불필요한 계정으로 나열됩니다.
- 계정을 사용자에게 복사하여 기존 계정이 사용자에게 할당되었습니다.
- 사용자를 역할에 할당하는 방법이 아닌 다른 방법에 의해 사용자에게 대한 계정이 생성되었습니다. 예를 들어 해당 사용자에게 대한 프로비저닝 역할에 없는 계정 템플릿에 사용자를 복사했습니다. 계정은 불필요한 계정으로 나열되거나 불필요한 계정 템플릿이 있는 계정으로 나열됩니다. 기본 계정 템플릿을 사용하여 계정을 만들기 위해 사용자를 끝점에 복사하는 경우 해당 계정은 불필요한 계정이 될 수 있습니다.

다음 섹션에서는 세 가지 유형의 동기화를 수행하는 방법을 설명합니다.

1. [사용자를 역할과 동기화](#) (페이지 190)
2. [사용자를 계정 템플릿과 동기화](#) (페이지 191)
3. [끝점 계정을 계정 템플릿과 동기화](#) (페이지 192)

사용자를 역할과 동기화

이 태스크는 사용자에게 할당된 프로비저닝 역할을 준수하도록 계정을 생성, 업데이트 또는 삭제합니다. 예를 들어 관리자가 끝점의 기본 도구를 사용하여 계정을 추가하거나 삭제하지만 사용자가 해당 끝점을 다시 탐색하여 프로비저닝 디렉터리를 업데이트하지 않았습니까. 따라서 사용자에게 불필요한 계정이나 누락된 계정이 있습니다. 또한 이 태스크를 수행하면 각 계정이 올바른 계정 템플릿에 속하게 됩니다.

다음 단계를 수행하십시오.

1. 사용자 콘솔에 로그인합니다.
2. "태스크", "사용자", "동기화", "역할 동기화 검사"를 차례로 선택합니다.
3. 사용자를 선택합니다.

예상된 계정, 불필요한 계정 및 누락된 계정을 보여 주는 화면이 나타납니다.

4. "동기화"를 클릭하여 계정을 이 역할에 있는 템플릿과 일치하도록 만듭니다.
 - a. 확인란을 선택하여 끝점에 계정을 만들 수 있습니다. 사용자의 여러 계정 템플릿이 동일한 계정을 미리 지정하는 경우 모든 관련 계정 템플릿을 병합하여 계정이 생성됩니다.

이 계정은 이러한 계정 템플릿에 할당되었는데, 이 템플릿은 현재 계정과 동기화되어 있지 않습니다.
 - b. 확인란을 선택하여 불필요한 계정을 삭제할 수 있습니다. 그러나 해당 계정을 가지고 있어야 하는 합당한 이유가 사용자에게 있을 수 있습니다. 이 경우 이 옵션을 선택 해제된 상태로 둡니다.

특정 끝점에서는 계정 삭제 기능이 사용되지 않으므로 계정이 삭제되지 않습니다.

사용자를 계정 템플릿과 동기화

이 태스크는 끝점 계정의 특성을 사용자의 관련 계정 템플릿과 동기화합니다. 그러나 전체 동기화는 다음과 같은 요소에 따라 결정됩니다.

- 계정의 전체 동기화는 두 가지 상황에서 발생합니다. 즉, 계정 템플릿이 [강력한 동기화](#) (페이지 194)를 사용하는 상황이나 둘 이상의 계정 템플릿이 계정에 추가된 상황에서 발생합니다.
- 계정 템플릿이 [약한 동기화](#) (페이지 193)를 사용하는 경우 이 태스크는 이 템플릿만 포함하는 계정 동기화를 시작합니다. 계정이 이 업데이트 이전에 다른 계정 템플릿과 계정 동기화되지 않았으면 그 후에도 여전히 계정이 동기화되지 않을 수 있습니다.

다음 단계를 수행하십시오.

1. 사용자 콘솔에 로그인합니다.
2. "태스크", "사용자", "동기화", "계정 템플릿 동기화 검사"를 차례로 선택합니다.
3. 사용자를 선택합니다.
예상된 계정, 불필요한 계정 및 누락된 계정을 보여 주는 화면이 나타납니다.
4. "동기화"를 클릭하여 계정을 템플릿과 일치하도록 만듭니다.
 - a. 확인란을 선택하여 끝점에 계정을 만들 수 있습니다. 사용자의 여러 계정 템플릿이 동일한 계정을 미리 지정하는 경우 관련 계정 템플릿을 병합하여 계정이 생성됩니다.
이 계정은 해당 계정과 동기화되지 않은 계정 템플릿에 할당됩니다. 새로 생성된 계정에는 계정 동기화가 필요 없습니다.
 - b. 확인란을 선택하여 불필요한 계정을 삭제할 수 있습니다. 그러나 해당 계정을 가지고 있어야 하는 합당한 이유가 사용자에게 있을 수 있습니다. 이 경우 이 옵션을 선택 해제된 상태로 둡니다.
특정 끝점에서는 계정 삭제 기능이 사용되지 않으므로 계정이 삭제되지 않습니다.

새 계정 전용 특성

계정 템플릿에서 일부 특성은 계정을 만들 때만 적용됩니다. 예를 들어, 암호 특성은 새 계정의 암호를 정의하는 규칙 식이며, 이 규칙 식은 계정의 암호를 업데이트하지 않습니다. 암호 규칙 식에 대한 변경 사항은 규칙 식이 설정된 후 생성된 계정에만 적용됩니다.

마찬가지로 읽기 전용 계정 특성에 대한 템플릿 규칙 식은 규칙 식이 설정된 후 생성된 계정에만 적용됩니다. 이러한 식을 변경해도 기존 계정에는 적용되지 않습니다.

끝점 계정을 계정 템플릿과 동기화

이 태스크는 관련 계정 템플릿 수정 후 끝점 계정을 동기화합니다. 예를 들어 **Active Directory** 계정에는 그룹이 없지만 관련 계정 템플릿은 그룹을 포함하도록 정의되어 있을 수 있습니다.

다음 단계를 수행하십시오.

1. 사용자 콘솔에 로그인합니다.
2. "태스크", "끝점", "끝점 관리", "끝점 계정 동기화 검사"를 차례로 선택합니다.
3. 끝점을 선택합니다.

해당 끝점의 계정, 관련 계정 템플릿, 동기화되지 않은 특성 등을 보여주는 화면이 나타납니다.

4. "동기화"를 클릭하여 해당 계정의 특성을 계정 템플릿에 정의된 것과 일치하도록 만듭니다.

계정 템플릿의 변경 내용은 다음과 같이 기존 계정에 영향을 줍니다.

- 기능 특성 값을 변경하면 해당 계정 특성이 업데이트되어 계정 템플릿 특성 값과 동기화됩니다. 약한 동기화와 강력한 동기화에 대한 설명을 참조하십시오.
- 특정 계정 특성은 계정 템플릿 변경 사항에서 업데이트되지 않으므로 커넥터에 의해 지정됩니다. 예를 들면 계정을 만드는 동안 끝점 유형만 설정할 수 있도록 허용하는 특정 특성, 암호 특성 등입니다.

업데이트된 특성

계정 템플릿에서 기능 특성을 변경할 때 계정의 해당 특성이 변경됩니다. 이 변경은 계정의 특성에 영향을 줍니다. 이 영향은 다음과 같은 요인에 기초합니다.

- 계정 템플릿이 약한 동기화 또는 강력한 동기화를 사용하도록 정의되었는지 여부
- 계정이 여러 계정 템플릿에 속하는지 여부

약한 동기화

*약한 동기화*를 사용하면 사용자의 계정이 최소 기능 특성을 가지게 됩니다. 약한 동기화는 대부분의 끝점 유형에서 기본값입니다. 약한 동기화를 사용하는 템플릿을 업데이트하는 경우 **CA Identity Manager** 는 다음과 같이 기능 특성을 업데이트합니다.

- 숫자 필드가 계정 템플릿에서 업데이트되고 새 숫자가 계정의 숫자보다 크면 **CA Identity Manager** 에서 계정의 값을 변경하여 새 숫자와 일치시킵니다.
- 계정 템플릿에서 확인란을 선택하지 않았는데 이후에 이 확인란을 선택하면 **CA Identity Manager** 에서 이 확인란이 선택되지 않은 계정의 확인란을 업데이트합니다.
- 목록이 계정 템플릿에서 변경되면 **CA Identity Manager** 에서 모든 계정을 업데이트하여 계정의 값 목록에 포함되지 않은 새 목록의 값을 포함합니다.

계정이 다른 계정 템플릿에 속하면(해당 템플릿에서 약한 동기화를 사용하든지 강력한 동기화를 사용하든지) **CA Identity Manager** 에서는 변경 중인 템플릿만 참조합니다. 이 동작은 모든 계정 템플릿을 검사하는 것보다 효율적입니다. 약한 동기화는 기능을 계정에만 추가하므로, 일반적으로 다른 계정 템플릿을 참조할 필요가 없습니다.

참고: 약한 동기화 계정 템플릿에서 전파할 때 기능을 제거하거나 낮추는 변경 사항은 일부 계정을 동기화하지 않은 상태로 둘 수 있습니다. 약한 동기화를 사용할 경우 기능은 제거되거나 낮춰지지 않습니다. 계정에 대한 다른 템플릿을 참조할 경우 약한 동기화로 충분하면 전파는 고려되지 않습니다.

이 경우 "사용자를 계정 템플릿과 동기화"를 사용하여 계정을 해당 계정 템플릿과 동기화합니다.

강한 동기화

강한 동기화는 계정 템플릿에 정의된 대로 계정에 정확한 계정 특성이 있는지 확인합니다.

예를 들어, 기존 UNIX 계정 템플릿에 그룹을 추가한다고 가정합니다. 원래 계정 템플릿은 **Staff** 그룹의 계정 구성원을 만들었습니다. 이제, **Staff** 및 **System** 그룹 모두의 계정 구성원을 만들려고 합니다. 각 계정이 **Staff** 및 **System** 그룹의 구성원(그리고 다른 그룹의 구성원이 아님)일 때 계정 템플릿과 관련된 모든 계정이 동기화되었다고 간주됩니다. **Staff** 그룹에 없는 모든 계정은 두 그룹 모두에 추가됩니다.

고려해야 할 일부 다른 요인은 다음 상황을 포함합니다.

- 계정 템플릿이 강한 동기화를 사용하는 경우, **Staff** 및 **System** 을 제외하고 그룹에 속하는 모든 계정이 이러한 추가 그룹에서 제거됩니다.
- 계정 템플릿이 약한 동기화를 사용하는 경우, 계정이 **Staff** 및 **System** 그룹에 추가됩니다. 정의된 추가 그룹이 있는 모든 계정은 이러한 그룹의 구성원으로 남아 있습니다.

참고: 계정이 계정 템플릿과 동기화 상태를 유지할 수 있도록 템플릿과 계정을 정기적으로 동기화하십시오.

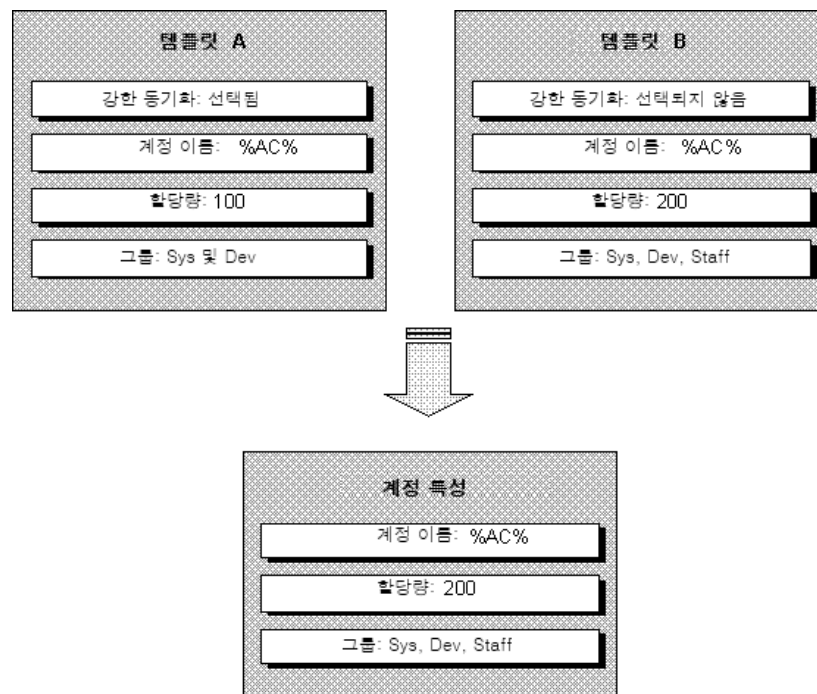
여러 템플릿이 있는 계정

동기화는 계정이 여러 계정 템플릿에 속하는지 여부에 영향을 받습니다. 계정에 단 하나의 계정 템플릿만 있고, 이 템플릿이 강한 동기화를 사용한다면 각 특성은 계정 템플릿 특성 값이 평가하는 것과 동일하게 일치하도록 업데이트됩니다. 결과는 특성이 초기 특성인 경우와 동일합니다.

사용자가 여러 프로비저닝 역할에 속하고, 각 역할이 동일한 관리 끝점에 대한 일부 액세스 수준을 규정하는 경우와 같이, 계정은 여러 계정 템플릿에 속할 수 있습니다. 이 경우, **CA Identity Manager** 는 개별 계정 템플릿의 하위 기능 집합을 규정하는 하나의 유효한 계정 템플릿으로 이러한 계정 템플릿을 결합합니다. 이 계정 템플릿은 개별 계정 템플릿이 약하거나 강한 동기화이거나 개별 계정 템플릿 중 하나가 강한 동기화인 경우 약한 동기화를 사용한다고 간주됩니다.

참고: 회사의 역할이 사용자가 필요로 하는 액세스를 완전히 정의하는지 여부에 따라 하나의 계정을 제어하는 계정 템플릿에 대해 약한 동기화만 사용하거나 강한 동기화만 사용하는 것이 일반적입니다. 사용자에게 적합한 역할이 명확하지 않고 사용자의 계정에 추가 기능을 부여하는 융통성이 필요한 경우 약한 동기화를 사용하십시오. 사용자가 필요로 하는 액세스를 정확히 지정하여 정의할 수 있으면 강한 동기화를 사용하십시오.

다음 예제는 여러 계정 템플릿이 하나의 유효한 계정 템플릿으로 통합되는 방법을 설명합니다. 이 예제에서 하나의 계정 템플릿이 약한 동기화로 표시되었고 다른 하나는 강한 동기화로 표시되었습니다. 따라서, 두 계정 템플릿을 결합하여 생성된 유효한 계정 템플릿은 강한 동기화 계정 템플릿처럼 처리됩니다. 정수 **Quota** 특성은 두 개의 계정 템플릿에서 더 큰 값을 취하고, 다중 값 **Groups** 특성은 두 정책 값의 합집합을 취합니다.



끝점 계정과 리버스 동기화

계정을 만들고 삭제하거나 수정하는 것은 CA CA Identity Manager 의 책임이지만 끝점 시스템 사용자가 이러한 작업을 직접 수행하는 것을 막을 수는 없습니다. 이러한 상황은 긴급하거나 또는 해커와 같은 악의적인 이유로 인해 발생할 수 있습니다. 리버스 동기화는 CA Identity Manager 계정과 끝점의 계정 간 차이를 식별하여 사용자가 각 끝점에 가지고 있는 계정을 제어할 수 있도록 보장합니다.

예를 들어, 계정이 Active Directory 도메인에서 외부 도구를 사용하여 만들어진 경우 CA CA Identity Manager 는 이 잠재적인 보안 문제를 인식해야 합니다. 또한 CA CA Identity Manager 를 바이패스하면 승인 프로세스를 거치지 않고 감사 보고서를 받지 않게 됩니다.

CA CA Identity Manager 와 관리 끝점 간의 두 가지 유형의 차이는 다음과 같습니다.

- 감지된 새 계정
- 기존 계정 내 변경 사항

변경 사항을 처리하기 위한 정책을 정의하여 두 가지 경우를 모두 처리할 수 있습니다. 그런 다음, CA CA Identity Manager 를 업데이트하기 위한 탐색 및 상관 관계 지정을 사용하여 정책의 실행을 트리거하십시오.

리버스 동기화의 작동 방식

끝점 계정과의 리버스 동기화는 다음과 같이 발생합니다.

1. 관리자 또는 악의적인 사용자가 끝점에 계정을 만들거나 수정합니다.
2. 해당 끝점에서 "탐색 및 상관 관계 지정"이 실행될 때 새 계정 또는 수정된 계정이 감지됩니다.
3. 프로비저닝 서버가 CA Identity Manager 서버에 알림을 보냅니다.
4. CA Identity Manager 서버가 끝점의 변경 사항과 일치하는 리버스 동기화 정책을 검색합니다.
5. 일치하는 정책이 발견되면 해당 정책을 실행합니다. 두 개 이상의 정책이 이 계정에 적용되고 이 정책의 범위가 같으면 우선 순위가 가장 높은 정책이 실행됩니다.
6. 정책에 따라 다음과 같은 동작이 발생합니다.
 - 새 계정의 경우 정책이 계정을 승인하거나 삭제 또는 일시 중지하거나 워크플로 승인을 위해 보냅니다.
 - 수정된 계정의 경우 정책이 값을 승인하거나 마지막 알려진 값으로 복원하거나 워크플로 승인을 위해 보냅니다.
7. 워크플로가 선택되면 워크플로에 대해 새 이벤트가 생성되고 승인자가 설정됩니다. 그런 다음, 다음 동작 중 하나가 발생합니다.
 - 새 계정의 경우 승인자가 계정을 승인하거나 삭제 또는 일시 중지하거나 사용자에게 할당합니다.
 - 수정된 계정의 경우 워크플로 프로세스는 거부된 값이 끝점에서 복원된다는 점을 제외하고 사용자 콘솔에서 값이 변경되는 경우와 같습니다.

끝점 특성 매핑

끝점 계정의 특성에 대해 리버스 동기화를 사용하려면 먼저 사용자 콘솔에 표시된 특성에 매핑해야 합니다. 계정 이름 및 암호와 같은 일부 특성은 기본적으로 매핑되어 있습니다. 다른 특성은 매핑되어 있지 않습니다. 예를 들어, Active Directory 특성 그룹 구성원 자격은 매핑되어 있지 않습니다. 일부 끝점 유형의 경우 특성이 매핑되지 않습니다.

특성이 매핑되는지 확인하려면

1. 사용자 콘솔에서 "끝점"을 클릭하거나 "태스크", "끝점"을 클릭합니다.
2. "리버스 수정", "리버스 동기화 수정된 계정 정책 만들기"를 클릭합니다.
3. 새 정책이나 정책 사본을 만듭니다.
4. "끝점 유형"을 클릭하고 **Active Directory** 와 같은 끝점을 선택합니다.
5. "특성 이름"을 클릭하여 매핑될 수 있는 특성의 목록을 표시합니다.
6. "취소"를 클릭합니다.

매핑할 수 있는 특성을 확인하는 용도로만 사용하는 것이므로 정책을 취소합니다.

중요! 끝점에서 네이티브 도구를 사용해서만 특정 특성을 관리할 수 있습니다. 따라서 끝점 사용자가 이 특성 유형을 수정하면 리버스 동기화 정책이 트리거될 경우 리버스 이벤트가 실패합니다. 하지만 해당 리버스 이벤트의 다른 특성에 대한 변경 내용은 리버스되지 않습니다. 따라서 해당 끝점에만 매핑될 수 있는 특성은 매핑하지 마십시오.

리버스 동기화를 위해 끝점 특성을 매핑하려면

1. "끝점", "끝점 수정"을 클릭합니다.
2. 리버스 동기화가 필요한 끝점을 검색하여 선택합니다.
3. "특성 매핑" 탭을 클릭합니다.
4. "사용자 지정 설정 사용"을 선택합니다.
5. 새 사용자 지정 특성을 추가하려면 "추가"를 클릭합니다.
6. 사용 가능한 사용자 지정 특성을 선택합니다. 예를 들어, 환경에서 사용되지 않는 경우 **CustomField 10** 을 사용하십시오.
7. 사용자 지정 특성을 관리할 계정 특성 이름에 매핑합니다.
8. 요구되는 모든 계정 특성과 선택된 사용자 지정 특성 간에 매핑을 추가하려면 5 - 7 단계를 반복합니다.

관리할 모든 특성에 대해 동일한 사용자 지정 특성(이 예제의 경우 **CustomField 10**)을 사용할 수 있습니다.

9. "제출"을 클릭합니다.

이 끝점에 대한 기본 값을 만들려면

끝점에 대한 모든 값이 매핑되면 끝점을 탐색할 수 있습니다. 이 오퍼레이션을 위해 인바운드 알림을 비활성화하고 탐색이 끝나면 다시 활성화합니다. 알림을 비활성화하면 불필요한 알림이 제거됩니다. 그렇지 않으면 새 특성에 대한 값을 가지고 있는 모든 계정이 탐색 오퍼레이션 중 알림을 생성합니다.

1. 프로비저닝 관리자에서 다음과 같이 인바운드 알림을 비활성화합니다.
 - a. "시스템", "도메인 구성", "CA Identity Manager 서버", "알림 사용"을 클릭합니다.
 - b. "아니요"를 선택합니다.
 - c. 프로비저닝 서버를 다시 시작하여 변경 사항을 적용합니다.
2. 사용자 콘솔에서 "끝점", "탐색 및 상관 관계 지정 실행"을 클릭합니다.
상관 관계가 선택 해제된 탐색 및 상관 관계 지정 정의를 선택합니다.
이 동작은 새 끝점 특성 데이터를 사용하여 사용자 저장소 특성을 다시 채웁니다. 끝점이 크면 이 태스크에 시간이 걸릴 수 있습니다.
3. 프로비저닝 관리자에서 인바운드 알림을 다시 활성화합니다.
4. 프로비저닝 서버를 다시 시작합니다.

해당 끝점에 대한 다음 탐색 및 상관 관계 지정 오퍼레이션 시 계정 수정 알림이 생성됩니다. 전역 사용자 특성에 매핑되는 특성이 변경되고 해당 특성에 정책이 적용되면 알림이 생성됩니다.

추가 정보:

[기능 및 초기 특성](#) (페이지 230)

리버스 동기화 정책

끝점에서 계정이 만들어지거나 수정되면 리버스 동기화 정책이 그에 대한 응답으로 적절한 동작을 취할 수 있습니다. 예를 들어, 한 사용자가 회사 도메인의 여러 OU에 몇 개의 **Active Directory** 계정을 만듭니다. 또한 이 사용자가 일부 **Microsoft Exchange** 계정을 수정합니다. 새로운 계정과 변경된 계정을 감지하고 이에 대한 응답으로 리버스 동기화 계정 정책을 사용하여 적절한 동작을 제공할 수 있습니다.

리버스 동기화를 사용하여 다음 작업을 수행할 수 있습니다.

- 새 계정을 승인 또는 거부하거나 워크플로 승인을 위해 보내기 위한 정책을 구성합니다.
- 특성의 변경 사항을 승인하거나 원래 특성으로 복원하거나 워크플로 승인을 위해 보내기 위한 정책을 구성합니다.
- 계정을 워크플로 승인을 위해 보내는 경우 승인자는 다음 작업 중 하나를 수행할 수 있습니다.
 - 계정을 거부(계정을 끝점에서 삭제/일시 중지하거나 값을 **CA Identity Manager** 사용자 저장소 값과 일치하도록 변경)
 - 계정을 승인하고 **CA Identity Manager** 사용자 저장소를 계정과 일치하도록 업데이트
 - 계정을 사용자 콘솔의 사용자에게 할당(계정 생성의 경우)

새 계정을 위한 정책 만들기

끝점에서 새 계정이 감지된 경우에 대한 프로세스를 정의하려면 새 계정에 적용되는 계정 정책을 만드십시오. 새 계정 정책은 탐색 및 상관 관계 지정 정의에 "상관 관계 지정" 옵션이 포함된 경우 계정이 감지되면 실행됩니다. 탐색만을 실행할 때 계정이 감지되면 다음에 끝점을 검색할 때 "상관 관계 지정" 옵션이 포함된 경우 정책이 실행됩니다.

새 계정을 위한 정책을 만들려면

1. 사용자 콘솔에서 "끝점"을 클릭하거나 "태스크", "끝점"을 클릭합니다.
2. "리버스 신규", "리버스 동기화 새 계정 정책 만들기"를 클릭합니다.
3. 정책의 이름과 설명을 입력합니다.
4. 다음 매개 변수를 입력합니다.
 - 우선 순위 - 정책의 우선 순위입니다. 숫자가 가장 낮은 정책이 우선 순위가 가장 높은 정책입니다. 두 정책의 우선 순위와 범위가 같은 경우 두 가지 정책 중 하나가 실행될 수 있습니다. 따라서 서로 다른 우선 순위 수준을 설정하십시오.
 - 끝점 유형 - 모든 끝점 또는 특정 끝점 유형입니다.
 - 끝점 - 특정 끝점 이름입니다. 끝점 유형이 "모두"인 경우 모든 끝점만 선택할 수 있습니다.
 - 컨테이너 - 계정이 위치한 컨테이너입니다. 이 필드는 계층적 끝점에만 적용됩니다. 컨테이너를 끝점으로 끝나는 노드 목록으로 입력하십시오. 예를 들어, 경로가 "ou=자식,ou=부모,ou=루트,dc=도메인,dc=이름"인 AD OU의 경우 "자식,부모,루트"가 올바른 형식입니다.
 - 상관 관계가 지정된 사용자 - 프로비저닝 디렉터리에서 상관 관계가 지정된 사용자가 감지되었는지 여부를 기반으로 정책을 실행할 시기를 제어합니다.

5. 다음 동작 중 하나를 선택합니다.

- 승인 - 계정에 대해 어떤 동작도 수행하지 않습니다. 이 선택 사항은 모든 새 계정을 거부하는 정책과 특정 OU에서 만들어진 계정을 승인하는 우선 순위가 더 높은 정책 등 두 가지 정책이 존재하는 경우 유용합니다. 따라서 계정이 해당 OU에서 만들어지면 승인됩니다. 거부 정책은 우선 순위가 더 낮기 때문에 실행되지 않습니다.
- 삭제 - 계정을 끝점에서 제거합니다.
- 일시 중지 - 계정을 끝점에 남겨두지만 일시 중지합니다.
- 승인을 위해 보내기 - 워크플로 승인을 위해 변경 사항을 제출합니다.

6. 동작을 "승인을 위해 보내기"로 설정하려면 다음 단계를 수행하십시오.

- a. "워크플로 프로세스" 옆의 아이콘을 클릭합니다.
- b. 워크플로 프로세스를 선택합니다.
- c. "확인"을 클릭합니다.

7. "제출"을 클릭합니다.

워크플로 프로세스를 정책에 할당한 경우 [승인 태스크를 만들어야](#) (페이지 204) 합니다.

수정된 계정을 위한 정책 만들기

끝점 계정의 모든 계정 특성은 [특성 매핑에 정의](#) (페이지 197)되는 한 "리버스 동기화"를 통해 관리할 수 있습니다.

기존 끝점 계정과 CA Identity Manager 에서 알려진 계정 값 사이에 차이가 발견된 경우에 대한 프로세스를 정의하기 위해 기존 계정에 적용되는 계정 정책을 만들 수 있습니다. 다중값 특성의 경우 하나 이상의 값이 추가되거나 제거되었을 수 있습니다. 이 경우, 정책이 각 값에 별도로 적용되거나 서로 다른 값에 대해 서로 다른 정책을 만들 수 있습니다.

수정된 계정을 위한 정책을 만들려면

1. 사용자 콘솔에서 "끝점"을 클릭하거나 "태스크", "끝점"을 클릭합니다.
2. "리버스 수정", "리버스 동기화 수정된 계정 정책 만들기"를 클릭합니다.
3. 정책의 이름과 설명을 입력합니다.
4. 다음 매개 변수를 입력합니다.
 - 우선 순위 - 정책의 우선 순위입니다. 숫자가 가장 낮은 정책이 우선 순위가 가장 높은 정책입니다. 두 정책의 우선 순위와 범위가 같은 경우 두 가지 정책 중 하나가 실행될 수 있습니다. 따라서 서로 다른 우선 순위 수준을 설정하십시오.
 - 끝점 유형 - 모든 끝점 또는 특정 끝점 유형입니다.
 - 끝점 - 특정 끝점 이름입니다. 끝점 유형이 "모두"인 경우 모든 끝점만 선택할 수 있습니다.
 - 컨테이너 - 계정이 위치한 컨테이너입니다. 이 필드는 계층적 끝점에만 적용됩니다. 컨테이너를 끝점으로 끝나는 노드 목록으로 입력하십시오. 예를 들어, 경로가 "ou=자식,ou=부모,ou=루트,dc=도메인,dc=이름"인 AD OU 의 경우 "자식,부모,루트"가 올바른 형식입니다.
 - 특성 - 물리적 이름입니다.
 - 값 - 값의 문자열 표시로, *(별표)를 와일드카드로 포함할 수 있습니다. 와일드카드는 변경 사항의 임의 값을 참조합니다.

5. 다음 동작 중 하나를 선택합니다.
 - 승인 - CA Identity Manager 사용자 저장소의 계정 값을 끝점 계정의 값과 일치하도록 업데이트합니다.
 - 거부 - 계정 특성의 다른 변경 사항에 영향을 미치지 않고 원래 값을 복원하기 위해 특성을 되돌립니다.
 - 승인을 위해 보내기 - 워크플로 승인을 위해 변경 사항을 제출합니다.
6. 동작을 "승인을 위해 보내기"로 설정하려면 다음 단계를 수행하십시오.
 - a. "워크플로 프로세스" 옆의 아이콘을 클릭합니다.
 - b. 워크플로 프로세스를 선택합니다.
 - c. "확인"을 클릭합니다.
7. "제출"을 클릭합니다.

워크플로 프로세스를 정책에 할당한 경우 [승인 태스크를 만들어야](#) (페이지 204) 합니다.

리버스 동기화를 위한 승인 태스크 만들기

"워크플로에 보내기" 동작이 있는 정책에 대해 리버스 승인 태스크를 만드십시오. 태스크 만들기에 대한 다음 지침을 고려하십시오.

- 새 계정을 승인하는 태스크의 경우 두 가지 선택이 가능합니다.
 - 계정에 대한 일반 승인 화면을 만들 수 있습니다. 태스크의 프로필 화면에는 계정에 대한 일반 정보만 표시됩니다. "리버스 새 계정 승인" 태스크는 다음과 같은 방식으로 작동합니다.
 - 승인자가 새 계정의 상세 정보를 확인해야 하는 경우 해당 화면이 끝점 유형별로 달라야 합니다. 따라서 화면이 있는 승인 태스크는 해당 끝점 유형 관련 정책에 대해서만 사용되어야 합니다. 태스크에는 "리버스 승인" 탭이 포함되어야 합니다.
- 계정 수정을 승인하는 태스크의 경우 승인 화면이 끝점 유형별로 달라야 하며, 따라서 승인자가 변경된 값을 볼 수 있어야 합니다.

리버스 승인 태스크는 계정 변경에 사용되는 승인 태스크와 동일합니다. 특정 끝점 유형에 대한 승인 태스크가 이미 존재하는 경우 해당 태스크를 사용할 수 있습니다. 새 계정에는 추가적인 리버스 승인 탭이 필요합니다. 끝점 유형에 대한 기존 승인 태스크가 존재하지 않으면 다음 절차를 사용하십시오.

리버스 동기화를 위한 승인 태스크를 만들려면

1. 사용자 콘솔에서 "태스크", "역할 및 태스크"를 클릭하거나 "역할 및 태스크"를 클릭합니다.
2. "관리자 태스크", "관리자 태스크 만들기"를 클릭합니다.
3. 끝점에 대한 수정 태스크를 선택합니다.
이름은 "수정"으로 끝나며 끝점 유형의 이름을 나타냅니다. 예: Active Directory 계정 수정
4. "프로필" 탭에서 다음과 같이 변경합니다.
 - 새 태스크의 이름을 변경합니다.
 - 태스크 태그를 변경합니다.
 - 동작을 "이벤트 승인"으로 변경합니다.
5. "탭" 탭에서 다음과 같이 변경합니다.
 - a. 모든 관계 탭을 제거합니다.
 - b. 태스크가 새 계정을 승인해야 하는 경우 "리버스 승인" 탭을 추가합니다. 첫 번째 탭이 되도록 이 탭을 이동합니다.
 - c. 탭에서 필요한 승인 화면을 복사하고 편집합니다.

참고: 승인 태스크에서 일부 계정 화면을 사용할 때 문제가 발생할 수 있습니다. 이 경우 탭에 대한 기본 계정 화면을 수정하여 해당 태스크에서 동작하도록 만드십시오.
6. "제출"을 클릭합니다.
7. 새 계정 승인을 위한 태스크의 경우 승인자가 속한 역할에 태스크를 추가합니다. 역할은 새 계정이 할당될 수 있는 사용자를 검색하기 위해 사용되는 사용자 범위를 정의합니다.

리버스 동기화 실행

리버스 동기화는 탐색 및 상관 관계 지정 실행 태스크를 사용할 때 발생합니다. 이 태스크를 사용하여 끝점의 새 계정 또는 변경된 계정으로 CA Identity Manager 프로비저닝 저장소를 업데이트하십시오.

리버스 동기화를 실행하려면

1. "상관 관계 지정" 옵션을 포함하는 탐색 및 상관 관계 지정 정의를 만듭니다. 상관 관계는 새 계정을 감지하기 위해 필요합니다.
2. "태스크", "끝점", "탐색 및 상관 관계 지정 실행"을 클릭합니다.
3. 새 계정 또는 변경된 계정이 있는 끝점에 적용되는 정의를 선택합니다.

참고: 기존 사용자와 상관 관계가 있는 경우 사용자가 프로비저닝 디렉터리에 존재해야 하며, 그렇지 않은 경우 사용자는 해당 디렉터리의 기본 사용자와 관련됩니다. CA Identity Manager 사용자 저장소는 "탐색 및 상관 관계 지정" 태스크의 범위에 없습니다.

4. "제출"을 클릭합니다.

정책에 워크플로 프로세스가 없으면 계정은 이미 정책에 정의된 대로 처리됩니다.

참고: 리버스 동기화 정책에 의해 감지된 계정에서 여러 특성이 거부되는 경우 모든 동작이 하나의 이벤트에 추가됩니다. 그러나 해당 이벤트가 특성 중 하나에 문제가 있어 실패한 경우에는 어떤 특성도 업데이트되지 않습니다.

워크플로가 정책의 일부이면 리버스 동기화에 의해 생성된 모든 승인이 승인자의 "워크플로", "내 작업 목록 보기" 아래 표시됩니다.

새 계정의 경우 승인자는 다음과 같이 선택할 수 있습니다.

- 승인자는 "삭제" 또는 "일시 중지"를 선택한 다음 "거부"를 클릭하여 끝점의 계정을 일시 중지하거나 삭제할 수 있습니다.
- 그렇지 않으면 승인자는 "승인"을 클릭하여 새 계정을 승인할 수 있습니다.

승인자가 "상관 관계가 지정된 사용자" 필드에서 사용자를 선택하지 않은 경우 계정이 기본 사용자에게 할당됩니다. 승인 태스크에서 "상관 관계가 지정된 사용자" 필드가 채워지면 계정이 이 사용자와 연결됩니다. "상관 관계가 지정된 사용자" 필드에는 사용자를 찾을 수 있는 경우 상관 관계 메커니즘으로 발견된 제안된 사용자가 포함됩니다.

수정된 계정의 경우 승인자는 다음과 같이 선택할 수 있습니다.

- 각 계정에 대해 승인자는 어느 값이 변경되었는지 확인하고 계정 관리 화면에서 변경이 시작된 것처럼 해당 값을 승인 또는 거부할 수 있습니다.
- 승인자는 Active Directory 그룹과 같은 기능 특성의 변경을 별도의 승인 이벤트로 간주합니다.

리버스 동기화가 성공했는지 확인하려면

1. "시스템", "제출한 태스크 보기"로 이동합니다.
2. 태스크 이름 필드를 다음과 같이 작성합니다: 프로비저닝 활동
3. "검색"을 클릭합니다.

리버스 동기화 이벤트가 성공적으로 완료되었는지 여부가 결과에 표시됩니다.

끝점의 사용자 지정 특성 확장

프로비저닝 서버는 사용자 지정 끝점 특성을 관리할 수 있습니다. CA CA Identity Manager 가 프로비저닝 역할과 관련된 사용자 지정 끝점 특성을 읽도록 하려면 추가 단계가 필요합니다.

끝점의 사용자 지정 특성을 확장하려면

1. 커넥터가 CA CA Identity Manager r12.5 이전 버전에서 생성된 경우 구문 분석기 테이블에서 메타데이터를 생성합니다.

Programming Guide for Java Connector Server(Java 커넥터 서버 프로그래밍 안내서)를 참조하십시오.

2. 다음과 같이 Connector Xpress 를 사용합니다.
 - a. 네임스페이스 노드에 메타데이터를 설치합니다.
 - b. 역할 정의 생성기를 사용하여 JAR 파일, 속성 파일, 역할 정의 파일을 생성합니다.

자세한 내용은 *Connector Xpress Guide*(Connector Xpress 안내서)를 참조하십시오.

3. JAR 파일을 이 위치에 복사합니다.
 - (Windows) *app server home/iam_im.ear/user_console.war/WEB-INF/lib*
 - (UNIX) *app server home\iam_im.ear\user_console.war\WEB-INF\lib*

참고: WebSphere 의 경우 JAR 파일을 다음 위치에 복사하십시오.
WebSphere_home/AppServer/profiles/Profile_Name/config/cells/Cell_name/applications/iam_im.ear/user_console.war/WEB-INF
4. 속성 파일을 이 위치에 복사합니다.
 - (Windows) *app server home/iam_im.ear/custom/provisioning/resourceBundles*
 - (UNIX) *app server home\iam_im.ear\custom\provisioning\resourceBundles*

참고: WebSphere 의 경우 속성 파일을 다음 위치에 복사하십시오.
WebSphere_home/AppServer/profiles/Profile_Name/config/cells/cell_name/applications/iam_im.ear\custom\provisioning\resourceBundles
5. 클러스터가 있는 경우 각 노드에 대해 앞의 두 단계를 반복합니다.
6. 응용 프로그램 서버를 다시 시작합니다.
7. 다음과 같이 역할 정의 파일을 가져옵니다.
 - a. 관리 콘솔에서 환경을 선택합니다.
 - b. "역할 및 태스크 설정"을 선택합니다.
 - c. "가져오기"를 클릭합니다.
 - d. 끝점 유형을 선택하고 "마침"을 클릭합니다.

계정 태스크

사용자 콘솔에서 Identity Manager 사용자와 관련된 끝점을 만들고, 수정하고, 보고, 삭제할 수 있습니다. 또한 CA CA Identity Manager 와 관련되지 않은 다른 끝점 계정을 사용자에게 할당할 수도 있습니다.

끝점 계정에는 4 개의 유형이 있습니다.

프로비저닝됨

사용자에게 프로비저닝 역할이 할당될 때 생성된 계정

예외

사용자에게 계정 템플릿이 할당될 때 생성된 계정

고아

끝점 시스템에서 생성되었고 어떠한 CA Identity Manager 사용자와도 관련되지 않은 계정

System

끝점 시스템에서 생성되었고 어떠한 CA Identity Manager 사용자와도 관련되지 않았으며 끝점 시스템을 관리하기 위해 사용하는 계정

끝점 계정 보기 또는 수정

끝점에서 해당 사용자의 계정을 나열하는 "계정" 탭을 포함하여, "사용자 보기" 또는 "내 프로필 수정"과 같은 사용자의 프로필을 보도록 허용하는 태스크입니다.

계정 정보

지금 동작을 수행할 계정 이름을 클릭하십시오.

선택	이름	끝점 유형	끝점	일시 중지됨	잠김
☒	 ken.davis	WindowNT	iamfw	활동적인	잠금 해제

계정 만들기

선택한 계정에 대한 동작

계정 새로 고침 일시 중지 다시 시작 잠금 해제 암호 변경 할당 취소 할당 삭제

각 계정에 대해 Identity Manager 는 계정 이름, 계정이 있는 끝점, 계정의 상태와 같은 정보를 표시합니다. 수정 태스크의 경우 사용자의 암호를 변경하고 계정을 잠그거나 일시 중지하는 추가 옵션이 있습니다.

이 예에서 "계정" 탭은 "검색" 단추를 포함하고 있습니다. 즉, 이 탭은 검색 화면을 사용하여 구성되었습니다. 이 탭을 구성하여 목록 화면, 검색 화면 또는 둘 모두를 사용할 수 있습니다.

- 두 화면이 구성되면 검색 화면이 검색 결과의 필드를 결정합니다.
- 목록 화면만 구성된 경우 이 필드가 검색 결과의 필드를 결정합니다.
- 두 화면 모두 구성되지 않은 경우에는 계정 탭이 정적 목록 표시를 사용합니다. 즉, 이 "계정" 탭은 표시 열에 대해 사용자 지정할 수 없습니다.

"계정" 탭에 제공할 수 있는 다른 옵션에 대한 자세한 내용은 "Configure Accounts"(계정 구성) 탭에 대한 사용자 콘솔 도움말을 참조하십시오.

프로비저닝된 계정 만들기

CA Identity Manager 사용자에게 대한 끝점 계정을 만드는 권장되는 방법은 사용자에게 프로비저닝 역할을 할당하는 것입니다. 이 사용자는 해당 역할에 대한 계정 템플릿에 정의된 특성이 있는 계정을 받습니다. 필요한 경우 Exchange 계정의 사서함 크기와 같은 변경 사항이 끝점 계정을 업데이트합니다.

프로비저닝된 계정을 만들려면

1. 사용자 콘솔에서 "사용자 관리", "사용자 수정"을 선택합니다.
2. 수정할 사용자를 선택합니다.
3. "프로비저닝 역할" 탭을 클릭합니다.
4. "프로비저닝 역할 추가"를 클릭합니다.
5. 역할을 선택합니다.
6. "제출"을 클릭합니다.

예외 계정 만들기

사용자에 대해 "사용자 수정"을 사용할 때 "계정" 탭에서 직접 계정을 만들 수 있습니다. 이 계정은 예외 계정이라고 부릅니다. 하지만 이 계정에는 관련된 프로비저닝 역할이 없으므로 사용자와 역할의 동기화는 이 계정을 업데이트하지 않습니다.

예외 계정을 만들려면

1. 사용자 콘솔에서 "사용자", "사용자 끝점 계정 수정"을 선택합니다.
2. 수정할 사용자를 선택합니다.
3. "만들기"를 클릭합니다.
4. 끝점을 선택합니다.
5. 이 끝점 유형에 대해 컨테이너가 필요한 경우 컨테이너를 선택합니다.
6. 각 탭에 있는 필드를 입력합니다.
7. "제출"을 클릭합니다.

고아 계정 할당

사용자 콘솔에서 고아 계정, 즉 CA Identity Manager 사용자와 관련되지 않은 계정을 관리할 수 있습니다.

고아 계정에 대한 기본 사용자를 만들려면

프로비저닝 디렉터리가 CA Identity Manager 사용자 저장소와 분리된 경우 CA Identity Manager 사용자 저장소에 프로비저닝 서버 기본 사용자를 만듭니다. 고아 계정에는 기본 사용자가 사용됩니다.

1. "사용자 콘솔"에서 "사용자"를 클릭합니다.
2. "사용자 관리", "사용자 만들기"를 클릭합니다.
3. 다음과 같이 대괄호를 포함하여 사용자의 이름을 지정합니다.

[기본 사용자]

이제 고아 계정을 사용자에게 할당할 수 있습니다.

고아 계정을 할당하려면

1. "사용자 콘솔"에서 "끝점"을 클릭합니다.
2. "고아 계정 관리"를 클릭합니다.
3. 사용자를 검색하여 선택합니다.
4. 고아 사용자에게 할당할 사용자를 클릭합니다.

시스템 계정 할당

사용자 콘솔에서 시스템 계정, 즉 끝점 시스템을 관리하는 데 사용되는 끝점 계정을 관리할 수 있습니다.

사용자에게 시스템 계정을 할당하려면 "시스템 계정 관리" 태스크를 기반으로 관리자 태스크를 만듭니다. 새 태스크에는 특정 끝점에 대해 적용되는 특정 **CA Identity Manager** 사용자가 있습니다. 각 끝점 유형에 대해 하나의 태스크를 만들 수 있습니다.

시스템 계정을 할당하기 위한 태스크를 구성하려면

1. 사용자 콘솔에서 "역할 및 태스크", "관리자 태스크", "관리자 태스크 만들기"를 클릭합니다.
2. 새 태스크가 시스템 계정 관리에 기반하도록 합니다.
예를 들어, **Oracle** 끝점 유형의 시스템 계정을 할당하기 위해 **Oracle 시스템 계정 관리**란 이름의 태스크를 만들 수 있습니다.
3. "검색" 탭에서 "찾아보기" 단추를 클릭하여 검색 화면을 편집합니다. 이 화면에서 이 시스템 계정에 할당할 사용자에게 대한 검색 필터를 추가합니다.
4. 태스크를 제출합니다.
5. 역할에 이 태스크를 추가합니다.
6. 끝점에 대한 시스템 계정을 사용자에게 할당해야 할 사용자에게 역할을 할당합니다.

이 역할이 있는 사용자는 새 태스크를 실행하여 시스템 사용자를 **CA Identity Manager** 사용자에게 할당할 수 있습니다.

계정 이동 태스크 화면

이 태스크 화면을 사용하여 끝점의 한 컨테이너에서 다른 컨테이너로 계정을 이동할 수 있습니다. 이 화면의 필드가 아래에 나열되어 있습니다.

계정 이동 상세 정보

이동할 계정, 부모 컨테이너, 대상 컨테이너, 끝점 및 끝점 유형을 지정합니다.

컨테이너 선택 단추

끝점에 속하는 사용 가능한 계정 컨테이너를 검색하려면 클릭하십시오.

끝점 계정 삭제

두 가지 방법으로 끝점 계정을 삭제할 수 있습니다.

1. "프로비저닝 역할" 탭에서 "사용자 수정" 태스크를 사용하여 해당 계정을 만든 역할을 제거합니다.
2. "사용자의 끝점 계정 수정" 태스크를 사용하여 계정을 삭제합니다.

"사용자의 끝점 계정 수정"을 사용하여 계정을 삭제하려면

1. 사용자 콘솔에서 "사용자", "사용자 끝점 계정 수정"을 선택합니다.
2. 수정할 사용자를 선택합니다.
3. 끝점 유형을 기반으로 계정을 검색합니다.
4. 계정을 선택합니다.
5. "삭제" 단추를 클릭합니다.

삭제된 계정은 다음과 같이 프로비저닝 관리자를 사용할 때 다시 만들어집니다.

- "역할을 사용해 사용자 동기화"는 사용자에게 프로비저닝 역할이 있을 때 만들어진 계정인 프로비저닝 계정을 다시 만듭니다.
- "계정 템플릿을 사용해 계정 동기화"는 예외(계정에 계정 템플릿이 있는 경우)와 프로비저닝된 계정을 다시 만듭니다.

끝점 계정에 대한 암호 변경

현재 암호를 알 필요 없이 끝점 계정의 암호를 변경할 수 있습니다.

끝점 계정의 암호를 변경하려면

1. 사용자 콘솔에서 "사용자", "사용자 끝점 계정 수정"을 선택합니다.
2. 수정할 사용자를 선택합니다.
3. 끝점 유형을 기반으로 계정을 검색합니다.
4. 하나 이상의 계정을 선택합니다.
5. "암호 변경" 단추를 클릭합니다.
6. 새 암호를 입력합니다.

CA CA Identity Manager 암호 정책이 새 암호의 유효성을 검사합니다.

7. "제출"을 클릭합니다.

여러 계정에서 동작 수행

하나 이상의 계정에서 여러 다른 동작을 수행할 수 있습니다. 예를 들어, 중지된 계정을 다시 시작하거나, 사용자가 잘못된 암호를 입력하여 잠긴 계정의 잠금을 해제하거나, 사용자에게 계정을 할당/할당 취소할 수 있습니다. 이러한 동작은 선택된 모든 계정에 적용되며 그 절차는 동일합니다.

여러 계정에서 태스크를 수행하려면

1. 사용자 콘솔에서 "사용자", "사용자 끝점 계정 수정"을 선택합니다.
2. 수정할 사용자를 선택합니다.
3. 끝점 유형을 기반으로 계정을 검색합니다.
4. 하나 이상의 계정을 선택합니다.
5. "선택한 계정에 대한 동작" 아래의 아무 단추나 누릅니다.
6. 표시되는 대화 상자에 응답하고 "제출"을 클릭합니다.

고급 계정 오퍼레이션

프로비저닝 매니저에서 계정에 대해 여러 추가 오퍼레이션을 수행할 수 있습니다.

- 계정을 다른 전역 사용자와 연계합니다.
- 자동으로 계정을 탐색합니다.
- 계정을 삭제합니다.
- "삭제 보류"를 사용합니다.
- 삭제된 계정을 재생성합니다.

계정에 대한 전역 사용자 변경

다음과 같은 경우에 계정을 다른 전역 사용자와 연계하면 유용합니다.

- 동일한 이름을 사용하는 두 명의 전역 사용자가 있고, **CA CA Identity Manager**에 의해 계정이 다른 사람과 잘못 연계되었습니다.
- 계정이 **CA CA Identity Manager**에 의해 [기본 사용자] 개체와 상관 관계가 지정되었고, 이제 다른 전역 사용자 개체와 연계하려고 합니다.
- "새로 만들기"를 사용하여 계정을 만들었고, 이제 전역 사용자와 계정을 연계하려고 합니다.

프로비저닝 매니저에서 다른 전역 사용자와 계정을 연계하려면 계정을 올바른 전역 사용자로 끌어 이동하십시오.

자동 탐색이 동작하는 방식

끝점에 대해 네이티브한 도구를 사용하여 계정 또는 다른 개체를 추가 또는 삭제할 때는 끝점을 탐색할 때까지 CA CA Identity Manager 가 이 동작을 인식하지 못합니다. 탐색 프로세스는 발생한 추가 및 삭제(및 일부의 경우 수정)에 대해 알리고 이러한 변경 사항을 프로비저닝 디렉터리에서 CA Identity Manager 가 개체를 표시할 때 적용합니다.

하지만 프로비저닝 매니저를 사용하여 이 탐색이 발생하기 전에 동일한 이름으로 개체를 만들려고 시도하면 CA CA Identity Manager 가 동일한 이름을 사용하는 개체가 이미 있다고 인식하여 이 오류를 보고합니다. CA CA Identity Manager 는 그런 후 해당 개체를 탐색하여 프로비저닝 디렉터리에 이 개체를 표시합니다. 해당 개체에 대한 작업은 즉시 시작할 수 있습니다. 개체가 프로비저닝 디렉터리에 없을 때 "추가", "이동" 또는 "이름 변경" 오퍼레이션이 끝점에서 이미 존재하는 오류를 생성할 때마다 자동 단일 개체 탐색이 발생합니다.

자동 탐색을 *Provisioning Reference Guide*(프로비저닝 참조 안내서)에 설명된 "Synchronization/Automatic Correlation"(동기화/자동 상관 관계 지정) 도메인 구성 매개 변수와 결합할 수 있습니다. 이러한 기능이 함께 동작하면 새 계정을 만들기 위한 시도로서 이러한 기능들은 먼저 계정 템플릿으로부터 계정을 생성하려는 시도를 처리합니다. 그런 다음, 이 프로세스는 다음 단계를 사용합니다.

- 탐색되지 않은 계정을 알립니다.
- 해당 계정을 자동으로 탐색합니다.
- 계정과 전역 사용자 사이에 자동으로 상관 관계를 지정합니다.
- 이 전역 사용자와 상관 관계가 지정된 기존 계정인 경우라도 계정에 계정 템플릿을 추가합니다.

계정을 삭제합니다.

계정을 반드시 삭제해야 하는 경우, 프로비저닝 매니저에서 다음 방법을 사용할 수 있습니다.

- 계정을 마우스 오른쪽 단추로 클릭한 다음 "삭제"를 선택합니다.
- 전역 사용자를 마우스 오른쪽 단추로 클릭한 다음 "Delete User and Accounts"(사용자 및 계정 삭제)를 선택합니다.
- "계정 삭제" 마법사를 실행합니다.
- 전역 사용자를 프로비저닝 역할과 동기화하고 추가 계정을 삭제하도록 지정합니다.

프로비저닝 역할에서 전역 사용자를 제거할 때 프로비저닝 매니저는 계정 삭제를 위한 다음과 같은 선택 사항을 제공합니다.

- 이러한 계정을 삭제하기로 결정하는 경우 **CA Identity Manager** 는 프로비저닝 디렉터리에서 이 계정을 제거합니다.
- 계정을 삭제하지 않기로 결정하는 경우 **"Synchronize User with Roles"**(사용자와 역할 동기화) 옵션을 사용하여 "계정 삭제"를 선택할 수 있습니다.

계정을 삭제하기 전에 프로비저닝 역할에서 전역 사용자를 제거하는 경우 전역 사용자에 대한 계정을 나열할 수 있습니다. 전역 사용자를 마우스 오른쪽 단추로 클릭한 다음 **"List Accounts"**(계정 나열)를 선택하십시오.

- 계정 목록에는 각 계정이 속하는 프로비저닝 역할이 표시됩니다. 계정이 하나의 프로비저닝 역할에 속하는 경우, 역할에서 이 사용자를 제거하고 계정을 삭제하기 위해 사용자 동기화 동작을 승인하면 이 계정이 삭제됩니다.
- 계정이 프로비저닝 역할에 속하지 않는 경우 이 계정은 추가 계정이며 **"Check User Synchronization"**(사용자 동기화 검사)에 의해 보고됩니다. 전역 사용자에 대해 **"Synchronize the User with Roles"**(사용자와 역할 동기화) 메뉴 항목을 선택하는 경우 계정이 삭제됩니다.

"삭제 보유"를 사용합니다.

CA CA Identity Manager 는 끝점별 기준에 따라 구성될 수 있으므로, 일반적으로 계정을 삭제하는 삭제 또는 동기화 동작을 관리자가 실행할 때 끝점에서 계정이 삭제되지 않습니다. 대신, 계정은 CA CA Identity Manager 에서 "삭제 보유" 상태로, 그리고 관리 끝점에서 "일시 중지됨" 상태로 남아 있습니다.

"삭제 보유" 계정은 프로비저닝 매니저에서 계정 속성의 "통계" 탭으로 확인할 수 있습니다. 일시 중지된 계정에는 "삭제 보유"의 일시 중지된 이유와 이 상태가 된 때의 타임스탬프가 있습니다. 저장된 "삭제 보유" 상태 및 "일시 중지됨" 타임스탬프를 이용하면 이러한 삭제 보유 계정을 식별하여 프로비저닝 서버 및 관리 끝점에서 이러한 계정을 나중에 삭제하는 유틸리티를 작성할 수 있습니다.

삭제된 계정 다시 만들기

CA Identity Manager 가 아닌 다른 도구를 사용하여 관리 끝점에서 계정을 삭제하는 경우, 계정이 관리 끝점이 아닌 프로비저닝 디렉터리에 있으므로 "Check Account Synchronization"(계정 동기화 검사) 기능이 해당 계정이 없다고 보고합니다. 이 경우 계정과 관련된 계정 템플릿을 사용하여 계정을 다시 만드는 "Synchronize Account with Account Templates"(계정 템플릿을 사용해 계정 동기화) 기능을 호출하여 끝점에서 계정을 다시 만드십시오.

계정이 다시 만들어지면 CA Identity Manager 가 이 계정을 다시 생성된 계정으로 로깅합니다. 관리자는 기능 특성(예: 암호)이 아닌 다른 특성이 원래 계정 템플릿 값으로 설정되었음을 알아야 하므로 이러한 계정은 업데이트된 계정과 별도로 식별될 수 있습니다.

제 9 장: 프로비저닝 역할

이 섹션은 다음 항목을 포함하고 있습니다.

[프로비저닝 역할 및 계정 템플릿](#) (페이지 219)

[계정을 할당하기 위한 역할 만들기](#) (페이지 220)

[역할 및 템플릿 태스크](#) (페이지 224)

[계정 템플릿의 특성](#) (페이지 229)

[고급 규칙 식](#) (페이지 233)

[프로비저닝 역할 성능](#) (페이지 240)

[기존 환경에 대한 프로비저닝 태스크](#) (페이지 242)

프로비저닝 역할 및 계정 템플릿

계정 관리를 단순화하기 위해 프로비저닝 역할에서 사용되는 계정 템플릿을 사용하여 계정을 만들고 유지 관리하십시오. 프로비저닝 역할은 하나 이상의 계정 템플릿을 포함합니다. 해당 역할을 사용자에게 적용할 때 사용자는 템플릿에 정의된 대로 계정을 수신합니다.

이러한 템플릿은 특정 끝점 유형의 계정에 대한 기준을 제공하고, eTrust Admin 에서 제공된 프로비저닝 정책과 동일한 유형의 기능을 제공합니다.

계정 템플릿을 사용하여 다음 작업을 수행할 수 있습니다.

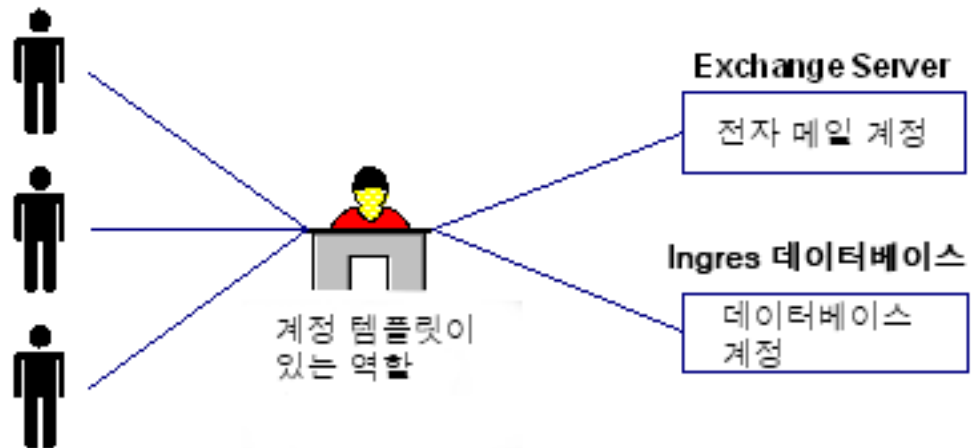
- CA CA Identity Manager 사용자가 계정을 만들 때 끝점에서 가지는 계정 특성을 제어합니다.
- 규칙 문자열 또는 값을 사용하여 특성을 정의합니다.
- 여러 프로비저닝 역할의 계정 특성을 조합하여 전역 사용자가 특정 끝점에 필요한 모든 계정 특성을 가지는 하나의 계정을 가지도록 합니다.
- 전역 사용자가 프로비저닝 역할을 변경할 때 계정 특성을 만들거나 업데이트합니다.
- 전역 사용자가 필요한 특성만 가지도록 계정 특성을 동기화합니다.
- 동기화 오퍼레이션 중 만들거나 업데이트 또는 삭제할 계정을 볼 쿼리를 수행합니다.
- 프로비저닝 역할과 동기화할 수 있는 계정 특성과 동기화할 수 없는 계정 특성을 판별합니다.

계정을 할당하기 위한 역할 만들기

대부분의 조직에서 관리자는 사용자에게 다양한 시스템과 응용 프로그램에 대한 로그인 계정을 제공하느라 상당한 시간을 소비합니다. 이 반복 활동을 간소화하기 위해 프로비저닝 역할, 즉 계정 템플릿을 포함하는 역할을 만들 수 있습니다. 템플릿은 한 가지 유형의 계정에 존재하는 특성을 정의합니다. 예를 들어 Exchange 계정의 계정 템플릿은 사서함 크기와 같은 특성을 정의합니다. 계정 템플릿은 계정에 사용자 특성이 매핑되는 방법도 정의합니다.

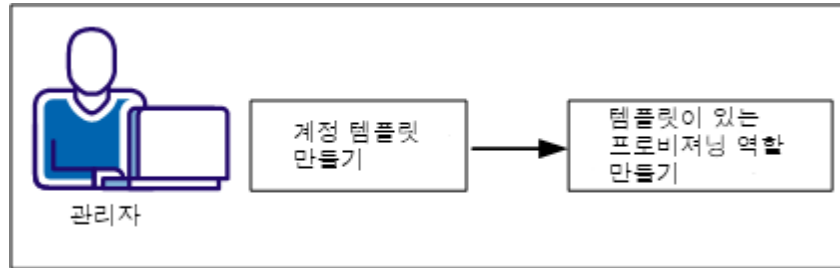
Forward, Inc.의 모든 직원에게 데이터베이스와 전자 메일에 대한 액세스가 필요한 경우를 예로 들어 봅시다. 관리자는 각 직원에 대해 한 번에 하나씩 데이터베이스 계정과 전자 메일 계정을 만드는 작업을 피하고 싶습니다. 따라서 관리자는 해당 회사의 프로비저닝 역할을 만듭니다. 이 역할에는 전자 메일 계정을 제공하기 위한 Microsoft Exchange 서버용 계정 템플릿과 Oracle 데이터베이스용 템플릿이 포함되어 있습니다. 이 예에서 Exchange 서버 및 Oracle 데이터베이스를 '끝점'이라고 부르며, 이는 계정이 존재하는 시스템 또는 응용 프로그램입니다.

참고: Forward, Inc.는 지침 제공의 목적으로만 사용되는 가상의 회사 이름으로, 기존 회사를 가리키지 않습니다.



역할이 만들어지면 매니저 또는 지원 담당자와 같은 비즈니스 관리자가 사용자에게 해당 역할을 할당하여 끝점의 계정을 제공할 수 있습니다. 그런 다음 역할을 받은 사용자가 끝점에 로그인할 수 있습니다.

계정 템플릿을 포함하는 프로비저닝 역할 만들기는 다음과 같이 두 단계로 진행되는 프로세스입니다.



다음 섹션에서는 계정을 할당하는 데 사용할 수 있는 역할을 만드는 방법을 설명합니다.

1. [계정 템플릿 만들기](#) (페이지 222)
2. [프로비저닝 역할 만들기](#) (페이지 223)

계정 템플릿 만들기

계정 관리를 단순화하기 위해 프로비저닝 역할에서 사용되는 계정 템플릿을 사용하여 계정을 만들고 유지 관리하십시오. 프로비저닝 역할은 하나 이상의 계정 템플릿을 포함합니다. 해당 역할을 사용자에게 적용할 때 사용자는 템플릿에 정의된 대로 계정을 수신합니다.

이러한 템플릿은 특정 끝점 유형의 계정에 대한 기준을 제공하고,

계정 템플릿을 사용하여 다음 작업을 수행할 수 있습니다.

- 사용자가 계정을 만들 때 끝점에서 가지는 계정 특성을 제어합니다.
- 규칙 문자열 또는 값을 사용하여 특성을 정의합니다.
- 여러 프로비저닝 역할의 계정 특성을 조합하여 전역 사용자가 특정 끝점에 필요한 모든 계정 특성을 가지는 하나의 계정을 가지도록 합니다.
- 전역 사용자가 프로비저닝 역할을 변경할 때 계정 특성을 만들거나 업데이트합니다.

각 끝점 유형의 기본 계정 템플릿이 **CA Identity Manager** 서버와 함께 설치됩니다. 프로비저닝 역할에서 기본 계정 템플릿을 사용하거나 사용자가 구성한 끝점에 대해 사용자 자신의 계정 템플릿을 만들 수 있습니다.

계정 템플릿을 만들려면

1. 끝점(주로 태스크 아래에 표시됨)으로 이동한 다음 "계정 템플릿", "계정 템플릿 만들기"를 클릭합니다.
2. 템플릿의 끝점 유형을 선택합니다.
3. "끝점 이름"을 끝점 또는 해당되는 경우 **localhost**의 시스템 이름으로 정의합니다.
4. "끝점" 탭에서 사용할 끝점을 선택합니다.
5. 탭의 필드를 입력하거나 기본값을 사용합니다.
각 끝점 유형마다 다른 탭들이 표시됩니다. 필드 정의를 보려면 "도움말"을 클릭하십시오.
6. "제출"을 클릭합니다.

참고: "계정 템플릿"에서 끝점 개체를 검색할 때 둘 이상의 끝점이 지정된 경우 관련 개체의 공통 부분(교집합)이 반환됩니다. "계정 템플릿"에 연결된 각 선택된 끝점에 존재하는 **Active Directory** 그룹을 예로 들 수 있습니다. 검색 결과에 개체 이름이 아닌 특성이 표시되는 경우 첫 번째 끝점에 연결된 개체의 특성 값이 표시됩니다. **PeopleSoft** 커넥터에 있는 언어 개체의 설명 특성을 예로 들 수 있습니다.

프로비저닝 역할 만들기

역할 요구 사항에 대해 결정한 후 프로비저닝 역할을 만듭니다.

- 다른 계정이 필요한 사용자
- 역할과 연결할 계정
- 역할의 구성원, 관리자 및 소유자가 될 사용자

프로비저닝 역할을 만들려면

1. 사용자 콘솔에서 "역할 및 태스크", "프로비저닝 역할", "프로비저닝 역할 만들기"로 이동합니다.

각 탭에 대한 자세한 내용을 보려면 화면에서 도움말 링크를 클릭하십시오.

2. "프로필" 탭을 완료합니다. "이름" 필드만 필수입니다.

참고: "프로필" 탭에서 프로비저닝 역할에 대한 추가 정보를 지정하는 사용자 지정 특성을 지정할 수 있습니다. 이 추가 정보를 사용하여 수많은 역할을 포함하는 환경에서 역할을 쉽게 검색할 수 있습니다.

3. "계정 템플릿" 탭을 완료합니다.

a. "끝점 유형"(예: **ActiveDirectory**)을 클릭합니다.

b. 계정 템플릿을 클릭합니다.

클릭할 수 있는 템플릿은 끝점 유형에 따라 다릅니다.

c. 여러 끝점 유형에 필요한 경우 다른 계정 템플릿을 추가합니다.

4. 이 탭에서 프로비저닝 역할을 중첩시키려면 "프로비저닝 역할" 탭을 완료합니다.

이 단계를 수행하려면 이 환경에 대해 [중첩된 역할](#) (페이지 228)을 사용하도록 설정해야 합니다.

5. 이 역할의 구성원과 관리자를 관리하는 사람을 제어하는 관리자 규칙을 추가하여 "관리자" 탭을 완료합니다.

6. 이 역할을 수정할 수 있는 사람을 제어하는 소유자 규칙을 추가하여 "소유자" 탭을 완료합니다.
7. "제출"을 클릭합니다.
8. 역할이 만들어졌는지 확인하려면 "프로비저닝 역할", "프로비저닝 역할 보기"를 클릭합니다.

역할 및 템플릿 태스크

사용자 콘솔에서 "역할 및 태스크"를 선택하고 "프로비저닝 역할" 아래 태스크를 선택하여 프로비저닝 역할을 만들고 관리할 수 있습니다. 사용자를 역할 구성원으로 만들고 역할을 수정 또는 삭제하는 것과 같은 표준 오퍼레이션에 대한 태스크가 존재합니다.

프로비저닝 역할을 만들기 전에 해당 역할 또는 가져올 프로비저닝 역할에 포함할 계정 템플릿이 필요합니다. 프로비저닝 관리자 또는 eTrust Admin 에서 생성한 역할을 가져올 수 있습니다. 그러나 CA Identity Manager 는 eTrust Admin 에서 생성된 중첩된 역할을 지원하지 않습니다.

프로비저닝 역할 가져오기

사용자 콘솔에서 프로비저닝 역할을 관리하는 경우에도 프로비저닝 관리자나 외부 응용 프로그램에서 일부 프로비저닝 역할이 만들어졌을 수 있습니다. 이러한 프로비저닝 역할의 경우 사용자 콘솔에서 관리할 수 있도록 역할 소유자를 CA Identity Manager 관리자로 다시 설정할 수 있습니다.

프로비저닝 역할을 가져오려면

1. 시스템 매니저 권한을 가진 사용자로 사용자 콘솔에 로그인합니다. "태스크", "역할 및 태스크"를 클릭합니다.
2. "프로비저닝 역할", "프로비저닝 역할 소유자 재설정"을 차례로 선택한 다음 프로비저닝 관리자에서 만들어진 프로비저닝 역할을 선택합니다.
3. 이 역할을 수정할 수 있는 사람을 제어하는 소유자 규칙을 추가하여 "소유자" 탭을 완료합니다.

4. "제출"을 클릭합니다.

이제 "프로비저닝 역할" 범주의 작업을 사용하여 역할을 수정 또는 할당하거나 볼 수 있습니다.

프로비저닝 역할에 대한 새 소유자 할당

하나 이상의 프로비저닝 역할을 선택하고 역할을 수정할 수 있는 사용자를 제어하기 위해 소유자 정책을 할당할 수 있습니다.

프로비저닝 역할에 대한 새 소유자를 할당하려면

1. 시스템 매니저 권한을 가진 사용자로 사용자 콘솔에 로그인합니다.
2. "태스크", "역할" 또는 "역할", "태스크"를 클릭합니다.
3. "프로비저닝 역할", "프로비저닝 역할에 대한 소유자 정책 만들기"를 클릭합니다.
4. 하나 이상의 프로비저닝 역할을 선택합니다.
5. 이 역할을 수정할 수 있는 사람을 제어하는 소유자 규칙을 추가하여 "소유자" 탭을 완료합니다.
6. "제출"을 클릭합니다.

새 소유자 정책을 충족하는 사용자는 선택된 프로비저닝 역할을 수정할 수 있습니다.

프로비저닝 역할에 의해 생성된 계정의 암호

사용자에게 프로비저닝 역할이 할당된 경우 CA Identity Manager 사용자의 암호가 끝점의 암호 요구 사항을 충족시키지 못하면 해당 사용자에 대한 계정 만들기가 실패합니다. 이러한 상황에는 임시 암호를 사용하여 새 사용자를 만드는 경우가 포함됩니다.

따라서 암호 정책을 끝점 암호 요구 사항과 같거나 보다 엄격하게 설정하십시오. CA Identity Manager 암호 정책 또는 프로비저닝 암호 프로필을 사용하여 암호 정책을 설정할 수 있습니다. 두 방법을 모두 사용하는 경우 정책이 일치해야 합니다.

프로비저닝 역할 이벤트 처리 순서

일부 기본 CA Identity Manager 태스크에는 프로비저닝 역할 구성원을 결정하는 *이벤트*, 즉 CA Identity Manager 가 태스크를 완료하기 위해 수행하는 동작이 포함됩니다. 예를 들어 기본 "사용자 수정" 태스크에는 AssignProvisioningRoleEvent 및 RevokeProvisioningRoleEvent 가 포함됩니다. 프로비저닝 역할을 할당하거나 해지하면 끝점에서 계정이 추가되거나 제거될 수 있습니다. 경우에 따라 끝점에서 "동작 제거"를 수행하기 전에 모든 "동작 추가"를 수행해야 할 수도 있습니다.

CA Identity Manager 가 추가 동작을 먼저 처리하도록 하려면 관리 콘솔에서 "프로비저닝 역할 구성원 이벤트 누적" 설정을 사용하십시오. 이 설정을 사용하면 CA Identity Manager 가 모든 추가 및 제거 동작을 AccumulatedProvisioningRolesEvent 라는 단일 이벤트로 누적합니다. 예를 들어 "사용자 수정" 태스크에서 사용자를 세 가지 프로비저닝 역할에 할당하고 두 가지 다른 프로비저닝 역할에서 제거하는 경우 세 개의 추가 동작과 두 개의 제거 동작 등 5 개의 동작을 포함하는 AccumulatedProvisioningRolesEvent 가 생성됩니다.

이 이벤트를 실행할 때 모든 추가 동작은 단일 오퍼레이션으로 결합되어 처리를 위해 프로비저닝 서버로 보내집니다. 추가 동작의 처리가 완료되면 CA Identity Manager 가 제거 동작을 단일 오퍼레이션으로 결합하여 프로비저닝 서버로 보냅니다.

이 설정을 사용하면 다음과 같은 CA Identity Manager 기능에 영향을 미칩니다.

- 사용자 태스크의 프로비저닝 역할 탭

관리자가 "프로비저닝 역할" 탭을 사용하여 프로비저닝 역할에서 사용자를 추가 또는 제거하는 경우 CA Identity Manager 는 해당 동작을 단일 이벤트로 누적합니다.

- ID 정책

ID 정책 평가의 결과로 생성되는 모든 프로비저닝 역할 구성원 이벤트(`AssignProvisioningRoleEvent` 또는 `RevokeProvisioningRoleEvent`)는 단일 `AccumulatedProvisioningRolesEvent` 로 누적됩니다. CA Identity Manager 는 이 이벤트를 다른 보조 이벤트와 같이 실행합니다. 예를 들어, 두 개의 ID 정책 "정책 A"와 "정책 B"를 포함하는 ID 정책 세트가 있다고 가정합니다. 정책 A 는 프로비저닝 역할 A 의 구성원 자격을 해지하며 정책 B 는 사용자를 프로비저닝 역할 B 의 구성원으로 할당합니다. CA Identity Manager 는 사용자가 더 이상 정책 A 를 만족하지 못하지만 정책 B 를 만족한다는 것을 확인한 경우 두 가지 동작(제거를 위한 동작 및 추가를 위한 동작)을 포함하는 `AccumulatedProvisioningRolesEvent` 가 생성됩니다. 추가 동작이 먼저 실행된 다음 제거 동작이 실행됩니다.

- 제출된 태스크 보기

각 개별 동작의 상태와 `AccumulatedProvisioningRolesEvent` 의 상태를 보려면 "제출한 태스크 보기" 태스크를 사용하여 이벤트 상세 정보를 확인하십시오.

개별 동작 중에서 하나가 실패하면 이벤트 상태는 실패가 되고, 태스크가 실패 상태로 이동합니다.

- 워크플로

워크플로 프로세스를 `AccumulatedProvisioningRolesEvent` 와 연결할 수 있습니다. 이 경우 승인자는 전체 이벤트를 승인 또는 거부할 수 있으며, 이 결과에 따라 개별 이벤트도 승인 또는 거부됩니다.

`AccumulatedProvisioningRolesEvent` 내에서 개별 이벤트에 대한 워크플로를 활성화하려면 추가 구성이 필요합니다.

- 감사

CA Identity Manager 가 `AccumulatedProvisioningRolesEvent` 및 각 개별 이벤트에 대한 정보를 감사합니다.

프로비저닝 역할 구성원 이벤트 누적 사용

CA CA Identity Manager 가 관리 콘솔에서 프로비저닝 역할 구성원 이벤트의 모든 추가 및 제거 동작을 단일 오퍼레이션으로 결합할 수 있는 구성 설정을 제공합니다. 단일 오퍼레이션으로 결합한 후에는 CA CA Identity Manager 가 제거 동작을 처리하기 전에 추가 동작을 단일 오퍼레이션으로 처리합니다.

이렇게 하면 일부 끝점 유형에서 요구되는 대로 이벤트의 순서를 지정할 수 있습니다.

참고: 이 기능은 기본적으로 사용되지 않습니다.

프로비저닝 역할 구성원 이벤트 누적을 사용하려면

1. Identity Manager 관리 콘솔에 액세스합니다.
2. "환경"을 클릭합니다.
3. 구성할 환경을 선택합니다.
4. "고급 설정", "프로비저닝"을 엽니다.
5. "프로비저닝 역할 구성원 이벤트 누적 사용" 확인란을 선택합니다.
6. 응용 프로그램 서버를 다시 시작합니다.

환경에서 중첩된 역할 사용

한 프로비저닝 역할이 다른 프로비저닝 역할을 포함할 수 있습니다. 포함된 역할을 중첩된 역할이라고 합니다.

예를 들어, Employee 프로비저닝 역할을 만든다고 가정합니다. 이 Employee 역할은 전자 메일 계정과 같이 모든 직원에게 필요한 계정을 제공할 수 있습니다. 그런 다음 Finance 역할과 Sales 역할 같은 부서별 프로비저닝 역할에 Employee 역할을 포함시킵니다. 부서별 프로비저닝 역할은 부서와 관련된 계정만 제공할 수 있습니다. 이 역할 조합을 통해 각 사용자에게 올바른 계정을 제공할 수 있습니다.

환경에서 중첩된 역할을 사용하려면

1. 관리 콘솔에서 환경을 선택합니다.
2. "역할 및 태스크 설정", "가져오기"를 차례로 클릭합니다.
3. "중첩된 프로비저닝 역할 지원"을 선택합니다.

4. "마침"을 클릭합니다.
5. 환경을 다시 시작합니다.

프로비저닝 역할에 역할 포함

프로비저닝 역할에 역할을 포함시키려면

1. "역할 및 태스크", "프로비저닝 역할", "프로비저닝 역할 수정"으로 이동합니다.
2. "역할 추가"를 클릭하여 "프로비저닝 역할" 탭을 완성하고 프로비저닝 역할을 선택합니다.

성능상의 이유로 역할 중첩은 3 단계로 제한하는 것이 좋습니다. 예를 들어 현재 프로비저닝 역할(첫 번째 수준 역할)에 다른 역할(두 번째 수준 역할)을 포함시키면 이 역할에 다시 세 번째 수준 역할을 포함시킬 수 있습니다. 세 번째 수준 역할에는 역할을 포함시키지 않는 것이 좋습니다.

3. 소유자 규칙을 수정하여 소유자 정책을 완료합니다.
범위는 추가한 역할의 범위와 같거나 그보다 포괄적이어야 합니다.
4. "제출"을 클릭합니다.

계정 템플릿의 특성

계정 템플릿의 특성은 계정에 특성을 정의하는 방식을 결정합니다.

기능 및 초기 특성

계정 템플릿은 다음 두 가지 유형의 특성을 포함합니다.

- **기능 특성**은 저장소 크기, 수량, 빈도 제한 또는 그룹 구성원과 같은 계정 정보를 나타냅니다. 프로비저닝 관리자는 기능 특성을 쉽게 식별할 수 있도록 모든 계정 템플릿 화면에서 기능 특성을 굵게 표시합니다.
- **초기 특성**은 계정 이름, 암호 및 계정 상태와 같은 계정에 대해 초기에 설정된 모든 정보와 이름, 주소 및 전화 번호와 같은 개인 정보를 나타냅니다.

계정은 모든 기능 특성이 동기화되어 있을 때 계정 템플릿과 동기화된다고 간주됩니다. 이것은 그룹 구성원, 권한, 할당량, 로그인 제한과 같이 끝점 유형마다 다르고 계정에 로그인할 때 사용자가 수행할 수 있는 작업을 제어하는 특성입니다.

동기화는 다른 계정 특성을 업데이트하지 않습니다. 이러한 특성은 계정 생성 중 계정 템플릿에서 초기화되며, 전파 기능 중 업데이트될 수도 있습니다. 프로비저닝 서버는 계정 템플릿을 변경할 때 즉시 계정 업데이트와 전역 사용자 특성을 변경할 때 계정 업데이트의 두 가지 전파 기능을 제공합니다.

기능 및 초기 특성 찾기

기능으로 정의된 특성과 초기 특성을 찾으려면 **eTACapability.txt** 파일을 생성해야 합니다. Windows 명령 프롬프트에서 다음과 같은 명령을 입력합니다.

```
PS_HOME\dumpptt.exe -c > eTACapability.txt
```

PS_Home

C:\Program Files\CA\Identity Manager\Provisioning Server\bin 을 지정합니다.

설치한 커넥터 모두에 대해 파일 버전이 생성됩니다.

계정 템플릿의 규칙 문자열

계정 템플릿을 만들 때 규칙 문자열을 사용하여 많은 계정 특성의 형식을 정의합니다. 규칙 문자열은 실제 값의 변수입니다. 규칙 문자열은 한 계정에서 다른 계정으로 변경되는 특성을 생성할 때 유용합니다. 규칙을 평가할 때 **CA Identity Manager** 는 계정 템플릿에 입력된 규칙 문자열을 사용자 개체에서 지정된 데이터로 바꿉니다.

참고: 탐색 중 생성된 계정 또는 프로비저닝 역할 없이 생성된 계정에서는 규칙 평가가 수행되지 않습니다.

다음 테이블에서 **CA Identity Manager** 의 규칙 문자열을 나열합니다.

규칙 문자열	설명
%AC%	계정 이름
%D%	dd/mm/yyyy 형식의 현재 날짜(날짜는 전역 사용자 정보를 포함하지 않는 계산된 값입니다). 이 규칙 문자열은 다음 중 하나와 같습니다. %\$\$\$DATE()% %\$\$\$DATE%
%EXCHAB%	Exchange 주소록에서 사서함 숨기기
%EXCHS%	사서함 홈 서버 이름
%EXCMS%	사서함 저장소 이름
%GENUID%	숫자 UNIX/POSIX 사용자 ID. 전역 사용자 UID 값이 설정된 경우 이 규칙은 %UID%과(와) 동일합니다. 하지만 전역 사용자에게 할당된 UID 값이 없고 UID 생성이 활성화된 경우(시스템 태스크의 전역 속성) 몇몇 동작이 발생합니다. 다음 사용 가능한 UID 값이 지정되고, 전역 사용자에게 할당되고, 이 규칙 변수의 값으로서 사용됩니다.
%P%	암호
%U%	전역 사용자 이름
%UA%	전체 주소(시/군/구, 거리, 우편 번호에서 생성됨)
%UB%	건물
%UC%	시/군/구

규칙 문자열	설명
%UCOMP%	회사 이름
%UCOUNTRY%	국가
%UCUxx% 또는 %UCUxxx%	사용자 지정 필드(xx 또는 xxx 는 "시스템 태스크" 프레임의 "사용자 지정 사용자" 필드 탭에 지정된 대로 2-3 자릿수 필드 ID 를 나타냄)
%UD%	설명
%UDEPT%	부서
%UE%	전자 메일 주소
%UEP%	기본 전자 메일 주소
%UES%	보조 전자 메일 주소
%UF%	이름
%UFAX%	팩스 번호
%UHP%	홈 페이지
%UI%	이니셜
%UID%	숫자 UNIX/POSIX 사용자 ID
%UL%	성
%ULOC%	위치
%UMI%	중간 이니셜
%UMN%	중간 이름
%UMP%	휴대폰 번호
%UN%	전체 이름
%UO%	사무실 이름
%UP%	전화 번호
%UPAGE%	호출기 번호
%UPC%	우편 번호
%UPE%	전화 번호 내선 번호
%US%	시/도
%USA%	주소

규칙 문자열	설명
%UT%	직책
%XD%	XML <code>dateTimeValue</code> 형식의 고정 길이 문자열 형식으로 현재 시간 스탬프를 생성합니다. <code>dateValue</code> 또는 <code>timeValue</code> 특성에 <code>(:offset,length)</code> 하위 문자열 식을 작성하여 <code>dateTimeValue</code> 의 날짜 또는 시간 부분을 추출할 수 있습니다. 예를 들어, <code>%XD:1,10%</code> 는 <code>YYYY-MM-DD</code> 를 생성하고 <code>%XD:12,8%</code> 는 <code>HH:MM:SS</code> 를 생성합니다.

특성 값

계정 특성에 대한 특정 상수 값을 사용하려면 규칙 문자열 대신 계정 템플릿 필드에 값을 입력하십시오. 예를 들어, 빈도 제한 또는 수량 크기를 지정하기 위한 값을 입력할 수 있습니다.

상수 특성 값이 두 개 이상의 퍼센트 부호를 포함해야 하는 경우 매번 두 개의 퍼센트 부호(%%)를 입력하십시오. CA CA Identity Manager에서는 계정 특성 값을 작성할 때 해당 값을 퍼센트 부호(%) 하나로 변환합니다. 계정 템플릿 값이 퍼센트 부호를 하나만 포함하는 경우 CA CA Identity Manager에서는 오류를 생성하지 않습니다. 규칙에 따르면 25%의 리터럴 값을 원할 경우 25%%를 지정해야 합니다. 그러나 특수한 경우 25%가 허용됩니다.

고급 규칙 식

단순한 전역 사용자 특성 대체 이상의 보다 큰 융통성을 제공하기 위해 다음을 포함한 고급 규칙 식을 입력할 수 있습니다.

- Offset 및 Length 를 사용하는 규칙 식의 하위 문자열
- 규칙 문자열과 값의 조합
- 다중 값 계정 특성에 대한 다중 값을 설정하는 규칙 식
- 기타 전역 사용자 특성에 대한 규칙 변수
- 기본 제공 함수의 호출
- 고객이 작성한 프로그램 종료 함수의 호출

규칙 문자열과 값 결합

규칙 문자열과 상수 값을 계정 템플릿 특성 값으로 결합할 수 있습니다. 예를 들어, %UI% 규칙 문자열이 없는 경우 여러 규칙 식을 다음과 같이 연결하여 동일한 효과를 얻을 수 있습니다.

```
%UF:,1%UMI:,1%UL:,1%
```

%UA% 규칙 문자열은 다음과 동일합니다.

```
%USA%, %UC%, %US%, %UPC%
```

또한 규칙 문자열을 상수 값과 결합하여 다음과 같이 UNIX 홈 끝점 특성을 만들 수도 있습니다.

```
/u/home/%AC%
```

규칙 하위 문자열

다음은 규칙 변수의 하위 문자열 값을 만들기 위한 구문입니다.

```
%var[:offset,length]%
```

var

앞의 표에서 정의된 대로 미리 정의된 규칙 변수의 이름을 나타냅니다.

offset

(선택 사항) 하위 문자열 접두사의 시작 오프셋을 정의합니다. 숫자 1 은 첫 번째 문자를 나타냅니다.

length

(선택 사항) 하위 문자열 접두사의 끝 오프셋을 정의합니다. length 값 별표 (*)는 값의 끝을 나타냅니다.

예를 들어, 계정 특성을 전역 사용자의 '작성 중' 특성의 첫 번째 4 개 문자로 설정하는 경우 다음을 사용하여 변수를 정의하십시오.

```
%JB:1,4%
```

'작성 중' 특성이 비어 있거나 문자 수가 4 개보다 적은 경우 결과 계정 특성 값은 4 개 문자보다 적습니다.

다중 값 규칙 식

대부분의 규칙 식은 하나의 값을 갖습니다. 이러한 식은 하나의 사용자 특성 값(대부분 빈 값)으로 시작하여 하나의 계정 특성 값(역시 대부분 빈 값)으로 끝납니다. 하지만 때때로 0 값의 빈 사용자 특성을 사용할 필요가 있습니다. 때때로 다중 값 계정 특성 값을 전파하기 위해 다중 값을 생성해야 할 필요가 있습니다.

다음 규칙 구문을 사용하면 사용자 특성에 포함할 수 있는 0 개 이상의 값을 사용하여 작업할 수 있습니다.

```
%*var%
```

규칙 식의 첫 번째 백분율 기호 % 바로 다음에 나오는 선택 사항인 다중 값 플래그 별표(*)는 참조된 사용자 특성이 얼마나 많은 값을 포함하고 있는지에 따라 이 규칙 식의 결과가 0, 1 또는 1 을 초과하는 값을 나타냅니다.

대부분의 사용자 특성 값은 하나의 값을 사용하므로 0 또는 1 값만 사용할 수 있습니다. 하지만 사용자 지정 특성(CustomField01 ~ CustomField99)은 여러 특성을 사용하므로 이러한 특성을 참조하는 규칙 변수는 0, 1 또는 1 을 초과하는 값을 포함할 수 있습니다.

사용자 특성이 1 을 초과하는 값을 갖지만 규칙 식에 별표(*)를 포함하지 않으면 규칙 평가의 결과는 첫 번째 값의 결과가 됩니다. 하지만 대부분의 경우 특성 값은 공식적으로 순서가 없으므로 CA Identity Manager 가 처음 고려하는 값을 예측할 수 없습니다.

사용자 특성에 여러 값이 있고 규칙 식에 *를 포함한 경우 계정 특성에 대해 다중 값이 생성됩니다. 계정 템플릿 특성에서 설정되는 계정 특성 자체가 다중 값이 아닌 경우 계정 템플릿에 이러한 다중 값 규칙 식을 정의하지 마십시오.

ADS 끝점 유형의 확장된 계정 특성을 다중 값으로 정의하고 이 다중 값 규칙 식 구문을 사용하여 해당 특성을 설정할 수 있습니다. 예를 들어, 이름이 'patents'인 확장된 ADS 계정 특성을 정의하고 역시 이름이 'patents'인 사용자 지정 사용자 특성 번호 3 을 정의하는 환경을 만들 수 있습니다.

ADS 계정 템플릿은 'patents' 특성에 대해 규칙 문자열 `%*UCU03%`를 정의할 수 있습니다. 그런 다음 사용자의 하나 이상의 값을 추가하여 'patents' 특성을 변경할 수 있습니다. 사용자에게 변경 사항을 적용할 때 사용자 계정을 업데이트하는 옵션을 선택하십시오. 이렇게 하면 계정의 계정 템플릿을 참조하고, 규칙 변수 `%*UCU03%`를 찾고, 사용자의 모든 patents 를 계정의 patents 특성에 복사합니다.

비슷하게, 계정을 만들 때 규칙 문자열이 평가됩니다. 또한 계정 템플릿 변경 중에 규칙 문자열이 변경된 경우 계정 템플릿과 관련된 모든 계정의 규칙을 다시 계산할지 여부를 결정할 수 있습니다.

`%*var%` 구문은 또한 단일 값 사용자 특성을 참조하는 변수 `var`에 대해 의미가 있습니다. 이것은 연결이 사용되고 참조된 특성이 사용자에게 대해 설정되지 않은 경우에만 해당됩니다.

선택 사항인 다중 값 플래그 별표(*)는 사용자 특성에 값이 없는 경우 `%*var%` 규칙 변수를 포함하는 규칙이 값으로 평가되지 않음을 나타냅니다. 이것은 빈 문자열인 경우에도 항상 단일 값으로 평가되는 단일 값 규칙 식 `%var%`와 차이가 있습니다.

이 차이를 이해하려면 다음 규칙 문자열을 고려하십시오.

```
(310)%UP%
(310)%*UP%
```

두 규칙 문자열은 지역 번호 310 을 전화 번호에 추가하는 것처럼 보입니다. 하지만 사용자가 자신의 전화 번호에 대한 값이 없는 경우 첫 번째 규칙이 계정 값 (310)으로 평가되므로 이 둘은 서로 다릅니다. 두 번째 규칙 문자열은 값을 생성하지 않으며 계정 특성을 설정되지 않은 상태로 둡니다.

한편, 다음 규칙 문자열은 전화 내선 번호를 전화 번호에 추가하는 것처럼 보입니다.

```
%UP% %UPE%
%UP% %*UPE%
```

모두에게 전화 번호가 있지만 일부에게 내선 번호가 없는 경우, 첫 번째 규칙 문자열은 내선 번호가 없는 각 사용자에게 대한 전화 번호를 포함하는 값을 생성합니다. 두 번째 규칙 문자열은 값을 생성하지 않습니다. 이 경우 `%UPE%`과 함께 첫 번째 규칙을 사용하십시오.

명시적 전역 사용자 특성 규칙

각 사용자는 이전 규칙 테이블에 나열된 것보다 더 많은 특성을 갖습니다. 아마도 이러한 기타 특성을 참조하는 규칙 식을 만들 필요는 없을 것입니다. 하지만 그러한 필요가 있는 경우 다음 구문을 사용하여 특정 사용자 특성을 참조할 수 있습니다.

`%#ldap-attribute%`

예를 들어, 사용자의 "일시 중지됨" 필드의 값을 파악해야 하는 경우 이 필드에 대한 해당 LDAP 특성 이름(`eTSuspended`)을 파악하고 `eTSuspended` 와 같이 0 또는 1로 평가되는 규칙 식을 만듭니다.

`##eTSuspended%`

또 다른 예와 같이 다음 규칙 식을 사용하여 사용자의 할당된 프로비저닝 역할을 가져올 수 있습니다.

`%%*#eTRoleDN%`

이러한 프로비저닝 역할은 전체 LDAP 고유 이름 값입니다. 기본 제공 함수 `RDNVALUE`(이후 테이블 참조)와 결합하면 값이 더욱 유용해질 수도 있습니다. 다중 값 표시기 별표(*)는 사용자의 할당된 모든 프로비저닝 역할을 다중 값으로 가져옵니다.

하위 문자열 구문도 이러한 규칙 식에 적용할 수 있으므로 `##eTTelephone:6,*%`를 사용하여 `%UP:6,*`와 동일한 효과를 얻을 수 있습니다. 각각은 CA CA Identity Manager 에게 사용자의 전화 번호 필드에서 첫 번째 5 개의 문자를 제거하도록 요구합니다.

기본 제공 규칙 함수

값에서 여러 변환을 수행하기 위해 규칙 식에서 기본 제공 규칙 함수를 사용할 수 있습니다. 기본 제공 함수 호출의 일반 형식은 다음과 같습니다.

```
%[*]$$function(arg[,...])[:offset,length]%
```

다중 값 표시기 별표(*), offset, length 하위 문자열 사양은 선택 사항입니다.

식별된 기본 제공 함수는 다음과 같습니다.

기본 제공 규칙 함수	설명
ALLOF	모든 매개 변수를 다중 값 특성으로 병합합니다. 순서가 유지되며 중복 항목은 제거됩니다. 예를 들어, 사용자 특성이 다음과 같이 설정되는 경우: eTCustomField01: { A, B } eTCustomField02: { A, C } 다음 규칙은: <pre>%*ALLOF(%*UCU01%,%*UCU02%)%</pre> 3 개의 값{ A, B, C }으로 평가됩니다.
DATE	dd/mm/yyyy 형식의 현재 날짜로 평가됩니다. 규칙 식 %D%는 다음 중 하나와 동일합니다. <pre>\$\$\$DATE()% \$\$\$DATE%</pre>
FIRSTOF	매개 변수의 첫 번째 값을 반환합니다. 특성이 설정되지 않은 경우 기본값을 삽입하기 위해 사용됩니다. <pre>\$\$\$FIRSTOF(%UCU01%, 'unknown')% \$\$\$FIRSTOF(%LN%, %UCU01%, %U%)%</pre> 어떠한 값도 설정되지 않은 경우 결과는 값 없음입니다. 인수에 상수 문자열을 입력하려면 작은따옴표로 묶으십시오.

기본 제공 규칙 함수	설명
INDEX	다중 값이 있는 특성의 값 하나를 반환합니다. 색인 1 은 첫 번째 값입니다. 색인이 값의 개수보다 많으면 결과는 설정되지 않은(빈) 값입니다. 다음 규칙은 다음과 동일합니다. <pre> \$\$\$INDEX(%*UCU01%,1)% \$\$\$FIRSTOF(%*UCU01%)% </pre>
NOTEEMPTY	인수 하나의 단일 값을 반환하지만 이 특성 값이 설정되지 않은 경우 오류를 보고합니다. 예 1: 사용자에게 할당된 UID 특성이 없는 경우 계정 생성 또는 업데이트가 실패합니다. <pre> \$\$\$NOTEEMPTY(%UID%)% </pre> 예 2: 설정된 경우 이름을 사용하고 설정되지 않은 경우 성을 사용합니다. 둘 다 설정되지 않은 경우 계정 생성 또는 업데이트가 실패합니다. <pre> \$\$\$NOTEEMPTY(\$\$\$FIRSTOF(%UF%, %UL%)%)% </pre>
PRIMARYEMAIL	여러 전자 메일 주소에서 추출한 기본 전자 메일 주소를 반환합니다. 식 %UE%는 다음과 동일합니다. <pre> \$\$\$PRIMARYEMAIL(%UEP)% </pre>

기본 제공 규칙 함수	설명
RDNVALUE	특성 값을 LDAP 고유 이름처럼 다루고 해당 DN 에서 개체의 일반 이름을 추출합니다. <code>%%*\$\$RDNVALUE(%#eTRoleDN%)%</code> 이 함수는 할당된 모든 프로비저닝 역할의 일반 이름을 반환합니다. 사용자가 동일한 일반 이름을 사용하는 프로비저닝 역할에 속하는 경우 해당 역할 이름은 한 번만 나열됩니다.
TOLOWER	대문자 텍스트를 소문자로 변환합니다. <code>%%\$\$TOLOWER(%AC%)%</code>
TOUPPER	소문자 텍스트를 대문자로 변환합니다. <code>%%\$\$TOUPPER(%U%)%</code>
TRIM	특성 값에서 맨 앞 및 맨 뒤의 공백 문자를 제거합니다. 예를 들어, "<code>%UF %UL%</code>"는 일반적으로 이름과 성이 공백 문자로 구분된 값을 만듭니다. 하지만 사용자의 이름 특성이 비어 있으면 이 규칙은 끝에 공백을 넣는 값을 생성합니다. 하지만 다음을 사용하면 <code>“%%\$\$TRIM(%UF% %UL%)%</code> 이름 또는 성 중 하나가 설정되지 않은 경우라도 계정 특성 값의 앞 또는 뒤에서 공백이 제거됩니다.

프로비저닝 역할 성능

프로비저닝 서버와 함께 CA Identity Manager 를 사용하는 경우 고려할 수 있는 일부 프로비저닝 성능 향상이 있습니다.

JIAM 개체 캐시

Identity Manager 는 Java IAM(JIAM) API 를 사용하여 프로비저닝 서버와 통신합니다. 통신 성능을 높이려면 프로비저닝 서버에서 검색되는 개체에 대한 캐시를 구성할 수 있습니다.

JIAM 캐시 사용

JIAM 캐시를 사용하려면

1. 관리 콘솔을 통해 환경 설정에 액세스합니다. "고급 설정", "기타"를 클릭합니다.
2. JIAM 캐시에 대한 사용자 정의된 속성을 구성합니다.
 - 속성- JIAMCache
 - 값- true
3. "추가"를 클릭합니다.
4. "저장"을 클릭합니다.
사용자 정의된 속성이 저장됩니다.

JIAM 캐시 TTL(Time-to-live) 정의

JIAM 캐시는 데이터가 만료되기 전 지정된 기간 동안 정보를 저장합니다. 이 기간을 TTL(Time-to-Live)이라고 합니다. 데이터가 캐시에 얼마나 오래 남아 있는지 정의하려면 JIAM 캐시 TTL(초)을 설정합니다.

로컬에서 캐시에 저장된 데이터의 이점을 최대한 활용하려면 성능상 이점과 데이터 보존 기간 사이의 균형점을 찾아야 합니다. 최소 TTL 값 1 일과 최대 값 7 일을 권장합니다. 다음 표에서 사용할 time-to-live 값을 참조하십시오.

원하는 수명	TTL 설정(초)
24 시간(1 일)	86,400
72 시간(3 일)	259,200
120 시간(5 일)	432,000

168 시간(7 일)

604,800

JIAM 캐시 TTL 을 정의하려면

1. 관리 콘솔을 통해 환경에 액세스합니다. "고급 설정", "기타"를 클릭합니다.
2. JIAM 캐시 TTL 에 대한 사용자 정의된 속성을 구성합니다.
 - 속성—JIAMCacheTTL
 - 값—데이터가 JIAM 캐시에 남아 있는 시간(초)
기본값: 300
3. "추가"를 클릭합니다.
4. "저장"을 클릭합니다.

사용자 정의된 속성이 저장됩니다.

세션 풀링

성능을 높이기 위해 **Identity Manager** 는 프로비저닝 서버와 통신할 때 사용할 수 있도록 여러 세션을 풀에 미리 할당할 수 있습니다.

세션 풀링에 대한 자세한 내용은 *관리 콘솔 온라인 도움말* 을 참조하십시오.

