



Sun Java™ System
Access Manager 6
관리 설명서

2005Q1

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

부품 번호 : 819-1939

Copyright © 2005 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. 모든 권리는 저작권자의 소유입니다 . Sun Microsystems, Inc. 는 이 문서에 설명된 제품의 기술 관련 지적 재산을 소유합니다 . 특히 이 지적 재산권에는 <http://www.sun.com/patents> 에 나열된 하나 이상의 미국 특허권이 포함될 수 있으며 , 미국 및 다른 국가에서 하나 이상의 추가 특허권 또는 출원 중인 특허권이 제한 없이 포함될 수 있습니다 .

이 제품에는 SUN MICROSYSTEMS, INC. 의 기밀 정보 및 무역 비밀이 포함되어 있습니다 . SUN MICROSYSTEMS, INC. 의 명시된 사전 서면 승인 없이는 해당 기밀의 사용 , 공개 또는 복제가 금지됩니다 .

미국 정부의 권리 - 상용 소프트웨어 . 정부 사용자는 Sun Microsystems, Inc. 표준 사용권 계약과 해당 FAR 규정 및 모충 규정을 준수해야 합니다 . 이 배포에는 타사에서 개발한 자료가 포함되어 있을 수 있습니다 .

제품 중에는 캘리포니아 대학에서 허가한 Berkeley BSD 시스템에서 파생된 부분이 포함되어 있을 수 있습니다 . UNIX 는 미국 및 다른 국가에서 X/Open Company, Ltd. 를 통해 독점적으로 사용권이 부여되는 등록 상표입니다 .

Sun, Sun Microsystems, Sun 로고 , Java, Solaris, JDK, Java Naming & Directory Interface, JavaMail, JavaHelp, J2SE, iPlanet, Duke 로고 , Java Coffee Cup 로고 , Solaris 로고 , SunTone Certified 로고 및 Sun ONE 로고는 미국 및 다른 국가에서 Sun Microsystems, Inc. 의 상표 또는 등록 상표입니다 .

모든 SPARC 상표는 사용 허가를 받았으며 미국 및 다른 국가에서 SPARC International, Inc. 의 상표 또는 등록 상표입니다 . SPARC 상표를 사용하는 제품은 Sun Microsystems, Inc. 가 개발한 구조를 기반으로 하고 있습니다 .

Legato 및 Legato 로고는 Legato Systems, Inc. 의 등록 상표이고 Legato NetWorker 는 Legato Systems, Inc. 의 상표 또는 등록 상표입니다 . Netscape Communications Corp 로고는 Netscape Communications Corporation 의 상표 또는 등록 상표입니다 .

OPEN LOOK 및 Sun(TM) 그래픽 사용자 인터페이스 (GUI) 는 Sun Microsystems, Inc. 가 자사의 사용자 및 정식 사용자용으로 개발했습니다 . Sun 은 컴퓨터 업계를 위한 시각적 또는 그래픽 사용자 인터페이스 (GUI) 의 개념을 연구 개발한 Xerox 사의 선구적인 노력을 높이 평가하고 있습니다 . Sun 은 Xerox 와 Xerox 그래픽 사용자 인터페이스 (GUI) 에 대한 비독점적 사용권을 보유하고 있습니다 . 이 사용권은 OPEN LOOK GUI 를 구현하는 Sun 의 정식 사용자에게도 적용되며 그렇지 않은 경우에는 Sun 의 서면 사용권 계약을 준수해야 합니다 .

이 서비스 설명서에서 다루는 제품과 수록된 정보는 미국 수출 관리법에 의해 규제되며 다른 국가의 수출 또는 수입 관리법의 적용을 받을 수도 있습니다 . 이 제품과 정보를 직간접적으로 핵무기 , 미사일 또는 생화학 무기에 사용하거나 핵과 관련하여 해상에서 사용하는 것은 엄격하게 금지됩니다 . 미국 수출 금지 국가 또는 금지된 개인과 특별히 지정된 국민 목록을 포함하여 미국 수출 금지 목록에 지정된 대상으로의 수출이나 재수출은 엄격하게 금지됩니다 .

설명서는 " 있는 그대로 " 제공되며 , 법률을 위반하지 않는 범위 내에서 상품성 , 특정 목적에 대한 적합성 또는 비침해에 대한 묵시적인 보증을 포함하여 모든 명시적 또는 묵시적 조건 , 표현 및 보증을 배제합니다 .

목 록

대상	21
이 설명서를 읽기 전에	22
이 설명서에 사용된 규약	22
활자체 규약	22
기호	23
기본 경로 및 파일 이름	24
셸 프롬프트	24
관련 설명서	25
이 설명서 세트의 문서	25
Access Manager 정책 에이전트 설명서	26
기타 서버 설명서	26
Sun 자원 온라인 액세스	27
Sun 기술 지원 문의	27
관련된 타사 웹 사이트 참조	27
사용자 의견 환영	28
1 부 Access Manager 구성	29
1 장 Access Manager 2005Q1 구성 스크립트	31
Access Manager 2005Q1 설치 개요	32
Access Manager amconfig 스크립트 작업	33
Access Manager 샘플 구성 스크립트 입력 파일	35
배포 모드 변수	35
Access Manager 구성 변수	36
웹 컨테이너 구성 변수	38

Sun Java System Web Server 6.1 SP4	39
Sun Java System Application Server 7.0 Update 3	40
Sun Java System Application Server 8.1	41
BEA WebLogic Server 6.1 SP4 및 SP5	42
BEA WebLogic Server 8.1	43
IBM WebSphere 5.1	44
Directory Server 구성 변수	45
Access Manager amconfig 스크립트	46
Access Manager 배포 시나리오	47
추가 Access Manager 인스턴스 배포	47
추가 Access Manager 인스턴스를 배포하려면	47
Access Manager 인스턴스 재구성	49
Access Manager 인스턴스 제거	50
모든 Access Manager 인스턴스 제거	51
2 장 SSL 모드에서 Access Manager 구성	53
보안 Sun Java System Web Server 를 사용하여 Access Manager 구성	54
보안 Sun Java System Application Server 를 사용하여 Access Manager 구성	57
SSL 을 사용하여 Application Server 6.2 설정	57
SSL 을 사용하여 Application Server 8.1 설정	60
SSL 모드에서 Access Manager 구성	62
보안 BEA WebLogic Server 로 AMSDK 구성	62
보안 IBM WebSphere Application Server 로 AMSDK 구성	65
SSL 모드에서 Access Manager 를 Directory Server 로 구성	66
SSL 모드에서 Directory Server 구성	66
Access Manager 를 SSL 사용 Directory Server 로 연결	67

2 부 콘솔을 통한 Access Manager 관리 **69**

3 장 Identity 관리	71
Access Manager 콘솔	71
헤더 창	71
탐색 표시 영역	72
데이터 표시 영역	72
Identity 관리 보기	73
사용자 프로필 보기	73
등록 정보 기능	73
Identity 관리 인터페이스	74
Access Manager 객체 관리	74
조직	74
정책에 조직 추가	76

그룹	76
정책 그룹에서 구성원 추가 또는 제거	78
필터링된 그룹 만들기	79
정책에 그룹 추가	80
사용자	80
정책에 사용자 추가	82
서비스	83
역할	84
정책에 역할 추가	91
역할에 대한 서비스 사용자 정의	92
정책에 역할 추가	93
정책	93
에이전트	94
에이전트 만들기	94
컨테이너	95
사용자 컨테이너	96
그룹 컨테이너	97
디스플레이 옵션	97
표시 옵션 변경	97
사용 가능한 작업	98
사용자에 대한 사용 가능한 작업 설정	98
4 장 현재 세션	101
현재 세션 인터페이스	101
세션 관리 프레임	101
세션 정보 창	101
세션 종료	103
5 장 정책 관리	105
개요	106
정책 관리 기능	106
URL 정책 에이전트 서비스	106
정책 에이전트	107
정책 에이전트 프로세스	108
정책 유형	109
일반 정책	109
규칙	109
주제	109
참조 정책	111
규칙	111
참조	112
정책 정의 유형 문서	112

Policy 요소	113
Rule 요소	113
ServiceName 요소	113
ResourceName 요소	114
AttributeValuePair 요소	114
Attribute 요소	114
Value 요소	114
Subjects 요소	115
Subject 요소	115
Referrals 요소	115
Referral 요소	115
Conditions 요소	116
Condition 요소	116
정책 서비스 추가	116
새 정책 서비스 추가	116
정책 만들기	117
amadmin 으로 정책 만들기	117
Access Manager 콘솔을 사용하여 정책 생성	118
피어 및 하위 조직에 대한 정책 만들기	119
하위 조직에 대한 정책을 만들려면	119
정책 관리	120
일반 정책 수정	120
참조 정책 수정	126
정책 구성 서비스	127
주제 평가 캐싱	127
amldapuser 정의	128
정책 구성 서비스 추가	128
정책 구성 서비스를 추가하려면	128
정책 기반 자원 관리	129
제한 사항	129
6 장 인증 관리	131
사용자 인터페이스 로그인 URL	132
로그인 URL 매개 변수	132
goto 매개 변수	133
gotoOnFail 매개 변수	133
org 매개 변수	134
user 매개 변수	134
role 매개 변수	134
locale 매개 변수	135
module 매개 변수	136
service 매개 변수	136
arg 매개 변수	136

authlevel 매개 변수	137
domain 매개 변수	137
iPSPCookie 매개 변수	137
IDTokenN 매개 변수	138
인증 유형	138
인증 유형에 따른 액세스 결정 방법	139
URL 리디렉션	140
조직 기반 인증	141
조직 기반 인증 로그인 URL	141
조직 기반 인증 리디렉션 URL	141
조직 기반 인증 구성	143
역할 기반 인증	143
역할 기반 인증 로그인 URL	144
역할 기반 인증 리디렉션 URL	145
역할 기본 인증 구성	146
서비스 기반 인증	147
서비스 기반 인증 로그인 URL	147
서비스 기반 인증 리디렉션 URL	148
서비스 기반 인증을 구성하려면	149
사용자 기반 인증	150
사용자 기반 인증 로그인 URL	150
사용자 기반 인증 리디렉션 URL	150
사용자 기반 인증을 구성하려면	152
인증 수준 기반 인증	152
인증 수준 기반 인증 로그인 URL	153
인증 수준 기반 인증 리디렉션 URL	153
모듈 기반 인증	155
모듈 기반 인증 로그인 URL	155
모듈 기반 인증 리디렉션 URL	156
인증 구성	157
인증 구성 사용자 인터페이스	157
인증 모듈 체이닝	160
조직에 대한 인증 구성	161
역할에 대한 인증 구성	161
서비스에 대한 인증 구성	162
사용자에 대한 인증 구성	163
계정 잠금	163
물리적 잠금	164
메모리 잠금	165
인증 서비스 파일오버	165
정규화된 도메인 이름 (FQDN) 매핑	166
FQDN 매핑의 용도	167
영구 쿠키	167