기존 환경에 대한 프로비저닝 태스크

사용자 지정 역할 정의를 가져오고 환경에서 프로비저닝을 활성화하려는 경우 관리 콘솔에서 "프로비저닝 전용" 역할 정의도 가져와야 합니다. 이러한 역할 정의는 다음 폴더에 있습니다.

iam_im.ear\management_console.war\WEB-INF\Template\environment

참고: 역할 정의 가져오기에 대한 자세한 내용은 *Configuration Guide* (구성 안내서)를 참조하십시오.

제 10 장: 관리되는 서비스(기본 액세스 요청)

이 섹션은 다음 항목을 포함하고 있습니다.

[서비스 만들기](#) (페이지 244)

[사용자에게 서비스 제공](#) (페이지 256)

[서비스 수정](#) (페이지 260)

[액세스 요청 및 보기에 검색 추가](#) (페이지 261)

[서비스 삭제](#) (페이지 262)

[서비스에 대한 액세스 갱신](#) (페이지 264)

서비스 만들기

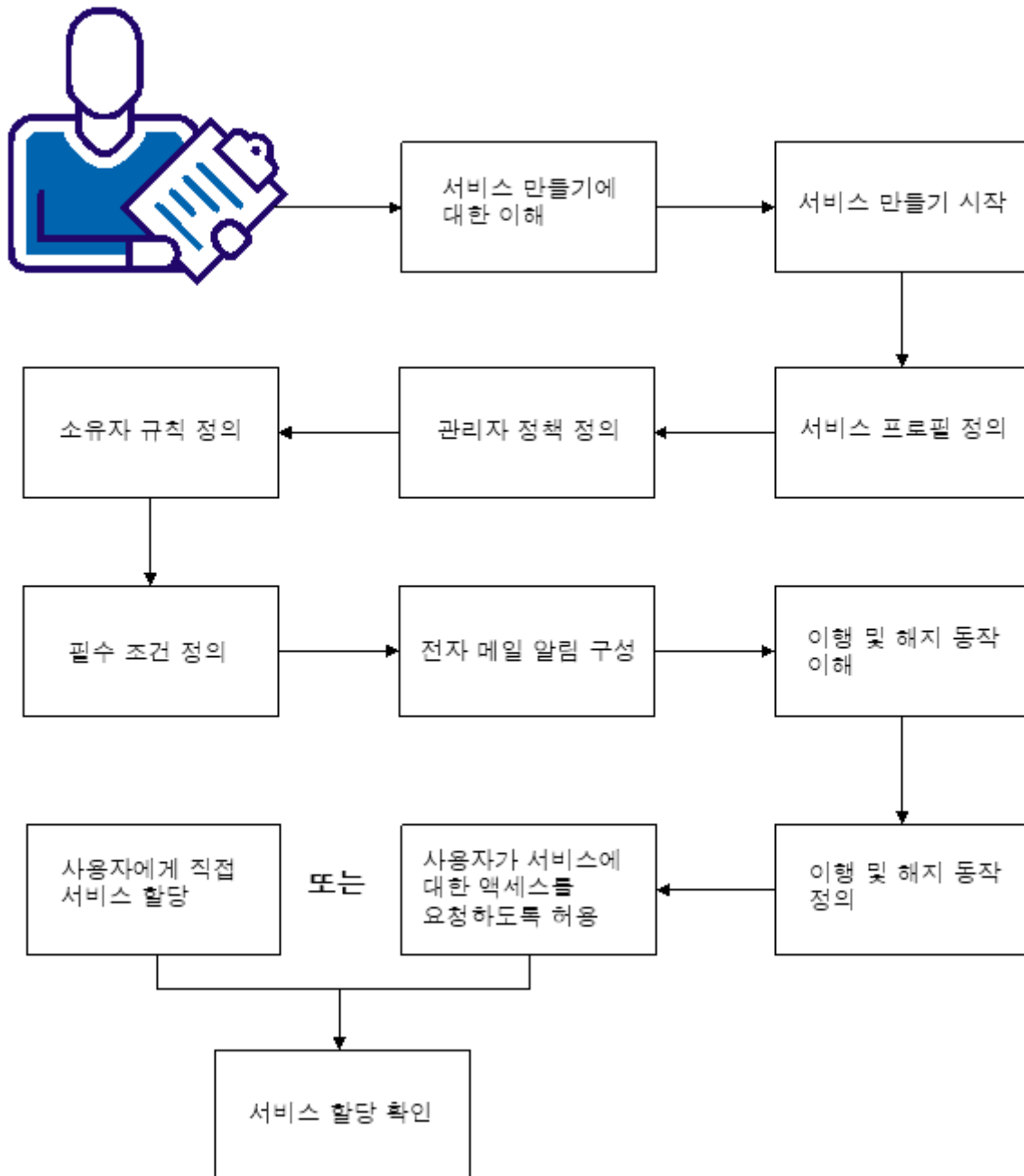
서비스는 권한 관리를 간소화합니다. 서비스는 지정된 비즈니스 역할에 대해 사용자에게 필요한 권한(태스크, 역할, 그룹 및 특성)을 모두 함께 번들로 제공합니다. 서비스는 CA CloudMinder 사용자 콘솔에서 "액세스 요청" 태스크를 통해 사용자에게 제공됩니다. "액세스 요청" 태스크를 사용하면 사용자나 관리자가 서비스를 요청, 할당, 해지 및 갱신할 수 있습니다.

서비스를 사용하면 관리자가 사용자 권한을 하나의 집합으로 관리되는 단일 패키지로 조합할 수 있습니다. 예를 들어 새 "영업" 직원 모두에게 특정 끝점 시스템에서 정의된 태스크 및 계정 집합에 대한 액세스가 필요한 경우를 생각해 봅시다. 사용자 계정 프로필에 추가된 특정 정보도 필요합니다. 관리자는 새 "영업" 직원에게 필요한 태스크, 역할, 그룹 및 프로필 특성 정보를 모두 포함하는 "영업 관리"라는 서비스를 만듭니다. 관리자가 사용자에게 "영업 관리" 서비스를 할당하는 경우 해당 사용자는 서비스로 정의된 전체 역할, 태스크, 그룹 및 계정 특성 집합을 받습니다.

사용자가 서비스에 액세스할 수 있는 다른 방법은 스스로 액세스를 요청하는 것입니다. 사용자 콘솔에는 각 사용자가 자신의 요청에 사용할 수 있는 서비스 목록이 있습니다. 이 목록은 대개 서비스를 만드는 동안 적절한 권한이 있는 관리자가 "자체 구독"으로 표시한 서비스로 채워집니다. 사용자가 가능한 서비스 목록에서 사용자가 자신에게 필요한 서비스에 대한 액세스를 요청할 수 있습니다. 사용자가 서비스에 대한 액세스를 요청하면 요청이 자동으로 이행되고 연결된 권한이 사용자에게 즉시 할당됩니다. 적절한 권한이 있는 관리자가 워크플로 승인을 요구하거나 전자 메일 알림을 생성하도록 서비스 이행을 구성할 수도 있습니다.

다음 다이어그램에서는 서비스를 만들기 위해 이해해야 할 정보와 수행해야 할 단계를 보여 줍니다.

서비스 만들기



다음 항목에서는 서비스를 만들어 사용자에게 제공하는 방법을 설명합니다.

1. [서비스 만들기 이해](#) (페이지 246)
2. [서비스 만들기 시작](#) (페이지 247)
3. [서비스 프로필 정의](#) (페이지 247)
4. [서비스에 대한 관리자 정책 정의](#) (페이지 250)
5. [서비스에 대한 소유자 규칙 정의](#) (페이지 251)
6. [서비스에 대한 필수 조건 정의](#) (페이지 251)
7. [서비스 갱신에 대한 전자 메일 알림 구성](#) (페이지 252)
8. [이행 및 해지 동작 이해](#) (페이지 253)
9. [서비스에 대한 이행 및 해지 동작 정의](#) (페이지 253)
10. 사용자가 서비스에 대한 액세스를 요청할 수 있도록 허용
사용자가 사용자 콘솔에서 "내 액세스", "액세스 요청 및 보기"를 차례로 클릭하면 해당 요청에 사용할 수 있는 서비스 목록이 표시됩니다. 이 목록에 나타나는 서비스는 대개 서비스를 만드는 동안 적절한 권한이 있는 관리자가 "자체 구독"으로 표시한 것입니다.
11. [사용자에게 서비스 직접 할당](#) (페이지 94)
12. 서비스 할당 확인

서비스 만들기 이해

서비스를 만들기 전에 서비스 만들기 및 이행에 필요한 필수 조건 정보와 권한을 고려하십시오.

다음 질문을 고려하십시오.

1. 이 서비스로 충족되는 비즈니스 요구 사항은 무엇입니까? 예를 들어 새 직원 모두에게 **Salesforce.com** 계정을 제공하는 서비스를 만들 수 있습니다.
2. 서비스 구성원에게 특정 관리자 역할이 필요합니까? 그렇다면 해당 관리자 역할을 만들거나 식별하십시오.

3. 서비스 구성원이 하나 이상의 끝점에 대한 액세스를 받아야 합니까? 그렇다면 해당 끝점을 만들거나 식별하십시오.
4. 서비스 구성원에게 끝점에 대한 액세스가 필요한 경우 연결된 프로비저닝 역할과 계정 템플릿을 만들거나 식별하십시오.
5. 서비스 구성원이 특정 그룹의 구성원이 되어야 합니까? 그렇다면 해당 그룹을 만들거나 식별하십시오.
6. 사용자가 서비스 구성원이 될 때 특정 사용자 특성을 참조하거나 수정해야 합니까? 예를 들어 사용자가 **Salesforce.com** 서비스를 받는 경우 해당 사용자의 부서 특성이 "Sales"로 설정되었는지 여부를 확인해야 합니까? 그렇다면 해당 사용자 특성을 만들거나 식별하십시오.

이러한 필수 조건을 만들거나 식별했으면 [서비스 만들기를 시작](#) (페이지 247)할 수 있습니다.

서비스 만들기 시작

사용자 콘솔에서 서비스를 만듭니다.

다음 단계를 수행하십시오.

1. 서비스 관리 권한이 있는 계정에 로그인합니다.
예를 들어 환경의 첫 번째 사용자는 "서비스 만들기" 태스크가 있는 "시스템 매니저" 역할을 가지고 있습니다.
2. 탐색 메뉴에서 서비스를 선택합니다(주로 "태스크" 아래에 표시됨).
3. "서비스 관리", "서비스 만들기"를 차례로 클릭합니다.
4. 서비스 프로필을 정의합니다.

서비스 프로필 정의

"프로필" 탭에서 서비스의 기본 특징을 정의할 수 있습니다.

다음 단계를 수행하십시오.

1. 이름 및 태그를 입력합니다. 태그는 서비스의 고유 식별자입니다.
참고: 태그는 영숫자와 밑줄만 포함할 수 있고 숫자로 시작할 수 없습니다. 생성된 태그 이름은 나중에 서비스가 삭제되더라도 변경하거나 다시 사용할 수 없습니다.

2. 서비스를 만드는 즉시 사용자에게 제공하려면 "사용"을 선택하십시오.
3. 이 서비스를 사용자가 요청하는 데 사용할 수 있는 서비스 목록에 표시하려면 "자체 구독"을 선택하십시오. "자체 구독"이 사용되도록 설정한 경우 사용자는 사용자 콘솔을 통해 이 서비스에 대한 액세스를 요청할 수 있습니다.
4. (선택 사항) 하나 이상의 범주를 추가합니다. 범주 이름을 입력하고 위쪽 화살표를 클릭하여 서비스에 추가합니다.

범주는 서비스에 추가 정보를 추가합니다. 이 추가 정보를 사용하여 수많은 서비스를 포함하는 환경에서 서비스를 쉽게 검색할 수 있습니다.

5. 사용자가 서비스를 요청할 때 추가 사용자 데이터를 수집하려면 "서비스 런타임 사용자 데이터 화면"을 지정하십시오.

"서비스 런타임 사용자 데이터 화면"을 사용하면 서비스를 이행하는 데 필요한 사용자 데이터가 모두 시스템에 존재하는지 확인할 수 있습니다. 예를 들어 **Google Apps** 계정을 만드는 서비스를 이행하려면 올바른 전자 메일 주소가 필요합니다. 사용자의 전자 메일 주소가 **CA CloudMinder** 사용자 저장소에 존재하지 않으면 사용자가 서비스를 요청할 때 해당 전자 메일 주소를 제공해야 합니다.

- a. "찾아보기"를 클릭합니다.

사용 가능한 프로필 화면 목록이 나타납니다. 이러한 화면은 일반적으로 사용자 데이터를 수집하는 데 사용됩니다.

- b. 수집할 사용자 데이터를 포함하는 프로필 화면을 선택합니다. 다음 옵션 중 하나를 선택합니다.

- 해당 화면에 포함된 사용자 데이터를 모두 수집하려면 "선택"을 클릭합니다.

또는

- 수집할 사용자 데이터를 사용자 지정하려면 "복사"를 클릭합니다. 새 화면의 이름과 고유한 태그를 지정합니다. 사용자 데이터 요소를 추가, 편집 또는 제거하고 "확인"을 클릭합니다.

또는

- 해당 화면에 포함된 사용자 데이터를 변경하려면 "편집"을 클릭합니다. 사용자 데이터 요소를 추가, 편집 또는 제거하고 "확인"을 클릭합니다.

중요! 사용자 데이터 화면을 편집하면 사용자 콘솔에서 해당 화면이 사용되는 모든 곳에 변경 내용이 적용됩니다. 대신에 프로필 화면을 복사하고 사용자 지정하는 것이 좋습니다.

- c. "선택"을 클릭합니다.

사용자가 서비스를 요청할 때 선택한 사용자 데이터 요소가 수집됩니다.

참고: 사용자가 서비스를 요청할 때 필요한 데이터가 시스템에 존재하는 경우 해당 데이터가 프로필 화면에 미리 채워집니다.

6. [서비스에 대한 관리자 정책 정의](#) (페이지 250)

서비스에 대한 관리자 정책 정의

"관리자" 탭에서는 사용자를 이 서비스의 구성원과 관리자로 추가하거나 제거할 수 있는 사람을 정의합니다. 관리자 정책에는 관리자 및 범위 규칙과 하나 이상의 관리자 권한("구성원 관리" 또는 "관리자 관리")이 포함됩니다.

관리자 규칙은 이 서비스를 관리할 수 있는 사람을 정의합니다. 범위 규칙은 관리자가 될 수 있는 사용자를 제한합니다. 예를 들어 관리자 규칙에서 "영업" 그룹의 모든 구성원이 서비스를 관리할 수 있도록 허용한 다음 범위 규칙에서 해당 사용자를 메사추세츠주 Boston 에 있는 "영업" 그룹의 구성원으로 제한할 수 있습니다.

다음 단계를 수행하십시오.

1. "관리자" 탭에서 "추가"를 클릭합니다.
"관리자 정책" 화면이 나타납니다.
2. 이 서비스를 관리할 수 있는 사용자에 대한 관리자 규칙을 정의합니다.
예를 들어 "영업" 그룹에 속한 사용자나 "영업 매니저"의 특정 직책 프로필 특성이 있는 사용자를 지정할 수 있습니다.
규칙의 이전에 지정된 부분을 편집하려면 왼쪽 화살표를 클릭합니다.
3. 이 서비스를 관리할 수 있는 사용자를 제한하기 위한 범위 규칙을 정의합니다. 예를 들어 관리자 규칙에서 "영업" 그룹에 속한 사용자를 지정한 경우 해당 규칙의 범위를 메사추세츠주 Boston 시의 사용자로 제한할 수 있습니다.
참고: 각 서비스마다 규칙과 권한이 다른 관리자 정책을 여러 개 추가할 수 있습니다.
4. 관리자가 이 서비스의 구성원을 추가하거나 제거할 수 있도록 허용하려면 "이 서비스의 구성원 관리 가능"을 클릭합니다.
5. "확인"을 클릭합니다.
6. 정책을 더 편집하려면 "편집" 아이콘을 클릭합니다. 정책을 제거하려면 빼기 기호 아이콘을 클릭합니다.
7. [서비스에 대한 소유자 규칙을 정의합니다.](#) (페이지 251)

서비스에 대한 소유자 규칙 정의

"소유자" 탭에서는 서비스의 소유자가 될 수 있는 사람에 대한 규칙을 정의합니다. 소유자는 서비스를 수정할 수 있는 사용자입니다.

다음 단계를 수행하십시오.

1. "소유자" 탭에서 "추가"를 클릭합니다.
"소유자 규칙" 화면이 나타납니다.
2. 이 서비스를 소유할 수 있는 사용자에게 대한 소유자 규칙을 정의합니다.
예를 들어 "영업" 그룹에 속한 사용자나 "영업 매니저"의 특정 직책 프로필 특성이 있는 사용자를 지정할 수 있습니다.
규칙의 이전에 지정된 부분을 편집하려면 왼쪽 화살표를 클릭합니다.
3. "확인"을 클릭합니다.
4. [서비스에 대한 필수 조건을 정의합니다.](#) (페이지 251)

서비스에 대한 필수 조건 정의

"필수 조건" 탭에서는 사용자가 이 서비스를 요청하기 전에 가지고 있어야 하는 서비스를 정의합니다. 서비스는 지정된 사용자가 모든 필수 조건 서비스의 구성원인 경우에만 해당 사용자가 사용할 수 있는 서비스 목록에 나타납니다.

필수 조건 서비스에 대한 기간을 설정한 경우 해당 기간은 정의 중인 서비스에 적용됩니다. 예를 들어 서비스 A가 서비스 B에 대한 필수 조건인 경우를 생각해 봅시다. 서비스 A의 기간은 1주일입니다. 서비스 B도 1주일 후에 만료됩니다.

다음 단계를 수행하십시오.

1. "필수 조건" 탭에서 "서비스 추가"를 클릭합니다.
검색 화면이 나타납니다.
2. 이 서비스에 대한 필수 조건으로 지정할 서비스를 검색합니다.
관리 권한이 있는 서비스를 모두 나열하는 목록을 표시하려면 검색 조건을 수정하지 않고 "검색"을 클릭합니다.
3. 서비스를 선택하고 "선택"을 클릭합니다.
이 서비스에 대한 필수 조건 목록이 업데이트되어 나타납니다.

서비스 갱신에 대한 전자 메일 알림 구성

일부 서비스는 특정 기간이 경과한 후에 만료됩니다.

"전자 메일" 탭에서는 서비스 구성원에게 구성원 자격이 만료되기 전에 갱신하도록 미리 알려 주는 전자 메일 알림을 구성할 수 있습니다. 이 경우 구성원은 "서비스 갱신" 태스크를 사용하여 해당 액세스를 갱신할 수 있습니다.

CA CloudMinder 는 동적 콘텐츠를 포함하는 기본 전자 메일 템플릿을 제공합니다. 이 콘텐츠는 전자 메일이 전송될 때 자동으로 채워집니다. 전자 메일 알림 편집기에 중괄호({ })로 묶여 나타나는 동적 콘텐츠는 전자 메일에 특정 사용자 이름, 서비스 이름 및 만료 날짜를 추가합니다.

편집기에서 전자 메일 알림 콘텐츠를 수정할 수 있습니다. 예를 들어 본문 또는 제목 텍스트를 수정하거나 글꼴을 변경하거나 동적 콘텐츠를 제거할 수 있습니다.

전자 메일 알림을 구성하는 경우 다음 항목을 참고하십시오.

- 전자 메일 알림에 동적 콘텐츠를 포함하는 경우 중괄호({ })로 묶인 텍스트를 수정하지 마십시오.
- 서비스에 만료되는 필수 조건 서비스가 있는 경우 전자 메일 알림은 필수 조건 서비스에 대해서만 전송되는데, 이는 두 서비스 모두에 대해 전자 메일 알림을 구성한 경우에도 마찬가지입니다.

다음 단계를 수행하십시오.

1. "전자 메일" 탭에서 "서비스가 만료되기 전에 사용자에게 전자 메일 알림" 확인란을 선택하여 알림을 사용하도록 설정합니다.
2. (선택 사항) 편집기의 컨트롤을 사용하여 전자 메일 알림을 사용자 지정합니다.

전자 메일 알림 편집기는 HTML 을 지원합니다. 도구 모음에서 "Toggle HTML Source"(HTML 소스 전환) 단추(<>)를 클릭하여 전자 메일 알림 본문에 HTML 콘텐츠를 추가할 수 있습니다.

3. [이행 및 해지 동작을 이해합니다.](#) (페이지 253)

이행 및 해지 동작 이해

"동작" 탭에서는 서비스가 할당되거나 해지될 때 추가, 수정 또는 제거할 권한과 정보(태스크, 역할, 그룹 및 특성)를 정의합니다. 간단히 말해 서비스 동작은 서비스가 수행하는 동작을 정의합니다.

CA CloudMinder 는 Policy Xpress 정책을 사용하여 이행 및 해지 동작이 발생하는 상황을 정의합니다. CA CloudMinder 가 이 정책을 미리 구성하므로 사용자가 서비스를 요청할 때마다 적절한 조건과 데이터가 존재합니다. 서비스는 자동으로 이행되거나 해지됩니다.

관리자는 서비스를 이행하거나 해지할 때 수행되는 시스템 동작을 정의해야 합니다. 예를 들어 서비스를 만드는 경우 관리자는 서비스 구성원이 "영업 매니저" 관리자 역할, "Salesforce.com" 프로비저닝 역할 및 "영업" 그룹을 받도록 지정할 수 있습니다. 마찬가지로 관리자는 서비스가 해지될 때 해당 권한이 제거되도록 지정할 수 있습니다.

서비스에 대한 이행 및 해지 동작 정의

"동작" 탭에서는 서비스를 사용자에게 할당하거나 사용자로부터 제거할 때 추가, 수정 또는 제거되는 권한과 정보를 정의합니다.

다음 단계를 수행하십시오.

1. "동작" 탭을 클릭합니다.

"이행 동작" 및 "해지 동작" 화면이 나타납니다.

2. "이행 동작 관리" 또는 "해지 동작 관리" 단추를 클릭합니다.

"Policy Xpress 정책 만들기" 화면이 나타납니다.

동작 규칙을 만들기 위해 다음과 같은 필드가 미리 정의되어 있습니다.

이름

동작 규칙의 이름을 제공합니다. 이 이름은 고유해야 합니다.

설명

동작 규칙의 의미를 정의합니다.

우선 순위

여러 동작 규칙이 일치하는 경우 실행할 동작 규칙을 정의합니다. 이 필드는 기본 동작을 정의할 때 유용합니다. 예를 들어, 각각 부서 이름에 대한 여러 규칙이 있는 경우 조건 없이 규칙을 추가하지만 우선 순위를 낮게 지정(예를 들어, 다른 모두가 5 일 때 10 으로 설정)하여 기본값을 설정하는 것이 가능합니다. 일치하는 부서 규칙이 없는 경우 이 기본값이 사용됩니다.

3. "동작 규칙 조건" 아래에서 일치할 조건을 지정합니다.

4. "동작 추가" 아래에서 "일치할 때 동작 추가" 단추를 클릭합니다.

"일치할 때 동작 추가" 화면이 나타납니다. 이 화면에서는 규칙이 일치할 때 수행되는 시스템 동작을 정의합니다.

5. 동작의 용도를 정의하는 이름을 입력합니다.

예를 들어 "Add the Sales Manager Admin Role"(영업 매니저 관리자 역할 추가)을 입력합니다.

6. 원하는 시스템 동작 범주를 선택합니다.

예를 들어 역할을 추가하려면 "역할" 범주를 선택합니다.

7. 원하는 시스템 동작 유형을 선택합니다.

예를 들어 관리자 역할을 추가하거나 제거하려면 "관리자 역할 설정" 유형을 선택합니다.

8. 원하는 시스템 기능을 선택합니다.

예를 들어 관리자 역할을 추가하려면 "추가" 기능을 선택합니다.

참고: 기능을 선택하면 해당 기능에 대한 설명이 나타납니다. 이 설명을 사용하면 선택한 기능으로 원하는 시스템 동작이 얻어지는지 여부를 확인하는 데 도움이 됩니다.

9. 원하는 특정 시스템 동작을 정의합니다.

예를 들어 "영업 매니저"라는 관리자 역할을 추가하려면 역할 이름을 입력하거나, "찾아보기" 단추를 클릭하고 사용 가능한 관리자 역할 목록에서 "영업 매니저"를 선택합니다.

10. "확인"을 클릭합니다.

이 서비스에 대해 원하는 동작을 모두 추가할 때까지 이 절차를 반복합니다.

11. "확인"을 클릭합니다.

지정된 이행 및 해지 동작이 서비스에 연결됩니다. 사용자가 서비스를 받는 경우 연결된 권한과 정보가 추가, 수정 또는 제거됩니다.

12. 이제 [사용자에게 서비스를 할당](#) (페이지 94)할 수 있습니다.

사용자에게 서비스 할당

개별 사용자에게 서비스를 직접 할당할 수 있습니다. 이 사용자는 서비스의 구성원이 됩니다.

다음 단계를 수행하십시오.

1. "서비스", "액세스 요청 및 보기"로 이동합니다.

관리할 수 있는 서비스 목록이 나타납니다.

2. 사용자에게 할당할 서비스를 선택하고 "선택"을 클릭합니다.

서비스에 할당된 사용자 목록이 나타납니다.

3. "액세스 요청"을 클릭합니다.

4. 서비스를 할당할 사용자를 검색합니다.

관리 권한이 있는 사용자를 모두 나열하는 목록을 표시하려면 검색 조건을 수정하지 않고 "검색"을 클릭합니다.

5. 사용자를 선택하고 "선택"을 클릭합니다.

서비스에 할당된 사용자 목록이 업데이트되어 나타납니다.

6. "변경 내용 저장"을 클릭합니다.

사용자가 지정된 서비스를 받습니다. 이 사용자는 서비스에 추가한 모든 응용 프로그램, 역할, 그룹, 특성을 받습니다.

서비스 할당 확인

사용자에게 서비스를 할당한 후 해당 서비스와 관련된 태스크가 성공적으로 완료되었는지 확인하십시오.

다음 단계를 수행하십시오.

1. "서비스", "서비스 액세스 요청 기록 보기"로 이동합니다.
검색 화면이 나타납니다.
2. 사용자에게 할당한 서비스를 검색합니다.
관리 권한이 있는 서비스를 모두 나열하는 목록을 표시하려면 검색 조건을 수정하지 않고 "검색"을 클릭합니다.
관리할 수 있는 서비스 목록이 나타납니다.
3. 할당한 서비스를 선택하고 "선택"을 클릭합니다.
서비스와 관련된 동작 기록이 나타납니다.
4. "마지막 변경"을 클릭하여 가장 최근의 동작부터 표시합니다.
5. 해당 사용자가 서비스를 성공적으로 받았는지 확인합니다.
6. "닫기"를 클릭합니다.

사용자에게 서비스 제공

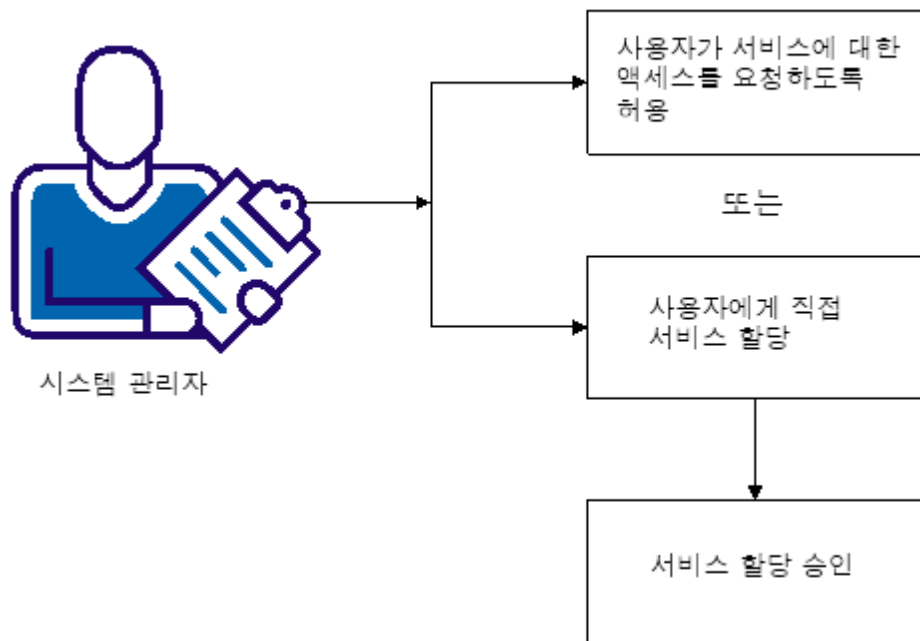
서비스는 권한 관리를 간소화합니다. 서비스는 지정된 비즈니스 역할에 대해 사용자에게 필요한 권한을 모두 함께 번들로 제공합니다. 서비스는 사용자 콘솔의 "액세스 요청" 태스크를 통해 사용자에게 제공됩니다. "액세스 요청" 태스크를 사용하면 사용자나 관리자가 사용자 인터페이스를 통해 서비스를 요청, 할당, 해지 및 갱신할 수 있습니다.

서비스를 사용하면 시스템 관리자가 사용자 활동과 정보(태스크, 역할, 그룹 및 특성)를 하나의 집합으로 관리되는 단일 패키지로 조합할 수 있습니다. 예를 들어 모든 새 영업 직원은 정의된 태스크 집합, 특정 끝점 시스템 계정, 해당 영업 직원의 사용자 계정 프로필에 추가된 특정 정보 등에 액세스해야 합니다. 시스템 관리자는 새 영업 직원에게 필요한 태스크, 역할, 그룹 및 프로필 특성 정보를 모두 포함하는 "영업 관리"라는 서비스를 만듭니다. 관리자가 사용자에게 "영업 관리" 서비스를 할당하는 경우 해당 사용자는 서비스로 정의된 전체 역할, 태스크, 그룹 및 계정 특성 집합을 받습니다.

사용자가 서비스에 액세스할 수 있는 다른 방법은 스스로 액세스를 요청하는 것입니다. 사용자 콘솔에는 각 사용자가 자신의 요청에 사용할 수 있는 서비스 목록이 있습니다. 이 목록은 대개 서비스를 만드는 동안 적절한 권한이 있는 시스템 관리자가 "자체 구독"으로 표시한 서비스로 채워집니다. 사용 가능한 서비스 목록에서 사용자가 자신에게 필요한 서비스에 대한 액세스를 요청할 수 있습니다. 사용자가 서비스에 대한 액세스를 요청하면 요청이 자동으로 이행됩니다. 관련 태스크, 역할, 그룹 및 특성이 사용자에게 즉시 할당됩니다. 적절한 권한이 있는 CA CloudMinder 관리자가 워크플로 승인을 요구하거나 전자 메일 알림을 생성하도록 서비스 이행을 구성할 수도 있습니다.

다음 다이어그램에서는 사용자에게 서비스를 제공하기 위해 파악해야 할 정보와 수행해야 할 단계를 보여 줍니다.

사용자가 서비스를 사용할 수 있도록 만들기



다음과 같은 방법을 사용하여 사용자에게 서비스를 제공할 수 있습니다.

1. 사용자가 스스로 액세스를 요청할 수 있도록 허용

CA CloudMinder 사용자 콘솔에서 사용자가 "내 액세스", "액세스 요청 및 보기"를 차례로 클릭하면 해당 사용자의 요청에 사용할 수 있는 서비스 목록이 표시됩니다. 이 목록에 나타나는 서비스는 대개 서비스를 만드는 동안 적절한 권한이 있는 CA CloudMinder 관리자가 "자체 구독"으로 표시한 것입니다.

사용자가 액세스를 요청하면 시스템은 서비스를 사용자에게 할당합니다. 이 사용자는 서비스와 관련된 모든 응용 프로그램, 역할, 그룹, 특성을 받습니다. 서비스가 응용 프로그램에 대한 "실행 역할"을 포함하는 경우 이 응용 프로그램에 대한 아이콘과 링크가 사용자 콘솔 홈 페이지에 표시됩니다.

2. [사용자에게 서비스 직접 할당](#) (페이지 94)

3. 사용자에게 서비스를 할당하는 경우 [서비스 할당을 확인](#) (페이지 259)합니다.

사용자에게 서비스 할당

개별 사용자에게 서비스를 직접 할당할 수 있습니다. 이 사용자는 서비스의 구성원이 됩니다.

다음 단계를 수행하십시오.

1. "서비스", "액세스 요청 및 보기"로 이동합니다.
관리할 수 있는 서비스 목록이 나타납니다.
2. 사용자에게 할당할 서비스를 선택하고 "선택"을 클릭합니다.
서비스에 할당된 사용자 목록이 나타납니다.
3. "액세스 요청"을 클릭합니다.
4. 서비스를 할당할 사용자를 검색합니다.

관리 권한이 있는 사용자를 모두 나열하는 목록을 표시하려면 검색 조건을 수정하지 않고 "검색"을 클릭합니다.

5. 사용자를 선택하고 "선택"을 클릭합니다.
서비스에 할당된 사용자 목록이 업데이트되어 나타납니다.
6. "변경 내용 저장"을 클릭합니다.
사용자가 지정된 서비스를 받습니다. 이 사용자는 서비스에 추가한 모든 응용 프로그램, 역할, 그룹, 특성을 받습니다.

서비스 할당 확인

사용자에게 서비스를 할당한 후 해당 서비스와 관련된 태스크가 성공적으로 완료되었는지 확인하십시오.

다음 단계를 수행하십시오.

1. "서비스", "서비스 액세스 요청 기록 보기"로 이동합니다.
검색 화면이 나타납니다.
2. 사용자에게 할당한 서비스를 검색합니다.
관리 권한이 있는 서비스를 모두 나열하는 목록을 표시하려면 검색 조건을 수정하지 않고 "검색"을 클릭합니다.
관리할 수 있는 서비스 목록이 나타납니다.
3. 할당한 서비스를 선택하고 "선택"을 클릭합니다.
서비스와 관련된 동작 기록이 나타납니다.
4. "마지막 변경"을 클릭하여 가장 최근의 동작부터 표시합니다.
5. 해당 사용자가 서비스를 성공적으로 받았는지 확인합니다.
6. "닫기"를 클릭합니다.

서비스 수정

시스템 관리자는 자신이 이전에 만든 서비스를 수정할 수 있습니다. 예를 들어 서비스에 역할을 추가하여 해당 서비스가 서비스 구성원에게 부여하는 권한을 변경할 수 있습니다. 서비스의 관리자 및 소유자 규칙, 서비스 필수 조건 및 기타 관리 정보를 조정할 수도 있습니다.

CA CloudMinder가 지정된 사용자에게 대한 서비스를 이행한 경우 서비스의 변경 내용은 해당 사용자에게 전파되지 않습니다. 서비스를 수정하도록 결정하는 경우 변경 전에 서비스를 받은 사용자에게는 원래 권한이 있습니다. 변경 후에 서비스를 받는 사용자에게는 수정된 서비스가 부여하는 권한이 있습니다. 예를 들어 다음과 같은 경우를 생각해 봅시다.

시스템 관리자가 서비스 구성원에게 "영업 매니저" 역할과 "영업" 그룹을 부여하는 "영업 매니저" 서비스를 만듭니다. 사용자가 "영업 매니저" 서비스를 요청하면 CA CloudMinder가 사용자에게 적절한 역할과 그룹을 부여하여 서비스를 이행합니다. 시스템 관리자는 "직원 매니저" 역할을 포함하도록 "영업 매니저" 서비스를 수정하기로 결정합니다. 이 경우 서비스의 기존 구성원은 "직원 매니저" 역할을 받지 않습니다. "영업 매니저" 서비스의 새 구성원만 "영업 매니저" 역할과 "영업" 그룹 외에도 "직원 매니저" 역할을 받습니다.

따라서 서비스 구성원이 없는 경우에만 서비스를 수정하는 것이 좋습니다. 즉, 서비스를 요청하여 받은 사용자도 없고 사용자에게 서비스를 할당할 관리자도 없는 경우에만 서비스를 수정하십시오.

서비스의 관리 정보, 관리자 및 소유자 규칙, 서비스 필수 조건, 권한(태스크, 역할, 그룹 및 특성) 등을 수정할 수 있습니다.

다음 단계를 수행하십시오.

1. 서비스 관리 권한이 있는 CA CloudMinder 계정에 로그인합니다.
예를 들어 환경의 첫 번째 사용자에게 "서비스 수정" 태스크를 가진 "시스템 매니저" 역할이 있습니다.
2. 탐색 메뉴에서 "태스크", "서비스"를 선택합니다.
3. "서비스 관리", "서비스 수정"을 차례로 클릭합니다.
검색 화면이 나타납니다.
4. 수정할 서비스를 검색합니다.
관리 권한이 있는 서비스를 모두 나열하는 목록을 표시하려면 검색 조건을 수정하지 않고 "검색"을 클릭합니다.

5. 서비스를 선택하고 "선택"을 클릭합니다.
확인 메시지가 표시됩니다.
6. "예"를 클릭합니다.
7. "제출"을 클릭합니다.
CA CloudMinder 가 변경 내용을 서비스에 적용합니다.

액세스 요청 및 보기에 검색 추가

"액세스 요청 및 보기" 태스크는 서비스 목록을 표시하지만 추가 서비스 검색을 위한 필드가 없습니다. 검색 필드를 추가하려면:

1. "역할 및 태스크", "관리자 태스크", "관리자 태스크 수정"을 선택합니다.
2. "액세스 요청 및 보기"를 찾습니다.
3. 서비스 카탈로그에서 태스크를 선택합니다.
4. "탭"을 클릭합니다.
5. 탭 아래에서 "액세스 관리"의 왼쪽에 있는 편집 아이콘을 클릭합니다.
6. "목록 화면" 줄에서 "찾아보기"를 클릭합니다.
7. 적절한 옵션을 구성하여 올바른 검색을 추가합니다.
8. 필요한 화면을 선택하고 "편집" 단추를 클릭하여 화면을 편집합니다.
9. "Configure Standard List Screen"(표준 목록 화면 구성)에서 '사용자가 검색을 수행할 필드 선택:' 섹션으로 이동합니다.
10. 검색 필드를 선택하고 검색 필드 이름을 구성합니다.
11. "확인"을 클릭하여 변경 내용을 저장합니다.

서비스 요청 기간 및 사용자 데이터와 같은 서비스 요청에 대한 정보가 서비스 요청 승인 워크플로 항목에 표시됩니다. 또한, AddServiceToUserEvent 정책 기반 워크플로를 "액세스 요청 및 보기" 태스크에 할당하는 경우 이 정보를 전자 메일로 받아 볼 수도 있습니다.

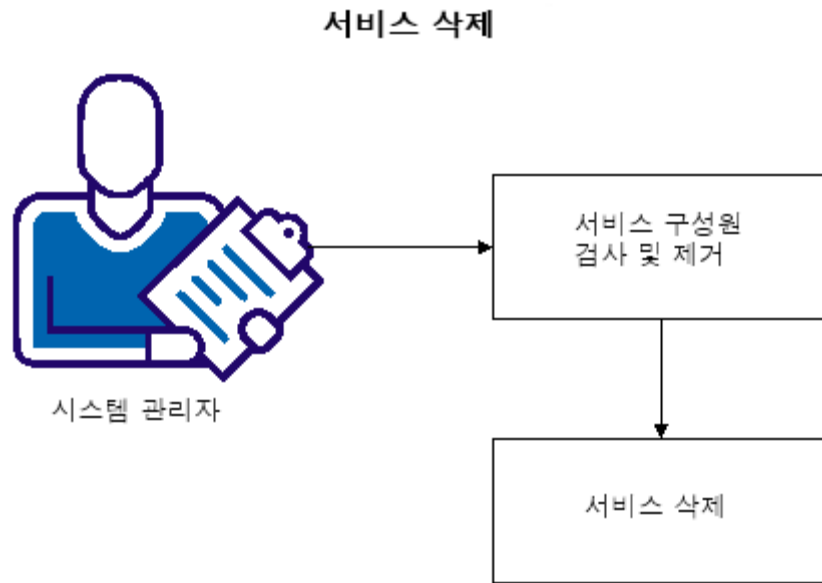
서비스 삭제

시스템 관리자가 서비스를 삭제할 수 있습니다. 삭제한 서비스는 시스템에서 완전히 제거됩니다.

사용자에게 서비스가 할당되어 있는 경우에는 해당 서비스를 삭제할 수 없습니다. 서비스를 삭제하기 전에 먼저 할당된 사용자 또는 **구성원**이 있는지 검사하여 모두 제거하십시오.

참고: 마찬가지로 서비스 구성원인 사용자도 삭제할 수 없습니다. 이 경우 먼저 서비스 구성원인 사용자를 제거한 다음 해당 사용자를 삭제하십시오.

다음 다이어그램에서는 서비스를 삭제하기 위해 이해해야 할 정보와 수행해야 할 단계를 보여 줍니다.



다음 항목에서는 서비스를 삭제하는 방법을 설명합니다.

1. [서비스 구성원 확인 및 제거](#) (페이지 263)
2. [서비스 삭제](#) (페이지 263)

서비스 구성원 확인 및 제거

서비스를 삭제하기 전에 먼저 기존 구성원이 있는지 검사하여 제거하십시오.

다음 단계를 수행하십시오.

1. 서비스 관리 권한이 있는 CA CloudMinder 계정에 로그인합니다.
예를 들어 환경의 첫 번째 사용자에게 "서비스 수정" 태스크를 가진 "시스템 매니저" 역할이 있습니다.
2. "태스크", "서비스", "액세스 요청 및 보기"를 차례로 선택합니다.
관리할 수 있는 서비스 목록이 나타납니다.
3. 삭제할 서비스를 선택하고 "선택"을 클릭합니다.
서비스에 할당된 사용자 목록이 나타납니다.
4. 서비스에 구성원이 있는 경우 모든 사용자 옆에 있는 확인란을 선택 해제합니다.
5. "변경 내용 저장"을 클릭합니다.
확인 메시지가 표시됩니다.
6. "예"를 클릭합니다.
CA CloudMinder 가 서비스에서 구성원을 제거합니다.

서비스 삭제

서비스 구성원이 없는 서비스를 삭제할 수 있습니다.

서비스를 삭제하려면

1. 서비스 관리 권한이 있는 계정으로 CA CloudMinder 에 로그인합니다.
예를 들어 환경의 첫 번째 사용자에게 "서비스 삭제" 태스크를 가진 "시스템 매니저" 역할이 있습니다.
2. 왼쪽 창에 있는 서비스로 이동하거나 태스크를 선택하여 서비스로 이동합니다.
3. "서비스 관리", "서비스 삭제"를 차례로 클릭합니다.
검색 화면이 나타납니다.

4. 삭제할 서비스를 검색합니다.

관리 권한이 있는 서비스를 모두 나열하는 목록을 표시하려면 검색 조건을 수정하지 않고 "검색"을 클릭합니다.

5. 서비스를 선택하고 "선택"을 클릭합니다.

확인 메시지가 표시됩니다.

6. "예"를 클릭합니다.

서비스가 삭제됩니다.

서비스에 대한 액세스 갱신

일부 서비스는 특정 기간이 지난 후에 만료됩니다. 관리자는 사용자 액세스가 중단되지 않도록 해당 사용자에 대한 서비스를 갱신할 수 있습니다.

다음 방법 중 하나로 서비스를 갱신할 수 있습니다.

- 서비스를 선택한 다음 갱신할 사용자 액세스 선택
- 사용자를 선택한 다음 갱신할 서비스 선택

참고: 환경을 구성한 방법에 따라 최종 사용자가 "액세스 갱신" 태스크를 사용하여 자신의 액세스를 갱신할 수도 있습니다.

다음 절차에서는 서비스를 먼저 선택하여 액세스를 갱신하는 방법을 설명합니다. 사용자를 먼저 선택하려면 "사용자" 범주에서 "사용자 액세스 요청", "사용자 갱신 요청 관리" 태스크를 사용하십시오.

다음 단계를 수행하십시오.

1. 사용자 콘솔에서 "서비스", "액세스 갱신"을 차례로 클릭합니다.
2. 갱신할 서비스를 검색하여 선택합니다.

선택한 서비스에 대한 액세스 권한을 현재 가지고 있는 사용자와 해당 사용자의 액세스가 만료되는 날짜를 나열하는 목록이 사용자 콘솔에 표시됩니다.

3. "액세스 요청" 열에서 갱신 기간을 선택하고 "확인"을 클릭합니다.
"기간" 필드에 있는 옵션은 서비스가 생성될 때 결정됩니다.
4. "변경 내용 저장"을 클릭합니다.

사용자 콘솔에서 "서비스 액세스 요청 기록 보기"를 사용하여 서비스 갱신 상태를 볼 수 있습니다.

제 11 장: 동기화

이 섹션은 다음 항목을 포함하고 있습니다.

[서버 사이에서 사용자 동기화](#) (페이지 267)

[사용자 생성 또는 수정 태스크에서 사용자 동기화](#) (페이지 270)

[동기화 태스크](#) (페이지 272)

서버 사이에서 사용자 동기화

회사 디렉터리와 프로비저닝 디렉터리의 사용자가 일치하는 데이터를 갖도록 Identity Manager 에서 동기화를 구성합니다. 이 두 디렉터리에서 변경 내용을 처리하기 위해 인바운드 및 아웃바운드 동기화를 구성합니다.

인바운드 동기화

인바운드 동기화는 CA Identity Manager 사용자에게 프로비저닝 디렉터리에서 발생한 최근 변경 내용을 지속적으로 업데이트합니다. 프로비저닝 디렉터리의 변경 내용에는 프로비저닝 서버에 대한 커넥터가 있는 시스템을 사용하여 수행된 변경 내용이 포함됩니다. 동기화는 관리 콘솔의 프로비저닝 화면에서 정의된 매핑을 사용합니다.

인바운드 동기화에 대한 장애 조치

대체 Identity Manager 서버 URL 로의 장애 조치는 URL 에 의해 명명된 응용 프로그램 서버가 실행 중이지 않은 경우에만 발생합니다. 응용 프로그램 서버가 실행 중이고 알림을 받지만 이후 구성 오류(알 수 없는 환경 또는 환경이 시작되지 않은 오류 등)가 발생하는 경우 이러한 오류로 인해 알림이 전달되지 않습니다. 인바운드 알림 기능이 올바르게 동작하려면 이러한 문제를 반드시 해결해야 합니다.

아웃바운드 동기화

아웃바운드 동기화는 Identity Manager 를 사용하여 프로비저닝 디렉터리에서 사용자를 만들고 업데이트하는 것과 관련이 있습니다.

프로비저닝 디렉터리 사용자 만들기

프로비저닝 디렉터리에서 사용자의 생성은 사용자에게 프로비저닝 역할을 할당하는 것과 같은 프로비저닝 관련 이벤트에 대해서만 발생합니다. 오직 사용자를 만드는 역할을 지정하는 관리자 태스크를 사용하는 경우에만 사용자가 프로비저닝 디렉터리에 생성됩니다.

참고: 프로비저닝 디렉터리 사용자를 전역 사용자라고도 합니다. 전역 사용자는 끝점 계정을 연결하는 단일 사용자입니다.

CA Identity Manager 에서의 사용자 생성이 프로비저닝 디렉터리에서의 사용자 생성을 트리거하는 경우 CA Identity Manager 는 프로비저닝 디렉터리에서 정의된 임시 암호가 포함된 전자 메일을 새 사용자의 전자 메일 주소로 전송합니다. 사용자는 해당 암호를 사용하여 사용자 콘솔에 로그인할 수 있지만, 로그인한 다음 반드시 암호를 변경해야 합니다. 따라서, 이 암호는 사용자 저장소와 프로비저닝 디렉터리 사이에서 동기화됩니다.

전자 메일 주소가 없는 사용자는 사용자 저장소에서 암호를 변경해야 사용자 콘솔에 액세스할 수 있습니다.

참고: 임시 암호를 전자 메일로 보내려면 전자 메일 알림이 "환경"에 대해 사용되고, `CreateProvisioningUserNotificationEvent` 가 전자 메일 알림에 대해 구성되어 있어야 합니다. 자세한 내용은 *Configuration Guide*(구성 안내서)를 참조하십시오.

Identity Manager 를 사용하여 전역 사용자 업데이트

사용자를 수정하는 관리자 태스크를 사용하는 경우 프로비저닝 디렉터리의 사용자에 대한 업데이트가 발생합니다. 전역 사용자가 없는 경우 동기화가 발생하지 않습니다.

아웃바운드 매핑은 Identity Manager 사용자 이벤트를 프로비저닝 디렉터리에 영향을 주는 아웃바운드 이벤트와 일치시킵니다.

Identity Manager User Event	Outbound Event
☐ DeleteUserEvent	POST_DELETE_GLOBAL_USER
☐ DisableUserEvent	POST_DISABLE_GLOBAL_USER
☐ EnableUserEvent	POST_ENABLE_GLOBAL_USER
☐ ModifyUserEvent	POST_MODIFY_GLOBAL_USER
☐ ResetPasswordEvent	POST_CHANGE_GLOBAL_USER_PWD

사용자가 프로비저닝 디렉터리에는 있지만 Identity Manager 에는 없는 경우 사용자 콘솔에서 해당 사용자를 만들 수 있습니다. 생성 태스크에 대한 특성을 매핑했고 사용자가 동일한 사용자 ID 를 갖는 경우, 프로비저닝 사용자에게 대한 특성이 프로비저닝 디렉터리에서 업데이트됩니다. 이제 Identity Manager 에서 해당 사용자를 관리할 수 있습니다.

참고: 이벤트가 사용자 특성을 업데이트하고 이 값을 CA Identity Manager 로 동기화하려는 경우 아웃 바운드 이벤트 POST_MODIFY_GLOBAL_USER 로 이벤트를 매핑해야 합니다.

Identity Manager 를 사용하여 전역 사용자 삭제

기본적으로, 아웃바운드 동기화는 "사용자 삭제" 이벤트에 대해 구성됩니다. Identity Manager 에서 사용자를 삭제하면 이 사용자는 프로비저닝 디렉터리와 모든 끝점 계정에서도 삭제됩니다.

CA Identity Manager 가 관리 계정에서 사용자의 계정을 삭제할 수 없는 경우, 나머지 계정에서는 사용자가 삭제되지만 프로비저닝 디렉터리에서는 삭제되지 않습니다.

예를 들어, 사용자 A 에게 프로비저닝 서버에서 관리되는 UNIX 계정과 Exchange 계정이 하나씩 있다고 가정합니다. 사용자 A 가 Identity Manager 에서 삭제되면 프로비저닝 서버는 이 사용자 계정을 삭제하려고 시도합니다. 통신 오류로 인해 프로비저닝 서버가 Exchange 계정을 삭제하지 못하면 사용자 A 의 UNIX 계정을 삭제하지만 프로비저닝 디렉터리에서 이 사용자를 삭제하지 않습니다. 하지만 사용자 A 는 사용자 저장소에서 복원되지 않습니다.

암호 동기화 사용

프로비저닝 서버는 Identity Manager 사용자와 관련 끝점 사용자 계정 사이에서 암호를 동기화할 수 있게 해 줍니다. 끝점에서 시작된 변경 사항을 가능하게 하려면 두 가지 구성이 필요합니다.

- 끝점은 끝점에서 시작된 변경 사항을 캡처하고 이 변경 사항을 프로비저닝 서버로 전달하도록 구성되어야 합니다.

참고: 암호 동기화를 위해 끝점을 구성하는 방법에 대한 자세한 내용은 *CA CA Identity Manager 관리 안내서*를 참조하십시오.

- "Enable Password Synchronization Agent"(암호 동기화 에이전트 사용) 특성이 전역 사용자에게 활성화되어 있어야 합니다.

암호 동기화를 사용하려면

1. 관리 콘솔에서 "Advanced Settings"(고급 설정), "Provisioning"(프로비저닝)을 선택합니다.
2. "Enable Password Changes from Endpoint Accounts"(끝점 계정에서 암호 변경 사용)를 선택합니다.
3. "저장"을 클릭합니다.
4. 응용 프로그램 서버를 다시 시작합니다.

사용자 생성 또는 수정 태스크에서 사용자 동기화

사용자를 생성 또는 수정하는 태스크의 프로필 탭에서 동기화 컨트롤은 Identity Manager에 대한 변경 사항이 전역 사용자에게도 반영되도록 합니다. 사용자를 생성 또는 수정하는 관리자 태스크를 만들고 있으며 ID 정책이 있는 경우 동기화 컨트롤을 다음과 같이 설정하십시오.

- "사용자 동기화"를 "태스크 완료 시"로 설정합니다.
- "계정 동기화"를 "태스크 완료 시"로 설정합니다.

참고: 최상의 성능을 얻으려면 "태스크 완료 시" 옵션을 선택하십시오. 그러나 여러 이벤트가 포함된 태스크에 대해 "태스크 완료 시" 옵션을 선택하면 태스크의 모든 이벤트가 완료될 때까지 **Identity Manager**가 동기화하지 않습니다. 워크플로 승인이 필요한 이벤트가 하나 이상 있는 경우 모든 이벤트가 완료되는 데 며칠이 걸릴 수 있습니다. 모든 이벤트가 완료될 때까지 **Identity Manager**가 ID 정책을 적용하거나 계정을 동기화하지 않고 대기하는 것을 방지하려면 "모든 이벤트 발생 시" 옵션을 선택하십시오.

사용자를 관리하는 관리자 태스크에 특성을 추가하려면 관리 콘솔의 프로비저닝 화면에서 "특성 매핑"을 업데이트해야 합니다. **Identity Manager**의 각 사용자 특성에는 기본 프로비저닝 특성이 있습니다.

User Attribute	Provisioning Attribute
☐ %ADMIN_ROLE_CONSTRAINT%	%ADMIN_ROLE_CONSTRAINT%
☐ %EMAIL%	%EMAIL%
☐ %ENABLED_STATE%	%ENABLED_STATE%
☐ %FIRST_NAME%	%FIRST_NAME%
☐ %FULL_NAME%	%FULL_NAME%
☐ %IDENTITY_POLICY%	%IDENTITY_POLICY%
☐ %LAST_NAME%	%LAST_NAME%
☐ %PASSWORD%	%PASSWORD%
☐ %PASSWORD_DATA%	%PASSWORD_DATA%
☐ %USER_ID%	%USER_ID%

동기화 태스크

다음과 같은 유형의 동기화를 수행할 수 있습니다.

사용자 동기화

각 사용자가 적절한 관리 끝점에서 필요한 계정을 가지고 있고 각 계정이 사용자의 프로비저닝 역할에 의해 호출된 대로 적절한 계정 템플릿에 할당되도록 합니다.

계정 동기화

계정의 기능 특성 값이 계정의 할당된 계정 템플릿에 표시된 대로 적절한 값이 되도록 합니다. 계정 동기화는 강하거나 약할 수 있습니다. 약한 동기화는 계정 기능 특성이 적어도 계정 템플릿에 필요한 최소 기능을 포함하도록 합니다. 강한 동기화는 계정 기능 특성이 계정 템플릿에 필요한 정확한 기능을 포함하도록 합니다. **"Strong Synchronization"**(강한 동기화) 확인란이 선택된 하나 이상의 계정 템플릿에 계정이 속하는 경우 강한 계정 동기화가 됩니다.

"사용자 동기화"를 제어하는 관련 **"Strong Synchronization"**(강한 동기화) 확인란은 없지만 유사한 개념이 존재합니다. 사용자에게 대해 "사용자를 역할과 동기화" 메뉴 항목을 실행하면 다음 두 개의 동기화 옵션이 제공됩니다.

- 누락된 계정과 계정 템플릿 할당을 추가합니다.
- 불필요한 계정과 계정 템플릿 할당을 삭제합니다.
- "추가" 확인란만 선택(약한 계정 동기화와 유사)하는 것은 전역 사용자가 자신에게 할당된 프로비저닝 역할에 필요한 최소한의 계정을 모두 가지고 있도록 하는 것이지만 실제로는 사용자가 현재 프로비저닝 역할에서 미리 지정되지 않은 추가 계정을 가질 수 있습니다.

프로비저닝 역할이 사용자에게 필요한 계정을 정확히 정의하도록 하려면 "추가" 및 "삭제" 확인란을 모두 선택(강한 계정 동기화와 유사)하십시오. 모든 추가 계정은 삭제됩니다.

얼마나 정확하게 프로비저닝 역할이 정의되는지에 따라 약한/강한 계정 동기화 또는 약한/강한 사용자 동기화를 선택하십시오. 사용자가 명확히 정의된 프로비저닝 역할(계정 액세스가 이러한 역할과 연결됨)에 적합한 경우 강한 동기화를 사용할 수 있습니다.

참고: 일부 끝점 유형은 기본적으로 강한 동기화로 설정되어 있습니다. 자세한 내용은 *Connectors Guide*(커넥터 안내서)를 참조하십시오.

사용자 동기화 및 계정 동기화는 따로 수행해야 하는 별도의 태스크입니다. 일반적으로, 모든 필요한 계정이 생성되도록 사용자 동기화를 먼저 수행한 다음 프로비저닝 서버가 계정 특성의 값을 할당 또는 변경하도록 계정 동기화를 나중에 수행합니다.

프로비저닝 서버는 개체에 대해 다음과 같이 두 가지 동기화 메뉴 집합을 제공합니다.

- 동기화 검사 메뉴 옵션은 동기화를 검사하고 프로비저닝 역할 또는 계정 템플릿을 준수하지 않는 계정의 목록을 반환합니다.
- 동기화 메뉴 옵션은 전역 사용자를 이 사용자의 프로비저닝 역할과 동기화하고, 계정을 이 계정의 계정 템플릿과 동기화합니다.

동기화 검사 기능을 먼저 수행하면 프로비저닝 서버는 동기화 기능이 수행할 수정 조치에 대한 정보를 표시합니다. 동기화 검사 기능이 문제점을 찾지 못하면 동기화 기능이 실행되지 않습니다.

사용자가 동기화되지 않는 이유

사용자가 프로비저닝 역할 또는 계정 템플릿과 동기화되지 않는 일부 이유는 다음과 같습니다.

- 네트워크에서 하드웨어 또는 소프트웨어 문제로 인해 필요한 계정을 만들려는 앞의 시도가 실패했고, 이로 인해 누락된 계정이 발생합니다.
- 프로비저닝 역할 및 계정 템플릿이 변경되었고, 이로 인해 불필요한 또는 누락된 계정이 발생합니다.
- 계정이 생성된 후에 계정 템플릿에 할당되었으므로 계정 템플릿과 동기화되지 않은 계정이 존재합니다.
- 계정이 나중에 생성되도록 지정되었기 때문에 새 계정의 생성이 지연되었습니다.
- 새 끝점이 획득되었습니다. 탐색 및 상관 관계 지정 중에 프로비저닝 서버가 사용자에게 프로비저닝 역할을 자동으로 할당하지 않으므로 새 끝점에서 계정을 가지고 있어야 하는 사용자를 나타내도록 역할을 업데이트해야 합니다. 사용자와의 상관 관계가 지정된 모든 계정은 사용자가 동기화될 때 불필요한 계정으로 나열됩니다.

- 계정을 사용자에게 복사하는 방식으로 기존 계정이 사용자에게 할당되어, 수동 상관 관계가 지정되었으며 불필요한 계정이 설정되었습니다.
- 사용자를 역할에 할당하는 방법이 아닌 다른 방법에 의해 사용자에게 계정이 생성되었습니다. 예를 들어 사용자를 해당 사용자의 프로비저닝 역할에 없는 계정 템플릿에 복사하는 경우 이 계정은 불필요한 계정으로 나열되거나 불필요한 계정 템플릿이 있는 계정으로 나열됩니다. 끝점의 기본 계정 템플릿을 사용하여 계정을 만들기 위해 사용자를 끝점에 복사하는 경우 이 계정은 불필요한 계정이 될 수 있습니다.

사용자 동기화

사용자 동기화는 사용자에게 할당된 프로비저닝 역할을 준수하도록 계정을 생성, 업데이트 또는 삭제합니다. 따라서, 만약 관리자가 기본 도구를 사용하여 관리 끝점에서 계정을 추가 또는 삭제하고, 끝점을 최근에 다시 탐색하여 프로비저닝 디렉터리를 업데이트하지 않은 경우 실제로 사용자에게 불필요한 또는 누락된 계정이 있음에도 불구하고 "사용자 동기화"에는 아무런 문제가 없는 것으로 표시될 수 있습니다.

사용자를 역할과 동기화

사용자에 대한 동기화를 검사하여 불필요한 계정 또는 계정 템플릿과 누락된 계정을 나열할 수 있습니다. 사용자를 역할과 동기화하도록 요청하는 경우 프로비저닝 서버는 사용자가 개인의 프로비저닝 역할에 필요한 계정을 모두 가지고 있고 각 계정이 올바른 계정 템플릿에 속하도록 합니다.

- 이 태스크를 수행하는 경우 확인란을 선택하여 끝점에 계정을 만들 수 있습니다. 사용자의 프로비저닝 역할에 있는 둘 이상의 계정 템플릿이 동일한 계정을 미리 지정하는 경우 이 계정은 모든 관련 계정 템플릿을 병합하여 생성됩니다.
- 사용자를 역할과 동기화하는 동안 불필요한 계정을 삭제하는 옵션을 사용할 수 있습니다. 사용자가 자신의 프로비저닝 역할에 필요한 계정이 아닌 다른 계정이 필요한 타당한 이유가 있는지 판단하십시오. 타당한 이유가 있는 경우 이 삭제 옵션을 선택해서는 안 됩니다.

삭제되는 계정이 계정 삭제가 비활성화된 관리 끝점에 있는 경우 이 계정은 실제로 삭제되지 않습니다.

계정 만들기

프로비저닝 역할에 계정 템플릿이 포함되고 계정 템플릿이 끝점과 연결되므로 사용자는 올바른 계정 특성과 함께 각 끝점에 나열된 계정을 가지고 있어야 합니다.

이 태스크를 수행하는 경우 확인란을 선택하여 끝점에 계정을 만들 수 있습니다. 사용자의 프로비저닝 역할에 있는 둘 이상의 계정 템플릿이 동일한 계정을 미리 지정하는 경우 이 계정은 모든 관련 계정 템플릿을 병합하여 생성됩니다.

이 계정은 이러한 계정 템플릿에 할당되었는데, 이 템플릿은 현재 계정과 동기화되어 있지 않습니다. 새로 생성된 계정에는 계정 동기화가 필요 없습니다.

계정을 삭제합니다.

사용자를 역할과 동기화하는 동안 불필요한 계정을 삭제하는 옵션을 사용할 수 있습니다. 사용자가 자신의 프로비저닝 역할에 필요한 계정이 아닌 다른 계정이 필요한 타당한 이유가 있는지 판단하십시오. 타당한 이유가 있는 경우 이 삭제 옵션을 선택해서는 안 됩니다.

삭제되는 계정이 계정 삭제가 비활성화된 관리 끝점에 있는 경우 이 계정은 실제로 삭제되지 않습니다.

계정에 계정 템플릿 추가

계정에 하나 이상의 계정 템플릿 할당이 누락된 경우 사용자를 계정 템플릿과 동기화하면 기존 계정이 해당 계정 템플릿에 할당됩니다. 계정이 하나 이상의 새 계정 템플릿에 할당된 경우, 계정 동기화가 자동으로 실행되어 계정의 기능 특성을 계정 템플릿에 의해 지정된 기능으로 업데이트합니다.

사용자를 계정 템플릿과 동기화하는 경우 계정 업데이트 후 계정이 계정 템플릿과 동기화되어 있을 수도 있고 동기화되어 있지 않을 수도 있습니다. 추가된 계정 템플릿 중 하나가 강한 동기화 계정 템플릿이거나 둘 이상의 계정 템플릿이 계정에 추가된 경우 사용자를 역할과 동기화하면 계정에 대한 전체 계정 동기화가 시작됩니다. 하지만 하나의 약한 동기화 계정 템플릿만 추가된 경우 사용자를 계정 템플릿과 동기화하면 이 하나의 계정 템플릿만 포함하는 계정 동기화가 시작됩니다. 계정이 이 업데이트 이전에 다른 계정 템플릿과 동기화되지 않은 경우 그 후에도 계정이 계속 동기화되지 않았을 수 있습니다.

계정에서 계정 템플릿 제거

사용자를 역할과 동기화하는 태스크는 계정에서 불필요한 계정 템플릿을 제거할 때도 사용할 수 있습니다. 삭제 옵션을 선택하는 경우에만 이 작업을 수행할 수 있습니다. 사용자 동기화가 하나 이상의 불필요한 계정 템플릿을 제거하기 위해 계정을 업데이트해야 한다고 결정하는 경우, 계정 동기화가 계정에 대해 자동으로 실행되어 기능 특성을 계정에 남아 있는 계정 템플릿과 동기화합니다.

계정에서 계정 템플릿을 제거할 때 발생하는 이 계정 동기화는 나머지 계정 템플릿 중 하나가 강한 동기화로 표시된 경우 강한 동기화를 사용하고, 나머지 계정 템플릿 모두가 약한 동기화로 표시된 경우 약한 동기화를 사용합니다.

약한 동기화 또는 강한 동기화가 사용되는지 여부는 계정 템플릿이 계정에 할당될 때 앞에서 부여된 계정 기능이 계정 템플릿이 나중에 제거될 때 무효화될지 여부에 영향을 줍니다. 강한 동기화를 사용하는 경우, 그룹 구성원 자격 또는 더 높은 할당량 같은 계정 템플릿에 의해 부여된 기능은 계정에 남아 있는 어떠한 계정 템플릿에도 해당 기능을 규정하지 않으면 무효화(그룹 구성원 자격이 제거되거나 할당량이 낮아짐)됩니다. 하지만 약한 동기화를 사용하는 경우, 프로비저닝 서버가 주문형 추가 기능과 계정 템플릿을 통해 부여된 기능을 구분하지 않으므로 일반적으로 계정이 변경되지 않습니다.

SyncRemoveValues 특성으로서 지정된, 일부 다중 값을 갖는 기능 특성은 이 규칙에서 예외입니다. 계정에 할당된 여러 값을 나타내는, 다중 값을 갖는 단순한 특성은 일반적으로 **SyncRemoveValues** 특성으로서 나열됩니다. 이러한 특성의 경우 계정에서 계정 템플릿을 제거할 때 발생하는 약한 동기화 동작은 제거되는 계정 템플릿에 의해 규정되는 값이 나머지 계정 템플릿 중 하나에 의해서도 규정되지 않는 한 이 값을 제거합니다.

예를 들어 각 계정 템플릿을 만들어, 각 계정 템플릿이 고유한 그룹 구성원 자격을 계정에 할당하도록 하는 경우, 이 **SyncRemoveValues** 기능은 특정 계정 템플릿이 필요 없도록 전역 사용자의 프로비저닝 역할을 변경하여 계정이 해당 계정 템플릿에 의해 규정되는 그룹에 더 이상 속하지 않도록 계정을 업데이트합니다. 계정 템플릿에 규정된 것을 초과하여 계정에 주어진 그룹 구성원 자격이 유지되므로 이 기능은 강한 동기화와 정확히 동일하지는 않습니다.

모든 단일 값 특성 및 **SyncRemoveValues** 특성으로 지정되지 않은 일부 다중 값 특성의 경우, 약한 동기화 동작은 (계정에서 계정 템플릿을 제거하기는 하지만) 일반적인 약한 동기화 동작과 동일합니다(기능이 제거되지 않음).

약한 동기화에 의해 기능이 제거되지 않도록 하려면 도메인 구성 매개 변수 **"Synchronize/Remove Account Template Values from Accounts"**(계정에서 계정 템플릿 값 동기화/제거)를 **"No"**로 설정하여 **SyncRemoveValues** 기능을 비활성화하십시오.

계정 템플릿 동기화

계정 템플릿의 변경 내용은 다음과 같이 기존 계정에 영향을 줍니다.

- 기능 특성 값을 변경하면 필요한 경우 해당 계정 특성이 업데이트되어 계정 템플릿 특성 값과 동기화됩니다. 약한 동기화와 강력한 동기화에 대한 설명을 참조하십시오.
- 특정 계정 특성은 계정 템플릿 변경 사항에서 업데이트되지 않으므로 커넥터에 의해 지정됩니다. 예를 들면 계정을 만드는 동안 끝점 유형만 설정할 수 있도록 허용하는 특정 특성, 암호 특성 등입니다.

업데이트된 특성

계정 템플릿에서 기능 특성을 변경할 때 계정의 해당 특성이 변경됩니다. 이 변경은 계정의 특성에 영향을 줍니다. 이 영향은 다음과 같은 요인에 기초합니다.

- 계정 템플릿이 약한 동기화 또는 강력한 동기화를 사용하도록 정의되었는지 여부
- 계정이 여러 계정 템플릿에 속하는지 여부

약한 동기화

약한 동기화를 사용하면 사용자의 계정이 최소 기능 특성을 가지게 됩니다. 약한 동기화는 대부분의 끝점 유형에서 기본값입니다. 약한 동기화를 사용하는 템플릿을 업데이트하는 경우 CA Identity Manager 는 다음과 같이 기능 특성을 업데이트합니다.

- 숫자 필드가 계정 템플릿에서 업데이트되고 새 숫자가 계정의 숫자보다 크면 CA Identity Manager 에서 계정의 값을 변경하여 새 숫자와 일치시킵니다.
- 계정 템플릿에서 확인란을 선택하지 않았는 데 이후에 이 확인란을 선택하면 CA Identity Manager 에서 이 확인란이 선택되지 않은 계정의 확인란을 업데이트합니다.
- 목록이 계정 템플릿에서 변경되면 CA Identity Manager 에서 모든 계정을 업데이트하여 계정의 값 목록에 포함되지 않은 새 목록의 값을 포함합니다.

계정이 다른 계정 템플릿에 속하면(해당 템플릿에서 약한 동기화를 사용하든지 강력한 동기화를 사용하든지) CA Identity Manager 에서는 변경 중인 템플릿만 참조합니다. 이 동작은 모든 계정 템플릿을 검사하는 것보다 효율적입니다. 약한 동기화는 기능을 계정에만 추가하므로, 일반적으로 다른 계정 템플릿을 참조할 필요가 없습니다.

참고: 약한 동기화 계정 템플릿에서 전파할 때 기능을 제거하거나 낮추는 변경 사항은 일부 계정을 동기화하지 않은 상태로 둘 수 있습니다. 약한 동기화를 사용할 경우 기능은 제거되거나 낮춰지지 않습니다. 계정에 대한 다른 템플릿을 참조할 경우 약한 동기화로 충분하면 전파는 고려되지 않습니다.

이 경우 "사용자를 계정 템플릿과 동기화"를 사용하여 계정을 해당 계정 템플릿과 동기화합니다.

강한 동기화

강한 동기화는 계정 템플릿에 정의된 대로 계정에 정확한 계정 특성이 있는지 확인합니다.

예를 들어, 기존 UNIX 계정 템플릿에 그룹을 추가한다고 가정합니다. 원래 계정 템플릿은 **Staff** 그룹의 계정 구성원을 만들었습니다. 이제, **Staff** 및 **System** 그룹 모두의 계정 구성원을 만들려고 합니다. 각 계정이 **Staff** 및 **System** 그룹의 구성원(그리고 다른 그룹의 구성원이 아님)일 때 계정 템플릿과 관련된 모든 계정이 동기화되었다고 간주됩니다. **Staff** 그룹에 없는 모든 계정은 두 그룹 모두에 추가됩니다.

고려해야 할 일부 다른 요인은 다음 상황을 포함합니다.

- 계정 템플릿이 강한 동기화를 사용하는 경우, **Staff** 및 **System** 을 제외하고 그룹에 속하는 모든 계정이 이러한 추가 그룹에서 제거됩니다.
- 계정 템플릿이 약한 동기화를 사용하는 경우, 계정이 **Staff** 및 **System** 그룹에 추가됩니다. 정의된 추가 그룹이 있는 모든 계정은 이러한 그룹의 구성원으로 남아 있습니다.

참고: 계정이 계정 템플릿과 동기화 상태를 유지할 수 있도록 템플릿과 계정을 정기적으로 동기화하십시오.

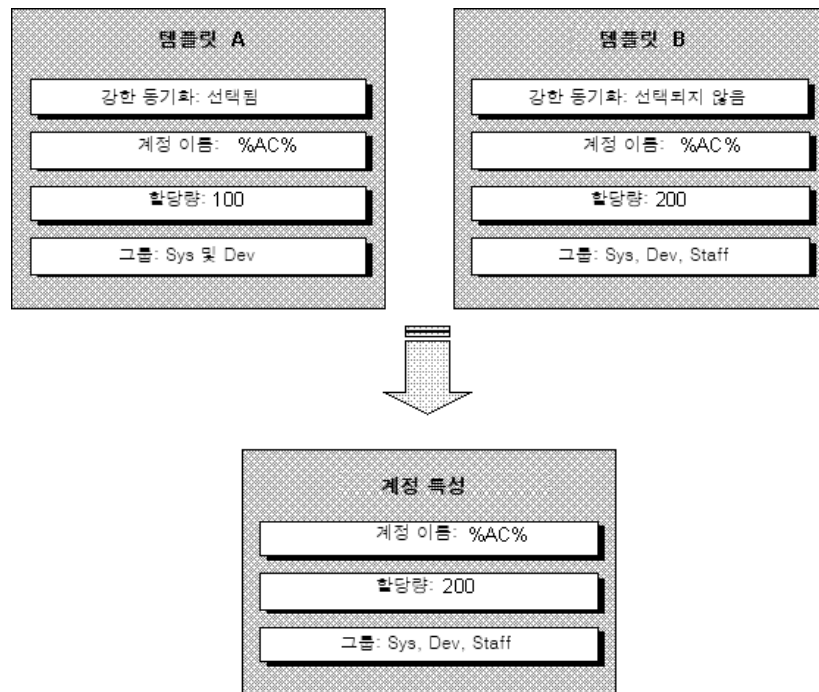
여러 템플릿이 있는 계정

동기화는 계정이 여러 계정 템플릿에 속하는지 여부에 영향을 받습니다. 계정에 단 하나의 계정 템플릿만 있고, 이 템플릿이 강한 동기화를 사용한다면 각 특성은 계정 템플릿 특성 값이 평가하는 것과 동일하게 일치하도록 업데이트됩니다. 결과는 특성이 초기 특성인 경우와 동일합니다.

사용자가 여러 프로비저닝 역할에 속하고, 각 역할이 동일한 관리 끝점에 대한 일부 액세스 수준을 규정하는 경우와 같이, 계정은 여러 계정 템플릿에 속할 수 있습니다. 이 경우, **CA Identity Manager** 는 개별 계정 템플릿의 하위 기능 집합을 규정하는 하나의 유효한 계정 템플릿으로 이러한 계정 템플릿을 결합합니다. 이 계정 템플릿은 개별 계정 템플릿이 약하거나 강한 동기화이거나 개별 계정 템플릿 중 하나가 강한 동기화인 경우 약한 동기화를 사용한다고 간주됩니다.

참고: 회사의 역할이 사용자가 필요로 하는 액세스를 완전히 정의하는지 여부에 따라 하나의 계정을 제어하는 계정 템플릿에 대해 약한 동기화만 사용하거나 강한 동기화만 사용하는 것이 일반적입니다. 사용자에게 적합한 역할이 명확하지 않고 사용자의 계정에 추가 기능을 부여하는 융통성이 필요한 경우 약한 동기화를 사용하십시오. 사용자가 필요로 하는 액세스를 정확히 지정하여 정의할 수 있으면 강한 동기화를 사용하십시오.

다음 예제는 여러 계정 템플릿이 하나의 유효한 계정 템플릿으로 통합되는 방법을 설명합니다. 이 예제에서 하나의 계정 템플릿이 약한 동기화로 표시되었고 다른 하나는 강한 동기화로 표시되었습니다. 따라서, 두 계정 템플릿을 결합하여 생성된 유효한 계정 템플릿은 강한 동기화 계정 템플릿처럼 처리됩니다. 정수 **Quota** 특성은 두 개의 계정 템플릿에서 더 큰 값을 취하고, 다중 값 **Groups** 특성은 두 정책 값의 합집합을 취합니다.



새 계정 전용 특성

계정 템플릿에서 일부 특성은 계정을 만들 때만 적용됩니다. 예를 들어, 암호 특성은 새 계정의 암호를 정의하는 규칙 식이며, 이 규칙 식은 계정의 암호를 업데이트하지 않습니다. 암호 규칙 식에 대한 변경 사항은 규칙 식이 설정된 후 생성된 계정에만 적용됩니다.

마찬가지로 읽기 전용 계정 특성에 대한 템플릿 규칙 식은 규칙 식이 설정된 후 생성된 계정에만 적용됩니다. 이러한 식을 변경해도 기존 계정에는 적용되지 않습니다.

계정 동기화

계정 동기화는 기능 특성을 업데이트하여 계정이 계정 템플릿으로 지정된 기능을 가지고 있도록 합니다. 이 동기화는 계정의 초기 특성에 영향을 주지 않습니다.

계정 템플릿의 기능 특성 변경 내용을 해당 계정과 동기화하려면 이 섹션에서 설명한 동기화 메뉴 옵션 중 하나를 사용하십시오.

계정 동기화 검사

끝점과 사용자에 대한 계정 동기화를 검사할 수 있습니다. 이 동작은 계정 템플릿을 준수하지 않는 계정의 목록을 나열합니다. 다음 표는 각 끝점에서 계정의 동기화를 검사할 때 어떤 일이 발생하는지 설명합니다.

개체	동기화
끝점	끝점의 각 계정에 대한 계정 특성을 동기화하고 이 특성이 관련 계정 템플릿을 준수하는지 확인합니다.
전역 사용자	각 사용자의 계정에 대한 계정 특성을 동기화하고 이 특성이 관련 계정 템플릿을 준수하는지 확인합니다.

계정 동기화

끝점, 사용자 및 계정 템플릿에 대한 계정 동기화를 수행할 수 있습니다.
다음 표는 각 개체에 대한 계정 동기화의 영향을 나열합니다.

개체	동기화
끝점	관련 계정 템플릿으로 끝점에 있는 각 계정을 동기화합니다.
전역 사용자	관련된 각 전역 계정 템플릿으로 전역 사용자의 각 계정을 동기화합니다.

제 12 장: 워크플로

이 섹션은 다음 항목을 포함하고 있습니다.

[워크플로 개요](#) (페이지 283)

[워크플로 제어 - 템플릿 방법 사용](#) (페이지 287)

[WorkPoint 방법을 사용하는 방법](#) (페이지 308)

[Workpoint 작업 보기](#) (페이지 342)

[정책 기반 워크플로](#) (페이지 345)

[온라인 요청](#) (페이지 365)

[워크플로 동작 단추](#) (페이지 369)

[작업 목록 및 작업 항목](#) (페이지 374)

워크플로 개요

CA Identity Manager 워크플로 기능을 사용하면 워크플로 프로세스에서 CA Identity Manager 작업을 제어할 수 있습니다. *워크플로 프로세스*는 CA Identity Manager가 워크플로 제어 하의 태스크를 완료하기 전에 수행해야 하는 하나 이상의 단계입니다. *작업*은 워크플로 프로세스의 런타임 인스턴스입니다.

*WorkPoint Designer*는 CA Identity Manager와 통합되는 Planet Group, Inc.의 자회사인 Workpoint LLC에서 제작한 소프트웨어입니다. WorkPoint Designer를 사용하여 워크플로 프로세스와 워크플로 작업을 관리할 수 있습니다.

워크플로 프로세스는 직원 사용자 계정 만들거나 수정과 같은 일부 비즈니스 작업을 완료하기 위해 수행해야 하는 하나 이상의 단계(*활동*이라고 함)로 구성됩니다. 일반적으로 워크플로 프로세스에는 권한 있는 사용자 또는 참여자가 작업을 승인하거나 거부해야 하는 하나 이상의 수동 활동이 포함되어 있습니다.

*참여자*는 워크플로 활동을 수행할 권한이 있는 사람입니다. CA Identity Manager에서는 참여자가 워크플로에서 제어되는 태스크를 승인하거나 거부해야 하므로 *승인자*라고도 합니다. *참여자 해결 프로그램*은 참여자가 누구인지 결정하기 위한 규칙 또는 조건 세트입니다.

워크플로의 개별 수동 활동을 CA Identity Manager 에서 *작업 항목*이라고 합니다.

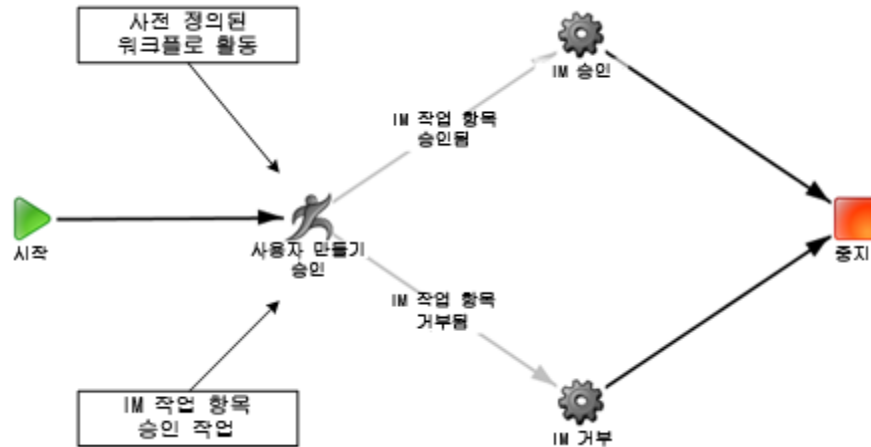
작업 목록은 태스크 승인 권한이 있는 참여자의 사용자 콘솔에 표시되는 승인 태스크 또는 *작업 항목*의 워크플로에서 생성된 목록입니다.

WorkPoint 프로세스 다이어그램

일반적으로 CA Identity Manager 태스크는 CA Identity Manager 이벤트를 트리거합니다. 예를 들어, 사용자를 만들려면 관리자는 "사용자 만들기" 작업을 선택합니다. 이 작업이 시작되면 CreateUserEvent 이벤트가 트리거됩니다.

다음 다이어그램은 WorkPoint Designer 에 표시되는 단순한 워크플로 프로세스(미리 정의된 CreateUserApproveProcess 프로세스)의 예입니다. 이 프로세스는 "사용자 만들기" 작업이 워크플로 제어 하에 있을 경우 CreateUserEvent 에 의해 호출됩니다.

이 프로세스에는 동일한 이름을 가진 CA Identity Manager 워크플로 승인 태스크에 해당하는 수동 활동인 "사용자 만들기 승인"이 포함됩니다. 워크플로 제어 하의 태스크가 완료될 때까지 실행되려면 참여자가 주로 사용자 콘솔에서 단추를 클릭하여 승인 태스크를 승인하거나 거부해야 합니다.



워크플로 및 전자 메일 통보

태스크를 시작하면 CA CA Identity Manager 가 처리를 위해 태스크를 제출하고 다음과 같은 승인 메시지를 표시합니다.

확인: 태스크가 완료되었습니다.

그러나 태스크에 워크플로 제어가 적용되고 승인이 필요한 경우 메시지는 다음과 같습니다.

알림: 태스크가 보류 중입니다.

화면 메시지 외에도 CA CA Identity Manager 는 다음과 같은 경우 자동으로 전자 메일 알림을 생성할 수 있습니다.

- 워크플로 승인자의 승인이나 거부가 필요한 이벤트 또는 작업이 보류 중인 경우
- 승인자가 이벤트 또는 작업을 승인하는 경우
- 승인자가 이벤트 또는 작업을 거부하는 경우
- 이벤트 또는 작업이 완료된 경우

추가 정보:

[전자 메일 알림](#) (페이지 389)

WorkPoint 설명서

워크플로 개념에 대한 일반 정보와 WorkPoint Designer 의 워크플로 프로세스, 활동 및 작업에 대한 지침은 WorkPoint 설명서를 참조하십시오. 이렇게 하려면 다음 HTML 페이지를 엽니다.

`admin_tools\WorkPoint\docs\designer\default.htm`

admin_tools

CA Identity Manager 관리 도구의 설치 디렉터리를 정의합니다. 기본 설치 디렉터리는 다음과 같습니다.

- **Windows:** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools

참고: Workpoint 는 CA CA Identity Manager 와 함께 설치되는 타사 제품입니다. CA CA Identity Manager 는 WorkPoint 기능의 하위 집합을 지원합니다. 예를 들어 CA CA Identity Manager 는 WpConsole 을 지원하지 않습니다. 하지만 WorkPoint 설명서에는 제품의 모든 기능이 설명되어 있습니다. Workpoint 설명서 중 일부는 CA CA Identity Manager 사용자에게 해당되지 않습니다.

워크플로 제어 방법

CA Identity Manager 는 태스크에 워크플로 제어를 적용하는 두 가지 방법을 제공합니다.

템플릿 방법

CA Identity Manager 에는 태스크에 워크플로 제어를 적용하는 데 사용할 수 있는 워크플로 프로세스 템플릿이 포함되어 있습니다. *템플릿 방법*을 사용하면 이러한 템플릿을 통해 완전히 사용자 콘솔 내에서 워크플로를 구성하고 관리할 수 있습니다. CA Identity Manager r12 에 도입된 이러한 일반 프로세스 템플릿을 구성하여 대부분의 CA Identity Manager 태스크와 이벤트를 제어할 수 있습니다.

템플릿 방법은 다음과 같은 새로운 기능을 허용합니다.

- 작업 수준 및 이벤트 수준 워크플로 제어
- 워크플로 승인자에 대한 단순한 참여자 해결 프로그램 구성
- 다른 사용자가 작업 항목을 승인하도록 사용자가 위임할 수 있도록 하여 "부재 중" 시나리오를 처리하는 작업 항목 위임
- 승인을 위해 실행 중인 태스크를 다른 사용자에게 재할당할 수 있도록 하는 작업 항목 재할당

WorkPoint 방법

CA Identity Manager 에는 특정 CA Identity Manager 태스크에 해당하는 기본 이벤트 매핑이 있는 미리 정의된 워크플로 프로세스 세트도 포함되어 있습니다. *WorkPoint* 방법을 사용하는 경우 *WorkPoint Designer* 내에서 이러한 프로세스를 구성하고 사용자 지정해야 합니다. 미리 정의된 프로세스는 CA Identity Manager r12 이전 릴리스와 호환됩니다.

또한 *WorkPoint* 방법을 통해 다음 새 기능을 사용할 수 있습니다.

- 작업 수준 및 이벤트 수준 워크플로 제어
- 다른 사용자가 작업 항목을 승인하도록 사용자가 위임할 수 있도록 하여 "부재 중" 시나리오를 처리하는 작업 항목 위임
- 승인을 위해 실행 중인 태스크를 다른 사용자에게 재할당할 수 있도록 하는 작업 항목 재할당

참고: 가능한 경우 유연성을 높이고 사용하기 쉽도록 템플릿 방법을 사용하는 것이 좋습니다.

추가 정보:

[워크플로 제어 - 템플릿 방법 사용](#) (페이지 287)

워크플로 제어 - 템플릿 방법 사용

CA Identity Manager r12 에 도입된 템플릿 방법을 사용하면 *WorkPoint Designer* 를 열 필요 없이 사용자 콘솔에서 워크플로 프로세스 템플릿을 구성할 수 있습니다.

템플릿 방법의 장점은 다음과 같습니다.

- 다단계 프로세스 템플릿은 *WorkPoint Designer* 내에서 사용자 지정할 필요 없이 대부분의 워크플로 요구를 충족할 수 있습니다.
- 템플릿은 태스크 수준 및 이벤트 수준 워크플로 제어를 지원합니다.
- 프로세스 디자인 자체가 변경되지 않는 한 동일한 워크플로 프로세스 템플릿을 다양한 태스크에 사용하기 위해 구성할 수 있습니다.
- 사용자 콘솔에서 쉽게 참여자 해결 프로그램을 지정할 수 있습니다.
- 사용자 콘솔에서 작업 항목 위임을 수행할 수 있습니다.

사전 요구 사항: 워크플로를 사용하도록 설정

CA Identity Manager 태스크를 제어하는 데 워크플로를 사용하려면 먼저 워크플로를 사용하도록 설정해야 합니다. 기본적으로 워크플로는 사용되지 않습니다.

다음 단계를 수행하십시오.

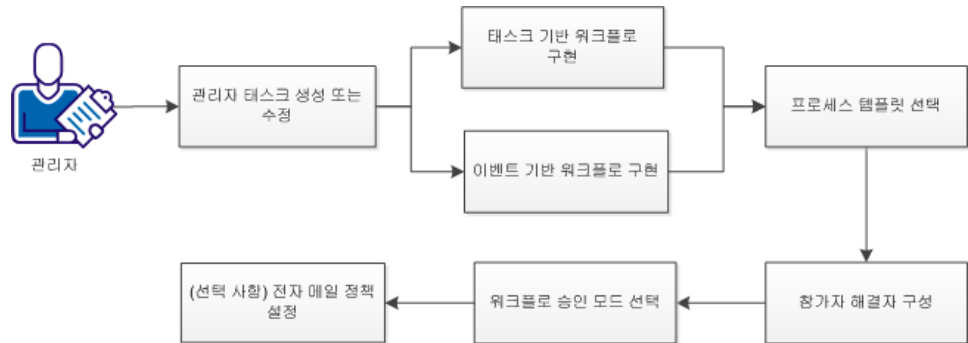
1. 관리 콘솔에서 "환경"을 선택합니다.
2. "고급 설정", "워크플로"로 이동합니다.
3. "사용" 확인란을 선택하고 "저장"을 클릭합니다.

참고: 이 화면의 이벤트 매핑은 **WorkPoint** 방법을 사용하여 워크플로를 구성하는 경우에만 적용됩니다. 템플릿 방법을 사용하는 경우(권장) 이 관리 콘솔을 사용하여 이벤트를 프로세스에 매핑하지 마십시오.

4. 응용 프로그램 서버를 다시 시작합니다.
5. (선택사항) [WorkPoint 관리 도구를 구성합니다](#) (페이지 309).

워크플로 제어 - 템플릿 방법 아래에 관리자 태스크 배치

관리자는 템플릿 방법을 사용하는 워크플로 제어 아래에 관리자 태스크를 배치할 수 있습니다.



다음 단계를 수행하십시오.

1. 사용자 콘솔에서 "역할 및 태스크", "관리자 태스크", "관리자 태스크 수정(또는 만들기)"을 선택합니다.
2. 워크플로 컨트롤을 적용할 태스크를 검색하고 "선택"을 클릭합니다.
3. 다음 작업 중 *하나*를 수행하십시오.
 - "프로필" 탭에서 "워크플로 프로세스" 편집 단추를 클릭하여 [태스크 수준 워크플로를 구현합니다](#) (페이지 290).
 - "이벤트" 탭에서 하나 이상의 이벤트를 선택하여 [이벤트 수준 워크플로를 구현합니다](#) (페이지 293).
4. [프로세스 템플릿을 선택합니다](#) (페이지 296).
5. [참여자 해결 프로그램을 구성합니다](#) (페이지 300).
6. 워크플로 승인 모드를 선택합니다.
7. [\(선택 사항\) 워크플로 프로세스의 전자 메일 정책을 설정합니다](#) (페이지 305).

참고: EscalationApproval 프로세스를 선택하는 경우 "승인 시간 만료(분)" 필드가 표시됩니다. 이 필드는 분 단위로 지정되며 비워둘 수 없습니다. 기본적으로, 시간은 60 분으로 설정됩니다.

워크플로 제어가 구성되면 적합한 역할의 사용자는 관리자 태스크를 구성하고 지정된 워크플로 참여자가 태스크 또는 이벤트를 승인하거나 거부합니다.

태스크 또는 이벤트 기반 워크플로

CA Identity Manager 를 사용하면 워크플로 프로세스를 태스크 또는 이벤트와 연결할 수 있습니다. 즉, 참여자가 전체 CA Identity Manager 태스크 또는 태스크 내의 특정 이벤트를 승인하거나 거부할 수 있습니다.

예를 들어, 일부 CA Identity Manager 태스크는 여러 이벤트를 생성하며 승인자가 요청을 승인하거나 거부하기 전에 모든 이벤트를 검토해야 할 수 있습니다. 이 작업은 태스크 수준 워크플로에서 가능합니다. 워크플로 프로세스가 태스크 내의 특정 이벤트와 연결되어 있으면 승인자가 요청이 수행된 전체 태스크 컨텍스트를 볼 수 없습니다.

태스크 수준 워크플로

태스크 수준 워크플로를 사용하면 승인자가 요청을 승인하거나 거부하기 전에 모든 이벤트를 검토할 수 있습니다. 태스크 수준 워크플로는 태스크 활동이 처리되기 전에 발생합니다. 워크플로 프로세스 작업이 시작되기 전에는 이벤트 또는 중첩된 태스크가 실행되지 않습니다.

태스크 수준 워크플로가 거부되면 이 태스크의 어떤 부분도 실행되지 않습니다.

참고: 태스크 수준 워크플로 제어에 대해 구성된 태스크를 이벤트 수준 워크플로 제어에 대해서도 동시에 구성할 수 있습니다. 동시 이벤트 수준 워크플로를 전역적으로 또는 특정 태스크에 대해 적용할 수도 있습니다.

태스크 수준 프로세스 특성

태스크 수준 워크플로와 모두 호환되는 워크플로 프로세스에는 **WorkPoint Designer** 내에 정의된 특수 특성이 있습니다. 이 프로세스 수준 사용자 데이터 특성인 **TASK_LEVEL**은 다음 프로세스 템플릿에서 기본적으로 **True**로 설정됩니다.

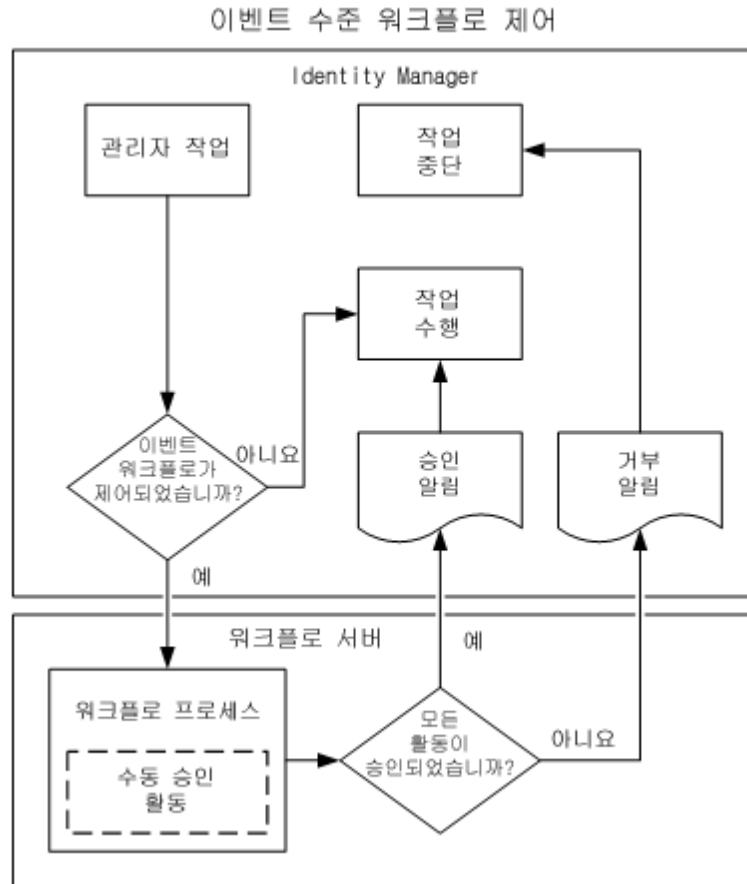
- SingleStepApproval
- TwoStageApprovalProcess
- EscalationApproval

태스크 수준 워크플로에 대한 관리자 태스크를 선택하면 해당 프로세스 템플릿만 사용할 수 있습니다.

참고: **TASK_LEVEL**이 **True**로 설정된 경우라도 프로세스 템플릿은 계속 이벤트 수준 워크플로에 사용될 수 있습니다. 이 **TASK_LEVEL** 특성 값을 변경하지 마십시오.

작업 수준 제어 다이어그램

다음 다이어그램은 일반적인 태스크 수준 워크플로 프로세스가 시작될 때 CA Identity Manager 와 워크플로 서버 간의 상호 작용을 보여 줍니다.



추가 정보:

[이벤트 수준 제어 다이어그램](#) (페이지 294)

작업 수준 워크플로를 구성하는 방법

작업 수준 워크플로는 작업 활동이 처리되기 전에 발생합니다. 워크플로 프로세스 작업이 시작되기 전에는 이벤트 또는 중첩된 작업이 실행되지 않습니다.

태스크 수준 워크플로를 구성하려면

1. 사용자 콘솔에서 "역할 및 태스크", "관리자 태스크", "관리자 태스크 수정(또는 만들기)"을 선택합니다.
"관리자 작업 선택" 화면이 나타납니다.
2. 워크플로 제어를 적용할 작업을 검색하고 "선택"을 클릭합니다.
"관리자 작업 수정(또는 만들기)" 화면이 나타납니다.
3. "프로필" 탭에서 "워크플로 사용"을 선택했는지 확인합니다.
4. "프로필" 탭에서 "워크플로 프로세스" 단추를 클릭합니다.
"작업 수준 워크플로 구성" 탭이 나타납니다.
5. "워크플로 프로세스" 목록에서 다음 프로세스 템플릿 중 하나를 선택합니다.
 - SingleStepApproval
 - TwoStageApprovalProcess"작업 수준 워크플로 구성" 탭이 확장됩니다.
6. 프로세스 템플릿에 필요한 경우 참여자 해결 프로그램을 구성합니다.
참여자 요청이 프로세스에 추가됩니다.
7. "확인"을 클릭합니다.
CA Identity Manager 에서 태스크 수준 워크플로 구성을 저장합니다.
8. "제출"을 클릭합니다.
CA Identity Manager 에서 태스크 수정을 처리합니다.

이벤트 수준 워크플로

이벤트를 워크플로 프로세스에 매핑할 수 있습니다. 워크플로 프로세스에 매핑된 이벤트가 트리거되면 워크플로 프로세스가 시작됩니다. 이벤트를 트리거한 태스크는 보류 중 상태가 되고 워크플로 제어가 적용됩니다.

워크플로 프로세스에서 참여자가 이벤트 또는 태스크를 승인하거나 거부해야 프로세스를 완료할 수 있습니다. 참여자의 수동 워크플로 승인이 필요한 태스크는 워크플로 제어가 적용되지 않는 태스크보다 완료하는 데 더 오래 걸립니다.

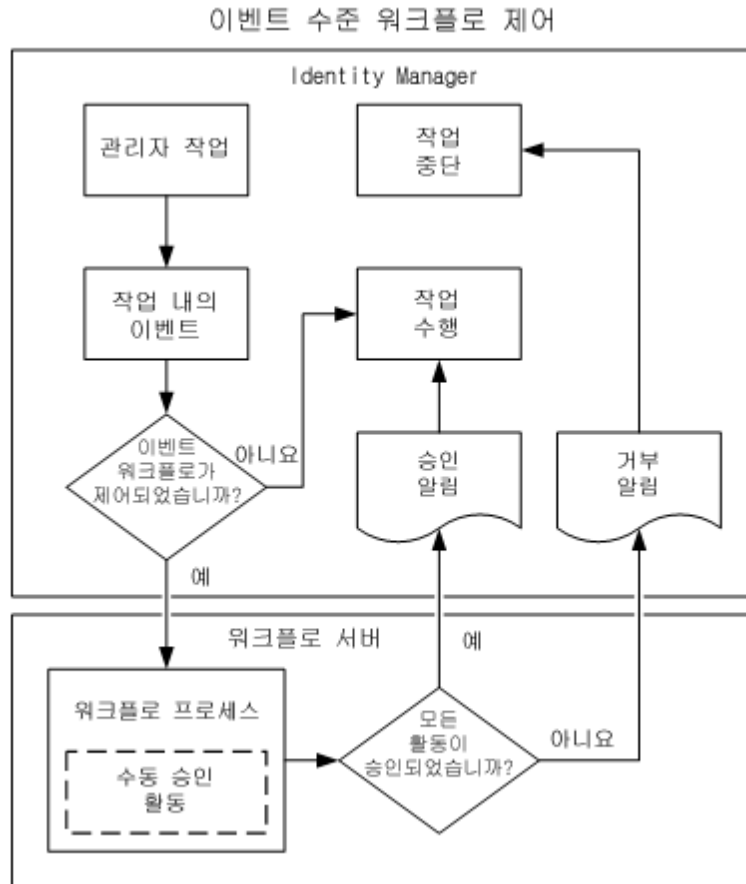
워크플로 프로세스의 모든 활동이 수행된 후 워크플로 프로세스에 매핑된 이벤트가 워크플로 제어에서 방출됩니다. 지정된 태스크에서 트리거한 모든 이벤트가 워크플로 제어에서 릴리스되면 워크플로에서 제어되는 태스크가 완료됩니다.