다중 LDAP 인증 모듈 구성	168
세션 업그레이드	171
플러그인 인터페이스 검증	171
JAAS 공유 상태	172
JAAS 공유 상태 활성화	172
JAAS 공유 상태 저장소 옵션	173
7장 인증 옵션	175
핵심 인증	176
핵심 모듈 추가 및 활성화	176
활성 디렉토리 인증	177
활성 디렉토리 인증 추가 및 활성화	177
활성 디렉토리 인증을 사용하여 로그인	178
익명 인증	178
익명 인증 추가 및 활성화	178
익명 인증을 사용하여 로그인	179
인증서 기반 인증	180
인증서 기반 인증 추가 및 활성화	180
인증서 기반 인증의 플랫폼 서버 목록에 서버 URL 추가	181
인증서 기반 인증을 사용하여 로그인	181
HTTP 기본 인증	182
HTTP 기본 인증 추가 및 활성화	182
HTTP 기본 인증을 사용하여 로그인	183
 JDBC 인증	183
JDBC 인증 추가 및 활성화	183
JDBC 인증을 사용하여 로그인	184
LDAP 디렉토리 인증	185
LDAP 인증 추가 및 활성화	185
LDAP 인증을 사용하여 로그인	186
LDAP 인증 파일오버 사용	186
다중 LDAP 구성	186
구성원 인증	187
구성원 인증 추가 및 활성화	187
구성원 인증을 사용하여 로그인	188
MSISDN 인증	188
MSISDN 인증 추가 및 활성화	188
MSISDN 인증을 사용하여 로그인	189
Windows NT 인증	190
Samba 클라이언트 설치	190
Windows NT 인증 추가 및 활성화	191
Windows NT 인증을 사용하여 로그인	191
RADIUS 서버 인증	192
RADIUS 인증 추가 및 활성화	192

RADIUS 인증을 사용하여 로그인	193
SafeWord 인증	194
SafeWord 인증 추가 및 활성화	194
SafeWord 인증을 사용하여 로그인	195
Sun ONE Application Server 에서 SafeWord 구성	195
SAML 인증	197
SAML 인증 추가 및 활성화	197
SAML 인증을 사용하여 로그인	198
SecurID 인증	198
SecurID 인증 추가 및 활성화	199
SecurID 인증을 사용하여 로그인	199
Unix 인증	200
Unix 인증 추가 및 활성화	201
Unix 인증을 사용하여 로그인	202
Windows 데스크탑 SSO 인증	202
Internet Explorer 의 알려진 제한 사항	203
Windows 데스크탑 SSO 인증 추가 및 활성화	203
Windows 2000 도메인 제어기에서 사용자를 생성하려면	203
Internet Explorer 를 설정하려면	204
Internet Explorer 의 알려진 제한 사항	205
Windows 데스크탑 SSO 인증을 추가하고 구성하려면	205
Windows 데스크탑 SSO 인증을 사용하여 로그인	206
8 장 비밀번호 재설정 서비스	207
비밀번호 재설정 서비스 등록	207
다른 조직의 사용자에게 대해 비밀번호 재설정을 등록하려면	207
비밀번호 재설정 서비스 구성	208
서비스를 구성하려면	208
비밀번호 재설정 잠금	209
메모리 잠금	209
물리적 잠금	209
최종 사용자에게 대한 비밀번호 재설정	210
비밀번호 재설정 사용자 정의	210
잊어버린 비밀번호 재설정	211
비밀번호 정책	212

3 부 명령줄 참조 설명서 **213**

9 장 amadmin 명령줄 도구	215
amadmin 명령줄 실행 파일	215
amadmin 구문	216

amadmin 옵션	216
연합 관리를 위해 amadmin 사용	219
Directory Server 에 Liberty 메타 호환 XML 로드	219
XML 파일에 엔티티 내보내기 (XML 디지털 서명 사용 안 함)	220
--entityname (--e)	220
--export (-o)	220
XML 파일에 엔티티 내보내기 (XML 디지털 서명 사용)	221
--entityname (--e)	221
--exportwithsig (-o)	221
자원 번들에 대해 amadmin 사용	221
자원 번들 추가	221
자원 문자열 가져오기	222
자원 번들 제거	222
10 장 amserver 명령줄 도구	223
amserver 명령줄 실행 파일	223
amserver 구문	223
11 장 am2bak 명령줄 도구	225
am2bak 명령줄 실행 파일	225
am2bak S 구문	225
am2bak 옵션	226
백업 절차	227
12 장 bak2am 명령줄 도구	229
bak2am 명령줄 실행 파일	229
bak2am 구문	229
bak2am 옵션	230
13 장 ampassword 명령줄 도구	231
ampassword 명령줄 실행 파일	231
ampassword 구문	231
ampassword 옵션	232
SSL 에서 ampassword 실행	232
14 장 VerifyArchive 명령줄 도구	235
VerifyArchive 명령줄 실행 파일	235
VerifyArchive 구문	236
VerifyArchive 옵션	236

15 장 amsecuridd 도우미	237
amsecuridd 도우미 명령줄 실행 파일	237
amsecuridd 구문	238
amsecuridd 옵션	238
amsecuridd 도우미 실행	238
필수 라이브러리	239

4 부 속성 참조 설명서 241

16 장 관리 서비스 속성	243
전역 속성	243
연합 관리 사용	244
사용자 관리 사용	244
사용자 컨테이너 표시	244
보기 메뉴에 컨테이너 표시	245
그룹 컨테이너 표시	245
관리 대상 그룹 유형	245
기본 역할 권한	246
사용 권한 없음	246
조직 관리	246
조직 지원 안내 관리	246
조직 정책 관리자	246
도메인 구성 요소 트리 사용 가능	247
관리 그룹 사용 가능	248
호환 사용자 삭제 사용 가능	248
동적 관리 역할 ACI	248
컨테이너 지원 안내 관리	249
조직 지원 안내 관리	249
컨테이너 관리	249
조직 정책 관리자	249
사용자 컨테이너 관리	249
그룹 관리	250
최상위 수준 관리자	250
조직 관리	250
사용자 프로필 서비스 클래스	250
DC 노드 속성 목록	251
삭제된 객체에 대한 필터 검색	251
기본 사용자 컨테이너	251
기본 그룹 컨테이너	252
기본 에이전트 컨테이너	252
조직 속성	252

그룹 기본 사용자 컨테이너	253
그룹 사용자 컨테이너 목록	253
사용자 프로필 디스플레이 클래스	253
최종 사용자 프로필 디스플레이 클래스	254
사용자 프로필 페이지에 역할 표시	254
사용자 프로필 페이지에 그룹 표시	254
사용자 그룹 자동 가입 사용 가능	254
사용자 프로필 디스플레이 옵션	254
사용자 작성 기본 역할	255
관리 콘솔 탭	255
검색에서 반환되는 최대 결과 수	255
검색 시간 초과	255
JSP 디렉토리 이름	256
온라인 도움말 문서	256
필수 서비스	256
사용자 검색 키	256
사용자 검색 반환 속성	257
사용자 작성 알림 목록	257
사용자 삭제 알림 목록	258
사용자 수정 알림 목록	258
페이지당 표시되는 최대 항목	259
Event Listener 클래스	259
사전 처리 및 사후 처리 클래스	259
외부 속성 불러오기 사용 가능	260
잘못된 사용자 아이디 문자	260
사용자 아이디 및 비밀번호 검증 플러그 인 클래스	260
17 장 활성 디렉토리 인증 속성	261
주 활성 Directory Server	262
보조 활성 Directory Server	262
사용자 검색을 시작할 DN	263
루트 사용자 바인드용 DN	263
루트 사용자 바인드용 비밀번호	263
루트 사용자 바인드용 비밀번호 (확인)	264
사용자 프로필 검색 시 사용되는 활성 디렉토리 속성	264
인증될 사용자 검색 시 사용되는 활성 디렉토리 속성	264
사용자 검색 필터	264
검색 범위	265
SSL 이 활성 Directory Server 에 액세스 가능	265
인증할 사용자 DN 반환	265
활성 Directory Server 확인 간격	266
사용자 작성 속성 목록	266
인증 수준	266

18 장 익명 인증 속성	267
유효한 익명 사용자 목록	267
기본 익명 아이디	268
대소문자 구분 사용자 아이디 사용	268
인증 수준	268
19 장 인증서 인증 속성	271
LDAP 에서 인증서 일치	272
LDAP 에서 인증서 검색 시 사용되는 주제 DN 속성	272
CRL 에 인증서 일치	272
LDAP 에서 CRL 검색 시 사용되는 발급자 DN 속성	272
CRL 업데이트용 HTTP 매개 변수	273
OCSP 검증 사용 가능	273
인증서가 저장되는 LDAP 서버	273
LDAP 검색 시작 DN	274
LDAP 서버 기본 사용자	274
LDAP 서버 기본 비밀번호	274
프로필 아이디의 LDAP 속성	274
LDAP 액세스에 SSL 사용	275
사용자 프로필 액세스에 사용되는 인증서 필드	275
사용자 프로필 액세스에 사용되는 기타 인증서 필드	275
신뢰할 수 있는 원격 호스트	276
SSL 포트 번호	276
인증 수준	276
20 장 핵심 인증 속성	277
전역 속성	277
플러그 가능 인증 모듈 클래스	278
지원되는 클라이언트용 인증 모듈	278
LDAP 연결 풀 크기	278
기본 LDAP 연결 풀 크기	278
조직 속성	279
조직 인증 모듈	280
사용자 프로필	280
관리자 인증 구성	280
사용자 프로필 동적 작성 기본 역할	281
영구 쿠키 모드 사용 가능	281
영구 쿠키 최대 시간	281
모든 사용자를 위한 사용자 컨테이너	282
별칭 검색 속성 이름	282
아이디 지정 속성	282
기본 인증 로컬	283
조직 인증 구성	284

로그인 실패 잠금 모드 사용 가능	285
로그인 실패 잠금 수	285
로그인 실패 잠금 간격	285
잠금 알림을 보낼 전자 메일 주소	285
N 회 실패 후 사용자에게 경고	285
로그인 실패 잠금 기간	286
잠금 속성 이름	286
잠금 속성 값	286
기본 성공 로그인 URL	286
기본 실패 로그인 URL	287
인증 사후 처리 클래스	287
사용자 아이디 생성 모드 사용 가능	287
플러그 가능 아이디 생성기 클래스	287
기본 인증 수준	288
21 장 HTTP 기본 인증 속성	289
인증 수준	289
22 장 JDBC 인증 속성	291
연결 유형	292
연결 풀 JNDI 이름	292
JDBC 드라이버	294
JDBC URL	294
데이터베이스에 연결할 사용자	294
데이터베이스에 연결할 비밀번호	294
데이터베이스에 연결할 비밀번호 (확인)	294
데이터베이스의 비밀번호 열	294
준비된 명령문	295
비밀번호 구문을 변환할 클래스	295
인증 수준	295
23 장 LDAP 인증 속성	297
주 LDAP 서버	298
보조 LDAP 서버	298
사용자 검색을 시작할 DN	299
루트 사용자 바인드용 DN	299
루트 사용자 바인드용 비밀번호	299
루트 사용자 바인드용 비밀번호 (확인)	300
사용자 프로필 검색 시 사용되는 LDAP 속성	300
인증될 사용자 검색 시 사용되는 LDAP 속성	300
사용자 검색 필터	300
검색 범위	300

SSL 이 LDAP 서버에 액세스 가능	301
인증할 사용자 DN 반환	301
LDAP 서버 확인 간격	301
사용자 작성 속성 목록	302
인증 수준	302
24 장 구성원 인증 속성	303
최소 비밀번호 길이	304
기본 사용자 역할	304
등록 후 사용자 상태	304
주 LDAP 서버	304
보조 LDAP 서버	305
사용자 검색을 시작할 DN	305
루트 사용자 바인드용 DN	306
루트 사용자 바인드용 비밀번호	306
루트 사용자 바인드용 비밀번호 (확인)	306
사용자 프로필 검색 시 사용되는 LDAP 속성	306
인증될 사용자 검색 시 사용되는 LDAP 속성	306
사용자 검색 필터	306
검색 범위	307
SSL 이 LDAP 서버에 액세스 가능	307
인증할 사용자 DN 반환	307
인증 수준	308
25 장 MSISDN 인증 속성	309
신뢰할 수 있는 게이트웨이 IP 주소	309
MSISDN 번호 인수	309
LDAP 서버 및 포트	310
LDAP 시작 검색 DN	310
LDAP 검색에 사용할 속성	310
LDAP 서버 기본 사용자	311
LDAP 서버 기본 비밀번호	311
LDAP 서버 기본 비밀번호 (확인)	311
LDAP 액세스에 대해 SSL 설정	311
MSISDN 헤더 검색 속성	311
인증 수준	312
26 장 Windows NT 인증 속성	313
Windows NT 인증 도메인	314
Windows NT 인증 호스트	314
Windows NT Samba 구성 파일 이름	314
인증 수준	314

27 장 RADIUS 인증 속성	317
RADIUS 서버 1	317
RADIUS 서버 2	318
RADIUS 공유 비밀	318
RADIUS 공유 비밀 (확인)	318
RADIUS 서버 포트	318
시간 초과	318
인증 수준	318
28 장 SafeWord 인증 속성	321
SafeWord 서버	322
SafeWord 서버 검증 파일 디렉토리	322
SafeWord 로깅 사용	322
SafeWord 로깅 수준	322
SafeWord 로그 파일	322
SafeWord 인증 연결 시간 초과	323
SafeWord 클라이언트 유형	323
SafeWord eassp 버전	323
SafeWord 최소 인증 강도	323
인증 수준	324
29 장 SAML 인증 속성	325
인증 수준	325
30 장 SecurID 인증 속성	327
SecurID ACE/ 서버 구성 경로	327
SecurID 도우미 구성 포트	328
SecurID 도우미 인증 포트	328
인증 수준	328
31 장 Unix 인증 속성	329
전역 속성	329
Unix 도우미 구성 포트	330
Unix 도우미 인증 포트	330
Unix 도우미 시간 초과	330
Unix 도우미 스레드	330
조직 속성	330
인증 수준	330
32 장 Windows 데스크탑 SSO 인증 속성	333
서비스 기본	333

키템 파일 이름	334
커버로스 영역	334
커버로스 서버 이름	334
도메인 이름과 함께 기본 반환	334
인증 수준	334
33 장 인증 구성 서비스 속성	337
인증 구성	337
로그인 성공 URL	338
로그인 실패 URL	338
인증 사후 처리 클래스	339
확인 수준 충돌	339
34 장 클라이언트 검색 서비스 속성	341
클라이언트 유형	341
클라이언트 관리자	342
기본 클라이언트 유형	344
클라이언트 검색 클래스	344
클라이언트 검색 사용 가능	344
35 장 국제화 설정 서비스 속성	345
각 로캘이 지원하는 문자 집합	345
문자 집합 별칭	345
자동 생성된 공통 이름 형식	346
36 장 로깅 서비스 속성	347
최대 로그 크기	348
기록 파일 수	348
로그 파일 위치	348
로깅 유형	349
데이터베이스 사용자 이름	349
데이터베이스 사용자 비밀번호	349
데이터베이스 사용자 비밀번호 (확인)	349
데이터베이스 드라이버 이름	349
구성 가능한 로그 필드	349
로그 확인 빈도	350
로그 서명 시간	350
보안 로깅 사용 가능	350
최대 레코드 수	350
아카이브당 파일 수	351
버퍼 크기	351
DB 실패 메모리 버퍼 크기	351

버퍼 시간	351
시간 버퍼링 사용 가능	351
37 장 이름 지정 서비스 속성	353
프로필 서비스 URL	354
세션 서비스 URL	354
로그 서비스 URL	354
정책 서비스 URL	354
인증 서비스 URL	354
SAML 웹 프로필 / 아티팩트 서비스 URL	355
SAML SOAP 서비스 URL	355
SAML 웹 프로필 /POST 서비스 URL	355
SAML 명제 관리자 서비스 URL	355
연합 명제 관리자 서비스 URL	356
Identity SDK 서비스 URL	356
보안 토큰 관리자 URL	356
JAXRPC 종점 URL	356
38 장 비밀번호 재설정 서비스 속성	357
사용자 검증	358
비밀 문제	358
검색 필터	358
기본 DN	358
바인드 DN	358
바인드 비밀번호	359
비밀번호 재설정 옵션	359
비밀번호 변경 알림 옵션	359
비밀번호 재설정 사용 가능	359
개인 질문 사용 가능	359
최대 질문 수	360
다음 로그인 시 반드시 비밀번호 변경	360
비밀번호 재설정 실패 잠금 사용 가능	360
비밀번호 재설정 실패 잠금 수	360
비밀번호 재설정 실패 잠금 간격	360
잠금 알림을 보낼 전자 메일 주소	360
N 회 실패 후 사용자에게 경고	361
비밀번호 재설정 실패 잠금 기간	361
비밀번호 재설정 잠금 속성 이름	361
비밀번호 재설정 잠금 속성 값	361
39 장 플랫폼 서비스 속성	363
서버 목록	363

플랫폼 로컬	364
쿠키 도메인	364
로그인 서비스 URL	364
로그아웃 서비스 URL	364
사용 가능한 로컬	365
클라이언트 문자 집합	365
40 장 정책 구성 서비스 속성	367
전역 속성	367
자원 비교기	368
거부 결정에 대한 평가 계속	368
조직 속성	368
LDAP 서버 및 포트	370
LDAP 기본 DN	370
LDAP 사용자 기본 DN	370
Access Manager 역할 기본 DN	371
LDAP 바인드 DN	371
LDAP 바인드 비밀번호	371
LDAP 바인드 비밀번호 (확인)	371
LDAP 조직 검색 필터	371
LDAP 조직 검색 범위	371
LDAP 그룹 검색 필터	372
LDAP 그룹 검색 범위	372
LDAP 사용자 검색 필터	372
LDAP 사용자 검색 범위	372
LDAP 역할 검색 필터	372
LDAP 역할 검색 범위	373
Access Manager 역할 검색 범위	373
LDAP 조직 검색 속성	373
LDAP 그룹 검색 속성	373
LDAP 사용자 검색 속성	373
LDAP 역할 검색 속성	373
검색에서 반환되는 최대 결과 수	374
검색 시간 초과	374
LDAP SSL 사용 가능	374
LDAP 연결 풀 최소 크기	374
LDAP 연결 풀 최대 크기	374
선택한 정책 주제	374
선택한 정책 조건	375
선택한 정책 참조	375
주제 결과 수명	375
사용자 별칭 사용 가능	375

41 장 SAML 서비스 속성	377
사이트 아이디 및 사이트 발급자 이름	378
SAML 요청에 서명	378
SAML 응답에 서명	378
서명 명제	378
SAML 아티팩트 이름	378
대상 지정자	379
아티팩트 시간 초과	379
notBefore 시간에 대한 명제 비대칭 요소	379
명제 시간 초과	379
신뢰할 수 있는 파트너 사이트	379
대상 URL 에 POST	383
42 장 세션 서비스 속성	385
보조 구성 인스턴스	385
인스턴스 이름	385
세션 저장소 사용자	385
세션 저장소 비밀번호	386
세션 저장소 비밀번호 (확인)	386
세션 클러스터 서버 목록	386
최대 대기 시간	386
JDBC 드라이버 구현 클래스	386
JDBC URL	386
최소 풀 크기	386
최대 풀 크기	387
전역 속성	387
최대 검색 결과 수	387
검색 시간 초과 (초)	387
동적 속성	387
최대 세션 시간 (분)	388
최대 유효 시간 (분)	388
최대 캐싱 시간 (분)	388
43 장 SOAP 바인드 서비스 속성	389
요청 처리기 목록	389
웹 서비스 인증자	390
지원되는 인증 기법	390
44 장 사용자 속성	391
사용자 서비스 속성	391
사용자 기본 언어	392
사용자 기본 표준 시간대	392

상속된 로컬	392
관리자 DN 시작 보기	392
기본 사용자 상태	392
사용자 프로필 속성	393
이름	393
성	393
성명	393
비밀번호	393
비밀번호 (확인)	393
전자 메일 주소	394
사원 번호	394
전화 번호	394
주소 (집)	394
사용자 상태	394
계정 만료일	395
사용자 인증 구성	395
사용자 별칭 목록	395
기본 로컬	395
성공 URL	395
실패 URL	396
고유 사용자 아이디	396
부록 A 오류 코드	399
Access Manager 콘솔 오류	399
인증 오류 코드	400
정책 오류 코드	403
amadmin 오류 코드	405
용어집	411

설명서 소개

*Sun Java™ System Access Manager 2005Q1 관리 설명서*에서는 사용자 및 명령줄 인터페이스를 통해 Sun Java System Access Manager(이전 명칭 Sun™ ONE Access Manager) 를 관리하는 방법을 설명합니다.

이 머리말은 다음 내용으로 구성되어 있습니다.