태스크에 워크플로 제어가 적용되는 동안 태스크 화면의 콘텐츠가 태스크 지속 데이터베이스에 저장됩니다. 워크플로 작업 상태(워크플로 관련 데이터)는 WorkPoint 데이터베이스에 저장됩니다.

참고: 이벤트 탭은 태스크에서 각 탭으로 생성된 이벤트를 나열합니다. 새 탭을 태스크에 추가한 후 새 이벤트가 "이벤트" 탭에 표시되기 전에 "관리자 태스크 수정"을 사용하여 태스크를 제출한 다음 다시 열어야 합니다.

이벤트 수준 제어 다이어그램

다음 다이어그램은 일반적인 이벤트 수준 워크플로 프로세스가 시작될 때 CA Identity Manager 와 워크플로 서버 간의 상호 작용을 보여줍니다.



추가 정보:

[작업 수준 제어 다이어그램](#) (페이지 291)

이벤트 수준 워크플로를 구성하는 방법

워크플로 프로세스에 매핑된 이벤트가 트리거되면 이벤트 수준 워크플로가 시작됩니다. 이벤트를 트리거한 작업은 참여자가 작업을 승인하거나 거부할 때까지 보류 중 상태가 됩니다.

이벤트 수준 워크플로를 구성하려면

1. 사용자 콘솔에서 "역할 및 태스크", "관리자 태스크", "관리자 태스크 수정(또는 만들기)"을 선택합니다.
"관리자 작업 선택" 화면이 나타납니다.
2. 워크플로 제어를 적용할 작업을 검색하고 "선택"을 클릭합니다.
"관리자 작업 수정(또는 만들기)" 화면이 나타납니다.
3. "프로필" 탭에서 "워크플로 사용"을 선택했는지 확인합니다.
4. "이벤트" 탭에서 프로세스 템플릿에 매핑할 이벤트를 선택합니다.
워크플로 매핑 화면이 나타납니다.
5. "워크플로 프로세스" 목록에서 다음 프로세스 템플릿 중 하나를 선택합니다.
 - SingleStepApproval
 - TwoStageApprovalProcess
 워크플로 매핑 화면이 확장됩니다.
6. 프로세스 템플릿에 필요한 경우 참여자 해결 프로그램을 구성합니다.
참여자 요청이 프로세스에 추가됩니다.
7. "확인"을 클릭합니다.
CA Identity Manager 에서 이벤트 수준 워크플로 구성을 저장합니다.
8. 워크플로 제어를 적용할 각 이벤트에 대해 3 - 6 단계를 반복합니다.
9. "제출"을 클릭합니다.
CA Identity Manager 에서 태스크 수정을 처리합니다.

참고: "워크플로 프로세스" 목록에는 템플릿 방법과 WorkPoint 방법에서 모두 사용할 수 있는 프로세스가 들어 있습니다.

- 템플릿 방법 프로세스를 선택하면(SingleStepApproval 또는 TwoStageApprovalProcess) 페이지가 확장되어 참여자 해결 프로그램 구성의 사용을 허용합니다.
- WorkPoint 방법 프로세스를 선택하면 페이지가 확장되지 않습니다. 참여자 해결 프로그램은 WorkPoint Designer 에서 구성됩니다.

프로세스 템플릿의 유형

워크플로 프로세스 템플릿에는 다음과 같은 특징이 있습니다.

- WorkPoint Designer 에서 정의됩니다.
- CA Identity Manager 승인 태스크에 해당하는 수동 활동이 있습니다.
- 참여자(승인자라고도 함)를 식별할 정보가 포함된 특수 특성을 포함합니다.

워크플로 프로세스 템플릿에는 특정 참여자를 선택하기 위한 정보가 포함되어 있지 않습니다. 이것은 사용자가 워크플로 및 해당 참여자 해결 프로그램을 구성한 후 CA Identity Manager 에서 제공됩니다. 이 정보는 이벤트 수준 워크플로 컨트롤의 경우 이벤트에 매핑되고, 태스크 수준 워크플로 컨트롤의 경우 태스크에 매핑됩니다.

템플릿 방법을 사용하는 경우 모든 워크플로 및 참여자 구성이 사용자 콘솔 내에서 수행됩니다.

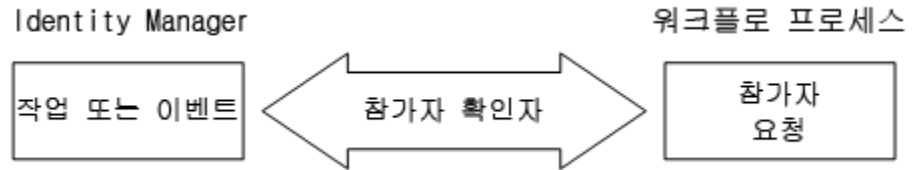
템플릿 방법에 사용할 다음 세 개의 프로세스 템플릿이 있습니다.

- SingleStepApprovalProcess
- TwoStageApprovalProcess
- EscalationApprovalProcess

프로세스 템플릿 작동 방법

워크플로 프로세스 템플릿에는 참여자 목록을 요청하는 많은 위치가 있습니다. 템플릿이 CA CA Identity Manager 태스크 또는 이벤트에 매핑된 경우 이러한 목록에 대해 참여자 해결 프로그램을 구성해야 합니다.

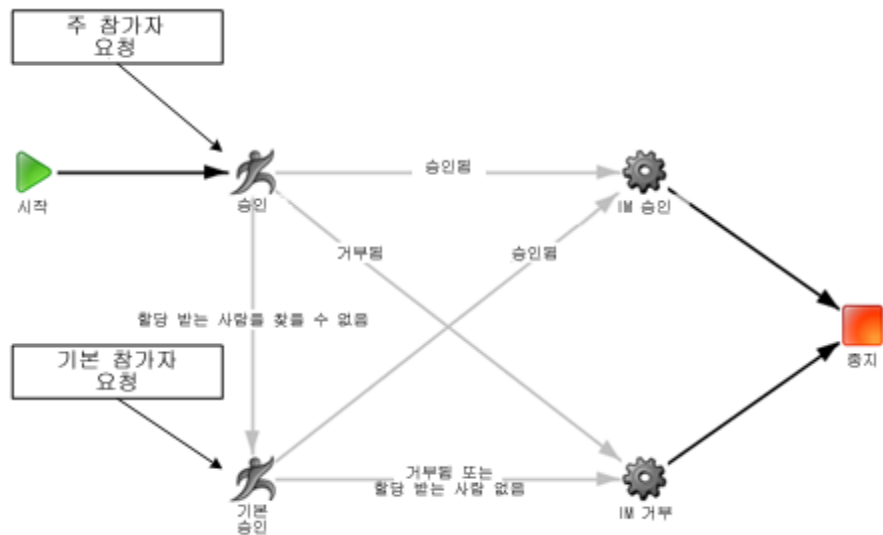
다음 그림과 같이 CA CA Identity Manager 는 실행 시 구성된 정보를 기준으로 워크플로 프로세스에 참여자 목록을 제공합니다.



단일 단계 템플릿 다이어그램

다음 다이어그램은 WorkPoint Designer 에 표시되는 SingleStageApproval 프로세스 템플릿을 보여 줍니다. 프로세스 템플릿에는 다음 두 개의 수동 활동이 포함되어 있습니다.

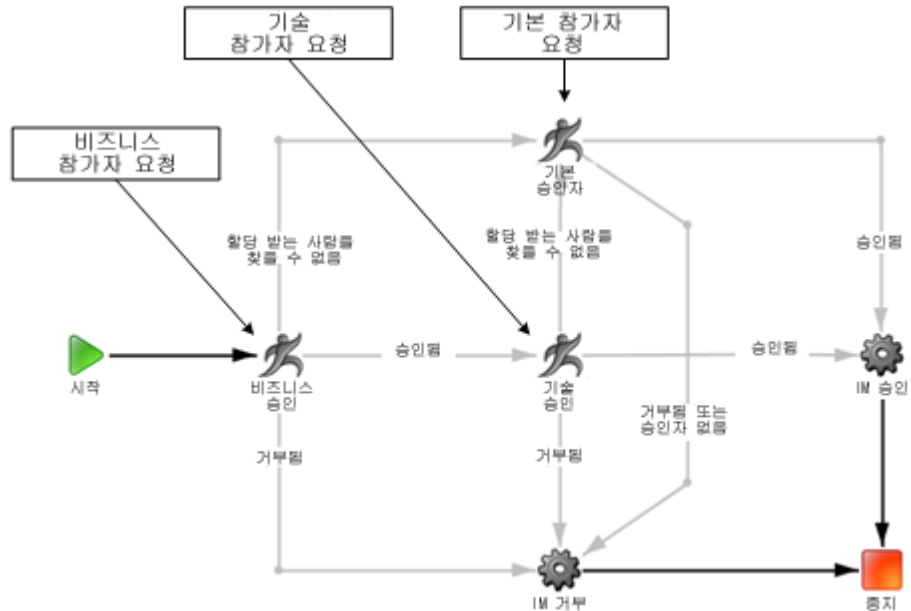
- 주 참여자에 대한 승인 노드. 이 사용자가 요청을 승인하거나 거부하면 프로세스가 완료될 때까지 실행됩니다.
- 기본 참여자에 대한 승인 노드. 주 참여자가 없거나 응답하지 않는 경우 이 사용자가 작업을 승인하거나 거부할 수 있습니다.



2 단계 템플릿 다이어그램

다음 다이어그램은 WorkPoint Designer 에 표시되는 TwoStageApproval 프로세스 템플릿을 보여 줍니다. TwoStageApproval 프로세스 템플릿에는 다음 세 개의 수동 활동이 포함되어 있습니다.

- 비즈니스 참여자에 대한 승인 노드. 이 사용자가 요청을 승인하거나 거부하면 프로세스가 기술 승인자 단계로 계속 진행합니다.
- 기술 참여자에 대한 승인 노드. 이 사용자가 요청을 승인하거나 거부하면 프로세스가 완료될 때까지 실행됩니다.
- 기본 참여자에 대한 승인 노드. 비즈니스 또는 기술 참여자가 없거나 응답하지 않는 경우 이 사용자가 작업을 승인하거나 거부할 수 있습니다.

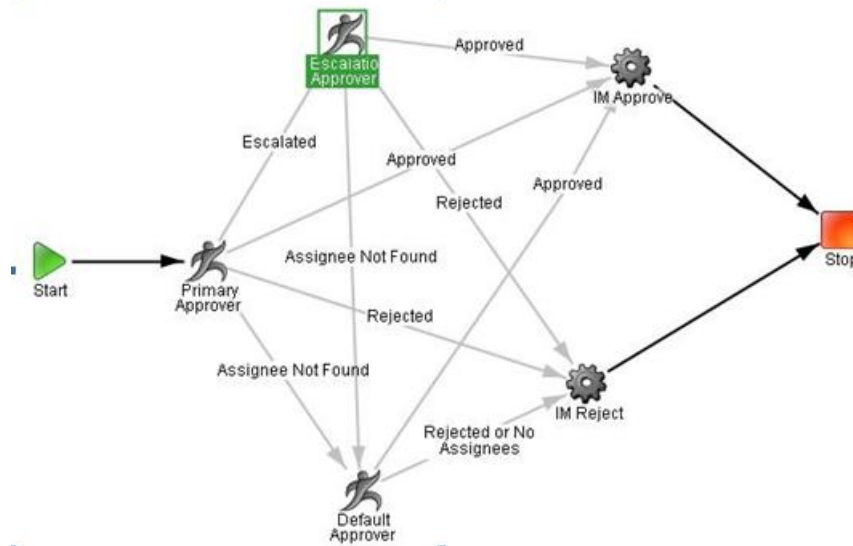


에스컬레이션 승인 템플릿 다이어그램

다음 다이어그램은 WorkPoint Designer 에 표시되는 EscalationApproval 프로세스 템플릿을 보여 줍니다. 프로세스 템플릿에는 다음과 같은 수동 활동이 포함되어 있습니다.

- 주 참가자에 대한 승인 노드. 이 사용자가 요청을 승인하거나 거부하면 프로세스는 완료될 때까지 실행됩니다.
- 기본 참가자에 대한 승인 노드. 주 참가자가 없는 경우 이 사용자가 요청을 승인하거나 거부할 수 있습니다.

- 일정 시간 후 작동하도록 설정된 주 승인자에서 에스컬레이션 승인자로의 전환 승인 노드. 기본 참가자를 찾았지만 구성된 시간 만료 기간 동안 이 참가자가 응답하지 않는 경우 이 사용자는 요청을 승인 또는 거부할 수 있습니다.



참고: 기존 프로세스에 시간 만료 옵션을 추가하려면 사용자 데이터 필드 `PARTICIPANT_TIMEOUT` 을 활동 노드에 추가하고 '에스컬레이션된' 트랜잭션을 작업 항목을 에스컬레이션해야 하는 노드에 추가하십시오.

에스컬레이션 승인 템플릿 사용

에스컬레이션 승인 템플릿을 사용하려면 r12.5 에서 r12.5 SP1 로 업그레이드할 때 다음 zip 파일을 수동으로 가져와야 합니다.

Workflow 12.5 to 12.5 SP1 upgrade.zip

zip 파일은 관리 도구 아래 workflowScripts 폴더에 있습니다.

기본적으로 관리 도구는 다음 위치에 설치됩니다.

- Windows: <설치 경로>\tools
- UNIX: <설치 경로 2>/tools

참여자 해결 프로그램의 유형

템플릿 방법의 경우 7 가지 참여자 해결 프로그램 유형이 있습니다.

승인 작업 역할 구성원

참여자가 승인 태스크에 대한 액세스를 부여하는 역할의 구성원임을 지정합니다.

사용자 목록

참여자가 지정된 사용자 목록임을 지정합니다.

그룹 구성원

참여자가 지정된 그룹 목록의 구성원임을 지정합니다.

관리자 역할 구성원

참여자가 지정된 관리자 역할 목록의 구성원임을 지정합니다.

관리자 태스크 구성원

참여자가 지정된 관리자 태스크 목록과 관련된 관리자 역할의 구성원임을 지정합니다.

동적 해결 프로그램

참여자가 승인되는 태스크나 이벤트에 따라 동적으로 선택됨을 지정합니다.

Null 해결 프로그램

사용자가 없는 Null 목록으로 해결됩니다.

사용자 지정

참여자가 사용자 지정 참여자 해결 프로그램에서 결정됨을 지정합니다.

비즈니스 소유자 해결자

엔터티의 비즈니스 소유자로서 카탈로그 규칙에 구성된 참여자의 목록을 지정합니다.

관리 소유자 해결자

엔터티의 관리 소유자로서 카탈로그 규칙에 구성된 참여자의 목록을 지정합니다.

매니저 해결자

사용자 개체의 매니저로서 설정된 참여자를 지정합니다.

승인 태스크 역할 구성원

이 해결 프로그램은 승인 태스크에 대한 액세스를 부여하는 모든 **CA Identity Manager** 역할의 모든 구성원에게 활동을 할당합니다. 이 해결 프로그램에는 추가 구성이 필요하지 않습니다.

사용자 목록

이 해결 프로그램은 지정된 사용자 목록에 작업 항목을 할당합니다.

범위 지정은 시행되지 않습니다. 워크플로 구성 화면에 액세스할 수 있는 사람은 누구나 이 목록에서 모든 사용자를 추가 또는 제거할 수 있습니다.

이 해결 프로그램에는 다음과 같은 유효성 검사 규칙이 있습니다.

- 하나 이상의 사용자 이름을 제공해야 합니다.
- 사용자 이름은 현재 존재하는 사용자의 이름이어야 합니다.

그룹 구성원

이 해결 프로그램은 그룹 목록에 지정된 모든 그룹의 모든 구성원에 작업 항목을 할당합니다.

누가 그룹 구성원인지에 대한 평가는 참여자 해결 프로그램이 지정되는 때가 아닌 작업 항목이 생성될 때 수행됩니다.

범위 지정은 시행되지 않습니다. 워크플로 구성 화면에 액세스할 수 있는 사람은 누구나 이 목록에서 그룹을 추가 또는 제거할 수 있습니다.

이 해결 프로그램에는 다음과 같은 유효성 검사 규칙이 있습니다.

- 하나 이상의 그룹을 지정해야 합니다.
- 그룹 이름은 현재 존재하는 그룹의 이름이어야 합니다.

관리자 역할 구성원

이 해결 프로그램은 관리자 역할 목록에 지정된 관리자 역할의 모든 구성원에 작업 항목을 할당합니다.

누가 역할 구성원인지에 대한 평가는 참여자 해결 프로그램이 지정되는 때가 아닌 작업 항목이 생성될 때 수행됩니다.

범위 지정은 시행되지 않습니다. 워크플로 구성 화면에 액세스할 수 있는 사람은 누구나 이 목록에서 모든 역할을 추가 또는 제거할 수 있습니다.

이 해결 프로그램에는 다음과 같은 유효성 검사 규칙이 있습니다.

- 최소한 하나 이상이 관리자 역할을 지정해야 합니다.
- 관리자 역할 이름은 현재 존재하는 관리자 역할의 이름이어야 합니다.

관리자 태스크 구성원

이 해결 프로그램은 관리자 태스크 목록에 지정된 관리자 태스크에 연결된 모든 관리자 역할의 모든 구성원에게 작업 항목을 할당합니다.

범위 지정은 시행되지 않습니다. 워크플로 구성 화면에 액세스할 수 있는 사람은 누구나 이 목록에서 모든 태스크를 추가 또는 제거할 수 있습니다.

누가 역할 구성원인지에 대한 평가와 어떤 역할이 해당 태스크에 제공되는지에 대한 평가는 참여자 해결 프로그램이 지정되는 때가 아닌 작업 항목이 생성될 때에 수행됩니다.

이 해결 프로그램에는 다음과 같은 유효성 검사 규칙이 있습니다.

- 하나 이상의 관리자 태스크를 지정해야 합니다.
- 관리자 태스크 이름은 현재 존재하는 관리자 태스크의 이름이어야 합니다.

동적 해결 프로그램

이 해결 프로그램은 런타임 시 확인된 동적 규칙에 따라 사용자 목록을 반환합니다. 다음 선택을 사용하여 동적 규칙 제약 조건을 설정합니다.

승인자

이 태스크를 승인할 사용자 유형을 지정합니다.

참고: 이 항목을 선택하면 사용자(또는 승인자)를 포함할 수 있는 개체만 표시됩니다.

사용자 또는 개체

승인자를 찾을 수 있는 사용자 또는 개체를 지정합니다.

- 이벤트와 관련된 개체 - 워크플로 제어하의 이벤트입니다.
- 이 태스크의 초기자 - 관리자 태스크를 시작한 사용자입니다.
- 이 태스크의 기본 개체 - 태스크에서 생성/수정하는 개체입니다.
- 이 태스크의 이전 승인자 - 이 태스크의 이전 승인자입니다.

이 계정과 관련된 사용자

끝점 계정 특성 대신, CA Identity Manager 사용자 특성을 나열하도록 사용자 또는 개체 특성 필드를 업데이트합니다. 해결 프로그램은 CA Identity Manager 사용자 수준에서 특성에 대한 작업을 수행합니다. 이 확인란은 Active Directory 계정과 같이 끝점 계정 개체를 선택하는 경우에 적용됩니다.

특성

승인자가 포함된 특성을 지정합니다.

참고: 특성 목록은 사전순으로 정렬되고 특성 목록에는 고유 표시 이름의 목록이 포함됩니다. 확장 특성은 목록에서 제외됩니다.

이벤트 개체 유형

이벤트의 개체 유형을 지정합니다.

참고: 이 항목은 "이벤트와 관련된 개체"가 선택된 경우에만 나타납니다.

참고: 그룹 만들기가 있는 동적 해결 프로그램을 사용하려면 개체가 존재해야 합니다. 그룹 구성원 자격/관리자 정보는 기존 그룹의 동적/일치 특성 해결 프로그램에만 사용될 수 있습니다.

동적 해결 프로그램이 향상되어 이전 승인자를 지원되는 개체 목록에 추가할 수 있게 되었습니다. 물리적 특성 호스팅 매니저 정보를 선택한 경우 매니저에게 승인이 전송됩니다.

관리자 승인 해결 프로그램을 위한 해결 프로그램을 구성하려면:

- 승인자를 "사용자"로 설정합니다.
- 사용자 또는 개체 드롭다운 목록에서 "이 태스크의 이전 승인자"를 선택합니다.
- 특성을 매니저 정보가 포함된 물리적 특성으로 설정합니다.

특성 일치 해결 프로그램

이 해결 프로그램은 사용자 유형 개체에서만 작동합니다. 사용 가능한 모든 개체의 값은 사용자 개체의 필드와 일치합니다. 다음 선택을 사용하여 특성 일치 규칙 제약 조건을 설정하십시오.

승인자

이 태스크를 승인할 사용자 유형을 지정합니다.

사용자 또는 개체

아래에서 선택한 특성에서 승인자가 사용하게 될 값을 지정합니다.

참고: 사용자 또는 개체에서 검색되는 값은 사용자에게 대해 선택한 특성을 검색할 때 허용 가능한 값이어야 합니다.

- 이벤트와 관련된 개체 - 워크플로 제어하의 이벤트입니다.
- 이 태스크의 초기자 - 관리자 태스크를 시작한 사용자입니다.
- 이 태스크의 기본 개체 - 태스크에서 생성/수정하는 개체이며, 태스크 수준 이벤트 매핑에서만 사용 가능합니다.
- 이 태스크의 이전 승인자 - 이 태스크의 이전 승인자입니다.

이 계정과 관련된 사용자

끝점 계정 특성 대신, CA Identity Manager 사용자 특성을 나열하도록 사용자 또는 개체 특성 필드를 업데이트합니다. 해결 프로그램은 CA Identity Manager 사용자 수준에서 특성에 대한 작업을 수행합니다. 이 확인란은 Active Directory 계정과 같이 끝점 계정 개체를 선택하는 경우에 적용됩니다.

사용 또는 개체 특성

승인자에 대한 검색에서 사용할 값이 포함된 특성을 지정합니다.

승인자 검색 특성

위에 식별된 값과 일치시키기 위해 검색에 사용되는 특성을 지정합니다.

참고: '사용자 만들기 승인' 태스크를 사용자에게 대해 작동하는 일치 특성 해결 프로그램인 참여자 해결 프로그램으로 설정할 때 Workpoint Designer 에서 imApprovers 스크립트에 대한 메서드 서명을 TwoStageProcessDefinition 에 대한 고유한 이름을 가리키도록 변경해야 합니다.

Null 해결 프로그램

Null 해결 프로그램은 사용자를 반환하지 않습니다. 워크플로 프로세스가 설계된 방식에 따라 Null 해결 프로그램으로 인해 프로세스가 승인을 전체적으로 건너뛸 수 있습니다. Null 해결 프로그램에는 추가 구성이 필요하지 않습니다.

사용자 지정 참여자 해결 프로그램

사용자 지정 참여자 해결 프로그램은 워크플로 활동 참여자를 결정하는 Java 개체이며 CA Identity Manager 에 목록을 반환합니다. 그런 다음 이 목록은 워크플로 엔진으로 전달됩니다. 일반적으로 표준 참여자 정책에서 활동에 필요한 참여자 목록을 제공할 수 없는 경우에만 사용자 지정 참여자 해결 프로그램을 작성합니다.

참고: 참여자 해결 프로그램 API 를 사용하여 사용자 지정 참여자 해결 프로그램을 만듭니다. 자세한 내용은 *Programming Guide for Java*(Java 프로그래밍 안내서)를 참조하십시오.

워크플로 프로세스의 전자 메일 정책 설정

워크플로 프로세스의 각 단계에 대해 전자 메일 정책을 지정할 수 있습니다. 정의된 전자 메일 정책에 따라 프로세스가 해당 단계 또는 활동에 도달하면 전자 메일이 발송됩니다. 워크플로 프로세스 관련 전자 메일 알림의 경우 *보낼 조건 유형 워크플로 보류 중인 전자 메일*만 선택할 수 있습니다.

참고: 전자 메일 정책에 대한 자세한 내용은 "전자 메일 알림 정책을 만드는 방법"을 참조하십시오.

워크플로 예: 사용자 만들기

회사의 CA CA Identity Manager 관리자가 다음 시나리오를 처리하려면 워크플로 및 사용자 역할을 정의해야 합니다.

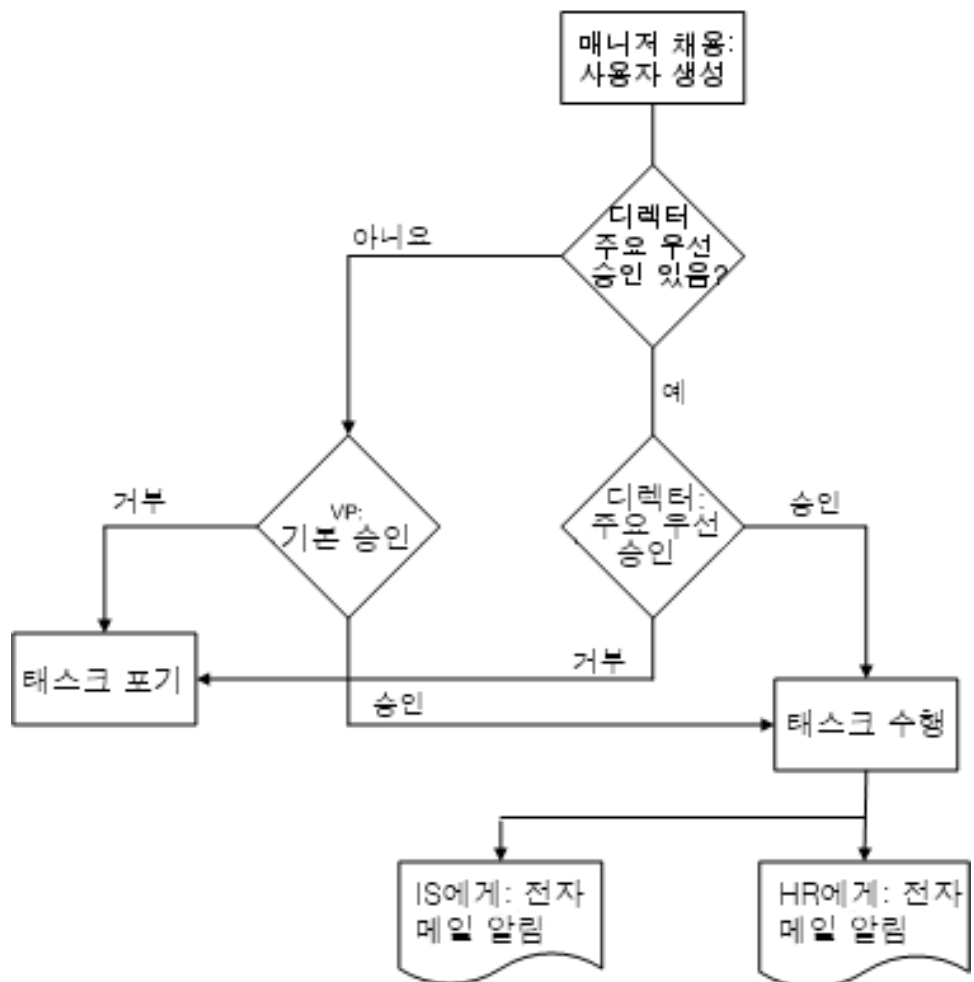
- 회사 영업 관리자가 새로운 영업 직원을 고용합니다. 영업 관리자는 새 고용에 대해 CA CA Identity Manager 사용자를 만들 수 있어야 합니다.
- 고용 프로세스를 단순화하기 위해 참여자는 단일 작업 항목만 수행하여 작업을 승인하거나 거부하려고 합니다.

- 영업 이사가 모든 새 고용의 주 승인자여야 합니다. 영업 이사가 어떤 이유로든 이 작업을 수행할 수 없는 경우 영업 부사장이 기본 승인자여야 합니다.
- 새 고용이 승인되면 CA CA Identity Manager 에서 새 사용자 전자 메일 알림을 HR(인사) 및 IS(정보 서비스) 부서로 보내야 합니다.

사용자 만들기 제어 다이어그램

다음 다이어그램은 사용자 만들기 시나리오에 대한 논리적 흐름을 보여줍니다.

태스크 수준 워크플로 예제: 사용자 생성



워크플로 예 구현

이 예제 시나리오를 구현하려면 관리자가 다음 작업을 수행해야 합니다.

- 태스크 초기자가 필요한 관리자 역할의 구성원인지 확인합니다.

영업 관리자는 "사용자 관리자" 관리자 역할의 구성원이어야 합니다. 이 역할은 영업 관리자에게 새 고용 영업 직원에 대해 "사용자 만들기" 관리자 작업을 시작하는 데 필요한 권한을 부여합니다.

- "사용자 만들기" 관리자 태스크에 대해 태스크 수준 워크플로를 사용하도록 설정합니다.

작업 수준 워크플로는 "사용자 만들기" 작업을 완료하기 위해 작업 항목이 한 개만 생성되도록 합니다. "사용자 만들기" 작업과 관련된 개별 이벤트가 여러 개 있으므로 이벤트 수준 워크플로에서 작업 항목을 여러 개 생성하며 구성하기도 더 어렵습니다.

- 참여자 해결 프로그램을 구성합니다.

가능한 참여자 해결 프로그램 수는 선택한 워크플로 프로세스 템플릿에 의해 결정됩니다. `SingleStageApproval` 템플릿에는 주 승인자와 기본 승인자가 포함되어 있고 다른 템플릿은 더 많은 승인자를 허용합니다.

이 시나리오에는 두 명의 개별 승인자만 필요하므로 "사용자 목록" 참여자 해결 프로그램이 가장 간단한 솔루션을 제공합니다. 이 해결 프로그램에서는 역할이나 그룹으로 여러 사용자를 선택하는 대신 이름으로 개별 승인자를 선택할 수 있습니다.

- 전자 메일 알림을 구성합니다.

관리 콘솔에서는 특정 작업과 이벤트에 대해 전자 메일 통보를 사용할 수 있습니다. 이 시나리오에서는 작업 전자 메일이 사용되고 "사용자 만들기" 작업이 완료될 때 전자 메일 통보가 전송됩니다.

적절한 제목 줄과 메시지 텍스트가 포함된 전자 메일을 HR 및 IS 부서로 보내려면 사용자 지정 전자 메일 템플릿이 필요합니다.

WorkPoint 방법을 사용하는 방법

WorkPoint 방법은 CA Identity Manager r12 이전 릴리스에 적용됩니다. 기본적으로 특정 CA Identity Manager 이벤트에 매핑되는 14 개의 미리 정의된 WorkPoint 워크플로 프로세스가 있습니다. WorkPoint Designer 를 사용하여 참여자 해결 프로그램을 구성하거나 워크플로 프로세스를 수정해야 합니다.

WorkPoint 방법에서는 관리 콘솔을 사용하여 워크플로 프로세스를 승인 이벤트에 매핑하는 방식으로 환경 내에서 전역적으로 해당 작업에 워크플로 제어를 적용해야 합니다.

이 섹션에서는 WorkPoint 방법을 사용하여 관리자 태스크에 워크플로 제어를 적용하는 과정과 관련된 고급 단계를 보여 줍니다.

참고: 가능한 경우 유연성을 높이고 사용하기 쉽도록 템플릿 방법을 사용하는 것이 좋습니다.

WorkPoint 방법을 사용하려면

1. [WorkPoint 관리 도구를 구성합니다.](#) (페이지 309)
2. 관리 콘솔에서 다음을 수행하십시오.
 - a. "고급 설정", "워크플로"에서 "사용" 확인란을 선택하여 사용자 환경에서 워크플로를 사용하도록 설정합니다.
참고: 이 화면의 이벤트 매핑은 WorkPoint 방법을 사용하여 워크플로를 구성하는 경우에만 적용됩니다. 템플릿 방법을 사용하는 경우(권장) 이 관리 콘솔을 사용하여 이벤트를 프로세스에 매핑하지 마십시오.
 - b. (선택 사항) 전역 이벤트 매핑의 경우 하나 이상의 이벤트를 미리 정의된 적절한 워크플로 프로세스에 연결합니다.
 - c. 필요한 경우 CA Identity Manager 환경을 다시 시작합니다.
3. 사용자 콘솔:
 - a. 태스크별 이벤트 매핑의 경우 하나 이상의 이벤트를 미리 정의된 적절한 워크플로 프로세스에 연결합니다. (옵션)

4. WorkPoint Designer:
 - a. 승인 태스크를 워크플로 프로세스와 연결합니다(선택 사항).
 - b. 워크플로 프로세스를 사용하여 참여자 해결 프로그램을 구성합니다(선택 사항).
5. 사용자 콘솔:
 - a. 워크플로 제어가 구성된 후 적절한 역할을 가진 사용자가 관리자 태스크를 수행합니다.
 - b. 지정된 워크플로 참여자가 이벤트를 승인하거나 거부합니다.

WorkPoint 관리 도구 구성

WorkPoint Designer 는 CA Identity Manager 와 통합되는 Planet Group, Inc.의 자회사인 Workpoint LLC 에서 제작한 소프트웨어입니다. WorkPoint Designer 를 사용하여 워크플로 프로세스와 워크플로 작업을 관리할 수 있습니다. WorkPoint 관리 도구는 WorkPoint Designer 및 WorkPoint Archive 를 포함합니다. WorkPoint 관리 도구를 구성하려면 CA Identity Manager 관리 도구를 설치하십시오. CA Identity Manager 관리 도구를 설치하지 않았으면 설치 프로그램을 실행하고 CA Identity Manager 관리 도구 옵션을 선택할 수 있습니다.

참고: 워크플로에 대해 관리 도구를 사용하려면 지원되는 JDK 가 관리 도구를 설치한 시스템에 설치되어 있어야 합니다. 지원되는 플랫폼 및 버전의 전체 목록은 [CA CA Identity Manager 지원 사이트](#)의 CA CA Identity Manager Support Matrix 를 참조하십시오.

워크플로 클라이언트 도구는 CA Identity Manager 관리 도구의 WorkPoint 디렉터리에 있습니다. 기본적으로 관리 도구는 다음 위치에 설치됩니다.

- **Windows:** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools

이 디렉터리의 도구를 사용하여 다음 작업을 수행할 수 있습니다.

- 워크플로 데이터베이스 스키마 만들기
- 기본 워크플로 스크립트 로드
- 워크플로 프로세스 및 작업 설계 및 모니터링

JBoss 에서 WorkPoint 관리 도구 구성

JBoss 에서 WorkPoint 관리 도구를 구성하려면 `init.bat/sh` 및 `workpoint-client.properties` 파일을 편집하십시오.

`init.bat/init.sh` 편집

`init.bat/init.sh` 를 편집하려면

1. 텍스트 편집기에서 다음 파일 중 하나를 편집합니다.
 - **Windows:**
`admin_tools\Workpoint\bin\init.bat`
 - **UNIX:**
`admin_tools/Workpoint/bin/init.sh`
2. 파일의 JBoss 섹션에서 `EJB_CLASSPATH` 줄의 주석을 제거합니다.
참고: 기타 응용 프로그램 서버에 대한 모든 섹션에 설명이 있는지 확인하십시오.
3. `jboss_home\client\`의 `jbossall-client.jar` 을 다음 위치에 복사합니다.
`admin_tools\Workpoint\lib`

`workpoint-client.properties` 편집

CA CA Identity Manager 설치 중 선택한 응용 프로그램 서버 유형에 따라 `workpoint-client.properties` 파일을 편집합니다.

`workpoint-client.properties` 파일을 구성하려면

1. 텍스트 편집기에서 `admin_tools\Workpoint\conf\workpoint-client.properties` 를 엽니다.
`admin_tools` 는 관리 도구가 설치된 위치입니다. 기본적으로 관리 도구는 다음 위치에 설치됩니다.
 - **Windows:** `C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools`
 - **UNIX:** `/opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools`
2. JBOSS SETTINGS 제목의 섹션을 찾습니다.

3. 해당 섹션에서 모든 속성 값의 설명을 제거합니다.

예:

```
java.naming.provider.url=localhost
java.naming.factory.initial=org.jnp.interfaces.NamingContextFactory
java.naming.factory.url.pkgs=org.jboss.naming
```

참고: java.naming.provider.url 속성 값을 편집해야 할 수 있습니다. 예를 들어, localhost 를 jnp://서버 이름 또는 ip:port 로 바꾸십시오. jnp 포트 번호 1099 를 사용하십시오.

4. 파일을 저장합니다.

WebLogic 에서 WorkPoint 관리 도구 구성

WebLogic 에서 WorkPoint 관리 도구를 구성하려면 init.bat/sh 및 workpoint-client.properties 파일을 편집하십시오.

init.bat/init.sh 편집

init.bat/init.sh 를 편집하려면

1. 텍스트 편집기에서 다음 파일 중 하나를 편집합니다.

- **Windows:**

admin_tools\Workpoint\bin\init.bat

- **UNIX:**

admin_tools/Workpoint/bin/init.sh

2. 파일의 WebLogic 섹션에서 EJB_CLASSPATH 의 주석을 제거합니다.

참고: 기타 응용 프로그램 서버에 대한 모든 섹션에 설명이 있는지 확인하십시오.

3. *weblogic_home\server\lib* 의 wlclient.jar 파일을 다음 위치에 복사합니다.

admin_tools\Workpoint\lib

workpoint-client.properties 편집

CA CA Identity Manager 설치 중 선택한 응용 프로그램 서버 유형에 따라 workpoint-client.properties 파일을 편집합니다.

workpoint-client.properties 파일을 구성하려면

1. 텍스트 편집기에서 `admin_tools\Workpoint\conf\workpoint-client.properties` 를 엽니다.
2. 파일의 WebLogic 섹션을 찾습니다.
3. 해당 섹션에서 모든 속성 값의 주석을 제거합니다.
4. 파일을 저장합니다.

참고: `java.naming.provider.url` 속성은 CA Identity Manager 서버를 설치한 시스템의 완전한 도메인 이름과 WebLogic 포트 번호를 가리켜야 합니다.

WebSphere 에서 WorkPoint 관리 도구 구성

WebSphere 에서 WorkPoint 관리 도구를 구성하려면 `init.bat/sh` 및 `workpoint-client.properties` 파일을 편집하십시오.

init.bat/init.sh 편집

init.bat/init.sh 를 편집하려면

1. 텍스트 편집기에서 다음 파일 중 하나를 편집합니다.

- **Windows:**

`admin_tools\Workpoint\bin\init.bat`

- **UNIX:**

`admin_tools/Workpoint/bin/init.sh`

2. IBM WebSphere 섹션의 주석을 제거합니다.

참고: COMMON WP_CLASSPATH 섹션에서 WP_CLASSPATH 항목에 대한 설명을 제거하십시오.

3. 기타 응용 프로그램 서버에 대한 모든 섹션이 주석 처리되어 있는지 확인하십시오.
4. 필요한 경우 JAVA_HOME 및 WAS_HOME 에 대한 값을 사용자 환경에 적합한 경로로 바꾸십시오.

workpoint-client.properties 편집

CA CA Identity Manager 설치 중 선택한 응용 프로그램 서버 유형에 따라 workpoint-client.properties 파일을 편집합니다.

workpoint-client.properties 파일을 구성하려면

1. 텍스트 편집기에서 `admin_tools\Workpoint\conf\workpoint-client.properties` 를 엽니다.

`admin_tools` 는 관리 도구가 설치된 위치입니다. 기본적으로 관리 도구는 다음 위치에 설치됩니다.

- **Windows:** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools

2. IBM WEBSPPHERE SETTINGS 제목의 섹션을 찾습니다.
3. 해당 섹션에서 모든 속성 값의 설명을 제거합니다.

예:

```
java.naming.factory.initial=com.ibm.websphere.naming.WsnInitialContextFactory
java.naming.provider.url=iiop://localhost:bootstrap_port
```

참고: 부트스트랩 포트 번호는 WebSphere Administrative Console 에 지정된 포트 번호와 일치해야 합니다. 올바른 포트 번호를 찾으려면 "서버", "끝점", "부트스트랩" 서버 주소로 이동하십시오.

4. 다음과 같이 WebSphere 프로필에 대한 BOOTSTRAP_ADDRESS 포트를 업데이트합니다.
 - a. WebSphere 관리 콘솔에서 "응용 프로그램 서버", "서버 이름", "통신"으로 이동합니다.
 - b. "포트"를 확장합니다.
 - c. iam_im.ear/config 아래 workpoint-client.properties 파일을 편집합니다.
 - d. WebSphere 섹션의 기본 포트 2809 를 BOOTSTRAP_ADDRESS 에 대한 프로필의 포트로 변경합니다.
5. 파일을 저장합니다.

WorkPoint Designer 시작

WorkPoint Designer 를 시작하려면 다음 파일을 실행합니다.

- **Windows:** `admin_tools\WorkPoint\bin\Designer.bat`
- **UNIX:** `admin_tools/WorkPoint/bin/Designer.sh`

여기서 `admin_tools` 는 CA Identity Manager 관리 도구의 설치 디렉터리입니다. 기본적으로 관리 도구는 다음 위치에 설치됩니다.

- **Windows:** `C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools`
- **UNIX:** `/opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools`

참고: WorkPoint Designer 를 실행하려면 워크플로 구성 요소가 설치 및 구성되어 있어야 합니다. 자세한 내용은 해당 응용 프로그램 서버에 대한 "WorkPoint 관리 도구 구성" 절을 참조하십시오.

추가 정보:

[JBoss 에서 WorkPoint 관리 도구 구성](#) (페이지 310)

[WebLogic 에서 WorkPoint 관리 도구 구성](#) (페이지 311)

[WebSphere 에서 WorkPoint 관리 도구 구성](#) (페이지 312)

WorkPoint 프로세스

CA CA Identity Manager 에는 WorkPoint Designer 에서 미리 정의된 많은 워크플로 프로세스가 포함되어 있습니다. 기본 이벤트 매핑이 있는 미리 정의된 프로세스를 사용하고, 워크플로 프로세스를 다른 이벤트에 매핑하고, 활동을 추가하거나 제거하여 워크플로 프로세스를 수정하고, 새 워크플로 프로세스를 만들 수 있습니다.

이벤트 매핑에 대한 전역 프로세스

워크플로 프로세스의 전역 수준 이벤트로의 매핑은 정책 기반이 아니거나 정책 기반일 수 있습니다.

정책 기반 워크플로를 사용하여 이벤트를 워크플로 프로세스에 매핑하는 방법에 대한 자세한 내용은 전역 이벤트 정책 기반 워크플로 매핑을 참조하십시오.

이 표에서는 관리 콘솔에서 지정된 기본 전역 워크플로 프로세스와 이벤트 매핑을 보여 줍니다.

중요: 이것은 전역 매핑입니다. 매핑된 워크플로 프로세스는 해당 이벤트가 환경에 있는 임의의 태스크에 의해 생성될 때마다 실행됩니다.

워크플로 프로세스	매핑된 이벤트
CertifyRoleApproveProcess	CertifyRoleEvent
CreateGroupApproveProcess	CreateGroupEvent
CreateOrganizationApproveProcess	CreateOrganizationEvent
CreateUserApproveProcess	CreateUserEvent
DeleteGroupApproveProcess	DeleteGroupEvent
DeleteOrganizationApproveProcess	DeleteOrganizationEvent
DeleteUserApproveProcess	DeleteUserEvent
ModifyAccessRoleMembershipApproveProcess	AssignAccessRoleEvent RevokeAccessRoleEvent
ModifyAdminRoleMembershipApproveProcess*	
ModifyGroupMembershipApproveProcess*	
ModifyOrganizationApproveProcess	ModifyOrganizationEvent
SelfRegistrationApproveProcess	SelfRegisterUserEvent

참고: 별표(*)로 표시된 워크플로 프로세스는 기본적으로 이벤트에 매핑되지 않습니다.

프로세스를 이벤트에 매핑

WorkPoint Designer 에서 워크플로 프로세스를 만들고 수정합니다. CA Identity Manager 에 대해 워크플로 프로세스를 만드는 경우 특정 CA CA Identity Manager 태스크를 염두에 두고 작업을 수행합니다. 이 작업의 실행은 워크플로 프로세스에서 제어됩니다.

워크플로 프로세스를 만드는 것 외에도 다음 작업도 수행해야 합니다.

- 관리자 태스크 및 이벤트에 설명되어 있는 CA Identity Manager 태스크에서 생성된 이벤트를 식별합니다. 이벤트를 생성하는 CA Identity Manager 태스크에 대해 워크플로 프로세스를 만들 수 있습니다.
- 다음 중 하나를 수행하여 워크플로 프로세스를 이벤트에 매핑합니다.
 - 이벤트에 전역적으로 워크플로 프로세스를 할당합니다.

이 전역 매핑을 사용하면 이벤트를 생성하는 작업에 관계없이 환경에서 이벤트가 생성될 때마다 워크플로 프로세스가 수행됩니다.
 - 특정 작업에서 생성된 이벤트에 워크플로 프로세스를 할당합니다.

이 작업별 매핑을 사용하면 지정된 작업에서 이벤트를 생성하는 경우에만 워크플로 프로세스가 수행됩니다.

참고: 이벤트를 워크플로 프로세스에 전역적으로 매핑하는 동시에 특정 작업에도 매핑하는 경우 특정 작업과 관련된 워크플로 프로세스가 우선 적용됩니다.

- 워크플로 프로세스의 워크플로 활동에 대해 참여자 해결 프로그램을 지정합니다.
- 워크플로 활동을 승인 작업과 연결합니다.

프로세스를 이벤트에 전역적으로 매핑

워크플로 프로세스를 이벤트에 전역적으로 매핑하여 환경의 임의 작업에서 이벤트가 생성될 때 워크플로 프로세스가 실행되도록 합니다.

워크플로 프로세스를 이벤트에 전역적으로 매핑하려면

1. 브라우저에 다음 URL 을 입력하여 관리 콘솔을 엽니다.

`http://hostname/iam/immanage`

hostname

CA CA Identity Manager 가 설치된 서버의 정규화된 도메인 이름을 정의합니다. 예를 들어, `myserver.mycompany.com:port` 와 같이 입력합니다.

2. "환경"을 클릭하고 적절한 CA CA Identity Manager 환경의 이름을 선택합니다.
3. "고급 설정"을 클릭한 다음 "워크플로"를 클릭합니다.
4. 다음을 수행하여 이벤트를 워크플로 프로세스에 매핑합니다.
 - a. "이벤트" 목록 상자에서 이벤트를 선택합니다.
 - b. "프로세스 승인" 목록 상자에서 워크플로 프로세스를 선택합니다.
 - c. "추가"를 클릭합니다.
5. 이벤트를 워크플로 프로세스에 매핑하는 작업을 완료한 후 "저장"을 클릭합니다.
6. CA Identity Manager 환경을 다시 시작하여 변경 사항을 적용합니다.

추가 정보:

[이벤트 매핑에 대한 전역 프로세스 \(페이지 315\)](#)

프로세스를 특정 작업의 이벤트에 매핑

특정 작업에서 생성된 이벤트에 워크플로 프로세스를 할당할 수 있습니다. 이 경우 특정 작업에서 매핑된 이벤트가 생성되는 경우에만 워크플로 프로세스가 수행됩니다.

작업별 매핑을 사용하면 동일한 이벤트에 대해 실행할 수 있는 워크플로 프로세스를 변수로 제어할 수 있습니다. 예를 들어, 다음 다이어그램은 동일한 이벤트를 생성하지만 다음과 같이 서로 다른 워크플로 프로세스를 트리거하는 두 가지 작업을 보여 줍니다.



이 다이어그램에서 각 태스크는 서로 다른 워크플로 프로세스를 사용합니다.

사용자 만들기

기본 워크플로 프로세스인 `CreateUserApproveProcess`에 매핑되는 `CreateUserEvent`를 트리거하는 기본 관리자 태스크를 지정합니다.

계약자 만들기

사용자 만들기에 기반한 사용자 지정 태스크를 지정합니다. 이 경우 `CreateUserEvent`는 새 계약자 계정을 승인하기 위해 만든 사용자 지정 워크플로 프로세스인 `CreateContractorApproveProcess`에 매핑됩니다.

워크플로 프로세스를 기존 작업의 이벤트에 매핑하려면

1. 사용자 콘솔에서 "역할 및 태스크", "관리자 태스크", "관리자 태스크 수정"을 선택합니다.
2. 관리자 작업을 검색합니다.
3. 작업(예: "사용자 수정" 또는 "사용자 만들기" 작업)을 선택하고 "선택"을 클릭합니다.

4. "이벤트" 탭에서 작업의 이벤트에 대한 워크플로 프로세스를 선택합니다.
참고: 이 탭에 표시할 워크플로 프로세스 드롭다운 메뉴 및 이벤트 이름에 대해 워크플로가 사용되어야 합니다.
5. "워크플로 프로세스" 드롭다운 메뉴를 사용하여 이벤트 이름에 워크플로 프로세스를 할당하고 "확인"을 클릭합니다.
6. "제출"을 클릭합니다.
7. 관리 콘솔을 열고 CA Identity Manager 환경을 다시 시작하여 변경 사항을 적용합니다.

워크플로 프로세스를 새 작업의 이벤트에 매핑하려면

1. 사용자 콘솔에서 "역할 및 태스크", "관리자 태스크", "관리자 태스크 만들기"를 선택합니다.
참고: 기존 워크플로 승인 작업(예: "그룹 만들기 승인" 또는 "사용자 만들기 승인")을 새 워크플로 승인 작업의 템플릿으로 선택해야 합니다.
2. "프로필" 탭의 해당 필드에 정보를 입력합니다.
3. "이벤트" 탭에서 작업의 이벤트에 대한 워크플로 프로세스를 선택합니다.
참고: 이 탭에 표시할 워크플로 프로세스 드롭다운 메뉴 및 이벤트 이름에 대해 워크플로가 사용되어야 합니다.
4. "워크플로 프로세스" 드롭다운 메뉴를 사용하여 이벤트 이름에 워크플로 프로세스를 할당하고 "확인"을 클릭합니다.
5. "제출"을 클릭합니다.
6. 관리 콘솔을 열고 CA Identity Manager 환경을 다시 시작하여 변경 사항을 적용합니다.

참고: "워크플로 프로세스" 목록에는 템플릿 방법과 WorkPoint 방법에서 모두 사용할 수 있는 프로세스가 들어 있습니다.

- 템플릿 방법 프로세스를 선택하면(SingleStepApproval 또는 TwoStageApprovalProcess) 페이지가 확장되어 참여자 해결 프로그램 구성의 사용을 허용합니다.
- WorkPoint 방법 프로세스를 선택하면 페이지가 확장되지 않습니다. 참여자 해결 프로그램은 WorkPoint Designer 에서 구성됩니다.

추가 정보:

[이벤트 매핑에 대한 전역 프로세스](#) (페이지 315)

워크플로 활동

CA Identity Manager 에는 WorkPoint Designer 에서 미리 정의된 많은 워크플로 활동이 포함되어 있습니다. 이러한 활동은 미리 정의된 워크플로 프로세스에 할당됩니다.

미리 정의된 워크플로 프로세스는 단일 단계 프로세스입니다. 즉, 각 프로세스에 미리 정의된 하나의 활동이 포함되어 있습니다.

미리 정의된 각 활동은 CA Identity Manager 에서 미리 정의된 동일한 이름을 가진 워크플로 승인 태스크에 해당합니다. 다른 워크플로 프로세스에서 미리 정의된 활동을 사용하거나 새 활동을 만들 수 있습니다.

미리 정의된 워크플로 프로세스를 수정하지 않고 사용하거나 워크플로 프로세스에 다른 활동을 추가할 수 있습니다. 워크플로 프로세스에 활동을 추가하는 방법에 대한 자세한 내용은 WorkPoint 설명서를 참조하십시오.

프로세스, 작업 및 활동

아래 표에서는 미리 정의된 워크플로 활동과 각 활동이 기본적으로 할당되는 미리 정의된 워크플로 프로세스를 보여 줍니다.

참고: 미리 정의된 워크플로 활동과 해당 워크플로 승인 작업은 이름이 같습니다.

워크플로 프로세스	워크플로 작업/활동
CertifyRoleApprovalProcess**	역할 인증 승인
협업 프로세스*	
CreateGroupApproveProcess	그룹 만들기 승인
CreateOrganizationApproveProcess	조직 만들기 승인
CreateUserApproveProcess	사용자 만들기 승인
DeleteGroupApproveProcess	그룹 삭제 승인

워크플로 프로세스	워크플로 작업/활동
DeleteOrganizationApproveProcess	조직 삭제 승인
DeleteUserApproveProcess	사용자 삭제 승인
ModifyAccessRoleMembershipApproveProcesses	액세스 역할 멤버십 수정 승인
ModifyAdminRoleMembershipApproveProcesses	관리자 역할 멤버십 수정 승인
ModifyGroupMembershipApproveProcess	그룹 멤버십 수정 승인
ModifyIdentityPolicySetApproveProcess	아이덴티티 정책 세트 수정 승인
ModifyOrganizationApproveProcess	조직 수정 승인
ModifyUserApproveProcess	사용자 수정 승인
SelfRegistrationApproveProcess	자체 등록 승인
SingleStepApproval*	
TwoStageApprovalProcess*	

참고: 별표(*) 한 개가 표시된 워크플로 프로세스는 템플릿 방법에 사용하도록 디자인되었습니다. 사용자 콘솔에서 구성되므로 관련된 기본 작업이나 활동이 없습니다. **CertifyRoleApprovalProcess(**)**는 사용자 지정 참여자 해결 프로그램을 보여 주는 샘플 프로세스입니다.

워크플로 활동을 승인 작업과 연결

워크플로 활동을 워크플로 승인 작업과 연결하려면 **WorkPoint Designer** 에서 이름/값 쌍을 정의합니다.

참고: 워크플로 활동에 대해 이름/값 쌍이 정의되어 있지 않으면 기본적으로 **CA Identity Manager** 에서 승인 태스크와 일치하는 이름을 가진 태스크를 사용합니다.

워크플로 활동을 승인 작업과 연결하려면

1. **WorkPoint Designer** 를 시작합니다.
2. "파일", "열기", "프로세스"를 클릭합니다.
3. 워크플로 프로세스를 선택하고 "열기"를 클릭합니다.

4. 프로세스의 활동 노드를 마우스 오른쪽 단추로 클릭하고 "속성"을 선택합니다.
5. "유형" 드롭다운 메뉴에서 "텍스트"를 선택합니다.
6. "사용자 데이터" 탭에서 다음을 입력합니다.
 - 이름 - TASK_TAG
 - 값 - 승인 작업 태그 이름
7. "추가"를 클릭합니다.
8. OK 를 클릭하여 변경 사항을 저장합니다.

끝점에 대한 승인 태스크 만들기

계정 관리 화면에 대한 승인 태스크를 만들 수 있습니다. 계정 수정을 승인하는 태스크의 경우 승인 화면이 끝점 유형별로 달라야 하며, 따라서 승인자가 변경된 값을 볼 수 있어야 합니다. 태스크 만들거나 수정에 대한 승인 태스크를 만들려면 다음 절차를 수행하십시오.

끝점을 위한 승인 태스크를 만들려면

1. 사용자 콘솔에서 "역할 및 태스크", "관리자 태스크", "관리자 태스크 만들기"를 클릭합니다.
2. 끝점에서 계정을 관리하는 데 사용되는 "관리자 태스크 사본 만들기"를 선택합니다.

이름은 **create** 로 시작하며 끝점 유형의 이름을 나타냅니다. 예를 들어 **Create Active Directory Account** 입니다.

3. "프로필" 탭에서 다음과 같이 변경합니다.
4. 새 태스크의 이름을 변경합니다.
 - 태스크 태그를 변경합니다.
 - 동작을 "이벤트 승인"으로 변경합니다.
5. "탭" 탭에서 다음과 같이 변경합니다.
 - a. 모든 관계 탭을 제거합니다.
 - b. 탭에서 필요한 승인 화면을 복사하고 편집합니다.

참고: 승인 태스크에서 계정 화면을 사용할 때 문제가 발생할 수 있으며 승인 태스크에서 작동할 수 있도록 기본 계정 화면을 변경해야 할 수 있습니다.

6. "제출"을 클릭합니다.

참여자 해결 프로그램: WorkPoint 방법

WorkPoint 방법을 사용하여 참여자를 지정하려면 WorkPoint Designer 에서 다음과 같은 활동 속성을 정의하십시오.

- CA Identity Manager 와 워크플로 서버 간의 통신을 가능하게 하는 미리 정의된 CA Identity Manager 스크립트의 이름. 이 스크립트는 활동 참여자에 대한 요청을 CA Identity Manager 에 통보한 다음 해당 목록을 워크플로 서버에 제공합니다.
- 하나 이상의 참여자 해결 프로그램에 대한 참조

참여자 해결 프로그램의 유형

워크플로 활동 속성에 특정 참여자 목록을 입력하는 대신 참여자가 *참여자 해결 프로그램*에 매핑된 임의 이름으로 참조됩니다.

미리 정의된 프로세스 모델의 경우 4 가지 참여자 해결 프로그램 유형이 있습니다.

역할 참여자 해결 프로그램

참여자가 특정 역할의 구성원임을 지정합니다.

그룹 참여자 해결 프로그램

참여자가 특정 그룹의 구성원임을 지정합니다.

사용자 지정 참여자 해결 프로그램

참여자가 사용자 지정 참여자 해결 프로그램에서 결정됨을 지정합니다.

필터 참여자 해결 프로그램

참여자가 검색 필터를 통해 선택됨을 지정합니다.

역할 참여자 해결 프로그램

역할 유형 참여자 해결 프로그램을 사용하면 CA Identity Manager 에서 해당 역할의 모든 구성원을 검색하여 참여자로 반환합니다.

"활동" 대화 상자의 UserData 매개 변수에 해결 프로그램 유형이 지정되어 있지 않으면 기본적으로 역할 유형 해결 프로그램이 사용됩니다.

"WorkPoint 활동 속성" 대화 상자의 "사용자 데이터" 탭에서 참여자 해결 프로그램을 지정하지 않으면 기본적으로 CA Identity Manager 는 이 승인 태스크가 포함된 사용 가능한 모든 역할을 찾아 해당 역할 구성원을 참여자로 반환합니다.

역할 참여자 해결 프로그램을 구성하려면

1. WorkPoint Designer 를 시작합니다.
2. "파일", "열기", "프로세스"를 클릭합니다.
3. 워크플로 프로세스를 선택하고 "열기"를 클릭합니다.
4. 프로세스의 활동 노드를 마우스 오른쪽 단추로 클릭하고 "속성"을 선택합니다.
5. "유형" 드롭다운 메뉴에서 "텍스트"를 선택합니다.
6. "사용자 데이터" 탭에서 다음을 입력합니다.
 - 이름 - APPROVER_ROLE_NAME
 - 값 - CA Identity Manager 역할의 이름(예: 보안 관리자)
7. "추가"를 클릭합니다.

참고: 이 역할에 승인 작업이 포함될 필요는 없습니다.
8. "유형" 드롭다운 메뉴에서 "텍스트"를 선택합니다.
9. "사용자 데이터" 탭에서 다음과 같은 이름/값 쌍을 입력합니다(선택 사항).

이름—APPROVERS_REQUIRED

값 - YES

10. "추가"를 클릭합니다.

참고: 기본 승인 설정은 APPROVERS_REQUIRED=NO 입니다. 이 경우 참여자가 없으면 활동은 자동으로 승인됩니다.

APPROVERS_REQUIRED=YES 이고 CA Identity Manager 에서 참여자를 찾지 못하면 활동이 성공적으로 완료되지 않습니다.
11. OK 를 클릭하여 변경 사항을 저장합니다.

그룹 참여자 해결 프로그램

그룹 유형 참여자 해결 프로그램을 사용하면 CA Identity Manager 에서 해당 그룹의 모든 구성원을 검색하여 참여자로 반환합니다.

그룹 참여자 해결 프로그램을 구성하려면

1. WorkPoint Designer 를 시작합니다.
2. "파일", "열기", "프로세스"를 클릭합니다.

3. 워크플로 프로세스를 선택하고 "열기"를 클릭합니다.
4. 프로세스의 활동 노드를 마우스 오른쪽 단추로 클릭하고 "속성"을 선택합니다.
5. "유형" 드롭다운 메뉴에서 "텍스트"를 선택합니다.
6. "사용자 데이터" 탭에서 다음을 입력합니다.
 - 이름 - APPROVER_GROUP_UNIQUENAME
 - 값 - CA Identity Manager 그룹의 이름
7. "추가"를 클릭합니다.
8. "유형" 드롭다운 메뉴에서 "텍스트"를 선택합니다.
9. "사용자 데이터" 탭에서 다음과 같은 이름/값 쌍을 입력합니다(선택 사항).
 - 이름 - APPROVERS_REQUIRED
 - 값 - YES
10. "추가"를 클릭합니다.

참고: 기본 승인 설정은 APPROVERS_REQUIRED=NO 입니다. 이 경우 참여자가 없으면 활동은 자동으로 승인됩니다.

APPROVERS_REQUIRED=YES 이고 CA Identity Manager 에서 참여자를 찾지 못하면 활동이 성공적으로 완료되지 않습니다.
11. OK 를 클릭하여 변경 사항을 저장합니다.

사용자 지정 참여자 해결 프로그램

사용자 지정 참여자 해결 프로그램은 워크플로 활동 참여자를 결정하는 Java 개체이며 CA Identity Manager 에 목록을 반환합니다. 그런 다음 이 목록은 워크플로 엔진으로 전달됩니다. 일반적으로 표준 참여자 정책에서 활동에 필요한 참여자 목록을 제공할 수 없는 경우에만 사용자 지정 참여자 해결 프로그램을 작성합니다.

참고: 참여자 해결 프로그램 API 를 사용하여 사용자 지정 참여자 해결 프로그램을 만듭니다. 자세한 내용은 *Programming Guide for Java*(Java 프로그래밍 안내서)를 참조하십시오.

사용자 지정 참여자 해결 프로그램을 구성하려면

1. 브라우저에 다음 URL 을 입력하여 관리 콘솔을 엽니다.

`http://hostname/iam/immanage`

hostname

CA CA Identity Manager 가 설치된 서버의 정규화된 도메인 이름을 정의합니다. 예를 들어, `myserver.mycompany.com:port` 와 같이 입력합니다.

2. "환경"을 클릭하고 적절한 CA CA Identity Manager 환경의 이름을 선택합니다.
3. "고급 설정", "워크플로 참여자 해결 프로그램"을 클릭합니다.
4. "워크플로 참여자 해결 프로그램" 화면에서 "새로 만들기"를 클릭하고 다음을 입력합니다.

이름

사용자 지정 참여자 해결 프로그램 이름을 지정합니다(예: `APPROVER_CUSTOMRESOLVER_NAME`).

설명

사용자 지정 참여자 해결 프로그램에 대한 설명을 지정합니다.

클래스

Java 클래스 이름을 지정합니다(예: `com.netegrity.samples.GroupFinder`).

5. "저장"을 클릭합니다.
6. WorkPoint Designer 를 시작합니다.
7. "파일", "열기", "프로세스"를 클릭합니다.
8. 워크플로 프로세스를 선택하고 "열기"를 클릭합니다.
9. 프로세스의 활동 노드를 마우스 오른쪽 단추로 클릭하고 "속성"을 선택합니다.
10. "유형" 드롭다운 메뉴에서 "텍스트"를 선택합니다.

11. "사용자 데이터" 탭에서 다음을 입력합니다.

이름

사용자 지정 참여자 해결 프로그램 이름을 지정합니다. 이 이름은 CA Identity Manager 관리 콘솔의 "사용자 지정 유형 참여자 해결 프로그램" 화면에서 입력한 이름과 일치해야 합니다. 예:

APPROVER_CUSTOMRESOLVER_NAME

값

사용자 지정 해결 프로그램의 고유한 이름을 지정합니다(예: GroupFinder).

12. "추가"를 클릭합니다.

참고: 기본 승인 설정은 APPROVERS_REQUIRED=NO 입니다. 이 경우 참여자가 없으면 활동은 자동으로 승인됩니다.

APPROVERS_REQUIRED=YES 이고 CA Identity Manager 에서 참여자를 찾지 못하면 활동이 성공적으로 완료되지 않습니다.

13. OK 를 클릭하여 변경 사항을 저장합니다.

필터 참여자 해결 프로그램

필터 참여자 해결 프로그램을 사용하면 CA Identity Manager 가 필터 조건과 일치하는 사용자나 그룹을 검색할 수 있습니다. WorkPoint Designer 에서 검색 필터를 지정하면 CA Identity Manager 가 해당 워크플로 활동에 대해 일치하는 승인자를 반환합니다.

WorkPoint 활동 속성 대화 상자의 "사용자 데이터" 탭에서 필터 참여자 해결 프로그램을 만듭니다.

참여자 해결 프로그램 필터 구문

검색 필터를 만들기 위해 결합되는 세 가지 필수 특성은 다음과 같습니다.

- 승인자 특성. 예: 직책
- 승인자 특성 오퍼레이션. 예: 같음
- 승인자 특성 값. 예: 관리자

필수 검색 필터 특성은 다음과 같은 순서로 결합됩니다.

특성 오퍼레이션 값

예:

직책 같음 관리자이거나 부서 포함 급여

필수 참여자 해결 프로그램 필터 특성

필수 참여자 해결 프로그램 필터 특성은 다음과 같습니다.

참고: 각 필터에서 *n* 은 검색 필터 번호를 나타내는 양의 정수입니다.
기본값은 1 입니다.

APPROVER_FILTER_n_ATTRIBUTE

승인자 특성을 지정합니다. 예를 들어, 직함, 부서, 사용자 ID 등이 있습니다. 승인자 특성 이름 문자열은 CA Identity Manager 사용자 특성 이름 문자열과 일치해야 합니다.

APPROVER_FILTER_n_OP

승인자 특성과 관련된 오퍼레이션을 지정합니다. 예를 들어, 같음, 같지 않음, 포함 등이 있습니다. 연산 키워드는 대소문자를 구분하지 않습니다.

이 필터에 유효한 항목은 다음과 같습니다.

- 같음
- 다음으로 시작
- 같지 않음
- 포함
- 다음으로 끝남
- 보다 큼
- 보다 작음
- 크거나 같음
- 작거나 같음

APPROVER_FILTER_n_VALUE

승인자와 관련된 값을 지정합니다. 예를 들어, 관리자, 급여, 엔지니어링 등이 있습니다.

선택적 참여자 해결 프로그램 필터 특성

선택적 참여자 해결 프로그램 필터 특성은 다음과 같습니다.

APPROVER_OBJECTTYPE

사용자 또는 그룹(대소문자를 구분하지 않음)

기본값은 사용자입니다.

APPROVER_ORG_UNIQUENAME

승인자 조직의 고유 이름입니다. 조직 이름 문자열은 Identity Manager 조직 이름 문자열과 일치해야 합니다.

기본값은 root 입니다.

APPROVER_ORG_AND_LOWER

승인자의 조직이나 하위 조직입니다.

- 0 은 승인자 조직의 검색을 의미합니다.
- 1 은 승인자 조직에 있는 모든 하위 조직의 검색을 의미합니다.

기본값은 1 입니다.

APPROVER_FILTER_NO

사용 중인 검색 필터 수입니다. 필터가 두 개 있으면 이 개수는 2 가 됩니다.

기본값은 1 입니다.

참고: 필터 수가 1 보다 클 경우 이 필터는 필수입니다.

APPROVER_FILTER_n_CONJ_TYPE

OR 또는 AND 결합 유형을 사용하여 검색 필터를 결합할 수 있습니다.

참고: OR 결합으로 구분된 필터는 AND 로 구분된 필터보다 우선합니다.

예를 들어, "직함 같음 관리자" AND "부서 같음 개발"을 검색하는 경우 AND 결합 유형을 지정할 수 있습니다.

참고: n 은 검색 필터 번호를 나타내는 1 보다 큰 양의 정수입니다.

참여자 해결 프로그램 필터 추가

참여자 해결 프로그램 필터를 추가하려면

1. WorkPoint Designer 를 시작합니다.
2. "파일", "열기", "프로세스"를 클릭합니다.

3. 워크플로 프로세스를 선택하고 "열기"를 클릭합니다.
4. 프로세스의 활동 노드를 마우스 오른쪽 단추로 클릭하고 "속성"을 선택합니다.
5. "유형" 드롭다운 메뉴에서 "텍스트"를 선택합니다.
6. "사용자 데이터" 탭에서 다음을 입력합니다.
 - 이름 - APPROVER_FILTER_1_ATTRIBUTE
 - 값 - 고유한 역할 식별자(예: 직함)
7. "추가"를 클릭합니다.
8. 검색 필터의 각 특성에 대해 6 단계와 7 단계를 반복합니다.

참고: 기본 승인 설정은 APPROVERS_REQUIRED=NO 입니다. 이 경우 참여자가 없으면 활동은 자동으로 승인됩니다.

APPROVERS_REQUIRED=YES 이고 CA Identity Manager 에서 참여자를 찾지 못하면 활동이 성공적으로 완료되지 않습니다.

9. OK 를 클릭하여 변경 사항을 저장합니다.

예: 필터 참여자 해결 프로그램

다음 표의 사용자 저장소에는 사용자 ID, 직함 및 부서 특성을 가진 네 사용자(Holly, Sarah, John 및 Dave)가 포함되어 있습니다.

User	ID	제목	부서
Holly	admin1	시스템 관리	관리
Sarah	test1	시스템 관리	개발
John	admin2	관리자	개발
Dave	admin3	시스템 관리	회계

CA Identity Manager 는 앞의 사용자 저장소에 대해 다음 테이블에 정의된 세 개의 필터를 적용합니다.

이름	값
APPROVER_FILTER_NO	3
APPROVER_FILTER_1_ATTRIBUTE	uid

이름	값
APPROVER_FILTER_1_OP	같음
APPROVER_FILTER_1_VALUE	admin*
APPROVER_FILTER_2_CONJ_TYPE	AND
APPROVER_FILTER_2_ATTRIBUTE	부서
APPROVER_FILTER_2_OP	같음
APPROVER_FILTER_2_VALUE	관리
APPROVER_FILTER_3_CONJ_TYPE	OR
APPROVER_FILTER_3_ATTRIBUTE	직함
APPROVER_FILTER_3_OP	같음
APPROVER_FILTER_3_VALUE	시스템 관리

CA Identity Manager 는 다음 순서대로 필터를 적용합니다.

1. OR 결합으로 연결된 두 번째 필터와 세 번째 필터를 평가합니다.

"부서 같음 관리" OR "직함 같음 시스템 관리"

여기서 John 은 제외되고 Holly, Sarah 및 Dave 가 반환됩니다.

2. AND 결합으로 연결된 첫 번째 필터와 두 번째 필터를 평가합니다(여기서 *는 와일드카드 문자임).

"uid 같음 admin*" AND "부서 같음 관리"

여기서 Sarah 가 제외되고 Holly 와 Dave 가 반환됩니다.

사용자 저장소에서 반환되는 최종 사용자는 Holly 와 Dave 입니다.

참여자 해결 프로그램 우선 순위 순서

참여자 해결 프로그램을 지정하지 않으면 기본적으로 Identity Manager 는 승인 작업이 포함된 사용 가능한 모든 역할을 식별하여 해당 역할 구성원을 참여자로 반환합니다.

참여자 해결 프로그램을 두 개 이상 지정하면 Identity Manager 는 이 우선 순위 순서를 사용하여 평가합니다.

1. Custom
2. 역할

3. 필터
4. Group

Identity Manager 는 이 우선 순위 순서에서 첫 번째 해결 프로그램을 식별 및 적용하고 나머지 해결 프로그램은 모두 무시합니다.

한 번에 하나의 해결 프로그램만 있어야 합니다. 또한 Identity Manager 가 참여자를 올바르게 식별하도록 해결 프로그램이 제대로 구성되었는지 확인합니다.

워크플로 리소스 스크립트 지정

Identity Manager 에는 Identity Manager 와 워크플로 서버 간에 정보를 전달하는 IM 승인자라는 스크립트가 포함되어 있습니다.

워크플로 활동에 참여자 목록이 필요한 경우 스크립트에서 활동 이름, WorkPoint 활동 속성 대화 상자의 "사용자 데이터" 탭에 제공된 참여자 식별자 및 "사용자 데이터" 탭에 제공된 다른 모든 정보를 Identity Manager 에 전달합니다. Identity Manager 는 참여자를 검색하여 목록을 다시 스크립트에 전달합니다. 그런 다음 스크립트에서 이 목록을 워크플로 서버에 제공합니다.

새 워크플로 프로세스 정의가 있고 워크플로 프로세스 활동이 Identity Manager 워크플로 승인 작업이면 WorkPoint 활동 속성 대화 상자의 "리소스" 탭에서 IM 승인자 스크립트를 지정해야 합니다.

WorkPoint Designer 에서 IM 승인자 스크립트를 지정하려면

1. "리소스" 탭에서 "선택"을 클릭합니다.
2. "리소스 선택" 대화 상자의 드롭다운 목록에서 "규칙"을 선택합니다. 이 동작은 활동과 연결할 수 있는 규칙(스크립트)을 표시합니다.
3. 스크립트 이름인 IM 승인자를 선택하고 "추가"를 클릭합니다.
4. "확인"을 클릭한 다음 "활동 속성" 대화 상자에서 "적용"을 클릭합니다.

참고: IM 승인자 스크립트를 수정하지 마십시오.

사용자 인증 작업에 대해 참여자 지정

"사용자 인증" 작업은 `CertifyRoleEvent` 이벤트를 생성합니다. 이 이벤트에는 미리 정의된 `CertifyRoleApproveProcess` 프로세스를 통해 워크플로 승인이 적용될 수 있습니다.

`Identity Manager`에는 기본적으로 환경에 표시되는 미리 정의된 참여자 해결 프로그램인 `CertifyRoleParticipantResolver`도 포함되어 있습니다. `CertifyRoleApprovalProcess`의 활동에 대한 참여자는 `CertifyRoleParticipantResolver`를 통해 지정됩니다.

참여자 구성 정보를 제공하려면

1. 브라우저에 다음 URL을 입력하여 관리 콘솔을 엽니다.

`http://hostname/iam/immanage`

hostname

CA CA Identity Manager가 설치된 서버의 정규화된 도메인 이름을 정의합니다. 예를 들어, `myserver.mycompany.com:port`와 같이 입력합니다.

2. "환경"을 클릭하고 적절한 CA CA Identity Manager 환경의 이름을 선택합니다.
3. "고급 설정"을 클릭한 다음 "기타"를 클릭합니다.
4. 인증할 각 역할에 대해 승인자를 지정하는 이름/값 쌍을 정의합니다.
 - "속성" 필드에서는 *역할 유형.역할 이름* 형식을 사용합니다.
*역할 유형*은 관리자, 액세스, 프로비저닝 역할 중 하나여야 합니다.
*역할 이름*은 기존 역할의 이름입니다.
 역할 이름과 역할 유형을 마침표(.)로 구분해야 합니다.
 - "값" 필드에서 승인자의 ID를 지정하고 ID를 세미콜론(;)으로 구분합니다.

다음 예에서는 다음 참여자가 다음 역할에 대해 사용자 인증을 승인할 수 있습니다.

- jsmith01 과 ajones19 는 "사용자 관리자" 역할에 대한 인증을 승인할 수 있습니다.
- plewis12 는 "시스템 관리자" 역할의 유일한 승인자입니다.
- rtrevor8 과 pkitt3 은 "내 액세스 역할"에 대한 인증을 승인할 수 있습니다.

속성	값
관리자.사용자 관리자	jsmith01;ajones19
관리자.시스템 관리자	plewis12
액세스.내 액세스 역할	rtrevor8;pkitt3

참고: 지정되지 않은 모든 역할에는 CertifyRoleEvent 에 대한 승인자가 없습니다.

WorkPoint Designer 의 프로세스

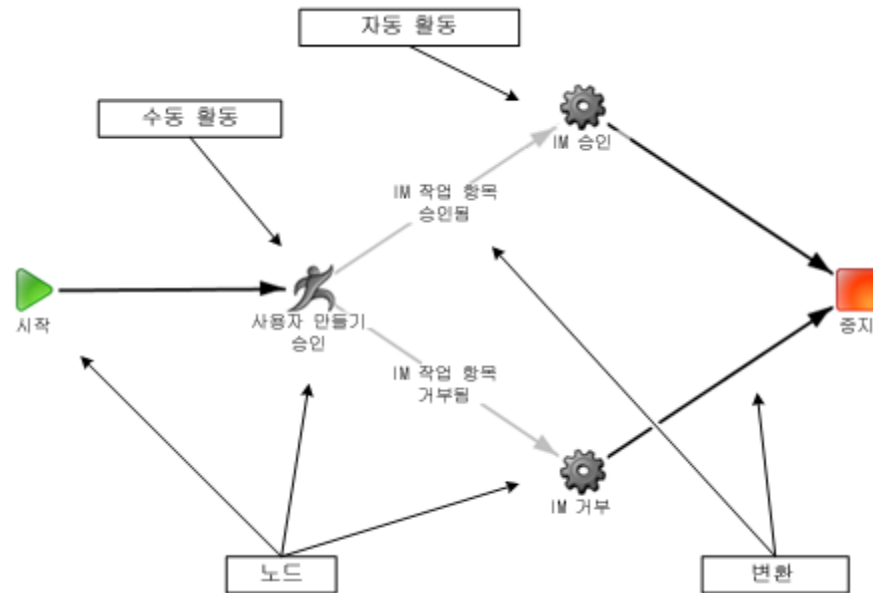
WorkPoint Designer 에서 Identity Manager 와 함께 제공되는 기본 워크플로 프로세스와 활동을 사용자 지정하거나 새로 만들 수 있습니다.

이 문서에서는 Identity Manager 와 관련된 WorkPoint 워크플로 정보를 제공합니다. 자세한 내용은 WorkPoint Designer 설명서를 참조하십시오.

참고: 기존 Identity Manager 프로세스의 사본을 만든 다음 요구에 맞게 새 프로세스를 수정하여 워크플로 프로세스를 만들 수 있습니다. 이런 방식으로 만든 워크플로 프로세스에는 전환 스크립트, 자동화된 활동 등 Identity Manager 와 관련된 기본 요소와 노드가 포함되어 있습니다.

WorkPoint 프로세스 다이어그램

다음 다이어그램은 Identity Manager 작업을 제어하는 프로세스에 대한 최소 구성 요소 세트가 있는 일반적인 워크플로 프로세스를 보여 줍니다. 또한 "사용자 만들기" 작업의 실행을 제어하는 미리 정의된 CreateUserApproveProcess 프로세스를 보여 줍니다.



WorkPoint 프로세스 구성 요소

워크플로 프로세스에는 다음 노드와 전환이 포함되어 있습니다.

시작

모든 워크플로 프로세스가 이 노드로 시작합니다.

중지

모든 워크플로 프로세스가 이 노드로 끝납니다.

수동 활동

수동 활동은 참여자에 의한 Identity Manager 작업의 승인 또는 거부가 필요하며, Identity Manager 워크플로 승인 작업과 동일한 이름을 가져야 합니다.

Identity Manager 작업을 제어하는 워크플로 프로세스에는 해당 작업의 승인을 요청하는 수동 활동이 하나 이상 포함되어 있어야 합니다.

자동화된 활동

자동화된 활동에는 다음 두 스크립트 중 하나가 할당됩니다.

- IM 승인 통보 - 워크플로 제어 하에 Identity Manager 작업을 실행하도록 Identity Manager 에 알립니다.
- IM 거부 통보 - Identity Manager 작업 실행을 취소하도록 Identity Manager 에 알립니다.

일반적으로 "IM 승인 통보" 스크립트는 모든 수동 활동이 승인된 경우에 활성화되고, "IM 거부 통보" 스크립트는 거부된 수동 활동이 있는 경우에 활성화됩니다.

무조건 전환

무조건 전환은 워크플로 프로세스에 있는 한 노드에서 다른 노드로의 경로이며 조건 스크립트와 연결되어 있지 않습니다.

조건부 전환

조건부 전환은 워크플로 프로세스에 있는 한 노드에서 다른 노드로의 대체 경로이며 조건 스크립트와 연결되어 있습니다.

조건 스크립트는 관련된 활동의 결과를 평가하여 전환을 수행할지 여부를 결정합니다. 스크립트에서 True 를 반환하면 전환이 수행되고 프로세스가 표시된 다음 노드로 이동합니다.

둘 이상의 조건 스크립트에서 True 를 반환하도록 할 수 있습니다. 이렇게 하면 각 스크립트에 서로 다른 전환이 연결되므로 활동이 병렬로 수행될 수 있습니다.

참고: 조건부 전환에 사용자 지정 스크립트를 사용할 수 있습니다. 자세한 내용은 *Programming Guide for Java*(Java 프로그래밍 안내서)를 참조하십시오.

수동 활동 속성

다음 표에서는 Identity Manager 와 관련된 속성 설정을 보여 줍니다. 이러한 설정은 WorkPoint Designer 활동 속성 대화 상자의 지정된 탭에서 정의됩니다.

속성 탭	속성 설명
리소스	IM 승인자 - "포함" 목록에서 지정됩니다. 이 스크립트는 Identity Manager 와 워크플로 서버 간에 정보를 전달합니다.

속성 탭	속성 설명
에이전트	자동 완료되지 않음 - "비동기" 목록에서 지정되고 "사용 가능" 상태와 연결됩니다. 이 스크립트는 활동 참여자가 없는 경우 활동을 승인된 것으로 간주할지 여부를 결정합니다.
사용자 데이터	Identity Manager 가 활동 참여자를 검색하는 데 사용하는 이름/값 쌍을 정의합니다. 선택적으로, 사용자 지정 참여자 해결 프로그램에 전달할 데이터를 정의할 수도 있습니다.

조건부 전환 속성

다음 기본 스크립트는 "전환 속성" 대화 상자의 "조건" 탭에 나타납니다.

IM 작업 항목 승인됨

관련된 활동이 승인된 경우 **True** 를 반환합니다. 워크플로 프로세스가 전환에 표시된 다음 노드로 이동합니다.

IM 작업 항목 거부됨

관련된 활동이 거부된 경우 **True** 를 반환합니다. 워크플로 프로세스가 전환에 표시된 다음 노드로 이동합니다.

작업 및 프로세스 인스턴스

워크플로 프로세스는 Identity Manager 가 특정 작업을 완료하기 전에 수행해야 하는 단계를 정의합니다. 작업은 워크플로 프로세스의 런타임 인스턴스입니다.

예를 들어, 기본 워크플로 프로세스인 **CreateUserApproveProcess** 는 새 사용자가 승인되려면 수행해야 하는 단계를 정의합니다. 새 사용자가 실제로 Identity Manager 에서 만들어졌으며 작업이 승인을 위해 제출된 경우 **CreateUserApproveProcess** 의 작업 인스턴스가 WorkPoint Designer 에서 만들어집니다.

워크플로 프로세스 편집에 사용되는 인터페이스와 유사한 인터페이스를 사용하여 WorkPoint Designer 에서 작업을 열어서 보고 수정할 수 있습니다.

동일한 프로세스를 기반으로 하는 여러 작업이 동시에 존재할 수 있습니다.

작업 필터링

WorkPoint Designer에는 다양한 조건을 기반으로 작업을 검색할 수 있는 필터링이 포함되어 있습니다. 예를 들어, 다음과 같은 작업을 검색할 수 있습니다.

- 하나 이상의 선택된 워크플로 프로세스를 기반으로 하는 작업
- 사용자 정의 작업 참조나 고유한 작업 ID가 있는 작업
- 특정 상태(예: 활성화, 완료 또는 일시 중지됨)에 있는 작업
- 지정한 데이터 범위 내에서 만들어졌거나 시작된 작업

참고: 작업 필터링에 대한 지침과 참조 정보는 WorkPoint Designer 설명서를 참조하십시오.

작업 상태 및 속성

작업을 열면 작업의 워크플로 다이어그램이 표시됩니다. 워크플로 활동 노드와 전환은 수행되었는지 여부를 나타내는 색으로 렌더링됩니다.

다음은 보고, 경우에 따라 수정할 수 있습니다.

- 참여자 및 작업 기록 정보를 비롯한 작업의 속성
- 열린 작업의 상태(예: 완료되었는지 여부)
- 작업에 포함된 개별 노드 및 전환의 속성

활동 및 작업 항목 속성

다음은 비롯한 작업 활동 속성과 프로세스 활동 속성을 보고, 경우에 따라 수정할 수 있습니다.

- 활동 상태 정보
- 활동 승인 정보
- 승인 작업(WorkPoint Designer에서는 *작업 항목*이라고 함) 정보. 예:
 - 다른 승인자의 작업 목록에서 항목을 제거하는 보류된 작업 항목을 가진 참여자가 없는 경우 "사용 가능" 상태가 되고 참여자 사용자 ID는 표시되지 않습니다.

- 참여자가 작업 항목을 보류했지만 완료하지 않은 경우 "열림" 상태가 되고 참여자의 사용자 ID 와 보류 시간이 표시됩니다.
- 작업 항목이 완료된 경우 "완료" 상태가 됩니다. 워크플로 제어 하의 작업을 승인하거나 거부한 참여자의 사용자 ID 가 완료 시간과 함께 표시됩니다.

특정 작업 항목 속성에는 다음이 포함됩니다.

- 작업 항목 이름 및 현재 상태
- 지정된 상태에 대해 책임이 있는 참여자의 사용자 ID 를 비롯한 상태 기록 정보
- 권한 있는 작업 항목 참여자 정보

참고: 작업, 활동 및 작업 항목 속성에 대한 자세한 내용은 WorkPoint Designer 설명서를 참조하십시오.

워크플로 활동 수행

워크플로 프로세스에서 수동 활동은 승인 작업과 관련된 이벤트를 승인하거나 거부하는 활동 참여자로 지정된 사람에 의해 수행됩니다. 참여자는 Identity Manager 에서 이 활동을 수행합니다.

Identity Manager 승인 작업과 관련된 활동을 수행하면 다음과 같은 작업이 수행됩니다.

1. Identity Manager 가 참여자에게 통보합니다.
2. 참여자가 작업을 승인하거나 거부합니다.
3. 워크플로 서버에서 활동을 완료합니다.

참여자 찾기 및 통보

Identity Manager 승인 작업과 관련된 워크플로 활동이 시작되면 워크플로 서버에서 활동 참여자에 대한 정보를 Identity Manager 에 전달합니다. 이 정보는 활동 속성에서 정의됩니다. Identity Manager 는 이 정보를 사용하여 활동 참여자를 검색하고 승인 작업이 보류 중이라고 알립니다.

참여자를 식별한 후 Identity Manager 는 각 참여자의 작업 목록에 새 작업 항목(승인 작업)을 추가합니다. 선택적으로, Identity Manager 는 각 참여자에게 새 작업 항목에 대한 전자 메일 통보도 보냅니다.

참고: APPROVERS_REQUIRED 활동 속성이 False 로 설정되어 있고 참여자가 없으면 기본적으로 작업이 승인된 것으로 간주됩니다.

참고: "상태" 열의 원은 참여자가 승인 작업을 가져갈 수 있음을 나타냅니다. 확인 표시는 작업 목록 소유자가 승인 작업에 동의했지만 아직 완료하지 않았음을 나타냅니다.

승인 작업에 동의 및 수행

참여자가 있으면 한 참여자가 승인 작업에 동의하고 워크플로 제어 하의 작업을 승인하거나 거부할 때까지 활동을 완료할 수 없습니다.

참여자는 워크플로 활동 콘솔에서 작업 항목 이름을 클릭한 다음 "항목 보류"를 클릭하여 승인 작업에 동의합니다. 항목을 보류하면 다른 승인자의 작업 목록에서 해당 항목이 제거됩니다.

참여자는 승인 작업에 동의한 후 워크플로 제어 하의 작업에 대한 승인 또는 거부 결정을 합니다. 여러 참여자가 동일한 승인 작업에 동의할 수 없으므로 다른 참여자의 작업 목록에서 승인 작업이 제거됩니다.

참여자가 승인 작업에 동의한 후 승인 화면이 나타납니다. 참여자는 여기서 다음 동작 중 하나를 수행할 수 있습니다.

- 워크플로 제어 하의 작업을 즉시 승인하거나 거부합니다.
- 다른 참여자가 사용할 수 있도록 승인 작업을 방출합니다.
- 대화 상자를 닫고 나중에 활동을 완료합니다. 참여자가 위에 표시된 "사용자 만들기 승인" 대화 상자를 다시 열려면 작업 목록에서 승인 작업의 이름을 클릭합니다.

참여자는 승인 화면에서 수정 가능한 필드(있는 경우)를 하나 이상 업데이트할 수도 있습니다. 작업을 만들 때 이 화면의 필드를 수정 가능하도록 설정할 수 있습니다.

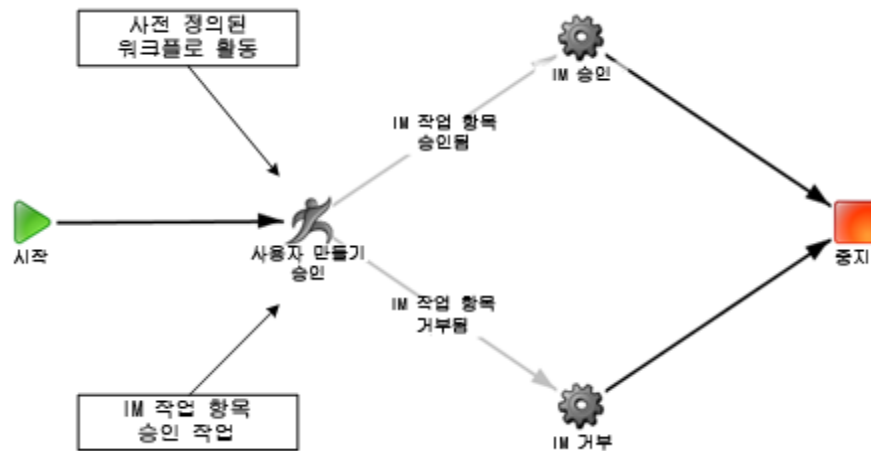
참여자가 워크플로 제어 하의 작업을 승인하거나 거부한 후 활동이 완료되고, 다음 섹션에 설명된 대로 워크플로 프로세스가 활동 결과에서 결정된 경로를 따라 계속될 수 있습니다.

워크플로 서버에서 활동 완료

수동 활동에서 발생한 둘 이상의 조건부 전환과 함께 수동 활동이 Designer 창에 나타납니다.

각 조건부 전환에는 스크립트가 연결되어 있습니다. 참여자가 활동을 완료하면 스크립트에서 활동 결과를 평가합니다. 이러한 평가 결과에 따라 프로세스 흐름의 방향이 결정됩니다.

다음 그림에서는 Designer 의 "사용자 만들기 승인" 활동 및 동일한 이름을 가진 Identity Manager 의 해당 승인 작업을 보여 줍니다.



활동 참여자(또는 승인자)가 Identity Manager 에서 "승인" 또는 "거부" 단추를 클릭하면 다음 작업이 수행됩니다.

1. 프로세스 작업 인스턴스의 "사용자 만들기 승인" 활동이 끝납니다. 조건부 전환과 관련된 스크립트에서 활동 결과를 평가합니다.
2. True 로 평가되는 조건부 전환에 따라 작업 인스턴스가 계속됩니다.
 - 활동이 승인되면 IM 작업 항목 승인됨 스크립트에서 True 를 반환합니다. 워크플로에서 IM 작업 항목 승인됨 전환을 다음 노드로 이동합니다. 자동화된 활동인 IM 승인은 Identity Manager 에 "사용자 만들기" 작업을 실행하도록 통보합니다.
 - 활동이 거부되면 IM 작업 항목 거부됨 스크립트에서 True 를 반환합니다. 워크플로에서 IM 작업 항목 거부됨 전환을 다음 워크플로 노드로 이동합니다. 자동화된 활동인 IM 거부는 Identity Manager 에 "사용자 만들기" 작업을 취소하도록 통보합니다.

Workpoint 작업 보기

다음은 통해 사용자 콘솔에서 **Workpoint** 작업의 런타임 상태를 볼 수 있습니다.

- 승인 태스크
- 제출한 태스크 보기.

새 환경에서 모든 승인 태스크는 기본적으로 "태스크 보기" 탭을 포함합니다. 이 릴리스에서 생성된 이벤트만 "제출한 태스크 보기"의 선택한 이벤트 또는 태스크에 대해 호출된 모든 프로세스 정의에 대한 작업 이미지 보기를 지원합니다. 이전 릴리스에서 생성된 이벤트는 워크플로 작업 보기 기능을 지원하지 않습니다.

기존 승인 탭에 작업 보기 탭 추가

승인 태스크의 경우 해당 작업 항목에 대한 작업 이미지를 보려면 새 "작업 보기" 탭을 모든 기존 태스크에 추가해야 합니다.

참고: 새 환경에는 모든 승인 태스크에 대해 이 탭이 포함됩니다.

기존 태스크에 작업 보기 탭을 추가하려면

1. "관리자 태스크 및 역할" 범주에서 "관리자 태스크", "관리자 태스크 수정"을 선택하여 **ModifyAdminTask** 를 실행합니다.
2. "검색"을 클릭하고 승인 태스크(예를 들어, 사용자 만들기 승인)를 선택한 다음 "선택"을 클릭합니다.
"관리자 태스크 수정: 사용자 만들기 승인" 대화 상자가 나타납니다.
3. "탭" 탭을 클릭하고 드롭다운 메뉴에서 "작업 보기(JobView)"를 선택한 다음 "제출"을 클릭합니다.

"작업 보기" 탭이 승인 태스크에 추가되었습니다.

모든 기존 승인 태스크에 대해 반복합니다.

작업 보기 탭 구성

다음 항목을 사용하여 이 탭을 구성하십시오.

이름

탭에 할당하는 이름입니다.

태그

작업 내에서 고유한 탭의 식별자입니다. 문자나 밑줄로 시작해야 하며 문자, 숫자 또는 밑줄만 사용해야 합니다. 태그는 주로 XML 문서나 HTTP 매개 변수를 통해 데이터 값을 설정하는 데 사용됩니다.

탭 숨기기

탭이 작업에 표시되지 않도록 합니다. 이 옵션은 탭을 숨겨야 하지만 탭의 특성에 대한 액세스가 필요한 응용 프로그램에 유용합니다.

작업 보기

이 탭에는 지정된 작업 항목에 대한 작업 이미지가 표시됩니다.

승인 태스크에서 작업 보기 탭 보기

승인 태스크에서 "작업 보기" 탭을 보려면 다음 절차를 수행하십시오.

작업 보기 탭을 보려면

1. "작업 목록" 대화 상자에서 보려는 승인 태스크를 선택합니다.
2. "작업 보기" 탭을 클릭하여 태스크의 런타임 상태를 확인합니다.

여기서 태스크를 "승인", "거부", "보류"하거나 탭을 닫을 수 있습니다.

또는 "홈" 탭과 "View my Worklist(내 작업 목록 보기)"를 클릭하여 "작업 목록" 대화 상자를 열 수 있습니다.

EventLevel 워크플로의 워크플로 작업 보기

"제출한 태스크 보기"에서 EventLevel 워크플로의 워크플로 작업을 보려면 다음 절차를 수행하십시오.

워크플로 작업을 보려면

1. "시스템" 탭에서 "제출한 태스크 보기"를 선택하고 검색 기준을 입력한 다음 "검색"을 선택합니다.
2. 이벤트를 선택하고 연필을 클릭하여 이벤트의 상세 정보를 확인합니다.
3. "이벤트 워크플로 작업 보기" 아래에서 프로세스를 선택하고 연필을 클릭하여 이 이벤트의 작업 이미지를 확인합니다.

태스크 수준 워크플로에 대한 워크플로 작업 보기

"제출한 태스크 보기"에서 태스크 수준 워크플로에 대한 워크플로 작업을 보려면 다음 절차를 따르십시오.

워크플로 작업을 보려면

1. "시스템" 탭에서 "제출한 태스크 보기"를 선택하고 검색 기준을 입력한 다음 "검색"을 선택합니다.
2. 태스크를 선택하고 연필을 클릭하여 태스크 상세 정보를 봅니다.

"태스크 워크플로 작업 보기" 아래에서 프로세스를 선택하고 연필을 클릭하여 이 태스크에 대한 작업 이미지를 봅니다.

정책 기반 워크플로

정책 기반 워크플로를 사용하여 규칙 평가에 따라 이벤트 또는 관리자 태스크에 워크플로 컨트롤을 적용할 수 있습니다. 이것은 워크플로 프로세스를 항상 실행하는 이벤트 또는 관리자 태스크 대신, 이벤트 또는 관리자 태스크와 관련된 규칙이 **true** 인 경우에만 워크플로 프로세스가 작업 항목을 실행하고 생성함을 의미합니다.

승인 규칙은 워크플로 프로세스를 시작할지 여부를 결정하는 조건입니다. 워크플로 프로세스가 시작되면 작업 항목을 승인자의 작업 목록에 추가하여 이벤트 또는 관리자 태스크에 워크플로 컨트롤을 적용합니다.

승인 정책은 승인 규칙, 규칙 평가 유형, 정책 순서, 정책 설명, 워크플로 프로세스의 조합입니다.

예를 들어, 새 그룹을 만들 때 **CreateGroupEvent** 에 워크플로 컨트롤을 적용하고 새 그룹이 지정된 상위 조직의 부분인 경우에만 작업 항목을 만드는 승인 정책을 정의할 수 있습니다. 새 그룹이 해당 조직에 속하지 않으면 워크플로 프로세스는 실행되지 않고 작업 항목이 만들어지지 않습니다.

이벤트에 여러 규칙이 있는 경우 이벤트가 승인되려면 이벤트와 연결된 모든 작업흐름 프로세스가 승인되어야 합니다. 관리자 태스크의 경우에도 마찬가지로 **CreateGroupTask** 에 워크플로 컨트롤을 적용하고 새 그룹의 이름이 **Sales** 로 시작하는 경우에만 작업 항목을 만드는 승인 정책을 정의할 수 있습니다. 새 그룹의 이름이 **Sales** 로 시작하지 않으면 워크플로 프로세스가 실행되지 않고 작업 항목이 만들어지지 않습니다.

항상 평가되거나 관리 개체의 지정된 특성이 변경될 때만(예를 들어, 직원의 급여 값을 변경할 때) 평가되는 정책 규칙을 만들 수 있습니다.

참고: 정책 기반 워크플로의 이전 버전에서는 승인자가 특성을 변경하는 경우 특성이 재승인을 위해 발송되었습니다. 특성 수준 승인 및 거부를 사용하면 변경 내용은 아무 단계에서나 단 한 번 승인됩니다. 규칙에 포함된 특성이 수정되는 경우에도 작업 항목은 재승인을 위해 제출되지 않습니다. 승인자가 변경 내용을 승인하면 새 변경 내용이 제출되거나 태스크가 다시 제출되지 않는 승인자에게 해당 변경 내용이 다시 표시되지 않습니다.

기본 워크플로 프로세스

모든 기본 워크플로 템플릿 및 미리 정의된 워크플로 프로세스는 다음과 같이 워크플로 규칙을 지원합니다.