- 대상
- 이 설명서를 읽기 전에
- 이 설명서에 사용된 규약
- 관련 설명서
- Sun 자원 온라인 액세스
- Sun 기술 지원 문의
- 관련된 타사 웹 사이트 참조
- 사용자 의견 환영

대상

이 *관리 설명서*는 Sun Java System 서버와 소프트웨어를 사용하여 통합 아이디 관리와 웹 액세스 플랫폼을 구현하는 IT 관리자 및 소프트웨어 개발자를 대상으로 합니다.

이 설명서를 이해하려면 다음과 같은 개념과 기술에 대해 잘 알고 있어야 합니다.

- Sun Java System Directory Server
- LDAP (Lightweight Directory Access Protocol) 개념
- Java™ 기술

- JavaServer Pages™ (JSP) 기술
- HTTP (HyperText Transfer Protocol)
- HTML (HyperText Markup Language)
- XML (eXtensible Markup Language)

이 설명서를 읽기 전에

Access Manager 는 네트워크나 인터넷 환경을 통해 배포된 엔터프라이즈 응용 프로그램을 지원하는 소프트웨어 기반 구조인 Sun Java Enterprise System 의 구성 요소입니다 . Sun Java Enterprise System 과 함께 제공된 설명서를 잘 이해하고 있어야 합니다 . 이 설명서는 다음 위치에서 이용할 수 있습니다 .

<http://docs.sun.com/prod/entsys.05q1> 및
<http://docs.sun.com/prod/entsys.05q1?l=ko>

Sun Java System Directory Server 가 Access Manager 배포의 데이터 저장소로 사용되기 때문에 Directory Server 설명서의 내용도 잘 이해하고 있어야 합니다 . 이 설명서는 다음에서 온라인으로 액세스할 수 있습니다 .

http://docs.sun.com/coll/DirectoryServer_05q1 및
http://docs.sun.com/coll/DirectoryServer_05q1_ko

이 설명서에 사용된 규약

이 절의 표는 이 설명서에 사용된 규약을 설명합니다 .

활자체 규약

다음 표는 이 설명서에 사용된 활자체 규약을 설명합니다 .

표 1 활자체 규약

활자체	의미	예
AaBbCc123 (고정 폭)	API 및 언어 요소, HTML 태그, 웹 사이트 URL, 명령 이름, 파일 이름, 디렉토리 경로 이름, 화면 상 컴퓨터 출력, 샘플 코드	.login 파일을 편집합니다. ls -a 를 사용하여 모든 파일을 나열합니다. % You have mail.
AaBbCc123 (고정 폭 굵게)	컴퓨터 화면 출력과 대조하면서 사용자가 입력하는 내용	% su Password:
AaBbCc123 (기울임꼴)	설명서 제목, 새 용어, 강조할 단어 실제 이름이나 값으로 대체할 명령 및 경로 이름의 자리 표시자	사용자 안내서의 6 장을 읽으십시오. 이를 클래스 옵션이라 합니다. 파일을 저장하지 마십시오. 파일은 install-dir/bin 디렉토리에 있습니다.

기호

다음 표는 이 설명서에 사용된 기호 규약을 설명합니다.

표 2 기호 규약

기호	설명	예	의미
[]	선택 가능한 명령 옵션을 포함합니다.	ls [-l]	-l 옵션은 필수 사항이 아닙니다.
{ }	필수 명령 옵션에 대한 선택 사항 세트를 포함합니다.	-d {y n}	-d 옵션의 경우 y 인수나 n 인수 중 하나를 사용해야 합니다.
-	동시에 여러 키를 누릅니다.	Control-A	Ctrl 키와 A 키를 함께 누릅니다.
+	여러 키를 차례로 누릅니다.	Ctrl+A+N	Ctrl 키를 눌렀다가 놓고 연속하여 나머지 키를 누릅니다.
>	그래픽 사용자 인터페이스의 메뉴 항목 선택을 나타냅니다.	파일 > 새로 만들기 > 템플리트	파일 메뉴에서 새로 만들기를 선택합니다. 새로 만들기 하위 메뉴에서 템플리트를 선택합니다.

기본 경로 및 파일 이름

다음 표는 이 설명서에 사용된 기본 경로와 파일 이름을 설명합니다.

표 3 기본 경로 및 파일 이름

용어	설명
<i>AccessManager-base</i>	Access Manager의 기본 설치 디렉토리를 나타냅니다. Access Manager 2005 기본 설치 및 제품 디렉토리는 각 플랫폼에 따라 다릅니다. Solaris™ 시스템 : /opt/SUNWam Linux 시스템 : /opt/sun/identity
<i>DirectoryServer-base</i>	Sun Java System Directory Server의 기본 설치 디렉토리를 나타냅니다. 해당 경로 이름의 제품 설명서를 참조하십시오.
<i>ApplicationServer-base</i>	Sun Java System Application Server의 기본 설치 디렉토리를 나타냅니다. 특정 경로 이름의 제품 설명서를 참조하십시오.
<i>WebServer-base</i>	Sun Java System Web Server의 기본 설치 디렉토리를 나타냅니다. 특정 경로 이름에 대해서는 제품 설명서를 참조하십시오.

셸 프롬프트

다음 표는 이 설명서에 사용된 셸 프롬프트를 설명합니다.

표 4 셸 프롬프트

셸	프롬프트
UNIX 또는 Linux의 C 셸	<i>machine-name%</i>
UNIX 또는 Linux의 C 셸 슈퍼유저	<i>machine-name#</i>
UNIX 또는 Linux의 Bourne 셸 및 Korn 셸	\$
UNIX 또는 Linux의 Bourne 셸 또는 Korn 셸 슈퍼유저	#
Windows 명령줄	C:\

관련 설명서

온라인으로 Sun 기술 설명서를 이용하려면 <http://docs.sun.com>으로 이동하십시오.

설명서 아카이브를 찾아보거나 특정 설명서 제목, 부품 번호, 주제 등을 검색할 수 있습니다.

이 설명서 세트의 문서

표 5 Access Manager 6 2005Q1 설명서 세트

설명서 제목	설명
Technical Overview http://docs.sun.com/doc/817-7643	Access Manager 구성 요소들이 함께 작동하여 ID 관리를 통합하고 엔터프라이즈 자산과 웹 기반 응용 프로그램을 보호하는 방법에 대한 개요를 자세히 다룹니다. 기본 Access Manager 개념과 용어를 설명합니다.
Deployment Planning Guide http://docs.sun.com/doc/817-7644	기존의 정보 기술 기반구조 안에서 배포를 계획하는 것에 대한 정보를 제공합니다.
관리 안내서 (본 안내서) http://docs.sun.com/doc/819-1939	Access Manager 콘솔을 사용하고 명령줄을 통해 사용자 및 서비스 데이터를 관리하는 방법을 설명합니다.
Migration Guide http://docs.sun.com/doc/817-7645	기존 데이터와 Sun Java System 제품 배포를 Access Manager 최신 버전으로 마이그레이션하는 방법을 설명합니다. Access Manager 및 기타 제품의 설치 및 업그레이드에 대해서는 <i>Sun Java Enterprise System 2005Q1 설치 안내서</i> 를 참조하십시오.
Performance Tuning Guide http://docs.sun.com/doc/817-7646	Access Manager 및 관련 구성 요소를 조정하는 방법을 설명합니다.
Federation Management Guide http://docs.sun.com/doc/817-7648	Liberty Alliance Project를 기반으로 한 연합 관리의 정보를 제공합니다.
Developer's Guide http://docs.sun.com/doc/817-7649	Access Manager 를 사용자 정의하고 조직의 현재 기술 기반구조로 그 기능을 통합하는 방법에 대한 정보를 제공합니다. 또한 제품 및 API 의 프로그램 사양에 대한 정보를 제공합니다.
Developer's Reference http://docs.sun.com/doc/817-7650	Access Manager 공개 C API 를 구성하는 데이터 유형, 구조, 기능 등의 요약을 제공합니다.
릴리스 노트 http://docs.sun.com/doc/819-1947	제품 출시 후 사용할 수 있습니다. 이 릴리스의 새로운 기능에 대한 설명, 알려진 문제점과 제한 사항, 설치 노트, 소프트웨어 또는 설명서에 관한 문제를 보고하는 방법 등의 최신 정보가 이 파일에 포함되어 있습니다.

Access Manager 정책 에이전트 설명서

Access Manager 정책 에이전트의 설명서를 다음 웹 사이트에서 사용할 수 있습니다.

http://docs.sun.com/coll/S1_IdServPolicyAgent_21

Access Manager 정책 에이전트 사용 일정은 서버 제품 자체의 일정과 다릅니다. 따라서 정책 에이전트 설명서 세트는 Access Manager 핵심 설명서 세트와 별도로 사용할 수 있습니다. 이 설명서 집합에 포함된 제목은 다음과 같습니다.

- *Policy Agents For Web and Proxy Servers Guide*에서는 다양한 웹 서버 및 프록시 서버에 Access Manager 정책 에이전트를 설치하여 구성하는 방법에 대해 설명합니다. 또한 이 설명서에는 각 에이전트별 정보와 문제 해결이 포함되어 있습니다.
- *J2EE Policy Agents Guide*에서는 다양한 호스트 J2EE 응용 프로그램을 보호할 수 있는 Access Manager 정책 에이전트를 설치하여 구성하는 방법에 대해 설명합니다. 또한 이 설명서에는 각 에이전트별 정보와 문제 해결이 포함되어 있습니다.
- *릴리스 노트*는 에이전트 세트 릴리스 후 온라인으로 사용할 수 있습니다. *릴리스 노트*에는 해당 릴리스의 새로운 기능에 대한 설명, 알려진 문제점과 제한 사항, 설치 주의 사항 및 소프트웨어 또는 설명서에 관한 문제를 보고하는 방법 등의 최신 정보가 포함되어 있습니다.

기타 서버 설명서

기타 서버 설명서를 보려면 다음으로 이동하십시오.

- Directory Server 설명서
http://docs.sun.com/coll/DirectoryServer_05q1 및
http://docs.sun.com/coll/DirectoryServer_05q1_ko
- Web Server 설명서
http://docs.sun.com/coll/WebServer_05q1 및
http://docs.sun.com/coll/WebServer_05q1_ko
- Application Server 설명서
http://docs.sun.com/coll/ApplicationServer_05q1 및
http://docs.sun.com/coll/ApplicationServer_05q1_ko
- Web Proxy Server 설명서
<http://docs.sun.com/prod/s1.webproxys#hic>

Sun 자원 온라인 액세스

제품 다운로드, 전문가 서비스, 패치, 지원 및 추가 개발자 정보를 보려면 다음으로 이동하십시오.

다운로드 센터

<http://www.sun.com/software/download/>

전문가 서비스

<http://www.sun.com/service/sunps/sunone/index.html>

Sun 엔터프라이즈 서비스, Solaris 패치 및 지원

<http://sunsolve.sun.com/>

개발자 정보

<http://developers.sun.com/prodtech/index.html>

Sun 기술 지원 문의

이 제품에 대한 기술적 질문의 답변을 해당 제품 설명서에서 확인할 수 없을 때는 다음으로 이동하십시오.

<http://www.sun.com/service/contacting>

관련된 타사 웹 사이트 참조

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

사용자 의견 환영

Sun 은 설명서의 내용을 개선하기 위해 노력하고 있으며 사용자의 의견 및 제안을 환영합니다.

의견을 보내려면 <http://docs.sun.com> 에서 의견 보내기를 누릅니다. 온라인 양식에 설명서 제목과 부품 번호를 입력합니다. 부품 번호는 해당 설명서의 제목 페이지나 문서 맨 위에 있으며 일반적으로 7 자리 또는 9 자리 숫자입니다. 예를 들어 이 설명서의 제목은 *Sun Java™ System Access Manager 6 2005Q1 관리 안내서*이고 부품 번호는 819-1939 입니다. 사용자 의견을 제출할 때 해당 양식에 영문 설명서 제목과 부품 번호를 입력해야 할 수도 있습니다. 본 설명서의 영문 부품 번호와 제목은 817-7647, *Sun Java™ System Access Manager 6 2005Q1 Administration Guide* 입니다.

Access Manager 구성

*Sun Java™ System Access Manager 6 2005Q1 관리 설명서*의 1 부입니다. 이 부분에서는 Access Manager 설치 후 수행할 수 있는 구성 옵션에 대해 설명하며 다음 내용으로 구성되어 있습니다.

- 31 페이지의 "Access Manager 2005Q1 구성 스크립트 "
- 53 페이지의 "SSL 모드에서 Access Manager 구성 "

Access Manager 2005Q1 구성 스크립트

이 장에서는 amconfig 스크립트와 샘플 자동 설치 모드 입력 파일 (amsamplesilent) 을 사용하여 Sun Java™ System Access Manager 를 구성하고 배포하는 방법에 대해 설명합니다. 이 장에 포함된 항목은 다음과 같습니다.

- 32 페이지의 "Access Manager 2005Q1 설치 개요 "
- 35 페이지의 "Access Manager 샘플 구성 스크립트 입력 파일 "
 - 배포 모드 변수
 - Access Manager 구성 변수
 - 웹 컨테이너 구성 변수
 - Directory Server 구성 변수
- 46 페이지의 "Access Manager amconfig 스크립트 "
- 47 페이지의 "Access Manager 배포 시나리오 "
 - 추가 Access Manager 인스턴스 배포
 - Access Manager 인스턴스 재구성
 - Access Manager 인스턴스 제거
 - 모든 Access Manager 인스턴스 제거

Access Manager 2005Q1 설치 개요

새로 설치하는 경우에는 항상 Sun Java Enterprise System 설치 프로그램을 실행하여 Access Manager 2005Q1의 첫 번째 인스턴스를 설치하십시오. 설치 프로그램을 실행할 때 다음 Access Manager 구성 옵션 중 하나를 선택할 수 있습니다.

- 지금 구성 옵션을 선택하면 설치하는 동안 Access Manager 설치 패널에서 선택하는 값 또는 기본값에 의해 첫 번째 인스턴스를 구성할 수 있습니다.
- 나중에 구성 옵션을 선택하면 Access Manager 2005Q1 구성 요소를 설치한 후 [Access Manager 인스턴스 재구성](#)에 설명된 것처럼 구성 요소를 구성해야 합니다. 이 옵션을 선택하면 현재 설치 중인 제품이 하나도 구성되지 않습니다. 예를 들어 Access Manager 및 Application Server 설치를 선택하고 나중에 구성 옵션을 선택하면 두 응용 프로그램 모두 구성되지 않습니다.

설치 프로그램에 대한 내용은 *Sun Java Enterprise System 2005Q1 설치 설명서* (<http://docs.sun.com/doc/819-0809>)를 참조하십시오.

주 Solaris에서 Access Manager 2005Q1 버전을 확인하려면 Access Manager 패치를 찾아 설치된 Access Manager 버전을 확인합니다. 다음 명령을 입력합니다.

```
# showrev -p | grep SUNWam
```

Java Enterprise System 설치 프로그램은 Access Manager 2005Q1 amconfig 스크립트와 샘플 자동 설치 모드 입력 파일 (amsamplesilent)을 Solaris 시스템의 *AccessManager-base/SUNWam/bin* 디렉토리나 Linux 시스템의 *AccessManager-base/identity/bin* 디렉토리에 설치합니다.

*AccessManager-base*는 Access Manager 기본 설치 디렉토리를 나타냅니다. Solaris 시스템에서는 /opt가 기본 설치 디렉토리이고 Linux 시스템에서는 /opt/sun이 기본 설치 디렉토리입니다. 그러나, 설치 프로그램을 실행할 때 다른 디렉토리를 지정할 수도 있습니다.

amconfig 스크립트는 요청된 작업을 수행하기 위해 필요할 때 다른 스크립트를 호출하는 최상위 스크립트입니다. 자세한 내용은 [Access Manager amconfig 스크립트](#)를 참조하십시오.

샘플 자동 설치 모드 입력 파일 (amsamplesilent)은 amconfig 스크립트를 자동 설치 모드로 실행할 때 지정해야 하는 입력 파일의 한 예입니다.

이 샘플 자동 설치 모드 입력 파일은 Access Manager 구성 변수가 포함된 ASCII 텍스트 파일입니다. `amconfig` 스크립트를 실행하기 전에 `amsamplesilent` 파일을 복사하고 (원하는 경우 이름 다시 지정) 그 파일에서 변수를 편집합니다. 구성 변수의 형식은 다음과 같습니다.

변수 - 이름 = 값

예를 들면 다음과 같습니다.

```
DEPLOY_LEVEL=1
NEW_INSTANCE=true
SERVER_HOST=ishost.example.com
```

구성 스크립트 입력 파일에서 설정할 수 있는 변수의 목록은 [Access Manager 샘플 구성 스크립트 입력 파일](#)을 참조하십시오.

주의 `amconfig` 스크립트를 자동 설치 모드로 실행할 때 사용되는 자동 설치 모드 입력 파일의 형식은 Java Enterprise System 자동 설치 상태 파일과 동일한 형식을 따르거나 동일한 이름을 사용하지 않을 수 있습니다. 이 파일에는 관리자 비밀번호와 같은 민감한 데이터가 포함되므로 확실히 보호 또는 삭제하도록 합니다.

Access Manager `amconfig` 스크립트 작업

Sun Java Enterprise System 설치 프로그램을 사용하여 Access Manager의 첫 번째 인스턴스를 설치한 후 `amconfig` 스크립트를 실행하면 자동 설치 모드 입력 파일에 있는 변수의 값에 따라 다음과 같은 작업을 수행할 수 있습니다.

- Access Manager의 추가 인스턴스를 동일한 호스트 시스템에 배포하고 구성합니다. 예를 들어, 한 웹 컨테이너의 추가 인스턴스를 구성한 후 그 웹 컨테이너 인스턴스에 대해 새 Access Manager 인스턴스를 배포하고 구성할 수 있습니다.
- Access Manager의 첫 번째 인스턴스와 추가 인스턴스를 모두 다시 구성합니다.
- 다음 제품을 지원할 수 있도록 Access Manager SDK를 배포하고 구성합니다.
 - BEA WebLogic Server 6.1 SP4 및 SP5
 - BEA WebLogic Server 8.1 SP3
 - IBM WebSphere 5.1

- 콘솔 또는 연합 관리 모듈 등 특정 Access Manager 구성 요소를 배포하고 구성합니다.
- amconfig 스크립트를 사용하여 배포했던 Access Manager의 인스턴스와 구성 요소를 제거합니다.

Access Manager 샘플 구성 스크립트 입력 파일

Java Enterprise System 설치 프로그램을 실행한 후 Solaris 시스템의 *AccessManager-base/SUNWam/bin* 디렉토리 또는 Linux 시스템의 *AccessManager-base/identity/bin* 디렉토리에서 Access Manager 샘플 자동 설치 모드 입력 파일 (amsamplesilent) 을 사용할 수 있습니다.

구성 변수를 설정하려면 먼저 amsamplesilent 파일을 복사하고 이름을 바꿉니다. 그런 다음 수행하려는 작업을 위한 변수를 복사본에서 설정합니다.

이 샘플 자동 설치 모드 입력 파일에는 다음과 같은 구성 변수가 포함되어 있습니다.

- 배포 모드 변수
- Access Manager 구성 변수
- 웹 컨테이너 구성 변수
- Directory Server 구성 변수

배포 모드 변수

표 1-1에서는 필수 DEPLOY_LEVEL 변수의 값에 대해 설명합니다. 이 변수에 따라 amconfig 스크립트에서 수행할 작업이 결정됩니다.

표 1-1 Access Manager DEPLOY_LEVEL 변수

작업	DEPLOY_LEVEL 변수 값 및 설명
설치	1 = 새 인스턴스를 위한 전체 Access Manager 설치 (기본값) 2 = Access Manager 콘솔만 설치 3 = Access Manager SDK 만 설치 4 = SDK 만 설치하고 컨테이너 구성 5 = 연합 관리 모듈만 설치 6 = 서버만 설치
제거 (구성 해제)	11 = 전체 제거 12 = 콘솔만 제거 13 = SDK 만 제거 14 = SDK 만 제거하고 컨테이너 구성 해제 15 = 연합 관리 모듈 제거 16 = 서버만 제거

표 1-1 Access Manager DEPLOY_LEVEL 변수 (계속)

작업	DEPLOY_LEVEL 변수 값 및 설명
다시 설치 (재배포 또는 재구성)	21 = 모든 (콘솔, 비밀번호, 서비스 및 일반) 웹 응용 프로그램 재배포 26 = 모든 (콘솔, 비밀번호, 서비스 및 일반) 웹 응용 프로그램 배포 해제

Access Manager 구성 변수

표 1-2에서는 Access Manager 구성 변수에 대해 설명합니다.