- **프로세스 템플릿** - 사용자 콘솔에서 승인자(또는 참여자 해결 프로그램)를 구성할 수 있습니다.
- **미리 정의된 워크플로 프로세스** - WorkPoint Designer 에서 참여자 해결 프로그램을 구성해야 합니다.

또한 워크플로 규칙과 함께 사용할 사용자 지정 워크플로 프로세스를 만들 수 있습니다.

규칙 개체

CA Identity Manager 관리자는 다음 개체를 기반으로 이벤트 또는 관리자 태스크에 대한 승인 정책을 만들 수 있습니다. 다음은 지정된 이벤트에 적용되거나 이벤트 실행 시 존재할 경우 이벤트에 대한 개체입니다.

- **태스크의 초기화 프로그램** - 태스크를 실행하는 CA Identity Manager 관리자
- **이벤트의 기본 개체** - 이벤트와 연결된 기본 개체
- **이벤트의 보조 개체** - 이벤트와 연결되고 기본 개체에 상대적인 보조 개체

다음은 관리자 태스크에 대한 개체입니다.

- **태스크의 기본 개체** - 태스크와 관련된 기본 개체입니다
- **태스크의 초기화 프로그램** - 태스크를 실행하는 Identity Manager 관리자입니다,
- **ID 정책 위반** - ID 정책 위반의 경우 규칙은 위반을 유발한 ID 정책의 정책 이름을 기반으로 합니다(예를 들어, 정책 이름이 TitlePolicy 와 같음). 위반 메시지는 "제출한 태스크 보기 태스크 상세 정보"와 같은 승인 화면의 "태스크 상세 정보" 탭에 표시됩니다. SOD 위반 메시지는 "ID 정책 위반"이라는 새 섹션 머리글 아래 표시됩니다. 승인자는 이 메시지를 보고 태스크의 승인 또는 거부를 결정할 수 있습니다.

규칙 평가

정책 규칙은 한 이벤트에 대해 다음 두 가지 방법으로 평가할 수 있습니다.

■ 항상

평가 유형이 "항상"인 정책은 정책에 포함된 특성의 변경 여부에 관계 없이 정책이 **True** 로 평가되는 경우 호출됩니다. 평가 유형이 "항상"인 정책의 결과로 생성된 작업 항목에 대한 승인 화면에서 승인자는 승인 화면에서 편집 가능한 모든 특성을 변경할 수 있습니다.

참고: 승인자가 "거부" 단추를 클릭하면 이벤트가 이전의 경우와 같이 거부됩니다.

■ 승인 조건에 지정된 특성이 변경된 경우에만

평가 유형이 "변경 시"인 정책은 정책이 **True** 로 평가되고 정책에 포함된 특성이 변경된 경우에만 호출됩니다. 평가 유형이 "변경 시"인 정책의 결과로 생성된 작업 항목에 대한 승인 화면에서 해당 특성이 해당 승인 화면에 대한 읽기-쓰기 권한을 가지고 있는 경우 승인자는 정책에 포함된 특성의 값만 변경할 수 있습니다. 승인 화면의 기타 모든 특성은 읽기 전용 권한을 가지고 있습니다.

참고: 승인자가 "거부" 단추를 클릭하면 승인 정책에 포함된 특성의 변경 사항만 거부되고 다음 순서의 승인 정책이 평가됩니다.

이 옵션은 이벤트의 기본 개체 또는 태스크의 기본 개체에만 적용됩니다.

예를 들어 "사용자 수정" 관리자 태스크의 `ModifyUserEvent` 에 대한 모든 정책을 확인해 보십시오.

정책	규칙	평가
정책 1	사용자 ID = Smith01 인 사용자	항상
정책 2	직책 = 관리자인 사용자	직책 특성이 변경된 경우
정책 3	급여 >= 80000 인 사용자	급여 특성이 변경된 경우

정책 1 은 변경되는 특성에 관계없이 관리자가 사용자 Smith01 에 대해 "사용자 수정" 태스크를 호출할 때마다 평가됩니다.

정책 2 는 관리자가 사용자 개체의 직책 특성을 변경하기 위해 "사용자 수정" 태스크를 호출할 때 평가됩니다. 직책이 관리자로 변경되면 정책 2 가 true 입니다.

정책 3 은 관리자가 사용자 개체의 급여 특성을 변경하기 위해 "사용자 수정" 태스크를 호출할 때 평가됩니다. 급여가 80000 이상으로 변경되면 정책 3 이 true 입니다.

이 예제에서 관리자가 "사용자 수정" 태스크를 사용하여 사용자 Smith01 의 직책 특성을 관리자로 변경하면 정책 1 과 정책 2 모두 true 로 평가되며 각 워크플로 프로세스가 시작됩니다. 이 경우 표준 순서 우선 순위가 적용됩니다.

한 작업 항목의 승인자는 조건부 규칙 평가를 통해 이벤트가 여전히 보류 중인 동안 동일한 이벤트의 다른 작업 항목에 영향을 미치는 특성을 변경할 수 있습니다. 이는 평가 유형이 "항상"인 승인 정책의 경우에만 가능합니다. 위의 예제에서 관리자가 사용자 Smith01 의 특성을 변경하면 정책 1 이 true 이고 작업 항목을 생성합니다. 이 승인자는 정책 1 에 의해 생성된 작업 항목을 승인하는 동안 동일한 승인 화면에서 Smith01 의 급여 특성을 변경할 수 있습니다. 이 경우 Smith01 의 새 급여 값에 따라 정책 3 이 ModifyUserEvent 의 동일한 인스턴스에 대해 작업 항목을 생성하는지 여부가 결정됩니다. 승인자가 급여를 90000 으로 변경하면 정책 3 이 이벤트 자체가 승인되기 전에 승인되어야 하는 새 작업 항목을 생성합니다. 표준 순서 우선 순위가 적용됩니다.

규칙 평가 예제

"사용자 수정" 관리자 태스크의 ModifyUserEvent 에 대한 다음 모든 정책을 확인해 보십시오.

정책	규칙	평가
정책 1	사용자 ID = Smith01 인 사용자	항상
정책 2	직책 = 관리자인 사용자	직책 특성이 변경된 경우
정책 3	급여 >= 80000 인 사용자	급여 특성이 변경된 경우

정책 1 은 변경되는 특성에 관계없이 관리자가 사용자 Smith01 에 대해 "사용자 수정" 태스크를 호출할 때마다 평가됩니다.

정책 2 는 관리자가 사용자 개체의 직책 특성을 변경하기 위해 "사용자 수정" 태스크를 호출할 때 평가됩니다. 직책이 관리자로 변경되면 정책 2 가 true 입니다.

정책 3 은 관리자가 사용자 개체의 급여 특성을 변경하기 위해 "사용자 수정" 태스크를 호출할 때 평가됩니다. 급여가 80000 이상으로 변경되면 정책 3 이 true 입니다.

이 예제에서 관리자가 "사용자 수정" 태스크를 사용하여 사용자 Smith01 의 직책 특성을 관리자로 변경하면 정책 1 과 정책 2 모두 true 로 평가되며 각 워크플로 프로세스가 시작됩니다. 이 경우 표준 순서 우선 순위가 적용됩니다.

한 작업 항목의 승인자는 조건부 규칙 평가를 통해 이벤트가 여전히 보류 중인 동안 동일한 이벤트의 다른 작업 항목에 영향을 미치는 특성을 변경할 수 있습니다. 이는 평가 유형이 "항상"인 승인 정책의 경우에만 가능합니다. 위의 예제에서 관리자가 사용자 Smith01 의 특성을 변경하면 정책 1 이 true 이고 작업 항목을 생성합니다. 이 승인자는 정책 1 에 의해 생성된 작업 항목을 승인하는 동안 동일한 승인 화면에서 Smith01 의 급여 특성을 변경할 수 있습니다. 이 경우 Smith01 의 새 급여 값에 따라 정책 3 이 ModifyUserEvent 의 동일한 인스턴스에 대해 작업 항목을 생성하는지 여부가 결정됩니다. 승인자가 급여를 90000 으로 변경하면 정책 3 이 이벤트 자체가 승인되기 전에 승인되어야 하는 새 작업 항목을 생성합니다. 표준 순서 우선 순위가 적용됩니다.

정책 순서

모든 승인 정책에는 가장 낮은 값에서 가장 높은 값 순으로 정렬된 양의 정수 값이 우선 순위를 지정하는 "정책 순서" 필드가 있습니다. 각 정책의 우선 순위에 따라 다음 사항이 결정됩니다.

- 승인 규칙이 평가되는 순서
- true 인 규칙의 경우 워크플로 프로세스가 시작되는 순서입니다.

정책은 정수 값이 낮을수록 우선 순위가 높으며, 정책의 규칙이 높은 정수 값을 가지는 정책보다 먼저 평가됩니다. true 인 이벤트 또는 관리자 태스크에 대한 모든 정책의 경우 우선 순위가 가장 높은 정책이 먼저 워크플로 프로세스를 시작합니다.

정책 순서 예제

이 예제는 정책 순서를 지정하는 방식에 대해 설명합니다. 이 예제에서는 정책 규칙이 항상 평가된다고 가정합니다.

이벤트에 항상 평가되는 여러 개의 정책이 포함되어 있는 경우 이벤트 자체를 승인하려면 모든 정책이 승인되어야 합니다. 그러나 정책 평가 유형이 "항상"인 이벤트와 관련된 하나의 정책이 거부되면 이벤트 자체가 거부됩니다.

참고: 이벤트와 관련된 정책의 평가 유형이 "변경 시"인 경우 해당 정책에 포함된 특성과 관련된 변경 사항만 거부됩니다. 이벤트 자체는 거부되지 않으며 다음 차례의 정책이 평가됩니다.

이 예제에서 정책 1, 정책 2, 정책 3의 정책 평가 유형이 모두 "항상"입니다. 정책 1은 false로 평가되고, 프로세스 1 워크플로 프로세스는 실행되지 않으며, 사용자 1에 대한 작업 항목이 생성되지 않습니다. 이벤트 컨트롤은 즉시 정책 2로 전달됩니다. 정책 2와 정책 3은 모두 true로 평가됩니다. 워크플로 프로세스 2는 우선 순위가 높기 때문에 먼저 실행되고 사용자 2에 대한 작업 항목을 생성합니다.

사용자 2가 작업 항목을 승인하면 워크플로 프로세스 3이 실행되고 사용자 3에 대한 작업 항목을 생성합니다. 그런 다음 이벤트 자체가 승인되려면 사용자 3이 작업 항목을 승인해야 합니다. 이 동작은 다음 표에 나와 있습니다.

우선 순위	정책	결과	워크플로	승인자	동작
1	정책 1	False	프로세스 1	사용자 1	—
2	정책 2	True	프로세스 2	사용자 2	승인됨
3	정책 3	True	프로세스 3	사용자 3	승인됨

그러나 사용자 2가 작업 항목을 거부하면 다음 표에 표시된 대로 이벤트 자체가 거부되고 사용자 3에 대한 작업 항목이 생성되지 않습니다.

우선 순위	정책	결과	워크플로	승인자	동작
1	정책 1	False	프로세스 1	사용자 1	—

우선 순위	정책	결과	워크플로	승인자	동작
2	정책 2	True	프로세스 2	사용자 2	거부됨
3	정책 3	True	프로세스 3	사용자 3	—

다음으로 정책 1, 정책 2, 정책 3의 정책 평가 유형은 모두 "변경 시"입니다. 사용자 2가 작업 항목을 거부하면 정책 2에 포함된 특성과 관련된 변경 사항만 거부됩니다. 그런 다음 정책 3이 평가되며 워크플로 프로세스 3이 실행되고 사용자 3에 대한 작업 항목을 생성합니다. 사용자 3이 작업 항목을 거부하면 이 이벤트에 대한 모든 변경 사항이 거부되었기 때문에 이벤트가 거부됩니다. 사용자 3이 작업 항목을 승인하면 이벤트가 승인되고 정책 3에 포함된 특성 변경 사항이 지속됩니다.

우선 순위	정책	결과	워크플로	승인자	동작
1	정책 1	False	프로세스 1	사용자 1	—
2	정책 2	True	프로세스 2	사용자 2	거부됨
3	정책 3	True	프로세스 3	사용자 3	승인됨

정책 설명

선택 사항인 검색 가능하지 않은 문자열 설명 특성이 승인 정책 관리 개체에 추가되었으며 결과 작업 항목에 나타납니다.

지원되는 최대 문자 수: 255 자

설명에 대한 번들/키 정보를 다음 형식으로 입력할 수 있습니다.

\$ (bundle=<정규화된 리소스 번들 이름> : key=<키>)

승인 화면에서 변경된 특성 강조 표시

승인자가 어떤 특성이 수정되었는지 확인하거나 필요한 경우 해당 특성을 실행 취소할 수 있도록 이 특성이 변경되었음을 승인자에게 알려주는 실행 취소 아이콘이 승인자 프로필 화면에 추가되었습니다.

승인자는 실행 취소 단추를 클릭하여 편집 가능한 특성의 원래 값을 보고 특성의 값을 다른 값으로 변경할 수 있습니다.

Enabled ☒

•First Name

•Last Name

•Full Name

Email

Employee Number

Employee Type

Title

Address

City

State

Postal code

Business Phone

Cell Phone

승인 정책 및 다중값 특성

다중값 특성에 대해 규칙이 설정된 경우 다중값 특성에 대해 새로 추가되거나 제거된 값에만 이 규칙이 적용되도록 지정할 수 있는 방법이 없었습니다. 이제 다중값 특성을 기준으로 한 규칙의 정책 평가 유형을 보는 것으로 이 작업을 수행할 수 있습니다. 규칙 평가 유형이 "변경 시"인 경우 이 규칙은 다중값 특성의 모든 값이 아니라 새로 추가되거나 제거된 값에만 적용될 수 있습니다. 값이 새로 추가되거나 제거되었는지 여부에 관계 없이 규칙이 다중값 특성의 모든 값을 기준으로 해야 할 경우에는 해당 규칙의 평가 유형이 "항상"이어야 합니다.

프로필 화면에서 다중값 특성의 변경 사항은 실행 취소 아이콘과 함께 강조 표시됩니다. 다중값 특성에 새 값이 추가되었거나 다중값 특성에서 새 값이 제거되었기 때문에 규칙의 평가 결과가 **true** 인 경우 이 변경 사항을 승인하는 승인은 다중값 특성의 모든 값을 보게 됩니다. 실행 취소 아이콘을 클릭하면 해당 특성의 값이 원래 값으로 복원됩니다. 승인이 제거된 값을 보려는 경우 실행 취소 아이콘을 클릭하면 원래 값의 집합이 표시됩니다. 다시 실행 아이콘을 클릭하면 승인이 제거된 값과 추가된 값을 구분할 수 있는 새로운 값의 집합이 표시됩니다. 승인 단추를 클릭하면 이 다중값 특성의 모든 변경 사항이 승인됩니다. 거부 단추를 클릭하면 이 다중값 특성의 모든 변경 사항이 거부됩니다. 이 다중값 특성과 관련된 모든 후속 규칙은 이 다중값 특성의 값에 새로운 변화가 없는 경우 평가되지 않습니다.

참고: 다중값 특성 기반 규칙의 경우 다중값 특성에 포함된 값이 실제 값이며 표시 값이 아닙니다. 예를 들어, **MA** 주의 표시 값은 **Massachusetts** 입니다. 주 특성을 기반으로 하는 승인 정책을 만드는 경우 규칙은 **주=MA** 와 같아야 합니다.

"사용자 수정" 관리자 태스크의 **ModifyUserEvent** 에 대한 다음 예제의 모든 정책을 확인해 보십시오.

정책	규칙	평가
정책 1	사용자 위치(주 = MA)	변경 시
정책 2	사용자 위치(주 = DC)	항상

정책 1 은 관리자가 주 특성을 변경하기 위해 "사용자 수정" 태스크를 호출할 때마다 평가되며 MA 값이 주 특성에 추가되거나 주 특성에서 제거되는 경우 true 로 평가됩니다.

정책 2 는 관리자가 주의 값이 DC 인 사용자에게 대해 "사용자 수정" 태스크를 호출할 때마다 평가됩니다.

워크플로 승인 화면에서 특성이 변경된 항목으로 강조 표시됨

관리자가 원래 태스크에서 변경하지 않은 경우에도 승인 화면에서 추가 특성이 변경된 항목으로 강조 표시될 수 있습니다. 이 문제는 화면 초기화 또는 일부 다른 특성의 변경 사항에 대한 화면 유효성 검사의 일부로서 화면에 포함된 여러 특성의 값을 변경할 수 있는 스크립트가 화면에 포함되기 때문입니다.

정책 예

다음 비즈니스 사용 사례는 워크플로 승인 정책을 이벤트에 적용할 수 있는 방법을 나타냅니다.

예 1:

사용 사례 – 관리자가 직원에게 속하는 관계형 데이터베이스 계정을 수정합니다.

관리자 태스크 – ModifyMSSQLAccount

이벤트 – ModifyMSSQLAccountEvent

승인 규칙 – 직책 = RDBAcctManager 인 사용자

워크플로 프로세스 – ModAcctApproval(사용자 지정 워크플로 프로세스)

개체 – 태스크의 초기화 프로그램

평가 – 항상 규칙 평가

예 2:

사용 사례 – 관리자가 직원의 급여를 수정하여 새 임금 인상을 반영합니다.

관리자 태스크 – 사용자 수정

이벤트 – ModifyUserEvent

승인 규칙 - 급여 ≥ 100000 인 사용자

워크플로 프로세스 - SalaryChangeApproval(사용자 지정 워크플로 프로세스)

개체 - 이벤트의 주 개체(사용자)

평가 - 급여 특성이 변경될 때만 평가

예 3:

사용 사례 - 사용자의 직책이 계약자로 변경될 때 관리자가 해당 사용자를 계약자 그룹에 추가합니다. 이 예는 다음의 두 가지 승인 정책으로 나눌 수 있습니다.

정책 1:

관리자 태스크 - 사용자 수정

이벤트 - ModifyUserEvent

승인 규칙 - 직책 = 계약자인 사용자

워크플로 프로세스 - SingleStepApproval(기본 프로세스 템플릿)

개체 - 이벤트의 주 개체(사용자)

평가 - 직책 특성이 변경될 때만 평가

정책 2:

관리자 태스크 - 그룹 수정(또는 그룹 구성원 자격 수정)

이벤트 - AddToGroup

승인 규칙 - 그룹 위치(그룹 이름 = 계약자)

워크플로 프로세스 – SingleStepApproval(기본 프로세스 템플릿)

개체 – 이벤트의 보조 개체(그룹)

평가 – 항상 규칙 평가

다음 비즈니스 사용 사례는 워크플로 승인 정책을 태스크에 적용할 수 있는 방법을 나타냅니다.

예 1:

사용 사례 – 관리자가 직원에게 속하는 Active Directory 계정을 수정합니다.

관리자 태스크 – ModifyActiveDirectoryAccount

개체 – 태스크의 초기화 프로그램

승인 규칙 – 직책 = ActiveDirectoryManager 인 사용자

워크플로 프로세스 – 단일 단계 승인

평가 – 항상 규칙 평가

예 2:

사용 사례 – 관리자가 직원 코드가 HighSecurity 인 사용자를 수정합니다.

관리자 태스크 – 사용자 수정

개체 – 태스크의 기본 개체

승인 규칙 – employeenumber = HighSecurity 인 사용자

워크플로 프로세스 – 단일 단계 승인

평가 – 항상 규칙 평가

예 3:

사용 사례 – 관리자가 관리자 역할 CheckApprover 와 CheckSigner 를 할당하기 위해 사용자를 수정합니다.

관리자 태스크 – 사용자 수정

개체 – ID 정책 위반

승인 규칙 – IdentityPolicy 위치(이름 = CheckRoles)

워크플로 프로세스 – 단일 단계 승인

평가 – 항상 규칙 평가

이벤트에 대한 정책 기반 워크플로를 구성하는 방법

정책 기반 워크플로를 구성하기 위한 절차는 이벤트 수준 워크플로를 구성하는 절차와 유사하며, 워크플로 실행 여부를 결정하는 승인 정책을 정의하는 추가 단계가 있습니다.

정책 기반 워크플로를 구성하려면

1. 사용자 콘솔에서 "역할 및 태스크", "관리자 태스크", "관리자 태스크 수정(또는 만들기)"을 선택합니다.
"관리자 태스크 선택" 화면이 나타납니다.
2. 워크플로 컨트롤을 적용할 태스크를 검색하고 "선택"을 클릭합니다.
"관리자 태스크 수정(또는 만들기)" 화면이 나타납니다.
3. "프로필" 탭에서 "워크플로 사용"을 선택했는지 확인합니다.
4. "이벤트" 탭에서 프로세스 템플릿에 매핑할 이벤트를 선택합니다.
워크플로 매핑 화면이 나타납니다.
5. "정책 기반" 라디오 단추를 선택한 다음 "추가"를 클릭합니다.
"승인 정책" 화면이 나타납니다.
6. [승인 정책을 구성합니다](#) (페이지 359).
7. 선택한 워크플로 프로세스에서 필요한 대로 참여자 해결 프로그램을 구성합니다.
참여자 요청이 프로세스에 추가됩니다.
8. "확인"을 클릭합니다.
CA Identity Manager 에서 이벤트 수준 워크플로 구성을 저장합니다.
9. "제출"을 클릭합니다.
CA Identity Manager 에서 태스크 수정을 처리합니다.

참고: "워크플로 프로세스" 목록에는 템플릿 방법과 WorkPoint 방법에서 모두 사용할 수 있는 프로세스가 들어 있습니다.

- 템플릿 방법 프로세스를 선택하면(SingleStepApproval 또는 TwoStageApprovalProcess) 페이지가 확장되어 참여자 해결 프로그램 구성의 사용을 허용합니다.
- WorkPoint 방법 프로세스를 선택하면 페이지가 확장되지 않습니다. 참여자 해결 프로그램은 WorkPoint Designer 에서 구성됩니다.

태스크에 대한 정책 기반 워크플로를 구성하는 방법

태스크에 대한 정책 기반 워크플로를 구성하기 위한 절차는 태스크 수준 워크플로를 구성하는 절차와 유사하며, 워크플로 실행 여부를 결정하는 승인 정책을 정의하는 추가 단계가 있습니다.

정책 기반 워크플로를 구성하려면

1. 사용자 콘솔에서 "역할 및 태스크", "관리자 태스크", "관리자 태스크 수정(또는 만들기)"을 선택합니다.
"관리자 태스크 선택" 화면이 나타납니다.
2. 워크플로 컨트롤을 적용할 태스크를 검색하고 "선택"을 클릭합니다.
"관리자 태스크 수정(또는 만들기)" 화면이 나타납니다.
3. "프로필" 탭에서 "워크플로 사용"을 선택했는지 확인합니다.
4. "프로필" 탭에서 "워크플로 프로세스" 필드 옆의 연필 아이콘을 클릭합니다.
워크플로 매핑 화면이 나타납니다.
5. "정책 기반" 라디오 단추를 선택한 다음 "추가"를 클릭합니다.
"승인 정책" 화면이 나타납니다.
6. [승인 정책을 구성합니다](#) (페이지 359).
7. 선택한 워크플로 프로세스에서 필요한 대로 참여자 해결 프로그램을 구성합니다.
참여자 요청이 프로세스에 추가됩니다.
8. "확인"을 클릭합니다.

CA Identity Manager 에서 태스크 수준 워크플로 구성을 저장합니다.

9. "제출"을 클릭합니다.

CA Identity Manager 에서 태스크 수정을 처리합니다.

참고: "워크플로 프로세스" 목록에는 태스크 수준 정책 기반 워크플로를 위해 템플릿 방법과 함께 사용할 수 있는 프로세스가 포함됩니다.

- 템플릿 방법 프로세스를 선택하면(SingleStepApproval 또는 TwoStageApprovalProcess) 페이지가 확장되어 참여자 해결 프로그램 구성의 사용을 허용합니다.

추가 정보

[승인 정책을 구성하는 방법](#) (페이지 359)

승인 정책을 구성하는 방법

이벤트 또는 태스크에 대한 승인 정책을 구성하려면 다음 단계를 수행합니다.

1. 테스트할 개체를 선택합니다.
2. 개체에 대한 승인 규칙을 정의합니다.
3. 주 개체의 경우 이것이 조건부 평가인지 결정합니다.
4. 정책 평가의 순서를 입력합니다.
5. 규칙이 **true** 인 경우 실행하도록 워크플로 프로세스를 구성합니다.

승인 정책을 구성하려면

1. "승인 정책" 화면의 드롭다운 목록에서 테스트할 규칙에 대한 개체를 선택합니다.
화면이 변경되어 선택 항목을 반영합니다.
2. 개체 이름 옆에 있는 새 드롭다운에서 조건식 템플릿을 선택합니다.
화면이 변경되어 선택 항목을 반영합니다.
3. 조건식을 만들고 필요에 따라 편집합니다.
4. "규칙 평가" 옵션 단추를 선택하여 규칙이 항상 평가되는지 또는 승인 조건의 특성이 변경될 경우에만 평가될지 나타냅니다.
5. 이벤트에 대한 정책이 여러 개 있는 경우 정책 평가 순서를 지정하는 양의 정수 값을 입력합니다.
6. 규칙이 **true** 로 평가되는 경우 실행되는 워크플로 프로세스를 선택하고 구성합니다.
7. "확인"을 클릭하여 승인 정책을 저장합니다.

정책 기반 워크플로 상태

CA Identity Manager 관리자는 다음 표준 시스템 도구를 사용하여 워크플로 승인 정책이 포함된 태스크 상태를 표시할 수 있습니다.

- 제출한 태스크 보기 탭
- 사용자 기록 탭
- 보고서 및 로그

제출한 태스크 및 태스크 기록 정보는 다음 사항을 포함합니다.

- 태스크 및 이벤트 정보
- 워크플로 및 승인 규칙 정보
- 승인 규칙 평가 결과

제출한 태스크 기록 설명에 대해서는 시스템 탭 설명서를 참조하십시오.

전역 이벤트 수준 정책 기반 워크플로 매핑

이벤트를 관리 콘솔에서 워크플로 프로세스로 매핑하거나 특정 태스크의 정책 기반 워크플로 승인 정책과 연결할 수 있습니다. 관리자가 새로운 "이벤트에 대한 전역 정책 기반 워크플로 구성" 태스크를 사용하여 환경 수준에서 이벤트에 대한 정책 기반 워크플로 매핑을 설정할 수 있습니다. 관리자 태스크에서 이벤트에 대한 정책 기반 워크플로를 설정하는 것과 달리, 구성된 정책 기반 워크플로 매핑은 이벤트를 생성하는 모든 태스크에 적용됩니다.

참고: "이벤트에 대한 전역 정책 기반 워크플로 구성" 태스크는 워크플로가 활성화된 경우에만 작동합니다. 워크플로가 비활성화된 상태에서 이 태스크를 실행하면 오류가 발생합니다.

이 태스크는 "시스템" 탭에 추가되었습니다. 태스크가 제출되면 이 태스크에 있는 각 이벤트의 워크플로 프로세스는 다음과 같은 방법으로 검색됩니다.

해당 관리자 태스크의 이벤트에 대해 구성된 워크플로가 우선 순위를 갖습니다. 이벤트는 정책 기반 또는 정책 기반이 아닌 워크플로에 대해 구성할 수 있습니다. 해당 관리자 태스크의 이벤트에 대해 정책 기반 워크플로가 구성된 경우 정책과 관련된 워크플로 프로세스가 호출됩니다. 일치하는 규칙이 없으면 이벤트에 대해 워크플로가 호출되지 않습니다. 마찬가지로, 해당 관리자 태스크의 이벤트에 대해 정책 기반이 아닌 워크플로가 구성된 경우 정책과 관련된 워크플로 프로세스가 호출됩니다. 관리자 태스크의 이벤트에 대해 구성된 워크플로가 없으면 해당 이벤트에 대한 전역 워크플로 구성이 우선 순위를 갖습니다.

이벤트에 대한 전역 정책 기반 워크플로 구성 태스크 화면

관리자는 "이벤트에 대한 전역 정책 기반 워크플로 구성" 태스크를 사용하여 현재 환경의 모든 이벤트에 대한 정책 기반 또는 정책 기반이 아닌 워크플로를 구성할 수 있습니다. 태스크를 클릭하면 워크플로 프로세스 정의에 대한 기본 이벤트 매핑이 표시됩니다. 각 이벤트 매핑을 수정 또는 삭제할 수 있으며 아직 구성되지 않은 이벤트에 대해 새 이벤트 매핑을 추가할 수 있습니다.

홈

사용자

조직

그룹

역할 및 태스크

끝점

정책

전자 메일

보고서

시스템

태스크

이벤트에 대한 전역 정책 기반 워크플로 구성

이 환경의 이벤트와 관련되어 있는 워크플로 프로세스입니다.

이벤트 이름	워크플로 프로세스
AssignAccessRoleEvent	ModifyAccessRoleMembershipApproveProcess
AssignRoleEvent	CertifyRoleApproveProcess
CreateGroupEvent	CreateGroupApproveProcess
CreateOrganizationEvent	CreateOrganizationApproveProcess
CreateUserEvent	CreateUserApproveProcess
DeleteGroupEvent	DeleteGroupApproveProcess
DeleteOrganizationEvent	DeleteOrganizationApproveProcess
DeleteUserEvent	DeleteUserApproveProcess
ModifyOrganizationEvent	ModifyOrganizationApproveProcess
RevokeAccessRoleEvent	ModifyAccessRoleMembershipApproveProcess
SelfRegisterUserEvent	SelfRegistrationApproveProcess

새 매핑 추가

이벤트

AccountChangePasswordEvent

추가

이 화면의 필드가 아래 나열되어 있습니다.

이 환경의 이벤트와 관련된 워크플로 프로세스입니다.

승인 정책과 관련된 워크플로 프로세스를 지정합니다.

새 매핑 추가

워크플로 프로세스에 매핑하기 위한 승인 정책을 지정합니다.

추가 단추

새 매핑을 추가합니다.

매핑을 추가하거나 수정하면 프로세스 매핑과 승인 정책을 선택할 수 있는 워크플로 매핑 화면이 열립니다. 동작은 이벤트 수준 워크플로 구성과 동일합니다. 워크플로 매핑 페이지에서 "추가" 단추를 클릭하면 승인 정책을 구성할 수 있는 다른 페이지가 표시됩니다.

추가 정보

[이벤트에 대한 정책 기반 워크플로를 구성하는 방법](#) (페이지 357)

[승인 정책을 구성하는 방법](#) (페이지 359)

이벤트에 대한 전역 정책 기반 워크플로 구성

이 탭을 사용하여 이벤트에 대한 전역 정책 기반 워크플로를 구성하십시오.

이름

탭에 할당하는 이름입니다.

태그

태스크 내에서 고유한 탭의 식별자입니다. 문자나 밑줄로 시작해야 하며 문자, 숫자 또는 밑줄만 사용해야 합니다. 태그는 주로 XML 문서나 HTTP 매개 변수를 통해 데이터 값을 설정하는 데 사용됩니다.

탭 숨기기

탭이 태스크에 표시되지 않도록 합니다. 이 옵션은 탭을 숨겨야 하지만 탭의 특성에 대한 액세스가 필요한 응용 프로그램에 유용합니다.

사용자 검색 화면

사용자를 표시하는 데 사용할 검색 화면을 정의합니다.

사용자 목록 화면

이 탭의 열과 정렬을 결정하는 화면을 정의합니다.

그룹 검색 화면

그룹을 표시하는 데 사용할 검색 화면을 정의합니다.

그룹 목록 화면

이 탭의 열과 정렬을 결정하는 화면을 정의합니다.

관리자 역할 검색 화면

관리자 역할을 표시하는 데 사용할 검색 화면을 정의합니다.

관리자 역할 목록 화면

이 탭의 열과 정렬을 결정하는 화면을 정의합니다.

관리자 태스크 검색 화면

관리자 태스크를 표시하는 데 사용할 검색 화면을 정의합니다.

관리자 태스크 목록 화면

이 탭의 열과 정렬을 결정하는 화면을 정의합니다.

온라인 요청

CA Identity Manager 를 사용하면 일반 용도의 온라인 요청 작업을 만들 수 있습니다. 기본 온라인 요청 구현은 자체 수정 요청과 관리자 사용자 수정 요청에 대한 관련 작업 세트로 구성되어 있습니다. 하지만 다른 CA Identity Manager 요청 작업에 대해 쉽게 온라인 요청 기능을 구현할 수 있습니다.

사용자 수정 요청은 작업 항목을 생성하는 워크플로 프로세스를 트리거합니다. 워크플로 참여자는 작업 항목을 승인 및 구현하거나 거부할 수 있습니다. 작업을 시작하는 사용자는 CA Identity Manager 가 요청 기록을 유지 관리하는 데 사용하는 텍스트 영역인 기록 편집기에 요청에 대한 설명을 입력합니다. 참여자가 작업 항목에 수행하는 동작에 대한 설명을 남길 수 있도록 이 기록 편집기를 구성할 수 있습니다. 이러한 설명은 누적 작업 항목 기록에 포함됩니다.

표준 승인 및 거부 동작 외에(또는 대신) 새 동작을 사용할 수도 있습니다. 예를 들어, 비즈니스 참여자는 요청을 설명할 수 있고 기술 참여자는 요청을 구현할 수 있습니다. 이러한 새 활동은 "설명" 및 "구현"과 같이 승인 작업의 표준 "승인" 및 "거부" 단추에 추가할 수 있는 새 워크플로 동작 단추로 표시될 수 있습니다.

온라인 요청 작업

함께 작동하여 기본 온라인 요청 구현을 만드는 5 개 작업이 있습니다. 이러한 작업에서는 사용자 지정 요청, 기록 및 워크플로 동작 단추의 사용을 보여 줍니다.

참고: 관리자 작업("내 계정 만들기" 및 "온라인 요청 만들기")은 기본적으로 "협업의 프로세스" 템플릿을 사용하여 이벤트 수준 워크플로에 대해 구성됩니다.

내 계정 변경

사용자 계정 변경 요청을 만드는 자체 수정 관리자 작업입니다. 이 작업에는 요청을 설명하기 위한 기록 편집기가 포함된 "요청" 탭과 읽기 전용 사용자 상세 정보가 포함된 "프로필" 탭이 있습니다.

온라인 요청 만들기

특정 사용자에게 대한 계정 변경 요청을 만드는 사용자 수정 관리자 작업입니다. 이 작업에는 요청을 설명하기 위한 기록 편집기가 포함된 "요청" 탭과 읽기 전용 사용자 상세 정보가 포함된 "서브젝트 프로필" 탭이 있습니다.

온라인 요청 승인

비즈니스 참여자가 작업을 승인 또는 거부하거나 작업에 대한 추가 설명을 요청할 수 있게 하는 승인 작업입니다. 이 작업에는 쿼리 또는 설명을 위한 기록 표시와 기록 편집기, 읽기 전용 "서브젝트 프로필" 탭 및 "할당받은 사람" 탭이 포함된 "요청" 탭이 있습니다.

온라인 요청 설명

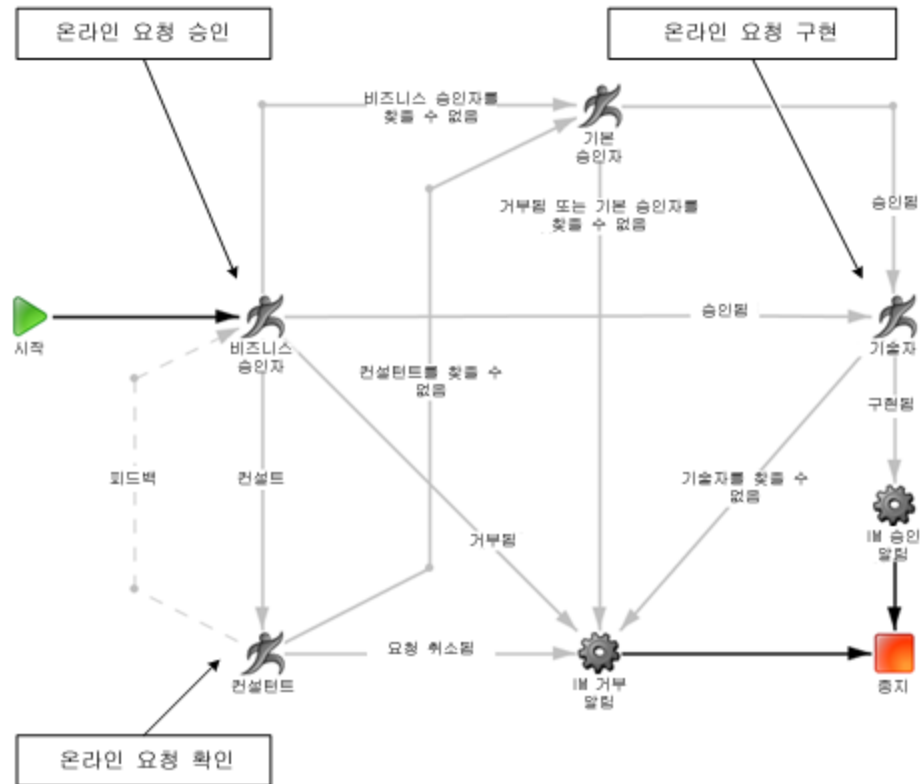
설명하는 참여자가 설명 요청에 응답할 수 있게 하고 승인을 위해 작업을 다시 비즈니스 참여자에게 보내는 승인 작업입니다. 이 작업에는 설명을 위한 기록 표시와 기록 편집기 및 읽기 전용 "서브젝트 프로필" 탭이 포함된 "요청" 탭이 있습니다.

온라인 요청 이행

기술 참여자가 작업을 구현하고 작업 기록에 설명을 추가할 수 있게 하는 승인 작업입니다. 이 작업에는 설명을 위한 기록 표시와 기록 편집기, 읽기 전용 "서브젝트 프로필" 탭 및 "할당받은 사람" 탭이 포함된 "요청 이행" 탭이 있습니다.

온라인 요청 프로세스

온라인 요청 작업은 WorkPoint Designer 에 표시되는 대로 "협의 프로세스"라는 워크플로 프로세스 템플릿에 의해 제어됩니다.



"협의 프로세스"에는 온라인 요청 이행의 승인 작업에 해당하는 4 개의 수동 활동이 포함되어 있습니다.

- 작업 항목을 거부 및 승인하고 기술자에게 전달하거나 컨설턴트의 추가 설명을 요청하는 비즈니스 승인자의 활동
- 작업 항목을 설명하고 다시 비즈니스 승인자에게 보내는 컨설턴트의 활동
- 비즈니스 승인자나 컨설턴트에 연락할 수 없는 경우 작업을 수행하는 기본 승인자의 활동
- 요청을 이행하고 작업 항목을 완료하는 기술자의 활동

온라인 요청 기록

온라인 요청 기록 기능을 사용하면 참여자가 작업 항목 동작의 레코드를 만들 수 있습니다. 작업 항목에 대한 책임이 한 참여자에서 다른 참여자에게 전달되면 새 참여자가 동작을 수행하기 전에 작업 항목 기록을 검토할 수 있습니다.

다음 두 컨트롤을 사용하여 온라인 요청 기록이 구현됩니다.

- 기록 표시는 이전 기록 항목의 상세 정보가 시간순으로 포함된 읽기 전용 테이블입니다.
- 기록 편집기는 새 기록 항목을 만들기 위한 텍스트 상자입니다. 작업 항목을 제출하지 않고 여러 항목을 추가하기 위한 선택적 단추도 있습니다.

기본적으로 기록 편집기 및 기록 표시는 온라인 요청 이행과 관련된 모든 작업에 대한 "요청" 탭에 나타납니다. 다음 화면에서는 "온라인 요청 설명" 작업의 기록 컨트롤을 보여 줍니다.

요청 설명

서브젝트 프로파일

요청을 승인할 권한이 부여된 사용자가 진행 전에 추가 정보를 요청했습니다. 해당 설명은 요청 기록에 명백히 표시되어야 합니다. 추가 정보를 제공한 다음 '돌아가기'를 클릭해 요청을 승인자에게 다시 돌려보내 주십시오. 또는, '취소'를 클릭해 영구적으로 이 요청을 철회하십시오.

요청 및 기록:

원본	설명	▲ 시간
SuperAdmin (SuperAdmin)에 의한 사용자 설명, 현재 요청자(으)로 작동 중추진 "SalesDir"를 "SalesVP"		2008-05-12 23:15:25.983
SalesMgr (Sales Manager)에 의한 사용자 설명, 현재 요청자(으)로 작동 중외 "SalesVeep"대신에?		2008-05-12 22:48:39.467
SaleCon (Sales Consult) 에 의한 사용자 설명, 현재 요청자(으)로 작동 중자, 가자 "Sales Veep"		2008-05-12 23:20:16.78

추가 정보

기록 편집기

기록 표시

기록 이벤트 추가

돌아가기

요청 취소

항목 보류

닫기

온라인 요청 사용

다음 단계에서는 온라인 요청 워크플로 프로세스에 대해 설명합니다. 각 단계에 대해 생성된 IM 작업이 괄호 안에 나타납니다. 프로세스의 모든 단계에서 참여자는 기록 편집기에 설명을 추가할 수 있습니다. 이 설명은 워크플로 프로세스의 다음 참여자에 대한 기록 표시에 나타납니다.

1. "작업 초기화 프로그램"에서 IM 사용자 수정을 요청합니다(온라인 요청 만들기).
2. 비즈니스 승인자가 작업 항목을 받고 다음 중 하나를 수행합니다.
 - 작업 항목을 승인합니다(온라인 요청 승인).
 - 작업 항목을 거부하고 워크플로 프로세스를 종료합니다. 새 작업이 생성되지 않습니다.
 - 컨설턴트의 설명을 요청합니다(온라인 요청 설명).
3. 컨설턴트가 작업 항목을 받고 다음 중 하나를 수행합니다.
 - 설명을 추가하고 작업 항목을 비즈니스 승인자에게 반환합니다. 새 작업이 생성되지 않습니다.
 - 작업 항목을 취소하고 워크플로 프로세스를 종료합니다. 새 작업이 생성되지 않습니다.
4. 기술자가 작업 항목을 받고 요청을 이행합니다(온라인 요청 이행).

워크플로 동작 단추

CA Identity Manager의 승인 태스크는 일반적으로 해당 작업 항목 화면에 표시되는 "승인" 또는 "거부" 동작 단추가 있습니다. 워크플로 동작 단추를 사용하여 관리자는 태스크 승인을 위한 작업 단추를 추가하고 기존 단추를 제거 또는 수정함으로써 CA Identity Manager 태스크 및 워크플로의 기능을 확장할 수 있습니다. (표준 승인 및 거부 단추는 사용자 지정 워크플로 작업 단추와 동일한 방법으로 구현됨)

예를 들어, 워크플로 프로세스는 중간 수준 참가자가 특정 케이스를 최종 승인 또는 거부 결정을 얻기 위해 상위 수준 참가자에게 에스컬레이트할 수 있는 동작이 필요할 수 있습니다. 이러한 중간 수준 참가자는 기록 편집기를 사용하여 설명 또는 추천 글을 추가한 다음, 검토하여 승인 또는 거부할 수 있도록 상위 참가자에게 작업 항목을 보낼 수 있습니다.

워크플로 동작 단추를 추가 또는 제거하려면 이러한 새 동작의 처리를 위한 비즈니스 로직을 제공하는 WorkPoint 워크플로 프로세스에 대한 적절한 변경이 필요합니다.

추가 정보:

[CA Identity Manager 의 단추 구성](#) (페이지 370)

[승인 작업의 워크플로 단추](#) (페이지 370)

[WorkPoint Designer 의 단추 구성](#) (페이지 373)

승인 작업의 워크플로 단추

워크플로 동작 단추는 **WorkPoint** 프로세스 다이어그램에서 수동 활동 노드의 반대쪽을 가리키는 전환 노드에 해당합니다. 예를 들어, "협의 프로세스"에서 "기술자" 활동 노드에는 "구현됨"이라는 단일 전환이 있습니다. 이 전환은 다음 그림에 표시된 "온라인 요청 이행" 승인 작업의 "구현됨" 단추에 해당합니다.

요청 이행
서브젝트 프로파일
할당 받은 사람

프로필이 제공된 사용자에게 대해 여기에 설명된 변경 요청은 승인을 마쳤으며 이제 시행되어야 합니다. 제공된 단추를 사용해 작업을 시작해 이 요청을 구현하십시오. 이 작업이 완료되면 '구현됨'을 클릭해 요청을 닫습니다.

요청 및 기록:

원본	설명	▲ 시간
SuperAdmin (SuperAdmin)에 의한 사용자 설명, 현재 요청자(으)로 작동 중	변경 내용을 Sales Rep 오스트 레일 리마	2008-05-13 03:49:18.32
SuperAdmin (SuperAdmin)에 의한 사용자 설명, 현재 요청자(으)로 작동 중	우리가 필요로 Aussie rep, 그래서 그녀가 이동을 Sydney	2008-05-13 03:49:18.327
SuperAdmin (SuperAdmin)에 의한 사용자 설명, 현재 요청자(으)로 작동 중	그녀가 커버 뉴질랜드까지?	2008-05-13 03:49:18.33

설명

"SaleRepasia"사용자 계정이 요구한대로 구현

추가

이 작업을 사용해 이 요청을 구현하십시오:

워크플로 동작 단추
구현됨
항목 보류
닫기

참고: "항목 보류" 및 "닫기" 단추는 **CA Identity Manager** 프로그래밍 로직으로 제어되며 워크플로에서 제어되지 않습니다.

CA Identity Manager 의 단추 구성

워크플로 동작 단추를 구성하려면 승인 태스크의 "프로필" 탭에서 "워크플로 동작 단추"라는 단추를 클릭합니다.

단추 "프로필" 탭에는 각 워크플로 동작 단추에 대한 행이 포함된 테이블이 있습니다. 각 단추 행에는 테이블의 열에 해당하는 다음 4 개의 속성이 있습니다.

표시 이름

승인 화면의 단추에 표시되는 이름입니다. 이 이름은 조건부로 지역화된 값으로, 리소스 파일에 있는 지역화된 문자열의 키이거나 문자열일 수 있습니다.

동작

옵션이 선택된 경우 워크플로 프로세스로 다시 전달되는 값입니다. 이 값은 WorkPoint 프로세스 다이어그램에 있는 해당 전환 노드의 특성으로, 지역화되지 않은 문자열입니다. 기본 설정은 "승인됨" 및 "거부됨"입니다.

도구 설명

사용자가 마우스 커서를 단추 위로 이동할 때 표시되는 단추 동작에 대한 간단한 설명(또는 도구 설명)입니다. 이 도구 설명은 조건부로 지역화된 값으로, 리소스 파일에 있는 지역화된 문자열의 키이거나 문자열일 수 있습니다.

자세한 설명

"제출한 태스크 보기" 화면에 동작을 설명하는 메시지를 추가하는 단추 동작에 대한 자세한 설명입니다. 설명이 비어 있는 경우 "제출한 태스크 보기" 화면에 표시된 메시지가 단추 이름입니다. 이 이름은 조건부로 지역화된 값으로, 리소스 파일에 있는 지역화된 문자열의 키이거나 문자열일 수 있습니다.

추가 정보:

[WorkPoint Designer 의 단추 구성](#) (페이지 373)

워크플로 동작 단추 추가

기존 워크플로 프로세스에 새 단추를 추가하려면 다음과 같은 고급 단계를 수행합니다.

1. Identity Manager 에서 워크플로 단추를 추가합니다.

자세한 내용은 [워크플로 동작 단추를 추가하는 방법](#) (페이지 372)을 참조하십시오.

2. 필요한 경우 지역화 키를 추가합니다.
자세한 내용은 *Configuration Guide*(구성 안내서)를 참조하십시오.
3. WorkPoint Designer 에서 필요한 새 노드를 모두 추가합니다.
자세한 내용은 WorkPoint Designer 온라인 도움말을 참조하십시오.
4. WorkPoint Designer 전환 노드에서 스크립트를 정의합니다.
자세한 내용은 [WorkPoint Designer 의 단추 구성](#) (페이지 373)을 참조하십시오.

워크플로 동작 단추를 추가하는 방법

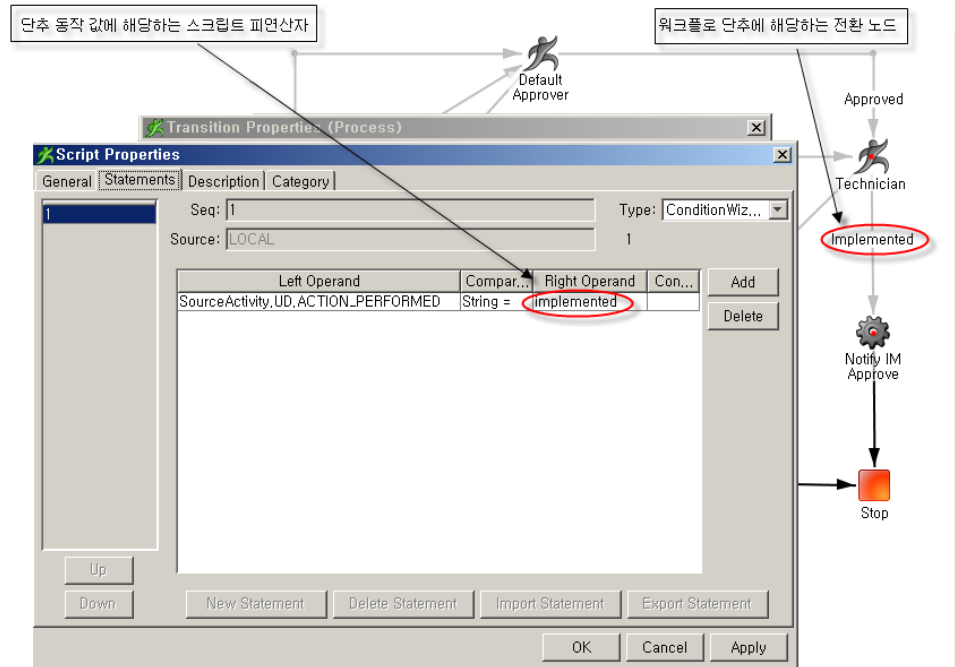
CA Identity Manager 에서 승인 태스크에 워크플로 동작 단추를 추가할 수 있습니다.

관리자 작업에 워크플로 동작 단추를 추가하려면

1. 사용자 콘솔에서 "역할 및 태스크", "관리자 태스크", "관리자 태스크 수정"을 선택합니다.
"관리자 작업 선택" 화면이 나타납니다.
2. 승인 작업을 검색하고 "선택"을 클릭합니다.
"관리자 작업 수정" 화면이 나타납니다.
3. "프로필" 탭에서 "워크플로 동작 단추"라는 단추를 클릭합니다.
"워크플로 동작 단추 프로필" 탭이 나타납니다.
4. "단추 추가"를 클릭하여 승인 작업에 새 단추를 추가합니다.
5. 단추 속성 정보를 입력합니다.
6. "확인"을 클릭합니다.
CA Identity Manager 에서 새 단추 정보를 저장합니다.
7. "제출"을 클릭합니다.
CA Identity Manager 에서 태스크 수정을 처리합니다.

WorkPoint Designer의 단추 구성

WorkPoint Designer에서 워크플로 동작 단추는 다음 그림과 같이 전환 노드 스크립트 속성을 사용하여 구성됩니다.



기본적으로 워크플로 동작 단추는 다음과 같은 스크립트 속성을 사용하여 문자열을 비교합니다.

- 왼쪽 피연산자 - 이전 수동 활동 노드의 "사용자 데이터" 속성에서 정의된 -ACTION_PEFORMED 입니다.
- 오른쪽 피연산자 - 사용자 콘솔의 단추 프로필 탭에서 정의된 단추의 "동작" 값입니다.

참고: 활동 노드 및 전환 노드 스크립트와 속성에 대한 자세한 내용은 WorkPoint Designer 온라인 도움말을 참조하십시오.

추가 정보:

[CA Identity Manager의 단추 구성](#) (페이지 370)

작업 목록 및 작업 항목

작업 목록은 태스크 승인 권한이 있는 참여자의 사용자 콘솔에 표시되는 작업 항목(또는 승인 태스크) 목록입니다. 작업 항목은 워크플로 프로세스의 수동 활동에 해당합니다. 작업 항목은 작업 목록에 행으로 표시됩니다.

다음과 같은 방법으로 작업 목록에 작업 항목을 추가할 수 있습니다.

- 참여자 해결 프로그램에서 승인자 목록 결정
- 다른 사용자로부터 위임된 작업 항목 받기
- 다른 사용자에게 재할당

다음과 같은 방법으로 작업 목록에서 작업 항목을 제거할 수 있습니다.

- 작업 항목 완료(승인 또는 거부)
- 다른 사용자에게 재할당
- 작업 항목 보류 작업 항목을 보류하면 다른 참여자의 작업 목록에서 해당 항목이 제거됩니다.

참고: 작업 항목을 수락하거나 거부하는 경우 변경이 즉시 이루어지지 않습니다. 예를 들어, 작업 항목을 거부하면 워크플로 프로세스가 정보를 기록하고 프로세스를 다음 노드로 진행할 때까지는 해당 항목이 여전히 작업 목록에 표시됩니다.

작업 항목에 표시되는 정보 탭은 태스크 수준 또는 이벤트 수준 컨트롤이 적용된 워크플로에서 작업 항목이 생성되었는지 여부에 따라 달라집니다.

- **프로필** - 이벤트의 영향을 받는 개체에 대한 프로필 정보를 제공합니다(이벤트 수준에만 해당).
- **태스크 상세 정보** - 태스크 내 모든 이벤트에 대한 상세 정보를 제공합니다(태스크 수준에만 해당).
- **승인자** - 태스크 또는 이벤트에 대한 개별 승인자와 위임자를 모두 표시합니다(태스크 수준 및 이벤트 수준).

작업 목록 표시

다른 사용자가 시작한 태스크(또는 작업 항목)를 승인하도록 참여자로 할당된 경우 사용자 콘솔에 로그인하면 자동으로 작업 목록이 나타납니다.

수동으로 작업 목록을 표시하려면

1. 사용자 콘솔에서 "홈", "내 작업 목록 보기"를 선택합니다.
작업 목록이 나타납니다.
2. 작업 항목의 이름을 클릭하여 표시합니다.
선택한 작업 항목이 나타납니다.

관리자는 범위가 있는 사용자에게 대해 작업 항목을 관리할 수 있습니다.

참고: 사용자의 작업 항목을 관리하면 관리자가 작업 항목을 보류할 수 있습니다. 사용자의 작업 목록을 보는 경우 종류에 관계없이 작업 항목 변경이 허용되지 않습니다.

다른 사용자의 작업 목록을 보려면

1. 사용자 콘솔에서 "사용자", "작업 항목 관리", "사용자의 작업 목록 보기"를 선택합니다.
사용자 선택 화면이 나타납니다.
2. 작업 목록을 보려는 사용자를 검색하고 "선택"을 클릭합니다.
사용자의 작업 목록 화면이 나타납니다.

다른 사용자의 작업 항목을 관리하려면

1. 사용자 콘솔에서 "사용자", "작업 항목 관리", "사용자의 작업 항목 관리"를 선택합니다.
사용자 선택 화면이 나타납니다.
2. 작업 항목을 관리할 사용자를 검색하고 "선택"을 클릭합니다.
사용자의 작업 목록 화면이 나타납니다.
3. 작업 항목의 이름을 클릭하여 표시합니다.
선택한 작업 항목이 나타납니다.

작업 항목 보류

작업 항목을 보류하여 "체크 아웃"하고 다른 참여자의 작업 목록에서 제거할 수 있습니다. 작업 항목을 보류하면 보류를 수행하는 사용자에게 해당 항목이 보유됩니다.

보류하는 사용자가 작업 항목을 방출하면 다른 참여자의 작업 목록에서 다시 사용할 수 있습니다. 보류하는 사용자가 작업 항목을 승인하거나 거부하면 작업 항목이 완료되고 다른 참여자가 더 이상 사용할 수 없습니다.

재할당 및 보류된 작업 항목

사용자에게 재할당되는 동안 보류된 작업 항목이 있으면 보류된 상태로 유지됩니다. 그러나 사용자가 해당 작업 항목을 방출하면 액세스가 손실됩니다.

관리자는 다른 사용자의 작업 항목을 재할당, 보류 또는 방출할 수 있지만 다른 사용자의 작업 항목을 승인하거나 거부할 수는 없습니다. 할당된 작업 항목 참여자만 이 작업을 수행할 수 있습니다.

추가 정보:

[작업 항목 재할당](#) (페이지 383)

위임 및 보류된 작업 항목

위임이 활성화되어 있는 동안 위임받은 사람 또는 위임자가 작업 항목을 보류할 수 있습니다. 한 사용자가 보류한 작업 항목은 다른 사용자의 작업 목록에 표시될 수 없습니다.

예를 들어, 위임받은 사람에게 위임이 철회된 동안 보류된 작업 항목이 있는 경우 작업 항목이 보류된 상태로 유지됩니다. 그러나 위임받은 사람이 해당 작업 항목을 방출하면 액세스가 손실됩니다.

위임받은 사람에게 보류된 작업 항목이 있는 동안 위임받은 사람인 사용자가 삭제되는 경우 위임받은 사람이 계속 작업 항목을 유지합니다. 그런 다음 위임받은 사람이 작업 항목을 승인하면 감사 중에 더 이상 누가 위임했는지 확인할 수 없습니다.

위임받은 사람에게 위임이 철회된 동안 보류된 작업 항목이 있는 경우 작업 항목이 완료되거나 방출될 때까지 위임받은 사람이 계속 액세스할 수 있습니다.

작업 항목을 보류 또는 방출하는 방법

작업 항목을 보류하여 "체크 아웃"하고 다른 참여자의 작업 목록에서 제거합니다.

보류된 작업 항목을 방출하여 다른 참여자의 작업 목록에서 사용할 수 있게 합니다.

참고: 보류된 작업 항목을 해제하는 유일한 방법은 명시적으로 방출하는 것입니다.

작업 항목을 보류하거나 방출하려면

1. 사용자 콘솔에서 "홈", "내 작업 목록 보기"를 선택합니다.
작업 목록이 나타납니다.
2. 보류하거나 방출할 작업 항목을 선택합니다.
확장된 작업 항목 화면이 나타납니다.
3. "항목 보류" 또는 "항목 방출"을 클릭합니다.
CA Identity Manager 에서 동작을 확인합니다.

작업 항목 위임

작업 항목 *위임*을 사용하면 다른 사용자(위임받은 사람)가 위임자의 작업 목록에 있는 작업을 승인할 수 있도록 사용자(위임자)가 지정할 수 있습니다. 위임자는 "부재 중"인 기간 동안 다른 승인자에게 작업 항목을 할당할 수 있습니다. 위임 기간 동안 위임자는 작업 항목에 대한 모든 액세스 권한을 유지합니다.

위임된 작업 항목은 어떤 방식으로든 변경되지 않습니다. 로깅은 작업 항목이 위임되었는지 여부를 나타냅니다.

위임은 위임받은 사람이 위임자를 "가장"하고 위임자의 작업 목록에 있는 항목을 볼 수 있도록 하여 작동합니다. 작업 목록을 보는 동안 위임받은 사람에게는 해당 작업 항목은 물론 위임자의 작업 항목도 표시됩니다.

위임은 전이적입니다. 위임받은 사람은 위임자가 직접 할당한 작업 항목만 볼 수 있습니다. 예를 들어, 사용자 A가 사용자 B에게 작업 항목을 위임하고 사용자 B가 사용자 C에게 작업 항목을 위임하면 사용자 C는 사용자 B에 속하는 작업 항목만 볼 수 있고 사용자 A가 사용자 B에 위임한 작업 항목은 볼 수 없습니다.

추가 정보:

[위임 및 보류된 작업 항목](#) (페이지 376)

위임의 알려진 특성

위임은 다음과 같은 알려진 특성을 사용합니다.

%DELEGATORS%

이 알려진 특성은 해당 특성을 사용하여 사용자에게 위임하는 사용자의 이름과 위임이 만들어진 시간을 저장합니다.

위임을 사용하도록 설정하는 방법

다른 사용자에게 대한 위임 작업 항목을 사용하려면 먼저 워크플로 승인 위임을 사용하도록 설정해야 합니다. 기본적으로 위임은 사용되지 않습니다.

워크플로 승인 위임을 사용하도록 설정하려면

1. 브라우저에 다음 URL 을 입력하여 관리 콘솔을 엽니다.

`http://hostname/iam/immanage`

hostname

CA CA Identity Manager 가 설치된 서버의 정규화된 도메인 이름을 정의합니다. 예를 들어, `myserver.mycompany.com:port` 와 같이 입력합니다.

2. "환경"을 클릭하고 적절한 CA CA Identity Manager 환경의 이름을 선택합니다.
3. "고급 설정"을 클릭한 다음 "워크플로 승인 위임"을 클릭합니다.
4. "사용" 확인란을 선택하고 "저장"을 클릭합니다.

자신을 위해 위임하는 방법

"부재 중"인 기간 동안 다른 사용자에게 작업 항목을 위임할 수 있습니다.
위임 기간 동안 위임자는 작업 항목에 대한 모든 액세스 권한을 유지합니다.

자신의 작업 항목을 위임하려면

1. 사용자 콘솔에서 "홈", "부재 중 알림"을 선택합니다.
"부재 중 알림" 화면이 나타납니다.
2. "사용자 추가"를 클릭합니다.
사용자 선택 화면이 나타납니다.
3. 위임받은 사람 역할을 할 사용자를 하나 이상 검색하여 선택합니다.
위임 목록에 사용자가 추가됩니다.
4. "제출"을 클릭합니다.
작업이 제출되고 위임이 저장됩니다.

참고: 이미 위임받은 사람인 사용자는 위임을 추가할 때 검색 결과에 나타나지 않습니다.

추가 정보:

[위임을 사용하도록 설정하는 방법](#) (페이지 378)

시간 기반 작업 항목 위임

이전 릴리스에서는 위임의 시작 시간을 지정할 수 있었지만 종료 시간은 지정할 수 없었습니다. 새로 만들어진 위임의 날짜는 **true** 로 설정되며 기본 시작 시간은 지금으로 설정됩니다.

수정 시 시작 및 종료 날짜는 변경할 수 있습니다. 기본 종료 시간은 시작 날짜로부터 1 주일입니다.

시작 날짜 또는 종료 날짜를 바꾸려면 다음 작업을 수행하십시오.

1. 사용자 콘솔의 "홈" 탭에서 "부재 중 알림"을 선택합니다.
2. 위임 정보를 변경할 사용자 ID 옆의 연필 아이콘을 클릭합니다.
"위임 상세 정보 편집" 화면이 나타납니다.
3. 위임 시작 날짜를 변경하려면 "시작 날짜" 옆의 달력을 클릭합니다.
참고: 선택된 "위임 시작 날짜"가 현재 날짜 이전이면 오류 메시지가 표시됩니다.
4. 종료 날짜를 선택하려면 "종료 날짜 있음" 확인란을 선택하십시오.
이제 "종료 날짜" 필드를 사용하여 종료 날짜를 설정할 수 있습니다.
5. 위임이 종료되는 날짜를 설정하려면 "종료 날짜" 옆의 달력을 클릭합니다.
6. 날짜가 설정되면 "확인"을 클릭합니다.

또는 사용자를 만들거나 수정할 때 "작업 항목 위임" 탭에서 동일한 작업을 수행할 수 있습니다.

시간 기반 작업 항목 위임 활성화

업그레이드 시 기존 환경에서 시간 기반 작업 항목 위임을 활성화하려면 다음 작업을 수행하십시오.

관리 콘솔

1. "환경" 페이지로 이동합니다.
2. 선택한 "환경", "고급 설정", "작업 항목 위임"으로 드릴다운합니다.
3. "사용" 확인란을 선택 해제합니다.
4. 변경 사항을 저장하고 "환경"을 다시 시작합니다.
5. "고급 설정", "작업 항목 위임"으로 드릴다운합니다.
6. "사용" 확인란을 선택합니다.
7. 변경 사항을 저장하고 "환경"을 다시 시작합니다.

참고: 이 절차는 기존 환경에만 해당됩니다. 새 환경의 경우 시간 기반 워크플로 항목 위임이 활성화됩니다.

부재 중 알림 화면

다음 "부재 중 알림" 화면을 사용하여 자신을 위해 위임을 추가하고 제거하십시오.

"부재 중 알림" 화면에는 현재 위임 목록이 표시됩니다. 위임을 식별하는 열 외에도 다음 세 개의 추가 열이 목록에 포함됩니다.

시작 날짜

위임이 만들어진 날짜를 표시합니다.

끝 날짜

위임이 끝나는 날짜를 표시합니다.

위임 있음

위임에서 다른 사용자에게 작업 항목을 위임했는지 여부를 나타냅니다.

선택한 사용자 ID 옆의 연필 아이콘을 클릭하면 위임의 시작 날짜를 변경하고 위임 종료 날짜를 지정할 수 있는 "위임 정보 편집" 화면이 나타납니다.

다른 사용자를 위해 위임하는 방법

관리자는 한 사용자(위임자)의 작업 항목을 다른 사용자에게 위임할 수 있습니다. 예를 들어, 사용자가 예기치 않게 부재 중이거나 관리자가 큰 작업 부하를 여러 사용자에게 할당해야 할 수도 있습니다.

관리자는 범위가 있는 사용자의 작업 항목만 위임할 수 있습니다. 마찬가지로, 위임 목록에서만 관리하는 사용자를 추가하거나 제거할 수 있습니다.

다른 사용자의 작업 항목을 위임하려면

1. 사용자 콘솔에서 "사용자", "작업 항목 관리", "작업 항목 위임"을 선택합니다.
사용자 선택 화면이 나타납니다.
2. 작업 항목을 위임할 사용자(위임자)를 검색하고 "선택"을 클릭합니다.
작업 항목 위임 화면이 나타납니다.
3. "사용자 추가"를 클릭합니다.
사용자 선택 화면이 나타납니다.
4. 위임받은 사람 역할을 할 사용자를 하나 이상 검색하여 선택합니다.
위임 목록에 사용자가 추가됩니다.
5. "제출"을 클릭합니다.
작업이 제출되고 위임이 저장됩니다.

참고: 이미 위임받은 사람인 사용자는 위임을 추가할 때 검색 결과에 나타나지 않습니다.

추가 정보:

[위임을 사용하도록 설정하는 방법](#) (페이지 378)

위임을 제거하는 방법

사용자가 위임이 있는 CA CA Identity Manager 에 로그인하면 CA CA Identity Manager 에서 다음과 같은 미리 알림을 표시합니다.

위임이 있습니다. 이러한 위임이 아직 필요한지 확인하십시오.

자신을 위해 위임을 제거하려면

1. 사용자 콘솔에서 "홈", "부재 중 알림"을 선택합니다.
"부재 중 알림" 화면이 나타납니다.
2. 제거할 위임의 빼기 부호(-)를 클릭합니다.
위임이 목록에서 사라집니다.
3. "제출"을 클릭합니다.
작업이 제출되고 위임이 제거됩니다.

다른 사용자를 위해 위임을 제거하려면

1. 사용자 콘솔에서 "사용자", "작업 항목 관리", "작업 항목 위임"을 선택합니다.
사용자 검색 화면이 나타납니다.
2. 위임을 제거할 사용자를 검색하여 선택합니다.
위임 목록이 나타납니다.
3. 제거할 위임의 빼기 부호(-)를 클릭합니다.
위임이 목록에서 사라집니다.
4. "제출"을 클릭합니다.
작업이 제출되고 위임이 제거됩니다.

참고: 해당 사용자에 대한 범위가 있는 경우에만 위임을 제거할 수 있습니다.

작업 항목 재할당

재할당을 사용하면 사용자와 관리자가 작업 항목이 만들어진 후 작업 항목의 할당받은 사람을 변경할 수 있습니다. 관리자는 다음을 수행할 수 있습니다.

- 다른 사용자의 작업 목록을 볼 수 있습니다.
- 작업 항목의 할당받은 사람을 추가 및 제거할 수 있습니다.
- 작업 항목의 예약 상태를 변경할 수 있습니다.

예를 들어, 관리자는 작업하지 않는 사용자로부터 작업 항목을 재할당하거나 예약된 작업 항목을 릴리스할 수 있습니다.

재할당된 상태의 작업 항목을 예약하는 경우 작업 항목을 예약된 상태로 유지할 수 있습니다. 하지만 이후에 해당 작업 항목을 릴리스하면 해당 작업 항목에 대한 액세스 권한을 손실하게 됩니다.

위임이 철회된 상태에서 위임자가 작업 항목을 예약하면 작업 항목이 완료 또는 릴리스될 때까지 위임자는 액세스 권한을 보유합니다.

추가 정보:

[재할당 및 보류된 작업 항목](#) (페이지 376)

승인자 탭

현재 작업 항목 승인자나 할당받은 사람을 나열하는 목록을 표시하는 "Work Item Approvers"(작업 항목 승인자) 탭에서 재할당을 수행합니다. 재할당을 수행하면 개설된 작업 항목이 목록에 나열된 승인자 모두에게 할당됩니다. 따라서 새 할당받은 사람에게 작업 항목을 재할당하려면 현재 할당받은 사람을 제거해야 합니다.

작업 항목 재할당 방법

다음 두 단계 프로세스를 사용하여 한 사용자의 작업 항목을 다른 사용자에게 재할당할 수 있습니다.

- 새 승인자를 선택합니다.
- 현재 승인자를 제거합니다.

참고: 재할당하려는 사용자의 범위를 지정해야 합니다.

사용자 자신의 작업 항목을 재할당하려면

1. "홈", "내 작업 목록 보기"를 차례로 선택합니다.
작업 목록이 나타납니다.
2. 작업 항목을 선택하여 확장합니다.
3. "승인자" 탭을 선택합니다.
관리하는 작업 목록의 사용자를 포함하여 현재 모든 승인자 목록이 나타납니다.
4. "할당받은 사람 추가"를 클릭합니다.
사용자 선택 화면이 나타납니다.

5. 재할당할 사용자를 하나 이상 검색하여 선택합니다.

참고: ALL 및 SUBSET 승인 모드의 경우 작업 항목을 *단일* 사용자에게만 할당할 수 있습니다.

6. 할당받은 사람에서 사용자 자신을 제거하려면 음수 기호 단추(-)를 클릭합니다.
7. "재할당 수행"을 클릭합니다.

작업 항목이 재할당된 사용자의 작업 목록에 나타납니다.

참고: 관리자는 다른 사용자의 작업 항목을 재할당, 예약 또는 릴리스할 수 있지만 다른 사용자의 작업 항목을 승인 또는 거부할 수 없습니다. 오직 작업 항목의 소유자만 승인 또는 거부할 수 있습니다.

다른 사용자의 작업 항목을 재할당하려면

1. "사용자", "작업 항목 관리", "사용자의 작업 항목 관리"를 차례로 선택합니다.

사용자 선택 화면이 나타납니다.

2. 작업 항목을 재할당할 사용자를 검색하고 "선택"을 클릭합니다.
"사용자의 작업 항목 관리" 화면이 나타납니다.

3. 작업 항목을 선택하여 확장합니다.

4. "승인자" 탭을 선택합니다.

관리하는 작업 목록의 사용자를 포함하여 현재 모든 승인자 목록이 나타납니다.

5. "할당받은 사람 추가"를 클릭합니다.

사용자 선택 화면이 나타납니다.

6. 재할당할 사용자를 하나 이상 검색하여 선택합니다.
7. 현재 할당받은 사람에서 제거하려면 음수 기호 단추(-)를 클릭합니다.
8. "재할당 수행"을 클릭합니다.

작업 항목이 재할당된 사용자의 작업 목록에 나타납니다.

작업 항목에 대한 대량 오퍼레이션

이 CA Identity Manager 릴리스에서는 선택된 작업 항목에 대해 다음과 같은 대량 오퍼레이션을 수행할 수 있습니다.

- 승인
- 거부
- 보류
- 해제

사용자 콘솔에서 "작업 목록 구성" 탭이 새로운 "지원" 대량 워크플로 오퍼레이션 확인란을 포함하여 향상되었습니다. 이 확인란을 선택하면 사용자가 자신이 소유한 작업 항목 또는 위임자에게 받은 작업 항목을 대량 승인, 거부, 릴리스, 예약할 수 있습니다. 관리자가 작업 항목에 대해 이러한 대량 오퍼레이션을 수행하려면 "사용자의 작업 항목 관리" 태스크를 사용해야 합니다.

참고: 대량 오퍼레이션은 "내 작업 목록 보기"와 같은 보기 유형 태스크에 대해 사용할 수 없습니다.

대량 오퍼레이션을 위한 작업 목록 탭 구성

작업 항목에서 대량 오퍼레이션을 지원하도록 "작업 목록" 탭을 구성하려면 이 절차를 수행하십시오.

사용자 콘솔의 역할 및 태스크 탭

1. 둘 중 하나를 선택합니다.
 - 역할 및 태스크
 - 태스크, 역할 및 태스크
2. "관리자 태스크", "관리자 태스크 관리"를 선택합니다.
3. "검색"을 클릭합니다.
4. "사용자의 작업 항목 관리"를 선택합니다.
5. "탭" 탭에서 "작업 목록" 옆의 연필 아이콘을 클릭합니다.
"작업 목록 구성" 화면이 나타납니다.
6. "지원" 대량 워크플로 오퍼레이션을 선택합니다.
7. 변경 내용을 저장하고 태스크를 제출합니다.
이제 작업 항목에 대해 대량 오퍼레이션을 사용할 수 있습니다.

제 13 장: 전자 메일 알림

이 섹션은 다음 항목을 포함하고 있습니다.

[CA CA Identity Manager 의 전자 메일 알림](#) (페이지 390)

[전자 메일 알림 방식을 선택하는 방법](#) (페이지 391)

[SMTP 설정 구성](#) (페이지 393)

[전자 메일 알림 정책을 만드는 방법](#) (페이지 396)

[전자 메일 템플릿을 사용하는 방법](#) (페이지 406)

CA CA Identity Manager 의 전자 메일 알림

전자 메일 알림은 CA CA Identity Manager 사용자에게 시스템의 태스크와 이벤트에 대해 알려줍니다. 예를 들어, CA CA Identity Manager 는 이벤트 또는 태스크의 승인이 필요할 때 승인자에게 전자 메일을 보냅니다.

CA CA Identity Manager 에서는 다음 두 가지 방법으로 전자 메일 알림을 구성할 수 있습니다.

■ 전자 메일 알림 정책

전자 메일 알림 정책을 통해 비즈니스 관리자는 사용자 콘솔의 태스크를 사용하여 전자 메일 알림을 만들고, 보고, 수정하고, 삭제할 수 있습니다. 전자 메일 알림을 만들기 위해 코딩은 필요하지 않습니다.

관리자는 전자 메일의 내용, 보내는 시기 및 받는 사람을 정의할 수 있습니다. HTML 편집기에서 정의되는 전자 메일의 콘텐츠는 전자 메일이 발송될 때 CA CA Identity Manager 가 채우는 현재 날짜 또는 이벤트 정보와 같은 동적 정보를 포함할 수 있습니다. 예를 들어, 새 사용자가 생성될 때 승인자에게 전송되는 전자 메일 알림을 구성할 수 있습니다. 이 전자 메일에는 사용자의 로그인 정보, 채용 날짜 및 관리자가 포함될 수 있습니다.

참고: 전자 메일 알림 정책은 별도의 태스크 집합에 의해 생성되고 관리되는 [Policy Xpress 정책](#) (페이지 527)입니다.

■ 전자 메일 템플릿

이 방법에서는 전자 메일 템플릿에서 전자 메일 알림이 생성됩니다. CA CA Identity Manager 는 설치된 대로 사용하거나 시스템 관리자가 사용자 지정할 수 있는 기본 전자 메일 템플릿을 제공합니다. 이 관리자는 "Email Template"(전자 메일 템플릿) API 를 사용하여 받는 사람의 목록과 같은 동적 콘텐츠 및 전자 메일을 트리거하는 이벤트에 대한 정보를 지정합니다.

CA CA Identity Manager 는 다음과 같은 경우 전자 메일 알림을 생성할 수 있습니다.

■ 워크플로 승인자의 승인이나 거부 필요 이벤트가 보류 중인 경우

참고: 두 개 이상의 승인 활동이 포함된 Workpoint 승인 프로세스가 있는 경우 사용자 콘솔에서 구성된 전자 메일 알림이 각 활동에 대해 알림을 보냅니다. 동일한 알림에 대해 여러 개의 전자 메일 템플릿을 사용하는 경우에는 (이벤트가 보류 상태에 도달할 때) 하나의 전자 메일만 승인자에게 전송됩니다.

- 승인자가 이벤트 또는 태스크를 승인하는 경우
- 승인자가 이벤트 또는 태스크를 거부하는 경우
- 이벤트 또는 태스크가 시작하거나 실패 또는 완료되는 경우
- 사용자가 생성되거나 수정되는 경우

CA CA Identity Manager 전자 메일 알림을 사용하려면 [SMTP 설정](#) (페이지 393)을 구성하십시오. 전자 메일 템플릿 방법을 사용하는 경우 CA CA Identity Manager의 전자 메일 알림 기능도 활성화됩니다.

전자 메일 알림 방식을 선택하는 방법

다음 표는 전자 메일 알림 정책과 전자 메일 템플릿 사이의 차이에 대해 요약합니다.

활동	전자 메일 관리 태스크	전자 메일 템플릿
전자 메일 알림 구성	관리자가 "사용자 콘솔"에서 관리자 태스크를 사용하여 전자 메일 알림을 생성, 수정, 보기, 삭제합니다.	관리자가 CA Identity Manager 관리 도구에서 기본 템플릿을 수정합니다.

활동	전자 메일 관리 태스크	전자 메일 템플릿
전자 메일이 언제 발송될지 구성	CA CA Identity Manager 는 특정 이벤트 또는 태스크가 발생할 때 전자 메일 알림을 생성할 수 있습니다. 전자 메일 관리 태스크 및 전자 메일 템플릿은 동일한 이벤트 및 태스크를 지원하지만 일부의 경우에서 전자 메일 관리 태스크가 더 세부적입니다. 전자 메일 알림은 다음 태스크 및 이벤트에 대해 지원됩니다. ■ 워크플로 승인자의 승인이나 거부가 필요한 이벤트가 보류 중인 경우 ■ 참고: 여러 개의 승인 활동이 있는 Workpoint 승인 프로세스가 있는 경우 전자 메일 관리 태스크를 사용하여 구성된 전자 메일 알림이 각 활동에 대한 알림을 보냅니다. 동일한 알림에 대해 여러 개의 전자 메일 템플릿을 사용하는 경우에는 (이벤트가 보류 상태에 도달할 때) 하나의 전자 메일만 승인자에게 전송됩니다. ■ 승인자가 이벤트 또는 태스크를 승인하는 경우 ■ 승인자가 이벤트 또는 태스크를 거부하는 경우 ■ 이벤트 또는 태스크가 시작하거나 실패 또는 완료되는 경우 ■ 사용자가 생성되거나 수정되는 경우	
전자 메일에 동적 콘텐츠 추가	관리자가 "전자 메일 만들기" 또는 "전자 메일 수정" 태스크의 "콘텐츠" 탭에 있는 옵션 목록에서 옵션을 선택하여 전자 메일 메시지의 본문에 동적 콘텐츠를 추가합니다. CA CA Identity Manager 는 알림을 트리거하는 이벤트 또는 태스크의 정보를 기초로 동적 콘텐츠를 자동으로 채웁니다.	관리자가 "Email Template"(전자 메일 템플릿) API 를 사용하여 기본 전자 메일 템플릿(전자 메일 알림을 생성하는 데 사용됨)을 사용자 지정합니다.

활동	전자 메일 관리 태스크	전자 메일 템플릿
기존 전자 메일 알림 지원	전자 메일 관리 태스크를 사용하여 구성된 전자 메일 알림은 정책 Policy Xpress 정책에 기초합니다. CA CA Identity Manager 옵션 팩 1 에서 CA CA Identity Manager 12.6.4(으)로 업그레이드한 경우 Policy Xpress 에서 구성한 전자 메일 알림은 계속 동작합니다. 하지만 이러한 전자 메일 알림은 Policy Xpress 가 아닌 전자 메일 관리 태스크를 사용하여 관리합니다.	CA CA Identity Manager 의 이전 버전에서 전자 메일 템플릿 방법을 사용하여 생성한 전자 메일 알림은 CA CA Identity Manager 12.6.4 에서 계속 동작합니다.

SMTP 설정 구성

전자 메일 알림을 활성화하기 전에 SMTP 설정을 구성하십시오. 응용 프로그램 서버에 대해 SMTP 설정을 구성하려면 다음 절을 참조하십시오.

JBoss 에서 SMTP 설정 구성

1. 텍스트 편집기에서 다음과 같이 메일 서비스 배포 설명자를 엽니다.
단일 노드: `jboss_home\server\default\deploy\mail-service.xml`
클러스터: `jboss_home\server\all\deploy\mail-service.xml`
2. 다음과 같이 mail.smtp.host 속성을 SMTP 서버의 이름으로 수정합니다.
<-- Change to the SMTP gateway server -->
<property name="mail.smtp.host" value="your_smtp_server" />
예:
<property name="mail.smtp.host" value="smtp.mailserver.company.com" />
3. mail-service.xml 파일을 저장합니다.

4. 텍스트 편집기에서 다음 전자 메일 속성 파일을 엽니다.

단일 노드:

`jboss_home\server\default\deploy\iam_im.ear\config\com\netegrity\config\email.properties`

클러스터:

`jboss_home\server\all\deploy\iam_im.ear\config\com\netegrity\config\email.properties`

5. 워크플로 생성 전자 메일에서 사용되는 전자 메일 반환 주소를 설정하려면 `admin.email.address` 속성을 찾고 값을 적절한 전자 메일 주소로 설정합니다. 예:

`admin.email.address=admin@company.com`

6. 전자 메일 템플릿 방법을 사용하는 경우 관리 콘솔에서 전자 메일 알림을 활성화됩니다.

전자 메일 알림 정책을 사용하는 경우 관리 콘솔에서 전자 메일 알림을 활성화할 필요가 없습니다.

WebLogic 에서 SMTP 설정 구성

WebLogic Server Administration Console 과 `email.properties` 파일에서 전자 메일 설정을 구성합니다.

WebLogic 에 대해 전자 메일 설정을 구성하려면

1. WebLogic Server Administration Console 에서 다음 속성으로 메일 세션을 생성합니다.

- **mail.smtp.host** 속성: 이 값을 사용하는 SMTP 서버로 설정합니다. 예: `mail.smtp.host=mymailserver.company.com`

- **mail.transport.protocol** 속성: 이 값을 SMTP 로 설정합니다. 예: `mail.transport.protocol=smtp`

- **JNDI Name:** `nete/Mail`

- **Target:** WebLogic 서버 이름

2. 텍스트 편집기에서 CA CA Identity Manager 에 대한 다음과 같은 전자 메일 속성 파일을 엽니다.

`weblogic_domain\applications\iam.ear\config\com\netegrity\config\email.properties`

3. `admin.email.address` 속성을 찾아 값을 적절한 전자 메일 주소로 설정하여 워크플로 생성 전자 메일에서 사용되는 전자 메일 반환 주소를 설정합니다. 예:
`admin.email.address=admin@company.com`
4. 관리 콘솔에서 전자 메일 알림을 활성화합니다.
참고: 전자 메일 알림 정책을 사용하는 경우 관리 콘솔에서 전자 메일 알림을 활성화할 필요가 없습니다.

WebSphere 에서 SMTP 설정 구성

CA CA Identity Manager 구성 요소 설치 후에 실행하는 `imsSetup` 유틸리티는 `mailMail` 이란 이름의 새 메일 세션 개체를 구성합니다.

전자 메일 알림 기능이 올바르게 동작하도록 하려면 `mailMail` 세션에 대한 "Mail Transport Host"(메일 전송 호스트) 필드에 전자 메일을 보낼 때 WebSphere 가 연결하는 서버를 지정합니다.

`mailMail` 세션은 WebSphere Administrative Console 에서 "Resources"(리소스), "Mail Providers"(메일 공급자), "Built-in Mail Provider"(기본 메일 공급자), "Mail Sessions"(메일 세션), `mailMail` 에 있습니다.

참고: `mailMail` 개체를 보려면 "Mail Session"(메일 세션) 화면에서 "Scope"(범위)를 "Server"(서버)로 변경하십시오. 범위를 "Server"(서버)로 변경하지 않으면 `mailMail` 개체가 표시되지 않습니다.

WebSphere 메일 공급자를 구성하는 방법에 대한 자세한 내용은 WebSphere 설명서를 참조하십시오.

전자 메일 템플릿 방법을 사용하는 경우 SMTP 설정을 구성한 후에 관리 콘솔에서 전자 메일 알림을 활성화하십시오.

참고: 전자 메일 알림 정책을 사용하는 경우 관리 콘솔에서 전자 메일 알림을 활성화할 필요가 없습니다.

전자 메일 알림 정책을 만드는 방법

사용자 콘솔을 사용하여 특정 동작이 발생할 때 전자 메일을 보내는 전자 메일 알림 정책을 만들 수 있습니다. 예를 들어, 새 사용자가 만들어질 때 승인자에게 알리기 위해 전자 메일을 보내는 전자 메일 알림 정책을 만들 수 있습니다.

다음 단계를 수행하십시오.

1. "시스템", "전자 메일", "전자 메일 만들기"를 선택합니다.
2. 다음 옵션 중 하나를 선택하십시오.
 - "관리되는 전자 메일" 유형의 새 개체 만들기
 - "관리되는 전자 메일" 유형 개체의 복사본 만들기기존 전자 메일 알림 정책을 새 정책을 만들기 위한 템플릿으로 사용합니다.
3. "프로필" 탭에 전자 메일 알림 정책에 대한 기본 정보를 제공합니다.
4. "보낼 조건" 탭에 **CA Identity Manager** 가 전자 메일을 보내는 시기를 지정합니다.

"보낼 조건" 탭은 전자 메일 알림을 트리거하는 동작을 지정하기 위한 여러 가지 옵션을 제공합니다.
5. "받는 사람" 탭에 전자 메일을 받는 사람을 지정합니다.
6. "콘텐츠" 탭에 전자 메일의 제목과 내용을 정의합니다.

날짜, 태스크 또는 이벤트 이름, 사용자 특성과 같은 동적 콘텐츠를 전자 메일 내용에 지정할 수 있습니다.

전자 메일 알림 프로필 탭

전자 메일 관리 태스크의 "프로필" 탭을 사용하여 전자 메일 알림 정책에 대한 기본 정보를 지정할 수 있습니다. 이 탭에는 다음과 같은 필드가 있습니다.

전자 메일 이름

사용자 콘솔에서 전자 메일 알림 정책을 식별합니다.

참고: 전자 메일이 전송될 때 전자 메일 이름은 표시되지 않습니다. 이 이름은 사용자 콘솔에서 전자 메일 알림 정책을 관리하기 위해서만 사용됩니다.

범주

관리를 단순화하기 위해 전자 메일 알림 정책을 그룹으로 나눕니다.

드롭다운 목록에서 기존 범주를 선택하여 지정하거나 두 번째 옵션 단추를 선택하고 새 범주의 이름을 입력하십시오.

설명

전자 메일 알림 정책을 관리자에게 설명합니다.

전자 메일이 전송될 때 설명은 표시되지 않습니다.

사용

"보낼 조건" 탭에 정의된 조건이 충족될 때 CA CA Identity Manager 에서 전자 메일을 보내도록 지정합니다.

사용자 지정 데이터

Policy Xpress 에서 사용자 지정 받는 사람 또는 사용자 지정 콘텐츠를 구성하기 위해 사용할 수 있는 사용자 지정 데이터 요소를 만듭니다.

사용자 지정 데이터 요소는 또한 다른 데이터 요소에서 매개 변수로 사용할 수 있습니다.

참고: 데이터 요소에 대한 추가 정보는 [데이터](#) (페이지 534) 섹션에 나와 있습니다.

"사용자 지정 데이터"를 클릭하면 새 데이터 요소를 추가할 수 있는 화면이 열립니다.

진입 규칙

"보낼 조건" 탭의 기본 규칙이 충분히 세분화되지 않은 경우 CA CA Identity Manager 에서 전자 메일 알림을 보내는 시기에 대한 규칙을 정의합니다.

예를 들어, "보낼 조건" 탭은 사용자 프로필의 특성을 수정할 때 전자 메일을 보내는 기본 규칙을 제공합니다. 사용자 부서를 변경할 때만 CA CA Identity Manager 에서 전자 메일을 보내도록 하려는 경우 사용자 지정 진입 규칙을 만들 수 있습니다. 이 경우, 부서가 변경된 때를 식별하는 사용자 지정 데이터 요소를 만든 다음 이 사용자 지정 데이터 요소를 사용하는 진입 규칙을 만드십시오.

참고: 추가 정보는 [진입 규칙](#) (페이지 537) 섹션에 나와 있습니다.

보낼 조건 탭

CA Identity Manager 는 전자 메일이 전송되는 시기를 지정하는 여러 가지 기본 옵션을 제공합니다. 이 옵션 중 일부는 태스크 또는 이벤트 이름과 같은 추가 정보를 필요로 합니다. 예를 들어, 태스크를 시작할 때 전자 메일을 보내려면 전자 메일을 트리거하는 태스크를 선택해야 합니다.

다음 중 하나 이상의 "보낼 조건" 옵션을 선택할 수 있습니다.

사용자 생성됨

사용자가 생성되었을 때 전자 메일을 보냅니다. CreateUserEvent 가 완료될 때 전자 메일이 전송됩니다.

사용자 수정됨

사용자가 수정되었을 때 전자 메일을 보냅니다. ModifyUserEvent 가 완료될 때 전자 메일이 전송됩니다.

워크플로 보류

워크플로 프로세스가 승인자를 할당할 때 전자 메일을 보냅니다. 이 옵션을 선택할 경우에는 적용 가능한 워크플로 프로세스를 지정하십시오. 이 정책을 사용하여 정의된 전자 메일은 선택된 워크플로 프로세스의 모든 단계마다 승인자에게 개별 메일을 보냅니다.

워크플로 보류 중인 전자 메일

워크플로 프로세스가 지정된 활동에 도달할 때 전자 메일을 보냅니다. 이 옵션을 선택할 경우에는 적용 가능한 워크플로 프로세스를 지정하십시오. 이 정책을 사용하여 정의된 전자 메일은 각 승인 단계에 대한 개별 전자 메일 알림을 보냅니다.

이벤트 시작됨

이벤트가 "다음 이전" 상태에 도달할 때 전자 메일을 보냅니다. 이 옵션을 선택할 경우에는 이벤트를 지정하십시오.

참고: "이벤트 시작됨"을 지정한 경우 전자 메일이 전송에 실패하면 알림과 관련된 이벤트가 실행되지 않습니다.

이벤트 종료됨

이벤트가 "다음 이후" 상태에 도달할 때 전자 메일을 보냅니다. 이 옵션을 선택할 경우에는 이벤트를 지정하십시오.

이벤트 승인됨

이벤트가 "승인된" 상태에 도달할 때 전자 메일을 보냅니다. 이 옵션을 선택할 경우에는 이벤트를 지정하십시오.

이벤트 거부됨

이벤트가 "거부된" 상태에 도달할 때 전자 메일을 보냅니다. 이 옵션을 선택할 경우에는 이벤트를 지정하십시오.

이벤트 실패

이벤트가 실패할 때 전자 메일을 보냅니다. 이 옵션을 선택할 경우에는 이벤트를 지정하십시오.

태스크 제출됨

태스크가 처리를 시작할 때 전자 메일을 보냅니다. 이 옵션을 선택할 경우에는 태스크를 지정하십시오.

태스크 완료

태스크가 완료될 때 전자 메일을 보냅니다. 이 옵션을 선택할 경우에는 태스크를 지정하십시오.

태스크 실패

태스크가 실패하면 전자 메일을 보냅니다. 이 옵션을 선택할 경우에는 태스크를 지정하십시오.

받는 사람 탭

전자 메일의 "받는 사람", "참조", 또는 "숨은 참조" 필드에 대해 받는 사람을 여러 명 구성할 수 있습니다. 받는 사람 목록은 정적이거나, 전자 메일을 트리거하는 동작의 유형과 포함된 사용자에 따라 달라질 수 있습니다.

받는 사람을 지정하려면 "받는 사람" 탭에서 "받는 사람", "참조", 또는 "숨은 참조" 필드 옆의 "편집" 아이콘을 선택하십시오. 다음 옵션 중 하나를 선택하여 받는 사람 목록을 구성하십시오.

워크플로 승인자

워크플로 프로세스의 모든 승인자에게 전자 메일을 보냅니다. 이 옵션은 전자 메일이 워크플로 보류 이벤트를 위해 전송되는 경우에만 사용할 수 있습니다.

관리자

태스크가 수행된 사용자의 관리자에게 전자 메일을 보냅니다.

참고: "관리자" 받는 사람 옵션을 사용하려면 환경에 대해 관리자 특성을 구성하십시오. 관리자 특성을 구성하려면 관리 콘솔의 "환경", "환경 이름", "고급 설정", "기타"로 이동하십시오. `managerattribute` 를 사용자 관리자의 고유한 이름을 저장하는 물리적 특성 이름으로 설정하십시오.

관계형 데이터베이스의 경우 다음 형식을 사용하여 특성을 지정하십시오.

`tablename.attribute`

그룹 구성원

그룹의 모든 구성원에게 전자 메일을 보냅니다. 이 옵션을 선택하면 사용 가능한 그룹 이름의 드롭다운 목록이 열립니다.

역할 구성원

관리자 역할의 모든 구성원에게 전자 메일을 보냅니다. 이 옵션을 선택하면 사용 가능한 역할 이름의 드롭다운 목록이 열립니다.

고정 주소

선택한 전자 메일 주소에 전자 메일을 보냅니다. 사용 가능한 추가 텍스트 영역에 전자 메일 주소를 지정할 수 있습니다.

참고: 텍스트 영역에 두 개 이상의 주소를 지정하지 마십시오.

사용자

태스크가 수행된 사용자에게 전자 메일을 보냅니다.

요청의 초기자

요청한 사람에게 전자 메일을 보냅니다.

사용자 지정

사용자 지정 데이터 요소를 선택하여 받는 사람을 정의할 수 있습니다.

사용자 지정 옵션을 선택하면 사용 가능한 사용자 지정 데이터 요소의 드롭다운 목록이 표시됩니다.

참고: 데이터 요소에 대한 추가 정보는 [데이터](#) (페이지 534) 섹션에 나와 있습니다.

콘텐츠

단순 텍스트를 사용하여 전자 메일의 제목과 본문을 정의하거나, 전자 메일이 전송될 때 계산되는 동적 콘텐츠를 사용하여 전자 메일의 제목과 본문을 추가할 수 있습니다.

제목 줄은 메시지를 작성할 수 있는 일반 텍스트 필드입니다. 이 메시지가 전자 메일의 제목입니다.

본문은 **HTML** 편집기에 표시됩니다. 텍스트를 삽입하고 형식을 지정하여 전자 메일의 본문을 작성할 수 있습니다.

동적 콘텐츠를 포함하려면 드롭다운 목록에서 옵션을 선택하십시오. 편집기의 커서 위치에 다음과 같은 모양의 동적 콘텐츠 표시기가 추가됩니다.

{*유형*}

*유형*은 지원되는 동적 콘텐츠 유형 중 하나를 나타냅니다.

예를 들어, "특성" 동적 콘텐츠 유형을 선택하고 **FirstName** 특성을 지정하면 **HTML** 편집기가 "콘텐츠" 탭에 다음 항목을 표시합니다.

{특성: **FirstName**}

참고: 제목 줄에 동적 콘텐츠를 추가하려면 제목 줄 아래 드롭다운 목록을 사용하십시오. 전자 메일 본문에 동적 콘텐츠를 추가하려면 콘텐츠 상자 아래 드롭다운 목록을 사용하십시오.

전자 메일 메시지가 전송될 때 **CA CA Identity Manager** 가 동적 콘텐츠를 적절한 텍스트로 대체합니다. 텍스트에는 **HTML** 편집기에서 지정된 굵게 표시된 문자와 같은 서식이 유지됩니다.

동적 콘텐츠에는 다음과 같은 유형이 있습니다.

날짜

오늘 날짜를 사용자가 지정하는 형식으로 지정합니다.

태스크

전자 메일이 전송되는 태스크를 지정합니다.

개체 이름

전자 메일을 트리거하는 이벤트에 개체의 이름을 지정합니다. 이벤트가 사용자 이벤트인 경우 이 필드는 사용자 로그인 이름입니다.

사용자가 아닌 다른 항목을 개체로 지정할 수 있습니다. 예를 들어, 그룹, 관리자 역할 등과 같은 관리 개체를 지정할 수 있습니다.

특성

사용자 특성 중 하나의 값을 지정합니다. 사용자가 태스크의 대상입니다. 이 옵션을 사용하려면 드롭다운 목록에서 특성을 선택해야 합니다.

관리자 특성

사용자의 관리자 특성 중 하나의 값을 지정합니다. 사용자가 태스크의 대상입니다. 이 옵션을 사용하려면 드롭다운 목록에서 특성을 선택해야 합니다.

참고: "관리자" 받는 사람 옵션을 사용하려면 환경에 대해 관리자 특성을 구성하십시오. 관리자 특성을 구성하려면 관리 콘솔의 "환경", "환경 이름", "고급 설정", "기타"로 이동하십시오. `managerattribute` 를 사용자 관리자의 고유한 이름을 저장하는 물리적 특성 이름으로 설정하십시오.

관계형 데이터베이스의 경우 다음 형식을 사용하여 특성을 지정하십시오.

`tablename.attribute`

사용자 지정

사용자 지정 데이터 요소를 선택하여 받는 사람을 정의할 수 있습니다.

사용자 지정 옵션을 선택하면 사용 가능한 사용자 지정 데이터 요소의 드롭다운 목록이 표시됩니다.

참고: 데이터 요소에 대한 추가 정보는 [데이터](#) (페이지 534) 섹션에 나와 있습니다.

전자 메일 알림 정책 수정

기존 전자 메일 알림 정책을 비즈니스 요구 사항에 적합하도록 수정할 수 있습니다.

전자 메일 알림 정책을 수정하려면

1. "시스템", "전자 메일", "전자 메일 만들기"를 선택합니다.
CA Identity Manager 가 검색 화면을 표시합니다.
2. 수정할 전자 메일 알림 정책을 검색하여 선택합니다.
3. 필요에 따라 "프로필", "보낼 조건", "받는 사람" 및 "콘텐츠" 탭의 설정을 변경합니다.

전자 메일 알림 정책 비활성화

전자 메일 알림 정책을 만들거나 수정할 때 "프로필" 탭의 "사용" 확인란을 사용하여 전자 메일 알림 정책을 활성화하거나 비활성화할 수 있습니다. 전자 메일 알림 정책이 비활성화되면 선택한 전자 메일이 활성화되지 않으며 어떤 전자 메일도 전송되지 않습니다.

참고: 전자 메일 알림 정책은 기본적으로 활성화됩니다.

사용 사례: 환영 전자 메일 보내기

Forward, Inc.에서는 신입사원을 채용하면 해당 사용자에게 입사를 환영하는 전자 메일을 보내려고 합니다. 이 전자 메일은 신입사원에게 사원 홈 페이지에 대한 링크와 같이 중요한 정보 및 관리자와 부서에 대한 정보를 제공해야 합니다.

전자 메일을 만들기 위해 인사부 관리자는 사용자 콘솔의 "전자 메일 만들기" 태스크를 사용하여 다음 설정을 구성합니다.