표 1-2 Access Manager 구성 변수

변수	설명
BASEDIR	Access Manager 패키지를 위한 기본 설치 디렉토리 기본값 : PLATFORM_DEFAULT Solaris 시스템의 경우 PLATFORM_DEFAULT 는 /opt 입니다. Linux 시스템의 경우 PLATFORM_DEFAULT 는 /opt/sun 입니다.
SERVER_HOST	Access Manager 가 실행되고 있거나 설치될 시스템의 정규화된 호스트 이름 원격 SDK 설치의 경우에는 이 변수를 원격 클라이언트 호스트가 아니며 Access Manager 가 설치되어 있거나 설치될 호스트로 설정합니다.
SERVER_PORT	Access Manager 포트 번호 기본값 : 58080 원격 SDK 설치의 경우에는 이 변수를 원격 클라이언트 호스트가 아니며 Access Manager 가 설치되어 있거나 설치될 호스트의 포트로 설정합니다.
SERVER_PROTOCOL	서버 프로토콜 : http 또는 https 기본값 : http 원격 SDK 설치의 경우에는 이 변수를 원격 클라이언트 호스트가 아니며 Access Manager 가 설치되어 있거나 설치될 호스트의 프로토콜로 설정합니다.
CONSOLE_HOST	콘솔이 설치된 서버의 정규화된 호스트 이름 기본값 : Access Manager 호스트 (SERVER_HOST 변수) 를 위해 제공된 값
CONSOLE_PORT	콘솔이 설치되어 있고 연결을 수신하는 웹 컨테이너의 포트 기본값 : Access Manager 포트 (SERVER_PORT 변수) 를 위해 제공된 값
CONSOLE_PROTOCOL	콘솔이 설치되어 있는 웹 컨테이너의 프로토콜 기본값 : 서버 프로토콜 (SERVER_PROTOCOL 변수)
CONSOLE_REMOTE	콘솔이 Access Manager 서비스에서 원격인 경우 true 로 설정하고 그렇지 않을 경우 false 로 설정. 기본값 : false
DS_HOST	Directory Server 의 정규화된 호스트 이름
DS_PORT	Directory Server 포트 . 기본값 : 389

표 1-2 Access Manager 구성 변수 (계속)

변수	설명
DS_DIRMGRDN	디렉토리 관리자 DN. Directory Server 에 대한 무제한적인 액세스 권한을 가진 사용자 기본값 : "cn=Directory Manager"
DS_DIRMGRPWD	디렉토리 관리자 (DS_DIRMGRDN 변수) 의 비밀번호 ADMINPASSWD 설명의 특수 문자에 대한 부분 참조
ROOT_SUFFIX	디렉토리의 초기 또는 루트 접미어 . 이 값이 사용 중인 Directory Server 에 있다는 것을 확인해야 합니다 . ADMINPASSWD 설명의 특수 문자에 대한 부분 참조
ADMINPASSWD	관리자 (amadmin) 의 비밀번호 . amldapuser 의 비밀번호와 달라야 합니다 . 주 : 비밀번호에 포함되는 슬래시 (/) 나 백슬래시 (\) 같은 특수 문자는 작은따옴표 (') 안에 넣어야 합니다 . 예를 들면 다음과 같습니다 . ADMINPASSWD='\\\/\###\//' 그러나 작은따옴표를 실제 비밀번호의 문자 중 하나로 사용할 수는 없습니다 .
AMLDAPUSERPWD	amldapuser 의 비밀번호 . amadmin 의 비밀번호와 달라야 합니다 . ADMINPASSWD 설명의 특수 문자에 대한 부분 참조
CONSOLE_DEPLOY_URI	Access Manager 관리 콘솔 하위 구성 요소와 연관된 HTML 페이지 , 클래스 및 JAR 파일에 액세스하기 위한 URI 접두어 기본값 : /amconsole
SERVER_DEPLOY_URI	Identity Management and Policy Services Core 하위 구성 요소와 연관된 HTML 페이지 , 클래스 및 JAR 파일에 액세스하기 위한 URI 접두어 기본값 : /amserver
PASSWORD_DEPLOY_URI	Access Manager 를 실행하는 웹 컨테이너에서 사용자가 지정하는 문자열과 해당 배포 응용 프로그램 사이에 사용할 매핑을 결정하는 URI 기본값 : /ampassword
COMMON_DEPLOY_URI	웹 컨테이너의 공통 도메인 서비스에 액세스하기 위한 URI 접두어 기본값 : /amcommon
COOKIE_DOMAIN	Access Manager 가 사용자에게 세션 ID 를 부여할 때 브라우저로 반환하는 , 신뢰할 수 있는 DNS 도메인의 이름 . 최소한 하나의 값이 있어야 합니다 . 일반적으로 서버의 도메인 이름 앞에 마침표가 붙은 형식을 사용합니다 . 예 : .example.com
JAVA_HOME	JDK 설치 디렉토리에 대한 경로 기본값 : /usr/jdk/entsys-j2se 이 변수는 명령 줄 인터페이스 (예 : amadmin) 실행 파일에서 사용하는 JDK 를 제공합니다 .

표 1-2 Access Manager 구성 변수 (계속)

변수	설명
AM_ENC_PWD	비밀번호 암호화 키 : Access Manager 가 사용자 비밀번호를 암호화하기 위해 사용하는 문자열 . 기본값 : 없음 . 값이 없으므로 설정되면 amconfig 는 사용자에게 대해 비밀번호 암호화 키를 생성하므로 사용자가 지정하거나 amconfig 를 통해 만든 설치 프로그램에 대해 비밀번호 암호화가 사용됩니다 . 중요 : Access Manager 또는 원격 SDK 의 인스턴스를 여러 개 배포하는 경우 모든 인스턴스는 동일한 비밀번호 암호화 키를 사용해야 합니다 . 추가 인스턴스를 배포할 때 첫 번째 인스턴스의 AMConfig.properties 파일에서 am. encryption.pwd property 값을 복사합니다 .
PLATFORM_LOCALE	플랫폼의 로컬 . 기본값 : en_us(미국 영어)
NEW_OWNER	설치 후 Access Manager 파일의 새 소유자 . 기본값 : root
NEW_GROUP	설치 후 Access Manager 파일의 새 그룹 . 기본값 : other Linux 설치의 경우 NEW_GROUP 을 root 로 설정합니다 .
XML_ENCODING	XML 인코딩 . 기본값 : ISO-8859-1
NEW_INSTANCE	구성 스크립트가 새 사용자가 생성한 웹 컨테이너 인스턴스에 Access Manager 를 배포하는지 여부를 지정합니다 . <ul style="list-style-type: none"> • true = Java Enterprise System 설치 프로그램에 의해 생성된 인스턴스가 아닌 , 새 사용자가 생성한 웹 컨테이너 인스턴스에 Access Manager 를 배포 • false = 인스턴스를 재구성 기본값 : false

웹 컨테이너 구성 변수

Access Manager 의 웹 컨테이너를 지정하려면 자동 설치 모드 입력 파일의 WEB_CONTAINER 변수를 표 1-3 에 설명된 것처럼 설정합니다 .

표 1-3 Access Manager WEB_CONTAINER 변수

값	웹 컨테이너
WS6(기본값)	Sun Java System Web Server 6.1 SP4
AS7	Sun Java System Application Server 7.0 Update 3(이전 Access Manager 버전과의 호환성을 위해 제공)
AS8	Sun Java System Application Server 8.1
WL6	BEA WebLogic Server 6.1 SP4 및 SP5
WL8	BEA WebLogic Server 8.1
WAS4	IBM WebSphere 4.0.5(이전 Access Manager 버전과의 호환성을 위해 제공)

표 1-3 Access Manager WEB_CONTAINER 변수

값	웹 컨테이너
WAS5	IBM WebSphere 5.1

Sun Java System Web Server 6.1 SP4

표 1-4에서는 자동 설치 모드 입력 파일의 Web Server 6.1 SP4를 위한 구성 변수에 대해 설명합니다.

표 1-4 Web Server 6.1 SP2 구성 변수

변수	설명
WS61_INSTANCE	Access Manager가 배포되거나 배포 해제될 Web Server 인스턴스의 이름 기본값 : <code>https-web-server-instance-name</code> 여기서 <code>web-server-instance-name</code> 은 Access Manager 호스트 (<code>SERVER_HOST</code> 변수)입니다.
WS61_HOME	Web Server 기본 설치 디렉토리 기본값 : <code>/opt/SUNWwbsvr</code>
WS61_PROTOCOL	Access Manager가 배포될 Web Server 인스턴스 (<code>WS61_INSTANCE</code> 변수가 설정)에서 사용하는 프로토콜 : <code>http</code> 또는 <code>https</code> 기본값 : Access Manager 프로토콜 (<code>SERVER_PROTOCOL</code> 변수)
WS61_HOST	Web Server 인스턴스 (<code>WS61_INSTANCE</code> 변수)의 정규화된 호스트 이름 기본값 : Access Manager 호스트 인스턴스 (<code>SERVER_HOST</code> 변수)
WS61_PORT	Web Server가 연결을 수신하는 포트 기본값 : Access Manager 포트 번호 (<code>SERVER_PORT</code> 변수)
WS61_ADMINPORT	Web Server Administration Server가 연결을 수신하는 포트 기본값 : 8888
WS61_ADMIN	Web Server 관리자의 사용자 아이디 기본값 : "admin"
WS61_IS_SECURE	보안 포트 사용 여부 지정 <ul style="list-style-type: none"> • <code>true</code>: 보안 포트 사용 (HTTPS 프로토콜) • <code>false</code>: 보안 포트 사용 안 함 (HTTP 프로토콜) 기본값 : <code>false</code> (사용 안 함)

Sun Java System Application Server 7.0 Update 3

표 1-5에서는 자동 설치 모드 입력 파일의 Application Server 7.0 Update 3 용 구성 변수에 대해 설명합니다.

표 1-5 Application Server 7.0 Update 3 구성 변수

변수	설명
AS70_HOME	Application Server 7.0 이 설치된 디렉토리에 대한 경로 기본값 : /opt/SUNWappserver7
AS70_PROTOCOL	Application Server 인스턴스에 의해 사용되는 프로토콜 : http 또는 https 기본값 : Access Manager 프로토콜 (SERVER_PROTOCOL 변수)
AS70_HOST	Application Server 인스턴스가 연결을 수신하는 정규화된 도메인 이름 (FQDN) 기본값 : Access Manager 호스트 (SERVER_HOST 변수)
AS70_PORT	Application Server 인스턴스가 연결을 수신하는 포트 기본값 : Access Manager 포트 번호 (SERVER_PORT 변수)
AS70_ADMINPORT	Application Server 관리 서버가 연결을 수신하는 포트 기본값 : 4848
AS70_ADMIN	Application Server 가 표시되는 도메인을 위한 Application Server 관리 서버를 관리하는 사용자의 이름 기본값 : admin
AS70_ADMINPASSWD	Application Server 가 표시되는 도메인을 위한 Application Server 관리자의 비밀번호 ADMINPASSWD 설명의 특수 문자에 대한 부분 참조
AS70_INSTANCE	Access Manager 를 실행할 Application Server 인스턴스의 이름 기본값 : server1
AS70_DOMAIN	이 Access Manager 인스턴스를 배포하려는 도메인의 Application Server 디렉토리에 대한 경로 기본값 : domain1
AS70_INSTANCE_DIR	Application Server 가 인스턴스를 위한 파일을 저장하는 디렉토리에 대한 경로 기본값 : /var/opt/SUNWappserver7/domains/domain1/server1
AS70_DOCS_DIR	Application Server 가 문서를 저장하는 디렉토리 기본값 : /var/opt/SUNWappserver7/domains/domain1/server1/docroot

표 1-5 Application Server 7.0 Update 3 구성 변수 (계속)

변수	설명
AS70_IS_SECURE	<p>보안 포트 사용 여부 지정</p> <ul style="list-style-type: none"> • true: 보안 포트 사용 (HTTPS 프로토콜) • false: 보안 포트 사용 안 함 (HTTP 프로토콜) <p>기본값 : false(사용 안 함)</p> <p>Application Server admin 포트가 SSL 사용 포트이면 설치 도중 구성에 실패할 것입니다 . https 모드에서는 admin 서버를 사용하지 마십시오 .</p>

Sun Java System Application Server 8.1

표 1-6에서는 자동 설치 모드 입력 파일의 Application Server 8.1 을 위한 구성 요소에 대해 설명합니다 .

표 1-6 Application Server 8.1 구성 변수

변수	설명
AS81_HOME	<p>Application Server 8.1 이 설치된 디렉토리에 대한 경로</p> <p>기본값 : /usr/appserver1</p>
AS81_PROTOCOL	<p>Application Server 인스턴스에 의해 사용되는 프로토콜 : http 또는 https</p> <p>기본값 : Access Manager 프로토콜 (SERVER_PROTOCOL 변수)</p>
AS81_HOST	<p>Application Server 인스턴스가 연결을 수신하는 정규화된 도메인 이름 (FQDN)</p> <p>기본값 : Access Manager 호스트 (SERVER_HOST 변수)</p>
AS81_PORT	<p>Application Server 인스턴스가 연결을 수신하는 포트</p> <p>기본값 : Access Manager 포트 번호 (SERVER_PORT 변수)</p>
AS81_ADMINPORT	<p>Application Server 관리 서버가 연결을 수신하는 포트</p> <p>기본값 : 4849</p>
AS81_ADMIN	<p>Application Server 가 표시되는 도메인을 위한 Application Server 관리 서버를 관리하는 사용자의 이름</p> <p>기본값 : admin</p>
AS81_ADMINPASSWD	<p>Application Server 가 표시되는 도메인을 위한 Application Server 관리자의 비밀 번호</p> <p>ADMINPASSWD 설명의 특수 문자에 대한 부분 참조</p>
AS81_INSTANCE	<p>Access Manager 를 실행할 Application Server 인스턴스의 이름</p> <p>기본값 : server</p>

표 1-6 Application Server 8.1 구성 변수 (계속)

변수	설명
AS81_DOMAIN	Access Manager 인스턴스를 배포하려는 도메인의 Application Server 디렉토리에 대한 경로 기본값 : domain1
AS81_INSTANCE_DIR	Application Server 가 인스턴스를 위한 파일을 저장하는 디렉토리에 대한 경로 기본값 : /var//appserver/domains/domain1
AS81_DOCS_DIR	Application Server 가 문서를 저장하는 디렉토리 기본값 : /var/appserver/domains/domain1/docroot
AS81_IS_SECURE	보안 포트 사용 여부 지정 <ul style="list-style-type: none"> • true: 보안 포트 사용 (HTTPS 프로토콜) • false: 보안 포트 사용 안 함 (HTTP 프로토콜) 기본값 : false(사용 안 함) ampsamplesilent 의 경우 다음과 같이 응용 프로그램 서버 관리 포트가 안전한지 여부를 지정한 추가 설정이 있습니다. <ul style="list-style-type: none"> • true: 응용 프로그램 서버 관리 포트가 안전합니다 (HTTPS 프로토콜). • false: 응용 프로그램 서버 관리 포트가 안전하지 않습니다 (HTTP 프로토콜). 기본값 : true(사용 가능)

BEA WebLogic Server 6.1 SP4 및 SP5

표 1-7에서는 자동 설치 모드 입력 파일의 BEA WebLogic Server 6.1 을 위한 구성 변수에 대해 설명합니다.

표 1-7 BEA WebLogic Server 6.1 SP4 및 SP5 구성 변수

변수	설명
WL61_HOME	WebLogic 홈 디렉토리 . 기본값 : /export/boa61a
WL61_PROJECT_DIR	WebLogic 프로젝트 디렉토리 . 기본값 : user_projects
WL61_DOMAIN	WebLogic 도메인 이름 . 기본값 : mydomain
WL61_SERVER	WebLogic 서버 이름 . 기본값 : myserver
WL61_INSTANCE	WebLogic 인스턴스 이름 . 기본값 : WS61_HOME /wlserver6.1
WL61_PROTOCOL	WebLogic 프로토콜 . 기본값 : http
WL61_HOST	WebLogic 호스트 이름 .
WL61_PORT	WebLogic 포트 . 기본값 : 7001

표 1-7 BEA WebLogic Server 6.1 SP4 및 SP5 구성 변수 (계속)

변수	설명
WL61_SSLPORT	WebLogic SSL 포트. 기본값 : 7002
WL61_ADMIN	WebLogic 관리자. 기본값 : "system"
WL61_PASSWORD	WebLogic 관리자 비밀번호. ADMINPASSWD 설명의 특수 문자에 대한 부분 참조
WL61_JDK_HOME	WebLogic JDK 홈 디렉토리. 기본값 : WS61_HOME /jdk131

BEA WebLogic Server 8.1

[표 1-8](#)에서는 자동 설치 모드 입력 파일의 BEA WebLogic Server 8.1 을 위한 구성 요소에 대해 설명합니다.

표 1-8 BEA WebLogic Server 8.1 구성 변수

변수	설명
WL8_HOME	WebLogic 홈 디렉토리. 기본값 : /export/boa8
WL8_PROJECT_DIR	WebLogic 프로젝트 디렉토리. 기본값 : projects
WL8_DOMAIN	WebLogic 도메인 이름. 기본값 : mydomain
WL8_SERVER	WebLogic 서버 이름. 기본값 : myserver
WL8_INSTANCE	WebLogic 인스턴스 이름. 기본값 : /export/boa8/weblogic81
WL8_PROTOCOL	WebLogic 프로토콜. 기본값 : http
WL8_HOST	WebLogic 호스트 이름. 기본값 : 없음
WL8_PORT	WebLogic 포트. 기본값 : 7001
WL8_SSLPORT	WebLogic SSL 포트. 기본값 : 7002
WL8_ADMIN	WebLogic 관리자. 기본값 : "system"
WL8_PASSWORD	WebLogic 관리자 비밀번호 ADMINPASSWD 설명의 특수 문자에 대한 부분 참조
WL8_JDK_HOME	WebLogic JDK 홈 디렉토리. 기본값 : WL8_HOME /jdk141_03
WL8_CONFIG_LOCATION	WebLogic 시작 스크립트 위치의 부모 디렉토리로 설정해야 합니다.
WL8_IS_SECURE	보안 포트 사용 여부 지정 <ul style="list-style-type: none"> • true: 보안 포트 사용 (HTTPS 프로토콜) • false: 보안 포트 사용 안 함 (HTTP 프로토콜) 기본값 : false(사용 안 함)

IBM WebSphere 5.1

표 1-9에서는 자동 설치 모드 입력 파일의 IBM WebSphere Server 5.1을 위한 구성 변수에 대해 설명합니다.

표 1-9 IBM WebSphere 5.1 구성 변수

변수	설명
WAS51_HOME	WebSphere 홈 디렉토리 . 기본값 : /opt/WebSphere/AppServer
WAS51_JDK_HOME	WebSphere JDK 홈 디렉토리 . 기본값 : /opt/WebSphere/AppServer/java
WAS51_CELL	WebSphere 셀 . 기본값 : sample
WAS51_DOMAIN	WebSphere 도메인 이름 . 기본값 : mydomain
WAS51_NODE	WebSphere 노드 이름 . 기본값 : WebSphere 가 설치된 서버의 호스트 이름 . 기본값 : sample
WAS51_INSTANCE	WebSphere 인스턴스 이름 . 기본값 : server1
WAS51_PROTOCOL	WebSphere 프로토콜 . 기본값 : http
WAS51_HOST	WebSphere 호스트 이름 . 기본값 : sample
WAS51_PORT	WebSphere 포트 . 기본값 : 9080
WAS51_SSLPORT	WebSphere SSL 포트 . 기본값 : 9081
WAS51_ADMIN	WebSphere 관리자 . 기본값 : "admin"
WAS51_ADMINPORT	WebSphere 관리자 포트 . 기본값 : 9090
WAS51_IS_SECURE	보안 포트 사용 여부 지정 <ul style="list-style-type: none"> • true: 보안 포트 사용 (HTTPS 프로토콜) • false: 보안 포트 사용 안 함 (HTTP 프로토콜) 기본값 : false(사용 안 함)

Directory Server 구성 변수

Access Manager 2005Q1 은 Sun ONE Directory Server 5.1 과 Sun Java System Directory Server 5 2005Q1 을 지원합니다 . 표 1-10 에서는 자동 설치 모드 입력 파일 의 Directory Server 구성 변수에 대해 설명합니다 .