- "보낼 조건" 탭에서 "사용자 생성됨"을 선택합니다.
- "받는 사람" 탭에서 다음 단계를 완료합니다.
 - "받는 사람" 필드 옆의 "편집" 아이콘을 클릭합니다.
"사용자"를 선택한 다음 더하기 부호를 클릭합니다. 같은 방법을 사용하여 "관리자"를 선택한 다음 "확인"을 클릭합니다.
 - "참조" 필드 옆의 "편집" 아이콘을 클릭합니다.
"초기자"를 선택하고 더하기 부호를 클릭한 다음 "확인"을 클릭하여 CA CA Identity Manager 에서 사원을 만든 사용자에게 전자 메일의 복사본을 보냅니다.
- "콘텐츠" 탭에서 다음 단계를 완료합니다.
 - "제목" 필드에 **Welcome** 텍스트를 입력합니다.
입력한 텍스트 끝에 커서를 두고 드롭다운 목록에서 "특성"을 선택합니다. 그런 다음, 두 번째 드롭다운 목록에서 "전체 이름"을 선택한 다음 더하기 부호를 클릭합니다.
제목 줄이 다음과 비슷하게 표시됩니다.
Welcome, {'특성: eTFullName'}
참고: 특성 이름은 사용 중인 사용자 저장소와 특성에 따라 달라집니다.
 - "콘텐츠" 상자에 환영 텍스트를 추가합니다. 다음과 같이 사원 포털에 대한 링크를 포함하고 콘텐츠 상자 아래 동적 콘텐츠 옵션을 사용하여 사용자의 부서, 관리자, 관리자의 전화 번호를 표시하십시오.

프로필

보낼 조건

받는 사람

콘텐츠

•제목 Welcome, {'Attribute: cn'}

관리자 특성Business Phone (telephoneNumber)

formatfontsize

Hello, {'Attribute: givenName'},

Welcome to Forward, Inc. We are so glad that you joined our team!

Here are some helpful links to get you started in your new role:

[Employee home page](#)

[Intranet](#)

You may also need the following information about your department and manager:

Department: {'Attribute: departmentNumber'}

Manager: {'Manager Attribute: cn'}

Manager Phone: {'Manager Attribute: telephoneNumber'}

전자 메일 템플릿을 사용하는 방법

CA Identity Manager 는 전자 메일 메시지를 생성하는 데 사용할 수 있는 기본 전자 메일 템플릿을 포함하고 있습니다. 기본 템플릿은 설치된 대로 사용하거나 비즈니스 필요성에 맞게 사용자 지정할 수 있습니다.

전자 메일 템플릿을 사용하려면

1. CA Identity Manager 가 전자 메일 알림을 보내도록 SMTP 설정을 구성합니다.
2. [관리 콘솔에서 전자 메일 알림을 활성화합니다](#) (페이지 407).
3. [전자 메일을 보내도록 이벤트 또는 태스크를 구성합니다](#). (페이지 407)
4. (선택 사항) 필요한 경우 [기본 템플릿을 사용자 지정](#) (페이지 413)합니다.

전자 메일 알림 사용

CA Identity Manager 환경에 대한 전자 메일 알림을 사용 또는 사용하지 않을 수 있습니다. 전자 메일 알림을 사용하는 경우 CA CA Identity Manager 는 지정하는 이벤트 및 태스크에 대한 전자 메일 알림을 보냅니다.

참고: "잊어버린 암호" 기능을 사용하려면 전자 메일 알림을 사용 설정하십시오.

CA CA Identity Manager 에서 전자 메일 알림을 사용 설정하기 전에 응용 프로그램 서버에 대한 [SMTP 설정을 구성](#) (페이지 393)하십시오.

전자 메일 알림을 사용하려면

1. 관리 콘솔에서 "환경"을 클릭합니다.
CA Identity Manager 환경의 목록이 표시됩니다.
2. 적절한 Identity Manager 환경을 클릭합니다.
3. "Advanced Settings"(고급 설정, "Email"(전자 메일)로 이동합니다.
4. "Enabled"(사용) 확인란을 선택합니다.
5. [전자 메일을 트리거하는 이벤트와 태스크를 구성합니다](#) (페이지 407).
6. "저장"을 클릭합니다.
7. CA CA Identity Manager 가 설치된 응용 프로그램 서버의 인스턴스를 다시 시작합니다.

전자 메일을 보내도록 이벤트 또는 태스크 구성

전자 메일 알림이 사용되는 경우 전자 메일 알림을 트리거하는 이벤트 또는 태스크의 목록을 지정할 수 있습니다. 예를 들어, 다음과 같은 상황에서 전자 메일을 보낼 수 있습니다.

- "사용자 암호 재설정" 태스크 완료 시 시스템 관리자에게 전자 메일을 보냅니다.
- "사용자 만들기" 태스크 완료 시 새 직원의 관리자에게 전자 메일을 보냅니다. 또한, "사용자 만들기" 태스크가 승인된 기간 내 AddToGroupEvent 가 생성되면 새 사용자가 추가되는 그룹의 모든 구성원에게 또 다른 전자 메일을 보낼 수 있습니다.

전자 메일 알림을 트리거하는 이벤트 및 태스크를 지정하려면

1. 관리 콘솔에서 "환경"을 클릭합니다.
CA Identity Manager 환경의 목록이 표시됩니다.
2. 적절한 CA Identity Manager 환경을 클릭합니다.
3. "Advanced Settings"(고급 설정, "Email"(전자 메일)로 이동합니다.
"Email Properties"(전자 메일 속성) 화면이 열립니다.
4. 해당하는 다음과 같은 "Enable"(사용) 확인란을 선택합니다.
 - Events E-mail Enabled(이벤트 전자 메일 사용)
CA Identity Manager 이벤트에 대한 전자 메일 알림을 사용합니다.
 - Tasks Email Enabled(태스크 전자 메일 사용)
CA Identity Manager 태스크에 대한 전자 메일 알림을 사용합니다.
5. CA CA Identity Manager 가 전자 메일 메시지를 작성하는 데 사용하는 전자 메일 템플릿의 위치를 입력합니다.

전자 메일 템플릿은 다음 위치의 하위 디렉터리에 있습니다.

iam_im.ear\custom\emailTemplates

참고: 전자 메일 템플릿을 만들 때 템플릿의 파일 이름에 다른 언어를 사용하는 경우 운영 체제 세션이 해당 문자 세트를 지원하는 언어로 실행되고 있어야 합니다.

6. 다음과 같이 전자 메일 알림을 전달할 이벤트를 지정합니다.
 - 이벤트를 추가하려면 "Event"(이벤트) 목록 상자에서 이벤트를 선택한 다음 "Add"(추가)를 클릭하십시오.
CA CA Identity Manager 는 선택한 이벤트를 전자 메일 알림을 보낼 이벤트의 목록에 추가합니다.
참고: 워크플로 프로세스와 관련이 없는 이벤트를 선택하는 경우 CA CA Identity Manager 는 해당 이벤트가 완료될 때 전자 메일 알림을 보냅니다.
 - 이벤트를 삭제하려면 이벤트의 확인란을 선택한 다음 "Delete"(삭제)를 클릭하십시오.

7. 다음과 같이 전자 메일 알림을 전달할 태스크를 지정합니다.
 - 태스크를 추가하려면 첫 번째 필드에서 조건을 선택하여 태스크를 검색한 다음 두 번째 필드에 태스크 이름을 입력하십시오. "검색"을 클릭합니다.

와일드카드(*) 문자를 사용하여 태스크 이름의 일부만 입력할 수 있습니다. 예를 들어, 'Create' 태스크를 검색하려면 Create*를 입력하십시오.

검색 결과에서 하나 이상의 태스크를 선택하십시오. "추가"를 클릭합니다.

참고: 동작 유형이 "보기" 또는 "자체 보기"인 태스크에는 태스크 수준 전자 메일 알림을 사용할 수 없습니다. 태스크의 동작 유형을 보려면 "관리자 태스크 수정"으로 이동하여 "태스크"를 선택한 다음 태스크 프로필의 동작 필드를 확인하십시오.

 - 태스크를 삭제하려면 태스크의 확인란을 선택한 다음 "Delete"(삭제)를 클릭하십시오.

태스크를 삭제하면 "Task"(태스크) 표에서 태스크가 제거됩니다. 이렇게 해도 태스크가 삭제되지 않습니다.
8. 전자 메일 알림을 트리거하는 태스크와 이벤트의 구성을 완료한 다음에는 "Save"(저장)를 클릭합니다.
9. CA CA Identity Manager 가 설치된 응용 프로그램 서버를 다시 시작합니다.

전자 메일 내용

전자 메일 알림은 일반 템플릿과 전자 메일 API 를 통해 전자 메일에 추가되는 태스크별 정보로 구성됩니다. 예를 들어, 다음 정보는 "사용자 만들기" 태스크에 대한 전자 메일에 삽입될 수 있습니다.

- 태스크를 실행하는 관리자의 이름
- 새 사용자의 이름
- 사용자의 전자 메일 주소, 부서 이름, 기타 특성 데이터
- 사용자를 만드는 조직
- 워크플로 승인 상태 및 승인 시간
- 태스크 이름 및 태스크의 이벤트 이름

전자 메일 템플릿

전자 메일 알림은 전자 메일 템플릿으로부터 생성됩니다. Identity Manager 는 설치되었을 때 그대로 사용하거나 자체 전자 메일 템플릿을 만들 때 사용할 수 있는 기본 전자 메일 템플릿을 제공합니다.

각 전자 메일 템플릿은 다음을 포함하고 있습니다.

- **배달 정보**--전자 메일 수신자의 목록입니다. Identity Manager 는 태스크에 관련된 사용자를 기준으로 수신자 목록을 자동으로 생성합니다. 예를 들어, 승인 전자 메일은 태스크의 모든 승인자에게 전달됩니다.
- **제목**--메시지의 제목줄에 사용되는 텍스트입니다.
- **내용**--메시지 본문입니다. 본문은 주로 전자 메일을 트리거하는 작업 또는 이벤트를 기반으로 [set the value for eACPMI at the book level]가 결정하는 정적 텍스트 및 변수를 모두 포함합니다.

기본 전자 메일 템플릿은 Identity Manager 관리 도구가 설치된 emailTemplates 디렉터리에 있습니다. 관리 도구의 기본 설치 위치:

- Windows--C:\Program Files\CA\CA Identity Manager\
- UNIX--<home_directory>/CA/CA Identity Manager

emailTemplates 디렉터리에는 4 개의 폴더가 들어 있습니다. 각 폴더는 태스크 또는 이벤트 상태와 관련이 있습니다.

디렉터리	목적
승인됨	defaultEvent.tmpl--이벤트가 승인되었음을 수신자에게 알립니다.

디렉터리	목차
완료함	■ CertificationNonCertifiedActionCompletedNotification.tmpl--비 규정 준수 동작이 직원에게 적용되었음을 매니저에게 알립니다. ■ CertificationNonCertifiedActionPendingNotification.tmpl--비 규정 준수 동작이 직원에게 적용될 것임을 매니저에게 알립니다. ■ CertificationRequiredFinalNotification.tmpl--직원에 대해 "사용자 인증" 태스크를 완료해야 함을 매니저에게 마지막으로 알립니다. ■ CertificationRequiredNotification.tmpl--직원에 대해 인증 프로세스가 시작되었음을 매니저에게 알립니다. 매니저는 이 직원에 대해 "사용자 인증" 태스크를 반드시 완료해야 합니다. ■ CertificationRequiredReminderNotification.tmpl--직원에 대해 "사용자 인증" 태스크를 완료해야 함을 매니저에게 알립니다. ■ Certify Employee.tmpl--직원에 대한 인증 프로세스가 완료되었음을 관리자에게 알립니다. ■ CreateProvisioningUserNotificationEvent.tmpl--사용자의 계정이 프로비저닝 디렉터리에 생성된 경우 사용자에게 임시 암호를 보냅니다. ■ defaultTask.tmpl--Identity Manager 가 태스크를 완료했음을 수신자에게 알립니다. ■ ForgottenPassword.tmpl--잊어버린 암호 기능을 사용한 사용자에게 임시 암호를 보냅니다. ■ ForgottenUserID.tmpl--잊어버린 사용자 ID 기능을 사용한 사용자에게 사용자 ID 를 보냅니다. ■ Self Registration.tmpl--자체 등록 태스크가 성공적으로 완료되었음을 사용자에게 알립니다.
보류	■ defaultEvent.tmpl--승인자에게 작업 목록 항목의 검토가 필요함을 알립니다. ■ ModifyUserEvent.tmpl--기본 템플릿과 동일하지만 "사용자" 관리 개체의 특성을 검색하는 메서드를 포함합니다.

디렉터리	목차
거부됨	defaultEvent.tmpl--이벤트가 거부되었음을 수신자에게 알립니다.

사용자 지정 전자 메일 템플릿을 만들 때는 `<im_admin_tools_dir>\Identity Manager\emailTemplates` 디렉터리에 설치된 Identity Manager 템플릿과 템플릿 디렉터리 구조를 기초로 사용하십시오.

템플릿 디렉터리

[전자 메일 템플릿](#) (페이지 410)에 설명된 각 템플릿 디렉터리는 특정 태스크 또는 이벤트 상태와 관련이 있습니다. 예를 들어, 워크플로 프로세스에서 거부된 이벤트에 대해 전자 메일을 보내는 경우 Identity Manager 는 배포된 '거부됨' 디렉터리에서 사용할 템플릿을 찾습니다. 그런 다음 Identity Manager 는 이 디렉터리에 있는 적절한 전자 메일 템플릿으로부터 전자 메일을 생성합니다.

디렉터리의 전자 메일 템플릿

각 배포된 템플릿 디렉터리에는 하나 이상의 전자 메일 템플릿이 포함되어 있습니다. 전자 메일을 사용하는 이벤트에 대해 태스크 또는 이벤트가 발생하는 경우 Identity Manager 는 적절한 템플릿 디렉터리에서 해당 태스크 또는 이벤트의 이름과 동일한 템플릿 이름을 찾습니다. 해당 템플릿을 찾을 수 없으면 Identity Manager 는 디렉터리의 기본 템플릿을 사용합니다. 기본 템플릿 이름은 [전자 메일 템플릿](#) (페이지 410)에 나열되어 있습니다. 예를 들어, Identity Manager 는 '보류' 디렉터리에 있는 defaultEvent.tmpl 을 사용하여 승인자에게 새 작업 목록 항목이 있음을 알립니다.

템플릿 디렉터리 세트

템플릿 디렉터리 세트에는 '승인됨', '완료함', '보류', '거부됨' 디렉터리가 포함됩니다. 여러 템플릿 디렉터리 세트를 배포하고 특정 Identity Manager 환경에 사용할 하나의 세트를 지정할 수 있습니다.

템플릿 디렉터리 세트를 배포하는 방법에 대한 자세한 내용은 [전자 메일 템플릿 배포](#) (페이지 434)를 참조하십시오.

Identity Manager 가 지정된 환경에 올바른 세트를 사용하도록 전자 메일 템플릿 디렉터리를 구성하는 방법에 대한 자세한 내용은 *CA Identity Manager Configuration Guide*(CA Identity Manager 구성 안내서)를 참조하십시오.

전자 메일 템플릿 만들기

사용자 지정 전자 메일 메시지를 만들려면

1. 수정할 템플릿을 엽니다.

예를 들어, 보류 중인 "사용자 만들기" 이벤트에 대한 전자 메일 메시지를 만들려면 '보류' 디렉터리에서 `defaultEvent.tmpl` 을 여십시오.

2. 새 이름으로 동일한 디렉터리에 템플릿을 저장합니다. 이름은 전자 메일이 적용되는 이벤트의 이름과 일치해야 하며 확장명 `.tmpl` 을 사용해야 합니다.

예를 들어, 보류 중인 "사용자 만들기" 이벤트에 대한 메시지의 이름을 다음과 같이 지정할 수 있습니다.

`CreateUserEvent.tmpl`

이벤트의 목록은 "Identity Manager 이벤트"를 참조하십시오.

참고: 전자 메일 템플릿을 만들 때 템플릿의 파일 이름에 다른 언어를 사용하는 경우 운영 체제 세션이 해당 문자 세트를 지원하는 언어로 실행되고 있어야 합니다.

3. 다음 절 [사용자 지정 메일 템플릿](#) (페이지 414)의 설명을 참조하여 필요에 따라 메시지 템플릿을 수정합니다.

사용자 지정 전자 메일 템플릿

전자 메일 템플릿은 HTML 과 포함된 서버 측 JavaScript 를 모두 지원하는 동적 파일입니다. 템플릿을 사용하면 정적 텍스트에 변수 값을 삽입할 수 있으므로 하나의 템플릿에서 상황별 메시지를 생성할 수 있습니다.

반복해서 사용되는 상용구 정적 텍스트(예: 승인 내용)와 함께 지정된 컨텍스트와 관련된 가변 텍스트(예: 승인되는 이벤트의 이름)를 표시하기 위해 동일한 템플릿을 여러 번 다시 사용할 수 있습니다.

예를 들어, 다음은 이벤트의 승인을 보고하기 위한 템플릿입니다.

```
<!-- Define the E-mail Properties --->
<%
    _to = _util.getNotifiers("ADMIN");
    _cc = "" ;
    _bcc = "";
    _subject = _eventContextInformation.getEventName() + " approved";
%>
<!-- Start of Body --->
<html>
<body text="Navy">

Event: <b> <%= _eventContextInformation.getEventName() %> </b><br>
<%= _eventContextInformation.getPrimaryObjectTypeName() %>:
<b><%= _eventContextInformation.getPrimaryObjectName() %></b><br>
In <%= _eventContextInformation.getSecondaryObjectTypeName() %>:
<b><%= _eventContextInformation.getSecondaryObjectName() %></b><br>
Status: <b>Approved</b>
</body>
</html>
```

참고: 위의 예제에서 사용된 Identity Manager 개체 `_util` 및 `_eventContextInformation` 은 "Email Template"(전자 메일 템플릿) API 에 설명되어 있습니다.

이벤트 `CreateUserEvent` 에 대해 승인이 생성되면 사용자 John Jones 가 조직 HR 에 생성되고, 승인 템플릿으로부터 생성된 전자 메일 알림의 본문은 다음과 같습니다.

```
Event: CreateUserEvent
USER: John Jones
In ORGANIZATION: HR
Status: Approved
```

다음 절에서는 동적 전자 메일 메시지를 가능하게 하는 구문 및 Identity Manager 개체에 대해 설명합니다.

템플릿 요소

Identity Manager 전자 메일 템플릿 지원:

- 표준 HTML 태그
- 서버 측 JavaScript
- 템플릿의 인스턴스(즉, 전자 메일 메시지)에 대해 Identity Manager 가 사용 가능하게 만드는 하나 이상의 암시적 개체
- 템플릿에 JavaScript 를 포함하고, 암시적 Identity Manager 개체에서 메서드를 호출하고, 템플릿의 정적 텍스트에 변수 값을 삽입할 수 있게 해주는 Identity Manager 태그

Identity Manager 태그 확장

전자 메일 템플릿은 다음 태그를 지원합니다.

<% %>

JavaScript 를 전자 메일 템플릿에 포함합니다.

<%= %>

변수 값을 정적 테스트에 삽입합니다.

태그는 다음 절에서 설명합니다.

<% %>

이 태그는 인라인 실행을 위한 JavaScript 를 전자 메일에 삽입할 수 있게 해줍니다.

포함된 JavaScript 내에서 임의의 JavaScript 개체를 사용할 수 있습니다. 또한 포함된 JavaScript 내에서 Identity Manager 암시적 개체 메서드를 호출할 수도 있습니다.

예를 들어, 다음 코드는 [사용자 지정 전자 메일 템플릿](#) (페이지 414)에 표시된 승인 템플릿의 본문을 수정합니다. JavaScript 는 이벤트에서 보조 개체(예: USER 기본 개체가 추가될 때 ORGANIZATION 개체)가 관여되는지 여부를 파악하는 데 사용됩니다. 보조 개체가 없는 경우 보조 개체와 관련된 텍스트가 메시지에서 누락됩니다.

```
Event: <b> <%= _eventContextInformation.getEventName()%> </b><br>
<%= _eventContextInformation.getPrimaryObjectTypeName()%>:
<b><%= _eventContextInformation.getPrimaryObjectName()%></b><br>
<%
var secondaryType = _eventContextInformation.getSecondaryObjectTypeName();
if (secondaryType != "") {
    template.add("In " + secondaryType + ": ");
    template.add("<b> "+_eventContextInformation.getSecondary
                                ObjectName()+" </b><br>");
}
%>
Status: <b>Approved</b>
```

<%= %>

이 태그는 변수 값을 정적 텍스트에 삽입할 수 있게 해 줍니다. 값은 다음과 같을 수 있습니다.

- 템플릿에서 일부 이전에 실행된 JavaScript 에 정의된 변수. 예:

```
<%
var secondaryType = _eventContextInformation.getSecondaryObjectTypeName();
...           // More JavaScript processing
%>
...           // More HTML
The primary object was created in <%=secondaryType%>.
```

- Identity Manager 암시적 개체의 메서드에서 반환된 값. 예:

```
Event <%= _eventContextInformation.getEventName()%> is approved.
```

전자 메일 템플릿 API

템플릿에서 메시지가 생성되면 Identity Manager 는 아래 암시적 개체를 메시지에 대해 사용할 수 있게 만듭니다. 이러한 개체는 "Email Template"(전자 메일 템플릿) API 에서 메서드를 호출하여 메시지에 인스턴스 관련 정보를 삽입할 수 있게 해 줍니다.

템플릿은 다음 모든 개체에서 메서드를 호출할 수 있습니다.

- `_contentType`. 전자 메일에 대한 `contentType` 을 지정합니다.
- `_priority`. 전자 메일에 대한 우선 순위를 지정합니다.

- `_to`. 메시지의 받는 사람 필드에 받는 사람을 추가합니다.
- `_cc`. 메시지의 cc(사본 전달) 필드에 받는 사람을 추가합니다.
- `_bcc`. 메시지의 bcc(비밀 사본 전달) 필드에 받는 사람을 추가합니다.
- `_subject`. 전자 메일의 제목을 지정합니다.
- `_encoding`. 전자 메일의 인코딩을 지정합니다.
- `template`. JavaScript 코드 줄로부터 메시지에 텍스트 문자열을 추가할 수 있게 해 줍니다.
- `_util`. 유틸리티 개체입니다.
- `_eventContextInformation`. 이벤트 이름과 승인 상태와 같은 현재 태스크에 의해 생성된 이벤트에 대한 정보를 수록하고 있습니다.
- `_taskContextInformation`. 태스크 이름, 조직 이름, 구성 요소 이벤트와 같은 현재 태스크에 대한 여러 정보를 수록하고 있습니다.

이러한 개체는 다음 절에서 설명합니다.

`_contentType`

전자 메일에 대한 `contentType` 을 지정합니다.

`_contentType` 변수를 통해 지정된 `contentType` 이 없으면 기본 `contentType` "text/html"이 적용됩니다.

메서드: 없음

예:

```
<% _contentType = "text/html"; %>
```

_priority

전자 메일에 대한 우선 순위를 지정합니다. 우선 순위가 없으면 0 을 지정하고 가장 높은 우선 순위는 1 을 지정하십시오.

메서드: 없음

예:

```
<% _priority = "1"; %>
```

_to

메시지의 받는 사람 필드에 받는 사람을 추가합니다.

_to 변수의 값은 JavaScript 문자열입니다. 여러 받는 사람이 허용되지만 문자열은 다음 예제와 같이 JavaScript 구문을 준수해야 합니다.

메서드: 없음

예:

```
<%  
_to =  
_util.getNotifiers("USER") + ',' +  
_util.getNotifiers("USER_MANAGER", "ManagerLookup=managerattribute");  
_cc = "" ;  
_bcc = "" ;  
_subject = "Your new password ";  
%>
```

참고: 태스크가 보류 상태이고 워크플로 제어 중임을 알리는 전자 메일이 참여자들에게 전달될 때는 **_to** 개체는 참여자들의 주소에 미리 채워집니다. **_to** 개체는 "보류" 템플릿에서 사용할 수 없습니다.

_cc

메시지의 cc(사본 전달) 필드에 받는 사람을 추가합니다.

_to 변수의 값은 JavaScript 문자열입니다. 여러 받는 사람이 허용되지만 문자열은 다음 예제와 같이 JavaScript 구문을 준수해야 합니다.

메서드: 없음

예:

```
<%
_cc =
_util.getNotifiers("USER") + ',' +
_util.getNotifiers("USER_MANAGER", "ManagerLookup=managerattribute");
%>
```

_bcc

메시지의 bcc(비밀 사본 전달) 필드에 받는 사람을 추가합니다.

이 필드에 지정된 전자 메일 주소는 전자 메일에 표시되지 않습니다.

`_to` 변수의 값은 JavaScript 문자열입니다. 여러 받는 사람이 허용되지만 문자열은 다음 예제와 같이 JavaScript 구문을 준수해야 합니다.

메서드: 없음

예:

```
<%
_bcc =
_util.getNotifiers("USER") + ',' +
_util.getNotifiers("USER_MANAGER", "ManagerLookup=managerattribute");
%>
```

_subject

전자 메일의 제목을 지정합니다.

메서드: 없음

예:

```
<% _subject=_eventContextInformation.getEventName()+" approved";%>
```

_encoding

전자 메일의 인코딩을 지정합니다.

_encoding 또는 **LANG** 변수를 통해 지정된 인코딩이 없으면 전자 메일의 문자가 올바르게 표시되지 않을 수 있습니다. 올바른 로캘로 **_encoding** 또는 **LANG** 을 설정하십시오.

메서드: 없음

예:

```
<% _encoding = "UTF-8"; %>
```

_additionalHeaders

_additionalHeaders

전자 메일 템플릿에 추가 전자 메일 헤더 특성을 지정합니다.

이 특성에 **HashMap()**를 할당해야 합니다. **HashMap** 에 저장된 이름 및 값은 문자열이어야 합니다.

예: 사용자 지정 헤더 특성 추가

다음 예는 사용자 지정 헤더 특성인 "X-TCCCSWD" 및 "myheader"를 추가하는 방법을 설명합니다.

```
<!-- Define the E-mail Properties --->
<%
_to = "siteadmin@ca.com";
_cc = "" ;
_bcc = "" ;
_subject = _eventContextInformation.getEventName() +" completed";
var additionalHeaders = new java.util.HashMap();
additionalHeaders.put("header_a","1");
additionalHeaders.put("header_b","foo");
_additionalHeaders = additionalHeaders;
%>
```


template

JavaScript 코드 줄(즉, `<% %>` 태그 내 줄)로부터 메시지에 텍스트 문자열을 추가할 수 있게 해 줍니다. 이 문자열은 Identity Manager 암시적 개체의 메서드에 의해 반환된 HTML 태그, 정적 텍스트, 및/또는 변수 값을 포함할 수 있습니다.

참고: 템플릿 개체의 앞에는 밑줄(`_`) 문자가 오지 않습니다.

메서드:

- `add(String)`

Identity Manager 암시적 개체의 메서드에 대한 호출을 포함하여, 이 인수는 문자열로 평가되어야 합니다. 위의 예에서 `_eventContextInformation.getSecondaryObjectName()`을 참조하십시오.

예:

```
<%
var secondaryType = _eventContextInformation.getSecondaryObjectType();
if (secondaryType != "") {
    template.add("In " + secondaryType + ": ");
    template.add("<b> "+_eventContextInformation.getSecondary
                                ObjectName()+" </b><br>");
}
%>
```

_util

유틸리티 개체입니다.

메서드:

- `getNotifiers(String [,String])`

알림 규칙을 기준으로 전자 메일 ID 를 반환합니다.

첫 번째 인수는 다음과 같은 미리 정의된 알림 규칙(인용 부호로 묶임)을 지원합니다.

- "ADMIN". 태스크를 시작한 관리자에게 전자 메일을 보냅니다.
- "USER". 현재 컨텍스트의 사용자에게 전자 메일을 보냅니다.
- "USER_MANAGER". 현재 컨텍스트의 사용자의 매니저에게 전자 메일을 보냅니다.

또한 "Notification Rule"(알림 규칙) API 를 사용하여 만드는 사용자 지정 알림 규칙을 참조할 수도 있습니다. 자세한 내용은 *Programming Guide for Java*(Java 프로그래밍 안내서)를 참조하십시오.

두 번째 인수는 선택 사항입니다. 이 인수를 사용하여 하나 이상의 사용자 정의된 이름/값 쌍을 사용자 지정 알림 규칙에 전달할 수 있습니다. 각 이름/값 쌍은 다음 형식처럼 쉼표로 구분하십시오.
"name1=value1,name2=value2,..."

예:

<%

```
_to = _util.getNotifiers("ADMIN");_cc = "";
```

%>

<%

```
_to = _util.getNotifiers("MYRULE","type=loan,district=3");  
_cc = "";
```

%>

사용자 매니저에게 알림

USER_MANAGER 알림 규칙을 사용하여 원하는 사용자의 매니저에게 전자 메일을 보낼 수 있습니다. Identity Manager 는 사용자 권한 인증을 지원하는 전자 메일 템플릿에 이 규칙을 사용합니다.

참고: USER_MANAGER 알림 규칙은 하나의 사용자를 만들거나 관리하는 이벤트 또는 태스크에만 적용됩니다.

사용자 디렉터리 내에서 여러 다른 방식으로 사용자-매니저 관계가 지정될 수 있으므로 기본 "User Manager Notification Adapter"(사용자 매니저 알림 어댑터)는 getNotifiers() 메서드의 두 번째 매개 변수에 지정된 특성 식을 기준으로 이 관계를 확인합니다.

예:

<%

```
_to = _util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");  
_cc = "";
```

%>

"User Manager Notification Adapter"(사용자 매니저 알림 어댑터)는 두 가지 조회 옵션을 지원합니다.

- `managerattribute = <Manager AttributeName>`- 여기서 User 개체는 사용자 매니저의 DN 또는 UserID 를 나타내는 특성을 유지합니다.
- `commonattribute = <AttributeName>` - 여기서 사용자 및 사용자의 매니저는 "department"와 같은 공용 특성 값을 공유합니다.

이러한 조회 옵션은 Identity Manager 관리 콘솔에서 환경에 대한 "Miscellaneous Properties"(기타 속성)에서 구성합니다.

USER_MANAGER 알림 규칙을 구성하려면:

1. Identity Manager 관리 콘솔에서 "Identity Manager Environments"(Identity Manager 환경)를 선택합니다. 그런 다음 전자 메일 알림을 구성할 환경을 선택하십시오.
2. "Advanced Settings"(고급 설정)>"Miscellaneous Properties"(기타 속성)를 선택합니다.
3. "Miscellaneous Properties"(기타 속성) 페이지에서 사용할 조회 옵션에 대한 구성 단계를 완료합니다.
 - `managerattribute=<매니저 특성 이름>` 조회 옵션을 사용하려면:
 - a. "Property"(속성) 필드에서 `managerattribute` 를 입력합니다.
 - b. "Value"(값) 필드에서 매니저의 DN 또는 사용자 ID 를 저장하는 특성을 입력합니다.
 - c. "추가"를 클릭합니다.
 - d. "저장"을 클릭합니다.
 - `commonattribute=<AttributeName>` 조회 옵션을 사용하려면:
 - a. "Property"(속성) 필드에서 `commonattribute` 를 입력합니다.
 - b. "Value"(값) 필드에서 사용자 및 사용자의 매니저가 모두 가지고 있는 특성을 입력합니다.
 - c. "추가"를 클릭합니다.
 - d. "Property"(속성) 필드에서 다음을 입력합니다.
`ismanagerfilter`

- e. "Value"(값) 필드에서 다음 구분을 사용하는 검색 식을 입력합니다.

<특성> <연산자> <필터>

예: title EQUALS manager

- f. "추가"를 클릭합니다.

- g. "저장"을 클릭합니다.

사용자 지정 어댑터를 작성하고 사용자의 매니저에게 알리는 자체 규칙을 만들 수도 있습니다. *Programming Guide for Java*(Java 프로그래밍 안내서)를 참조하십시오.

_eventContextInformation

이벤트 이름과 승인 상태와 같은 현재 태스크에 의해 생성된 이벤트에 대한 정보를 수록하고 있습니다. 이 정보는 이벤트에 대한 *컨텍스트* 정보라고 불립니다.

_eventContextInformation 개체는 패키지 com.netegrity.imapi 의 ExposedEventContextInformation 클래스로부터 생성됩니다.

이 개체는 "승인됨", "보류", "거부됨" 템플릿을 기준으로 전자 메일 메시지에 사용할 수 있습니다. 이러한 템플릿에 대한 자세한 내용은 [전자 메일 템플릿](#) (페이지 410)을 참조하십시오.

메서드: 다음 메서드는 모두 문자열을 반환합니다.

메서드	설명
getAdminName()	이벤트를 생성한 태스크를 제출한 사람의 이름을 반환합니다. CA CA Identity Manager 5.6 에서 사용되지 않습니다. 다음의 상속된 메서드 중 하나를 사용하십시오. ■ getAdministrator() ■ getAdminFriendlyName()
getApprovalStatus()	이벤트의 승인 상태를 반환합니다. 이러한 값 중 하나: APPROVAL_STATUS_APPROVED APPROVAL_STATUS_REJECTED

메서드	설명
<code>getApprovalTime()</code>	이벤트가 승인된 시간을 반환합니다.
<code>getEventName()</code>	이벤트의 이름을 반환합니다. 이벤트 이름의 목록은 "CA Identity Manager 이벤트"를 참조하십시오.
<code>getOrgName()</code>	태스크가 실행되는 조직의 이름을 반환합니다. CA CA Identity Manager 5.6 에서 사용되지 않습니다. 상속된 메서드 <code>getObjectOrganizationFriendlyName()</code> 를 사용하십시오.
<code>getPassword()</code>	기본 개체의 유형이 USER 인 경우 사용자의 암호를 반환합니다.
<code>getPrimaryObjectTypeName()</code>	기본 개체의 유형을 반환합니다. 반환된 기본 개체 유형: ACCESSROLE ACCESSTASK ADMINROLE ADMINTASK GROUP ORGANIZATION USER

메서드	설명
getPrimaryObjectName()	이벤트의 영향을 받은 기본 개체의 이름을 반환합니다. <i>기본 개체</i>는 이벤트의 직접적인 영향을 받은 개체입니다. <i>보조 개체</i>는 기본 개체(있는 경우)가 마인딩된 개체입니다. 예: ■ CreateUserEvent 의 기본 개체 유형은 USER 입니다. 보조 개체는 사용자가 생성된 개체(즉, ORGANIZATION)입니다. ■ CreateAdminRoleEvent 의 기본 개체 유형은 ADMINROLE 입니다. 이 개체는 다른 개체에 마인딩되지 않으므로 보조 개체가 없습니다. 기본 개체 유형이 USER 인 경우 getPrimaryObjectName()는 John Jones 를 반환할 수 있습니다.
getSecondaryObjectTypeName()	보조 개체가 이벤트의 영향을 받은 경우 개체 유형을 반환합니다. 반환된 보조 개체 유형: ACCESSROLE ACCESSTASK ADMINROLE ADMINTASK GROUP ORGANIZATION USER

메서드	설명
<code>getSecondaryObjectName()</code>	보조 개체가 이벤트의 영향을 받은 경우 개체 이름을 반환합니다. 기본 및 보조 개체에 대한 정보는 <code>getPrimaryObjectName()</code>를 참조하십시오. 보조 개체의 유형이 ORGANIZATION 인 경우 메서드 <code>getSecondaryObjectName()</code>가 HR 을 반환할 수 있습니다.

참고: `_eventContextInformation` 의 메서드는 인터페이스

`ExposedEventContextInformation` 을 통해 제공됩니다.

`ExposedEventContextInformation` 이 핵심 CA CA Identity Manager API 에 있는 메서드를 상속하므로 `_eventContextInformation` 은 위의 표에 있는 메서드와 함께 이러한 메서드를 전자 메일 템플릿으로부터 호출할 수도 있습니다. 이러한 상속된 메서드에 대한 자세한 내용은 [추가 메서드](#) (페이지 431)를 참조하십시오.

예제--"보류" 이벤트에 대한 전자 메일 알림:

```
<%
_cc = "" ;_bcc = "";
_subject = _eventContextInformation.getEventName() +
                                     " Approval Request";
%>
<!-- Start of Body -->
<html>
<body text="Navy">

The following item has been added to your work list for approval:
<br><br><br>
Event: <b><%= _eventContextInformation.getEventName() %></b> <br>
<%= _eventContextInformation.getPrimaryObjectTypeName() %>:
<b><%= _eventContextInformation.getPrimaryObjectName() %></b><br>
In <%= _eventContextInformation.getSecondaryObjectTypeName() %>:
<b><%= _eventContextInformation.getSecondaryObjectName() %></b><br>
</body>
</html>
```

가능한 전자 메일 본문:

보낸 사람: lsmith@security.com [mailto:lsmith@security.com]

받는 사람: vimperioso@security.com

제목: CreateUserEvent Approval Request

The following item has been added to your work list for approval:

Event: **CreateUserEvent**

USER: **Richard Ferrigamo**

In ORGANIZATION: **Mortgages & Loans**

참고: "보낸 사람" 필드의 값은 email.properties 파일에서 파생됩니다. 이 값을 변경하려면 다음 파일을 편집하십시오.

<iam_im.ear>\config\com\netegrity\config\email.properties

여기서 <iam_im.ear>는 응용 프로그램 서버 도메인에서 CA CA Identity Manager 가 설치된 위치입니다. 예:

WebLogic:

<WebLogic_home>\user_projects\<domain>\applications\iam_im.ear

JBoss:

<Identity Manager_home>\jboss-3.2.2\server\default\deploy\iam_im.ear

WebSphere:

<im_admin_tools_dir >\WebSphere-ear\iam_im.ear

앞의 예제에서 이벤트의 영향을 받는 사용자에 대한 추가 정보를 전자 메일에 추가하려면 다음과 유사한 텍스트를 추가하십시오.

```
<% user = _eventContextInformation.getEvent().getUser(); %>
<b>User information:</b><br>
Last Name: <b><%=user.getAttribute("%LAST_NAME%")%></b><br>
First Name: <b><%=user.getAttribute("%FIRST_NAME%")%></b><br>
Full Name: <b><%=user.getAttribute("%FULL_NAME%")%></b><br>
Email: <b><%=user.getAttribute("%EMAIL%")%></b><br>
Organization Membership: <b><%=user.getAttribute("%ORG_MEMBERSHIP%")%></b><br>
```


가능한 전자 메일 본문:

보낸 사람: lsmith@security.com [mailto:lsmith@security.com]

받는 사람: vimperioso@security.com

제목: CreateUserEvent Approval Request

The following item has been added to your work list for approval:

Event: **CreateUserEvent**

USER: **Richard Ferrigamo**

In ORGANIZATION: **Mortgages & Loans**

User information:

Last Name: Ferrigamo

First Name: Richard

Full Name: Richard Ferrigamo

Email: rferrigamo@mybank.org

Organization Membership: **Mortgages & Loans**

_taskContextInformation

태스크 이름, 조직 이름, 구성 요소 이벤트와 같은 현재 태스크에 대한 여러 정보를 수록하고 있습니다. 이 정보는 태스크에 대한 *컨텍스트* 정보라고 불립니다.

이 개체는 "완료함" 템플릿에 기초하여 전자 메일 메시지에 사용할 수 있습니다. 이 템플릿에 대한 자세한 내용은 [전자 메일 템플릿](#) (페이지 410)을 참조하십시오.

메서드: Java Vector 를 반환하는 `getExposedEventContexts()` 메서드를 제외하고, 아래 모든 메서드는 문자열을 반환합니다.

메서드	설명
<code>getAdminName()</code>	태스크를 제출하는 사람의 이름을 반환합니다. Identity Manager 5.6 에서 사용되지 않습니다. 다음의 상속된 메서드 중 하나를 사용하십시오. ■ <code>getAdministrator()</code> ■ <code>getAdminFriendlyName()</code>

메서드	설명
<code>getExposedEventContexts()</code>	태스크와 관련된 모든 이벤트의 Java <code>Vector</code> 를 반환합니다. <code>Vector</code> 의 각 개체는 이벤트 컨텍스트 개체입니다. 지정된 이벤트 개체에 대한 컨텍스트 정보를 검색하기 위해 <code>_eventContextInformation</code> 에 나열된 메서드를 사용할 수 있습니다. 반환 개체는 표준 Java <code>Vector</code> 개체입니다. <code>Vector</code> 개체의 메서드(예: <code>get()</code> 및 <code>size()</code>)를 사용하여 <code>Vector</code> 에서 요소를 관리할 수 있습니다.
<code>getOrgName()</code>	태스크가 실행되는 조직의 이름을 반환합니다. Identity Manager 5.6 에서 사용되지 않습니다. 상속된 메서드 <code>getObjectOrganizationFriendlyName()</code>를 사용하십시오.
<code>getTaskName()</code>	실행 중인 태스크의 이름을 반환합니다. Identity Manager 5.6 에서 사용되지 않습니다. 다음의 상속된 메서드 중 하나를 사용하십시오. ■ <code>getAdminTask()</code> ■ <code>getTaskFriendlyName()</code>

참고: `_taskContextInformation` 의 메서드는 인터페이스 `ExposedTaskContextInformation` 을 통해 제공됩니다.

`ExposedTaskContextInformation` 이 핵심 Identity Manager API 에 있는 메서드를 상속하므로 `_taskContextInformation` 은 위의 표에 있는 메서드와 함께 이러한 메서드를 전자 메일 템플릿으로부터 호출할 수도 있습니다. 이러한 상속된 메서드에 대한 자세한 내용은 [추가 메서드](#) (페이지 431)를 참조하십시오.

예제--암호 변경을 위한 전자 메일 알림 템플릿의 본문:

```
<%
var imsEventContexts
=
    _taskContextInformation.getExposedEventContexts();
if(imsEventContexts != null)
{
    for(var i=0;i<imsEventContexts.size();i++)
    {
        var eventContext = imsEventContexts.get(i);
        template.add("Hi "+
eventContext.getPrimaryObjectName()
            + ",");
        template.add("<br>Your new password is: <b>" +
            eventContext.getPassword());<br>");
        template.add("<hr>");
    }
}
%>
```

가능한 전자 메일 본문:

Hi Victor Imperioso,
Your new password is: LFH7F1226

추가 메서드

`_taskContextInformation` 및 `_eventContextInformation`의 메서드는 각각 Identity Manager 개체 `ExposedTaskContextInformation` 및 `ExposedEventContextInformation`을 통해 제공됩니다.

이러한 개체는 핵심 Identity Manager API의 메서드를 상속합니다. 결과적으로, 상속된 메서드는 `_taskContextInformation` 및 `_eventContextInformation`에도 사용할 수 있습니다.

`TaskInfo` 개체에서 상속된 다음 메서드는 특히 전자 메일 템플릿에 유용합니다.

- `getAdministrator()`. 현재 태스크를 실행 중인 관리자에 대한 `User` 개체를 검색합니다.
- `getAdminTask()`. 현재 태스크에 대한 `AdminTask` 개체를 검색합니다.

이러한 검색된 개체는 관리자 및 태스크 관련 정보를 전자 메일에 삽입할 수 있게 해 줍니다. 예:

```
<!-- Define the E-mail Properties --->

<%
    _cc = "" ;
    _bcc = "" ;
    _subject = _eventContextInformation.getEventName() +
                                   " Approval Request";
%>

<!-- Start of Body --->
<html>
<body text="Navy">

The following item has been added to your work list for approval:<br>
<br>
User <b><%= _eventContextInformation.getAdministrator().
    getAttribute(Packages.com.netegrity.llsdk6.imsapi.
        managedobject.User.PROPERTY_FRIENDLY_NAME)%> </b>
from department <b><%= _eventContextInformation.
    getAdministrator().getOrg(null).getFriendlyName()
    %></b> initiated task <b><%= _eventContextInformation.
    getAdminTask().getFriendlyName() %></b>at
<b><%=
    _eventContextInformation.getSessionCreateTime() %></b>
<br><br>
<font color="green">Details: </font><b><%=_eventContextInformation.
    getEventName()%></b><br>
<font color="green"><%=_eventContextInformation.
    getPrimaryObjectTypeName()%>:</font>
<b><%=_eventContextInformation.getPrimaryObjectName()%></b>
                                   was modified
<br>
<font color="green">Updated Attributes:</font>
<table border="1">
<tr>
    <td><b>Name</b></td>
    <td><b>Value</b></td>
</tr>
```

```

<%
    var event = _eventContextInformation.getEvent();
    if(event instanceof Packages.com.netegrity.imapi.UserEvent) {
        var user = event.getUser();
        var attributes = user.getAttributes().keys();
        while(attributes.hasMoreElements()) {
            var attr = attributes.nextElement();
            var value = user.getAttribute(attr);
            if(user.hasAttributeChanged(attr)) {
                template.add("<tr><td>" + attr + "</td>");
                template.add("<td>" + value + "</td></tr>");
            }
        }
    }
%>
</table>
<br>
</body>
</html>

```

가능한 전자 메일 본문:

The following item has been added to your work list for approval:

User **Robert Jenkins** from department **HR** initiated task **Modify User** at **3:17 pm**

Details: **ModifyUserEvent**

User: **John Jones** was modified

Updated Attributes:

Name	Value
email	jjones@mycorp.com
phone	781 555 1234

"Email Template"(전자 메일 템플릿) API 에서 사용할 수 있는 상속된 메서드에 대한 자세한 내용은 Identity Manager Javadoc 에서 ExposedTaskContextInformation 및 ExposedEventContextInformation 개체를 참조하십시오.

Java 표준 출력 스트림

전자 메일 메시지는 또한 JavaScript 태그(<% %>) 내에서 Java 표준 출력 스트림을 호출할 수 있습니다. 예를 들어, 다음 호출은 서버 콘솔로 메시지 Done 을 보냅니다.

```
<%  
...      // JavaScript processing  
out.println("Done.");  
%>
```

Javadoc Reference

ExposedTaskContextInformation 및 ExposedEventContextInformation 개체와 이러한 개체가 핵심 Identity Manager API 에서 상속하는 메서드에 대한 자세한 내용은 Identity Manager Javadoc 을 참조하십시오.

Javadoc 페이지는 HTML 버전의 Java 용 프로그래밍 안내서에 통합되어 있으며, 이 안내서는 Identity Manager 북셀프에서 제공됩니다.

전자 메일 템플릿 개발

CA CA Identity Manager 는 전자 메일을 보내기 전에 응용 프로그램 서버 내의 다음과 같은 루트 위치에서 전자 메일을 생성하기 위한 템플릿을 검색합니다.

iam_im.ear\custom\emailTemplates

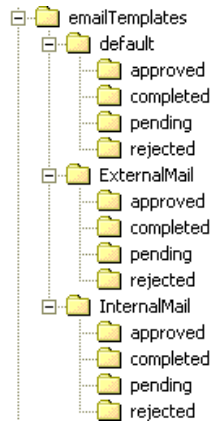
이 루트에 배포된 전자 메일 템플릿은 동일한 디렉터리 구조를 갖는 템플릿 집합에 포함되어 있습니다. 즉, 각 집합에는 승인됨, 완료됨, 보류, 거부됨 디렉터리가 있습니다.

템플릿 집합

emailTemplates 아래에 여러 전자 메일 템플릿 집합을 배포할 수 있습니다. 예를 들어, 설치 중에 다음과 같은 전자 메일 템플릿 집합이 iam_im.ear\custom\emailTemplates 에 생성됩니다.

default\approved
default\completed
default\pending
default\rejected

기본 전자 메일 템플릿 집합에는 [전자 메일 템플릿](#) (페이지 410)에서 설명한 설치된 템플릿이 포함되어 있습니다. 기본 집합 내에 사용자 지정 템플릿을 추가할 수 있습니다. 또한 기본 집합과 동일한 수준에 정의하는 디렉터리 구조에 다른 전자 메일 템플릿 집합을 배포할 수도 있습니다. 예를 들어, iam_im.ear\custom 은 다음과 같은 배포된 전자 메일 템플릿을 포함할 수 있습니다.



참고: CA CA Identity Manager 가 템플릿 집합 내에서 특정 전자 메일을 선택하는 방법에 대한 자세한 내용은 [템플릿 디렉터리](#) (페이지 412)를 참조하십시오.

환경에 대한 템플릿 집합을 지정하는 방법

Identity Manager 환경에 대한 전자 메일을 구성할 때 해당 환경에 사용할 전자 메일 템플릿 집합을 지정합니다. Identity Manager 환경에 대해 전자 메일을 구성하는 방법에 대한 자세한 내용은 *CA Identity Manager Configuration Guide*(CA Identity Manager 구성 안내서)를 참조하십시오.

템플릿 이름

사용자 지정 템플릿 집합의 디렉터리는 기본 템플릿 집합에 설치된 것과 동일한 이름을 사용하는 기본 템플릿을 포함해야 합니다. 기본 이름은 [전자 메일 템플릿](#) (페이지 410)에 나열되어 있습니다. Identity Manager 는 실행 중인 태스크 또는 이벤트와 일치하는 이름의 다른 템플릿을 찾지 못하면 이 기본 템플릿을 사용합니다.

선택적으로, 특정 템플릿으로부터 전자 메일을 생성하려면 템플릿 집합의 하나 이상의 디렉터리에 템플릿을 추가할 수 있습니다. 방법:

- 전자 메일이 생성되는 태스크 또는 이벤트와 동일한 이름을 템플릿에 할당합니다.
- 전자 메일이 생성될 태스크 또는 이벤트 상태와 관련된 디렉터리에 템플릿을 넣습니다.

예를 들어, `CreateUserEvent` 가 거부되었을 때 특정 템플릿에서 전자 메일이 생성되도록 하려면 `CreateUserEvent.tmpl` 이란 이름의 템플릿을 환경의 템플릿 집합에 있는 거부됨 디렉터리에 넣으십시오.

제 14 장: 보고

이 섹션은 다음 항목을 포함하고 있습니다.

[구성 개요](#) (페이지 437)

[보고서 프로세스](#) (페이지 439)

[스냅샷 보고서를 실행하는 방법](#) (페이지 440)

[비스냅샷 보고서를 실행하는 방법](#) (페이지 457)

[보고 옵션 설정](#) (페이지 463)

[사용자 지정 스냅샷 보고서를 만들고 실행하는 방법](#) (페이지 464)

[사용자, 계정 및 역할 동기화](#) (페이지 479)

[문제 해결](#) (페이지 487)

구성 개요

CA Identity Manager 에서 다음 두 가지 유형의 보고서를 실행할 수 있습니다.

스냅샷 보고서

CA Identity Manager 개체 저장소 및 사용자 저장소의 정보가 포함된 스냅샷 데이터베이스의 데이터를 포함합니다. 스냅샷 보고서의 예로 사용자 프로필 보고서가 있습니다. 포함할 정보를 지정하는 스냅샷 정의를 사용하여 스냅샷 데이터베이스에 추가되는 데이터를 정의하십시오.

비 스냅샷 보고서

감사 데이터베이스와 같은 기타 데이터 원본의 데이터를 포함합니다. 예를 들어, CA Identity Manager 는 기본 감사 보고서를 포함합니다. 이러한 보고서는 사용자 콘솔에서 이름에 "Audit - " 접두어를 가집니다. 기본적으로 CA Identity Manager 는 감사 보고서만 포함하지만 워크플로 또는 태스크 지속 데이터베이스와 같은 데이터 원본의 데이터를 포함하는 사용자 지정 보고서를 만들 수 있습니다.

CA Identity Manager 의 각 보고서는 실행하려면 초기 구성이 필요합니다. 구성 단계는 실행할 보고서의 유형에 따라 달라집니다.

다음 단계는 이 단원에 포함된 절차를 요약합니다.

스냅샷 보고서의 경우

1. 스냅샷 정의 파일을 만들어 스냅샷 데이터베이스에 추가되는 데이터를 정의합니다.
2. 보고서에 대한 스냅샷 데이터를 캡처합니다.
3. 사용자 콘솔에서 보고서 태스크를 수정하고 다음 작업을 수행합니다.
 - a. 스냅샷 정의를 태스크와 연결합니다.
 - b. rptParamConn 연결 개체를 태스크에 추가합니다.
4. 다음 방법 중 하나를 사용하여 보고서를 요청합니다.
 - 즉시 보고서 실행
 - 보고서 예약
5. 사용자 콘솔에서 보고서를 봅니다.

비 스냅샷 보고서의 경우:

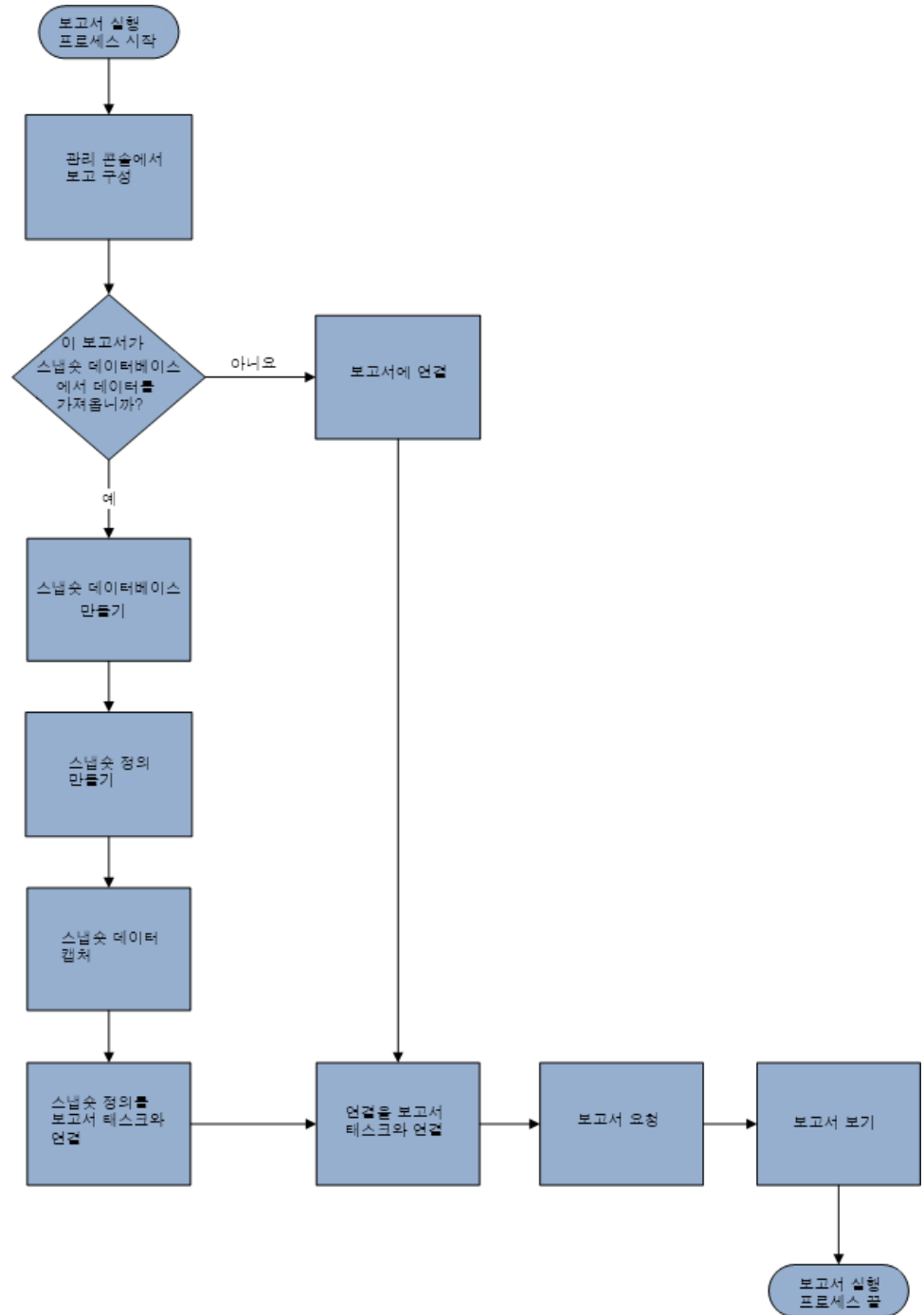
1. 보고서에 대한 데이터 원본 정보로 연결 개체를 만듭니다.
2. CA Identity Manager 에서 보고서 태스크를 수정하고 연결 개체를 태스크에 추가합니다.
3. 다음 방법 중 하나를 사용하여 보고서를 요청합니다.
 - 즉시 보고서 실행
 - 보고서 예약
4. 사용자 콘솔에서 보고서를 봅니다.

보고서에 대한 초기 구성이 완료되면 CA Identity Manager 내에서 보고서를 요청할 수 있습니다. 즉시 보고서를 실행하거나 나중에 실행하도록 보고서를 예약할 수 있습니다. 또한 CA Identity Manager 내에서 보고서에 대한 되풀이 일정을 만들 수 있습니다.

마지막으로, 사용자 콘솔에서 보고서를 보거나, 보고서를 다양한 형식으로 내보낼 수 있습니다.

보고서 프로세스

다음 그림은 보고서를 실행하고 보기 위해 필요한 프로세스를 설명합니다.



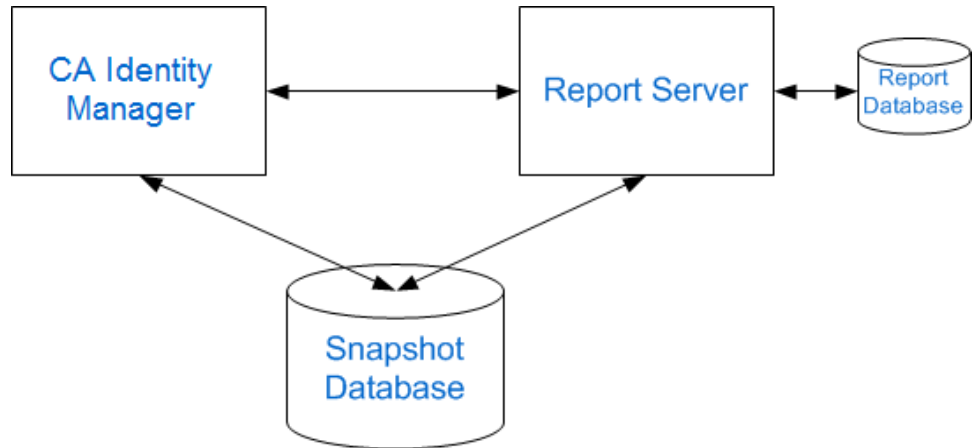
스냅샷 보고서를 실행하는 방법

CA Identity Manager 보고서를 사용하여 CA Identity Manager 환경의 현재 상태를 확인할 수 있습니다. 이 정보를 사용하여 내부 비즈니스 정책이나 외부 규제에 대한 컴플라이언스를 유지할 수 있습니다.

CA Identity Manager 환경의 개체 간 관계를 설명하는 관리 데이터에서 CA Identity Manager 보고서를 생성합니다. 관리 데이터 예는 다음과 같습니다.

- 사용자의 프로필 특성
- 특정 태스크를 포함하는 역할 목록
- 역할 또는 그룹 구성원
- 역할을 구성하는 규칙

CA Identity Manager 에서 보고 설정을 위해서는 다음과 같은 세 가지 주요 구성 요소가 필요합니다.



참고: 이 그림의 스냅샷 데이터베이스는 또한 감사 데이터베이스 또는 워크플로 데이터베이스도 될 수 있습니다.

보고서 서버

또한 CA Business Intelligence 로 알려진 이 서버는 CA Identity Manager 및 스냅샷 데이터베이스와 직접 통신하여 보고서를 생성합니다.

보고서 데이터베이스

CA 보고서 서버(Business Objects)가 자체 데이터를 저장하는 데이터베이스입니다.

CA Identity Manager

CA Identity Manager 는 CA Identity Manager 개체 데이터를 보고서 데이터베이스로 내보내도록 허용합니다.

스냅샷 데이터베이스

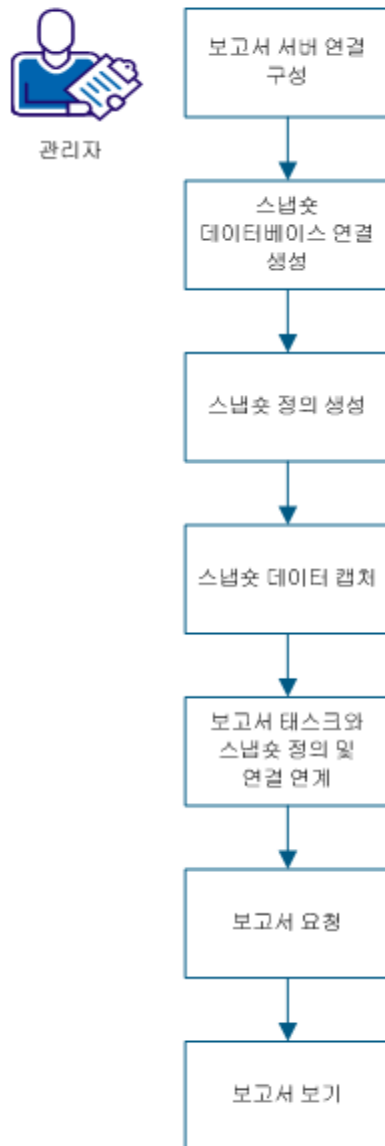
CA Identity Manager 에서 개체의 스냅샷 데이터를 수록한 별도 데이터베이스입니다.

중요! 보고서 서버는 Business Objects Enterprise 를 사용합니다. 환경에 보고서 서버가 이미 있고 CA Identity Manager 와 함께 이 서버를 사용하려는 경우, CA Identity Manager 가 요구하는 최소 버전은 CA Business Intelligence 3.2 SP5 입니다.

스냅샷 보고서는 CA Identity Manager 개체 저장소 및 CA Identity Manager 사용자 저장소의 정보가 포함된 스냅샷 데이터베이스의 데이터를 포함합니다. 스냅샷 보고서의 예로 사용자 프로필 보고서가 있습니다. 스냅샷 데이터베이스에 추가되는 스냅샷 데이터를 정의하고, 스냅샷 정의를 사용하여 포함할 정의를 지정합니다.

다음 그림은 스냅샷 보고서를 실행하기 위한 프로세스를 설명합니다.

스냅샷 보고서 실행 방법



스냅샷 보고서를 실행하려면 다음 단계를 수행하십시오.

1. [보고서 서버 연결을 구성합니다](#) (페이지 458).
2. 스냅샷 데이터베이스 연결을 만듭니다.
3. 스냅샷 정의를 만듭니다.
4. 스냅샷 데이터를 캡처합니다.
5. 스냅샷 정의와 연결을 보고서 태스크와 연결합니다.

6. 보고서를 요청합니다.
7. [보고서를 봅니다](#) (페이지 462).

보고서 서버 연결 구성

CA Identity Manager 와 보고서 서버 간의 연결을 구성합니다.

참고: 보고와 관련된 모든 시스템은 동일한 시간대 및 시간으로 설정하는 것이 좋습니다.

보고 기능을 구성하려면

1. 사용자 콘솔에서 "태스크", "시스템", "보고", "보고서 서버 연결"을 차례로 클릭합니다.
2. 보고서 서버 설정을 입력합니다. 다음에 주의하십시오.
 - 호스트 이름 및 포트 - 보고서 서버가 설치되어 있는 시스템의 호스트 이름과 HTTP URL 포트 번호입니다.
 - 보고서 폴더 이름 - 기본 CA Identity Manager 보고서의 위치입니다.
 - 사용자 ID - 보고서 서버용으로 만들어진 사용자입니다.
 - 암호 - 보고서 서버에서 만들어진 사용자의 암호입니다.
 - 보안 연결 - CA Identity Manager 와 보고서 서버 간에 SSL(Secure Sockets Layer) 연결을 사용하려면 이 확인란을 선택합니다.

참고: "보안 연결" 확인란을 선택하기 전에 BOServer 에서 인증서를 설치했는지 확인하십시오. SSL 구성에 대한 자세한 내용은 *설치 안내서*에서 "보고서 서버 설치" 단원을 참조하십시오.

 - 웹 서버 - Tomcat 에 대해 비 IIS 를 설정합니다.
3. "연결 테스트"를 클릭하여 연결을 확인합니다.
4. 제출을 클릭합니다.

보고 연결이 설정됩니다.

스냅샷 데이터베이스 연결 만들기

CA Identity Manager 에서 스냅샷 데이터를 내보낼 위치를 알고 있어야 합니다. CA Identity Manager 에서 스냅샷 데이터베이스로의 데이터베이스 연결을 만드십시오.

스냅샷 데이터베이스 연결을 만들려면

1. 사용자 콘솔에서 "태스크", "보고서", "스냅샷 태스크", "스냅샷 데이터베이스 연결 관리", "스냅샷 데이터베이스 연결 만들기"를 클릭합니다.
2. 필요한 필드를 모두 완료하여 새 스냅샷 데이터베이스 연결을 만듭니다.
3. 제출을 클릭합니다.
새 스냅샷 데이터베이스 연결이 만들어집니다.

스냅샷 정의 만들기

스냅샷은 CA Identity Manager 에서 지정된 시간의 개체 상태를 반영합니다. 이 스냅샷 데이터를 사용하여 보고서를 작성할 수 있습니다. CA Identity Manager 개체 데이터를 캡처하려면 데이터를 스냅샷 데이터베이스로 내보내는 스냅샷 정의를 만듭니다. 스냅샷 정의를 사용하여 사용자, 끝점, 관리자 역할, 프로비저닝 역할, 그룹 및 조직을 로드하기 위한 규칙을 정의합니다.

다음 단계를 수행하십시오.

1. 사용자 콘솔에서 "태스크", "보고서", "스냅샷 태스크", "스냅샷 정의 관리", "스냅샷 정의 만들기"로 이동합니다.
2. 스냅샷 유형의 개체를 만들거나 복사합니다.
3. 확인을 클릭합니다.
4. "프로필" 탭에서 다음 필드를 작성하여 스냅샷 정의 프로필을 만듭니다.

스냅샷 정의 이름

스냅샷 정의에 사용할 고유 이름을 식별합니다.

스냅샷 정의 설명

스냅샷을 설명할 추가 정보를 표시합니다.

사용

CA Identity Manager 가 예약된 시간에 현재 스냅샷 정의를 기준으로 스냅샷을 만들도록 지정합니다.

참고: 이 옵션을 선택하지 않으면 예약된 시간에 스냅샷 정의가 캡처되지 않습니다. 또한 "스냅샷 데이터 캡처" 화면에 스냅샷 정의가 표시되지 않습니다.

보존되는 스냅샷 수

스냅샷 데이터베이스에 보존되는 성공한 스냅샷 수를 지정합니다.

참고: 이 필드의 값을 지정하지 않으면 CA Identity Manager 가 제한 없이 스냅샷을 저장합니다.

5. "스냅샷 정책" 탭에서 내보낼 정책과 관련된 개체를 선택합니다.
6. "역할 설정" 탭에서 내보낼 스냅샷의 역할 구성 요소를 하나 이상 선택하고 사용 가능한 특성도 선택합니다.

참고: "스냅샷 정책" 탭에서 "액세스 역할" "관리자 역할" 또는 "프로비저닝 역할" 개체를 선택하는 경우 "역할 설정" 탭에서 특성을 선택하십시오.

7. "사용자 특성 정보" 탭에서 내보낼 스냅샷에 대한 하나 이상의 사용자 특성을 선택합니다.

참고: "스냅샷 정책" 탭에서 "사용자" 개체만 선택하는 경우 기본적으로 모든 사용자 특성 관련 데이터가 내보내기됩니다.

8. "끝점 계정 특성" 탭에서 끝점 유형에 대한 하나 이상의 계정 특성을 선택합니다.

참고: 선택한 끝점 유형의 경우, 기본적으로 끝점 계정 특성과 관련된 모든 데이터가 내보내기됩니다. 특정 특성과 관련된 데이터를 캡처하려면 적절한 특성을 선택하십시오. 끝점 유형에 대해 내보내기 위해 필요한 특성을 선택하는 방법에 대한 자세한 내용은 [구성 안내서](#)에서 "기본 보고서" 단원을 참조하십시오.

9. (선택 사항) 전역 사용자가 없는 끝점 계정을 프로비저닝 서버에 포함하려면 "고아 계정 내보내기" 확인란을 선택합니다.

참고: 비표준, 비표준 추세 및 고아 계정 보고서에 대한 보고서 데이터를 내보내려면 "exceptionAccount" 특성과 "고아 계정 내보내기" 확인란을 선택합니다.

10. 제출을 클릭합니다.

CA Identity Manager 가 스냅샷 정의에서 지정한 개체의 스냅샷을 만들도록 구성됩니다.

이제 스냅샷 정의를 만들었으므로 스냅샷 데이터를 즉시 캡처하거나 스냅샷 데이터를 나중에 내보내도록 예약할 수 있습니다. 추가 정보는 스냅샷 데이터 캡처 항목에 나와 있습니다.

추가 정보:

[되풀이 탭](#) (페이지 449)

예제: 사용자 권한 데이터에 대한 스냅샷 정의 만들기

다음 예제에서는 사용자 권한 보고서에 대한 스냅샷 정의를 만드는 프로세스를 설명합니다.

1. 사용자 콘솔에서 "태스크", "보고서", "스냅샷 태스크", "스냅샷 정의 관리", "스냅샷 정의 만들기"로 이동합니다.
2. "스냅샷 유형 유형의 새 개체 만들기"를 선택합니다.
3. 스냅샷 정의 이름, 설명 및 보존되는 스냅샷 수를 입력합니다.
4. "스냅샷 정책 정의" 탭에서 "추가"를 클릭합니다.

드롭다운에서 사용자를 선택하고 "모두"를 선택합니다. 마찬가지로 다음 화면에 표시된 대로 끝점, 프로비저닝 역할, 관리자 역할, 액세스 역할, 조직 및 그룹을 추가합니다.

내보낼 개체	
액세스 역할	
(모두)	
관리자 역할	
(모두)	
끝점	
(모두)	
그룹	
(모두)	
조직	
(모두)	
프로비저닝 역할	
(모두)	
사용자	
(모두)	

5. "역할 설정" 탭에서 모든 사용자 역할 확인란을 선택합니다.
6. "사용자 특성" 탭의 "사용 가능한 값" 목록에서 필수 특성을 선택하여 "현재 값" 목록으로 이동합니다.
7. 제출을 클릭합니다.

스냅샷 관리

CA Identity Manager 를 사용하여 스냅샷 정의를 보고 수정 및 삭제할 수 있습니다. 스냅샷 정의를 보거나 수정할 때 "프로필" 및 "유지 관리" 탭이 표시됩니다. "유지 관리" 탭은 스냅샷을 한 번 캡처한 후에만 표시됩니다. 스냅샷 상태가 실패인 경우에도 "유지 관리" 탭에서 스냅샷을 삭제할 수 있습니다.

스냅샷 정의를 보거나 수정 또는 삭제하려면 "보고서", "스냅샷 태스크", "스냅샷 정의 관리"로 이동하여 실행할 태스크를 클릭하십시오.

참고: 데이터를 스냅샷 데이터베이스로 내보내기 위해 스냅샷 정의를 사용하고 있는 경우에는 해당 스냅샷 정의를 삭제할 수 없습니다. 사용되는 스냅샷 정의를 삭제하면 스냅샷 데이터베이스로 데이터를 내보내는 작업이 중지되지만 스냅샷 정의는 계속 사용할 수 있습니다.

스냅샷 데이터 캡처

스냅샷 데이터를 즉시 캡처하거나 스냅샷 데이터 내보내기를 나중에 또는 되풀이 일정에 따라 예약하려면 "스냅샷 데이터 캡처" 태스크를 실행하십시오. 이 태스크는 스냅샷 정의에 의해 정의된 데이터를 스냅샷 데이터베이스로 즉시 내보냅니다.

중요! 많은 양의 데이터를 내보내는 경우 스냅샷 데이터를 내보내는 데 시간이 오래 걸릴 수 있습니다. 많은 양의 데이터를 내보낼 때는 스냅샷을 예약하는 것이 좋습니다.

스냅샷 데이터를 캡처하려면

1. 사용자 콘솔에서 "태스크", "보고서", "스냅샷 태스크", "스냅샷 데이터 캡처"로 이동합니다.
2. 데이터 내보내기를 즉시 실행하려면 "지금 실행"을 선택하고 데이터 내보내기를 나중에 또는 되풀이 일정에 따라 실행하려면 [새 작업 예약](#) (페이지 449)을 선택합니다.
3. "다음"을 클릭합니다.
4. 스냅샷 정의를 선택합니다.

5. 제출을 클릭합니다.

스냅샷 데이터가 스냅샷 데이터베이스로 내보내집니다.

참고: "스냅샷 데이터 캡처" 태스크가 시간이 오래 걸리는 것 같으면 "시스템" 탭으로 이동하고 "제출한 태스크 보기"를 클릭하여 태스크의 진행 상태를 확인할 수 있습니다.

되풀이 탭

되풀이 탭을 사용하여 작업을 예약할 수 있습니다. 이 탭에는 다음과 같은 필드가 있습니다.

지금 실행

작업을 즉시 실행합니다.

새 작업 예약

새 작업을 예약합니다.

기존 작업 수정

기존 작업을 수정한다는 것을 지정합니다.

참고: 이 필드는 이 태스크에 대해 작업이 이미 예약된 경우에만 표시됩니다.

작업 이름

만들거나 수정할 작업의 이름을 지정합니다.

시간대

서버 시간대를 지정합니다.

참고: 사용자의 시간대가 서버의 시간대와 다른 경우 새 작업을 예약할 때 사용자의 시간대 또는 서버의 시간대를 선택할 수 있도록 드롭다운 상자가 표시됩니다. 기존 작업을 수정할 때는 시간대를 변경할 수 없습니다.

일별 일정

특정 기간(일)마다 작업이 실행되도록 지정합니다.

매(일 수)

작업 실행 간의 일 수를 정의합니다.

주별 일정

일주일 중 특정 요일 및 시간에 작업이 실행되도록 지정합니다.

요일

작업이 실행되는 요일을 지정합니다.

월별 일정

월별로 작업이 실행될 요일 또는 날짜를 지정합니다.

연간 일정

연별로 작업이 실행될 요일 또는 날짜를 지정합니다.

고급 일정

추가 예약 정보를 지정합니다.

Cron 식

이 필드 작성에 대한 내용은 다음 웹 페이지를 참조하십시오.

<http://quartz-scheduler.org/api/2.1.0/org/quartz/CronExpression.html>

실행 시간

작업이 실행되는 시간을 24 시간 형식으로 지정합니다. 예: 14:15

스냅샷 정의를 보고서 태스크와 연결

CA Identity Manager 에서 보고서를 실행할 때 사용할 스냅샷 정의를 인식하도록 스냅샷 정의를 보고서 태스크에 할당하십시오. 또한 CA Identity Manager 보고서에 대한 정보는 여러 출처로부터 제공될 수 있으며 각 보고서는 보고서에서 볼 정보에 따라 특정 데이터 원본과 연결해야 합니다.

스냅샷 정의와 연결을 보고서 태스크와 연결하려면

1. 사용자 콘솔에서 "태스크", "역할 및 태스크", "관리자 태스크", "관리자 태스크 수정"으로 이동합니다.
2. 스냅샷 정의를 연결할 보고서 태스크를 검색합니다.
3. "탭" 탭으로 이동하고 "스냅샷 정의 연결" 탭 옆에 있는 "편집" 단추를 클릭합니다.
4. "추가"를 클릭합니다.

5. 보고서 태스크와 연결할 스냅샷 정의를 검색하고 "선택"을 클릭합니다.
스냅샷 정의를 보고서 태스크와 연결할 때 다음 사항에 주의하십시오.
 - 보고서는 하나 이상의 스냅샷 정의와 연결할 수 있습니다.
 - 스냅샷 정의는 둘 이상의 보고서와 연결될 수 있습니다.
 - 단일 보고서 태스크와 연결된 여러 스냅샷은 동일한 되풀이 시간을 가지면 안 됩니다.
6. 확인을 클릭합니다.
7. "검색" 탭으로 이동하고 "찾아보기"를 클릭하여 검색 화면을 찾습니다.
8. 보고서 태스크의 검색 화면을 편집하고 "보고서용 연결 개체" 아래에서 rptParamConn 을 선택합니다.
9. 확인을 클릭합니다.
10. "선택"을 클릭합니다.
11. 제출을 클릭합니다.

끝점 계정을 계정 템플릿과 동기화

이 태스크는 관련 계정 템플릿 수정 후 끝점 계정을 동기화합니다. 예를 들어 Active Directory 계정에는 그룹이 없지만 관련 계정 템플릿은 그룹을 포함하도록 정의되어 있을 수 있습니다.

다음 단계를 수행하십시오.

1. 사용자 콘솔에 로그인합니다.
2. "태스크", "끝점", "끝점 관리", "끝점 계정 동기화 검사"를 차례로 선택합니다.
3. 끝점을 선택합니다.
해당 끝점의 계정, 관련 계정 템플릿, 동기화되지 않은 특성 등을 보여주는 화면이 나타납니다.
4. "동기화"를 클릭하여 해당 계정의 특성을 계정 템플릿에 정의된 것과 일치하도록 만듭니다.
계정 템플릿의 변경 내용은 다음과 같이 기존 계정에 영향을 줍니다.
 - 기능 특성 값을 변경하면 해당 계정 특성이 업데이트되어 계정 템플릿 특성 값과 동기화됩니다. 약한 동기화와 강력한 동기화에 대한 설명을 참조하십시오.

- 특정 계정 특성은 계정 템플릿 변경 사항에서 업데이트되지 않으므로 커넥터에 의해 지정됩니다. 예를 들면 계정을 만드는 동안 끝점 유형만 설정할 수 있도록 허용하는 특정 특성, 암호 특성 등입니다.

관리자 태스크 예제

관리자 태스크를 만드는 경우 다음을 비롯하여 태스크 화면의 콘텐츠와 레이아웃을 정의합니다.

- 태스크 이름
- 태스크가 나타나는 범주
- 태스크에 사용할 탭 및 필드와 필드 표시 속성
- 관리자가 검색 쿼리에 사용할 수 있는 필드 및 검색 결과에 표시되는 필드

태스크의 요소를 이해하려면 사용자 수정 태스크를 확인합니다. 이 경우 "사용자"는 범주, "사용자 관리"는 하위 범주, "사용자 수정"은 태스크입니다. 태스크를 만들 때 범주와 태스크 이름을 만듭니다.



"사용자 수정"을 선택하면 검색 화면이 나타납니다. *검색 화면*에서는 보거나 수정할 개체를 찾는 데 사용할 수 있는 옵션을 제공합니다. 각 옵션을 *필터*라고 하며, 검색에서 찾는 개체를 제한합니다.

검색 화면에서 데이터를 입력하면 탭이 있는 화면이 나타납니다. 예를 들어, 다음 그림에서는 "사용자 수정" 태스크에 대한 탭을 보여 줍니다. "프로필" 탭이 첫 번째로 나타나 사용자 특성이 표시되고, 나머지 탭은 사용자의 역할 및 그룹 권한이 표시됩니다.

만든 태스크에 대해 포함할 탭을 결정하고 탭 순서와 콘텐츠를 지정합니다.

예를 들어, "사용자 수정" 태스크를 템플릿으로 사용하여 다음을 변경한 "계약자 수정" 태스크를 만들 수 있습니다.

- 프로필 탭의 필드
- 작업에 포함할 탭 및 해당 콘텐츠
- 태스크가 나타나는 범주

새 범주인 계약자 아래에 이 태스크를 만들 수도 있습니다.

"계약자 수정" 태스크에는 "사용자 수정" 태스크의 "프로필" 탭에 있는 필드 중 일부와 계약 시작 날짜, 계약자 회사 등의 다른 필드가 포함되어 있습니다. 관리자는 계약자 이름, 회사 및 시작 날짜를 기준으로 계약자를 검색할 수 있습니다.

계약자 수정: jhansen

프로필	그룹	계약자 역할
사용자 ID jhansen		
사용 ☒		
이름	Julia	
성	Hansen	
전자 메일	jhansen@wxyz.com	
시작 날짜	2008. 5. 11 	
회사		

새 작업에는 또한 계약자의 역할을 추가할 수 있는 "계약자 역할" 탭이 포함되어 있습니다.

보고서 요청

보고서를 보려면 보고서 관리 권한이 있는 사용자에게 보고서를 요청하십시오. 승인이 필요한 이유는 일부 보고서를 실행하는 데 오랜 시간이 걸리거나 상당한 시스템 리소스가 소비될 수 있기 때문입니다. 보고서 요청에 승인이 필요한 경우 시스템이 전자 메일 알림을 보냅니다.

다음 단계를 수행하십시오.

1. 보고서 태스크 사용자 권한을 사용하여 사용자 콘솔에 로그인합니다.
2. "태스크", "보고서", "보고 태스크", "보고서 요청"을 선택합니다.
보고서의 목록이 나타납니다.
3. 요청할 보고서를 선택합니다.
매개 변수 화면이 나타납니다.

필요한 매개 변수 정보를 제공합니다.

참고: 스냅샷 보고서를 실행 중이고 이 보고서에 사용할 수 있는 스냅샷이 없으면 먼저 스냅샷을 캡처해야 합니다.

- 일부 보고서에는 특정 시점의 시스템 상태가 표시됩니다. 이러한 유형의 보고서를 요청하는 경우에는 보려는 보고서 데이터의 시점을 선택합니다. 이 시점을 스냅샷이라고 합니다.

참고: 선택할 수 있는 스냅샷 날짜 및 시간은 미리 결정되어 있습니다. 대개 시스템 관리자나 보고서 관리 권한이 있는 다른 사용자가 스냅샷을 구성합니다. 요청할 보고서에 사용할 수 있는 스냅샷이 없으면 시스템 관리자에게 문의하십시오.

- 일부 보고서에는 일정 기간 동안의 활동이 표시됩니다. 이러한 보고서의 제목은 일반적으로 *감사*란 단어로 시작됩니다. 이러한 유형의 보고서를 요청하는 경우에는 보고서 데이터를 보려는 기간을 지정합니다. 예를 들어 지난 30 일 동안의 "감사-암호 다시 설정" 보고서를 실행할 수 있습니다.

4. "일정 보고서"를 클릭하고 보고서의 일정을 선택합니다.

지금

보고서가 즉시 실행됨을 지정합니다.

한 번

특정 기간 동안 보고서가 한 번 실행되도록 지정합니다. 보고서를 생성할 시작 날짜, 종료 날짜, 시작 시간 및 종료 시간을 선택합니다.

참고: 요청 중인 보고서에 대량의 데이터가 필요한 경우 이 옵션을 선택하는 것이 좋습니다. 시스템 리소스를 절약하려면 시스템 활동이 적은 시간을 선택합니다.

5. 제출을 클릭합니다.

보고서 요청이 제출됩니다. 환경 구성에 따라 요청은 즉시 실행되거나 관리자가 승인한 후에 실행됩니다.

대개 시스템 관리자나 보고서 관리 권한이 있는 다른 사용자가 보고서 요청을 승인해야 해당 보고서 요청이 완료됩니다. 승인이 필요한 이유는 일부 보고서를 실행하는 데 오랜 시간이 걸리거나 상당한 시스템 리소스가 필요하기 때문입니다. 보고서 요청에 대한 승인이 필요한 경우 시스템이 전자 메일 알림을 보냅니다.

보고서 보기

환경 구성에 따라 차이가 있지만 관리자가 해당 보고서 요청을 승인하면 보고서를 볼 수 있게 됩니다. 보고서 요청에 대한 승인이 보류 중인 경우 시스템이 전자 메일 알림을 보냅니다. 보려는 보고서는 승인된 후에야 검색 목록에 나타납니다.

참고: "내 보고서 보기" 태스크를 사용하여 CA Identity Manager 에서 보고서를 보려면 브라우저에서 타사 세션 쿠키를 사용하십시오.

다음 단계를 수행하십시오.

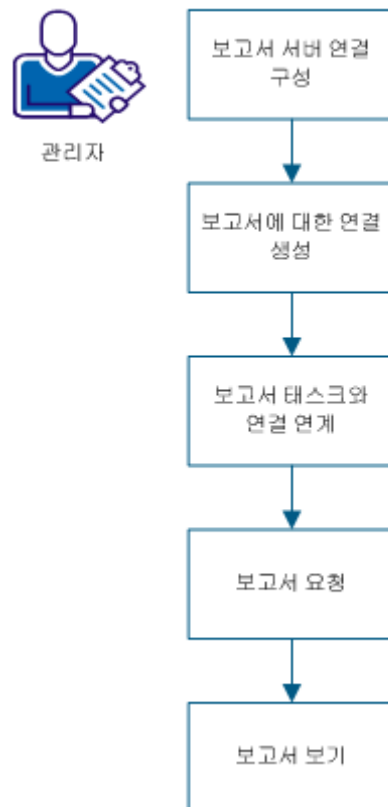
1. 사용자 콘솔에서 "태스크", "보고서", "보고 태스크"로 이동하고 "내 보고서 보기"를 클릭합니다.
2. 생성된 보고서 중에서 보려는 보고서를 검색합니다.
생성된 되풀이 보고서와 주문형 보고서가 모두 표시됩니다.
참고: 보고서의 상태가 보류 중/되풀이인 경우 보고서는 생성되지 않은 것이며 완료하는 데 시간이 걸릴 수 있습니다.
3. 보려는 보고서를 선택합니다.
4. (선택 사항) 왼쪽 위에 있는 "이 보고서 내보내기"를 클릭하여 보고서를 다음 형식으로 내보냅니다.
 - Crystal Reports
 - PDF
 - Microsoft Excel(97-2003)
 - Microsoft Excel(97-2003) 데이터 전용
 - Microsoft Excel(97-2003) - 편집 가능
 - RTF(서식 있는 텍스트 형식 파일)
 - CSV(쉼표로 구분된 값)
 - XML

비스냅샷 보고서를 실행하는 방법

비스냅샷 보고서는 감사, 워크플로, 태스크 지속 데이터베이스와 같은 기타 데이터 원본의 데이터를 포함합니다. CA Identity Manager 는 사용자 콘솔에서 이름에 접두사 "Audit-"가 붙은 기본 감사 보고서를 포함합니다. 기본적으로 CA Identity Manager 는 감사 보고서만 포함하지만 다른 데이터 원본의 데이터를 포함할 수 있는 사용자 지정 보고서를 만들 수 있습니다.

이 시나리오는 Super Administrator 가 보고서 데이터베이스 연결을 구성하고 비스냅샷 보고서를 실행하는 방법을 설명합니다.

비스냅샷 보고서 실행 방법



다음 다이어그램은 스냅샷 보고서를 실행하는 프로세스를 설명합니다.

비스냅샷 보고서를 실행하려면 다음 단계를 수행하십시오.

1. [보고서 서버 연결을 구성합니다.](#) (페이지 458)
2. 보고서에 대한 연결을 만듭니다.
3. 연결을 보고서 태스크와 연결합니다.

4. 보고서를 요청합니다.
5. [보고서를 봅니다.](#) (페이지 462)

보고서 서버 연결 구성

보고서 서버에서 데이터를 수집하려면 보고서 서버에 대한 연결을 구성해야 합니다. 절차를 시작하기 전에 보고서 서버에 대한 다음과 같은 정보를 수집하십시오.

이름	설명
호스트 이름	보고서 서버가 설치된 컴퓨터의 호스트 이름입니다.
포트	보고서 서버가 설치된 컴퓨터의 포트 이름입니다.
보고서 폴더 이름	기본 CA Identity Manager 보고서의 위치입니다.
사용자 ID	보고서 서버를 위해 만들어진 사용자를 지정합니다.
암호	보고서 서버에 만들어진 사용자에 대한 암호를 지정합니다.
보안 연결	보고서 서버에 대한 보안 연결을 지정합니다. CA Identity Manager 와 보고서 서버 사이에서 SSL(Secure Sockets Layer) 연결을 사용하려면 확인란을 선택하십시오. 참고: "보안 연결" 확인란을 선택하기 전에 BOSServer 에서 인증서를 설치했는지 확인하십시오. SSL 구성에 대한 자세한 내용은 설치 안내서 에서 "보고서 서버 설치" 단원을 참조하십시오.
웹 서버	웹 서버를 지정합니다. Tomcat 에 대해 "Non-IIS"를 설정하십시오.

참고: 보고와 관련된 모든 시스템은 동일한 시간대 및 시간으로 설정하는 것이 좋습니다.

다음 단계를 수행하십시오.

1. 사용자 콘솔에서 "시스템", "보고", "보고서 서버 연결"을 차례로 클릭합니다.
2. 보고서 서버 설정을 입력합니다.

3. "연결 테스트"를 클릭하여 연결을 확인합니다.
4. "제출"을 클릭합니다.

보고 연결이 설정됩니다.

보고서에 대한 연결 만들기

CA Identity Manager 보고서에 대한 정보는 여러 출처로부터 제공될 수 있습니다. 보고서의 다른 데이터 원본에 대한 연결 정보를 지정하려면 CA Identity Manager 내에 JDBC 연결을 만드십시오.

다음 단계를 수행하십시오.

1. 사용자 콘솔에서 "태스크", "시스템", "JDBC 연결 관리", "JDBC 연결 만들기"로 이동합니다.
2. 새 연결 개체를 만들거나 특정 JNDI 데이터 원본에 따라 연결 개체를 선택합니다.
3. 필요한 모든 필드를 완료하고 "제출"을 클릭합니다.
새 JDBC 연결이 만들어집니다.

중요! 보고서를 생성하기 위해 CA Identity Manager 개체 저장소 데이터베이스를 사용하지 않는 것이 좋습니다.

연결을 보고서 태스크와 연결

CA Identity Manager 보고서에 대한 정보는 여러 출처로부터 캡처되며 각 보고서는 보고서에서 볼 정보에 따라 특정 데이터 원본과 연결되어야 합니다.

연결을 보고서 태스크와 연결하려면

1. 사용자 콘솔에서 "태스크", "역할 및 태스크", "관리자 태스크", "관리자 태스크 수정"으로 이동합니다.
2. 연결할 보고서 태스크를 검색합니다.
3. "검색" 탭으로 이동하고 "찾아보기"를 클릭하여 검색 화면을 찾습니다.
4. 보고서 태스크의 검색 화면을 편집하고 "보고서용 연결 개체" 아래에서 연결을 선택합니다.
5. 확인을 클릭합니다.

6. "선택"을 클릭합니다.
7. 제출을 클릭합니다.

보고서 요청

보고서를 보려면 보고서 관리 권한이 있는 사용자에게 보고서를 요청하십시오. 승인이 필요한 이유는 일부 보고서를 실행하는 데 오랜 시간이 걸리거나 상당한 시스템 리소스가 소비될 수 있기 때문입니다. 보고서 요청에 승인이 필요한 경우 시스템이 전자 메일 알림을 보냅니다.

다음 단계를 수행하십시오.

1. 보고서 태스크 사용자 권한을 사용하여 사용자 콘솔에 로그인합니다.
2. "태스크", "보고서", "보고 태스크", "보고서 요청"을 선택합니다.
보고서의 목록이 나타납니다.
3. 요청할 보고서를 선택합니다.
매개 변수 화면이 나타납니다.
필요한 매개 변수 정보를 제공합니다.

참고: 스냅샷 보고서를 실행 중이고 이 보고서에 사용할 수 있는 스냅샷이 없으면 먼저 스냅샷을 캡처해야 합니다.

- 일부 보고서에는 특정 시점의 시스템 상태가 표시됩니다. 이러한 유형의 보고서를 요청하는 경우에는 보려는 보고서 데이터의 시점을 선택합니다. 이 시점을 **스냅샷**이라고 합니다.

참고: 선택할 수 있는 스냅샷 날짜 및 시간은 미리 결정되어 있습니다. 대개 시스템 관리자나 보고서 관리 권한이 있는 다른 사용자가 스냅샷을 구성합니다. 요청할 보고서에 사용할 수 있는 스냅샷이 없으면 시스템 관리자에게 문의하십시오.

- 일부 보고서에는 일정 기간 동안의 활동이 표시됩니다. 이러한 보고서의 제목은 일반적으로 **감사**란 단어로 시작됩니다. 이러한 유형의 보고서를 요청하는 경우에는 보고서 데이터를 보려는 기간을 지정합니다. 예를 들어 지난 30 일 동안의 "감사-암호 다시 설정" 보고서를 실행할 수 있습니다.

4. "일정 보고서"를 클릭하고 보고서의 일정을 선택합니다.

지금

보고서가 즉시 실행됨을 지정합니다.

한 번

특정 기간 동안 보고서가 한 번 실행되도록 지정합니다. 보고서를 생성할 시작 날짜, 종료 날짜, 시작 시간 및 종료 시간을 선택합니다.

참고: 요청 중인 보고서에 대량의 데이터가 필요한 경우 이 옵션을 선택하는 것이 좋습니다. 시스템 리소스를 절약하려면 시스템 활동이 적은 시간을 선택합니다.

5. 제출을 클릭합니다.

보고서 요청이 제출됩니다. 환경 구성에 따라 요청은 즉시 실행되거나 관리자가 승인한 후에 실행됩니다.

대개 시스템 관리자나 보고서 관리 권한이 있는 다른 사용자가 보고서 요청을 승인해야 해당 보고서 요청이 완료됩니다. 승인이 필요한 이유는 일부 보고서를 실행하는 데 오랜 시간이 걸리거나 상당한 시스템 리소스가 필요하기 때문입니다. 보고서 요청에 대한 승인이 필요한 경우 시스템이 전자 메일 알림을 보냅니다.

보고서 보기

환경 구성에 따라 차이가 있지만 관리자가 해당 보고서 요청을 승인하면 보고서를 볼 수 있게 됩니다. 보고서 요청에 대한 승인이 보류 중인 경우 시스템이 전자 메일 알림을 보냅니다. 보려는 보고서는 승인된 후에야 검색 목록에 나타납니다.

참고: "내 보고서 보기" 태스크를 사용하여 CA Identity Manager 에서 보고서를 보려면 브라우저에서 타사 세션 쿠키를 사용하십시오.

다음 단계를 수행하십시오.

1. 사용자 콘솔에서 "보고서", "보고 태스크"로 이동하고 "내 보고서 보기"를 클릭합니다.
2. 생성된 보고서 중에서 보려는 보고서를 검색합니다.
생성된 되풀이 보고서와 주문형 보고서가 모두 표시됩니다.
참고: 보고서의 상태가 보류 중/되풀이인 경우 보고서는 생성되지 않은 것이며 완료하는 데 시간이 걸릴 수 있습니다.
3. 보려는 보고서를 선택합니다.
4. (선택 사항) 왼쪽 위에 있는 "이 보고서 내보내기"를 클릭하여 보고서를 다음 형식으로 내보냅니다.
 - Crystal Reports
 - PDF
 - Microsoft Excel(97-2003)
 - Microsoft Excel(97-2003) 데이터 전용
 - Microsoft Excel(97-2003) - 편집 가능
 - RTF(서식 있는 텍스트 형식 파일)
 - CSV(쉼표로 구분된 값)
 - XML

보고 옵션 설정

사용자가 특정 보고서에 대해 생성할 수 있는 보고서 인스턴스 수를 구성합니다.

보고 옵션을 수정하려면

1. "태스크", "보고서", "보고 태스크", "보고 옵션 설정"을 선택합니다.

CA Identity Manager 에서 IAM 보고서 서버에 연결하여 모든 보고서 목록을 검색합니다.

2. 보고서를 선택하고 "수정"을 클릭합니다.

보고서의 특성 창이 나타납니다.

3. 다음 필드를 편집합니다.

이름

선택한 보고서의 표시 이름을 지정합니다.

인스턴스 수

사용자가 이 보고서에 대해 생성할 수 있는 허용되는 인스턴스 수를 지정합니다.

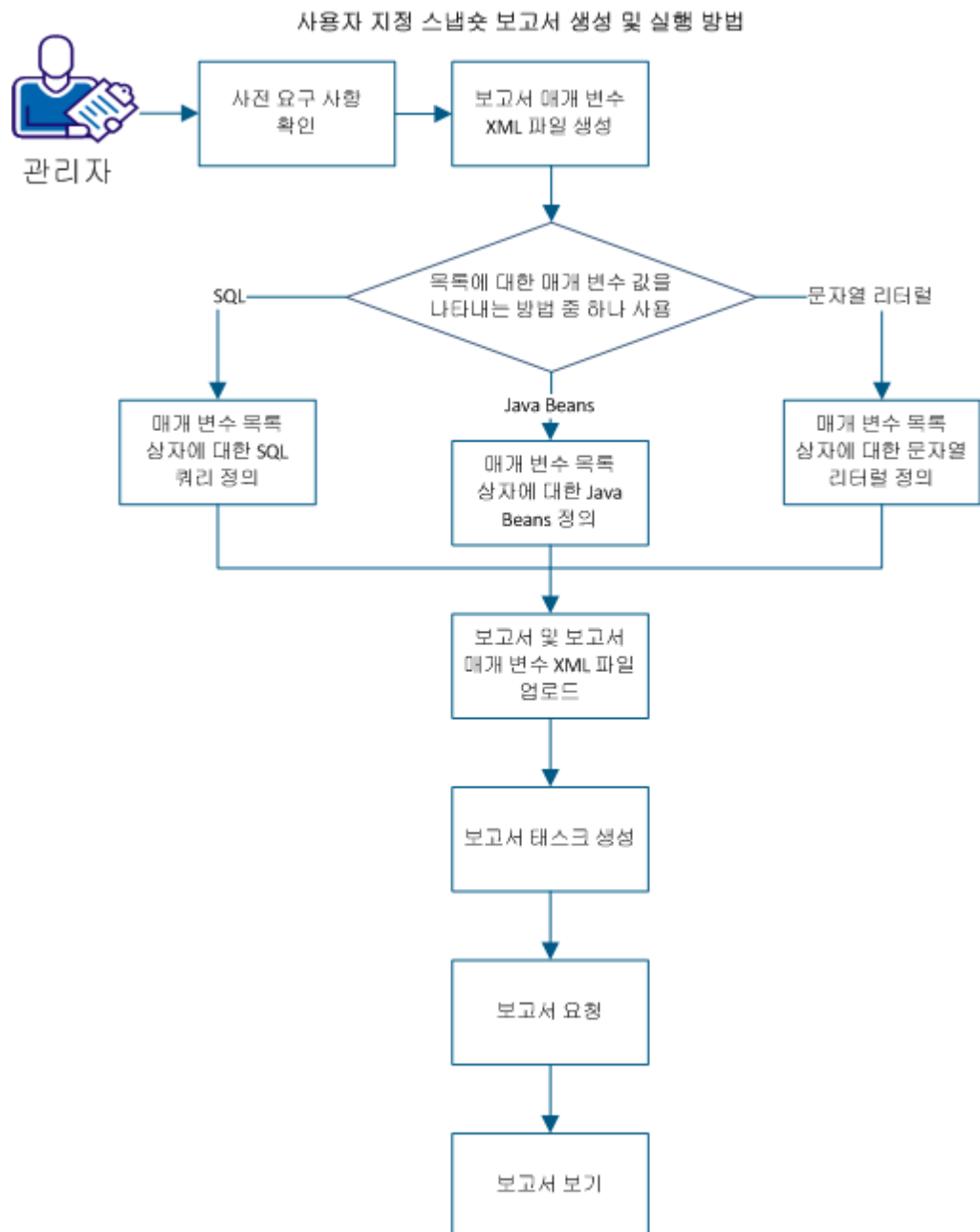
4. 확인을 클릭합니다.

보고서 특성이 변경됩니다.

사용자 지정 스냅샷 보고서를 만들고 실행하는 방법

CA Identity Manager 는 비즈니스 필요성에 맞게 보고서를 만들고 사용자 지정할 수 있게 해 줍니다. CA Identity Manager 는 보고서 특성과 관련된 모든 매개 변수를 포함하는 보고 매개 변수 XML 파일을 제공합니다. 비즈니스 필요성에 따라 스냅샷 데이터 원본으로부터 보고서 데이터를 채우기 위해 필요한 특성을 선택할 수 있습니다.

다음 그림은 사용자 지정 스냅샷 보고서를 만들고 실행하기 위한 프로세스를 설명합니다.



시스템 관리자가 다음 단계를 수행합니다.

1. [사전 요구 사항 확인](#) (페이지 466)
2. [보고서 매개 변수 XML 파일 만들기](#) (페이지 466)
3. 다음 방법 중 하나를 사용하여 목록에 대한 매개 변수 값을 나타내십시오.

- [매개 변수 목록 상자에 대한 SQL 쿼리 정의](#) (페이지 470)
 - [매개 변수 목록 상자에 대한 Java Beans 정의](#) (페이지 471)
 - [매개 변수 목록 상자에 대한 문자열 리터럴 정의](#) (페이지 471)
4. [보고서 및 보고서 매개 변수 XML 파일 업로드](#) (페이지 471)
 5. 보고서 태스크 만들기
 6. 보고서 요청
 7. [보고서 보기](#) (페이지 462)

Crystal Reports 에서 보고서를 만듭니다.

CA Identity Manager 에서 사용자 지정 보고서를 사용하려면 Crystal Reports Developer 에서 보고서(RPT 파일)를 만드십시오. Crystal Reports 에서 보고서를 만드는 방법에 대한 자세한 내용은 Crystal Reports 설명서를 참조하십시오.

참고: 사용자 지정 보고서를 만들기 위해 CA Identity Manager 스키마를 참조하려면 다음 위치에 CA Identity Manager 데이터베이스 스키마가 있습니다.

C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\db\objectstore

보고서 매개 변수 XML 파일 만들기

매개 변수는 보고서에 있는 필드 중 하나로서, 보고서를 필터링하는 데 사용할 수 있습니다. 매개 변수를 사용하여 데이터를 필터링함으로써 보고서를 생성할 수 있습니다. 보고서 검색 화면을 사용자 지정할 수 있도록 각 보고서(RPT 파일)은 보고서 매개 변수 XML 파일과 연계되어 있습니다. CA Identity Manager 에서 보고서 태스크를 만들고 보고서 생성 중에 사용자가 필요한 데이터를 입력 또는 선택할 수 있도록 검색 화면을 만들 수 있습니다.

참고: 보고서가 개체의 특성을 쿼리하는 경우 보고서 매개 변수 XML 파일만 필요합니다.

보고서 매개 변수 XML 파일은 보고서(RPT 파일)와 이름이 같아야 하며 확장명 .xml 을 사용해야 합니다. 예를 들어, 보고서 서버에 test1.rpt 란 이름의 보고서를 업로드하는 경우, XML 파일의 이름은 test1.xml 이어야 합니다.

보고서 매개 변수 XML 파일에는 다음과 같은 요소가 있습니다.

<product>

매개 변수가 사용되는 제품을 나타냅니다. 동일한 매개 변수 XML 파일을 사용하여 여러 제품에 대해 다른 매개 변수를 만들 수 있습니다.

<screen>

화면에 표시된 매개 변수를 정의합니다. 이 화면 요소를 사용하여 특정 화면에 매개 변수를 바인딩할 수 있습니다. 화면 ID 는 고유한 영숫자이며, 화면 및 해당 매개 변수를 식별하는 데 사용됩니다.

<parameters>

화면에 대한 매개 변수 집합을 지정합니다.

<param>

지정된 데이터를 보고서로 전달하는 매개 변수 요소를 정의합니다.

<param> 요소에는 다음과 같은 특성이 사용됩니다.

id

보고서에서 어떤 매개 변수와 연결할지 정의합니다.

참고: id 는 Crystal Report 의 매개 변수와 동일한 이름을 사용해야 합니다.

이름

이 필드는 현재 CA Identity Manager 에서 사용되지 않습니다. 이 특성을 id 와 동일한 값으로 설정하십시오.

displaytext

매개 변수에 대해 화면에 사용자에게 친숙한 텍스트가 표시되도록 지정합니다.

type

매개 변수의 유형을 정의합니다. 이 특성을 기준으로 화면 표시가 변경됩니다. 지원되는 매개 변수 유형은 다음과 같습니다.

- 텍스트 상자

예: `<param id="param1" displaytext="First Name" name="param1" type="string"/>`

- 날짜 및 시간

예: `<param id="dateVal" displaytext="Date" name="dateVal" type="date_str"/>`

`<param id="timeVal" displaytext="Time" name="timeVal" type="time_str"/>`

`<param id="datetimeVal" displaytext="Date & Time" name="datetimeVal" type="date_time_str"/>`

- 드롭다운 목록

예: `<param id="lastname1" displaytext="Name" name="lastname1" type="dropdown" default="key1%1FMy Value1%1Ekey2%1FMy Value2" selected_value="My Value2"/>`

- 목록 상자

예: `<param id="lstlastname1" displaytext="Name" name="lstlastname1" type="listbox" rows="10" default="key1%1FSuper%1Ekey2%1Fsql2kSuser01%1Ekey1F%Super"/>`

- 라디오 상자

예: `<param id="optionslist" displaytext="Option 1" name="optionslist" type="radiobox" value="option1"/>`

`<param id="optionslist" displaytext="Option 2" name="optionslist" type="radiobox" value="option2"/>`

`<param id="optionslist" displaytext="Option 3" name="optionslist" type="radiobox" value="option3"/>`

- 확인란

예: `<param id="enabled" displaytext="Enabled" name="enabled" type="checkbox"/>`

row

목록 상자에 표시될 수 있는 행 수를 정의합니다.

기본값: 5

기본값

지정된 매개 변수에 대한 화면에 표시되는 기본값을 정의합니다. 이 특성은 문자열, 목록 상자, 드롭다운 목록 유형에 사용할 수 있습니다.

매개 변수 목록 상자에 대한 SQL 쿼리 정의

보고서 매개 변수 XML 파일의 목록 상자 또는 드롭다운 상자의 일부로서 SQL 쿼리를 정의할 수 있습니다. 보고서에 매개 변수를 연결하고 보고서 태스크를 만들 때 매개 변수가 사용자에게 대한 목록 상자 또는 드롭다운 상자에 표시됩니다. 드롭다운 상자 또는 목록 상자 매개 변수에서 SQL 을 사용하려면 sql 특성에서 올바른 SQL 문을 제공하십시오.

예:

```
<param id="lstlastname2" displaytext="Name" name="lstlastname2" type="sqlstr"
multiselect="true" sql="select lastname, lastname from tblusers where firstname like
'S%"/>
```

앞의 예제에서는 이름(first name)이 S 로 시작하는 사용자 성(last name)이 모두 보고서에 제공됩니다.

하지만 S 로 시작하는 이름의 조건은 정적입니다. 이 쿼리는 사용자가 동일한 보고서 매개 변수 그룹에 사용된 이전 화면 중 하나에 입력된 매개 변수를 기준으로 값을 로드할 경우 융통성이 부족합니다. 다른 화면에 입력된 이전 값을 사용하기 위해 SQL 문은 ##<parameter id>##으로 증가될 수 있습니다.

예를 들어, String 유형의 id=User 인 매개 변수가 있는 경우:

```
<param id="User" displaytext="First Name" name="firstname" type="string"/>
```

이 매개 변수의 입력 값을 SQL 에서 사용하는 경우, SQL 문은 다음과 같을 수 있습니다.

```
<param id="lstlastname2" displaytext="Name" name="lstlastname2" type="sqlstr"
multiselect="true" sql="select lastname, lastname from tblusers where firstname like
'##User##"/>
```

CA Identity Manager 는 ##User##을 id=User 인 매개 변수에 대해 입력한 값으로 대체합니다.

참고: 대체할 매개 변수 값은 SQL 매개 변수와 동일한 화면에 있을 수 없습니다. 예를 들어, *lstlastname2* 가 화면 3 에 있는 경우 User 매개 변수는 이전 화면 중 하나에 있어야 합니다.

매개 변수 목록 상자에 대한 Java Beans 정의

SQL 을 사용하는 것이 적절히 많으면 java beans 를 사용하여 값을 계산하고 <key, value> 쌍의 목록을 CA Identity Manager 에 제공할 수 있습니다. java beans 는 CA Identity Manager 의 classpath 에 있어야 합니다.

예:

```
<param id="lastname2" displaytext="Name using Javabean" name="lastname2"
type="dropdown" class="com.ca.ims.reporting.unittests.TestDataCollector"/>
```

앞의 예제에서 TestDataCollector 는 자체 방식으로 값을 검색하여 보고서에 드롭다운 목록을 위한 데이터를 보냅니다. <key, value> 쌍은 %1F 로 구분됩니다.

java bean 는 iam_im.ear\custom 디렉터리에 있어야 합니다.

참고: java beans 구현에 대한 자세한 내용은 [Business Objects 설명서](#)를 참조하십시오.

매개 변수 목록 상자에 대한 문자열 리터럴 정의

목록 또는 드롭다운 상자에 대한 매개 변수를 제공하는 가장 쉬운 방법은 문자열 리터럴을 사용하는 것입니다. 키 값은 %1F 로 구분되고 각 <key, value> 쌍은 %1E 로 구분됩니다.

예:

```
<param id="lastname1" displaytext="Name" name="lastname" type="dropdown"
default="key1%1FMy Value1%1Ekey2%1FMy Value2" selected_value="My Value2"/>
```

보고서 및 보고서 매개 변수 XML 파일 업로드

보고서(RPT)와 해당 보고서 매개 변수 XML 파일을 작성한 후에는 이 두 파일을 보고서 서버(Business Objects)로 업로드하십시오.

다음 단계를 수행하십시오.

1. Business Objects Central Management 콘솔에 로그인합니다.
2. "폴더"를 클릭합니다
3. "IM Reports"(IM 보고서) 폴더를 선택합니다.

4. 개체 패키지를 만듭니다.
5. 새 개체 패키지에서 탐색하여 **Crystal Report** 를 추가합니다.
6. 만든 새 보고서(RPT)를 찾습니다.
참고: 보고서를 저장할 폴더로서 "IM Reports"(IM 보고서) 폴더가 선택되었는지 확인합니다.
7. "확인"을 클릭합니다.
Crystal Report 파일이 추가되었습니다.
8. 새 개체 패키지에서 새 로컬 문서를 추가하고 새 보고서 매개 변수 XML 파일을 찾습니다.
9. 파일 유형으로 **텍스트**를 선택합니다.
10. "확인"을 클릭합니다.

보고서 및 보고서 매개 변수 xml 파일이 이제 업로드되었습니다.
확인하려면 **IM** 보고서 폴더로 이동하여 새 파일을 모두 사용할 수 있는지 확인하십시오.

보고서 태스크 만들기

보고서 태스크는 사용자 콘솔에서 생성된 보고서에 대한 템플릿을 생성하고, 관리하고, 보고, 삭제하는 데 사용됩니다.

다음 단계를 수행하십시오.

1. 사용자 콘솔에서 "태스크", "역할 및 태스크", "관리자 태스크", "관리자 태스크 만들기"으로 이동합니다.
2. "새 관리자 태스크 만들기"를 선택하고 "확인"을 클릭합니다.
3. "Profile"(프로필) 탭에서 다음 필드를 완성합니다.

이름

보고서의 이름을 정의합니다. 각 보고서 태스크 이름은 고유해야 합니다.

태그

태스크의 고유한 식별자를 정의합니다. 이 필드는 URL, 웹 서비스 또는 속성 파일에 사용됩니다. 여기에는 문자, 숫자 및/또는 밑줄이 포함될 수 있으며, 문자 또는 밑줄로 시작됩니다.

범주

현재 태스크가 속하는 범주를 지정합니다.

참고: "보고서" 범주를 선택하십시오.

범주 2

현재 태스크가 속하는 하위 범주를 지정합니다. 이 필드에 문자열을 입력하십시오.

기본 개체

태스크가 실행되는 개체를 지정합니다.

참고: 기본 개체로서 "보고서 인스턴스"를 선택합니다.

작업

기본 개체에서 수행된 동작을 지정합니다.

참고: 동작으로 "만들기"를 선택하십시오.

4. 보고서 태스크에 대한 새 검색 화면을 만들려면 다음 단계를 수행하십시오.
 - a. "검색" 탭에서 "찾아보기"를 클릭하여 검색 화면을 찾습니다.
사용 가능한 검색 화면 목록이 표시됩니다.

- b. "New"(새로 만들기)를 클릭합니다.

"화면 만들기" 창이 나타납니다.

- c. 목록에서 "보고서 템플릿 선택 화면"을 선택한 다음 "확인"을 클릭합니다.

CA Identity Manager 가 보고서 서버에 연결하고 모든 보고서를 표시합니다.

- d. 다음 필드를 작성하십시오.

이름

보고서의 이름을 정의합니다. 각 보고서 태스크 이름은 고유해야 합니다.

태그

태스크 내에서 고유 식별자로 기능합니다. ASCII 문자(a-z, A-Z), 숫자(0-9) 또는 밑줄 문자를 사용할 수 있으며 문자나 밑줄로 시작해야 합니다.

제목

새 검색 화면의 제목을 정의합니다. 제목은 고유해야 합니다.

보고서 템플릿

검색 화면과 연결할 보고서를 식별합니다.

참고: 보고서 서버에 추가한 보고서 중 하나를 선택하십시오.

보고서용 연결 개체

보고서에 사용될 데이터 원본의 연결 정보를 정의합니다.

- 5. 확인을 클릭합니다.

이제 보고서에 대한 새 검색 화면이 생성되었습니다.

- 6. 보고서 태스크에 대한 "탭" 탭을 만들 때 다음 단계를 수행하십시오.

- a. "탭"을 클릭합니다.

사용자가 볼 수 있는 탭이 표시됩니다.

- b. "표준 탭 컨트롤러"를 선택합니다.

- c. 보고서가 스냅샷 정의를 사용하는 경우 다음 단계를 수행하십시오.

- a. "이 태스크에 어떤 탭이 나타나야 합니까?"에서 "스냅샷 정의 연결"을 선택합니다.

"스냅샷 정의 연결" 탭이 탭의 목록에 추가됩니다.

- b.  을 클릭하여 "스냅샷 정의 연결" 탭을 편집합니다.
- c. "추가"를 클릭하여 보고서 태스크를 스냅샷 정의와 연결합니다.
사용 가능한 스냅샷 정의의 목록이 표시됩니다.
- d. 스냅샷 정의를 선택하고 "확인"을 클릭합니다.
보고서 태스크가 스냅샷 정의와 연결됩니다.
- d. 제출을 클릭합니다.
보고서 태스크가 생성되었습니다.
- e. 새 보고서 태스크를 관리자 역할에 할당합니다.
CA Identity Manager 관리자 역할 사용자가 새 보고서 태스크를 사용할 수 있습니다.

보고서 태스크는 이제 관리자가 사용할 준비가 되었습니다.

참고: 보고서(RPT 파일)는 *하나*의 보고서 태스크에만 연계할 수 있습니다.

보고서 요청

보고서를 보려면 보고서 관리 권한이 있는 사용자에게 보고서를 요청하십시오. 대개 시스템 관리자나 보고서 관리 권한이 있는 다른 사용자가 보고서 요청을 승인해야 해당 보고서 요청이 완료됩니다. 승인이 필요한 이유는 일부 보고서를 실행하는 데 오랜 시간이 걸리거나 상당한 시스템 리소스가 소비될 수 있기 때문입니다. 보고서 요청에 승인이 필요한 경우 시스템이 전자 메일 알림을 보냅니다.

다음 단계를 수행하십시오.

1. 사용자 콘솔에 보고서 태스크에 대한 권한을 가진 사용자로 로그인합니다.
2. 탐색 메뉴에서 "태스크", "보고서", "보고 태스크", "보고서 요청"을 차례로 선택합니다.
보고서의 목록이 나타납니다.
3. 요청할 보고서를 선택합니다.
매개 변수 화면이 나타납니다.
4. 필요한 매개 변수 정보를 제공합니다.

참고: 스냅샷 보고서를 실행 중이고 이 보고서에 사용할 수 있는 스냅샷이 없으면 먼저 스냅샷을 캡처해야 합니다.

- 일부 보고서에는 특정 시점의 시스템 상태가 표시됩니다. 이러한 유형의 보고서를 요청하는 경우에는 보려는 보고서 데이터의 시점을 선택합니다. 이 시점을 **스냅샷**이라고 합니다.

참고: 선택할 수 있는 스냅샷 날짜 및 시간은 미리 결정되어 있습니다. 대개 시스템 관리자나 보고서 관리 권한이 있는 다른 사용자가 스냅샷을 구성합니다. 요청할 보고서에 사용할 수 있는 스냅샷이 없으면 시스템 관리자에게 문의하십시오.

- 일부 보고서에는 일정 기간 동안의 활동이 표시됩니다. 이러한 보고서의 제목은 일반적으로 **감사**란 단어로 시작됩니다. 이러한 유형의 보고서를 요청하는 경우에는 보고서 데이터를 보려는 기간을 지정합니다. 예를 들어 지난 30 일 동안의 "감사-암호 다시 설정" 보고서를 실행할 수 있습니다.
5. "일정 보고서"를 클릭하고 보고서의 일정을 선택합니다.

지금

보고서가 즉시 실행됨을 지정합니다.

한 번

특정 기간 동안 보고서가 한 번 실행되도록 지정합니다. 보고서를 생성할 시작 날짜, 종료 날짜, 시작 시간 및 종료 시간을 선택합니다.

참고: 요청 중인 보고서에 대량의 데이터가 필요한 경우 이 옵션을 선택하는 것이 좋습니다. 시스템 리소스를 절약하려면 시스템 활동이 적은 시간을 선택합니다.

6. 제출을 클릭합니다.

보고서 요청이 제출됩니다. 환경 구성에 따라 요청은 즉시 실행되거나 관리자가 승인한 후에 실행됩니다.

보고서 보기

환경 구성에 따라 차이가 있지만 관리자가 해당 보고서 요청을 승인하면 보고서를 볼 수 있게 됩니다. 보고서 요청에 대한 승인이 보류 중인 경우 시스템이 전자 메일 알림을 보냅니다. 보려는 보고서는 승인된 후에야 검색 목록에 나타납니다.

참고: "내 보고서 보기" 태스크를 사용하여 CA Identity Manager 에서 보고서를 보려면 브라우저에서 타사 세션 쿠키를 사용하십시오.

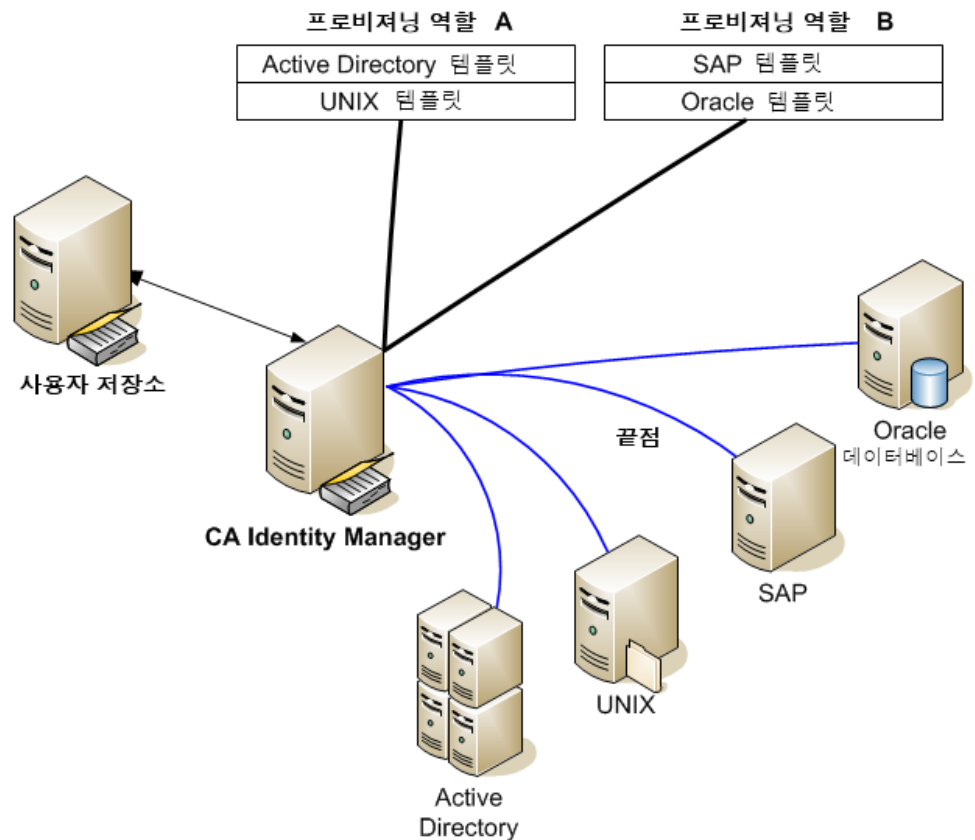
다음 단계를 수행하십시오.

1. 사용자 콘솔에서 "태스크", "보고서", "보고 태스크"로 이동하고 "내 보고서 보기"를 클릭합니다.
2. 생성된 보고서 중에서 보려는 보고서를 검색합니다.
생성된 되풀이 보고서와 주문형 보고서가 모두 표시됩니다.
참고: 보고서의 상태가 보류 중/되풀이인 경우 보고서는 생성되지 않은 것이며 완료하는 데 시간이 걸릴 수 있습니다.
3. 보려는 보고서를 선택합니다.
4. (선택 사항) 왼쪽 위에 있는 "이 보고서 내보내기"를 클릭하여 보고서를 다음 형식으로 내보냅니다.
 - Crystal Reports
 - PDF
 - Microsoft Excel(97-2003)
 - Microsoft Excel(97-2003) 데이터 전용
 - Microsoft Excel(97-2003) - 편집 가능
 - RTF(서식 있는 텍스트 형식 파일)
 - CSV(쉼표로 구분된 값)
 - XML

사용자, 계정 및 역할 동기화

여러 끝점과 계정을 단일 사용자 관리 시스템으로 통합하면 동기화가 이루어지지 않을 수 있습니다. 사용자에게 할당된 프로비저닝 역할이나 계정 템플릿이 해당 사용자에게 존재하는 실제 계정과 다를 수 있습니다.

예를 들어 두 개의 프로비저닝 역할, 즉 Active Directory 및 UNIX 계정 템플릿이 있는 프로비저닝 역할과 SAP 및 Oracle 템플릿이 있는 프로비저닝 역할이 존재하는 경우를 생각해 봅시다. 사용자 john_smith 에게 Active Directory 및 UNIX 계정 템플릿을 포함하는 프로비저닝 역할 A 가 있지만 해당 사용자가 가지고 있는 계정은 Active Directory 계정뿐입니다. UNIX 계정 템플릿은 사용자에게 할당된 후에 역할에 추가되었을 가능성이 있습니다. 따라서 관리자가 사용자를 현재 역할 정의와 동기화합니다.



다음 상황은 사용자와 프로비저닝 역할이나 계정 템플릿 간의 동기화가 이루어지지 않는 그 밖의 이유입니다.

- 네트워크에서 하드웨어 또는 소프트웨어 문제로 인해 필요한 계정을 만들려는 이전의 시도가 실패하고, 이로 인해 누락된 계정이 발생합니다.
- 프로비저닝 역할 및 계정 템플릿이 변경되고, 이로 인해 불필요하거나 누락된 계정이 발생합니다.
- 계정이 생성된 후 계정 템플릿에 할당되어 계정은 존재하나 계정 템플릿과 동기화되지 않은 계정이 존재합니다.
- 계정이 나중에 생성되도록 지정되었기 때문에 새 계정의 생성이 지연되었습니다.
- 새 끝점이 획득되었습니다. 탐색 및 상관 관계 지정 중에 프로비저닝 서버가 프로비저닝 역할을 사용자에게 자동으로 할당하지 않았습니다. 끝점에서 계정이 필요한 사용자를 나타내도록 역할을 업데이트하십시오. 사용자와의 상관 관계가 지정된 모든 계정은 사용자가 동기화될 때 불필요한 계정으로 나열됩니다.
- 계정을 사용자에게 복사하여 기존 계정이 사용자에게 할당되었습니다.
- 사용자를 역할에 할당하는 방법이 아닌 다른 방법에 의해 사용자에게 대한 계정이 생성되었습니다. 예를 들어 해당 사용자에게 대한 프로비저닝 역할에 없는 계정 템플릿에 사용자를 복사했습니다. 계정은 불필요한 계정으로 나열되거나 불필요한 계정 템플릿이 있는 계정으로 나열됩니다. 기본 계정 템플릿을 사용하여 계정을 만들기 위해 사용자를 끝점에 복사하는 경우 해당 계정은 불필요한 계정이 될 수 있습니다.

다음 섹션에서는 세 가지 유형의 동기화를 수행하는 방법을 설명합니다.

1. [사용자를 역할과 동기화](#) (페이지 190)
2. [사용자를 계정 템플릿과 동기화](#) (페이지 191)
3. [끝점 계정을 계정 템플릿과 동기화](#) (페이지 192)

사용자를 역할과 동기화

이 태스크는 사용자에게 할당된 프로비저닝 역할을 준수하도록 계정을 생성, 업데이트 또는 삭제합니다. 예를 들어 관리자가 끝점의 기본 도구를 사용하여 계정을 추가하거나 삭제하지만 사용자가 해당 끝점을 다시 탐색하여 프로비저닝 디렉터리를 업데이트하지 않았습니까. 따라서 사용자에게 불필요한 계정이나 누락된 계정이 있습니다. 또한 이 태스크를 수행하면 각 계정이 올바른 계정 템플릿에 속하게 됩니다.

다음 단계를 수행하십시오.

1. 사용자 콘솔에 로그인합니다.
2. "사용자", "동기화", "역할 동기화 검사"를 차례로 선택합니다.
3. 사용자를 선택합니다.

예상된 계정, 불필요한 계정 및 누락된 계정을 보여 주는 화면이 나타납니다.

4. "동기화"를 클릭하여 계정을 이 역할에 있는 템플릿과 일치하도록 만듭니다.
 - a. 확인란을 선택하여 끝점에 계정을 만들 수 있습니다. 사용자의 여러 계정 템플릿이 동일한 계정을 미리 지정하는 경우 모든 관련 계정 템플릿을 병합하여 계정이 생성됩니다.

이 계정은 이러한 계정 템플릿에 할당되었는데, 이 템플릿은 현재 계정과 동기화되어 있지 않습니다.
 - b. 확인란을 선택하여 불필요한 계정을 삭제할 수 있습니다. 그러나 해당 계정을 가지고 있어야 하는 합당한 이유가 사용자에게 있을 수 있습니다. 이 경우 이 옵션을 선택 해제된 상태로 둡니다.

특정 끝점에서는 계정 삭제 기능이 사용되지 않으므로 계정이 삭제되지 않습니다.

사용자를 계정 템플릿과 동기화

이 태스크는 끝점 계정의 특성을 사용자의 관련 계정 템플릿과 동기화합니다. 그러나 전체 동기화는 다음과 같은 요소에 따라 결정됩니다.

- 계정의 전체 동기화는 두 가지 상황에서 발생합니다. 즉, 계정 템플릿이 [강력한 동기화](#) (페이지 194)를 사용하는 상황이나 둘 이상의 계정 템플릿이 계정에 추가된 상황에서 발생합니다.
- 계정 템플릿이 [약한 동기화](#) (페이지 193)를 사용하는 경우 이 태스크는 이 템플릿만 포함하는 계정 동기화를 시작합니다. 계정이 이 업데이트 이전에 다른 계정 템플릿과 계정 동기화되지 않았으면 그 후에도 여전히 계정이 동기화되지 않을 수 있습니다.

다음 단계를 수행하십시오.

1. 사용자 콘솔에 로그인합니다.
2. "사용자", "동기화", "계정 템플릿 동기화 검사"를 차례로 선택합니다.
3. 사용자를 선택합니다.
예상된 계정, 불필요한 계정 및 누락된 계정을 보여 주는 화면이 나타납니다.
4. "동기화"를 클릭하여 계정을 템플릿과 일치하도록 만듭니다.
 - a. 확인란을 선택하여 끝점에 계정을 만들 수 있습니다. 사용자의 여러 계정 템플릿이 동일한 계정을 미리 지정하는 경우 관련 계정 템플릿을 병합하여 계정이 생성됩니다.
이 계정은 해당 계정과 동기화되지 않은 계정 템플릿에 할당됩니다. 새로 생성된 계정에는 계정 동기화가 필요 없습니다.
 - b. 확인란을 선택하여 불필요한 계정을 삭제할 수 있습니다. 그러나 해당 계정을 가지고 있어야 하는 합당한 이유가 사용자에게 있을 수 있습니다. 이 경우 이 옵션을 선택 해제된 상태로 둡니다.
특정 끝점에서는 계정 삭제 기능이 사용되지 않으므로 계정이 삭제되지 않습니다.

끝점 계정을 계정 템플릿과 동기화

이 태스크는 관련 계정 템플릿 수정 후 끝점 계정을 동기화합니다. 예를 들어 **Active Directory** 계정에는 그룹이 없지만 관련 계정 템플릿은 그룹을 포함하도록 정의되어 있을 수 있습니다.

다음 단계를 수행하십시오.

1. 사용자 콘솔에 로그인합니다.
2. "끝점", "끝점 관리", "끝점 계정 동기화 검사"를 차례로 선택합니다.
3. 끝점을 선택합니다.

해당 끝점의 계정, 관련 계정 템플릿, 동기화되지 않은 특성 등을 보여주는 화면이 나타납니다.

4. "동기화"를 클릭하여 해당 계정의 특성을 계정 템플릿에 정의된 것과 일치하도록 만듭니다.

계정 템플릿의 변경 내용은 다음과 같이 기존 계정에 영향을 줍니다.

- 기능 특성 값을 변경하면 해당 계정 특성이 업데이트되어 계정 템플릿 특성 값과 동기화됩니다. 약한 동기화와 강력한 동기화에 대한 설명을 참조하십시오.
- 특정 계정 특성은 계정 템플릿 변경 사항에서 업데이트되지 않으므로 커넥터에 의해 지정됩니다. 예를 들면 계정을 만드는 동안 끝점 유형만 설정할 수 있도록 허용하는 특정 특성, 암호 특성 등입니다.

업데이트된 특성

계정 템플릿에서 기능 특성을 변경할 때 계정의 해당 특성이 변경됩니다. 이 변경은 계정의 특성에 영향을 줍니다. 이 영향은 다음과 같은 요인에 기초합니다.

- 계정 템플릿이 약한 동기화 또는 강력한 동기화를 사용하도록 정의되었는지 여부
- 계정이 여러 계정 템플릿에 속하는지 여부

약한 동기화

약한 동기화를 사용하면 사용자의 계정이 최소 기능 특성을 가지게 됩니다. 약한 동기화는 대부분의 끝점 유형에서 기본값입니다. 약한 동기화를 사용하는 템플릿을 업데이트하는 경우 CA Identity Manager 는 다음과 같이 기능 특성을 업데이트합니다.

- 숫자 필드가 계정 템플릿에서 업데이트되고 새 숫자가 계정의 숫자보다 크면 CA Identity Manager 에서 계정의 값을 변경하여 새 숫자와 일치시킵니다.
- 계정 템플릿에서 확인란을 선택하지 않았는 데 이후에 이 확인란을 선택하면 CA Identity Manager 에서 이 확인란이 선택되지 않은 계정의 확인란을 업데이트합니다.
- 목록이 계정 템플릿에서 변경되면 CA Identity Manager 에서 모든 계정을 업데이트하여 계정의 값 목록에 포함되지 않은 새 목록의 값을 포함합니다.

계정이 다른 계정 템플릿에 속하면(해당 템플릿에서 약한 동기화를 사용하든지 강력한 동기화를 사용하든지) CA Identity Manager 에서는 변경 중인 템플릿만 참조합니다. 이 동작은 모든 계정 템플릿을 검사하는 것보다 효율적입니다. 약한 동기화는 기능을 계정에만 추가하므로, 일반적으로 다른 계정 템플릿을 참조할 필요가 없습니다.

참고: 약한 동기화 계정 템플릿에서 전파할 때 기능을 제거하거나 낮추는 변경 사항은 일부 계정을 동기화하지 않은 상태로 둘 수 있습니다. 약한 동기화를 사용할 경우 기능은 제거되거나 낮춰지지 않습니다. 계정에 대한 다른 템플릿을 참조할 경우 약한 동기화로 충분하면 전파는 고려되지 않습니다.

이 경우 "사용자를 계정 템플릿과 동기화"를 사용하여 계정을 해당 계정 템플릿과 동기화합니다.

강한 동기화

강한 동기화는 계정 템플릿에 정의된 대로 계정에 정확한 계정 특성이 있는지 확인합니다.

예를 들어, 기존 UNIX 계정 템플릿에 그룹을 추가한다고 가정합니다. 원래 계정 템플릿은 **Staff** 그룹의 계정 구성원을 만들었습니다. 이제, **Staff** 및 **System** 그룹 모두의 계정 구성원을 만들려고 합니다. 각 계정이 **Staff** 및 **System** 그룹의 구성원(그리고 다른 그룹의 구성원이 아님)일 때 계정 템플릿과 관련된 모든 계정이 동기화되었다고 간주됩니다. **Staff** 그룹에 없는 모든 계정은 두 그룹 모두에 추가됩니다.

고려해야 할 일부 다른 요인은 다음 상황을 포함합니다.

- 계정 템플릿이 강한 동기화를 사용하는 경우, **Staff** 및 **System** 을 제외하고 그룹에 속하는 모든 계정이 이러한 추가 그룹에서 제거됩니다.
- 계정 템플릿이 약한 동기화를 사용하는 경우, 계정이 **Staff** 및 **System** 그룹에 추가됩니다. 정의된 추가 그룹이 있는 모든 계정은 이러한 그룹의 구성원으로 남아 있습니다.

참고: 계정이 계정 템플릿과 동기화 상태를 유지할 수 있도록 템플릿과 계정을 정기적으로 동기화하십시오.

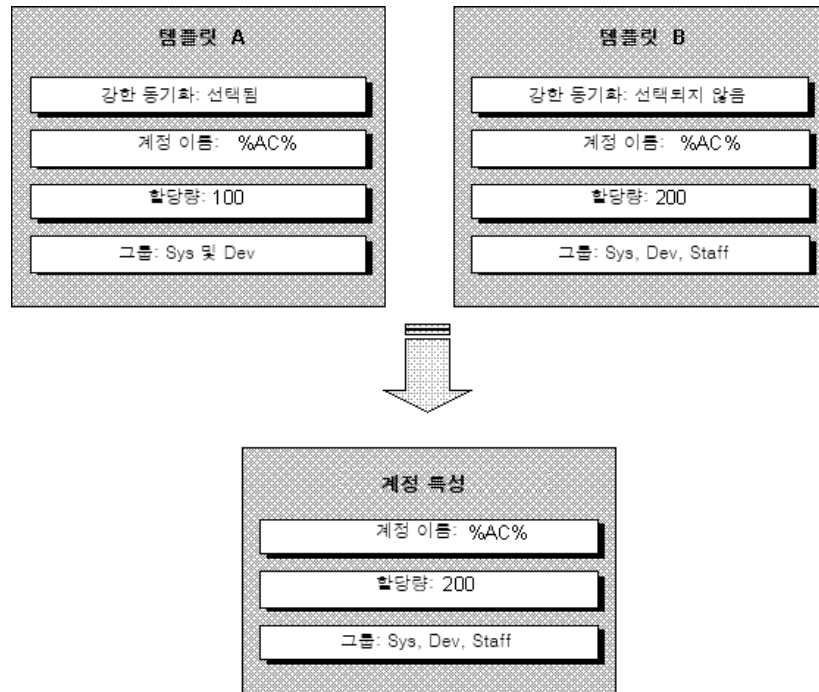
여러 템플릿이 있는 계정

동기화는 계정이 여러 계정 템플릿에 속하는지 여부에 영향을 받습니다. 계정에 단 하나의 계정 템플릿만 있고, 이 템플릿이 강한 동기화를 사용한다면 각 특성은 계정 템플릿 특성 값이 평가하는 것과 동일하게 일치하도록 업데이트됩니다. 결과는 특성이 초기 특성인 경우와 동일합니다.

사용자가 여러 프로비저닝 역할에 속하고, 각 역할이 동일한 관리 끝점에 대한 일부 액세스 수준을 규정하는 경우와 같이, 계정은 여러 계정 템플릿에 속할 수 있습니다. 이 경우, **CA Identity Manager** 는 개별 계정 템플릿의 하위 기능 집합을 규정하는 하나의 유효한 계정 템플릿으로 이러한 계정 템플릿을 결합합니다. 이 계정 템플릿은 개별 계정 템플릿이 약하거나 강한 동기화이거나 개별 계정 템플릿 중 하나가 강한 동기화인 경우 약한 동기화를 사용한다고 간주됩니다.

참고: 회사의 역할이 사용자가 필요로 하는 액세스를 완전히 정의하는지 여부에 따라 하나의 계정을 제어하는 계정 템플릿에 대해 약한 동기화만 사용하거나 강한 동기화만 사용하는 것이 일반적입니다. 사용자에게 적합한 역할이 명확하지 않고 사용자의 계정에 추가 기능을 부여하는 융통성이 필요한 경우 약한 동기화를 사용하십시오. 사용자가 필요로 하는 액세스를 정확히 지정하여 정의할 수 있으면 강한 동기화를 사용하십시오.

다음 예제는 여러 계정 템플릿이 하나의 유효한 계정 템플릿으로 통합되는 방법을 설명합니다. 이 예제에서 하나의 계정 템플릿이 약한 동기화로 표시되었고 다른 하나는 강한 동기화로 표시되었습니다. 따라서, 두 계정 템플릿을 결합하여 생성된 유효한 계정 템플릿은 강한 동기화 계정 템플릿처럼 처리됩니다. 정수 **Quota** 특성은 두 개의 계정 템플릿에서 더 큰 값을 취하고, 다중 값 **Groups** 특성은 두 정책 값의 합집합을 취합니다.



새 계정 전용 특성

계정 템플릿에서 일부 특성은 계정을 만들 때만 적용됩니다. 예를 들어, 암호 특성은 새 계정의 암호를 정의하는 규칙 식이며, 이 규칙 식은 계정의 암호를 업데이트하지 않습니다. 암호 규칙 식에 대한 변경 사항은 규칙 식이 설정된 후 생성된 계정에만 적용됩니다.

마찬가지로 읽기 전용 계정 특성에 대한 템플릿 규칙 식은 규칙 식이 설정된 후 생성된 계정에만 적용됩니다. 이러한 식을 변경해도 기존 계정에는 적용되지 않습니다.

문제 해결

다음 절은 보고와 관련된 문제 해결에 대해 설명합니다.

보고서를 보면 **Infoview** 로그인 페이지로 리디렉션됨

CA Identity Manager 에서 보고서를 볼 때 Business Objects Infoview 로그인 페이지로 리디렉션될 수도 있습니다.

리디렉션된 경우 보고서 보기

1. CA 보고서 서버(Business Objects)의 정규화된 도메인 이름을 사용하는지 확인합니다.
2. Infoview 로그인 웹 페이지를 마우스 오른쪽 단추로 클릭한 다음 "소스 보기"를 선택합니다.
3. 보고서에 대한 URL 을 찾습니다.
4. 이 URL 을 복사하여 새 브라우저 창에 붙여넣습니다.
5. 보고서를 볼 수 없으면 HTTP 추적 도구를 사용하여 자세한 정보를 확인합니다.
6. 보고서를 볼 수 있으면 다음 방법으로 브라우저 설정을 수정합니다.
 - 타사 쿠키를 허용합니다.
 - 세션 쿠키를 허용합니다.
 - 높은 보안 설정을 제거합니다.

20,000 개를 초과하는 레코드에 대해 사용자 계정 생성

레코드 수가 20,000 개를 초과하는 경우 사용자 계정 보고서를 생성하려면 일부 추가 단계가 필요합니다.

20,000 개를 초과하는 레코드에 대해 사용자 계정 보고서를 생성하려면

1. Business Objects Central Management 콘솔을 엽니다.
2. "Servers"(서버)를 선택하고 *servername.pageserver* 를 선택합니다.
3. "Database Records To Read When Previewing Or Refreshing a Report"(보고서를 검토 또는 갱신할 때 읽을 데이터베이스 레코드) 항목에 대해 "Unlimited"(제한 없음)를 선택합니다.
4. Crystal Reports 디자인어를 사용하여 사용자 계정 보고서를 엽니다.
5. "Database"(데이터베이스) > "Set Datasource Location"(데이터베이스 위치 설정)을 사용하여 스냅샷 데이터베이스에 대한 데이터베이스 위치를 지정합니다.
6. 이 변경 내용을 저장합니다.
7. "Database"(데이터베이스) > "Datasource Expert"(데이터 원본 내보내기)"를 사용하여 오른쪽 창에서 "Command"(명령)을 마우스 오른쪽 단추로 클릭합니다.

SQL 구문이 왼쪽에 표시되고 매개 변수 목록이 표시됩니다.

8. "Parameters Fields"(매개 변수 필드)에 표시된 그대로 매개 변수 이름을 보고서 템플릿에 입력합니다.
9. 왼쪽에서 쿼리를 변경하고 이 매개 변수를 쿼리에 추가합니다.

예를 들어, *reportid* 매개 변수가 있는 경우 쿼리는 다음과 같습니다.

```
Select * from endPointAttributes, endpointview, imreport6
where endPointAttributes.imr_endpointid = endpointview.imr_endpointid and
endPointAttributes.imr_reportid = endpointview.imr_reportid
    endpointview.imr_reportid = imreport6.imr_reportid and imreport6.imr_reportid
= {?reportid}
```

10. 보고서를 저장합니다.

제 15 장: 아이덴티티 정책

이 섹션은 다음 항목을 포함하고 있습니다.

[ID 정책](#) (페이지 489)

[보호 ID 정책](#) (페이지 514)

[ID 정책과 보호 ID 정책의 결합](#) (페이지 525)

ID 정책

ID 정책은 사용자가 특정 조건이나 규칙을 충족할 때 발생하는 일련의 비즈니스 변경 내용입니다. ID 정책 세트를 사용하여 다음 작업을 수행할 수 있습니다.

- 역할 및 그룹 구성원 자격 할당, 리소스 할당 또는 사용자 프로필 특성 수정과 같은 ID 관리 태스크를 자동화합니다.
- 직무 분리를 적용합니다. 예를 들어, 수표 서명자 역할의 구성원이 수표 승인자 역할을 갖지 못하도록 금지하고 회사의 모든 직원이 \$10,000 이상의 수표를 쓰지 못하도록 제한하는 ID 정책 세트를 만들 수 있습니다.
- 규정 준수를 적용합니다. 예를 들어, 특정 직함을 가지고 있으며 \$100,000 이상의 수입이 있는 사용자를 감사할 수 있습니다.
규정 준수를 적용하는 ID 정책을 *규정 준수 정책*이라고 합니다.

ID 정책과 연결된 비즈니스 변경에는 다음이 포함됩니다.

- 프로비저닝 역할을 비롯한 역할 할당 또는 해지(프로비저닝 디렉터리만 사용하는 경우)
- 그룹 구성원 자격 할당 또는 해지
- 사용자 프로필의 특성 업데이트

예를 들어, 회사에서 모든 부사장이 컨트리 클럽 구성원 그룹에 속하고 급여 승인자 역할을 갖도록 규정하는 ID 정책을 만들 수 있습니다. 사용자 직함이 부사장으로 변경되고 해당 사용자가 ID 정책과 동기화되면 CA Identity Manager 에서 이 사용자를 적절한 그룹과 역할에 추가합니다. 부사장이 CEO 로 승진되면 더 이상 부사장 ID 정책의 조건을 충족하지 않으므로 해당 정책에 의해 적용되는 변경이 해지되고 CEO 정책을 기반으로 하는 새 변경이 적용됩니다.

ID 정책을 기반으로 수행되는 변경 동작에는 워크플로 컨트롤을 적용하고 감사할 수 있는 이벤트가 포함되어 있습니다. 앞의 예에서 급여 승인자 역할은 구성원에게 상당한 권한을 부여합니다. 급여 승인자 역할을 보호하기 위해 회사에서 역할이 할당되기 전에 승인이 필요한 워크플로 프로세스를 만들 수 있으며, 역할 할당을 감사하도록 CA Identity Manager 를 구성할 수 있습니다.

ID 정책 관리를 단순화하기 위해 ID 정책은 ID 정책 세트로 그룹화되어 있습니다. 예를 들어, 부사장 및 CEO 정책은 임원 권한 ID 정책 세트에 포함될 수 있습니다.

참고: CA Identity Manager 에는 *예방적인 ID 정책* (페이지 514)이라고 하는 추가 유형의 ID 정책이 포함되어 있습니다. 관리자는 태스크가 제출되기 전에 실행되는 이 정책을 사용하여 권한을 할당하거나 프로필 특성을 변경하기 전에 정책 위반을 확인할 수 있습니다. 위반이 존재하는 경우 관리자가 태스크를 제출하기 전에 위반을 삭제할 수 있습니다.

ID 정책 세트 계획 워크시트

ID 정책 세트에는 하나 이상의 ID 정책이 포함됩니다. ID 정책 세트를 만들기 전에 다음 워크시트를 사용하여 세트의 각 ID 정책을 계획합니다.

질문	응답
ID 정책에 어떤 이름을 지정하시겠습니까?	
ID 정책이 어떤 사용자에게 적용됩니까?	
ID 정책을 사용자에게 적용할 때 CA CA Identity Manager 가 어떤 동작을 수행해야 합니까?	
사용자에게 적용된 ID 정책이 더 이상 적용되지 않는 경우 CA CA Identity Manager 가 어떤 동작을 수행해야 합니까?	
CA CA Identity Manager 가 ID 정책의 변경 사항을 여러 번 적용해야 합니까? 아니면 사용자가 정책의 조건을 처음 충족할 때만 한 번 적용합니까?	

정책 세트의 각 ID 정책에 대해 이 워크시트를 완료한 후 정책이 다른 정책과 충돌하지 않는지 확인합니다. 예를 들어, 특정 정책에서 다른 정책이 해지하는 권한을 부여하지 않는지 확인합니다.

ID 정책 세트 만들기

ID 정책 세트를 만들려면 "시스템 관리자" 역할 또는 "ID 정책 세트 만들기" 태스크가 포함된 역할을 가져야 합니다.

ID 정책 세트를 만들려면 다음 단계를 완료합니다.

1. [ID 정책 세트의 프로필 정의](#) (페이지 491)
2. [정책 세트 구성원 규칙 만들기](#) (페이지 492)
3. [ID 정책 만들기](#) (페이지 492)
4. [ID 정책 세트의 소유자 지정](#) (페이지 503)

참고: CA Identity Manager 환경에 대한 정책을 사용하려면 CA Identity Manager 관리 콘솔에서 ID 정책을 활성화하십시오. 자세한 내용은 *Configuration Guide*(구성 안내서)를 참조하십시오.

ID 정책 세트의 프로필 정의

"프로필" 탭을 사용하여 ID 정책 세트의 기본 속성을 정의할 수 있습니다.

ID 정책 세트 프로필을 정의하려면

1. 사용자 콘솔에서 "정책", "ID 정책 관리", "ID 정책 세트 만들기"를 선택합니다.

ID 정책을 관리할 수 있는 권한을 가진 사용자로 CA CA Identity Manager에 로그인되어 있어야 합니다. 기본 시스템 관리자 역할에는 이러한 권한이 포함됩니다.

2. 새 ID 정책 세트를 만들거나 기존 ID 정책 세트의 사본을 만들도록 선택합니다.

3. ID 정책 세트의 이름을 입력합니다.

4. ID 정책 세트의 범주를 입력합니다.

범주는 보고를 위해 목적이 비슷한 ID 정책 세트를 그룹화합니다. "범주" 필드는 필수입니다.

5. 선택적으로 ID 정책 세트에 대한 설명을 입력합니다.

6. ID 정책 세트를 사용 가능하도록 설정하지 않으려면 "사용" 확인란의 선택을 해제하십시오.
7. "프로필" 탭을 완료한 후에는 "정책" 탭을 선택하여 ID 정책 세트에 대한 ID 정책을 만드십시오.

정책 세트 구성원 규칙 만들기

정책 세트가 특정 사용자에게만 적용되도록 정책 세트에 대한 구성원 규칙을 만들 수 있습니다. 규칙은 세트의 ID 정책을 평가하기 전에 평가되어 상당한 시간을 절약할 수 있습니다. 예를 들어, 구성원 규칙이 ID 정책 평가를 사용자의 10 퍼센트로 제한하면 평가 시간의 90 퍼센트가 절약됩니다.

정책 세트 구성원 규칙을 만들려면

1. "정책" 탭을 선택합니다.
2. "정책 세트 구성원 규칙" 아래에서 "편집" 기호를 클릭합니다.
3. 특정 사용자에게만 정책을 적용하기 위한 규칙을 입력합니다.
4. "확인"을 클릭합니다.

추가 정보:

[ID 정책 만들기](#) (페이지 492)

ID 정책 만들기

ID 정책 세트의 프로필과 구성원 규칙을 정의한 후 해당 정책 세트의 ID 정책을 정의할 수 있습니다.

참고: 대규모 구현일 경우 ID 정책 규칙을 평가하는 데 오랜 시간이 걸릴 수 있습니다. 메모리 내 평가 옵션을 사용하여 사용자 특성이 포함된 규칙에 대한 평가 시간을 줄일 수 있습니다. 자세한 내용은 *Configuration Guide*(구성 안내서)를 참조하십시오.

ID 정책을 만들려면

1. "정책" 탭을 선택합니다.
2. "추가"를 클릭합니다.
3. ID 정책의 이름을 입력합니다.

4. 사용자가 처음 정책을 충족할 때 한 번만 정책을 적용해야 하는 경우 "한 번 적용" 확인란을 선택합니다.
5. "규정 준수" 확인란을 선택하여 이 정책에 규정 준수 정책으로 플래그를 지정합니다.
이 확인란을 선택한 경우
 - CA CA Identity Manager 가 규정 준수 정책과 동기화되지 않은 사용자에게 대한 보고서를 생성할 수 있습니다.
 - "정책 적용/제거 동작" 목록 상자에 "규정 준수 위반" 동작이 표시됩니다.
6. "정책 조건" 섹션에서 정책이 적용되는 사용자를 식별합니다.
7. "정책 적용 동작" 섹션에서 사용자에게 ID 정책을 적용할 때 CA CA Identity Manager 가 수행하는 동작을 정의합니다.
8. "정책 제거 동작" 섹션에서 사용자가 더 이상 ID 정책의 조건을 충족하지 않을 때 CA CA Identity Manager 가 수행하는 동작을 정의합니다.
9. "확인"을 클릭합니다.

참고: 만든 ID 정책 세트를 사용하기 전에 먼저 관리 콘솔에서 ID 정책을 사용하도록 설정해야 합니다. 자세한 내용은 *Configuration Guide*(구성 안내서)를 참조하십시오.

한 번 적용 설정

CA CA Identity Manager 는 "한 번 적용" 설정에 기초하여 ID 정책을 다르게 적용합니다.

한 번 적용 설정 사용 허용

"한 번 적용" 설정이 사용되는 경우 사용자가 정책에 정의된 조건을 처음 충족할 때 CA CA Identity Manager 가 ID 정책과 연결된 변경을 적용합니다. 정책과 연결된 변경 동작이 한 번만 수행됩니다. 따라서 정책이 이전에 적용된 경우 CA CA Identity Manager 가 정책 업데이트를 사용자에게 적용하지 않습니다.

사용자가 정책에 정의된 조건을 더 이상 충족하지 않으면 CA CA Identity Manager 가 정책의 제거 동작을 실행합니다.

"한 번 적용" 설정은 일반적으로 리소스를 프로비저닝할 때 사용됩니다. 예를 들어, 관리자에게 휴대폰을 할당하는 정책이 있을 수 있습니다. 사용자가 처음 관리자가 되면 휴대폰이 할당됩니다. CA CA Identity Manager 는 정책을 평가할 때마다 휴대폰을 발급하지 않고 한 번만 발급합니다. 새 휴대폰 모델을 포함하도록 휴대폰 정책을 업데이트하는 경우 CA CA Identity Manager 가 기존 관리자에게 새 휴대폰을 발급하지 않습니다.

참고: 리소스 프로비저닝은 CA CA Identity Manager 가 프로비저닝 서버와 통합되는 경우 사용할 수 있습니다.

한 번 적용 설정 사용 중지

"한 번 적용" 설정이 사용되지 않는 경우 ID 정책을 평가할 때마다 ID 정책과 연결된 변경 동작이 적용됩니다. 즉, CA CA Identity Manager 가 이전에 변경 동작이 적용되었는지 여부에 관계없이 정책의 조건을 충족하는 모든 사용자에게 대해 변경 동작을 적용합니다.

일반적으로 규정 준수를 적용하는 ID 정책에서는 "한 번 적용" 설정을 사용하지 않습니다. 예를 들어, 관리자의 지출 권한을 \$5,000 로 제한하는 ID 정책을 만들 수 있습니다. CA CA Identity Manager 가 지출 권한이 \$10,000 로 설정된 관리자를 발견하면 지출 권한을 \$5,000 로 재설정합니다. 관리자가 ID 정책과 동기화될 때마다 CA CA Identity Manager 가 지출 권한이 올바르게 설정되었는지 확인합니다.

사용자 프로필에 대한 수동 변경이 변경 동작과 충돌하는 경우 사용자를 정책과 동기화할 때 CA CA Identity Manager 가 변경을 덮어씁니다.

앞의 예에서 관리자의 지출 권한이 \$10,000 로 수동 증가된 경우 관리자를 정책과 동기화할 때 CA CA Identity Manager 가 지출 권한을 \$5,000 로 재설정합니다.

다음 표에는 "한 번 적용" 설정을 사용하거나 사용하지 않을 경우의 결과가 요약되어 있습니다.

"한 번 적용" 사용 여부 결과

활성화됨	■ ID 정책과 연결된 변경 동작이 한 번만 적용됩니다. ■ ID 정책이 적용된 후의 수동 변경이 유지됩니다. ■ CA CA Identity Manager 가 이전에 정책을 적용한 경우 ID 정책의 조건을 충족하는 사용자에게 업데이트가 적용되지 않습니다. ■ 사용자가 ID 정책의 조건을 더 이상 충족하지 않으면 CA CA Identity Manager 가 제거 동작을 실행합니다.
비활성화됨	■ 사용자를 정책과 동기화할 때마다 ID 정책과 연결된 변경 동작이 적용됩니다. ■ ID 정책을 적용할 때 수동 변경을 덮어씁니다. ■ 사용자를 동기화할 때 정책 업데이트가 적용됩니다. ■ 사용자가 ID 정책의 조건을 더 이상 충족하지 않으면 CA CA Identity Manager 가 제거 동작을 실행합니다.

정책 조건

정책 조건은 ID 정책이 적용되는 사용자 세트를 결정하는 규칙입니다.

다음 표에서는 사용 가능한 옵션에 대해 설명합니다.

구문	조건	예제
(모두)	ID 정책이 모든 사용자에게 적용됩니다.	
조건: <사용자-필터>	사용자가 하나 이상의 특성 값과 일치해야 합니다.	직책=관리자 및 지역=동부인 사용자

구문	조건	예제
다음에 속함: <조직-규칙>	사용자가 명명된 조직에 속해야 합니다. 참고: 이 옵션을 선택하면 새 목록 상자가 나타나 다음 옵션을 선택할 수 있습니다. ■ 조직:<조직> [및 하위] - 조직 검색 화면을 사용하여 조직을 선택하고, 선택적으로 조직의 자식 조직을 포함할 수 있습니다. ■ 다음에 해당하는 조직:<조직-필터> [및 하위] - 하나 이상의 조직을 선택하는 필터를 지정합니다.	영업 및 하위 조직 내 사용자
조건:<사용자-필터> 및 다음에 속해 있는 사람:<조직-규칙>	사용자가 특정 사용자 특성과 일치하고 특정 조직에 속해야 합니다.	직책=관리자 및 조직=영업*
다음의 구성원인 사람:<그룹-구성원-규칙>	사용자가 그룹의 특성에 의해 지정된 조건을 충족하는 그룹에 속해야 합니다. 참고: 이 옵션을 선택하면 새 목록 상자가 나타나 다음 옵션을 선택할 수 있습니다. ■ 그룹 <group> - 그룹 검색 화면을 사용하여 그룹을 선택할 수 있습니다. ■ 다음에 해당하는 그룹:<그룹-필터> - 하나 이상의 그룹을 선택하는 필터를 지정합니다.	소유자=CIO 인 그룹의 구성원인 사용자

구분	조건	예제
다음의 구성원인 사람: <역할-규칙>	사용자가 역할의 구성원이어야 합니다. 역할은 다음 중 하나일 수 있습니다. ■ 액세스 역할 ■ 관리자 역할 ■ 프로비저닝 역할 참고: 프로비저닝 역할을 사용하려면 CA CA Identity Manager 가 프로비저닝 서버와 통합되어야 합니다. 자세한 내용은 <i>Installation Guide</i>(설치 안내서)를 참조하십시오.	헬프 데스크 역할의 구성원인 사용자
다음의 관리자인 사람: <역할-규칙>	사용자가 역할의 관리자여야 합니다. 역할은 다음 중 하나일 수 있습니다. ■ 액세스 역할 ■ 관리자 역할 ■ 프로비저닝 역할 참고: 프로비저닝 역할을 사용하려면 CA CA Identity Manager 가 프로비저닝 서버와 통합되어야 합니다. 자세한 내용은 <i>Installation Guide</i>(설치 안내서)를 참조하십시오.	영업 관리자 역할의 관리자인 사용자

구분	조건	예제
다음의 소유자인 사람: <역할-규칙>	사용자가 역할의 소유자여야 합니다. 역할은 다음 중 하나일 수 있습니다. ■ 액세스 역할 ■ 관리자 역할 ■ 프로비저닝 역할 참고: 프로비저닝 역할을 사용하려면 CA CA Identity Manager 가 프로비저닝 서버와 통합되어야 합니다. 자세한 내용은 <i>Installation Guide</i>(설치 안내서)를 참조하십시오.	사용자 관리자 역할의 소유자인 사용자
쿼리 <LDAP-쿼리>에 의해 반환됨	사용자가 LDAP 쿼리를 기반으로 조건을 충족해야 합니다.	LDAP 쿼리의 조건을 충족하는 사용자입니다. 예: (departmentNumber=Accounts)
다음에 속함: <관리자-합집합-제약 조건>	사용자가 조건 목록에 있는 조건 중 하나 이상을 충족해야 합니다. 관리자 합집합 제약 조건에 다음 유형의 필터를 포함할 수 있습니다. ■ 액세스/관리자/프로비저 닝 역할의 구성원 ■ 액세스/관리자/프로비저 닝 역할의 관리자 ■ 액세스/관리자/프로비저 닝 역할의 소유자 ■ 그룹의 구성원	인증 관리자 역할의 구성원 또는 인증 관리자 역할의 소유자인 사용자

구문	조건	예제
다음에 속함: <관리자-교집합-계약 조건>	사용자가 조건 목록에 있는 모든 조건을 충족해야 합니다. 관리자 합집합 제약 조건에 다음 유형의 필터를 포함할 수 있습니다. ■ 액세스/관리자/프로비저 닝 역할의 구성원 ■ 액세스/관리자/프로비저 닝 역할의 관리자 ■ 액세스/관리자/프로비저 닝 역할의 소유자 ■ 그룹의 구성원	계약 초기자 역할 및 계약 승인자 역할의 구성원인 사용자

정책 적용/제거 동작

CA CA Identity Manager 에서 ID 정책을 평가할 때 실행할 변경 동작을 정의할 수 있습니다. 이러한 동작에는 다음이 포함됩니다.

정책 적용 동작

사용자가 정책 조건의 조건을 충족할 때 CA CA Identity Manager 에서 수행하는 일련의 동작입니다.

정책 제거 동작

사용자가 정책 조건의 조건을 더 이상 충족하지 않을 때 CA CA Identity Manager 에서 수행하는 일련의 동작입니다.

ID 정책이 적용 또는 제거될 때 CA CA Identity Manager 에서 수행할 수 있는 동작은 동일합니다. 자세한 내용은 다음 표를 참조하십시오.

변경 동작	설명
<그룹-이름> [...] 그룹에 추가	그룹에 사용자를 추가합니다. 이 옵션을 선택하면 원하는 그룹을 검색할 수 있는 화면이 나타납니다.

변경 동작	설명
사용자 조직의 <그룹-이름>에 추가	로컬 그룹에 사용자를 추가합니다. 이 옵션을 선택하면 원하는 그룹의 이름을 입력할 수 있는 텍스트 상자가 나타납니다.
<단일값-사용자-특성>을 <값>으로 설정	사용자 프로필에 특성 값을 설정합니다. 기존 값이 있으면 변경 동작에서 지정된 값으로 덮어씁니다.
<값>을 <다중값-사용자-특성>에 추가	다중값 사용자 특성에 값을 추가합니다. 이 옵션은 기존 값을 덮어쓰지 않습니다.
액세스 역할의 구성원 만들기	액세스 역할에 사용자를 할당합니다.
액세스 역할의 관리자 만들기	사용자를 액세스 역할의 관리자로 만듭니다.
관리자 역할의 구성원 만들기	사용자를 관리자 역할의 구성원으로 만듭니다.
관리자 역할의 관리자 만들기	사용자를 관리자 역할의 관리자로 만듭니다.
프로비저닝 역할의 구성원 만들기	사용자를 연결된 끝점 계정을 만드는 프로비저닝 역할의 구성원으로 만듭니다. 참고: 프로비저닝 역할을 사용하려면 CA CA Identity Manager 가 프로비저닝 서버와 통합되어야 합니다. 응용 프로그램 서버에 대한 <i>Installation Guide</i> (설치 안내서)를 참조하십시오.
프로비저닝 역할의 관리자 만들기	사용자를 프로비저닝 역할의 관리자로 만듭니다. 참고: 프로비저닝 역할을 사용하려면 CA CA Identity Manager 가 프로비저닝 서버와 통합되어야 합니다. 응용 프로그램 서버에 대한 <i>Installation Guide</i> (설치 안내서)를 참조하십시오.

변경 동작	설명
<그룹-이름> [...] 그룹에서 제거	그룹에서 사용자를 제거합니다. 이 옵션을 선택하면 원하는 그룹을 검색할 수 있는 화면이 나타납니다.
사용자 조직의 <그룹-이름>에서 제거	로컬 그룹에서 사용자를 제거합니다. 이 옵션을 선택하면 원하는 그룹의 이름을 입력할 수 있는 텍스트 상자가 나타납니다.
<값>을 <다중값-사용자-특성>에서 제거	다중값 사용자 특성에서 값을 제거합니다.
구성원을 액세스 역할에서 제거	액세스 역할을 해지합니다.
관리자를 액세스 역할에서 제거	특정 액세스 역할에 대한 관리자 권한을 해지합니다.
구성원을 관리자 역할에서 제거	관리자 역할을 해지합니다.
관리자를 관리자 역할에서 제거	특정 관리자 역할에 대한 관리자 권한을 해지합니다.
구성원을 프로비저닝 역할에서 제거	프로비저닝 역할을 해지합니다.
관리자를 프로비저닝 역할에서 제거	특정 프로비저닝 역할에 대한 관리자 권한을 해지합니다.
감사 메시지 보내기	만든 메시지를 감사 데이터베이스로 보냅니다. 이 메시지는 만든 보고서에 표시될 수도 있습니다.

변경 동작	설명
규정 준수 위반	만든 메시지를 감사 데이터베이스로 보냅니다. 규정 준수 보고서를 만드는 경우 ID 정책을 적용하거나 사용자로부터 제거할 때마다 이 메시지가 나타납니다. 감사에 대한 자세한 내용은 <i>Configuration Guide</i>(구성 안내서)를 참조하십시오. 참고: "규정 준수 위반" 옵션을 사용하려면 "ID 정책 세트"의 "프로필" 탭에 있는 "규정 준수" 확인란을 선택해야 합니다.
승인 (정책 적용 동작만)	예방적인 ID 정책 위반이 있을 때 태스크가 제출할 수 있도록 허용합니다. 이 동작을 선택한 경우 위반이 발생할 때 CA Identity Manager가 감사 데이터베이스에 기록하고 "제출한 태스크 보기"에 표시하는 메시지를 제공하십시오.
거부 (정책 적용 동작만)	ID 정책 위반이 발생한 경우 태스크가 제출하지 못하도록 방지합니다. 이 동작은 사용자가 이해의 충돌 또는 사기를 초래할 수 있는 권한을 받지 못하도록 방지하기 위해 예방적인 ID 정책과 함께 사용됩니다. 이 동작을 선택한 경우 위반이 발생할 때 CA Identity Manager에서 표시하는 메시지도 제공합니다. 메시지는 감사 데이터베이스에 저장되며 사용자 콘솔에 표시됩니다.

변경 동작	설명
경고 (정책 적용 동작만)	예방적인 ID 정책 위반이 발생할 때 해당 위반을 워크플로 승인 정책과 연결한 경우 워크플로 프로세스를 트리거합니다. 워크플로의 구성 여부에 관계없이 CA CA Identity Manager에서는 태스크가 제출할 수 있도록 허용합니다. 참고: 워크플로 프로세스를 예방적인 ID 정책에 연결하는 데 대한 정보는 워크플로 및 예방적인 ID 정책 (페이지 520)을 참조하십시오. 이 동작을 선택한 경우 위반이 발생할 때 CA CA Identity Manager에서 표시하는 메시지도 제공됩니다. 메시지는 감사 데이터베이스에 저장되며 "제출한 태스크 보기"에 표시됩니다.

추가 정보:

[보호 ID 정책](#) (페이지 514)

[워크플로 및 보호 ID 정책](#) (페이지 520)

아이덴티티 정책 세트의 소유자 지정

"소유자" 탭에서 아이덴티티 정책 세트의 소유자가 될 수 있는 사람에 대한 규칙을 정의합니다. 아이덴티티 정책 세트 소유자는 정책 세트에 대한 기본 정보를 수정할 수 있으며, 세트의 아이덴티티 정책을 추가, 변경 또는 제거할 수 있습니다.

"소유자" 탭을 완료하려면

1. 아이덴티티 정책 세트를 수정할 수 있는 사용자를 결정하는 소유자 규칙을 정의합니다.
2. "제출"을 클릭합니다.

ID 정책 세트 관리

CA CA Identity Manager 에는 ID 정책 세트를 관리하기 위한 다음 태스크가 포함되어 있습니다.

- ID 정책 세트 보기
- ID 정책 세트 수정
- ID 정책 세트 삭제

기본적으로 관리자가 이러한 태스크 중 하나를 사용하면 CA CA Identity Manager 가 해당 관리자가 소유자인 모든 ID 정책 세트의 목록을 표시합니다. 그런 다음 관리자는 목록에서 필요한 정책 세트를 선택할 수 있습니다.

많은 ID 정책 세트가 포함된 Identity Manager 환경에서는 ID 정책 세트를 목록에 표시하는 대신 관리자가 검색할 수 있도록 ID 정책 세트 보기, 수정 및 삭제 태스크를 사용자 지정할 수 있습니다.

이러한 태스크를 사용자 지정하려면

1. 사용자 콘솔에서 "역할 및 태스크", "관리자 역할", "관리자 태스크 수정"을 선택합니다.

"관리자 태스크 수정" 화면이 열립니다.

2. 사용자 지정할 태스크를 검색하여 선택합니다.
3. "범위" 탭에서 "모든 ID 정책 세트"를 선택합니다.

이 옵션을 선택하는 경우 CA CA Identity Manager 는 "기본 ID 정책 세트 검색" 화면 정의를 사용합니다.

4. "제출"을 클릭합니다.

사용자와 ID 정책의 동기화 방법

ID 정책을 사용하는 경우 CA CA Identity Manager 에서 정책을 평가하고 사용자에게 적용하는 방법을 이해하는 것이 중요합니다. 사용자 동기화 프로세스를 완전히 이해하지 않으면 예기치 않은 결과를 발생시키는 ID 정책 세트를 구성할 수 있습니다.

다음 절차는 CA CA Identity Manager 에서 ID 정책을 평가하고 적용하는 방법에 대해 설명합니다.

1. 사용자 동기화 프로세스가 시작됩니다.
 - 자동 - 사용자 동기화를 자동으로 트리거하도록 CA CA Identity Manager 태스크를 구성할 수 있습니다.
 - 수동 - 사용자 콘솔의 "사용자 동기화" 태스크를 사용하여 사용자를 동기화합니다.
2. CA CA Identity Manager 에서 사용자에게 적용할 ID 정책 세트를 확인합니다.
3. CA CA Identity Manager 에서 사용자에게 적용되는 ID 정책 세트를 이미 해당 사용자에게 적용한 정책 목록과 비교합니다.

참고: 사용자에게 적용된 정책 목록은 사용자 프로필의 잘 알려진 %IDENTITY_POLICY% 특성에 저장됩니다. 이 특성의 구성에 대한 자세한 내용은 *Configuration Guide*(구성 안내서)를 참조하십시오.

- ID 정책이 적용 가능한 정책 목록에 있고 이전에 해당 정책이 사용자에게 적용되지 않은 경우 CA CA Identity Manager 에서 이 정책을 할당 목록에 추가합니다.
 - ID 정책이 적용 가능한 정책 목록에 있고 이전에 해당 정책을 사용자에게 적용했으며 정책에 대해 "한 번 적용" 설정을 사용하지 않은 경우 CA CA Identity Manager 에서 이 정책을 재할당 목록에 추가합니다.
 - ID 정책이 적용 가능한 정책 목록에 없고, 해당 정책이 사용자에게 적용된 경우 이 사용자는 더 이상 정책 조건에 맞지 않습니다. CA CA Identity Manager 는 이러한 정책을 할당 취소 목록에 추가합니다.
4. CA CA Identity Manager 에서 사용자에 대한 모든 정책을 평가한 후 다음 순서대로 정책을 적용합니다.
 - a. 할당 취소 목록의 ID 정책
 - b. 할당 목록의 ID 정책
 - c. 재할당 목록의 ID 정책

5. ID 정책이 적용된 후 CA CA Identity Manager 는 정책을 재평가하여 첫 번째 동기화 프로세스(2-4 단계)에서 발생한 변경에 따라 추가 변경이 필요한지 여부를 확인합니다.

이것은 ID 정책 적용에 의한 변경에서 다른 ID 정책을 트리거하지 않았는지 확인하기 위한 것입니다.

6. CA CA Identity Manager 는 사용자가 적용 가능한 모든 정책과 동기화되거나 CA CA Identity Manager 가 관리 콘솔에서 정의된 최대 되풀이 수준에 도달할 때까지 계속해서 ID 정책을 재평가하여 적용합니다.

예를 들어, 사용자에게 역할이 할당되면 ID 정책이 해당 사용자의 부서를 변경할 수 있습니다. 새 부서가 다른 ID 정책을 트리거합니다. 그러나 재귀 수준이 1 로 설정되면 사용자가 다시 동기화될 때까지 후속 변경이 수행되지 않습니다.

재귀 수준 설정에 대한 자세한 내용은 관리 콘솔 온라인 도움말을 참조하십시오.

자동 사용자 동기화 구성

CA CA Identity Manager 에서 태스크 수명 주기의 여러 시점에 사용자 계정을 ID 정책과 자동으로 동기화할 수 있습니다.

CA CA Identity Manager 태스크는 태스크 처리 중에 발생하는 검색 가능한 활동인 이벤트를 생성합니다. 예를 들어, 기본 "사용자 만들기" 작업은 CreateUserEvent, AddUserToGroupEvent 및 AssignAccessRoleEvent 를 생성합니다. 태스크가 완료된 후 또는 각 이벤트가 완료될 때 사용자를 동기화하도록 CA CA Identity Manager 를 구성할 수 있습니다.

참고: [사용자와 아이덴티티 정책 동기화](#) (페이지 504) 섹션에서는 사용자 동기화 프로세스에 대한 추가 정보를 제공합니다.

사용자 동기화를 트리거하도록 작업을 구성하려면

1. 관리자 태스크를 수정할 수 있는 사용자로 CA CA Identity Manager 에 로그인합니다.
2. "역할 및 작업", "관리자 작업", "관리자 작업 수정"을 선택합니다.
CA CA Identity Manager 에서 검색 화면을 표시합니다.
3. 사용자 동기화를 트리거할 관리자 작업을 검색하여 선택합니다.

4. 작업의 "프로필" 탭에 있는 "사용자 동기화" 필드에서 다음 옵션 중 하나를 선택합니다.

- **끄기** - 이 작업은 사용자 동기화를 트리거하지 않습니다.
- **태스크 완료 시** - 모든 이벤트가 완료된 후 CA CA Identity Manager 에서 사용자 동기화 프로세스를 시작합니다. 이 설정은 "사용자 만들기", "사용자 수정" 및 "사용자 삭제" 작업의 기본 동기화 옵션입니다. 다른 모든 작업의 기본 설정은 "끄기"입니다.

참고: 여러 이벤트가 포함된 태스크에 대해 "태스크 완료 시" 옵션을 선택하면 태스크의 모든 이벤트가 완료될 때까지 CA CA Identity Manager 에서 사용자를 동기화하지 않습니다. 워크플로 승인이 필요한 이벤트가 하나 이상 있는 경우 모든 이벤트가 완료되는 데 며칠 정도 걸릴 수 있습니다. 모든 이벤트가 완료될 때까지 CA CA Identity Manager 에서 ID 정책을 적용하기 위해 대기하지 않도록 하려면 "모든 이벤트 발생 시" 옵션을 선택하십시오.

- **모든 이벤트 발생 시** - 태스크의 각 이벤트가 완료될 때 CA CA Identity Manager 에서 사용자 동기화 프로세스를 시작합니다.

동일한 사용자에게 주 이벤트와 보조 이벤트가 있는 작업의 경우 사용자 동기화를 "모든 이벤트 발생 시"로 설정하면 "작업 완료 시" 옵션이 선택된 경우보다 사용자에게 적용되는 정책에 대한 평가가 늘어날 수 있습니다.

수동으로 사용자 동기화

수동으로 사용자를 아이덴티티 정책 세트와 동기화하여 사용자 계정에 올바른 권한이 있는지 또는 컴플라이언스 정책을 준수하는지 확인할 수 있습니다.

CA CA Identity Manager 사용자 콘솔의 "사용자 동기화" 태스크를 사용하여 수동으로 사용자를 동기화할 수 있습니다.

참고: "사용자 동기화" 작업이 제대로 작동하려면 "사용자 동기화" 옵션을 "끄기"로 설정하고, "계정 동기화" 옵션을 "작업 완료 시" 또는 "모든 이벤트 발생 시"로 설정해야 합니다. 최상의 성능을 얻으려면 "작업 완료 시" 옵션을 선택합니다. 이러한 옵션은 "사용자 동기화" 작업의 "프로필" 탭에서 설정됩니다.

"사용자 동기화" 작업에는 다음 탭이 포함되어 있습니다.

- **현재 일치하는 정책** - "사용자 동기화" 태스크를 제출할 때 CA CA Identity Manager 에서 사용자에게 적용할 ID 정책 목록이 표시됩니다.

참고: "현재 일치하는 정책" 탭에는 "사용자 동기화" 작업에 액세스할 때 사용자에게 적용되는 아이덴티티 정책만 표시됩니다. 사용자를 이러한 정책과 동기화하면 다른 아이덴티티 정책을 트리거하는 변경이 발생할 수 있습니다. 새 정책을 검토할 때까지 CA CA Identity Manager 에서 새 정책을 적용하지 않도록 하려면 CA CA Identity Manager 관리 콘솔에서 ID 정책 세트의 되풀이 수준을 1 로 설정하십시오. "사용자 동기화" 작업을 제출한 후 다시 이 작업에 액세스하여 정책을 검토합니다.

- **정책이 이미 적용됨** - 이미 사용자에게 할당된 아이덴티티 정책 목록이 표시됩니다.
- **동기화 요약** - 사용자에게 적용되는 모든 아이덴티티 정책과 해당 정책에 대한 변경 동작이 표시됩니다.

사용자 계정을 동기화하려면

1. "사용자 동기화" 작업을 사용할 수 있는 사용자로 Identity Manager 에 로그인합니다. 기본적으로 "시스템 관리자" 역할을 가진 사용자는 이 작업을 사용할 수 있습니다.
2. "정책", "사용자 동기화"를 선택합니다.
"사용자 동기화" 작업이 열립니다.
3. "동기화 요약" 탭을 선택합니다.
4. CA CA Identity Manager 에서 사용자에게 적용할 정책 및 관련된 동작을 검토한 다음 "제출"을 클릭합니다.

사용자 동기화 확인

사용자를 아이덴티티 정책과 동기화할 때 적절한 변경이 수행되는지 확인하려면 "사용자 동기화" 작업의 "정책이 이미 적용됨" 탭을 확인합니다.

1. "사용자 동기화" 태스크를 사용할 수 있는 사용자로 CA CA Identity Manager 에 로그인합니다. 기본적으로 "시스템 관리자" 역할을 가진 사용자는 이 작업을 사용할 수 있습니다.
2. "정책", "사용자 동기화"를 선택합니다.
"사용자 동기화" 작업이 열립니다.

3. "정책이 이미 적용됨" 탭을 선택합니다.
4. CA CA Identity Manager 에서 사용자에게 적용한 정책 및 관련된 동작을 검토합니다.

Identity Manager 환경의 아이덴티티 정책 세트

다음 섹션에서는 아이덴티티 정책을 사용하는 여러 방법에 대해 설명합니다.

- [예: 자동으로 사용자 특성 채우기](#) (페이지 509)
- [예: 리소스 및 자격 할당](#) (페이지 510)
- [예: 컴플라이언스 적용](#) (페이지 511)
- [예: 업무 분리 적용](#) (페이지 512)

예: 자동으로 사용자 특성 채우기

아이덴티티 정책 세트를 사용하여 다른 특성값이나 사용자 자격을 기반으로 사용자 특성값을 자동으로 할당할 수 있습니다. 예를 들어, 사용자의 집 사무실을 기반으로 사용자의 메일 주소를 자동으로 채우는 아이덴티티 정책 세트를 만들 수 있습니다.

직원 주소에 대한 아이덴티티 정책 세트를 구성하려면 각 사무실 위치에 대해 다음 설정을 사용하여 아이덴티티 정책을 만듭니다.

설정	값
정책 조건	사무실 = <사무실 위치>
정책 적용 동작	주소 = <주소> 설정 시/군/구 = <시/군/구> 설정 시/도 = <시/도> 설정 우편 번호 = <우편 번호> 설정

다음 그림에서는 직원 주소 아이덴티티 정책 세트의 샘플 정책을 보여줍니다.

ID 정책

정책 세트

	정책 이름	정책 구성원 규칙	정책 적용 동작
	Boston	조건 (Office = "Boston")	Address을(를) 475# Rd(으)로 설정 City을(를) Boston(으)로 설정 State을(를) MA(으)로 설정 Postal code을(를) 10021(으)로 설정
	NY	조건 (Office = "NY")	Address을(를) 106# RD(으)로 설정 City을(를) NY(으)로 설정 State을(를) NY(으)로 설정 Postal code을(를) 10017(으)로 설정

예: 리소스 및 자격 할당

사용자가 정책 조건을 충족할 때 아이덴티티 정책에서 도메인 계정과 같은 리소스를 자동으로 할당하거나, 사용자를 역할의 구성원으로 만들기와 같이 자격을 부여할 수 있습니다. 예를 들어, 사용자의 직함을 기반으로 리소스와 역할을 할당하는 아이덴티티 정책 세트를 만들 수 있습니다.

리소스 및 역할을 할당하기 위한 아이덴티티 정책 세트를 만들려면 조직의 각 직함에 대해 다음 설정을 사용하여 아이덴티티 정책을 만듭니다.

설정	값
정책 조건	직함 = <직함>
정책 적용 동작	정책 조건을 충족하는 사용자에게 리소스나 자격을 할당하는 모든 동작입니다. 예를 들면 다음과 같습니다. ■ <그룹>의 구성원 만들기 ■ <관리자 역할> 관리자 역할의 구성원 만들기 ■ <프로비저닝 역할> 프로비저닝 역할의 구성원 만들기

설정	값
정책 제거 동작	사용자가 더 이상 정책 조건을 충족하지 않는 경우 리소스나 자격을 제거하는 모든 동작입니다. 예를 들어, 아이덴티티 정책이 적용될 때 Identity Manager 가 사용자를 역할의 구성원으로 만든 경우 사용자가 더 이상 정책 조건을 충족하지 않을 때 역할을 해지하도록 Identity Manager 를 구성할 수 있습니다.

다음 그림에서는 직원 리소스 아이덴티티 정책 세트의 샘플 정책을 보여줍니다.

ID 정책 정책 세트

정책 이름	정책 구성원 규칙	정책 적용 동작	정책 제거 동작
 매니저	조건 (Title = "매니저")	사용자 매니저 관리자 역할의 구성원 만들기 Us-P 프로비저닝 역할의 구성원 만들기	구성원을 사용자 매니저 관리자 역할에서 제거
 HR	조건 (Title = "HR")	UsM 관리자 역할의 구성원 만들기 Us-G 그룹에 추가 Us-P 프로비저닝 역할의 구성원 만들기	Us-G 그룹에서 제거 구성원을 Us-M 관리자 역할에서 제거 구성원을 Us-P 프로비저닝 역할에서 제거

예: 규정 준수 적용

있거나 없어야 하는 조건을 정의하고, 이러한 조건 평가를 기반으로 특정 동작을 수행하도록 ID 정책을 구성할 수 있습니다. 예를 들어, 관리자의 지출 제한을 \$5,000 로 규정하는 규정 준수 정책을 정의할 수 있습니다. 관리자의 지출 제한이 \$10,000 이면 CA CA Identity Manager 가 관리자의 지출 제한을 재설정하고 감사 목적을 위해 규정 준수 위반을 기록할 수 있습니다.

지출 제한 적용을 위해 규정 준수 정책 세트를 만들려면 다음 설정을 사용하여 ID 정책을 만듭니다.

설정	값
한 번 적용	사용할 수 없음
규정 준수	활성화됨

설정	값
정책 조건	규정 준수 또는 규정 준수 위반을 정의하는 모든 조건입니다. 예를 들면 다음과 같습니다. 직함=<직함> 및 지출 제한 > <지출 제한>
정책 적용 동작	정책 조건이 적용될 때 CA CA Identity Manager 가 수행해야 하는 동작입니다. 예를 들면 다음과 같습니다. ■ 규정 준수 위반 메시지: 지출 제한 초과 ■ 지출 제한을 <값>으로 설정

다음 그림은 이 예에서 설명하는 샘플 규정 준수 정책을 보여 줍니다.

ID 정책

정책 세트

	정책 이름	정책 구성원 규칙	정책 적용 동작
	매니저	조건 (Title = "매니저" 그리고 Spending Limit > "5000")	규정 준수 위반 메시지: 지출 한도는 limit 5000 에게 초과

예: 업무 분리 적용

아이덴티티 정책은 함께 사용할 수 없고 동일한 사용자에게 동시에 부여할 수 없는 역할을 정의할 수 있습니다. 예를 들어, 급여를 인상할 수 있는 사용자 관리자가 급여 승인자가 되지 못하도록 할 수 있습니다.

업무 분리를 적용하는 아이덴티티 정책 세트를 만들려면 다음 설정을 사용하여 아이덴티티 정책을 만듭니다.

설정	값
한 번 적용	사용할 수 없음
컴플라이언스	사용

설정	값
정책 조건	"다음에 속함: <관리자-교집합-계약 조건>" 옵션을 사용하여 비즈니스 정책을 위반하는 조건 세트를 정의합니다. 사용자가 모든 조건을 충족하면 Identity Manager 가 "정책 적용 동작" 필드의 동작을 수행합니다. 예를 들어, 다음과 같이 정책 조건을 설정합니다. 교집합 (다음의 구성원인 사람: <역할>) 및 다음의 구성원인 사람: <기타 역할>)
정책 적용 동작	정책 조건이 적용될 때 Identity Manager 가 수행해야 하는 동작입니다. 예를 들면 다음과 같습니다. ■ 컴플라이언스 위반 메시지: 사용자에게 함께 사용할 수 없는 역할이 있습니다. ■ 구성원을 <역할>에서 제거

다음 그림에서는 이 예의 아이덴티티 정책을 보여 줍니다.

ID 정책

정책 세트

	정책 이름	정책 구성원 규칙	정책 적용 동작
	제한	교집합 (다음의 구성원인 사람: (관리자 역할 "사용자 매니저") 그리고 다음의 구성원인 사람: (관리자 역할 "사용자 승인자"))	규정 준수 위반 메시지: 사용자가 상호 배타적인 권리를 가지고 구성원을 사용자 승인자 관리자 역할에서 제거

보호 ID 정책

보호 ID 정책은 사용자가 이해의 충돌 또는 사기 행위를 유발할 수 있는 권한을 받지 못하도록 방지하는 ID 정책 유형입니다. 이 정책은 회사의 업무 분리(SOD) 요구 사항을 지원합니다.

관리자는 태스크가 제출되기 전에 실행되는 보호 ID 정책을 사용하여 권한을 할당하거나 프로필 특성을 변경하기 전에 정책 위반을 확인할 수 있습니다. 위반이 존재하는 경우 관리자가 태스크를 제출하기 전에 위반을 삭제할 수 있습니다.

예를 들어, 회사에서 "사용자 관리자" 역할을 맡은 사용자가 "사용자 승인자" 역할도 맡지 못하도록 금지하는 보호 ID 정책을 만들 수 있습니다. 이 경우 관리자가 "사용자 수정" 태스크를 사용하여 "사용자 매니저"에게 "사용자 승인자" 역할을 부여하면 CA Identity Manager 에서 위반 메시지를 표시합니다. 관리자는 태스크를 제출하기 전에 위반을 삭제하기 위해 역할 할당을 변경할 수 있습니다.

다음 변경 사항에 대해 보호 ID 정책을 만들 수 있습니다.

- **역할 구성원 자격**

사용자가 특정한 여러 역할을 동시에 갖지 못하도록 방지합니다.

예를 들어, 사용자는 "사용자 관리자"와 "사용자 승인자" 역할을 동시에 가질 수 없습니다.

- **역할 관리자**

사용자가 다른 역할의 관리자인 경우 특정 역할의 관리자가 될 수 없도록 방지합니다.

예를 들어, 사용자는 동시에 "사용자 관리자"와 "사용자 승인자" 역할의 관리자가 될 수 없습니다.

- **사용자 특성**

사용자가 특정한 프로필 특성을 동시에 갖지 못하도록 방지합니다.

예를 들어, 사용자는 "선임 회계사" 직책을 가지고 IT 부서에 속할 수 없습니다.

- **조직 특성**

특정 조직에서 사용자 프로필이 만들어지지 않도록 방지합니다.

예를 들어, 관리자는 "공급자" 조직에서 직원 프로필을 만들 수 없습니다.

■ 그룹 특성

사용자가 특정 그룹의 구성원이 될 수 없도록 방지합니다.

예를 들어, 사용자는 "프로젝트 팀" 그룹 및 "회계 그룹"의 구성원이 될 수 없습니다.

추가 정보:

[보호 ID 정책 위반에 대한 동작](#) (페이지 515)

보호 ID 정책 위반에 대한 동작

보호 ID 정책이 비즈니스 변경 사항에 적용되는 경우 CA 는 위반을 처리하기 위해 특정 동작을 수행합니다.

이 동작 중 하나를 ID 정책에 지정할 경우 위반 내용을 설명하는 메시지를 지정합니다. 이 메시지는 감사 데이터베이스에 기록됩니다. 메시지는 또한 동작 유형에 따라, 사용자 콘솔의 사용자에게 표시되고 "제출한 태스크 보기"에 기록될 수도 있습니다.

보호 ID 정책에 대해 다음 동작을 구성할 수 있습니다.

승인

CA CA Identity Manager 가 "제출한 태스크 보기"에 위반 내용을 설명하는 메시지를 표시하지만 태스크가 제출될 수 있도록 허용합니다.

거부

CA CA Identity Manager 가 사용자 콘솔에 메시지를 표시하고 태스크가 제출되지 못하도록 금지합니다.

경고

CA CA Identity Manager 가 사용자 콘솔과 "제출한 태스크 보기"에 메시지를 표시합니다. 이 동작은 CA CA Identity Manager 가 태스크를 실행하기 전에 적절한 사용자의 승인을 필요로 하는 워크플로 프로세스를 선택적으로 트리거할 수 있습니다.

워크플로 프로세스를 트리거하려면 위반을 유발할 수 있는 태스크의 [정책 기반 워크플로 프로세스에 보호 ID 정책을 연결](#) (페이지 522)하십시오.

예를 들어, 사용자가 동시에 특정 역할을 받을 때 위반이 발생하면 해당 역할을 사용자에게 할당하는 모든 태스크에 대해 워크플로 프로세스를 구성하십시오.

참고: 태스크에 대해 정책 기반 워크플로 프로세스를 구성하는 경우 승인 규칙이 보호 ID 정책의 이름을 참조해야 합니다.

보호 ID 정책의 작동 방식

다음의 샘플 프로세스는 보호 ID 정책의 작동 방식을 보여 줍니다.

1. ID 정책 관리자가 "선임 회계사" 직책을 가진 사용자가 IT 부서에 속할 수 없도록 금지하는 보호 ID 정책을 만듭니다.

이 ID 정책을 정의할 때 관리자는 **CA CA Identity Manager**가 이 정책을 위반하는 모든 변경 사항을 거부해야 한다고 지정합니다.

2. 인사 관리자가 "사용자 만들기" 태스크를 사용하여 새 "선임 회계사"에 대한 사용자 프로필을 만듭니다. 인사 관리자가 사용자의 직책은 올바르게 선택했지만, 실수로 IT 부서를 선택합니다.

3. 인사 관리자가 "사용자 만들기" 태스크의 나머지 필드를 완료하고 "제출"을 클릭합니다.

4. **CA CA Identity Manager**가 ID 정책에 정의된 변경 사항이 태스크에 포함되어 있다는 것을 감지하고 변경 사항의 위반 여부를 평가합니다.

5. **CA CA Identity Manager**가 위반을 감지하고, 인사 관리자에게 메시지를 표시하고, 태스크가 제출되지 못하도록 방지합니다.

CA CA Identity Manager는 또한 메시지를 감사 데이터베이스에 기록합니다.

6. 인사 관리자가 메시지의 상세한 위반 정보를 보고 사용자 부서를 "재무"로 변경합니다. 그런 다음, 관리자가 태스크를 다시 제출합니다.
7. **CA CA Identity Manager**가 제안된 변경 사항을 해당되는 모든 ID 정책에 대해 평가한 다음 "사용자 만들기" 태스크 제출을 허용합니다.

보호 ID 정책에 대한 중요한 참고 사항

보호 ID 정책을 구현하기 전에 다음 사항을 참고하십시오.

- 보호 ID 정책은 현재 태스크에서 제안된 변경 사항으로 인해 발생하는 위반만 방지합니다. 기존 위반은 방지하지 않습니다.

예를 들어, 한 회사에서 사용자가 "사용자 관리자"와 "사용자 승인자" 역할을 동시에 갖지 못하도록 금지하는 보호 ID 정책을 만듭니다. 관리자가 이미 "사용자 관리자"와 "사용자 승인자" 역할을 가지고 있는 사용자에게 "그룹 관리자" 역할을 할당합니다. CA CA Identity Manager 는 이 변경 사항이 정책 위반을 직접 유발하지 않기 때문에 새 역할의 할당을 허용합니다.

- 여러 개의 보호 ID 정책이 제안된 변경 사항에 적용되는 경우 CA CA Identity Manager 는 거부 동작을 가진 정책을 먼저 적용합니다.
- 보호 ID 정책 조건에 동적 그룹을 지정하지 마십시오. 정책 조건에 따라 보호 ID 정책이 적용되는 사용자 집합이 결정됩니다.

예를 들어, 한 회사에서 직책이 "관리자"인 모든 사용자를 포함하는 동적 그룹을 가지고 있습니다. 이 회사는 또한 "관리자" 그룹의 구성원이 "계약자" 역할을 갖지 못하도록 금지하는 보호 ID 정책을 만듭니다.

관리자가 "계약자" 역할을 가지고 있는 사용자의 직책을 "관리자"로 변경합니다. 이 변경 사항에 따라 태스크가 성공적으로 제출된 후 사용자가 "관리자" 그룹의 구성원이 됩니다. 그러나 CA CA Identity Manager 가 정책을 평가할 때 사용자의 직책이 "관리자"가 아니기 때문에 위반이 감지되지 않습니다.

- 보호 ID 정책의 정책 조건에서 역할 소유자 필터와 LDAP 쿼리 필터가 지원되지 않습니다.

보호 ID 정책 만들기

보호 ID 정책을 만들기 전에 ID 정책을 논리적으로 구분하는 ID 정책 세트를 만듭니다.

참고: 시작하기 전에 [보호 ID 정책에 대한 중요한 참고 사항](#) (페이지 517)을 참조하십시오.

보호 ID 정책 세트를 만들려면

1. 사용자 콘솔에서 "정책", "ID 정책 세트 만들기"를 엽니다.
새로운 ID 정책 세트를 만들거나 기존 ID 정책 세트를 템플릿으로 사용합니다.
2. "프로필" 탭에서 [ID 정책 세트의 프로필을 정의합니다](#) (페이지 491).
3. "정책" 탭에서 [정책 세트 구성원 규칙을 만듭니다](#) (페이지 492).
4. 다음과 같이 보호 ID 정책을 만듭니다.

- a. "추가"를 클릭합니다.
- b. ID 정책의 이름을 입력합니다.

참고: "한 번 적용"과 "규정 준수" 설정은 보호 ID 정책에 적용되지 않습니다.

- c. "정책 조건" 섹션에서 정책이 적용되는 사용자를 식별합니다.

참고: 보호 ID 정책에 대해 역할 소유자 필터와 LDAP 쿼리 필터가 지원되지 않습니다.

- d. "정책 적용 동작" 필드에서 CA CA Identity Manager 가 정책 위반을 감지했을 때 CA CA Identity Manager 에서 수행할 동작을 정의합니다.

승인

CA CA Identity Manager가 "제출한 태스크 보기"에 위반 내용을 설명하는 메시지를 표시하지만 태스크가 제출될 수 있도록 허용합니다.

거부

CA CA Identity Manager가 사용자 콘솔에 메시지를 표시하고 태스크가 제출되지 못하도록 금지합니다.

경고

CA CA Identity Manager가 사용자 콘솔과 "제출한 태스크 보기"에 메시지를 표시합니다. 이 동작은 선택적으로 [워크플로 프로세스를 트리거](#) (페이지 520)할 수 있습니다.

이 동작 중 하나를 선택하면 위반이 발생할 때 나타나는 메시지를 지정할 수 있는 텍스트 상자가 표시됩니다.

- e. 텍스트 상자에 메시지를 지정합니다.

참고: 사용자 콘솔을 한글화하는 경우 메시지 필드에 텍스트 대신 리소스 키를 지정할 수 있습니다. 리소스 키에 대한 자세한 내용은 *User Console Design Guide*(사용자 콘솔 디자인 안내서)를 참조하십시오.

- f. 필요에 따라 동작을 추가하고 "확인"을 클릭합니다.

5. [ID 정책 세트의 소유자 지정](#) (페이지 503)

참고: 만든 ID 정책 세트를 사용하기 전에 먼저 관리 콘솔에서 ID 정책을 사용하도록 설정해야 합니다. 자세한 내용은 *Configuration Guide*(구성 안내서)를 참조하십시오.

사용 사례: 사용자가 상충되는 역할을 갖지 못하도록 방지

Forward, Inc.에서는 자사 직원들이 "사용자 관리자" 역할과 "사용자 승인자" 역할을 동시에 갖지 못하도록 방지하려고 합니다. 이러한 두 가지 역할을 모두 가지고 있는 직원들은 급여와 같은 사용자 특성을 수정하고 부적절하게 승인할 수 있습니다.

이러한 상황을 방지하기 위해 Forward, Inc.에서는 "사용자 관리자"와 "사용자 승인자" 역할을 가진 사용자에게 적용되는 보호 ID 정책을 만듭니다. 관리자가 사용자에게 이러한 역할을 부여하려고 시도하면 CA CA Identity Manager 에서 태스크 제출을 거부하고 위반 내용을 설명하는 메시지를 표시합니다.

이 사용 사례를 지원하려면 다음과 같이 보호 ID 정책을 구성하십시오.

- 만들려는 정책에 대한 ID 정책 세트를 만듭니다.
- 다음 설정으로 보호 ID 정책을 만듭니다.
 - 정책 조건:

다음 사용자에게 이 정책 적용:

사용자 교직원 ()

다음의 구성원인 사람: ()

관리자 역할 사용자 승인자)

그리고 다음의 구성원인 사람: ()

관리자 역할 사용자 관리자)

- 정책 적용 동작:
 - 메시지와 함께 거부: 사용자는 "사용자 승인자" 및 "사용자 관리자" 역할의 구성원일 수 없습니다

워크플로 및 보호 ID 정책

경고를 실행하도록 보호 ID 정책이 구성된 경우, 위반을 트리거할 수 있는 태스크에 대해, ID 정책과 관련된 태스크 수준 정책 기반 워크플로 프로세스를 정의할 수 있습니다. 예를 들어, ID 정책에서 "선임 회계사"가 IT 부서의 구성원이 될 수 없도록 금지하는 경우, "사용자 만들기" 및 "사용자 수정" 태스크에 대한 태스크 수준 정책 기반 워크플로 프로세스를 정의하십시오.

태스크 수준 정책 기반 워크플로의 결과로 생성되는 모든 작업 항목은 CA CA Identity Manager 에서 태스크를 실행하기 전에 승인되어야 합니다. 승인자는 사용자 콘솔에 로그인할 때 작업 목록 항목을 봅니다. 승인자가 작업 목록 항목을 클릭할 때 위반 내용을 설명하는 경고 메시지가 포함된 승인 태스크가 표시됩니다. 승인자는 위반을 기준으로 태스크를 승인하거나 거부할 수 있습니다.

정책 기반 워크플로 프로세스는 정책 이름에 의해 보호 ID 정책과 관련됩니다.

추가 정보:

[정책 기반 워크플로](#) (페이지 345)

승인 태스크의 ID 정책 위반

보호 ID 정책이 태스크에 대한 워크플로 프로세스와 관련된 경우 CA CA Identity Manager 가 해당 승인자에 대한 작업 목록 항목을 생성합니다. 이러한 승인자는 승인 태스크를 사용하여 정책 위반을 트리거한 변경 사항을 승인하거나 거부합니다.

기본 승인 태스크에는 ID 정책 위반을 나열하는 섹션이 포함됩니다. 제안된 변경 사항이 여러 개의 보호 ID 정책을 트리거한 경우 두 가지 이상의 위반이 있을 수 있습니다.

각 위반의 상태는 다음과 같습니다.

- **평가 보류**

CA CA Identity Manager 가 태스크에 대한 승인 규칙의 평가를 아직 시작하지 않았습니다. 이 상태가 초기 상태입니다.

- **대기 중인 승인**

CA CA Identity Manager 가 승인 규칙에 정의된 ID 정책과 일치하는 경우를 찾아 관련된 워크플로 프로세스를 트리거했습니다.

- **승인됨**

승인자가 제안된 변경을 승인했습니다. 보호 ID 정책 위반을 트리거한 변경 사항이 생성됩니다.

- **거부됨**

승인자가 제안된 변경을 거부했습니다. 태스크가 거부됩니다.

- **구성된 워크플로가 없습니다**

이 위반에 대해 구성된 워크플로 프로세스가 없습니다. 태스크가 어떠한 승인도 필요 없이 실행됩니다.

보호 ID 정책에 대해 워크플로를 구성하는 방법

ID 정책 위반을 트리거할 수 있는 변경 사항을 포함하는 관리자 태스크에서 보호 ID 정책에 대해 워크플로를 구성하십시오.

예를 들어, 보호 ID 정책이 사용자가 특정 관리자 역할을 동시에 갖지 못하도록 금지하는 경우 보호 ID 정책에 대한 워크플로를 지원하기 위해 관리자 역할을 할당하는 태스크를 구성하십시오.

참고: 워크플로를 구성하기 전에 다음 설정을 사용하여 보호 ID 정책을 만드십시오.

- 고유한 정책 이름

워크플로 프로세스가 정책 이름으로 보호 ID 정책과 관련되기 때문에 정책 이름은 모든 ID 정책 세트에 걸쳐 고유해야 합니다.

여러 개의 보호 ID 정책이 같은 이름을 갖는 경우 여러 워크플로 프로세스가 적용될 수 있습니다.

- 정책 적용 동작 필드의 경고

경고는 워크플로 프로세스를 트리거할 수 있는 유일한 동작입니다.

보호 ID 정책을 구성한 후 정책 위반을 트리거할 수 있는 태스크를 결정하십시오. 그런 다음, 이러한 태스크에 대해 [워크플로 승인 정책을 만드십시오](#) (페이지 523).

보호 ID 정책에 대해 워크플로 승인 정책 만들기

관리자 태스크에 대해 태스크 수준 정책 기반 워크플로 프로세스를 구성할 수 있습니다. 이 워크플로 프로세스에는 보호 ID 정책을 워크플로와 연결할 수 있는 하나 이상의 승인 정책이 포함됩니다. 관련된 보호 ID 정책의 위반이 발생할 때 CA CA Identity Manager 에서 워크플로를 실행합니다.

참고: 태스크 수준 정책 기반 워크플로 프로세스에 대해 자세한 내용은 [정책 기반 워크플로](#) (페이지 345)를 참조하십시오.

보호 ID 정책에 대해 워크플로 승인 정책 만들기

1. 보호 ID 정책의 위반을 트리거할 수 있는 변경을 허용하는 관리자 태스크를 수정하십시오.

예를 들어, 사용자가 "사용자 관리자"와 "사용자 승인자" 역할을 가지고 있기 때문에 ID 정책 위반이 발생하면 관리자가 "사용자 만들기", "사용자 수정", "관리자 역할 구성원/관리자 수정"과 같은 역할을 할당할 수 있도록 허용하는 관리자 태스크를 수정하십시오.
2. 워크플로 프로세스를 추가하려면 태스크에 대한 "프로필" 탭에서 "워크플로 프로세스" 필드 옆의 편집 아이콘을 클릭합니다.

"태스크 수준 워크플로 구성" 화면이 나타납니다.
3. "정책 기반"을 선택한 다음 "추가"를 클릭합니다.
4. "승인 규칙" 섹션에서 "ID 정책 위반" 개체를 선택합니다.
5. "ID 정책" 필드에서 어떤 ID 정책이 승인 정책과 관련된 워크플로를 트리거하는지 결정하는 필터를 선택합니다.

필터에 ID 정책 세트 이름이 아닌 ID 정책 이름을 포함합니다.
6. 필요에 따라 "규칙 평가", "정책 순서" 및 "정책 설명" 필드를 구성합니다.
7. 워크플로 프로세스를 선택한 다음 "확인"을 클릭합니다.

워크플로 프로세스를 선택할 때 추가 필드가 표시됩니다.
8. 필요에 따라 승인 태스크와 승인자를 지정합니다.

워크플로 프로세스가 보호 ID 정책과 연결됩니다.

사용 사례: 직책 승인

Forward, Inc.의 회사 정책에는 모든 관리자는 정규직이어야 한다고 명시되어 있습니다. 그러나 Forward, Inc.에서는 최근 특수 프로젝트를 위해 많은 계약자를 고용했습니다. 이러한 특수 프로젝트를 효율적으로 수행하기 위해 일부 계약자에게는 관리자 직책이 주어질 예정입니다. Forward, Inc.에서는 관리자가 계약자에게 관리자 직책을 할당할 수 있도록 허용하기 전에 인사 담당 이사의 승인을 받으려고 합니다.

이러한 상황에서 승인 프로세스를 자동화하기 위해 Forward, Inc.에서는 사용자 직책이 "관리자"이고 사용자 조직이 "계약자"인 경우를 감지하는, "계약자를 위한 관리자 직책"이라는 보호 ID 정책을 만듭니다. Forward, Inc.에서는 또한 "사용자 수정" 태스크에서 정책 기반 승인 프로세스를 구성합니다. 이 승인 프로세스는 "계약자를 위한 관리자 직책" 정책이 위반될 때 트리거됩니다.

관리자가 계약자의 직책을 "관리자"로 변경하는 경우 CA CA Identity Manager 는 경고 메시지를 표시하고, 인사 담당 이사에게 승인을 받기 위해 작업 항목을 보냅니다. 작업 항목이 승인될 때까지 계약자의 직책은 변경되지 않습니다.

이 사용 사례에 대해 지원을 구성하려면 CA CA Identity Manager 에서 다음 작업을 완료하십시오.

- 다음 설정을 사용하여 "계약자를 위한 관리자 직책"이라는 보호 ID 정책을 만듭니다.
 - 정책 조건: 직책 = "관리자" 및 조직 = "계약자"인 사용자
 - 정책 적용 동작: "관리자는 정규직이어야 합니다"라는 메시지와 함께 경고
- 다음 설정을 사용하여 "사용자 수정" 태스크를 워크플로 프로세스를 포함하도록 수정합니다.
 - 워크플로 프로세스: 정책 기반
 - 승인 규칙 개체: ID 정책 위반
 - ID 정책: 이름 = "계약자를 위한 관리자 직책"
 - 워크플로 프로세스: SingleStepApproval

ID 정책과 보호 ID 정책의 결합

업무 분리(SOD) 요구 사항을 처리하기 위해 ID 정책과 보호 ID 정책을 결합할 수 있습니다. 이 경우, ID 정책은 기존 SOD 위반을 처리하고 보호 ID 정책은 새 위반을 금지합니다.

이 사용 사례를 지원하기 위해 다음 두 가지 동작 유형을 갖는 ID 정책 세트를 구성하십시오.

- 사용자 동기화 중에 발생하는 동작

이 동작을 수행하면 사용자 특성, 그룹 및 역할 구성원, 관리자 또는 소유자가 변경됩니다. 예를 들어, 이 유형의 동작은 위반이 감지된 경우 역할에서 사용자를 제거할 수 있습니다.

이 동작은 태스크가 제출될 때 적용되지 않는다는 점에서 예방적인 동작과 다릅니다. 이 동작은 [사용자 동기화](#) (페이지 504) 중에만 적용됩니다.

- 예방적인 동작

이 동작은 태스크가 제출되기 전에 보호 ID 정책 위반이 발생할 때 CA CA Identity Manager 에서 실행할 동작을 결정합니다. CA CA Identity Manager 는 태스크 제출을 허용하거나 경고를 실행하고 워크플로 프로세스를 트리거하거나 태스크가 제출되지 않도록 방지할 수 있습니다.

각 경우마다 위반은 감사 데이터베이스에 기록됩니다.

한 회사에서 사용자가 동시에 "인사 관리자"와 "급여 승인자"의 역할을 갖는 것을 방지하려고 합니다. 이 회사는 다음 두 가지 정책 적용 동작을 갖는 ID 정책을 만듭니다.

- 급여 승인자 역할에서 사용자 제거

이 동작은 CA CA Identity Manager 에서 사용자를 ID 정책과 동기화할 때 발생합니다.

이 경우, 이 회사는 "사용자 수정" 태스크에 대한 사용자 동기화를 구성했습니다. 관리자가 사용자를 수정할 때 CA CA Identity Manager 에서 적용 가능한 모든 ID 정책을 평가하고 동작을 적용합니다. 이 예제에서 CA CA Identity Manager 는 "인사 관리자" 역할과 "급여 승인자" 역할을 갖는 사용자를 "급여 승인자" 역할에서 제거합니다.

- 태스크 거부

이 예방적인 동작은 관리자가 태스크를 제출하도록 허용하지 않음으로써 관리자가 두 가지 역할을 한 사람에게 할당하지 못하도록 금지합니다.

참고: 두 가지 동작을 갖는 ID 정책을 구성할 때는 각 동작이 충돌하지 않는지 확인하십시오. 예를 들어, 사용자가 "관리자"와 "계약자" 역할을 갖지 못하도록 방지하는 ID 정책을 구성할 수 있습니다. 이 정책에서는 다음 두 가지 동작을 지정합니다.

- 역할을 할당하기 전에 승인이 필요한 워크플로 프로세스를 트리거하는 경고
- 사용자를 "관리자" 역할에서 제거하는 동작

승인자가 "관리자" 및 "계약자" 역할에 대한 역할 할당을 승인하지만, 두 번째 동작은 사용자 동기화가 발생할 때 사용자를 "관리자" 역할에서 제거합니다.

제 16 장: Policy Xpress

이 섹션은 다음 항목을 포함하고 있습니다.

[Policy Xpress 개요](#) (페이지 527)

[정책을 만드는 방법](#) (페이지 528)

Policy Xpress 개요

Policy Xpress 를 사용하면 사용자 지정 코드를 개발할 필요 없이 CA Identity Manager 에서 복합 비즈니스 로직(정책)을 만들 수 있습니다. 그러나 Policy Xpress 정책 만들기에 관련된 개념은 매우 복잡하고 세심한 고려와 계획을 필요로 합니다. CA Identity Manager 포털 화면을 사용하는 관리자는 필요한 비즈니스 로직 중 가장 정교한 것조차도 구현하도록 Policy Xpress 내의 정책을 구성할 수 있습니다. 비즈니스 정책이 바뀌면 개발자가 기본 코드를 변경할 필요 없이, 특히 CA Identity Manager 서비스를 다시 시작하지 않고 적절한 변경 관리 절차를 통해 관리자가 CA Identity Manager 내의 구성 화면을 사용하여 정책을 수정할 수 있습니다.

참고: Policy Xpress 에 대한 자세한 내용은 [Policy Xpress Wiki](#) (Policy Xpress 위키)를 참조하십시오.

정책을 만드는 방법

Policy Xpress 를 사용하여 정책을 만들려면 정책의 다음과 같은 기본 요소를 정의하십시오.

프로필

정책 유형과 우선 순위를 정의하고 간편한 관리를 위해 유사한 정책을 하나의 그룹으로 묶을 수 있습니다.

이벤트

정책이 실행될 때를 정의하십시오.

참고: 이벤트 매개 변수는 주의하여 설정하십시오. 데이터 손실을 방지하고 성능을 높이기 위해 비즈니스 로직은 특정 시간에 실행되어야 합니다. 예를 들어, 사용자가 생성될 때 사용자를 활성화하는 설정이 발생해야 합니다. 이 로직이 어느 때나 실행되면 비활성화되어야 할 사용자 계정이 다시 활성화될 수도 있습니다. 다른 예는 특정 시스템에 대한 액세스를 부여하는 프로비저닝 역할을 사용자에게 제공하는 것입니다. 이 역할은 다른 역할이 할당되고 승인된 이후에만 사용자에게 할당되어야 합니다. Policy Xpress 를 사용하면 사용자 지정 어댑터와 유사하게 이벤트 및 비즈니스 로직 태스크 처리기 처리 중 비즈니스 로직을 활성화할 수 있습니다. 따라서 ID 정책과 달리, 로직은 태스크가 시작할 때뿐만 아니라 언제든지 트리거될 수 있습니다.

데이터(데이터 요소)

정책에서 사용되는 데이터를 지정합니다. 비즈니스 로직의 모든 유형은 작동하기 위해 일부 데이터가 필요합니다. 이러한 데이터는 의사 결정을 하거나 보다 복잡한 데이터를 만드는 데 사용될 수 있습니다. Policy Xpress 는 데이터를 수집하기 위해 많은 개별 구성 요소를 제공합니다. 이러한 구성 요소는 *데이터 요소*라고 합니다. 데이터 요소의 한 예는 사용자의 특성 값입니다. 예를 들어, Policy Xpress 는 사용자의 이름을 수집하여 나중에 사용하기 위해 데이터 요소로 저장할 수 있습니다.

진입 규칙

실행 전에 반드시 충족되어야 하는 요구 사항을 정의합니다. 진입 규칙을 정의하면 Policy Xpress 가 정책을 평가하는 시기를 지정할 수 있으므로 정책을 단순화하고 성능을 개선할 수 있습니다. 진입 규칙의 한 예로는 이름 또는 성이 변경된 *경우에만* 전체 이름 설정 정책을 실행하는 것입니다.

동작 규칙

수집된 정보를 기반으로 수행된 동작을 정의합니다. 예를 들어, 사용자의 부서 이름을 기반으로 Policy Xpress 는 사용자를 다른 역할에 할당하거나 다른 계정 값을 지정할 수 있습니다.

동작

수행할 작업을 지정합니다. 프로세스의 끝에서 Policy Xpress 는 비즈니스 로직에서 필요한 동작을 수행합니다. Policy Xpress 는 동작 규칙을 여러 동작에 연결하는 방식으로 작동하므로 규칙이 일치하면 동작이 수행됩니다. 동작은 사용자 또는 계정에 대한 특성 값 할당, 명령줄 실행, SQL 명령 실행, 새 이벤트 생성을 포함합니다.

프로필

Policy Xpress 정책의 프로필 탭은 정책을 관리하고 정책 기능을 자세히 기술하는 필드를 포함하고 있습니다.

참고: 정책은 정책이 생성된 환경에만 적용됩니다. 예를 들어, neteauto 환경에 로그인한 동안 정책을 만들면 이 정책은 neteauto 환경에 대해서만 실행됩니다.

정책을 만들 때 다음과 같은 프로필 정보를 제공하십시오.

정책 이름

정책의 고유 이름을 정의합니다.

정책 유형

정책을 트리거하는 [수신기](#) (페이지 531)를 정의합니다. 각 정책 유형은 다른 구성을 갖습니다.

참고: 정책이 저장된 다음에는 이 필드를 변경할 수 없습니다.

범주

관련된 정책의 그룹을 정의합니다. 이 필드에서는 쉬운 관리를 위해 정책을 그룹화할 수 있습니다.

설명

정책의 설명을 지정합니다.

우선 순위

하나의 이벤트에 대해 실행되는 정책이 여러 개인 경우 이 필드는 언제 정책이 실행되는지를 지정합니다. 정책은 각각의 우선 순위에 따라 실행됩니다. 숫자가 낮을수록 우선 순위는 더 높습니다(우선 순위 1 이 가장 먼저 실행되고 10 은 두 번째, 50 은 세 번째 등의 순서).

정책이 서로에게 종속성이 있거나 복잡한 정책을 두 개의 단순한 정책으로 나누려고 하거나 정책이 순차적으로 실행되는 경우 우선 순위를 지정하면 유용합니다.

예를 들어, 데이터베이스에 특정 값이 있으면 실행되는 3 개의 정책이 있습니다. 각 정책이 데이터베이스의 값을 확인하도록 하는 대신 다른 3 개의 정책 이전에 실행되어 값을 확인하는 하나의 정책을 만들 수 있습니다. 새 정책이 필요한 값과 일치하는 경우 Policy Xpress 는 변수를 설정할 수 있습니다. 다른 3 개의 정책은 해당 변수가 설정된 경우에만 실행되므로 데이터베이스에 대한 중복 액세스를 방지합니다.

사용

정책이 CA CA Identity Manager 에서 활성화되어 있는지 여부를 지정합니다. 이 확인란의 선택을 지우면 정책을 삭제하지 않고 비활성화할 수 있습니다.

한 번 실행

정책을 한 번만 실행할지 여부를 지정합니다. 일부 정책은 조건을 충족할 때마다 실행해야 하는 반면, 다른 정책은 한 번만 실행해도 됩니다. 이 값은 이전에 이미 실행된 동작 규칙이 다시 실행되어야 하는지 여부를 결정합니다.

예를 들어, 부서를 기준으로 SAP 역할을 사용자에게 추가하는 동작은 사용자가 해당 부서와 일치하는 첫 번째 경우에만 발생해야 하는 동작입니다. 또한, 직급을 기반으로 사용자의 급여 수준을 설정하는 정책은 권한이 없는 사람이 변경할 수 없도록 한 번만 실행되도록 설정되지 않습니다.

참고: "한 번 실행" 옵션은 개체에 적용되며 전체적으로 적용되지 않습니다.

수신기

Policy Xpress 정책은 시스템에서 발생하는 요인으로 인해 트리거됩니다. 이 기능을 구현하려면 시스템과 통합되는 수신기가 Policy Xpress 에게 언제 이벤트가 발생했는지를 알리고 발생한 이벤트에 대한 자세한 정보를 제공해야 합니다.

사용 가능한 수신기는 다음과 같습니다.

이벤트

시스템의 모든 이벤트와 이벤트와 관련된 모든 상태(이전, 승인됨, 거부됨 등)를 수신합니다. 이 수신기는 또한 이벤트의 이름을 Policy Xpress 에 보고합니다. 이벤트 수신기에 대해 다음과 같은 상태를 사용할 수 있습니다.

- 이전
- 거부됨
- 승인됨
- 다음 이후
- 실패

UI

동기화된 상태 중(즉, 사용자가 열린 태스크에 대한 사용자 인터페이스를 아직 가지고 있는 동안)에 시스템에서 실행되는 다른 태스크를 수신합니다. UI 수신기에 대해 다음과 같은 상태를 사용할 수 있습니다.

- 시작—태스크가 시작할 때
- 제목 설정—기본 개체를 찾을 수 있을 때
- [변경 내용의 유효성 검사](#) (페이지 532)—"변경 내용의 유효성 검사" 플래그를 사용하여 설정된 특성이 변경될 때
- 제출 시 유효성 검사—제출 단추를 클릭할 때
- 제출—태스크가 제출될 때

워크플로

승인자를 찾은 워크플로 프로세스를 수신합니다. 이 수신기는 승인자에게 전자 메일을 보내는 것과 같이 승인자에 기반한 로직을 수행할 때 유용합니다.

제출된 태스크

백그라운드로 실행되고 있지 않은 제출된 태스크를 수신합니다. 이 수신기는 이벤트 수신기와 유사하지만 태스크의 이벤트가 아닌 태스크 전체로서 태스크를 간주합니다. 제출된 태스크 수신기에 대해 다음과 같은 상태를 사용할 수 있습니다.

- 태스크 시작됨
- 태스크 완료
- 태스크 실패

역방향 동기화

CA CA Identity Manager 의 탐색기 기능과 관련된 시스템에서 알림을 수신합니다.

화면 특성 유효성 검사

정의된 트리거(정책 유형)에 추가로, Policy Xpress 는 또한 특성에 대한 유효성 검사를 수신할 수도 있습니다. 이렇게 하면 "변경 내용의 유효성 검사"로 플래그된 화면 특성이 업데이트될 때 실행할 수 있는 정책을 만들 수 있습니다.

이 기능은 종속 드롭다운 목록을 만들기 위해 사용될 수 있습니다. 예를 들어, 화면에 두 개의 드롭다운 목록이 있는 경우 Policy Xpress 는 첫 번째 드롭다운 옵션이 선택된 경우 실행되고, 그런 다음 첫 번째 드롭다운 목록에서 선택된 옵션을 기준으로 두 번째 드롭다운 목록에 대한 값을 설정합니다. 드롭다운 목록 및 다른 화면 갱신은 숫자 제한 없이 무제한 수행할 수 있습니다. 이것은 정적 옵션의 XML 파일을 가져오는 대신 임의의 로직을 사용하여 채워지는 드롭다운 옵션을 허용하므로 "선택란 데이터"와 다릅니다.

다른 용도는 한 특성의 값을 기준으로 다른 특성을 채우는 것입니다. 예를 들어, 관리자가 부서를 선택할 때 Policy Xpress 는 부서 관리자, 부서 번호, HR 부서 코드와 같은 기타 특성을 자동으로 채울 수 있습니다. 이렇게 하면 논리적 특성 처리기 사용자 지정 코드를 작성할 필요가 없습니다.

Policy Xpress 정책을 사용하여 유효성 검사를 구성하려면

1. 사용자 콘솔에서 태스크의 프로필 화면을 수정하고 수신할 필드를 선택합니다.
2. 필드의 속성에 액세스하여 "변경 내용의 유효성 검사"에 대한 드롭다운 목록에서 "예"를 선택합니다.

3. Policy Xpress 에서 '[UI](#) (페이지 531)' 유형의 정책을 만듭니다.
4. "이벤트 시 실행" 탭에서 "변경 내용의 유효성 검사" 상태와 1 단계에서 수정한 태스크를 선택합니다.

사용 사례: 부적절한 이름 검사

새 사용자가 생성될 때 사용자 이름이 부적절한지 여부를 검사할 필요가 있습니다. 다음 프로세스는 Policy Xpress 정책을 사용하여 부적절한 이름을 검사하는 방법에 대해 설명합니다.

1. "사용자 만들기" 태스크의 프로필 화면에 있는 적절한 필드가 "변경 내용의 유효성 검사 = 예"로 설정되어 있어야 합니다.
2. Policy Xpress 에서 'UI' 유형의 정책을 만듭니다.
3. "이벤트 시 실행" 탭 아래에서 '변경 내용의 유효성 검사'와 "새 사용자 만들기" 태스크를 선택합니다.
4. 이름을 검사하는 다음 데이터 요소를 만듭니다.
 - 이름 특성(특성, 사용자 특성, 가져오기) 가져오기
 - 이름을 모두 소문자로 구문 분석(일반, 문자열 파서, 소문자로)
 - 데이터베이스 테이블에 있는 부적절한 단어가 이름에 있는지 검사(데이터 원본, SQL 쿼리 데이터)
5. 성을 검사하기 위해 4 단계와 유사한 데이터 요소를 만듭니다.
6. 다음과 같이 동작 규칙을 만듭니다.
 - 조건—이름이 ""와 같지 않음(쿼리에서 이름이 부적절하다는 메시지가 반환된 경우 발생)
 - 동작—부적절한 이름을 나타내는 메시지(메시지, 화면 메시지)

이 규칙은 사용자가 "사용자 만들기" 태스크를 다시 제출하기 전에 이름을 변경하도록 강제합니다.
7. 성에 대해 6 단계와 유사한 동작 규칙을 만듭니다.

이벤트

프로필 탭에서 선택한 정책 유형에 따라 정책이 평가될 시간을 설정하는 활성화 시간을 구성할 수 있습니다. 예를 들어, "이벤트" 유형의 정책은 CreateUserEvent 전에 평가를 위해 설정될 수 있습니다. "태스크" 유형의 정책은 DisableUserEvent 의 제목 설정에서 평가를 위해 설정될 수 있습니다.

활성화 시간을 구성하려면 다음 필드를 선택해야 합니다.

시/도

정책을 활성화하는 이벤트와 관련된 시간 또는 동작을 지정합니다. 예를 들어, 정책은 이벤트가 발생하기 전에 실행하도록 설정할 수 있습니다.

이벤트 이름

CreateUserEvent 와 같이 정책을 활성화하는 이벤트를 지정합니다.

정책에는 여러 개의 활성화 시간이 있을 수 있습니다. 시스템에서 지정된 활성화 시간(상태 및 이벤트)이 발생할 때마다 Policy Xpress 는 이 활성화 시간이 있는 모든 정책을 검색하고 순서에 따라 각 정책을 평가합니다.

참고: 정책이 시스템에서 발생하는 활성화 시간과 일치해도 이것이 정책이 자동으로 실행되는 것을 의미하지는 않습니다. 프로세스에서 나중에 평가된 규칙 조건은 정책이 완료되었는지 여부를 결정합니다.

데이터 요소

데이터 요소는 정책 데이터를 만드는 데 사용됩니다. 정책은 정책에서 사용되는 정보를 나타내는 여러 데이터 요소를 포함할 수 있습니다.

Policy Xpress 는 데이터 요소 정보를 수집하기 위해 융통성 있는 플러그 인을 사용합니다. 각 플러그 인은 작은 전용 작업을 수행할 수 있습니다. 하지만 여러 플러그 인을 함께 사용하여 보다 복잡한 정책을 만들 수 있습니다. 데이터 요소 플러그 인의 예로는 사용자 특성 요소가 있습니다. 이 요소의 목표는 사용자 프로필의 일부인 특정 특성에 대한 정보를 수집하는 것입니다.

데이터 요소는 호출되었을 때 계산됩니다. 즉, 규칙이 데이터 요소를 사용하고 있거나 계산이 필요한 또 다른 요소가 매개 변수로서 데이터 요소를 사용하고 있습니다.

예를 들어, SQL 쿼리 데이터 요소는 테이블에서 값을 검색할 수 있지만 사용자의 부서가 쿼리를 만들어야 합니다. 이 경우 부서 데이터 요소는 SQL 쿼리 데이터 요소 전에 실행되어야 하며 그 이후에 [값이 매개 변수로 사용될 수 있습니다](#) (페이지 537).

다음 필드가 데이터 요소를 정의합니다.

이름

데이터 요소를 설명하는 이름을 정의합니다. 일부 데이터 요소는 예를 들어 데이터베이스에서 정보를 가져오거나 변수를 가져오는 것과 같이 복잡합니다. 데이터 요소 관리를 쉽게 하려면 의미 있는 이름을 선택하십시오.

범주

데이터 요소의 그룹화를 제공합니다. 이 필드는 데이터 요소를 정렬하고 선택을 쉽게 해 줍니다.

유형

자체 전용 용도를 함께 데이터 요소 유형을 지정합니다. 이 필드는 선택한 범주에 기반합니다.

함수

동일한 데이터의 가능한 변수를 정의합니다. 대부분의 데이터 요소는 Get 함수만 지원합니다.

예를 들어, 사용자 특성 데이터 요소는 다음 함수를 갖습니다.

- Get—특성의 값을 반환합니다.
- is multi valued—값이 다중 값인 경우 true 를 반환합니다.
- is logical—값이 논리 값인 경우 true 를 반환합니다.

함수 설명

함수의 이미 입력된 설명을 제공합니다. 선택한 각 함수는 그 용도와 기대되는 값에 대한 각각의 다른 설명을 제공합니다.

매개 변수

데이터 요소에 전달된 매개 변수를 정의합니다. 데이터 요소는 동적이며 매개 변수에 따라 다른 일을 할 수 있습니다. 사용자 특성 데이터 요소는 선택한 특성에 따라 다른 결과를 반환합니다. 하위 유형 옵션은 또한 매개 변수 수, 이름, 가능한 경우 선택적 값을 정의합니다.

필요한 경우 매개 변수를 추가할 수 있습니다. SQL 쿼리 예제는 데이터 원본 및 쿼리의 두 가지 필요한 매개 변수를 받습니다. 쿼리는 값을 대체될 "?"를 사용할 수 있습니다(준비된 구문과 유사). 매개 변수를 추가하면 이러한 값을 설정할 수 있습니다.

참고: Policy Xpress 에서 데이터 요소를 볼 때 '사용 중'이란 제목의 열이 있습니다. 이 열의 확인 표시는 데이터 요소가 규칙 또는 동작 매개 변수에 의해 사용되거나 다른 데이터 요소에 대한 매개 변수로 사용되고 있음을 의미합니다.

데이터 또는 동작 요소에서 동적 값 사용

동적 값은 계산된 데이터 요소의 결과이며 그 값은 런타임 중에만 결정됩니다. 이러한 값은 다른 데이터 요소의 매개 변수(우선 순위에 따라 차후에 계산됨)로 사용될 수 있습니다.

동적 값을 데이터 요소에 대한 매개 변수로 사용하려면

1. "정책 데이터" 탭에서 동적 값을 설정할 매개 변수를 찾습니다.
2. 빈 텍스트 필드에서 일반 텍스트를 입력하거나 오른쪽 드롭다운 목록에서 동적 값을 선택합니다.
3. "확인"을 클릭합니다.

변수

Policy Xpress에는 동작을 사용하여 설정되고 데이터 요소로 저장된 변수가 있습니다(변수 범주). 변수는 동시에 실행되는 모든 정책에서 공유되므로 설정된 변수는 우선 순위가 더 낮은 다른 정책에서 사용될 수 있습니다.

예를 들어, 변수는 정책에 의해 한 번 계산된 다음 이 값을 다시 계산할 필요가 없는 다른 정책 사이에서 공유되는 값을 포함할 수 있습니다. 최초 정책은 변수에 값을 설정하며, 나중에 실행되는 정책은 변수 이름을 매개 변수로 갖는 데이터 요소를 사용하여 이 값을 읽습니다.

변수는 또한 다른 정책에 대해 트리거될 수 있습니다. 이 경우 이전 정책이 실행된 경우에만 정책이 실행됩니다.

진입 규칙

진입 규칙은 정책이 언제 실행되어야 할지에 대한 조건을 정의합니다. 이러한 조건은 정책의 데이터 요소에서 수집된 값을 사용합니다.

정책에는 여러 진입 규칙이 있을 수 있으며, 하나의 진입 규칙에 여러 조건이 있을 수 있습니다. 진입 규칙은 반드시 하나 이상 일치해야 합니다. 즉, 동작 규칙으로 이동하기 위해 해당 진입 규칙의 모든 조건이 정책에 대해 일치해야 합니다.

다음 필드는 진입 규칙을 정의합니다.

이름

진입 규칙의 이름을 제공합니다.

설명

진입 규칙의 의미를 정의합니다.

조건

일치할 조건을 지정합니다.

참고: 진입 규칙의 조건은 둘 사이에 항상 AND 연산자가 있어야 합니다.

추가 정보:

[조건](#) (페이지 538)

조건

진입 규칙 및 동작 규칙에 조건이 사용되며 다음 구성 요소로 구성됩니다.

- 정책 데이터
- 연산자
- 값

예를 들어, 사용자의 부서가 변경되었는지 여부를 확인하는 조건을 만들려고 합니다. 먼저, "변경된 부서" 데이터 요소를 만든 다음 조건에서 "변경된 부서" 데이터 요소를 선택하고, 연산자를 "같음"으로 설정하고, 값을 True 로 설정합니다.

추가 정보:

[진입 규칙](#) (페이지 537)

[동작 규칙](#) (페이지 538)

동작 규칙

동작 규칙은 구조상 진입 규칙과 유사하지만 기능상 차이가 있습니다. 동작 규칙은 언제 동작이 수행되어야 할지를 정의합니다. 예를 들어, 사용자의 부서가 "영업부"로 변경되었을 때 정책이 동작을 수행하도록 하려면 '부서 = 영업부'일 때 정의하는 동작 규칙을 만드십시오.

또한 하나의 진입 규칙을 일치하는 대신 여러 동작 규칙이 일치시킬 수 있습니다. 가장 높은 우선 순위(0 이 가장 높음)를 갖는 하나의 동작 규칙이 *유일하게* 사용됩니다.

동작 규칙은 또한 하나 이상의 동작을 포함하며, 동작은 동작 추가와 동작 제거로 구분됩니다.

다음 필드는 동작 규칙을 정의합니다.

이름

동작 규칙의 이름을 제공합니다. 이 이름은 고유해야 합니다.

설명

동작 규칙의 의미를 정의합니다.

조건

일치할 조건을 지정합니다.

우선 순위

여러 동작 규칙이 일치하는 경우 실행할 동작 규칙을 정의합니다. 이 필드는 기본 동작을 정의할 때 유용합니다. 예를 들어, 각각 부서 이름에 대한 여러 규칙이 있는 경우 조건 없이 규칙을 추가하지만 우선 순위를 낮게 지정(예를 들어, 다른 모두가 5 일 때 10 으로 설정)하여 기본값을 설정하는 것이 가능합니다. 일치하는 부서 규칙이 없는 경우 이 기본값이 사용됩니다.

동작 추가

규칙이 일치할 때 수행한 동작의 목록을 정의합니다. 예를 들어, 사용자의 부서가 조건에 구성된 한 규칙과 일치하는 경우 특정 **Active Directory** 그룹을 추가하도록 지시하는 규칙을 구성할 수 있습니다. 동작 규칙은 "한 번 실행" 설정에 따라 다르게 동작합니다. 정책이 한 번 실행하도록 설정된 경우 연결된 동작은 규칙이 처음 일치할 때 수행됩니다. 동작은 각 이후 일치하는 각 규칙에 대해 다시 수행되지 않습니다. 위의 예제에서 **Active Directory** 그룹은 사용자에게 한 번만 추가되었습니다. "한 번 실행"이 설정되지 않으면 동작은 규칙이 일치하는 한 다시 실행됩니다. 이 필드는 값을 시행하는 데 있어 중요합니다.

동작 제거

규칙이 더 이상 일치하지 않을 때 수행할 동작의 목록을 정의합니다. 예를 들어, 이전 예제는 부서를 기준으로 **Active Directory** 그룹을 사용자에게 추가했습니다. 부서가 변경되면 제거 동작이 이 **Active Directory** 그룹을 제거합니다.

추가 정보:

[조건](#) (페이지 538)

동작

동작은 모든 의사 결정이 수행된 이후에 비즈니스 로직을 수행합니다. 동작은 끝을 제외하고 데이터 요소에 대해 비슷하게 작동합니다. 동작이 실행될 때 동작은 값을 반환하는 대신 태스크를 수행합니다.

참고: 동작은 사용자 콘솔에 표시되는 순서로 실행됩니다.

다음 필드는 동작을 정의합니다.

동작 이름

동작의 용도를 정의합니다.

범주

동작의 그룹화를 제공합니다. 이 필드는 동작을 정렬하고 선택을 쉽게 해 줍니다.

유형 및 함수

수행한 동작의 유형 및 함수를 정의합니다.

참고: 유형 및 함수에 대한 자세한 내용은 "데이터"를 참조하십시오.

함수 설명

함수의 이미 입력된 설명을 제공합니다. 선택한 각 함수는 그 용도와 기대되는 값에 대한 각각의 다른 설명을 제공합니다.

매개 변수

동작에 전달된 매개 변수를 정의합니다.

흐름 제어

기본적으로 정책은 우선 순위로 정렬된 다음 차례로 평가됩니다. 이 흐름 제어는 거의 항상 그대로 사용되지만 필요한 경우 흐름을 변경할 수 있습니다.

이 흐름 변경 기능은 다른 동작 규칙에 연결될 수 있는 동작에 의해 제공됩니다. 흐름 제어 기능은 동작의 "시스템" 범주 아래에 있습니다.

중요! 프로세스 흐름을 변경할 때는 주의하십시오. 이러한 동작을 사용할 때 무한 루프가 발생할 수 있습니다. 예를 들어, 조건 없이 동작 규칙에 '현재 정책 다시 실행'을 설정하면 규칙은 항상 **true** 가 되어 정책이 항상 다시 시작하고 종료되지 않습니다.

다음 4 개의 흐름 변경 함수를 사용할 수 있습니다.

처리 중지

현재 정책 이후의 모든 정책이 무시되고 Policy Xpress 가 종료되도록 합니다.

참고: Policy Xpress 만 종료됩니다. CA CA Identity Manager 도 중지되도록 하려면 "예외" 유형 동작 플러그 인을 사용할 수 있습니다.

모든 정책 다시 시작

나머지 정책의 처리를 중지하고 목록의 처음으로 돌아갑니다. 이 옵션은 한 정책의 동작으로 인해 다른 정책(이전에 실행되었고 수행되지 않았던 정책)이 이제 진입 조건을 충족하는 경우 유용합니다. 이 정책은 이제 다시 평가됩니다.

현재 정책 다시 실행

정책이 다시 실행되도록 합니다. 이 옵션은 반복에 유용합니다. 예를 들어, 고유 사용자 이름을 만들려면 정책이 고유 이름을 찾을 때까지 반복하여 실행되어야 합니다.

특정 정책으로 이동

이 동작은 기존 정책을 선택하도록 요구합니다. 해당 정책이 현재 정책과 동시에 실행되는 경우(이전 또는 이후) Policy Xpress 는 선택한 정책으로 이동합니다. 새 정책의 우선 순위가 더 낮은 경우 현재 정책과 선택한 정책 사이의 모든 정책은 무시됩니다. 새 정책 우선 순위가 더 높은 경우 프로세스는 뒤로 이동합니다.

참고: 동작으로 인해 Policy Xpress 가 특정 정책을 건너뛸 수 있으므로 이 동작 유형은 주의하여 사용하십시오.

계정과 관련된 개체 설정

"구성원"과 같이 계정과 관련된 개체를 설정하기 위해 "추가 동작"을 만들 때 개체를 나타내기 위해 특정 관계 형식이 사용됩니다. 다음 두 가지 유형의 형식으로 CA CA Identity Manager 에서 개체를 나타낼 수 있습니다.

- 예를 들어, Active Directory 그룹과 같이 개체와 계정 간의 간단한 관계를 나타내려면:

```
NativeGroup=Administrators,Container=Builtin,EndPoint=LocalAD,Namespace=ActiveDirectory,Domain=im,Server=Server
```

- 예를 들어, SAP 역할과 같이 개체와 계정 간의 바인딩 관계를 나타내려면:

```
{"validFromDate":"2009\12\01","roleName":"SAPRole=SAP_AUDITOR_ADMIN,EndPoint=sap_endpoint,Namespace=SAPR3,Domain=im,Server=Server","validToDate":"2009\12\31"}
```

바인딩 관계는 개체와 계정 간의 연결에 추가 데이터가 있다는 점에서 간단한 관계와 다릅니다. 이전 예제에서는 매개 변수 `validFromDate` 와 `validToDate` 만 계정과 SAP 역할 간의 연결에 관련된 데이터를 포함합니다. `validFromDate` 와 `validToDate` 데이터는 계정 또는 역할 개체에 존재하지 않습니다.

관계의 형식을 식별하려면 개체 값을 가져오는 데이터 요소를 만드십시오. 반환된 값은 해당 개체를 설정하기 위해 추가 동작에서 사용하는 형식입니다.

예: Active Directory 그룹

1. 다음 설정으로 Policy Xpress 정책을 만듭니다.
 - 정책 유형: 이벤트
 - 이벤트: 다음 이후 – 사용자 수정
2. "동작 규칙"에서 다음 추가 동작을 구성합니다.
 - 범주: 특성
 - 유형: 계정 데이터 설정
 - 함수: 설정
 - 끝점 유형: Active Directory
 - 끝점: `endpoint_name`
 - 계정 이름: `account`

- 특성: 구성원(groupMembership)
- 값:
NativeGroup=Administrators,Container=Builtin,Endpoint=endpoint_name,Namespace=ActiveDirectory,Domain=im,Server=Server

고급

Policy Xpress 는 많은 구성 변경을 허용하며 외부 구성 요소와도 상호 작용합니다. 이러한 융통성으로 인해 잘못 구성된 데이터 원본, 동적 데이터 요소에서 반환된 누락된 값, 응답하지 않는 끝점과 같이 버그라고는 할 수 없지만 여러 오류가 발생할 수 있습니다.

오류가 발생하면 일반적으로 시스템이 현재 단계에 대해 정책의 계산을 중지합니다. 하지만 오류 범주를 기반으로 기본 오류 응답을 변경할 수 있습니다. 예를 들어, 중요하지 않은 정책이 있는 경우 오류가 발생할 때 처리가 계속되도록 정의할 수 있습니다.

"고급" 탭에서는 필요한 경우 기본 오류 응답을 변경할 수 있습니다.

참고: 이러한 오류 응답은 기본 상태로 두는 것을 권장하지만 고급 사용자의 경우 정책별로 이러한 설정을 변경할 수 있습니다. 예를 들어, 중요하지 않은 정책이 있는 경우 정책이 실패해도 처리가 계속되도록 정의할 수 있습니다.

이 탭에서 다음 오류 범주를 구성할 수 있습니다.

- 유효성 검사—플러그 인에 잘못된 정보를 제공하여 유발되었습니다. 이 오류 유형은 동작이 시도되기 전에 보고됩니다.
- 환경—SQL 플러그에 대한 데이터베이스 서버 실패와 같은 환경 내 문제에 의해 유발되었습니다.
- 허용됨—중요하지 않은 오류입니다. 이 오류 유형에 대한 기본 동작은 (예를 들어 전자 메일 발송이 실패한 경우) 요청 처리를 계속하는 것입니다.

이전 오류 각각에 대해 다음 옵션이 설정될 수 있습니다.

- 실패 이벤트—현재 동작을 중지합니다. 대부분의 오류 유형에 대한 기본 옵션입니다.
- 실패 정책—현재 정책과 연결된 모든 동작을 중지합니다. 나머지 정책은 계속합니다.
- 무시—모든 실패를 로깅하지만 동작 또는 정책을 중지하지 않습니다.

제 17 장: CA Identity Manager 모바일 응용 프로그램

CA Identity Manager 모바일 응용 프로그램에서는 기존 CA Identity Manager 인프라를 활용할 수 있으므로 사용자가 스마트폰 또는 태블릿과 같은 모바일 장치에서 다음과 같은 태스크를 수행할 수 있습니다.

- 잊어버린 암호 다시 설정
- 암호 변경
- 승인 또는 거부로 승인 요청에 응답. 요청을 예약 또는 릴리스하려면 사용자 콘솔을 사용하십시오.
- 사용자 정보 보기

이 기능을 통해 조직의 다른 사용자에 대한 정보를 볼 수 있습니다. 예를 들어 승인 결정을 내리기 전에 작업 항목 승인자는 이름, 주소 등 사용자의 매니저에 대한 기본 정보를 볼 수 있습니다. 자세한 내용이 필요한 경우 승인자는 완료된 프로필을 볼 수 있는 링크를 클릭할 수 있습니다.

이 섹션은 다음 항목을 포함하고 있습니다.

[CA Identity Manager 모바일 응용 프로그램 아키텍처](#) (페이지 546)

[구현 프로세스 작동 방식](#) (페이지 550)

[응용 프로그램 구성이 작동하는 방법](#) (페이지 552)

[사용자 등록이 작동하는 방법](#) (페이지 552)

[모바일 응용 프로그램을 지원하도록 CA Identity Manager 를 구성하는 방법](#) (페이지 552)

[모바일 앱 구성](#) (페이지 564)

[추가 속성 구성](#) (페이지 567)

[모바일 앱 다운로드](#) (페이지 569)

[모바일 응용 프로그램 문제 해결](#) (페이지 570)

CA Identity Manager 모바일 응용 프로그램 아키텍처

CA Identity Manager 모바일 응용 프로그램 아키텍처는 스마트폰 및 태블릿 등과 같은 여러 모바일 장치를 위한 여러 CA Identity Manager 기능을 제공하기 위해 설계되었습니다. 모바일 응용 프로그램을 위한 기능은 중요 비즈니스 요구 사항 및 휴대용 기기에서 업무 적합성 여부를 기준으로 선택됩니다.

이 아키텍처는 CA Identity Manager 서버 기능을 노출하는 응용 프로그램 및 RESTful 웹 서비스에 대한 "구성" 구성 요소 사용의 핵심입니다. CA Identity Manager 서버는 해당 환경의 모바일 응용 프로그램 구성 및 이 응용 프로그램에서 사용되는 REST 웹 서비스의 구성을 관리하기 위한 기능을 지원합니다.

참고: REST 웹 서비스는 CA Identity Manager 모바일 응용 프로그램에 고유하며, SOAP 기반 TEWS(Task Execution Web Services)와 달리 공용 API 로 의도되지 않았습니다.

REST 웹 서비스는 각 CA Identity Manager 환경(IME)마다 여러 구성을 지원하며, 각 구성은 일반적으로 모바일 응용 프로그램과 같은 특정 REST 클라이언트와 연결됩니다. 아래 그림에는 모바일 응용 프로그램 구성과 웹 서비스 구성 사이의 아키텍처 및 관계가 개괄적으로 설명되어 있습니다.



REST 웹 서비스 구성에서는 모바일 응용 프로그램이 기능할 수 있도록 특정 옵션 집합을 선택해야 합니다. 웹 서비스 구성은 모바일 응용 프로그램 구성(관리 태스크에서 사용 가능)을 만들기 전에 웹 서비스 구성 태스크를 통해 정의되어야 합니다.

모바일 응용 프로그램 웹 서비스 구성 정보

REST 웹 서비스 구성은 다음 요소로 구성됩니다.

- 고유 구성 이름, 식별자 및 활성화된 플래그를 정의하는 프로필
- SSL, 페이로드 암호화, 암호화 키의 사용을 정의하는 보안 구성
- REST 를 통해 각 유형에 대해 지원되는 관리 개체 유형, 작업, 특성의 집합
- 지원되는 자체 서비스 작업(예: 암호 재설정) 및 허용되는 사용자 자체 서비스 특성 집합
- 사용자가 구성된 REST 작업을 호출할 권한이 있는 구성원 정책

아래 표에는 웹 서비스 구성 정보 및 모바일 응용 프로그램에 필요한 설정이 설명되어 있습니다.

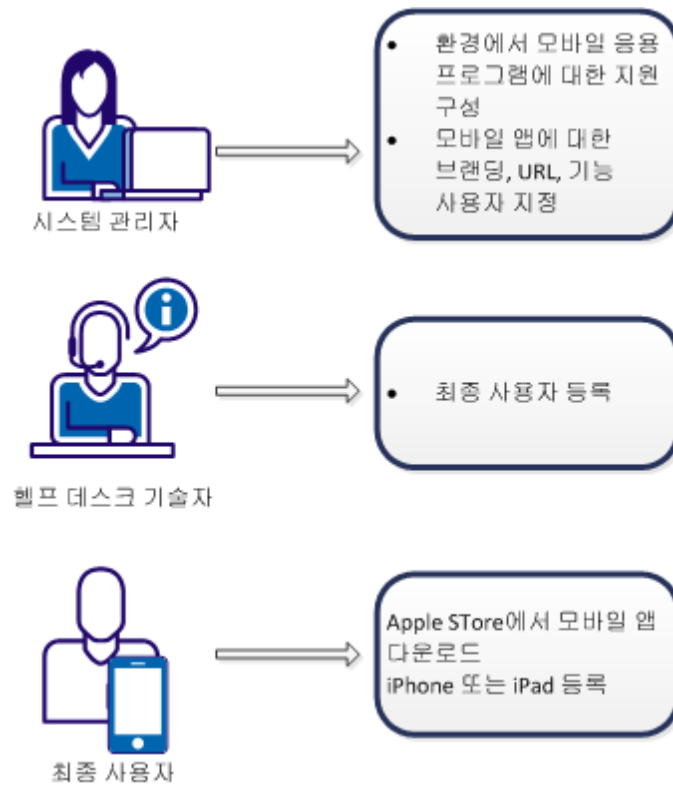
구성 섹션	항목	설명	모바일 앱 설정
프로필	이름	구성의 이름	배포 선택
	식별자	해당 클라이언트가 각 CA Identity Manager 서버 요청의 "Configuration-Id" http 헤더에 반드시 설정해야 하는 고유 식별자	배포 선택. 모바일 앱 구성 서비스는 이후 모든 REST 요청에서 사용되어야 하는 식별자를 반환합니다.
	사용	구성 활성화/비활성화	True
보안	보안 통신 필요	https 필요 여부	배포 선택. 모바일 앱 구성 서비스에 의해 다운로드된 값

	암호화 사용	비 SSL 에 대한 암호화 페이로드에 사용됨. 클라이언트 측 crypto 라이브러리, 암호화 키 정보 및 명시적 클라이언트 측 암호화/암호 해독 지원 필요	사용되지 않습니다. 선택 취소된 상태로 둡니다.
	구성 암호	REST 클라이언트-서버 트러스트 모델의 일부로서 필요한 공유 암호	반드시 지정해야 합니다. 배포 중 구성 인스턴스를 정의할 때 암호를 생성해야 합니다.
개체 유형	개체 유형	REST 리소스로서 노출된 개체 유형	사용자 개체 유형
	메서드 및 특성	선택한 개체 유형에 대해 지원되는 리소스 메서드(CRUD) 및 이러한 메서드에 대해 허용되는 특성 집합	배포 관련 사용자 스키마에 표시된 대로 다음 특성에 대한 액세스 보기 권한이 있는 사용자 개체 유형: ■ 회사 전화 ■ 부서 ■ 전자 메일 ■ 이름 ■ 성 ■ 매니저 ■ 사무실 ■ 제목

자체 관리	구성원 규칙	어떤 사용자가 자체 관리를 수행할 수 있는지를 나타내는 규칙	모바일 앱 구성의 구성원 규칙과 일치해야 합니다. 수정을 위한 특성 집합은 비워두어야 합니다.
	암호 재설정 사용	사용자가 자신의 암호를 재설정할 수 있게 합니다.	사용
	특성	사용자가 스스로 관리할 수 있는 특성 집합	빈 목록
구성원	구성원	사용자가 이 구성에 대해 정의된 REST 작업을 호출하도록 권한 부여되는 규칙을 정의합니다.	모바일 앱 사용자의 집합과 일치하는 구성원 규칙

구현 프로세스 작동 방식

모바일 응용 프로그램을 설정하는 과정에는 세 가지 유형의 사용자가 관련됩니다. 다음 그림에서는 이러한 사용자 유형과 각 사용자가 수행하는 태스크를 보여 줍니다.



최종 사용자가 **CA Identity Manager** 에서 모바일 응용 프로그램을 사용할 수 있도록 하려면 다음과 같은 활동을 수행해야 합니다.

1. 시스템 관리자가 환경에서 모바일 응용 프로그램에 대한 지원을 구성합니다.

구성에는 다음 활동이 포함됩니다.

- 활성화 및 다시 설정 코드 특성 구성
- 모바일 사용자 등록을 위한 태스크, **Policy Xpress** 정책 및 전자 메일 템플릿 추가
- 웹 서비스 정의 만들기
- 등록 전자 메일 수정

시스템 관리자는 모바일 사용자가 액세스할 수 있는 브랜딩, URL 및 기능도 구성합니다.

2. 헬프 데스크 기술자와 같은 관리자가 사용자 콘솔에서 해당되는 최종 사용자를 등록합니다.

등록 프로세스에서 각각의 최종 사용자에게 대한 활성화 코드를 트리거하고 이 코드와 등록 지침이 포함된 전자 메일을 최종 사용자에게 자동으로 보냅니다.

3. 최종 사용자가 **Apple** 스토어에서 모바일 응용 프로그램을 다운로드하고 전자 메일에서 받은 지침과 코드를 사용하여 스마트폰 또는 태블릿 같은 장치를 등록합니다.

최종 사용자가 모바일 응용 프로그램을 사용하여 **CA Identity Manager** 기능에 액세스할 수 있습니다.

참고: 사용자를 만드는 동안 "암호를 변경해야 함" 옵션이 선택된 경우 모바일 응용 프로그램 사용자는 활성화를 완료할 수 없습니다.

응용 프로그램 구성이 작동하는 방법

모바일 응용 프로그램은 CA Identity Manager 서버 구성 API 에서 구성을 가져옵니다. 모바일 응용 프로그램이 먼저 설치되고 다운로드한 구성이 없는 경우, 사용자에게 사용자 이름과 암호 입력을 요청하며 이러한 자격 증명을 사용하여 사용자 등록 전자 메일에 있는 링크로부터 정의된 구성을 다운로드합니다.

최초 구성 다운로드가 완료되면 응용 프로그램이 시작될 때마다 CA Identity Manager 서버에 있는 최신 버전과 구성 버전을 비교합니다. 최신 버전이 있는지 확인하기 위해 구성 버전 검사 API 가 사용됩니다.

사용자 등록이 작동하는 방법

모바일 응용 프로그램 액세스를 원하는 각 사용자는 CA Identity Manager 내에서 액세스를 요청해야 합니다. 액세스가 승인되면 사용자는 액세스가 부여되었음을 알리는 활성화 코드로 사용자가 업데이트됩니다. 모바일 앱 구성 구성원 정책 및 기반 웹 서비스 구성원 정책은 액세스를 요청하는 모바일 사용자에게 대해 정의된 모든 조건을 충족시켜야 합니다. 최소한 'Registered'의 %ACTCODE% 값 또는 '0'보다 큰 값이 정의되어야 합니다.

사용자의 모바일 액세스가 제거되는 경우 CA Identity Manager 서버는 활성화 특성을 재설정하여 모바일 응용 프로그램에 대한 사용자 액세스를 방지합니다.

모바일 응용 프로그램을 지원하도록 CA Identity Manager 를 구성하는 방법

모바일 응용 프로그램은 암호와 승인을 관리하기 위해 REST 웹 서비스를 사용하여 CA Identity Manager 와 통신합니다. 이러한 통신이 사용되도록 설정하려면 시스템 관리자가 다음 단계를 수행해야 합니다.

1. [응답 특성을 구성합니다](#) (페이지 553).
2. [관리자 태스크를 가져옵니다](#). (페이지 557)
3. [웹 서비스를 만듭니다](#) (페이지 558).
4. [등록 전자 메일을 수정합니다](#) (페이지 561).
5. 필요한 경우 모바일 앱을 지원하도록 SiteMinder 를 구성합니다.

응답 특성 구성

모바일 응용 프로그램을 통해 사용자 등록 및 액세스를 가능하게 하려면 CA Identity Manager 사용자 저장소에 다음과 같은 잘 알려진 특성을 포함해야 합니다.

- **%ACTCODE%** - 임의로 생성된 활성화 번호를 저장하는 특성을 나타냅니다. 사용자가 등록된 후 이 특성에는 **Registered(등록됨)**라는 단어가 포함됩니다.
- **%ACTCODEVAL%** - 등록 시 클라이언트가 설정하는 활성화 코드를 저장하는 특성을 나타냅니다. CA Identity Manager 는 이 값을 **%ACTCODE%**의 값과 비교합니다.
- **%CURRENT_AUTH_QUESTIONS%** - 챌린지 질문 값을 임의로 저장하는 특성을 나타냅니다. 사용자가 올바르게 응답하면 이 값은 삭제됩니다.
- **%MOBILE_PIN%** - 개인 식별 번호 또는 문자열 값을 저장하는 특성을 나타냅니다. 이 특성은 시스템에 대해 사용자를 인증하는 데 사용할 수 있는 사용자와 시스템 사이에 공유되는 영숫자 암호를 제공합니다.
- **%PWRESETCODE%** - 암호화된 코드를 저장하는 특성을 나타내며, 이 특성은 암호 다시 설정 시 1 단계 인증을 제공합니다.

이 잘 알려진 특성을 디렉터리 구성 파일(directory.xml)에서 사용 가능한 사용자 저장소 특성에 매핑합니다. 사용 가능한 특성이 없을 경우 사용자 저장소 스키마를 확장하십시오. 스키마 확장에 대한 자세한 내용은 사용자 저장소의 설명서를 참조하십시오.

특성 설명에 다음 데이터 분류가 포함됩니다.

<DataClassification name="sensitive"/>

태스크 화면, 감사 레코드 및 시스템 로그에서 와일드카드 문자로 다시 설정 코드 값을 바꿉니다.

중요! **%ACTCODE%** 특성 정의에서 중요한 데이터 분류를 포함하지 마십시오. 중요한 특성을 포함하는 경우 모바일 응용 프로그램이 제대로 작동하지 않습니다.

<DataClassification name=" AttributeLevelEncrypt "/>

정의된 암호화 키를 사용하여 사용자 저장소에서 기록하고 읽은 대로 다시 설정 코드 값을 암호화 및 암호 해독합니다.

<DataClassification name=" ignore_on_copy "/>

이 매개 변수를 설정하면 관리자가 사용자 콘솔에서 개체 사본을 만들 때 CA Identity Manager 가 특성을 무시합니다.

참고: 이러한 잘 알려진 특성의 예제는 이 절의 끝에 설명되어 있습니다.

다음 단계를 수행하십시오.

1. 관리 콘솔에 로그인합니다.
2. "디렉터리"를 선택한 후 모바일 사용자가 있는 디렉터를 클릭합니다.
3. 해당 디렉터를 내보냅니다.
4. 특성 설명을 추가 또는 수정하여 %ACTCODE% 잘 알려진 특성을 포함합니다.

사용 가능한 특성을 모두 %ACTCODE% 잘 알려진 특성에 매핑할 수 있습니다.

5. 4 단계를 반복하여 %ACTCODEVAL% 잘 알려진 특성을 정의합니다. 다음 데이터 분류를 포함합니다.

```
<DataClassification name="sensitive"/>
<DataClassification name="ignore_on_copy"/>
<DataClassification name=" AttributeLevelEncrypt"/>
```

6. %CURRENT_AUTH_QUESTIONS% 잘 알려진 특성에 대한 특성 설명을 추가합니다. 다음 데이터 분류를 포함하십시오.

```
<DataClassification name="ignore_on_copy"/>
```

7. %MOBILE_PIN% 잘 알려진 특성의 특성 설명을 추가합니다. 다음 데이터 분류를 포함합니다.

```
<DataClassification name="sensitive"/>
<DataClassification name="ignore_on_copy"/>
<DataClassification name=" AttributeLevelEncrypt"/>
```

8. %PWRESETCODE% 잘 알려진 특성의 특성 설명을 추가합니다. 다음 데이터 분류를 포함합니다.

```
<DataClassification name="sensitive"/>
<DataClassification name="ignore_on_copy"/>
<DataClassification name=" AttributeLevelEncrypt"/>
```

9. directory.xml 파일을 저장합니다.

10. 관리 콘솔의 "Directory Properties"(디렉터리 속성) 페이지에서 "Update"(업데이트)를 클릭하여 저장된 directory.xml 파일을 로드합니다.

예제

참고: 임의의 사용 가능한 특성을 이러한 잘 알려진 특성에 매핑할 수 있습니다.

%ACTCODE%

```
<ImManagedObjectAttr
  physicalname="attribute_name"
  displayname="your_attribute_display_name"
  description="your_attribute_description"
  valuetype="String"
  required="false"
  multivalued="false"
  wellknown="%ACTCODE%"
  maxlength="0"
  hidden="true"
  system="true">
  <DataClassification name="ignore_on_copy"/>
  <DataClassification name=" AttributeLevelEncrypt"/>
</ImManagedObjectAttr>
```

%ACTCODEVAL%

```
ImManagedObjectAttr
  physicalname="attribute_name"
  displayname="your_attribute_display_name"
  description="your_attribute_description"
  valuetype="String"
  required="false"
  multivalued="false"
  wellknown="%ACTCODEVAL%"
  maxlength="0"
  hidden="true"
  system="true">
  <DataClassification name="ignore_on_copy"/>
  <DataClassification name=" AttributeLevelEncrypt"/>
</ImManagedObjectAttr>
```

%CURRENT_AUTH_QUESTIONS%

```
<ImManagedObjectAttr
  physicalname="attribute_name"
  displayname="your_attribute_display_name"
  description="your_attribute_description"
  valuetype="String"
  required="false"
  multivalued="false"
  wellknown="%CURRENT_AUTH_QUESTIONS%"
  maxlength="0"
  hidden="true"
  system="true">
  <DataClassification name="ignore_on_copy"/>
```

%MOBILE_PIN%

```
<ImManagedObjectAttr
physicalname="attribute_name"
displayname="your_attribute_display_name"
description="your_attribute_description"
valuetype="String"
required="false"
multivalued="false"
wellknown="%MOBILE_PIN%"
maxlength="0"
hidden="true"
system="true">
  <DataClassification name="ignore_on_copy"/>
  <DataClassification name=" AttributeLevelEncrypt"/>
</ImManagedObjectAttr>
```

%PWRESETCODE%

```
<ImManagedObjectAttr
physicalname="attribute_name"
displayname="your_attribute_display_name"
description="your_attribute_description"
valuetype="String"
required="false"
multivalued="false"
wellknown="%PWRESETCODE%"
maxlength="0"
hidden="true"
system="true">
  <DataClassification name="ignore_on_copy"/>
  <DataClassification name=" AttributeLevelEncrypt"/>
</ImManagedObjectAttr>
```


관리자 태스크 가져오기

모바일 사용자가 CA Identity Manager 에 로그인하려면 먼저 관리자가 사용자 콘솔에서 모바일 사용자를 등록해야 합니다. 등록 프로세스에서 활성화 코드가 생성되고 모바일 사용자에게 전자 메일로 전송됩니다.

이러한 활동을 지원하려면 다음 기능을 환경에 추가하는 역할 정의 파일을 가져와야 합니다.

- 모바일 구성 태스크
- Register User for Mobile App(모바일 응용 프로그램에 사용자 등록) 및 Remove User from Mobile App(모바일 응용 프로그램에서 사용자 제거) 태스크
- 활성화 코드를 생성하고 사용자 계정에서 모바일 클라이언트의 등록을 취소하는 Policy Xpress 정책입니다.
- 전자 메일을 모바일 사용자에게 보내기 위한 전자 메일 템플릿

다음 단계를 수행하십시오.

1. 관리 콘솔에 로그인합니다.
2. "Environments"(환경)를 선택한 후 모바일 응용 프로그램을 지원하는 환경을 클릭합니다.
3. "Role and Task Settings"(역할 및 태스크 설정)를 선택한 후 다음 화면에서 "가져오기"를 클릭합니다.
4. MobileApp-RoleDefinitions 를 선택한 후 "마침"을 클릭합니다.
5. 환경을 다시 시작합니다.
6. 다음 태스크를 시스템 매니저 역할에 추가합니다.
 - 모바일 구성 만들기
 - 모바일 구성 수정
 - 모바일 구성 보기
 - 모바일 구성 삭제
 - Register User for Mobile App(모바일 응용 프로그램에 사용자 등록)
 - Remove User from Mobile App(모바일 응용 프로그램에서 사용자 제거)

"사용자" 및 "시스템" 범주에 새 태스크가 포함됩니다.

웹 서비스 구성 만들기

모바일 응용 프로그램에서는 REST 웹 서비스를 사용하여 CA Identity Manager 와 통신합니다. 모바일 응용 프로그램을 지원하려면 시스템 관리자가 사용자 콘솔에서 웹 서비스 정의를 만들어야 합니다.

참고: 웹 서비스 구성의 암호화를 사용하도록 설정하면 REST 호출은 작동하지 않습니다.

다음 단계를 수행하십시오.

1. 시스템 관리자 권한이 있는 사용자로 사용자 콘솔에 로그인합니다.
2. 다음과 같이 웹 서비스 정의를 만듭니다.
 - a. "시스템", "웹 서비스", "웹 서비스 구성 만들기"로 이동합니다.
 - b. "프로필" 탭에서 다음 필드를 완성합니다.
 - 이름: *필요한 이름*. 예를 들면 RestMobile 입니다.
 - Identifier(식별자): *고유한 식별자*. 기본값은 RestMobile 입니다.
"Identifier"(식별자) 필드의 값은 모바일 응용 프로그램 구성의 **restid** 값과 일치해야 합니다.
보안을 강화하기 위해 식별자 값과 **restid** 를 변경하는 것이 좋습니다.
 - Enable Attribute(특성 사용): 이 확인란을 선택합니다.

c. "보안" 탭에서 다음을 완료합니다.

- "보안 통신 필요" 옵션을 선택해야 하는지 결정하십시오.

참고: 모든 모바일 응용 프로그램 http 트래픽을 암호화하는 것이 좋습니다. 이 트래픽은 일반적으로 다음 두 가지 방법으로 구성할 수 있습니다.

- 프록시 서버 사용: 이 경우 CA Identity Manager 서버가 방화벽 내에 있습니다. 프록시 서버에서 CA Identity Manager 서버로의 통신을 보안 처리하지 않을 수 있습니다. 하지만 모바일 응용 프로그램과 프록시 서버 사이의 http 통신을 보안 처리해야 합니다. 이 경우 "보안 통신 필요"를 선택하지 마십시오.

참고: CA Identity Manager 와 SiteMinder 를 통합하지 않는 경우 웹 서비스 호출에 SSL 통신이 유지되도록 "보안 통신 필요" 옵션을 선택하십시오.

- CA Identity Manager 서버와 직접 통신: 이 경우 모바일 클라이언트는 CA Identity Manager 서버와 직접 통신하며, http 통신은 암호화되어야 합니다. 이 요구 사항을 반영하려면 "보안 통신 필요" 옵션을 선택하십시오.
- "암호화 사용"이 선택되지 않은 상태여야 합니다.

참고: 암호화를 사용하도록 설정한 경우 사용자 상세 정보는 모바일 응용 프로그램에 표시되지 않습니다.

d. "개체 유형" 탭에서 "사용자"를 찾은 후 "사용자"를 선택하고 "편집" 단추를 클릭합니다.

e. "보기 액세스 허용"만 선택합니다.

"수정 액세스 허용", "생성 액세스 허용" 및 "삭제 액세스 허용" 옵션에 대한 선택을 취소하여 다른 액세스 권한을 제거합니다.

- f. "Self Administration"(자체 관리자) 탭에서 다음 단계를 완료하십시오.
 - 구성원 규칙 아래의 "추가" 단추를 선택하여 구성원 역할을 만들고 "모두"를 지정합니다.
참고: 한 명의 구성원 규칙만 만들 수 있습니다.
 - 모바일 응용 프로그램에서 암호 변경 기능을 지원하려면 암호 다시 설정을 사용하도록 설정해야 합니다.
- g. "Member"(구성원) 탭에서 다음 조건을 사용하여 구성원 규칙을 작성합니다.
 - 활성화 코드 = 등록됨 또는
 - 활성화 코드 > 0
- h. 웹 서비스를 제출하고 저장합니다.

등록 전자 메일 수정

모바일 구성 개체의 URL 을 포함하도록 기본 등록 전자 메일을 편집합니다.

다음 단계를 수행하십시오.

1. 사용자 콘솔에서 "시스템", "전자 메일", "전자 메일 수정"으로 이동합니다.
2. 모바일 응용 프로그램 전자 메일의 등록된 사용자를 검색하여 선택합니다.
3. "콘텐츠" 탭에서 "HTML 소스 전환" 단추를 클릭합니다.
4. 다음과 같이 mobileregsvridm 의 href 항목에 모바일 구성 개체의 URL 을 지정합니다.

```
<a  
href="mobileregsvridm://{Attribute:%ACTCODE%}&https://FQN/iam  
/im/ws/Alias/mobile/ConfigName">
```

FQN

CA Identity Manager 서버의 IP 주소를 지정합니다.

Alias

환경의 이름을 지정합니다.

ConfigName

구성 개체의 이름을 지정합니다.

5. "제출"을 클릭합니다.

모바일 앱을 지원하도록 SiteMinder 를 구성하는 방법

모바일 응용 프로그램에서 사용되는 웹 서비스는 HTTP AUTHORIZATION 헤더 또는 SiteMinder 인증을 통해 모바일 응용 프로그램에서 전달되는 사용자 이름/암호 자격 증명을 사용한 네이티브 인증을 지원할 수 있습니다. 이전에 설명한 것처럼 웹 서비스 구성은 각 REST 리소스 및 메서드 요청에 대한 인증 정책을 정의합니다.

IM REST 웹 서비스 URL

IM REST 서비스는 다음 기준 URL 에 기초합니다.

`http[s]://[FQN]/iam/im/ws/[Alias]`

- FQN – CA Identity Manager 서버 액세스 지점의 정규화된 이름 및 포트
- Alias – 연결할 CA Identity Manager 환경의 공용 별칭

모바일 응용 프로그램 구성 URL

모바일 응용 프로그램 구성에는 모바일 앱 구성 다운로드에 필요한 부트스트랩 구성 정보를 가져오기 위한 특정 URL 이 포함되어 있습니다. 구성 URL 은 다음과 같습니다.

`http[s]://[FQN]/ iam/im/ws/[Alias]/mobile/[ConfigName]`

ConfigName - 지정된 모바일 응용 프로그램 사용자 집합에 대한 CA Identity Manager 환경에 대한 모바일 응용 프로그램 구성의 이름입니다. 응용 프로그램은 사용자의 모바일 응용 프로그램 액세스 요청이 승인되면 발송되는 등록 전자 메일에 있는 구성 URL 에 대한 링크를 통해 이 구성 이름을 알게 됩니다.

인증되지 않은 REST API

구성 API

다음 구성 API 는 인증이 필요 없습니다.

`http[s]://[FQN]/ iam/im/ws/[Alias]/mobile/[ConfigName]/image`
`http[s]://[FQN]/iam/im/ws/[Alias]/mobile/[ConfigName]/ver`

암호 API 재설정

`https://[FQN]/iam/im/ws/[Alias]/myself/resetpasswordWithResetCodeAndToken`

참고: resetPasswordWithResetCodeAndToken API 에는 모바일 응용 프로그램에서 http 헤더로 전달된 보안 토큰이 포함되어 있습니다. CA Identity Manager 서버는 이러한 토큰의 유무 및 유효성을 검사합니다.

CA Identity Manager 액세스를 보호하기 위해 SiteMinder 와 통합하는 경우 이러한 URL 은 보호되지 않거나 익명 인증 체계를 사용하여 보호되는 영역을 사용하여 정의될 수 있습니다.

인증된 REST API

다음 URL 은 모바일 응용 프로그램에서 사용되고 인증이 필요하며, 권한 부여를 위한 웹 서비스 구성 정책을 사용합니다.

구성

`http[s]://[FQN]/iam/im/ws/[Alias]/mobile/[ConfigName]/conf`

자체 서비스 사용자

`http[s]://[FQN]/iam/im/ws/[Alias]/myself`

작업 목록

`http[s]://[FQN]/iam/im/ws/[Alias]/worklist`

사용자

`http[s]://[FQN]/iam/im/ws/[Alias]/mo/User`

모바일 앱 구성

시스템 관리자는 사용자 콘솔에서 CA Identity Manager 모바일 앱을 구성합니다.

환경은 여러 모바일 앱 구성을 포함할 수 있습니다. 다른 구성을 만들면 다른 유형의 모바일 사용자를 위한 다른 브랜딩이나 기능을 지원할 수 있습니다. 예를 들어, 직원 암호 변경을 위한 하나의 구성을 만들고, 매니저들의 작업 항목 승인을 위한 또 다른 구성을 만들 수 있습니다.

관리자는 모바일 응용 프로그램에 대해 다음과 같은 속성을 구성할 수 있습니다.

- 브랜딩

모바일 응용 프로그램의 회사 로고를 지정합니다.

- 기능 테스트

다음 기능이 사용되도록 설정합니다.

- 잊어버린 암호 지원
- 암호 변경 지원
- 워크플로 승인 큐
- 매니저 링크 표시

- 지원 정보

- 특성 매핑

사용자 저장소의 특성을 모바일 응용 프로그램에 노출된 특성에 매핑합니다.

다음 단계를 수행하십시오.

1. 모바일 구성을 사용할 수 있는 사용자로 사용자 콘솔에 로그인합니다.
2. "태스크", "시스템", "모바일 구성", "모바일 구성 만들기"를 클릭합니다.
3. 기본 옵션인 "모바일 구성 유형의 새 개체 만들기"를 선택합니다.
4. "일반" 탭에서 필수 필드를 입력합니다. 모바일 앱에 대한 이미지를 선택할 수 있습니다.

기준 URL

현재 환경의 기준 URL 을 확인하십시오. 기준 URL 은 모바일 구성을 만들 때 자동으로 채워집니다.

CA Identity Manager 는 REST 호출을 위한 URL 을 구성하기 위해 모바일 앱이 사용하는 서버 이름, 포트, 프로토콜을 가져오기 위해 기준 URL 을 사용합니다.

구성

구성을 찾아보거나 고유 구성 이름을 입력하십시오.

버전

구성을 수정 또는 저장할 때마다 버전 번호를 증가시키십시오.

모바일 응용 프로그램은 버전 번호를 사용하여 새 버전의 구성을 다운로드할 시기를 결정합니다. 모바일 앱이 시작되면 서버의 버전 번호와 로드된 구성의 버전을 비교합니다. 새 버전이 있으면 모바일 앱은 구성을 업데이트합니다.

참고: 처음에 파일을 수정할 때는 버전 번호를 증가시키지 마십시오.

브랜딩 이미지

투명 배경을 사용하는 PNG 이미지의 전체 URL 을 지정하십시오. 이 이미지는 모바일 앱에서 화면 맨 위에 표시됩니다.

5. "기능" 탭에서 모바일 앱에 대한 기능을 선택합니다.

암호 재설정 동작

동작에 대해 사용할 방법을 선택하십시오. 이 방법은 필수 특성을 구성할 때 결정됩니다.

- 기본값
- PIN 질문
- QnA 질문

참고: "QnA 질문"을 선택하는 경우 "태스크", "환경 관리자"로 이동하여 '질문 및 대답 구성'을 선택해야 합니다. "확인" 확인을 선택하고 인증 질문의 숫자(1-5)를 입력한 다음 "제출"을 클릭하십시오. 기본 설정을 변경하지 않는 경우라도 구성 설정을 반영하려면 "제출" 단추를 클릭해야 합니다.

6. "지원" 탭에서 모바일 사용자에게 대한 지원 정보를 지정합니다.
7. "특성 매핑" 탭에서 모바일 앱 특성을 CA Identity Manager 사용자 저장소의 특성에 매핑합니다. 특성을 실제 특성 또는 잘 알려진 특성에 매핑할 수 있습니다.
8. "추가 속성" 탭에서 모바일 앱의 새 기능 또는 필드를 지원하기 위해 추가 속성 값 쌍을 지정합니다.

다음 형식을 사용합니다.

Key1=value1

Key2=value2

Key3=value3

참고: CA Technologies 는 관리자가 추가 속성을 추가해야 하는 경우 관련 지침을 제공합니다. 이 톨리스에서는 추가 속성을 지정할 필요가 없습니다.

9. "구성원" 탭에서 모바일 앱에 이 구성이 표시되는 사용자들을 결정하는 규칙을 지정합니다.
10. 제출을 클릭합니다.

추가 속성 구성

모바일 앱을 구성한 후에 필요한 경우 모바일 앱에서 새 기능을 지원하도록 추가 속성 키-값 쌍을 지정할 수 있습니다. "추가 속성" 탭을 사용하여 이 작업을 수행할 수 있습니다.

다음 형식을 사용합니다.

- demoMode="Disable/Enable"
- maxPinRetries=<any positive numerical value>
- multiAccount="Disable/Enable"
- managerTraversal="Disable/Enable"
- startupWithBrandLogo="true/false"

참고: CA Technologies 는 관리자가 추가 속성을 추가해야 하는 경우 관련 지침을 제공합니다.

하지만 다음 기능은 모바일 구성에서 기본적으로 활성화되어 있습니다.

- **DemoMode:** 모바일 앱의 데모 버전을 볼 수 있게 해 줍니다. 이 옵션은 모바일 앱의 "설정" 섹션에 있습니다.
- **maxPinRetries:** 관리자가 모바일 사용자에게 대한 잘못된거나 실패한 PIN 입력 시도 횟수를 구성할 수 있게 해 줍니다. 기본 실패 시도 횟수는 5 회입니다.
- **MultiAccount:** 특히 활성화 코드와 함께 여러 등록된 모바일 사용자를 추가하여 여러 계정을 추가할 수 있게 해 줍니다.
- **ManagerTraversal:** 작업 항목 정보에 승인자와 요청자의 매니저 정보를 표시합니다.
- **startupWithBrandLogo:** 사용자가 기본 CA 로고 대신 표시할 사용자 지정 계정 로고(계정의 브랜딩 이미지)를 지정할 수 있게 허용합니다. 이 키-값이 true 로 설정되었지만 어떤 이유에서 브랜드 로고 필드가 비어 있거나 잘못된 URL 이 들어 있는 경우 시작할 때 실행 화면이 빈 상태로 표시됩니다. 설치 후 앱이 먼저 실행되면 CA 로고가 항상 표시됩니다. 이 추가 속성은 계정 데이터의 일부이며 최초 실행 시에는 사용할 수 있는 계정 데이터가 없습니다.

참고: 이러한 변경 사항은 CA Identity Manager 서버와 성공적으로 통신한 후에만 이후 실행 시 반영됩니다.

모바일 클라이언트에서 이러한 기능을 비활성화하려면 CA Identity Manager 모바일 구성의 "추가 속성" 탭에서 다음 키-값 쌍을 추가해야 합니다.

- 데모 모드 기능을 활성화 또는 비활성화하려면
DemoMode 를 Enable 또는 Disable 로 설정
 - demoMode="Disable/Enable"
- maxPinRetries 기능을 활성화 또는 비활성화하려면
maxPinRetries 를 임의의 양수 값을 설정
 - maxPinRetries=<임의의 양수 값>. 기본 실패 시도 횟수는 5 회입니다.
- 다중 계정 기능을 활성화 또는 비활성화하려면
MultiAccount 를 Enable 또는 Disable 로 설정
 - multiAccount="Disable/Enable"
- 매니저 통과 기능을 활성화 또는 비활성화하려면
ManagerTraversal 을 Enable 또는 Disable 로 설정
 - managerTraversal="Disable/Enable"
- startupWithBrandLogo 기능을 활성화 또는 비활성화하려면
startupWithBrandLogo 를 true 또는 false 로 설정
 - startupWithBrandLogo="true/false"

다음 단계를 수행하십시오.

1. 관리자(superuser)로 CA Identity Manager 사용자 콘솔에 로그인합니다.
2. "태스크", "시스템", "모바일 구성", "모바일 구성 만들기"를 클릭합니다.
3. "추가 속성" 탭에서 모바일 앱의 새 기능을 지원하기 위해 추가 속성-키 값 쌍을 지정합니다.
 - demoMode="Disable/Enable"
 - maxPinRetries=<임의의 양수 값>. 기본 실패 시도 횟수는 5 회입니다.
 - multiAccount="Disable/Enable"
 - managerTraversal="Disable/Enable"
 - startupWithBrandLogo="true/false"

모바일 앱 다운로드

모바일 앱이 구성되면 최종 사용자가 **Apple** 스토어에서 앱을 다운로드할 수 있습니다. **Apple** 스토어에서 모바일 앱을 찾으려면 **CA Identity Manager** 로 검색하십시오.

그런 다음 최종 사용자는 전자 메일로 받은 지침 및 코드를 사용하여 스마트폰 또는 태블릿과 같은 본인의 장치를 등록할 수 있습니다.

모바일 응용 프로그램 문제 해결

지원부가 로그 파일 요청

모바일 응용 프로그램과 관련하여 문제가 있을 경우 지원 엔지니어가 문제 해결에 도움이 되는 로그 파일을 요청할 수 있습니다.

모바일 사용자가 iPhone 또는 iPad 를 통해 디버깅이 사용되도록 설정합니다. 디버깅이 사용되도록 설정되면 모바일 사용자가 모바일 응용 프로그램을 사용하여 로그를 지원용 전자 메일 주소로 보낼 수 있습니다.

모바일 응용 프로그램에서 로그를 생성하도록 설정하려면 모바일 사용자가 다음 단계를 완료해야 합니다.

1. 전화 또는 iPad 에서 "설정", "Identity Manager", "디버그"로 이동합니다.
2. 탭이 활성화됩니다.
3. 응용 프로그램을 다시 시작하고 로그에 표시할 동작을 수행합니다.
4. CA Identity Manager 모바일 응용 프로그램의 "설정" 탭에서 "Email Log"(로그를 전자 메일로 보내기)를 탭합니다.

모바일 응용 프로그램에서 로그 파일을 첨부하여 전자 메일을 작성합니다. 이 전자 메일은 사용자 콘솔에서 "지원"에 구성된 전자 메일 주소로 전송될 수 있습니다.

Identity Manager 태스크의 환경 관리자 아래에서 기본 질문 및 답변 구성 설정을 사용할 때 "암호 동작 재설정"으로서 QnA 가 실패합니다.

증상

기본 질문 및 답변 구성 설정을 사용하여 "암호 동작 재설정"으로 QnA 를 선택하면 다음 오류 메시지와 함께 암호 재설정이 실패합니다.

"오류 [im.webservices.QuestionAndAnswerResource] (http-/0.0.0.0:8443-1) 사용자 자격 증명 질문을 가져오지 못했습니다. 메시지:서버 로그 파일에 java.lang.NullPointerException"

해결책:

암호 재설정이 암호 동작 재설정으로서 QnA 와 동작하도록 하려면 다음 단계를 수행하십시오.

다음 단계를 수행하십시오.

1. SuperAdmin 으로 CA Identity Manager 에 로그인합니다.
2. "태스크", "환경 관리자"로 이동한 다음 '질문 및 답변 구성'을 선택합니다.
3. "제출" 단추를 클릭합니다.

참고: '사용' 옵션 및 '인증 질문 수'의 기본값도 이 단계를 수행한 후에만 적용됩니다.

제 18 장: CA 사용자 활동 보고 통합

이 섹션은 다음 항목을 포함하고 있습니다.

[CA UAR 기능](#) (페이지 573)

[추가 CA Enterprise Log Manager 보고서 또는 쿼리를 CA Identity Manager 와 통합](#) (페이지 586)

CA UAR 기능

CA UAR(CA 사용자 활동 보고)이 CA Identity Manager 와 통합된 경우 다음 기능이 제공됩니다.

- CA UAR 에이전트는 CA Identity Manager 감사 정보를 수집하여 CA CEG(Common Event Grammar)로 변환합니다.
- 사용자 콘솔은 반환된 정보를 필터링하는 데 사용되는 CA Identity Manager 컨텍스트 정보가 포함된 CA UAR 보고서 및 쿼리를 검색할 수 있습니다.
- CA Identity Manager 에는 다수의 기본 보고서와 CA UAR 보고서 및 쿼리를 기존 태스크 또는 새 태스크에 추가하기 위한 인프라가 들어 있습니다.

참고: 이전에는 CA UAR 을 CA 엔터프라이즈 로그 매니저라고 했습니다. 일부 경우 사용자 콘솔에서 CA 엔터프라이즈 로그 매니저라는 이름이 여전히 사용됩니다.

CA UAR 구성 요소

CA Identity Manager 가 CA UAR 과 통합되는 경우 다음 구성 요소가 CA Identity Manager 아키텍처에 추가됩니다.

- CA "엔터프라이즈 로그 매니저 뷰어" 탭을 사용해 CA UAR 개체를 새 태스크 또는 기존 태스크에 포함할 수 있습니다.

참고: CA UAR 서버 연결이 필요합니다.

- 역할 정의를 가져올 수 있습니다.

통합 제한 사항

다음은 CA UAR 과 통합할 때의 알려진 제한 사항입니다.

- 런타임에 태스크 구성에 대한 쿼리 및 보고서 목록을 검색할 때 실행 속도가 느릴 수 있습니다.
- CA UAR API 는 기본 Java 명령 시간대만 인식합니다.
- EQUAL 연산자는 복합 필터에서 사용될 때 대소문자를 구분합니다.
- CA UAR 서버에 대한 연결은 한 번에 하나씩만 지원됩니다.

CA UAR 을 CA Identity Manager 와 통합하는 방법

CA UAR 보고서 및 쿼리를 확인하고 관리하려면 먼저 관리자가 다음 단계를 완료해야 합니다.

1. CA UAR 에이전트를 설치합니다.
2. 커넥터를 만듭니다.
3. CA Identity Manager 에서 감사를 사용하도록 설정합니다.
4. CA UAR 서버를 구성합니다.

CA 엔터프라이즈 로그 매니저 에이전트 설치 필수 조건

CA UAR 에이전트를 설치하기 전에 다음 단계를 완료하십시오.

- CA Identity Manager 를 실행하거나 CA Identity Manager 감사 데이터베이스를 호스팅하는 시스템에서 CA UAR 서버 시스템에 연결할 수 있는지 확인합니다.
- 서버 시스템에서 에이전트 시스템에 연결할 수 있는지 확인합니다.
- 에이전트 시스템에서 [데이터 원본을 구성합니다](#) (페이지 575).
- Adobe Flash Player 의 버전이 9.0.28 이상인지 확인합니다. 이 플레이어는 다음 위치에서 다운로드할 수 있습니다.
<http://www.adobe.com/go/getflash>
- [에이전트 바이너리를 다운로드합니다](#) (페이지 576).
- [에이전트 인증 키를 가져옵니다](#) (페이지 576).
- 서버 이름/IP 가 바로 액세스 가능하도록 설정합니다.
- 보안에 해가 되지 않은 한도 내에서 계정 정보를 확보합니다.
에이전트가 서비스(Windows)로 실행될 때 이 계정이 사용됩니다.
- 커넥터가 있는 경우 기본 커넥터 정보를 내보내서 이 정보를 확보합니다.
- 시스템에 4 GB RAM 이 있는지 확인합니다.

에이전트 컴퓨터에서 데이터 원본 구성

에이전트 컴퓨터에서 데이터 원본을 구성하려면 다음 절차를 따르십시오.

데이터 원본을 구성하려면

1. "제어판", "관리 도구", "데이터 원본(ODBC)"으로 이동합니다.
2. "시스템 DSN" 탭에서 다음을 추가합니다.
감사 데이터베이스를 가리키는 imsauditevent12 데이터 원본(ODBC)
3. "적용"/"확인"을 클릭합니다.
데이터 원본이 구성되었습니다.

에이전트 바이너리 다운로드

에이전트 바이너리를 다운로드하려면 이 절차를 따르십시오.

다음 단계를 수행하십시오.

1. 다음 URL 을 사용하여 CA UAR 서버에 로그인합니다.
`https://<host>:5250/spin/calm/CALMSpindle.csp`
2. "관리", "Log Collection"(로그 수집), "Agent Explorer"(에이전트 탐색기), "Download Agent Binaries"(에이전트 바이너리 다운로드), OS 버전으로 이동합니다.
3. 파일을 저장합니다.

에이전트 인증 키 가져오기

에이전트 인증 키를 가져오려면 이 절차를 따르십시오.

다음 단계를 수행하십시오.

1. CA UAR 서버에서 "관리", "Log Collection"(로그 수집), "Agent Explorer"(에이전트 탐색기), "Agent Authentication Key"(에이전트 인증 키)로 이동합니다.
2. 보안에 해가 되지 않은 한도 내에서 이 키를 확보합니다.

CA UAR 에이전트 설치

CA UAR 에이전트는 이벤트를 수집하고 해당 정보를 CA UAR 서버로 발송하는 일을 수행합니다. 로깅을 사용하려면 CA Identity Manager 데이터베이스 서버 또는 끝점 컴퓨터에 에이전트를 설치하십시오.

참고: CA UAR 에이전트는 Windows 와 Linux 에서 지원됩니다.

다음 단계를 수행하십시오.

1. 데이터베이스 서버에서 `ca-elmagent-<버전>.exe` 설치를 실행하고 다음 정보를 지정합니다.
 - 서버 이름 또는 IP 주소
 - 인증 코드
 - 에이전트를 서비스/데몬으로 실행하는 데 사용되는 에이전트 서버 계정 정보
2. 기본 커넥터 목록 파일이 있는 경우 이 파일을 지정합니다.
3. 다음 URL 을 사용하여 CA UAR 서버에 로그인합니다.
`https://host:5250/spin/calm/CALMSpindle.csp`
4. "관리", "Log Collection"(로그 수집), "Agent Explorer"(에이전트 탐색기), "Default Agent Group"(기본 에이전트 그룹)으로 이동합니다.
5. 에이전트 컴퓨터를 선택하고 "Status and Command"(상태 및 명령) 뷰를 실행합니다.

역할 정의 가져오기

사용자 콘솔에서 엔터프라이즈 로그 매니저 연결을 구성하려면 먼저 CA Enterprise Role Definitions 를 먼저 가져오십시오.

역할 정의를 가져오려면:

1. 다음 URL 에서 관리 콘솔에 로그인합니다.
`http://host:port/iam/immanage`
2. "환경", "역할", "태스크" 설정으로 이동하여 "가져오기" 단추를 클릭한 다음 "엔터프라이즈 로그 매니저 - Enterprise Log Manager Role Definitions.xml"을 선택합니다.
3. "저장" 및 "닫기"를 클릭합니다.
4. 사용자 콘솔의 "시스템" 탭에서 "엔터프라이즈 로그 매니저 연결 구성"을 클릭한 다음 필요한 정보를 입력하고 "제출"을 클릭합니다.

새 커넥터 만들기

커넥터를 만들려면 이 절차를 따르십시오.

다음 단계를 수행하십시오.

1. 다음 URL 을 사용하여 CA UAR 서버에 로그인합니다.
`https://host:5250/spin/calm/CALMSpindle.csp`
2. "관리", "Log Collection"(로그 수집), "Agent Explorer"(에이전트 탐색기), "Default Agent Group"(기본 에이전트 그룹)으로 이동합니다.
3. 에이전트 컴퓨터를 선택합니다.
4. "커넥터" 보기로 전환합니다.
5. "Create a new Connector"(새 커넥터 만들기) 단추를 클릭하고 다음 정보를 입력합니다.

커넥터 정보

통합 유형으로 "CAIdentityManager"를 입력하고 필요한 경우 커넥터 이름을 변경합니다.

커넥터 구성

연결 문자열

- Driver={SQL 서버}; Server=<감사 DB 서버>; Database=<감사 DB>
- Driver={Microsoft ODBC for Oracle}; Dbq=<감사 DB TNSname>

사용자 이름: *감사DB 사용자*

암호: *감사DB 사용자 암호*

6. 12.6.4 에서 사용하기 위해 CA Identity Manager 커넥터에 다음과 같은 연결 구성 변경 사항을 적용합니다.
 - SourceName: 에이전트 컴퓨터의 데이터 원본 이름 - imsauditevent12
 - AnchorSQL: select max(id) from imsauditevent12
 - AnchorField: IMS_EVENTID
 - EventSQL:


```
select imsauditevent12.id as IMS_EVENTid ,imsauditevent12.audit_time as
IMS_AUDITTIME ,imsauditevent12.envname as ENVNAME
,imsauditevent12.admin_name as ADMINUNIQUENAME ,imsauditevent12.admin_dn as
ADMINID ,imsauditevent12.tasksession_oid as TRANSACTIONID
,imsauditevent12.event_description as
EVENTINFO ,imsauditevent12.event_state as
EVENTSTATE ,imsauditevent12.tasksession_oid as TASKOID
```

```
,imsaudittasksession12.task_name as  
TASKNAME ,imsauditeventobject12.object_type as OBJECTTYPE ,  
imsauditeventobject12.object_name as  
OBJECTUNIQUENAME ,imsauditobjectattributes12.attribute_name as  
ATTRNAME ,imsauditobjectattributes12.attribute_oldvalue as ATTROLDVALUE  
,imsauditobjectattributes12.attribute_newvalue as  
ATTRNEWVALUE ,imsauditobjectattributes12.attribute_newvalue as ATTRVALUE  
from  
imsaudittasksession12, imsauditevent12, imsauditeventobject12,  
imsauditobjectattributes12 where imsauditevent12.id >? and  
imsauditevent12.tasksession_id = imsaudittasksession12.id and  
imsauditevent12.tasksession_oid = imsaudittasksession12.tasksession_oid  
and  
imsauditeventobject12.parent_event_id = imsauditevent12.id and  
imsauditobjectattributes12.parent_object_id = imsauditeventobject12.id  
ORDER BY  
imsauditevent12.id ASC;
```

7. 저장하고 닫습니다.

커넥터가 작동하는지 확인하려면

1. "관리", "Log Collection"(로그 수집), "Agent Explorer"(에이전트 탐색기), "Default Agent Group"(기본 에이전트 그룹)으로 이동합니다.
2. 에이전트 컴퓨터를 선택합니다.
3. "Connectors"(커넥터) 뷰로 전환하여 "Launch Status and Command View"(상태 및 명령 뷰 실행) 단추를 클릭합니다.
상태가 실행됩니다.

CA Identity Manager 에서 감사를 사용하도록 설정

CA Identity Manager 에서 감사를 사용하도록 설정하려면

1. 관리 콘솔을 엽니다.

`http://host:port//iam/immanage`

2. "환경", <환경>, "고급 설정", "감사 중"으로 이동합니다.
3. 기존 설정을 내보내고 파일을 저장합니다.
4. 다음과 같이 저장된 파일을 수정하고 수정 내용을 저장합니다.

- `<Audit enabled="true" auditlevel="BOTH" datasource="java:/auditDbDataSource"`
- 이미 정의된 마지막 감사 프로필 아래에 암호 정책에 대한 감사 프로필을 추가합니다.

```
<AuditProfile objecttype="FWPASSWORDPOLICY"
auditlevel="BOTHCHANGED"/>
```

5. 파일을 관리 콘솔로 다시 가져오고 다음 중 하나를 실행하여 감사 정보의 집계를 트리거합니다.

- "사용자" 관리 개체에서 수행된 태스크
- "그룹" 관리 개체에서 수행된 태스크
- "암호 정책" 관리 개체에서 수행된 태스크

6. 다음 URL 을 사용하여 CA UAR 서버에 로그인합니다.

`https://host:5250/spin/calm/CALMSpindle.csp`

7. 기존 보고서를 실행하려면 "Queries and Reports"(쿼리 및 보고서), "Queries"(쿼리), "CA Identity Manager"로 이동합니다.

참고: CA UAR 서버가 미리 구성되어 있어야 합니다.

8. 수행한 태스크에 따라 다음 기본 보고서를 열어 이벤트가 수신되고 있는지 확인합니다.

- "사용자별 시스템 모든 이벤트" 태스크는 사용자 ID 로 필터링된 'CA Identity Manager - 시스템 모든 이벤트'를 호출합니다.
- "호스트별 계정 관리" 태스크는 있는 그대로 '호스트별 계정 관리'를 호출합니다.
- "계정별 계정 생성" 태스크는 있는 그대로 '계정별 계정 생성'을 호출합니다.

- "계정별 계정 삭제" 태스크는 있는 그대로 '계정별 계정 삭제'를 호출합니다.
- "계정별 계정 잠금" 태스크는 있는 그대로 '계정별 계정 잠금'을 호출합니다.
- "호스트별 인증서 프로세스 활동" 태스크는 있는 그대로 'CA Identity Manager - 호스트별 프로세스 활동'을 호출합니다.
- "암호 정책 수정 활동" 태스크는 있는 그대로 'CA Identity Manager - 정책 수정 활동'을 호출합니다.

CA Enterprise Log Manager 서버를 구성합니다.

관리할 CA Enterprise Log Manager 서버를 구성하기 전에 다음 사항을 확인하십시오.

- EiamAdmin 자격 증명이 있습니다.
- Adobe Flash Play 버전 9.0.28 이상이 있습니다.

CA Enterprise Log Manager 서버가 구성되면 다음 기능을 사용할 수 있습니다.

- 감사 이벤트를 산출하는 여러 환경이 하나의 CA Enterprise Log Manager 서버 또는 페더레이션된 계층에서 소비됩니다.
- 원격 시스템에 대한 데이터 권한 부여는 CA Enterprise Log Manager 의 데이터 액세스 필터를 통해 구현될 수 있습니다.

CA Enterprise Log Manager 서버를 구성하려면

1. 다음 URL 에서 CA Enterprise Log Manager Administrator 자격 증명을 사용하여 CA Enterprise Log Manager 서버 제품 등록 페이지에 로그인합니다.

`https://host:port/spin/calmap/products.csp`

2. "등록" 단추를 클릭하고 인증서 이름과 암호를 입력하여 CA Identity Manager 환경을 등록합니다.

참고: 각 환경에는 별도 등록(인증서 이름/암호) 쌍이 있어야 합니다.

3. "Administration"(관리), "User and Access Management"(사용자 및 액세스 관리), "New Data Access Filter"(새 데이터 액세스 필터)로 이동한 다음 만들 필터의 이름을 입력합니다.

4. 다음 단계로 진행합니다.

5. "All Identities"(모든 ID)에서 "Selected Identities"(선택한 ID)를 그대로 두고 다음 단계로 진행합니다.

6. "New Event Filter"(새 이벤트 필터) 단추를 클릭하여 액세스 필터를 만듭니다.

생성된 인증서를 CA CA Identity Manager 로부터 수집된 로그에 대해서만 컴퓨터/환경으로 제한하여 데이터 액세스 필터를 구성합니다. 관리 끝점에 대해서만 네이티브 끝점 정보를 액세스하도록 인증서를 제한할 수도 있습니다.

7. 저장하고 닫습니다.

8. "Open Access Policies"(액세스 정책 열기) 단추를 클릭하여 액세스 정책을 엽니다.
9. "Obligation Policies"(의무 정책)를 선택하고 사용 가능한 하나의 정책을 클릭합니다.
10. "All Identities"(모든 ID)를 제거하고 인증서 이름을 추가합니다.
11. 정책을 저장합니다.
12. Identity Manager 사용자 콘솔에 로그인하고 엔터프라이즈 로그 관리 연결을 구성합니다.

엔터프라이즈 로그 매니저 연결 구성

이 화면을 사용하여 새로 추가된 CA UAR 연결 태스크를 관리할 수 있습니다.

이 화면에는 다음 필드가 포함되어 있습니다.

연결 이름

단일 CA UAR 연결 관리 개체의 고유 이름을 지정합니다.

이 필드는 읽기 전용입니다.

호스트 이름(필수)

CA UAR 서버 호스트 이름 또는 IP 주소를 지정합니다.

포트 번호(필수)

CA UAR 서버 연결 포트를 지정합니다.

기본값: 52520

인증 기관이 서명한 SSL 인증서

이 확인란을 선택하면 CA UAR 서버에 연결할 때 엄격한 SSL 인증서 검사를 지정합니다.

기본적으로 CA UAR 과 함께 설치된 것과 같은 자체 서명된 SSL 인증서가 있는 경우 이 확인란을 선택 취소하십시오. 루트 인증 기관의 트러스트된 경로가 존재하지 않습니다.

인증서 이름(필수)

인증에 사용할 CA UAR 인증서의 이름을 지정합니다.

인증서 암호(필수)

CA UAR 암호를 지정합니다.

특성

지원 안 됨. 연결 정보를 테스트로 저장할 때 버전이 검색됩니다.

엔터프라이즈 로그 관리자 연결 삭제

목록에서 연결을 선택한 후 "삭제"를 클릭합니다. CA 엔터프라이즈 로그 관리자 연결 태스크가 삭제됩니다.

추가 CA Enterprise Log Manager 보고서 또는 쿼리를 CA Identity Manager 와 통합

"엔터프라이즈 로그 매니저 뷰어" 탭을 사용하여 추가 CA Enterprise Log Manager 보고서 또는 쿼리를 CA Identity Manager 와 통합할 수 있습니다. 이러한 새 보고서 또는 쿼리는 기존 태스크(마법사 포함) 및 새 태스크와 결합할 수 있습니다. 필요한 경우 CA Enterprise Log Manager 페더레이션된 데이터도 포함될 수 있습니다. "엔터프라이즈 로그 매니저 뷰어" 탭을 사용하여 검색된 정보에 필터를 적용할 수 있습니다. 이러한 필터는 다음을 사용할 수 있습니다.

- 상수 값
- 관리 개체의 특성
 - 예를 들어, physical - ::MyPhysicalAttribute::
logical - ::|MyLogicalAttribute|::
- CA Enterprise Log Manager CEG(Common Event Grammar)에 의해 기술된 모든 필드
 - dest_username
 - dest_objectname
 - dest_uid
 - source_username
 - source_objectname
 - source_uid
 - ...

엔터프라이즈 로그 매니저 뷰어 탭 구성

다음 필드를 하나 이상 포함하도록 CA "엔터프라이즈 로그 매니저 뷰어" 탭을 구성하십시오.

이름

탭에 할당하는 이름입니다.

태그

작업 내에서 고유한 탭의 식별자입니다. 문자나 밑줄로 시작해야 하며 문자, 숫자 또는 밑줄만 사용해야 합니다. 태그는 주로 XML 문서나 HTTP 매개 변수를 통해 데이터 값을 설정하는 데 사용됩니다.

탭 숨기기

탭이 작업에 표시되지 않도록 합니다. 이 옵션은 탭을 숨겨야 하지만 탭의 특성에 대한 액세스가 필요한 응용 프로그램에 유용합니다.

엔터프라이즈 로그 매니저 쿼리

CA UAR 쿼리가 표시됨을 지정합니다.

참고: CA 엔터프라이즈 로그 매니저 쿼리 또는 CA 엔터프라이즈 로그 매니저 보고서 중 하나를 지정할 수 있지만 둘 모두를 지정할 수는 없습니다.

엔터프라이즈 로그 매니저 보고서

CA UAR 보고서가 표시됨을 지정합니다.

엔터프라이즈 로그 매니저 ID

쿼리나 보고서에 대한 ID 를 지정합니다.

연결된 데이터 포함

연결된 데이터를 결과에 포함하거나 제외합니다. 기본적으로 이 필드는 선택되어 있지 않습니다.

확인 메시지 표시

CA UAR 확인 메시지 쿼리만 지정합니다. 기본적으로 이 필드는 선택되어 있지 않습니다.

필터

CA UAR 쿼리나 보고서에서 반환하는 결과를 좁히는 데 사용할 SQL 기반 고급 조건을 지정합니다. 상수 및 동적 값을 포함할 수 있습니다. 다음 코드는 샘플 식입니다.

```
((source_uid EQUAL ::logical.attribute.X:: ) AND (source_username  
EQUAL ::logical.attribute.Y:: ))
```

지원되는 오퍼레이션에는 다음이 포함됩니다.

- 다음과 같음(EQUAL)
- 다음과 같지 않음(NEQ)
- 미만(LESS)
- 초과(GREATER)
- 이하(LEQ)
- 이상(GREATEQ)
- 유사(LIKE)
- 유사하지 않음(NOTLIKE)
- 설정됨(INSET)
- 설정되지 않음(NOTINSET)

지원 접속사에는 다음이 포함됩니다.

- AND
- OR

괄호는 필수입니다. 조건식 왼쪽의 값 양쪽에 ":" 표시가 없는 경우, 이 값은 상수로 간주되어 CA UAR 로 있는 그대로 전송됩니다.

매개 변수/값 테이블

범위 지정에 사용할 필드와 값을 지정합니다.

범위 지정의 태그 및 태그 로직과 일치하는 쿼리나 보고서만 선택됩니다.

매개 변수

시작, 중지 및 제한 매개 변수에 대한 값을 지정합니다. 지원되는 매개 변수는 다음과 같습니다.

- 시간 단위(추세 전용)
- 시작 시간
- 종료 시간
- 가장 빠른 그룹 이벤트에 이후 날짜 설정(그룹화된 쿼리 전용)
- 가장 늦은 그룹화된 이벤트에 이후 날짜 설정(그룹화된 쿼리 전용)
- 가장 늦은 그룹화된 이벤트에 이전 날짜 설정(그룹화된 쿼리 전용)

- 그룹의 최소 이벤트 수(그룹화된 쿼리 전용)
- 그룹의 최대 이벤트 수(그룹화된 쿼리 전용)

제 19 장: 액세스 역할

액세스 역할은 CA Identity Manager 또는 다른 응용 프로그램에서 권한을 제공하는 추가적인 방법을 제공합니다. 예를 들어 액세스 역할을 사용하여 다음을 수행할 수 있습니다.

- 사용자 특성에 대한 간접 액세스 제공
- 복합 식 만들기
- 다른 응용 프로그램에서 권한을 결정하는 데 사용되는 사용자 프로필의 특성 설정

액세스 역할은 일련의 비즈니스 변경 내용을 사용자나 사용자 그룹에 적용한다는 점에서 ID 정책과 유사합니다. 그러나 액세스 역할을 사용하여 비즈니스 변경 내용을 적용하면 액세스 역할의 구성원을 확인하여 변경 내용이 적용되는 사용자를 알 수 있습니다.

대부분의 경우 액세스 역할은 태스크와 관련되지 않습니다.

참고: CA Identity Manager 가 CA SiteMinder 와 통합된 경우 액세스 역할이 CA SiteMinder 로 보호된 응용 프로그램에 대한 액세스를 제공할 수도 있습니다. 이 경우 액세스 역할에는 액세스 태스크가 포함됩니다. 자세한 내용은 *Configuration Guide*(구성 안내서)의 SiteMinder 통합 장을 참조하십시오.

이 섹션은 다음 항목을 포함하고 있습니다.

[액세스 역할이 권한을 관리하는 방법](#) (페이지 592)

[예: 간접 프로필 특성 수정](#) (페이지 592)

[액세스 역할 만들기](#) (페이지 593)

액세스 역할이 권한을 관리하는 방법

변경 동작을 지정함으로써 액세스 역할을 사용하여 권한을 관리할 수 있습니다. 변경 동작은 사용자가 역할의 구성원 또는 관리자를 추가 또는 제거할 때 발생합니다.

액세스 역할을 사용하려면 다음 단계를 완료하십시오.

1. 관리자가 액세스 역할을 만듭니다.
2. "구성원" 탭에서 관리자가 동작 추가 또는 제거를 지정합니다. 이러한 동작은 액세스 역할이 사용자에게 할당되었을 때 CA Identity Manager 가 취하는 동작을 결정합니다.
3. 필요한 경우 관리자가 관리자 및 소유자 정책을 지정하고 액세스 역할을 만들기 위해 이 태스크를 제출합니다.
4. 액세스 역할 관리자가 액세스 역할을 사용자에게 할당합니다.
5. CA Identity Manager 가 역할에 지정된 동작 추가를 완료합니다.

예: 간접 프로필 특성 수정

액세스 역할을 사용하여 사용자의 프로필에서 특성을 간접적으로 변경할 수 있습니다. 예를 들어, 회사에서는 사용자들이 직접 다른 사용자의 직함을 변경할 수 없도록 해야 할 것입니다. 이 경우, 회사는 관리자가 해당 역할을 사용자에게 할당할 경우 직함을 변경하는 액세스 역할을 만들 수 있습니다.

특성을 간접적으로 변경하려면 해당 액세스 역할에 대한 변경 동작을 설정합니다. 관리자가 이 역할을 할당하면 변경 동작이 사용자 프로필에서 하나 이상의 특성을 변경할 수 있습니다.

액세스 역할을 사용하여 특성을 간접적으로 수정하려면 다음을 수행하십시오.

1. 액세스 역할을 만듭니다.
2. "구성원" 탭에서 "관리자가 이 역할의 관리자를 추가하거나 제거할 수 있습니다" 확인란을 선택하고 화살표 아이콘을 클릭합니다.
CA Identity Manager 에 추가 "동작 추가" 또는 "동작 제거" 필드가 표시됩니다.
3. "동작 추가" 또는 "동작 제거" 필드의 목록 상자에서 동작을 선택합니다.
선택한 옵션에 따라 CA Identity Manager 에 추가 필드가 표시됩니다.

4. 필요한 경우 동작 추가 또는 제거를 구성합니다.
5. "관리자" 탭을 선택하여 생성하는 액세스 역할에 구성원을 추가할 수 있는 관리자를 지정합니다.
6. "소유자" 탭을 선택하여 액세스 역할 정의를 수정할 수 있는 관리자를 지정합니다.
7. "제출"을 클릭하여 액세스 역할 생성을 완료합니다.
8. 필요하면 액세스 역할을 사용자에게 할당합니다.

액세스 역할 만들기

액세스 역할을 만드는 과정에는 다음 단계가 포함됩니다.

- [액세스 역할 만들기 시작](#) (페이지 593)
- [액세스 역할의 프로필 정의](#) (페이지 594)
- [액세스 역할의 구성원 정책 정의](#) (페이지 594)
- [액세스 역할의 관리자 정책 정의](#) (페이지 595)
- [액세스 역할의 소유자 규칙 정의](#) (페이지 595)

액세스 역할 만들기 시작

1. 액세스 역할을 만드는 작업이 포함된 역할을 가진 Identity Manager 계정에 로그인합니다.
2. "액세스 역할", "액세스 역할 만들기"를 클릭합니다.
새 역할이나 역할 사본을 만드는 옵션을 선택합니다. "복사"를 선택한 경우 역할을 검색합니다.
3. 다음 섹션인 액세스 역할의 프로필 정의로 계속 진행합니다.

액세스 역할의 프로필 정의

액세스 역할의 프로필을 정의하려면

1. 이름과 설명을 입력하고, 역할에 대해 정의된 사용자 지정 특성을 완료합니다.

참고: "프로필" 탭에서 액세스 역할에 대한 추가 정보를 지정하는 사용자 지정 특성을 지정할 수 있습니다. 이 추가 정보를 사용하여 수많은 역할을 포함하는 환경에서 역할을 쉽게 검색할 수 있습니다.

2. 역할을 만드는 즉시 사용할 수 있게 하려면 "사용"을 선택합니다.
3. 다음 섹션인 [액세스 역할의 구성원 정책 정의](#) (페이지 594)로 계속 진행합니다.

액세스 역할의 구성원 정책 정의

"구성원" 탭에서 다음을 수행합니다.

1. "추가"를 선택하여 구성원 정책을 정의합니다.
2. (선택 사항) "구성원 정책" 페이지에서 선택적으로 이 역할을 사용할 수 있어야 하는 사람에 대한 구성원 규칙을 정의합니다.

이렇게 하면 구성원 정책의 조건과 일치하는 사용자에게 자동으로 역할이 할당됩니다.

3. 구성원 정책이 구성원 탭에 나타나는지 확인합니다.

정책을 편집하려면 왼쪽에 있는 화살표 기호를 클릭합니다. 정책을 제거하려면 빼기 기호 아이콘을 클릭합니다.

4. "구성원" 탭에서 "관리자가 이 역할의 구성원을 추가하거나 제거할 수 있습니다." 확인란을 선택합니다.

이 기능을 사용하도록 설정한 후 "추가 동작" 및 "제거 동작"을 정의합니다. 두 동작은 사용자가 역할의 구성원으로 추가되거나 삭제되는 경우에 수행되는 작업을 정의합니다.

5. 다음 섹션인 [액세스 역할의 관리자 정책 정의](#) (페이지 595)로 계속 진행합니다.

액세스 역할의 관리자 정책 정의

"관리자" 탭에서 다음을 수행합니다.

1. "관리자 관리" 옵션을 사용할 수 있게 하려는 경우 "관리자가 이 역할의 관리자를 추가하거나 제거할 수 있습니다." 확인란을 선택합니다.

이 기능을 사용하도록 설정한 후 사용자가 역할 관리자로 추가되거나 제거되는 경우에 대한 동작을 정의합니다.

2. "관리자" 탭에서 관리자 및 범위 규칙과 관리자 권한이 포함된 관리자 정책을 추가합니다. 각 정책에 적어도 하나의 권한("구성원 관리" 또는 "관리자 관리")이 필요합니다.

규칙을 충족하는 관리자에 대해 다른 규칙과 다른 권한을 사용하는 여러 관리자 정책을 추가할 수 있습니다.

3. 정책을 편집하려면 왼쪽에 있는 화살표 기호를 클릭합니다. 정책을 제거하려면 빼기 기호 아이콘을 클릭합니다.

4. 다음 섹션인 [액세스 역할의 소유자 규칙 정의](#) (페이지 595)로 계속 진행합니다.

액세스 역할의 소유자 규칙 정의

"소유자" 탭에서 다음을 수행합니다.

1. 역할을 수정할 수 있는 사용자를 결정하는 소유자 규칙을 정의합니다.
2. "제출"을 클릭합니다.

작업이 제출되었음을 나타내는 메시지가 표시됩니다. 사용자가 역할을 사용할 수 있기 전에 일시적인 지연이 발생할 수도 있습니다.

제 20 장: 시스템 작업

이 섹션은 다음 항목을 포함하고 있습니다.

- [기본 시스템 작업](#) (페이지 597)
- [피더 파일을 사용한 사용자 추가 방법](#) (페이지 599)
- [로더 레코드 정보 탭](#) (페이지 604)
- [로더 동작 매핑 탭](#) (페이지 605)
- [로더 알림 정보 탭](#) (페이지 606)
- [대량 로더 태스크 변경 사항 승인](#) (페이지 606)
- [대량 로더 태스크에 대한 전자 메일 알림 구성](#) (페이지 607)
- [Bulk Loader 태스크 예약](#) (페이지 608)
- [대량 로더의 구문 분석기 파일 수정](#) (페이지 608)
- [Bulk Loader 를 위한 웹 서비스 지원](#) (페이지 609)
- [JDBC 연결 관리](#) (페이지 610)
- [논리적 특성 처리기](#) (페이지 610)
- [선택란 데이터](#) (페이지 614)
- [상관 관계 특성 구성 태스크 화면](#) (페이지 615)
- [이벤트에 대한 전역 정책 기반 워크플로 구성 태스크 화면](#) (페이지 616)
- [CA Identity Manager 의 태스크 상태](#) (페이지 617)
- [제출된 태스크 정리](#) (페이지 636)
- [되풀이 태스크 삭제](#) (페이지 641)
- [엔터프라이즈 로그 매니저 연결 구성](#) (페이지 642)
- [엔터프라이즈 로그 매니저 연결 삭제](#) (페이지 643)
- [비밀 키 관리](#) (페이지 644)

기본 시스템 작업

CA CA Identity Manager 에는 관리자의 CA Identity Manager 환경 관리를 도와주는 다음과 같은 태스크가 포함되어 있습니다.

- 제출한 작업 보기 작업
관리자가 환경의 작업 상태를 볼 수 있게 합니다. 또한 더 이상 사용되지 않는 태스크를 "제출한 태스크 보기" 화면에서 제거합니다.
- Bulk Loader 작업
많은 관리 개체를 동시에 조작하는 데 사용되는 피더 파일을 업로드합니다.

- 대량 태스크

부서, 시/군/구, 종료일 등과 같은 개체의 특성을 기준으로 사용자와 같은 개체에 대해 태스크를 실행합니다. 이 태스크를 정기적으로 실행할 수 있습니다(예: 매주 토요일).

또한 이 태스크를 사용하여 대량 사용자 변경을 수행할 수 있습니다.

- 선택란 데이터 작업

관리자가 관리자 작업의 필드(예: 선택란)를 채우는 데 사용되는 파일을 업로드할 수 있게 합니다.

- 논리적 특성 처리기 작업

관리자가 사용자 저장소 특성(물리적 특성이라고 함)을 사용자에게 친숙한 형식으로 작업 화면에 표시하는 데 사용되는 논리적 특성을 관리할 수 있게 합니다.

- JDBC 연결 관리 태스크

CA CA Identity Manager 에서 데이터베이스 서버 연결 상세 정보를 구성합니다.

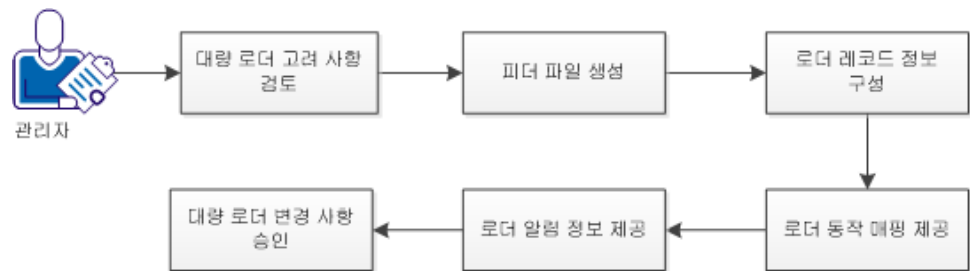
- 전자 메일 태스크

전자 메일 알림 정책을 관리합니다.

피더 파일을 사용한 사용자 추가 방법

"대량 로더" 탭에서 많은 관리 개체를 동시에 조작하는 데 사용되는 피더 파일을 업로드할 수 있습니다. 예를 들어, 시스템에서 수동으로 1000 명의 사용자를 만들거나 대량 로더를 사용할 수 있습니다. 대량 로더 태스크를 워크플로 프로세스에 매핑할 수도 있습니다.

대량 로드 클라이언트는 일괄 처리를 위해 존재하는 명령줄 유틸리티입니다. 클러스터 기반 환경인 경우(로드 균형 조정을 위해) 대량 로드 클라이언트를 사용하는 것이 좋습니다. 대량 로드 클라이언트는 프로비저닝 구성 요소 미디어에 있습니다.



다음 단계를 수행하십시오.

1. [대량 로더 고려 사항을 검토합니다](#) (페이지 600).
2. [CSV 또는 XLS 피더 파일을 만들고](#) (페이지 603) 업로드합니다.
3. ["로더 레코드 정보"를 구성합니다](#) (페이지 604).

이 탭을 사용하여 피더 파일에 동작 및 식별자 필드를 지정할 수 있습니다.

4. [로더 동작 매핑을 제공합니다](#) (페이지 605).

이 탭을 사용하여 기본 개체를 선택하고 개체에 대한 동작을 위해 실행할 태스크를 지정할 수 있습니다.

5. [로더 알림 정보를 제공합니다](#) (페이지 606).

이 탭을 사용하여 대량 로더 태스크 변경 내용을 인증할 사용자를 선택할 수 있습니다.

6. [대량 로더 태스크 변경 내용의 진행 사항을 보고 수정합니다](#) (페이지 606).

대량 로더 고려 사항

"대량 로더" 탭에서 많은 관리 개체를 동시에 조작하는 데 사용되는 피더 파일을 업로드할 수 있습니다. 대량 로더를 사용할 때는 다음 사항을 고려하십시오.

- 야간과 같이 바쁘지 않은 시간 동안 대량 로드를 수행하도록 예약하는 것이 좋습니다. 큰 규모의 대량 로드는 성능에 영향을 줄 수 있습니다. 경우에 따라 많은 하위 태스크가 포함된 대량 로드인 경우 대량 로드를 마칠 때까지 사용자의 제출한 태스크가 완료되지 않을 수 있습니다.
- 많은 개체 업로드와 같은 장기 실행 태스크 중에 서버가 중단될 경우 "제출된 태스크 보기" 탭에서 태스크를 다시 시작하십시오. 태스크가 다시 시작되면 성공적으로 실행된 마지막 레코드부터 태스크가 시작됩니다.
- LDAP 을 Solaris 에서 사용자 저장소로 사용하는 경우 가져오기 중에 대량 로더가 중단될 수 있습니다. 이 문제를 해결하려면 *Configuration Guide*(구성 안내서)의 "Specify LDAP Connection Settings"(LDAP 연결 설정 지정) 항목을 참조하고 해당 설정을 적용하십시오.
- 대량 로더를 사용하여 많은 수의 사용자를 가져오는 경우 메모리 부족 예외가 발생할 수 있습니다. 이 문제를 해결하려면 다음 힙 크기 메모리 매개 변수를 조정하십시오.
 - -Xmx
 - -XX:maxPermSize

참고: 메모리 매개 변수의 조정에 대한 자세한 내용은 응용 프로그램 서버 문서를 참조하십시오.

- 대량 로더를 사용하여 많은 사용자를 만드는 등 많은 관리 개체를 조작할 경우 성능이 저하될 수 있습니다. 성능을 향상시키려면 다음 권장 사항을 따르는 것이 좋습니다.
 - 사용자 콘솔을 사용하여 대량 로드 수행하는 경우 큰 CSV 파일 하나를 작은 파일 여러 개로 나눕니다. 예를 들어 사용자 10,000 명의 대량 로드 10 개를 수행하는 것이 사용자 100,000 명의 대량 로드 하나를 수행하는 것보다 빠릅니다.
- 참고:** CSV 파일 내의 항목이 50,000 개 이상이면 시스템에 문제가 발생할 수 있습니다.
- 대량 로드를 수행 중인 사용자의 태스크 수를 제한합니다. 예를 들어 대량 로드를 시작하는 관리자의 태스크가 적은 경우 성능이 향상됩니다. 관리자의 태스크가 많은 경우에는 CA Identity Manager가 더욱 포괄적인 권한 검사를 수행해야 하므로 성능이 저하될 수 있습니다.
 - 프로비저닝을 수반하는 대량 변경과 관련된 Policy Xpress 정책 수를 제한합니다. 또한 대량 로드 오퍼레이션 중에 복합 정책만큼 크게 성능을 저하시키지는 않는 단순 Policy Xpress 정책을 만드는 것이 좋습니다.
 - 시스템 리소스가 충분한지 확인합니다.

대량 로드 성능 개선을 위한 데이터 유효성 검사 제한

관리자 태스크는 일반적으로 여러 탭을 포함합니다. 기본적으로 대량 오퍼레이션은 태스크의 각 탭에서 데이터의 유효성을 검사합니다.

유효성 검사는 대량 오퍼레이션의 성능에 영향을 줄 수 있습니다. 성능을 개선하기 위해 태스크 탭에 대한 데이터 유효성 검사가 필요하지 않은 경우가 이 검사를 비활성화할 수 있습니다.

다음 단계를 수행하십시오.

1. 관리자 태스크를 수정할 수 있는 사용자로 사용자 콘솔에 로그인합니다.
2. "태스크", "관리자 태스크", "관리자 태스크 수정"을 선택합니다.
3. 대량 오퍼레이션에 적용되는 태스크를 검색하여 선택합니다.
4. "탭"을 선택한 다음 수정할 탭을 선택합니다.
5. "Do Not Validate in Bulk Operations"(대량 오퍼레이션에서 유효성 검사 안 함)을 선택한 다음 "확인"을 클릭합니다.

6. 데이터 유효성 검사가 필요 없는 각 탭에 대해 4 단계 및 5 단계를 반복합니다.
7. 제출을 클릭합니다.
수정한 탭에 대해 데이터 유효성 검사가 비활성화됩니다.

사용자 지정 비즈니스 로직 제한

대량 오퍼레이션에 사용된 태스크에 사용자 지정 비즈니스 로직(예: 비즈니스 로직 태스크 처리기 및 이벤트 수신기)을 추가하면 성능에 영향을 줄 수 있습니다.

성능을 개선하려면 대량 업로드 오퍼레이션에서 사용자 지정 비즈니스 로직을 비활성화하십시오.

다음 단계를 수행하십시오.

1. 관리 콘솔을 엽니다.
2. 이벤트 수신기 또는 비즈니스 로직 태스크 처리기를 포함하는 응용 프로그램 환경을 선택합니다.
3. "고급 설정", "비즈니스 로직 태스크 처리기"(사용 가능한 경우)를 선택합니다.
4. `UseInBulkOperation` 속성의 값을 `false` 로 설정한 다음 "저장"을 클릭합니다.
5. 이벤트 수신기에 대해 4 단계를 반복합니다.
6. 비즈니스 로직 태스크 처리기 및 이벤트 수신기에 대한 수정을 완료한 후에는 환경을 다시 시작합니다.

피더 파일 만들기

대량 로더 파일은 관리된 많은 개체에서 수행되는 반복 동작을 자동화하는데 사용됩니다. 피더 파일을 업로드하면 시스템은 이 피더 파일을 구문 분석하고 읽습니다.

피더 파일은 확장자가 CSV 또는 XLS 여야 하고 다음과 같은 속성이 있어야 합니다.

- 이 파일에는 관리 개체의 물리적 특성, 논리적 특성 또는 알려진 특성 이름을 지정하는 머리글 줄이 있어야 합니다.
- 머리글 줄에는 레코드에서 수행해야 하는 동작을 나타내는 열이 포함되어 있어야 합니다.
- 피더 파일의 각 행을 레코드라고 합니다. 레코드에는 머리글 줄에 지정된 각 특성의 값이 포함되어 있습니다. 다음 옵션은 특성에 대해 허용 가능한 값입니다.
 - Value - 특성이 지정한 값으로 설정됩니다.
 - Value;Value;Value;... - 특성이 지정한 여러 값의 특성으로 설정됩니다.
 - ''(비어 있음) - 특성이 변경되지 않습니다.
 - NULL - 특성이 삭제되었습니다. 삭제 시퀀스는 기본적으로 NULL 로 설정되지만 "대량 로더 파일 업로드 검색" 화면에서 편집할 수 있습니다.

참고: 피더 파일에 해시(#)를 사용하려면 해시 기호를 큰따옴표로 묶으십시오. 예를 들어, user#1 은 "user#1"로 지정해야 합니다.

중요! 피더 파일은 UTF-8 인코딩으로 저장해야 합니다.

사용자를 만들기 위한 샘플 피더 파일

이 샘플 피더 파일은 특정한 필수 특성이 있는 사용자를 만듭니다.

```
action,%USER_ID%,%FIRST_NAME%,%LAST_NAME%,%FULL_NAME%,%PASSWORD%,%EMAIL%
create,JD,John,Doe,John Doe,mypassword,Johndoe@a.com
create,BD,Baby,Doe,Baby Doe,mypassword2,Babydoe@a.com
```

앞의 코드에서 피더 파일에는 다음과 같은 속성이 있습니다.

머리글

코드의 첫 번째 줄은 머리글 줄입니다. 머리글 줄에는 관리 개체 '사용자'에 대한 물리적 특성이나 알려진 특성이 있습니다.

동작

동작 열은 각 레코드에 대해 수행해야 하는 태스크를 식별합니다. 예를 들어, 앞의 파일은 이름이 'John'에 대해 '만들기' 동작을 수행하도록 지정합니다.

사용자를 설정하기 위한 샘플 피더 파일

이 샘플 피더 파일은 |enabled| 논리적 특성의 값을 변경합니다. 파일의 머리글에서 논리적 특성을 지정하고 각 사용자 항목에서 값(이 경우 true 또는 false)을 지정합니다.

```
action,%USER_ID%,|enable|  
  
MODIFY,user1,false  
  
MODIFY,user2,true
```

로더 레코드 정보 탭

"로더 레코드 정보" 탭에는 피더 파일에서 사용할 수 있는 레코드의 짧은 미리 보기가 표시됩니다. 미리 보기 테이블에는 최대 5 개 레코드가 표시됩니다. 사용자는 미리 보기 테이블을 통해 올바른 파일이 업로드되고 있는지 확인할 수 있습니다. 이 탭에서 피더 파일에 지정된 관리 개체에서 수행할 동작을 식별할 수도 있습니다. 다음 필드를 완료해야 합니다.

개체에서 수행할 동작을 나타내는 필드는 무엇입니까?

관리 개체에서 수행할 동작을 지정하는 피더 파일의 필드를 식별합니다. 예를 들어, 값으로 "만들기", "수정" 및 "삭제"를 사용하는 '동작' 필드가 있는 피더 파일을 사용할 수 있습니다. [로더 동작 매핑](#) (페이지 605)에서 각 동작을 관리자 태스크에 매핑해야 합니다.

개체를 고유하게 식별하는 데 사용될 필드는 무엇입니까?

기본 개체를 고유하게 식별할 수 있는 피더 파일의 필드를 식별합니다.

참고: 피더 파일에 잘못된 머리글 줄이 있으면 "로더 레코드 정보" 탭에 해당 피더 파일 레코드가 표시되지 않습니다. 머리글 파일이 잘못된 경우 다른 피더 파일을 선택하십시오. 피더 파일에 잘못된 레코드가 있는 경우 "시스템" 탭 아래 "제출한 태스크 보기"에 자세한 업로드 상태가 포함됩니다.

로더 동작 매핑 탭

"로더 동작 매핑" 탭에서 피더 파일에 지정된 동작을 수행할 기본 개체를 선택할 수 있습니다. 또한 피더 파일의 동작을 선택한 기본 개체에 대한 관리자 태스크에 매핑해야 합니다.

주 개체는 무엇입니까?

CA Identity Manager 에서 피더 파일을 사용하여 조작할 기본 개체를 식별합니다. 다음 기본 개체 중 하나를 선택할 수 있습니다.

- 사용자
- 그룹
- 조직

'동작'에 대해 실행할 작업을 선택하십시오.

"삭제" 또는 "수정" 태스크와 같이 피더 파일에 의해 지정된 각 동작에 대해 수행될 관리자 태스크를 식별합니다.

참고: 피더 파일의 모든 동작을 관리자 태스크에 매핑해야 합니다. 또한 이 필드에 표시되는 관리자 태스크는 선택한 기본 개체에 따라 달라집니다. 예를 들어, '사용자'를 기본 개체로 선택한 경우 '사용자'와 관련된 관리자 태스크만 표시됩니다.

'동작'의 존재하지 않는 개체에 대한 태스크를 선택하십시오.

"만들기" 태스크와 같이 관리 개체가 CA Identity Manager 내에 아직 존재하지 않을 경우 피더 파일에 지정된 동작에 대해 수행될 대체 관리자 태스크를 식별합니다.

로더 알림 정보 탭

중요! 기본적으로 "대량 로더" 마법사에는 이 탭이 포함되지 않습니다. 따라서 "대량 로더" 태스크를 수정하고 "로더 알림 정보" 탭을 추가하여 수동으로 이 탭을 추가해야 합니다. 또한 이 탭을 사용하려면 해당 환경에서 워크플로를 사용하도록 설정해야 합니다.

"로더 알림 정보" 탭에서는 "대량 로더" 태스크에 대한 인증 매니저를 선택할 수 있습니다. 대량 로더 태스크가 완료되면 **CA Identity Manager** 가 이 태스크에 대해 구성된 모든 인증 매니저에 대한 대량 로더 알림을 만듭니다. 이 알림은 "홈" 탭의 "대량 로더 알림" 아래에 나타납니다. 알림을 클릭하면 대량 로드 오퍼레이션으로 시작된 태스크의 정보가 표시됩니다. 인증 매니저는 알림에 설명되어 있는 변경 내용을 검토하고 승인할 수 있습니다.

참고: 인증 매니저 목록을 제공하려면 드롭다운 목록에서 사용할 수 있는 참가자 해결 프로그램 중 하나를 사용하십시오. 참가자 해결 프로그램에 대한 자세한 내용은 이 안내서의 "워크플로" 섹션을 참조하십시오.

대량 로더 태스크 변경 사항 승인

대량 태스크 알림에는 대량 로더 태스크가 수행한 모든 변경 사항에 대한 정보가 수록되어 있습니다. 인증 매니저는 대량 로더 태스크로 시작된 모든 변경 사항을 검토하고 승인할 수 있습니다.

대량 로더 태스크 변경 사항을 검토하고 승인하려면

1. 대량 로더 태스크의 인증 매니저로 나열된 사용자로 사용자 콘솔에 로그인합니다.
2. "홈", "내 대량 로더 알림 보기"로 이동합니다.

3. 검토하려는 대량 로더 알림을 선택합니다.

"대량 로더 알림 관리" 화면이 나타나고 시작된 모든 대량 로더 태스크 변경 사항이 나열된 테이블이 표시됩니다.

이 화면에서 다음 작업을 수행할 수 있습니다.

- 개체 만들기 또는 수정을 위한 특정 태스크 정보를 검토하려면 "설명" 열 아래에 있는 하이퍼링크를 클릭합니다.
- 규정 준수 위반이 발생하거나 사용자에게 추가한 역할을 제거하려는 경우 사용자 ID 옆에 있는 "편집" 아이콘을 클릭하여 알림 화면에서 직접 사용자를 편집할 수 있습니다.
- 사용자에게 추가된 역할을 검토하려면 "요청된 역할 할당" 열 아래에서 사용자 ID 와 연결된 하이퍼링크를 클릭합니다.

4. 특정 개체에 대한 모든 변경 사항을 검토했으면 해당 개체에 대한 "승인" 확인란을 선택합니다.

5. 변경 사항 승인을 완료했으면 "승인"을 클릭하여 목록에서 선택한 모든 변경 사항 알림을 제거합니다.

참고: "모두 승인"을 선택하여 대량 로더 알림의 모든 변경 사항을 승인할 수 있습니다. 이렇게 하면 "홈" 탭에서 "대량 로더 알림"이 삭제됩니다. 또한 "승인" 열 맨 위에 있는 확인란을 선택하여 현재 화면에 표시된 모든 변경 알림을 선택할 수 있으며 화면 단위로 변경 사항을 승인할 수 있습니다.

대량 로더 태스크와 연결된 모든 사용자 변경 사항이 승인되면 "홈" 탭에서 "대량 로더 알림"이 사라집니다.

대량 로더 태스크에 대한 전자 메일 알림 구성

일부 환경에서 대량 오퍼레이션 전자 메일 알림은 기본적으로 구성됩니다. 대량 오퍼레이션 전자 메일이 시스템에서 구성되었는지 확인하려면 "시스템", "전자 메일 보기"로 이동한 다음 용어 '대량'을 찾으십시오.

환경에서 전자 메일 알림이 구성되어 있지 않은 경우 대량 오퍼레이션이 완료될 때 발송된 전자 메일을 구성하십시오.

다음 단계를 수행하십시오.

1. 사용자 콘솔에서 "시스템", "전자 메일", "전자 메일 만들기"로 이동합니다.
2. "프로필" 탭에서 필수 필드를 완성합니다.

3. "보낼 조건" 탭에서 다음 단계를 완료합니다.
 - a. 첫 번째 필드에서 "태스크 완료"를 선택합니다.
 - b. 두 번째 필드에서 "대량 로더"를 선택합니다.
4. "받는 사람"과 "콘텐츠" 탭을 완성한 다음 "제출"을 클릭합니다.
대량 로더 태스크에 대해 전자 메일 알림이 구성되었습니다.

Bulk Loader 태스크 예약

시스템에서 대량 로더 태스크를 예약할 수 있습니다. Bulk Loader 태스크를 예약하려면 태스크에 [스케줄러 탭을 추가](#) (페이지 73)하십시오.

대량 로더의 구문 분석기 파일 수정

피더 파일을 구문 분석하기 위해 사용하는 구문 분석기를 수정하려면 해당 관리자 태스크를 구성하십시오.

대량 로더 관리자 작업을 수정하려면

1. "역할 및 태스크", "관리자 태스크", "관리자 태스크 관리"로 이동합니다.
2. 대량 로더 태스크를 검색합니다.
3. 대량 로더 태스크를 선택하고 "선택"을 클릭합니다.
4. 대량 로드 태스크의 "검색" 탭을 선택합니다.
5. "찾아보기"를 클릭하여 검색 화면을 찾습니다.
사용 가능한 검색 화면 목록이 표시됩니다.
6. 검색 화면을 선택하고 "편집"을 클릭합니다.
검색 화면 상세 정보가 나타납니다.

7. (선택 사항) "구문 분석기 정식 이름"을 편집합니다.

"구문 분석기 정식 이름"은 구문 분석기 파일의 이름과 일치해야 합니다.

참고: 사용자 지정 CSV 구문 분석기 만들기에 대한 자세한 내용은 Javadoc 에서 FeederParser 클래스를 참조하십시오. 응용 프로그램 서버로 JBoss 를 사용하여 사용자 지정 구문 분석기를 만드는 경우 사용자 지정 구문 분석기 파일은

iam_im.ear/user_console_war/WEB-INF/classes 디렉터리에 있어야 합니다.

8. "확인"을 클릭합니다.

Bulk Loader 를 위한 웹 서비스 지원

대량 로더에는 CA Identity Manager TEWS(Task Execution Web Service) 인터페이스를 사용하여 호출할 수 있는 웹 서비스 API 가 포함되어 있습니다. TEWS 를 통해 클라이언트 응용 프로그램이 실행할 원격 태스크를 CA Identity Manager 로 제출할 수 있습니다. 이 인터페이스는 WSDL 및 SOAP 개방형 표준을 구현하여 CA Identity Manager 에 대한 원격 액세스를 제공합니다.

CA Identity Manager 에는 대량 로더를 웹 서비스로서 호출하는 방법을 설명하는 Java 클라이언트 예제가 포함되어 있습니다. Java 예제는 다음 소스 파일에 있습니다.

`admin_tools\samples\WebService\Axis\optional\ObjectsFeeder.java`

대량 로더를 웹 서비스로서 호출하는 데이터 샘플 및 문서는 다음 디렉터리에 있습니다.

`admin_tools\samples\Feeder\`

참고: 자세한 내용은 *Programming Guide for Java*(Java 프로그래밍 안내서)를 참조하십시오.

JDBC 연결 관리

CA CA Identity Manager 보고서에 대한 정보는 여러 출처로부터 제공될 수 있으며 각 보고서는 보고서에서 볼 정보에 따라 특정 데이터 원본과 연결되어야 합니다.

보고를 위한 다른 데이터 원본(감사 데이터베이스 또는 태스크 지속 데이터베이스 등)을 설정하려면 CA CA Identity Manager 에서 연결 관리 개체를 만드십시오. 연결을 만든 후 보고서 태스크를 수정하고 보고서 태스크의 검색 탭 아래 보고서용 연결 개체를 설정하여 보고서를 특정 연결 관리 개체와 연결할 수 있습니다.

JDBC 연결 만들기

다음 단계에 따라 CA CA Identity Manager 내에서 연결 상세 정보를 제공하십시오.

JDBC 연결을 만들려면

1. "시스템", "JDBC 연결 관리", "JDBC 연결 만들기"를 클릭합니다.
2. 새 연결 개체를 만들거나 특정 JNDI 데이터 원본에 따라 연결 개체를 선택합니다.
3. 필요한 모든 필드를 완료하고 "제출"을 클릭합니다.

새 JDBC 연결이 만들어집니다.

논리적 특성 처리기

CA Identity Manager 논리적 특성을 사용하면 사용자 저장소 특성(물리적 특성이라고 함)을 사용자에게 친숙한 형식으로 태스크 화면에 표시할 수 있습니다. CA Identity Manager 관리자는 태스크 화면을 사용하여 CA Identity Manager 의 기능을 수행합니다. 논리적 특성은 사용자 저장소에 없으며, 일반적으로 표현을 단순화하기 위해 하나 이상의 물리적 특성을 나타냅니다. 예를 들어, 논리적 특성 날짜는 물리적 특성 월, 일 및 연도를 나타낼 수 있습니다.

논리적 특성은 논리적 특성 API 를 사용하여 작성된 Java 개체인 논리적 특성 처리기에서 처리됩니다. *Programming Guide for Java*(Java 프로그래밍 안내서)를 참조하십시오. 예를 들어, 태스크 화면이 표시되면 논리적 특성 처리기가 사용자 저장소의 물리적 특성을 태스크 화면에 표시되는 논리적 특성 데이터로 변환할 수 있습니다. CA Identity Manager 에 포함된 미리 정의된 논리적 특성 및 논리적 특성 처리기를 사용하거나 논리적 특성 API 를 사용하여 새로 만들 수 있습니다.

참고: 논리적 특성에 대한 자세한 내용은 *Programming Guide for Java*(Java 프로그래밍 안내서)를 참조하십시오.

사용자 콘솔의 "환경" 범주에는 논리적 특성 처리기를 관리하는 태스크가 포함되어 있습니다. 목록에는 CA Identity Manager 에 포함된 미리 정의된 처리기와 사이트에서 정의된 모든 사용자 지정 처리기가 들어 있습니다.

"환경" 태스크 범주에서 다음을 수행할 수 있습니다.

- CA Identity Manager 를 사용하여 새 논리적 특성 처리기 만들기
- 처리기 복사
- 처리기 삭제
- 기존 처리기 구성 수정

참고: 논리적 특성 처리기의 실행 순서를 변경하려면 관리 콘솔을 사용하십시오.

논리적 특성 처리기 만들기

논리적 특성 처리기를 만들려면

1. "시스템", "논리적 특성", "논리적 특성 처리기 만들기"로 이동합니다.
2. "논리적 특성 처리기 만들기" 화면에서 "표준 논리적 특성 처리기 만들기"를 선택하고 "확인"을 클릭합니다.

3. "논리적 특성 처리기 만들기" 화면에서 논리적 특성 처리기의 설정을 구성합니다.
각 필드에 대한 설명을 보려면 이 화면에서 도움말 링크를 클릭합니다.
4. "제출"을 클릭합니다.
"논리적 특성 처리기" 화면의 처리기 목록에 해당 처리기가 추가됩니다.

참고: 사용자 콘솔을 사용하여 논리적 특성 처리기를 구성한 후 응용 프로그램 서버를 다시 시작할 필요는 없습니다.

논리적 특성 처리기 복사

논리적 특성 처리기를 복사하려면

1. "시스템", "논리적 특성", "논리적 특성 처리기 만들기"로 이동합니다.
2. "논리적 특성 처리기 만들기" 화면에서 "논리적 특성 처리기 정의 사본 만들기"를 선택하고 "검색"을 클릭합니다.
3. 논리적 특성 처리기(예: `ConfirmPasswordHandler`)를 선택하고 "확인"을 클릭합니다.
4. "논리적 특성 처리기 만들기" 화면에서 논리적 특성 처리기의 설정을 구성합니다.
각 필드에 대한 설명을 보려면 이 화면에서 도움말 링크를 클릭합니다.
5. "제출"을 클릭합니다.
"논리적 특성 처리기" 화면의 처리기 목록에 해당 처리기가 추가됩니다.

참고: 사용자 콘솔을 사용하여 논리적 특성 처리기를 구성한 후 응용 프로그램 서버를 다시 시작할 필요는 없습니다.

ForgottenPasswordHandler 논리적 특성 처리기 만들기

ForgottenPasswordHandler 논리적 특성 처리기는 다음에 대해 별도의 논리적 특성을 사용합니다.

- 구성
- 런타임 질문 및 대답

ForgottenPasswordHandler 논리적 특성 처리기를 만들려면

1. "시스템", "논리적 특성", "논리적 특성 처리기 만들기"로 이동합니다.
2. "논리적 특성 처리기 만들기" 화면에서 "표준 논리적 특성 처리기 만들기"를 선택하고 "검색"을 클릭합니다.
3. ForgottenPasswordHandler 를 선택하고 "확인"을 클릭합니다.
4. "논리적 특성 처리기 만들기: ForgottenPasswordHandler" 화면에서 논리적 특성 처리기의 설정을 구성합니다.
각 필드에 대한 설명을 보려면 이 화면에서 도움말 링크를 클릭합니다.
5. "제출"을 클릭합니다.
"논리적 특성 처리기" 화면의 처리기 목록에 해당 처리기가 추가됩니다.

참고: 사용자 콘솔을 사용하여 논리적 특성 처리기를 구성한 후 응용 프로그램 서버를 다시 시작할 필요는 없습니다.

논리적 특성 처리기 삭제

논리적 특성 처리기를 삭제하려면

1. "시스템", "논리적 특성", "논리적 특성 처리기 만들기"로 이동합니다.
2. "논리적 특성 처리기 삭제" 화면에서 삭제할 각 논리적 특성의 왼쪽에 있는 확인란을 선택합니다.
3. "선택"을 클릭합니다.
확인 메시지가 표시됩니다.
4. "예"를 눌러 삭제를 확인합니다.

논리적 특성 처리기 수정

논리적 특성 처리기를 수정하려면

1. "시스템", "논리적 특성", "논리적 특성 처리기 만들기"로 이동합니다.
2. "논리적 특성 처리기 수정" 화면에서 수정할 처리기를 선택하고 "선택"을 클릭합니다.
3. 논리적 특성 처리기(예: ConfirmPasswordHandler)를 선택하고 "확인"을 클릭합니다.

4. "논리적 특성 처리기 수정" 화면에서 논리적 특성 처리기의 설정을 구성합니다.

각 필드에 대한 설명을 보려면 이 화면에서 도움말 링크를 클릭합니다.

5. "제출"을 클릭합니다.

참고: 사용자 콘솔을 사용하여 논리적 특성 처리기를 구성한 후 응용 프로그램 서버를 다시 시작할 필요는 없습니다.

논리적 특성 처리기 보기

논리적 특성 처리기를 보려면

1. "시스템", "논리적 특성", "논리적 특성 처리기 만들기"로 이동합니다.
2. "논리적 특성 처리기 보기" 화면에서 보려는 처리기를 선택하고 "선택"을 클릭합니다.
3. 논리적 특성 처리기의 속성을 보고 "닫기"를 클릭합니다.

선택란 데이터

다음 필드에 사용 가능한 옵션을 채울 수 있습니다.

- 확인란 다중 선택
- 드롭다운
- 드롭다운 콤보
- 다중 선택
- 옵션 선택기
- 옵션 선택기 콤보

- 라디오 단추 단일 선택
- 단일 선택

이러한 옵션은 선택란 데이터 XML 파일에 저장됩니다. 예를 들어, 선택란 데이터 XML 파일을 사용하여 "사용자 만들기" 작업의 "프로필" 탭에 있는 "시/군/구" 또는 "시/도" 드롭다운 상자의 옵션을 채울 수 있습니다.

선택란 데이터 XML 파일을 사용하여 관리자 작업의 두 필드 간에 종속성을 구성할 수도 있습니다. 예를 들어, "시/군/구" 필드에 사용 가능한 옵션은 사용자가 "시/도" 필드에서 선택한 옵션에 따라 달라질 수 있습니다.

참고: 선택란 데이터에 대한 자세한 내용은 *User Console Design Guide*(사용자 콘솔 디자인 안내서)를 참조하십시오.

상관 관계 특성 구성 태스크 화면

이 항목은 CA CloudMinder에만 적용됩니다.

"상관 관계 특성 구성" 태스크 화면에서는 환경의 상관 관계 규칙을 구성할 수 있습니다.

CA Identity Manager는 구성 매개 변수를 메모리로 읽어들이고 메모리 버전과 공통 DSA의 데이터베이스 버전을 정기적으로 동기화합니다. 상관 관계 특성이 테넌트별로 적용되므로 프로비저닝 서버는 "탐색 및 상관 관계 지정" 오퍼레이션 중에 해당 테넌트 DSA에서 상관 관계 특성을 읽습니다. 업데이트된 상관 관계 규칙은 매개 변수 업데이트 시간을 기다릴 필요 없이 즉시 적용됩니다.

이벤트에 대한 전역 정책 기반 워크플로 구성 태스크 화면

관리자는 "이벤트에 대한 전역 정책 기반 워크플로 구성" 태스크를 사용하여 현재 환경의 모든 이벤트에 대한 정책 기반 또는 정책 기반이 아닌 워크플로를 구성할 수 있습니다. 태스크를 클릭하면 워크플로 프로세스 정의에 대한 기본 이벤트 매핑이 표시됩니다. 각 이벤트 매핑을 수정 또는 삭제할 수 있으며 아직 구성되지 않은 이벤트에 대해 새 이벤트 매핑을 추가할 수 있습니다.

홈

사용자

조직

그룹

역할 및 태스크

끝점

정책

전자 메일

보고서

시스템

태스크

이벤트에 대한 전역 정책 기반 워크플로 구성

이 환경의 이벤트와 관련되어 있는 워크플로 프로세스입니다.

이벤트 이름	워크플로 프로세스
AssignAccessRoleEvent	ModifyAccessRoleMembershipApproveProcess
AssignRoleEvent	CertifyRoleApproveProcess
CreateGroupEvent	CreateGroupApproveProcess
CreateOrganizationEvent	CreateOrganizationApproveProcess
CreateUserEvent	CreateUserApproveProcess
DeleteGroupEvent	DeleteGroupApproveProcess
DeleteOrganizationEvent	DeleteOrganizationApproveProcess
DeleteUserEvent	DeleteUserApproveProcess
ModifyOrganizationEvent	ModifyOrganizationApproveProcess
RevokeAccessRoleEvent	ModifyAccessRoleMembershipApproveProcess
SelfRegisterUserEvent	SelfRegistrationApproveProcess

새 매핑 추가

이벤트

AccountChangePasswordEvent

추가

이 화면의 필드가 아래 나열되어 있습니다.

이 환경의 이벤트와 관련된 워크플로 프로세스입니다.

승인 정책과 관련된 워크플로 프로세스를 지정합니다.

새 매핑 추가

워크플로 프로세스에 매핑하기 위한 승인 정책을 지정합니다.

추가 단추

새 매핑을 추가합니다.

매핑을 추가하거나 수정하면 프로세스 매핑과 승인 정책을 선택할 수 있는 워크플로 매핑 화면이 열립니다. 동작은 이벤트 수준 워크플로 구성과 동일합니다. 워크플로 매핑 페이지에서 "추가" 단추를 클릭하면 승인 정책을 구성할 수 있는 다른 페이지가 표시됩니다.

추가 정보

[이벤트에 대한 정책 기반 워크플로를 구성하는 방법](#) (페이지 357)

[승인 정책을 구성하는 방법](#) (페이지 359)

CA Identity Manager 의 태스크 상태

CA Identity Manager 태스크가 처리를 위해 제출되면 관리자가 해당 태스크의 상태를 추적할 수 있습니다. CA Identity Manager 는 태스크 상태를 보는 다음과 같은 방법을 제공합니다.

■ 제출한 태스크 보기 탭

이 탭에서 처리를 위해 제출된 CA Identity Manager 태스크를 검색하고 표시할 수 있습니다.

관리자는 상위 수준에서 태스크 상세 정보를 보거나 추가 수준의 상세 정보를 볼 수 있습니다.

"제출한 태스크 보기" 탭은 다음 두 개의 기본 태스크에 포함되어 있습니다.

- 내가 제출한 작업 보기

관리자가 처리를 위해 제출된 태스크에 대한 정보를 검색하고 표시할 수 있게 합니다.

- 제출한 태스크 보기

다른 관리자가 처리를 위해 제출한 태스크에 대한 정보를 관리자가 검색하고 표시할 수 있게 합니다.

■ 사용자 기록 탭

이 탭은 "사용자 보기" 또는 "사용자 수정"과 같은 사용자 태스크에 추가될 수 있으며, 관리자가 선택한 사용자에 대해 다음 정보를 볼 수 있게 합니다.

- 사용자에게 수행된 태스크

- 사용자가 수행한 태스크

- 사용자에게 의한 워크플로 승인

- 보고서

CA Identity Manager 보고서를 사용하여 CA Identity Manager 환경의 현재 상태를 확인할 수 있습니다. 이 정보를 사용하여 내부 비즈니스 정책이나 외부 규제에 대한 컴플라이언스를 유지할 수 있습니다.

보고에서는 보고서 설정 및 사용에 대한 추가 정보를 제공합니다.

- 로그

CA Identity Manager 설치의 모든 구성 요소에 대한 정보를 표시하고 CA Identity Manager 의 모든 작업에 대한 상세 정보를 제공합니다.

CA Identity Manager 로그에 대한 자세한 내용은 *Configuration Guide*(구성 안내서)를 참조하십시오.

CA Identity Manager 가 태스크 상태를 확인하는 방법

태스크는 사용자가 CA Identity Manager 에서 수행할 수 있는 관리자 기능입니다. 작업에는 CA Identity Manager 에서 태스크를 완료하기 위해 수행하는 동작인 *이벤트*가 포함되어 있습니다. 한 태스크에 여러 이벤트가 포함될 수도 있습니다. 예를 들어, "사용자 만들기" 작업에는 사용자 프로필을 만들고, 사용자를 그룹에 추가하고, 역할을 할당하는 이벤트가 포함될 수 있습니다.

CA Identity Manager 에서 필요한 동작을 수행하는 방법 및 기타 사용자 지정 비즈니스 로직을 결정하는 워크플로 프로세스와 CA Identity Manager 작업 및 이벤트를 연결할 수 있습니다. 작업을 다른 작업(중첩된 작업이라고 함)과 연결할 수도 있습니다. 이 경우 CA Identity Manager 는 중첩된 작업을 원래 작업과 함께 처리합니다.

작업의 상태는 관련된 이벤트, 워크플로 프로세스, 중첩된 작업 및 사용자 지정 비즈니스 로직의 상태에 따라 달라집니다.

제출된 태스크 보기

CA Identity Manager 에는 CA Identity Manager 환경의 태스크에 대한 정보를 제공하는 "제출된 태스크 보기" 기능이 있습니다. 이 기능을 사용하여 CA Identity Manager 에서 수행하는 동작에 대한 고급 상세 정보를 검색하고 볼 수 있습니다. 세부 정보 화면은 각 태스크와 이벤트에 대한 추가 정보를 제공합니다.

태스크 상태에 따라 "제출된 태스크 보기"를 사용하여 태스크를 중단하거나 다시 제출할 수 있습니다.

"제출된 태스크 보기"를 사용하여 태스크의 처리를 처음부터 끝까지 추적할 수 있습니다. 예를 들어, CA Identity Manager 태스크에 프로비저닝 역할 할당이 포함되어 있고 해당 할당으로 인해 다른 시스템의 계정 만들기가 트리거되는 경우 "제출된 태스크 보기" 탭에 원래 작업의 모든 상세 정보와 계정 만들기의 상세 정보가 표시됩니다.

"제출된 태스크 보기"에는 시스템에서 수행한 오퍼레이션의 상세 정보가 수록되어 있습니다. 이러한 오퍼레이션은 EnableUserEvent 와 같은 CA Identity Manager 이벤트의 결과일 수 있습니다. 시스템에서 보낸 알림은 이 이벤트 아래에 그룹화됩니다. "제출된 태스크 보기"는 종료 상세 정보를 보내기 전까지 알림이 진행 중임을 나타내는 메시지를 표시합니다. 그런 다음 메시지는 "완료됨"으로 변경됩니다.

기본적으로 CA Identity Manager 는 다음 두 개의 태스크에 "제출된 태스크 보기" 탭을 포함합니다.

- 제출된 태스크 보기
- 내 제출된 태스크 보기

제출된 작업 검색

제출한 작업을 검색하려면 다음 단계를 수행합니다.

제출한 작업을 검색하려면

1. "시스템", "제출한 태스크 보기"를 차례로 클릭합니다.

"제출한 작업 보기" 페이지가 나타납니다.

2. 검색 조건을 지정하고, 표시될 행 수를 입력한 다음 "검색"을 클릭합니다.

검색 조건에 맞는 작업이 표시됩니다.

참고: 검색 조건에 특성을 지정하는 방법에 대한 자세한 내용은 [제출한 태스크 보기의 검색 특성](#) (페이지 620)을 참조하십시오.

제출한 작업 보기의 검색 특성

처리를 위해 제출된 작업을 검토하려면 "제출한 작업 보기"의 검색 기능을 사용할 수 있습니다. 다음 조건을 기반으로 작업을 검색할 수 있습니다.

시작자

작업을 시작한 사용자의 이름을 검색 조건으로 식별합니다. 사용자 이름을 기반으로 검색이 수행됩니다. 유효한 사용자 이름을 입력했는지 확인하려면 "유효성 검사" 단추를 사용합니다.

승인 태스크를 수행한 사람

작업 승인자의 이름을 검색 조건으로 식별합니다. 사용자 이름을 기반으로 검색이 수행됩니다. 유효한 사용자 이름을 입력했는지 확인하려면 "유효성 검사" 단추를 사용합니다.

참고: "다음에 의해 승인된 작업" 조건을 선택하여 작업을 필터링하는 경우 "승인 작업 표시" 조건도 기본적으로 활성화됩니다.

작업 이름

작업 이름을 검색 조건으로 식별합니다. 같음, 포함, 다음으로 시작 또는 다음으로 끝남과 같은 조건을 "작업 이름 위치" 필드 값과 함께 지정하여 검색을 구체화할 수 있습니다. 예를 들어, 같음 조건을 선택하고 텍스트 필드에 "사용자 만들기"를 입력하여 "작업 이름 같음 사용자 만들기"라는 검색 조건을 지정할 수 있습니다.

작업 상태

작업 상태를 검색 조건으로 식별합니다. "작업 상태", 같음, 조건을 선택하여 작업 상태를 선택할 수 있습니다. 다음 조건을 기반으로 검색을 구체화할 수 있습니다.

- 완료됨
- 진행 중
- 실패
- 거부됨
- 부분 완료됨
- 중단됨
- 예약됨

참고: 자세한 내용은 [작업 상태 설명](#) (페이지 622)을 참조하십시오.

작업 우선 순위

작업 우선 순위를 검색 조건으로 식별합니다. "작업 우선 순위", 같음, 조건을 선택하여 작업 우선 순위를 선택할 수 있습니다. 다음 조건을 기반으로 검색을 구체화할 수 있습니다.

낮음

낮은 우선 순위를 가진 작업을 검색할 수 있도록 지정합니다.

중간

중간 우선 순위를 가진 작업을 검색할 수 있도록 지정합니다.

높음

높은 우선 순위를 가진 작업을 검색할 수 있도록 지정합니다.

다음에서 수행됨

선택한 개체 인스턴스에서 수행된 작업을 식별합니다. 개체 인스턴스를 선택하지 않으면 해당 개체의 모든 인스턴스에서 수행된 작업이 표시됩니다.

참고: 이 필드는 "제출한 작업 구성" 화면의 "다음에서 수행됨 구성" 필드가 채워진 경우에만 나타납니다. 이 화면을 사용하여 "제출한 작업" 탭을 구성합니다. 자세한 내용은 해당 화면에 대한 온라인 도움말을 참조하십시오.

날짜 범위

제출한 작업을 검색할 날짜 범위를 식별합니다. "시작 날짜" 및 "종료 날짜"를 제공해야 합니다.

제출되지 않은 작업 표시

"감사됨" 상태의 작업을 식별합니다. 제출되지 않은 다른 작업을 시작한 작업을 식별합니다. 이 탭을 선택하면 이러한 작업이 모두 감사 및 표시됩니다.

승인 작업 표시

작업흐름의 일부로 승인되어야 하는 작업을 식별합니다.

제출된 태스크의 검색 아카이브

아카이브된 제출된 태스크를 식별합니다.

작업 상태 설명

제출한 작업은 아래에 설명된 상태 중 하나에 있습니다. 작업 상태를 기반으로 작업 취소 또는 작업 다시 제출과 같은 동작을 수행할 수 있습니다.

참고: 작업을 취소하거나 다시 제출하려면 작업 상태를 기반으로 취소 및 다시 제출 단추를 표시하도록 "제출한 작업 보기"를 구성해야 합니다. 작업 취소 및 다시 제출에 대한 자세한 내용은 [제출한 작업 보기 탭 사용자 지정 \(페이지 626\)](#)을 참조하십시오.

진행 중

다음 중 하나가 발생하는 경우에 표시됩니다.

- 작업흐름이 시작되었지만 완료되지 않았음
- 현재 작업보다 먼저 시작된 작업이 진행 중임
- 중첩된 작업이 시작되었지만 완료되지 않았음
- 주 이벤트가 시작되었지만 완료되지 않았음
- 보조 이벤트가 시작되었지만 완료되지 않았음

이 상태의 작업은 취소할 수 있습니다.

참고: 작업을 취소하면 현재 작업의 불완전한 모든 중첩된 작업과 이벤트가 취소됩니다.

취소

진행 중인 작업이나 이벤트를 취소한 경우에 표시됩니다.

거부됨

CA Identity Manager 에서 워크플로 프로세스의 일부인 이벤트나 작업을 거부한 경우에 표시됩니다. 거부된 작업은 다시 제출할 수 있습니다.

참고: 작업을 다시 제출하면 CA Identity Manager 에서 실패 또는 거부된 중첩된 작업과 이벤트를 모두 다시 제출합니다.

부분 완료됨

이벤트나 중첩된 작업 중 일부를 취소한 경우에 표시됩니다. 부분 완료된 이벤트나 중첩된 작업은 다시 제출할 수 있습니다.

완료됨

작업이 완료된 경우에 표시됩니다. 현재 작업의 중첩된 작업 및 중첩된 이벤트가 완료되면 작업이 완료됩니다.

실패

작업, 중첩된 작업 또는 현재 작업에 중첩된 이벤트가 유효하지 않은 경우에 표시됩니다. 이 상태는 작업이 실패한 경우에 표시됩니다. 실패한 작업은 다시 제출할 수 있습니다.

예약됨

작업이 이후 날짜에 실행되도록 예약된 경우에 표시됩니다. 이 상태의 작업은 취소할 수 있습니다.

감사됨

현재 작업이 감사된 경우에 표시됩니다.

태스크 상세 정보 보기

CA CA Identity Manager 가 제출된 태스크 상태, 중첩된 태스크, 태스크와 관련된 이벤트와 같은 태스크 상세 정보를 제공합니다.

제출한 태스크의 상세 정보를 보려면

1. "제출한 태스크 보기" 탭에서 선택한 태스크 옆에 있는 오른쪽 화살표 아이콘을 클릭합니다.

태스크 상세 정보가 나타납니다.

참고: 이벤트 및 중첩된 태스크(있는 경우)이 "태스크 상세 정보" 페이지에 표시됩니다. 각 태스크 및 이벤트에 대해 태스크 상세 정보를 볼 수 있습니다.

2. "닫기"를 클릭합니다.

"태스크 상세 정보" 탭이 닫히고 CA CA Identity Manager 가 태스크 목록 내에 "제출한 태스크 보기" 탭을 표시합니다.

이벤트 상세 정보 보기

CA CA Identity Manager 는 제출한 이벤트의 상태, 이벤트 특성 및 이벤트에 대한 모든 추가 정보와 같은 이벤트 상세 정보를 제공합니다.

제출한 이벤트의 상세 정보를 보려면

1. "태스크 상세 정보 보기" 페이지에서 이벤트 옆에 있는 오른쪽 화살표 아이콘을 클릭합니다.

이벤트 상세 정보가 나타납니다.

2. "닫기"를 클릭합니다.

"이벤트 상세 정보" 페이지가 닫힙니다.

이벤트 상태 설명

CA Identity Manager 의 이벤트는 아래에 설명된 상태 중 하나일 수 있습니다. 이벤트 상태를 기반으로 이벤트를 취소하거나 실행을 위해 다시 제출할 수 있습니다.

참고: 관리자가 이벤트를 취소하거나 다시 제출할 수 있게 하려면 "취소" 및 "이벤트 다시 제출" 단추를 표시하도록 "제출한 태스크 보기"를 구성해야 합니다. 태스크를 구성할 때 이벤트를 취소하고 다시 제출할 수 있는 관리자를 지정할 수 있습니다. 이벤트 취소 및 다시 제출에 대한 자세한 내용은 [제출한 태스크 보기 탭 사용자 지정](#) (페이지 626)을 참조하십시오.

진행 중

다음 중 하나가 발생하는 경우에 표시됩니다.

- 워크플로 또는 사전 이벤트가 시작되었거나 진행 중이거나 승인됨
- CA Identity Manager 가 이벤트를 실행 중임
- CA Identity Manager 가 사후 이벤트를 실행함

이 상태의 이벤트는 취소할 수 있습니다.

거부됨

CA Identity Manager 가 워크플로의 일부인 이벤트를 거부한 경우에 표시됩니다. 거부된 이벤트는 다시 제출할 수 있습니다.

취소

진행 중인 이벤트를 취소한 경우에 표시됩니다. 취소된 이벤트는 다시 제출할 수 있습니다.

완료됨

이벤트가 완료된 경우에 표시됩니다.

실패

CA Identity Manager 가 이벤트를 실행하는 동안 예외가 발생한 경우에 표시됩니다. 취소된 이벤트는 다시 제출할 수 있습니다.

참고: 주 이벤트가 완료됨 상태가 될 때까지 보조 이벤트를 다시 제출할 수 없습니다.

예약됨

이벤트가 이후 날짜에 실행되도록 예약된 경우에 표시됩니다. 이 상태의 이벤트는 취소할 수 있습니다.

감사됨

현재 이벤트가 감사된 경우에 표시됩니다.

제출한 태스크 보기 탭 사용자 지정

다음과 같이 "제출한 태스크 보기" 탭을 사용자 지정할 수 있습니다.

- 다른 태스크 이름과 태그를 지정합니다.
- 기본 표시 속성을 변경합니다. 설치할 때 사용자가 탭에 표시되는 태스크를 결정하는 조건을 입력할 수 있는 검색 화면이 표시됩니다. 현재 날짜의 제출한 태스크를 자동으로 표시하여 사용자가 검색 조건을 입력할 필요가 없도록 탭을 구성할 수 있습니다.
- 감사 이벤트를 "태스크 상세 정보" 페이지에 표시할지 여부를 결정합니다.
- 태스크 표시에 다른 열을 추가합니다.
- 태스크 및 이벤트를 취소하거나 다시 제출할 조건을 지정합니다.

참고: 특정 태스크 및 이벤트 상세 정보는 급여나 암호와 같은 "제출된 태스크 보기" 탭에 일반 텍스트로 표시되면 안 되는 데이터를 포함할 수 있습니다. `directory.xml` 파일에서 특성을 정의할 때 데이터 분류 매개 변수를 지정하여 이러한 특성을 숨길 수 있습니다. `directory.xml` 파일에 대한 자세한 내용은 *Configuration Guide*(구성 안내서)를 참조하십시오.

해당 관리자 태스크를 수정하여 "제출한 태스크 보기" 탭을 구성할 수 있습니다.

제출한 태스크 보기 탭을 구성하려면

1. "역할 및 태스크", "관리자 태스크", "관리자 태스크 수정"을 클릭합니다.
"관리자 태스크 선택" 페이지가 나타납니다.
2. 관리자 태스크 검색 "위치" 필드에서 "이름" 또는 "범주"를 선택하고 검색할 문자열을 입력한 다음 "검색"을 클릭합니다.

CA CA Identity Manager 는 검색 조건에 맞는 관리자 태스크를 표시합니다.

3. "제출한 태스크 보기"를 선택하고 "선택"을 클릭합니다.
CA CA Identity Manager는 "제출한 태스크 보기" 관리자 태스크에 대한 태스크 상세 정보를 표시합니다.
4. "탭" 탭을 클릭합니다.
"제출한 태스크 보기" 탭에 사용되는 탭이 표시됩니다.
5. 오른쪽 화살표 아이콘을 클릭하여 "제출한 태스크" 탭을 편집합니다.
탭 상세 정보가 나타납니다.
6. 필드를 편집하여 필요에 따라 "제출한 태스크 보기" 탭을 사용자 지정합니다. [제출한 태스크 탭의 구성 설정](#) (페이지 627)을 참조하십시오.

제출한 작업 보기 탭의 구성 설정

다음 필드를 사용하여 "제출한 작업 보기" 탭의 모양과 기능을 변경할 수 있습니다.

이름

작업의 이름을 정의합니다.

태그

작업의 고유한 식별자를 정의합니다. URL, 웹 서비스 또는 속성 파일에서 사용됩니다. 문자, 숫자 또는 밑줄로 구성되고 문자나 밑줄로 시작해야 합니다.

탭 숨기기

사용자가 탭을 볼 수 있지만 탭이 실행되지 않도록 지정합니다. 이 옵션을 선택하면 CA Identity Manager에서 사용자에게 오류를 표시합니다.

로드 시 작업 목록 표시

현재 날짜에 제출된 작업이 표시됩니다.

참고: 이 옵션을 선택한 경우 사용자가 "제출한 작업 보기"를 클릭하면 동일한 날짜에 제출된 작업이 직접 표시됩니다.

감사 이벤트 표시

감사된 이벤트를 "제출한 작업 보기" 페이지의 작업에 포함할지 여부를 지정합니다.

사용자 지정 열 허용

"제출한 작업 보기" 탭과 "사용자 기록" 탭에서 볼 수 있는 작업 테이블에 사용자 지정 열을 추가할 수 있도록 지정합니다. 예를 들어, "사용자 기록" 탭에 표시되는 작업 테이블에 "사용자 ID" 열을 추가할 수 있습니다.

사용자 지정 열 머리글

사용자 지정 열의 표시 이름을 나타냅니다.

사용자 지정 열 특성

작업 테이블의 사용자 지정 열을 채우는 데 사용할 특성을 나타냅니다. 예를 들어, 조직의 직원에 대해 수행된 작업을 검색하는 경우 각 직원의 조직을 표시하는 조직 열을 추가할 수 있습니다.

작업 및 이벤트 취소

작업이나 이벤트의 취소 조건을 식별합니다. 다음 옵션 중 하나를 선택하여 이 필드의 범위를 설정할 수 있습니다.

작업 생성자는 현재 사용자여야 합니다.

자신이 만든 작업 또는 이벤트를 취소하거나 다시 제출할 수 있도록 지정합니다.

작업 생성자는 범위 안에 있어야 합니다.

탭에 대한 액세스 권한을 제공한 관리자 역할의 사용자 범위 규칙과 일치하는 다른 사용자가 시작한 작업을 취소하거나 다시 제출할 수 있도록 지정합니다.

예를 들어, "직원" 조직의 모든 사용자에게 대한 범위를 포함하는 멤버십 규칙의 조건을 충족하여 "제출한 작업 보기"가 포함된 "사용자 관리자" 역할을 받았습니다. "직원" 조직의 모든 사용자가 제출한 작업을 취소하거나 다시 제출할 수 있습니다.

제한 없음

모든 사용자가 작업 또는 이벤트를 취소하거나 다시 제출할 수 있도록 지정합니다.

허용 불가

작업 또는 이벤트를 취소하거나 다시 제출할 수 없도록 지정합니다.

작업 및 이벤트 다시 제출

작업이나 이벤트의 다시 제출 조건을 식별합니다. 다음 옵션 중 하나를 선택하여 이 필드의 범위를 설정할 수 있습니다.

작업 생성자는 현재 사용자여야 합니다.

자신이 만든 작업 또는 이벤트를 취소하거나 다시 제출할 수 있도록 지정합니다.

작업 생성자는 범위 안에 있어야 합니다.

탭에 대한 액세스 권한을 제공한 관리자 역할의 사용자 범위 규칙과 일치하는 다른 사용자가 시작한 작업을 취소하거나 다시 제출할 수 있도록 지정합니다.

예를 들어, "직원" 조직의 모든 사용자에 대한 범위를 포함하는 멤버십 규칙의 조건을 충족하여 "제출한 작업 보기"가 포함된 "사용자 관리자" 역할을 받았습니다. "직원" 조직의 모든 사용자가 제출한 작업을 취소하거나 다시 제출할 수 있습니다.

제한 없음

모든 사용자가 작업 또는 이벤트를 취소하거나 다시 제출할 수 있도록 지정합니다.

허용 불가

작업 또는 이벤트를 취소하거나 다시 제출할 수 없도록 지정합니다.

사용자 기록 탭

"사용자 기록" 탭에서는 사용자와 관련된 태스크를 볼 수 있습니다. 이 탭에 표시된 태스크 정보는 "제출된 태스크 보기" 탭에서도 볼 수 있습니다.

참고: "사용자 만들기"와 같은 생성 태스크에는 이 탭을 추가할 수 없습니다.

이 탭을 사용하여 다음과 같은 태스크의 기록을 볼 수 있습니다.

- **사용자에 대해 수행된 태스크**

선택한 사용자에 대해 수행된 모든 태스크를 표시합니다.

- **사용자가 수행한 태스크**

선택한 사용자에 의해 수행된 모든 태스크를 표시합니다.

- **사용자에 의한 워크플로 승인**

워크플로의 일부로서 사용자가 승인한 모든 태스크를 표시합니다.

참고: 이 탭에서 볼 수 있는 태스크의 유형은 탭의 구성에 따라 다릅니다. 자세한 내용은 [사용자 기록 탭 사용자 지정](#) (페이지 632)을 참조하십시오.

사용자 기록 보기의 검색 특성

처리를 위해 제출된 작업을 검토하려면 "제출한 작업 보기"의 검색 기능을 사용할 수 있습니다. 다음 조건을 기반으로 작업을 검색할 수 있습니다.

작업 이름

작업 이름을 검색 조건으로 식별합니다. 같음, 포함, 다음으로 시작 또는 다음으로 끝남과 같은 조건을 "작업 이름 위치" 필드 값과 함께 지정하여 검색을 구체화할 수 있습니다. 예를 들어, 같음 조건을 선택하고 텍스트 필드에 "사용자 만들기"를 입력하여 "작업 이름 같음 사용자 만들기"라는 검색 조건을 지정할 수 있습니다.

작업 상태

작업 상태를 검색 조건으로 식별합니다. "작업 상태", 같음, 조건을 선택하여 작업 상태를 선택할 수 있습니다. 다음 조건을 기반으로 검색을 구체화할 수 있습니다.

- 완료함
- 진행 중
- 실패
- 거부됨
- 부분 완료됨
- 취소
- 예약됨

참고: 자세한 내용은 [작업 상태 설명](#) (페이지 622)을 참조하십시오.

작업 우선 순위

작업 우선 순위를 검색 조건으로 식별합니다. "작업 우선 순위", 같음, 조건을 선택하여 작업 우선 순위를 선택할 수 있습니다. 다음 조건을 기반으로 검색을 구체화할 수 있습니다.

낮음

낮은 우선 순위를 가진 작업을 검색할 수 있도록 지정합니다.

중간

중간 우선 순위를 가진 작업을 검색할 수 있도록 지정합니다.

높음

높은 우선 순위를 가진 작업을 검색할 수 있도록 지정합니다.

날짜 범위

제출한 작업을 검색할 날짜 범위를 식별합니다. "시작 날짜" 및 "종료 날짜"를 제공해야 합니다.

사용자 기록 탭 사용자 지정

관리자는 다음과 같이 "사용자 기록" 탭을 사용자 지정할 수 있습니다.

- 다른 태스크 이름과 태그를 지정합니다.
- 기본 표시 속성을 변경합니다. 기본적으로 사용자는 탭에 나타나는 태스크를 결정하는 조건을 입력할 수 있습니다. 관리자는 현재 날짜의 태스크를 자동으로 표시하여 사용자가 검색 조건을 입력할 필요가 없도록 탭을 구성할 수 있습니다.
- 감사 이벤트를 "태스크 정보" 페이지에 표시할지 여부를 결정합니다.
- 태스크 표시에 열을 추가합니다.
- 태스크 및 이벤트를 취소하거나 다시 제출하기 위한 조건을 지정합니다.

다음 단계를 수행하십시오.

1. "역할 및 태스크", "관리자 태스크", "관리자 태스크 관리"로 이동합니다.
"관리자 태스크 선택" 페이지가 나타납니다.
2. "관리자 태스크 검색"의 필드에서 "이름" 또는 "범주"를 선택하고
검색할 문자열을 입력한 다음 "검색"을 클릭합니다.
CA Identity Manager 에서 검색 조건에 맞는 관리자 태스크가
표시됩니다.
3. "사용자 기록" 탭이 포함된 태스크를 선택하고 "선택"을 클릭합니다.
CA Identity Manager 에서 관리자 태스크에 대한 태스크 정보를
표시합니다.
4. "탭" 탭을 클릭합니다.
5. "사용자 기록" 탭 옆에 있는 "편집" 아이콘을 클릭합니다.
탭 상세 정보가 나타납니다.
6. 필드를 편집하여 "사용자 기록" 탭을 사용자 지정합니다.

사용자 기록 탭의 구성 설정

다음 필드를 사용하여 "사용자 기록" 탭의 모양과 기능을 변경할 수 있습니다.

이름

작업의 이름을 정의합니다.

태그

작업의 고유한 식별자를 정의합니다. URL, 웹 서비스 또는 속성 파일에서 사용됩니다. 문자, 숫자 또는 밑줄로 구성되고 문자나 밑줄로 시작해야 합니다.

탭 숨기기

사용자가 탭을 볼 수 있지만 탭이 실행되지 않도록 지정합니다. 이 옵션을 선택하면 CA Identity Manager에서 사용자에게 오류를 표시합니다.

로드 시 작업 목록 표시

현재 날짜에 제출된 작업이 표시됩니다.

참고: 이 옵션을 선택한 경우 사용자가 "제출한 작업 보기"를 클릭하면 동일한 날짜에 제출된 작업이 직접 표시됩니다.

감사 이벤트 표시

감사된 이벤트를 "제출한 작업 보기" 페이지의 작업에 포함할지 여부를 지정합니다.

사용자 지정 열 허용

"제출한 작업 보기" 탭과 "사용자 기록" 탭에서 볼 수 있는 작업 테이블에 사용자 지정 열을 추가할 수 있도록 지정합니다. 예를 들어, "사용자 기록" 탭에 표시되는 작업 테이블에 "사용자 ID" 열을 추가할 수 있습니다.

사용자 지정 열 머리글

사용자 지정 열의 표시 이름을 나타냅니다.

사용자 지정 열 특성

작업 테이블의 사용자 지정 열을 채우는 데 사용할 특성을 나타냅니다. 예를 들어, 조직의 직원에 대해 수행된 작업을 검색하는 경우 각 직원의 조직을 표시하는 조직 열을 추가할 수 있습니다.

작업 및 이벤트 취소

작업이나 이벤트의 취소 조건을 식별합니다. 다음 옵션 중 하나를 선택하여 이 필드의 범위를 설정할 수 있습니다.

작업 생성자는 현재 사용자여야 합니다.

자신이 만든 작업 또는 이벤트를 취소하거나 다시 제출할 수 있도록 지정합니다.

작업 생성자는 범위 안에 있어야 합니다.

탭에 대한 액세스 권한을 제공한 관리자 역할의 사용자 범위 규칙과 일치하는 다른 사용자가 시작한 작업을 취소하거나 다시 제출할 수 있도록 지정합니다.

예를 들어, "직원" 조직의 모든 사용자에게 대한 범위를 포함하는 멤버십 규칙의 조건을 충족하여 "제출한 작업 보기"가 포함된 "사용자 관리자" 역할을 받았습니다. "직원" 조직의 모든 사용자가 제출한 작업을 취소하거나 다시 제출할 수 있습니다.

제한 없음

모든 사용자가 작업 또는 이벤트를 취소하거나 다시 제출할 수 있도록 지정합니다.

허용 불가

작업 또는 이벤트를 취소하거나 다시 제출할 수 없도록 지정합니다.

작업 및 이벤트 다시 제출

작업이나 이벤트의 다시 제출 조건을 식별합니다. 다음 옵션 중 하나를 선택하여 이 필드의 범위를 설정할 수 있습니다.

작업 생성자는 현재 사용자여야 합니다.

자신이 만든 작업 또는 이벤트를 취소하거나 다시 제출할 수 있도록 지정합니다.

작업 생성자는 범위 안에 있어야 합니다.

탭에 대한 액세스 권한을 제공한 관리자 역할의 사용자 범위 규칙과 일치하는 다른 사용자가 시작한 작업을 취소하거나 다시 제출할 수 있도록 지정합니다.

예를 들어, "직원" 조직의 모든 사용자에게 대한 범위를 포함하는 멤버십 규칙의 조건을 충족하여 "제출한 작업 보기"가 포함된 "사용자 관리자" 역할을 받았습니다. "직원" 조직의 모든 사용자가 제출한 작업을 취소하거나 다시 제출할 수 있습니다.

제한 없음

모든 사용자가 작업 또는 이벤트를 취소하거나 다시 제출할 수 있도록 지정합니다.

허용 불가

작업 또는 이벤트를 취소하거나 다시 제출할 수 없도록 지정합니다.

작업 표시

"사용자 기록" 탭에 표시할 작업을 결정합니다.

사용자에 대해 수행된 작업

선택한 사용자에게 대해 수행된 모든 작업이 표시됩니다.

사용자가 수행한 작업

선택한 사용자가 수행한 모든 작업이 표시됩니다.

사용자에 의한 워크플로 승인

사용자가 워크플로의 일부로 승인한 모든 작업이 표시됩니다.

사용자 활동 보기 태스크

사용자 활동은 특정 사용자와 관련된 태스크의 기록입니다. 관리자는 "사용자 활동 보기" 태스크를 사용하여 다음과 같은 사용자 정보를 추적할 수 있습니다.

- 사용자에게 수행된 태스크
- 사용자가 수행한 태스크
- 사용자에게 의한 워크플로 승인

사용자 활동을 보려면

1. "사용자", "사용자 관리", "사용자 활동 보기"로 이동합니다.
"사용자 선택" 화면이 나타납니다.
2. 사용자를 검색하고 "선택"을 클릭합니다.
"사용자 활동 보기" 화면이 나타납니다.

참고: 표시되는 사용자 활동에 대한 자세한 내용은 사용자 콘솔 온라인 도움말을 참조하십시오.

제출된 태스크 정리

각 태스크를 제출했으면 태스크 지속 데이터베이스가 증가하여 태스크 및 이벤트의 런타임 성능이 느려집니다. 저장된 질차의 가비지 컬렉션은 태스크 지속 데이터베이스의 저장소 공간 부족으로 인해 발생할 수 있는 잠재적인 성능 문제나 시스템 정지를 완화시킵니다. 태스크를 보관하는 기능을 통해 관리자는 현재 태스크와 이벤트 정보뿐만 아니라 삭제된 태스크와 이벤트도 볼 수 있습니다.

사용자 콘솔에서 **CA Identity Manager** 관리자는 되풀이 일정에 따라 자동으로 가비지 컬렉션을 수행하고 보관하도록 작업을 예약할 수 있습니다.

되풀이 탭

되풀이 탭을 사용하여 작업을 예약할 수 있습니다. 이 탭에는 다음과 같은 필드가 있습니다.

지금 실행

작업을 즉시 실행합니다.

새 작업 예약

새 작업을 예약합니다.

기존 작업 수정

기존 작업을 수정한다는 것을 지정합니다.

참고: 이 필드는 이 태스크에 대해 작업이 이미 예약된 경우에만 표시됩니다.

작업 이름

만들거나 수정할 작업의 이름을 지정합니다.

시간대

서버 시간대를 지정합니다.

참고: 사용자의 시간대가 서버의 시간대와 다른 경우 새 작업을 예약할 때 사용자의 시간대 또는 서버의 시간대를 선택할 수 있도록 드롭다운 상자가 표시됩니다. 기존 작업을 수정할 때는 시간대를 변경할 수 없습니다.

일별 일정

특정 기간(일)마다 작업이 실행되도록 지정합니다.

매(일 수)

작업 실행 간의 일 수를 정의합니다.

주별 일정

일주일 중 특정 요일 및 시간에 작업이 실행되도록 지정합니다.

요일

작업이 실행되는 요일을 지정합니다.

월별 일정

월별로 작업이 실행될 요일 또는 날짜를 지정합니다.

연간 일정

연별로 작업이 실행될 요일 또는 날짜를 지정합니다.

고급 일정

추가 예약 정보를 지정합니다.

Cron 식

이 필드 작성에 대한 내용은 다음 웹 페이지를 참조하십시오.

<http://quartz-scheduler.org/api/2.1.0/org/quartz/CronExpression.html>

실행 시간

작업이 실행되는 시간을 24 시간 형식으로 지정합니다. 예: 14:15

지금 작업 실행

즉시 작업을 실행하려면 "제출된 태스크 정리" 마법사를 사용하십시오.

다음 단계를 수행하십시오.

1. "시스템", "제출된 태스크 정리"로 이동합니다.
마법사의 되풀이 단계가 나타납니다.
2. "지금 실행"을 선택한 후 "다음"을 선택합니다.
마법사의 "제출된 태스크 정리" 단계가 나타납니다.
3. 최소 사용 기간, 아카이브, 감사 만료, 시간 제한 및 태스크 제한 정보를 입력하고 "마침"을 클릭합니다.
작업이 즉시 제출됩니다.

새 작업 예약

새 작업을 예약하려면 "제출된 태스크 정리" 마법사를 사용하십시오.

다음 단계를 수행하십시오.

1. "시스템", "제출된 태스크 정리"로 이동합니다.
"되풀이" 단계가 나타납니다.
2. "새 작업 예약"을 선택한 다음 작업 이름 및 작업의 예약 정보를 입력하고 "다음"을 클릭합니다.
"제출된 태스크 정리" 단계가 나타납니다.
3. 최소 사용 기간, 아카이브, 감사 만료, 시간 제한 및 태스크 제한 정보를 입력하고 "마침"을 클릭합니다.
새 작업이 예약됩니다.

기존 작업 수정

기존 탭을 수정하려면 "제출된 태스크 정리" 마법사를 사용하십시오.

다음 단계를 수행하십시오.

1. "시스템", "제출된 태스크 정리"로 이동합니다.
"되풀이" 단계가 나타납니다.
2. 기존 작업 수정을 선택한 다음 기존 작업을 선택하고 일정 정보를 수정한 후 "다음"을 클릭합니다.
"제출된 태스크 정리" 단계가 나타납니다.
3. 최소 사용 기간, 아카이브, 감사 만료, 시간 제한 및 태스크 제한 정보를 수정하고 "마침"을 클릭합니다.
기존 작업이 수정됩니다.

되풀이 태스크 삭제

되풀이 태스크를 삭제하려면 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. "시스템"으로 이동하여 "되풀이 태스크 삭제"를 클릭합니다.
2. 삭제할 태스크를 선택합니다.
3. "제출"을 클릭합니다.

제출된 태스크 정리 탭

이 탭을 사용하여 태스크의 최소 사용 기간, 아카이브, 감사 만료, 시간 제한 및 태스크 제한을 지정할 수 있습니다. 모든 필수 필드를 입력했으면 "마침"을 클릭하십시오. 이 탭에는 다음과 같은 필드가 있습니다.

최소 사용 기간

마지막 상태(완료함, 실패, 거부됨, 취소됨, 또는 중단됨)에 있는 태스크가 정리될 최소 사용 기간을 지정합니다. 예를 들어 1 개월을 지정하면 지난 달에 마지막 상태에 도달한 태스크는 모두 유지됩니다. 한 달 이전에 마지막 상태에 도달한 모든 태스크는 정리 및 아카이브됩니다.

이것은 필수 필드입니다.

아카이브

태스크를 런타임 데이터베이스에서 삭제하기 전에 아카이브 데이터베이스에 백업합니다.

작업이 실행되면 아카이브가 선택된 경우 데이터가 아카이브 데이터베이스로 커밋되고 런타임 태스크 지속 데이터베이스에서 제거됩니다. 데이터는 아카이브 데이터베이스에 커밋이 성공할 때까지 제거되지 않습니다.

감사 만료

감사 상태에 있는 태스크가 정리되기 전까지의 기간을 지정합니다. 감사 상태의 태스크는 이 기간이 경과하기 전에는 마지막 상태에 있는 것으로 간주되지 않습니다. 감사 상태에 있는 태스크는 아직 제출되지 않았습니니다.

시간 제한

특정 시간에 만 정리하도록 제한합니다.

태스크 제한

특정 개수의 태스크만 정리하도록 제한합니다.

되풀이 태스크 삭제

태스크를 되풀이 일정에 따라 실행할 필요가 없을 때 CA CA Identity Manager 관리자는 태스크를 삭제할 수 있습니다. 태스크를 삭제했으면 해당 태스크에 대해 가비지 컬렉션 및 아카이브가 수행되지 않습니다.

"제출된 태스크 정리:되풀이" 마법사를 사용하여 예약된 모든 태스크가 이 페이지에 나열되고 CA CA Identity Manager 관리자는 삭제할 태스크를 선택할 수 있습니다.

참고: 태스크는 여전히 데이터베이스에 있지만 예약 되풀이만 삭제됩니다.

엔터프라이즈 로그 매니저 연결 구성

이 화면에서는 새로 추가된 CA UAR(CA 사용자 활동 보고) 연결 태스크를 관리할 수 있습니다.

참고: CA 엔터프라이즈 로그 매니저의 이름이 변경되었습니다. 이제 CA UAR 라고 합니다.

이 화면의 필드가 아래에 나열되어 있습니다.

연결 이름

단일 CA UAR 연결 관리 개체에 사용되는 고유 이름을 지정합니다.

이 필드는 읽기 전용입니다.

설명

CA UAR 연결을 설명합니다.

호스트 이름

CA UAR 서버 호스트 이름 또는 IP 주소를 지정합니다.

이것은 필수 필드입니다.

포트 번호

CA UAR 서버 연결 포트를 지정합니다.

기본값: 52520

이것은 필수 필드입니다.

인증 기관이 서명한 SSL 인증서

이 확인란을 선택하면 CA UAR 서버에 연결할 때 엄격한 SSL 인증서 검사를 지정합니다.

기본적으로 CA UAR 와 함께 설치된 인증서와 같은 자체 서명된 SSL 인증서가 있는 경우 루트 인증 기관의 트러스트된 경로가 존재하지 않으므로 이 확인란을 선택하면 안 됩니다.

인증서 이름

인증에 사용할 CA UAR 인증서의 이름을 지정합니다.

이것은 필수 필드입니다.

인증서 암호

CA UAR 암호를 지정합니다.

이것은 필수 필드입니다.

특성

지원 안 됨. 연결 정보를 테스트로 저장할 때 버전이 검색됩니다.

엔터프라이즈 로그 매니저 연결 삭제

목록에서 연결을 선택한 후 "삭제"를 클릭합니다. CA UAR 연결이 삭제됩니다.

비밀 키 관리

비밀 키를 사용하여 데이터를 암호화하거나 암호 해독하는 동적 키를 관리할 수 있습니다. 사용자가 키에 대한 무단 액세스를 얻었다고 의심되는 경우 키 저장소의 암호를 변경할 수 있습니다. 키 저장소는 암호 키를 저장하는 데이터베이스입니다. 이 암호를 변경하면 CA Identity Manager 가 키 값을 다시 암호화합니다.

각 환경마다 동적 키 집합과 키 저장소 암호가 있습니다. 여러 환경이 사용자 디렉토리를 공유하는 경우 각 환경에 대해 동일한 동적 키와 키 저장소 암호를 사용하십시오.

키 저장소 암호는 암호화 코드에 포함된 키나 CA Identity Manager 서버 설치 중에 입력된 매개 변수를 사용하여 암호화됩니다. 클러스터에서는 모든 노드가 동적 키에 대한 값과 키 저장소 암호를 공유합니다.

암호화 오퍼레이션은 해당 알고리즘과 환경에 대한 최신 동적 키를 사용합니다. 암호 해독 오퍼레이션은 암호화된 데이터에 키 ID 가 있는지 확인하여 올바른 키가 사용되도록 합니다. 추가 정보는 *Configuration Guide*(구성 안내서)의 Encrypted Text Formats(암호화된 텍스트 형식) 섹션에 나와 있습니다.

다음 단계를 수행하십시오.

1. 키 저장소의 암호를 입력하거나 수정합니다.
2. 다른 키가 필요한 경우 "키 추가"를 클릭합니다.
3. 알고리즘을 선택합니다.
4. 키의 암호를 입력합니다.

PBE 및 RC2 의 경우 최대 키 길이는 128 바이트입니다.

AES 의 경우 올바른 키 크기는 16 바이트, 24 바이트 및 32 바이트입니다.

5. "제출"을 클릭합니다.
6. 키 저장소 암호를 수정한 경우 "제출"을 클릭합니다.

CA Identity Manager 가 키 값을 다시 암호화합니다.

제 21 장: 태스크 지속

이 섹션은 다음 항목을 포함하고 있습니다.

[자동화된 태스크 지속 가비지 수집 및 아카이브](#) (페이지 645)

[되풀이 탭](#) (페이지 646)

[제출된 태스크 정리 탭](#) (페이지 648)

[지금 작업 실행](#) (페이지 649)

[새 작업 예약](#) (페이지 649)

[기존 작업 수정](#) (페이지 650)

[되풀이 태스크 삭제](#) (페이지 650)

[태스크 지속 데이터베이스를 마이그레이션하는 방법](#) (페이지 651)

자동화된 태스크 지속 가비지 수집 및 아카이브

이 릴리스에서 관리자는 태스크 지속 데이터베이스에서 태스크 및 이벤트 정보를 정리 및 아카이브하기 위해 "제출된 태스크 정리" 태스크를 사용하여 특정 매개 변수로 작업을 수정 및 예약할 수 있으며, 필요할 때 이러한 되풀이 태스크를 삭제할 수도 있습니다.

"시스템" 탭에서 "제출된 태스크 정리"를 선택하여 마법사를 실행할 수 있습니다. 이 마법사는 작업을 설정 및 예약하고 데이터의 아카이브 여부를 지정하는 과정을 안내합니다. 또한 "시스템" 탭에서 "되풀이 태스크 삭제"를 선택하여 필요할 때 되풀이 작업을 삭제하도록 선택할 수도 있습니다.

태스크 데이터를 정리 및 아카이브하는 태스크를 예약하면 잠재적인 성능 문제 또는 시스템 중단 가능성을 크게 줄일 수 있습니다. 아카이브 기능을 사용하여 런타임 데이터베이스에서 태스크를 삭제하기 전에 아카이브 데이터베이스에 태스크를 백업할 수 있습니다. 돌아가서 이러한 삭제된 태스크를 보려면 "제출한 태스크 보기"에 있는 아카이브 검색 확인란을 선택하여 삭제 및 아카이브된 모든 태스크의 목록을 검색하여 볼 수 있습니다.

되풀이 탭

되풀이 탭을 사용하여 작업을 예약할 수 있습니다. 이 탭에는 다음과 같은 필드가 있습니다.

지금 실행

작업을 즉시 실행합니다.

새 작업 예약

새 작업을 예약합니다.

기존 작업 수정

기존 작업을 수정한다는 것을 지정합니다.

참고: 기존 작업 수정 필드는 이 태스크에 대해 작업이 이미 예약된 경우에만 표시됩니다.

작업 이름

만들거나 수정할 작업의 이름을 지정합니다.

시간대

서버 시간대를 지정합니다.

참고: 사용자의 시간대가 서버의 시간대와 다른 경우 새 작업을 예약할 때 사용자의 시간대 또는 서버의 시간대를 선택할 수 있도록 드롭다운 상자가 표시됩니다. 기존 작업을 수정할 때는 시간대를 변경할 수 없습니다.

주별 일정

일주일 중 특정 요일 및 시간에 작업이 실행되도록 지정합니다.

고급 일정

추가 예약 정보를 지정합니다.

요일

작업이 실행되는 요일을 지정합니다.

실행 시간

작업이 실행되는 시간을 24 시간 형식으로 지정합니다. 예: 14:15

Cron 식

이 필드 작성에 대한 내용은 다음 웹 페이지를 참조하십시오.

<http://www.opensymphony.com/quartz/api/org/quartz/CronExpression.html>

참고: 이 필드는 "고급 일정"을 선택한 경우에 표시됩니다.

추가 정보

[되풀이 태스크 삭제](#) (페이지 639)

[새 작업 예약](#) (페이지 639)

[기존 작업 수정](#) (페이지 639)

[지금 작업 실행](#) (페이지 638)

제출된 태스크 정리 탭

이 탭을 사용하여 태스크의 최소 사용 기간, 아카이브, 감사 만료, 시간 제한 및 태스크 제한을 지정할 수 있습니다. 모든 필수 필드를 입력했으면 "마침"을 클릭하십시오. 이 탭에는 다음과 같은 필드가 있습니다.

최소 사용 기간

마지막 상태(완료함, 실패, 거부됨, 취소됨, 또는 중단됨)에 있는 태스크가 정리될 최소 사용 기간을 지정합니다. 예를 들어 1 개월을 지정하면 지난 달에 마지막 상태에 도달한 태스크는 모두 유지됩니다. 한 달 이전에 마지막 상태에 도달한 모든 태스크는 정리 및 아카이브됩니다.

이것은 필수 필드입니다.

아카이브

태스크를 런타임 데이터베이스에서 삭제하기 전에 아카이브 데이터베이스에 백업합니다.

작업이 실행되면 아카이브가 선택된 경우 데이터가 아카이브 데이터베이스로 커밋되고 런타임 태스크 지속 데이터베이스에서 제거됩니다. 데이터는 아카이브 데이터베이스에 커밋이 성공할 때까지 제거되지 않습니다.

감사 만료

감사 상태에 있는 태스크가 정리되기 전까지의 기간을 지정합니다. 감사 상태의 태스크는 이 기간이 경과하기 전에는 마지막 상태에 있는 것으로 간주되지 않습니다. 감사 상태에 있는 태스크는 아직 제출되지 않았습니다.

시간 제한

특정 시간에 만 정리하도록 제한합니다.

태스크 제한

특정 개수의 태스크만 정리하도록 제한합니다.

지금 작업 실행

즉시 작업을 실행하려면 "제출된 태스크 정리" 마법사를 사용하십시오.

다음 단계를 수행하십시오.

1. "시스템", "제출된 태스크 정리"로 이동합니다.
마법사의 되풀이 단계가 나타납니다.
2. "지금 실행"을 선택한 후 "다음"을 선택합니다.
마법사의 "제출된 태스크 정리" 단계가 나타납니다.
3. 최소 사용 기간, 아카이브, 감사 만료, 시간 제한 및 태스크 제한 정보를 입력하고 "마침"을 클릭합니다.
작업이 즉시 제출됩니다.

새 작업 예약

새 작업을 예약하려면 "제출된 태스크 정리" 마법사를 사용하십시오.

다음 단계를 수행하십시오.

1. "시스템", "제출된 태스크 정리"로 이동합니다.
"되풀이" 단계가 나타납니다.
2. "새 작업 예약"을 선택한 다음 작업 이름 및 작업의 예약 정보를 입력하고 "다음"을 클릭합니다.
"제출된 태스크 정리" 단계가 나타납니다.
3. 최소 사용 기간, 아카이브, 감사 만료, 시간 제한 및 태스크 제한 정보를 입력하고 "마침"을 클릭합니다.
새 작업이 예약됩니다.

기존 작업 수정

기존 탭을 수정하려면 "제출된 태스크 정리" 마법사를 사용하십시오.

다음 단계를 수행하십시오.

1. "시스템", "제출된 태스크 정리"로 이동합니다.
"되풀이" 단계가 나타납니다.
2. 기존 작업 수정을 선택한 다음 기존 작업을 선택하고 일정 정보를 수정한 후 "다음"을 클릭합니다.
"제출된 태스크 정리" 단계가 나타납니다.
3. 최소 사용 기간, 아카이브, 감사 만료, 시간 제한 및 태스크 제한 정보를 수정하고 "마침"을 클릭합니다.
기존 작업이 수정됩니다.

되풀이 태스크 삭제

되풀이 태스크를 삭제하려면 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. "시스템"으로 이동하여 "되풀이 태스크 삭제"를 클릭합니다.
2. 삭제할 태스크를 선택합니다.
3. "제출"을 클릭합니다.

태스크 지속 데이터베이스를 마이그레이션하는 방법

이전 릴리스에서 마이그레이션은 간단히 수행되었고 관리 콘솔을 사용했습니다. 많은 수의 태스크를 마이그레이션하는 경우 성능 병목 현상을 줄이기 위해 명령줄 마이그레이션 도구가 제공되었습니다. 또한 특정 환경, 태스크의 상태, 생성된 태스크로 마이그레이션을 세부 조율하고 특정 날짜 범위 내에서 실행할 수도 있습니다. 명령줄 도구인 `runmigration` 은 다음 폴더에 있습니다.

`admin_tools/tools/tpmigration`

태스크 지속 데이터베이스를 마이그레이션하려면 다음을 수행해야 합니다.

1. `tpmigration125.properties` 파일을 업데이트합니다.
2. `JAVA_HOME` 변수를 설정합니다.
3. `runmigration` 도구를 실행합니다.

tpmigration125.properties 파일 업데이트

태스크 지속 데이터베이스 마이그레이션을 설정하려면 tpmigration.properties 파일을 개체 저장소 및 태스크 지속 정보(저장소 값 포함)로 업데이트해야 합니다. tpmigration125.properties 파일은 다음 위치에 있습니다.

<IAM suite folder>/tools/tpmigration/com/ca/tp/migratetp125

마이그레이션을 설정하려면 속성 파일에서 다음 정보를 완성하십시오.

```
#####
# The object store is required to obtain the environment details.
#####
os.db.hostname=<hostname>
os.db.dbname=<database-name or SID>
os.db.username=<db user name>
os.db.password=<db user's password>
os.db.port=<db port number>
os.db.dbType=<type of the database. For ex. for SQL server sql2005 and for oracle
'oracle'>

#####
# Task persistence data where the old and new tables are.
#####
tp.db.hostname=<hostname>
tp.db.dbname=<database-name or SID>
tp.db.username=<db user name>
tp.db.password=<db user's password>
tp.db.port=<db port number>
tp.db.dbType=<type of the database. For ex. for SQL server sql2005 and for oracle
'oracle'>
```

JAVA_HOME 변수 설정

runmigration 도구가 올바르게 실행되도록 하려면 환경 변수 JAVA_HOME 이 설정되어 있어야 합니다.

runmigration 도구 실행

마이그레이션을 시작하려면 다음 절차를 따르십시오.

명령줄에서

1. runmigration 도구를 실행합니다.

Windows:

runmigration.bat

UNIX:

runmigration.sh

2. 다음 정보를 입력합니다.

- "Environment protected Alias"(환경 보호되는 별칭). 모든 환경의 경우 'all'을 입력하십시오.

참고: all 을 지정하지 않으면 단 하나의 환경만 입력할 수 있습니다.

- 태스크 상태

참고: all 을 지정하지 않으면 단 하나의 태스크 상태만 입력할 수 있습니다.

- (1-8.x, 2-12.0)에서 마이그레이션할 CA CA Identity Manager 버전

- "Do you want to specify a date range for the tasks to be migrated"(마이그레이션할 태스크의 날짜 범위를 지정할지 여부) (y/n)

참고: 'y'를 선택하는 경우 다음을 입력해야 합니다.

- "Enter the Start Date"(시작 날짜 입력) (mm/dd/yy)
- "Enter the End Date"(종료 날짜 입력) (mm/dd/yy)

마이그레이션이 시작됩니다.

마이그레이션이 완료된 후 마이그레이션된 태스크 수가 상태에 표시됩니다.