표 1-10 Directory Server 구성 변수

변수	설명
DIRECTORY_MODE	<p>Directory Server 모드 :</p> <p>1 = 디렉토리 정보 트리 (DIT) 의 새 설치를 위해 사용 .</p> <p>2 = 기존 DIT 를 위해 사용 . 이름 지정 속성 및 객체 클래스는 동일하므로 구성 스크립트는 installExisting.ldif 파일과 umsExisting.ldif 파일을 로드합니다 . 또한 구성 도중 입력된 실제 값 (예 : BASE_DIR, SERVER_HOST, ROOT_SUFFIX) 을 사용하여 LDIF 와 등록 정보를 업데이트합니다 . 구성 스크립트가 파일의 자리 표시자에 실제 구성 값을 대체하기 때문에 이 업데이트를 " 태그 스왑 " 이라고 부르기도 합니다 .</p> <p>3 = 수동 로드를 수행하려고 할 때 기존 DIT 를 위해 사용 . 이름 지정 속성과 객체 클래스가 다르므로 구성 스크립트는 installExisting.ldif 파일과 umsExisting.ldif 파일을 로드하지 않습니다 . 스크립트는 모드 2 에서 설명한 태그 스왑을 수행합니다 .</p> <p>LDIF 파일을 검사하여 필요한 부분을 수정한 다음 LDIF 파일과 서비스를 수동으로 로드해야 합니다 .</p> <p>4 = 기존의 다중 서버 설치를 위해 사용 . 기존 Access Manager 설치에 반하는 작업이기 때문에 LDIF 파일과 서비스를 로드하지 않습니다 . 스크립트는 태그 스왑만 수행하고 플랫폼 목록에 서버 항목을 추가합니다 .</p> <p>5 = 기존 업그레이드를 위해 사용 . 스크립트는 태그 스왑만 수행합니다 .</p> <p>기본값 : 1</p>
USER_NAMING_ATTR	<p>사용자 이름 지정 속성 : 관련 이름 공간 내에서 사용자 또는 자원의 고유 식별자 .</p> <p>기본값 : uid</p>
ORG_NAMING_ATTR	<p>사용자가 속한 회사 또는 조직의 이름 지정 속성 . 기본값 : o</p>
ORG_OBJECT_CLASS	<p>조직 객체 클래스 . 기본값 : sunManagedOrganization</p>
USER_OBJECT_CLASS	<p>사용자 객체 클래스 . 기본값 : inetOrgPerson</p>
DEFAULT_ORGANIZATION	<p>기본 조직 이름 . 기본값 : 없음</p>

Access Manager amconfig 스크립트

Java Enterprise System 설치 프로그램을 실행한 후 Solaris 시스템의 *AccessManager-base/SUNWam/bin* 디렉토리 또는 Linux 시스템의 *AccessManager-base/identity/bin* 디렉토리에서 amconfig 스크립트를 사용할 수 있습니다.

amconfig 스크립트는 자동 설치 입력 파일을 읽은 다음 요청받은 작업을 수행하기 위해 필요할 때 자동 설치 모드에서 다른 스크립트를 호출합니다.

amconfig 스크립트를 실행하려면 다음 구문을 사용합니다.

```
amconfig -s input-file
```

여기서

-s 는 amconfig 스크립트를 자동 설치 모드에서 실행합니다.

*입력-파일*은 수행하려는 작업을 위한 구성 변수가 포함된 자동 설치 입력 파일입니다. 세부 사항에 대해서는 [Access Manager 샘플 구성 스크립트 입력 파일](#)을 참조하십시오.

주 Access Manager 2005Q1 릴리스에서 다음 스크립트는 지원되지 않습니다.

- create 인수를 사용하는 amserver
- amserver.*instance*

또한 기본적으로 amserver start 는 인증 amsecuridd 및 amunixd 도우미만 시작합니다. amsecuridd 도우미는 Solaris OS SPARC 플랫폼에서만 사용할 수 있습니다.

Access Manager 배포 시나리오

Java Enterprise System 설치 프로그램을 사용하여 Access Manager의 첫 번째 인스턴스를 설치한 후 자동 설치 모드 입력 파일의 구성 변수를 편집한 다음 amconfig 스크립트를 실행하여 추가 Access Manager 인스턴스를 배포할 수 있습니다.

이 절에서는 다음 시나리오에 대해 설명합니다.

- 추가 Access Manager 인스턴스 배포
- Access Manager 인스턴스 재구성
- Access Manager 인스턴스 제거
- 모든 Access Manager 인스턴스 제거

추가 Access Manager 인스턴스 배포

Access Manager의 새 인스턴스를 배포하려면 먼저 웹 컨테이너용 관리 도구를 사용하여 새 웹 컨테이너 인스턴스를 생성하여 시작해야 합니다. 자세한 내용은 특정 웹 컨테이너 설명서를 참조하십시오.

- Web Server 6.1 SP2
http://docs.sun.com/coll/S1_websvr61_en 및
http://docs.sun.com/coll/S1_websvr61_ko
- Application Server 7.0 Update 3
http://docs.sun.com/coll/s1_asseu3_en 및
http://docs.sun.com/coll/s1_asseu3_ko

추가 Access Manager 인스턴스를 배포하려면

1. 인스턴스의 웹 컨테이너에 따라 관리자로 로그인합니다. 예를 들어, Web Server 6.1 이 새 인스턴스의 웹 컨테이너가 될 경우에는 슈퍼유저 (루트) 또는 Web Server Administration Server 를 위한 사용자 계정 중 하나로 로그인합니다.

2. `amsamplesilent` 파일을 쓰기 가능한 디렉토리에 복사하고 그 디렉토리를 현재 디렉토리로 만듭니다. 예를 들어, `/newinstances` 라는 이름의 디렉토리를 생성할 수 있습니다.

팁 `amsamplesilent` 파일의 복사본 이름을 배포하려는 새 인스턴스를 설명하는 이름으로 바꿉니다. 예를 들어, 다음 단계부터는 `amnews6instance` 라는 이름의 입력 파일을 사용하여 Web Server 6.1 을 위해 새 인스턴스를 설치할 수 있습니다.

3. 새 `amnews6instance` 파일에서 다음 변수를 설정합니다.

```
DEPLOY_LEVEL=1  
NEW_INSTANCE=true
```

생성하려는 새 인스턴스를 위해 필요한 `amnews6instance` 파일의 다른 변수를 설정합니다. 각 변수에 대한 설명은 다음 절의 표를 참조하십시오.

- [Access Manager 구성 변수](#)
- [웹 컨테이너 구성 변수](#)
- [Directory Server 구성 변수](#)

중요 모든 Access Manager 인스턴스는 반드시 동일한 비밀번호 암호화 키 값을 사용해야 합니다. 이 인스턴스를 위해 `AM_ENC_PWD` 변수를 설정하려면 첫 번째 인스턴스를 위한 `AMConfig.properties` 파일의 `am.encryption.pwd` 등록 정보 값을 복사합니다.

나중에 이 인스턴스를 제거할 필요가 있을 경우를 대비해 `amnews6instance` 파일을 저장해 둡니다.

4. 새 `amnews6instance` 파일을 지정하여 `amconfig` script 를 실행합니다. 예를 들어, Solaris 시스템에서는 다음과 같이 합니다.

```
cd AccessManager-base/SUNWam/bin/  
./amconfig -s /newinstances/amnews6instance
```

`-s` 옵션은 `amconfig` 스크립트를 자동 설치 모드로 실행합니다.

`amconfig` 스크립트는 `amnews6instance` 파일의 변수를 사용하여 새 인스턴스를 배포하는 데 필요한 다른 구성 스크립트를 호출합니다.

Access Manager 인스턴스 재구성

Java Enterprise System 설치 프로그램을 사용하여 설치한 Access Manager 의 첫 번째 인스턴스와 amconfig 스크립트를 실행하여 배포한 추가 Access Manager 인스턴스를 재구성할 수 있습니다.

예를 들면 , Access Manager 소유자와 그룹을 변경하기 위해 인스턴스를 재구성할 수 있습니다.

Access Manager 인스턴스 재구성

1. 인스턴스의 웹 컨테이너에 따라 관리자로 로그인합니다. 예를 들어 , Web Server 6.1 이 웹 컨테이너인 경우 슈퍼유저 (루트) 또는 Web Server Administration Server 를 위한 사용자 계정 중 하나로 로그인합니다.
2. 인스턴스를 배포하는 데 사용했던 자동 설치 입력 파일을 쓰기 가능한 디렉토리에 복사하고 그 디렉토리를 현재 디렉토리로 만듭니다. 예를 들어 , Web Server 6.1 을 위해 인스턴스를 재구성하려면 다음 단계부터 /reconfig 디렉토리에 있는 amnewinstanceforWS61 이라는 이름의 입력 파일을 사용합니다.
3. amnewinstanceforWS61 파일에서 DEPLOY_LEVEL 변수를 **다시 설치** 작업에 대해 설명한 값 중 하나로 설정합니다. 예를 들어 , 전체 설치를 재구성하려면 DEPLOY_LEVEL=21 로 설정합니다.
4. amnewinstanceforWS61 파일에서 NEW_INSTANCE 변수를 false 로 설정합니다.
`NEW_INSTANCE=false`
5. amnewinstanceforWS61 파일에서 인스턴스를 재구성하는 데 필요한 다른 변수를 설정합니다. 예를 들어 , 인스턴스의 소유자와 그룹을 변경하려면 NEW_OWNER 및 NEW_GROUP 변수를 새로운 값으로 설정합니다.

다른 변수에 대한 설명은 다음 절의 표를 참조하십시오 .

- [Access Manager 구성 변수](#)
- [웹 컨테이너 구성 변수](#)
- [Directory Server 구성 변수](#)

6. 편집된 입력 파일을 지정하여 `amconfig` 스크립트를 실행합니다. 예를 들어, Solaris 시스템에서는 다음과 같이 합니다.

```
cd AccessManager-base/SUNWam/bin/  
./amconfig -s /reconfig/amnewinstanceforWS61
```

-s 옵션은 스크립트를 자동 모드로 실행합니다. `amconfig` 스크립트는 `amnewinstanceforWS61` 파일의 변수를 사용하여 인스턴스를 재구성하는 데 필요한 다른 구성 스크립트를 호출합니다.

Access Manager 인스턴스 제거

`amconfig` 스크립트를 실행하여 설치한 Access Manager의 인스턴스를 제거할 수 있습니다. 또한 Access Manager 인스턴스를 일시적으로 구성 해제할 수 있으며 웹 컨테이너 인스턴스를 제거하지 않는 한 나중에 다른 Access Manager 인스턴스를 재배포하는 데 사용할 수 있습니다.

Access Manager 인스턴스 설치 제거

1. 인스턴스의 웹 컨테이너에 따라 관리자로 로그인합니다. 예를 들어, Web Server 6.1 이 웹 컨테이너인 경우 수퍼유저 (루트) 또는 Web Server Administration Server 를 위한 사용자 계정 중 하나로 로그인합니다.
2. 인스턴스를 배포하는 데 사용했던 자동 설치 입력 파일을 쓰기 가능한 디렉토리에 복사하고 그 디렉토리를 현재 디렉토리로 만듭니다. 예를 들어, Web Server 6.1 을 위해 인스턴스의 구성을 해제하려면 다음 단계부터 `/unconfigure` 디렉토리에 있는 `amnewinstanceforWS61` 이라는 이름의 입력 파일을 사용합니다.
3. `amnewinstanceforWS61` 파일에서 `DEPLOY_LEVEL` 변수를 **제거 (구성 해제)** 작업에 대해 설명한 값 중 하나로 설정합니다. 예를 들어, 전체 설치를 제거하거나 구성 해제하려면 `DEPLOY_LEVEL=11` 로 설정합니다.
4. 편집된 입력 파일을 지정하여 `amconfig` 스크립트를 실행합니다. 예를 들어, Solaris 시스템에서는 다음과 같이 합니다.

```
cd AccessManager-base/SUNWam/bin/  
./amconfig -s /unconfigure/aminstanceforWS61
```

-s 옵션은 스크립트를 자동 모드로 실행합니다. `amconfig` 스크립트는 `amnewinstanceforWS61` 파일을 읽은 다음 해당 인스턴스를 제거합니다.

웹 컨테이너 인스턴스는 나중에 다른 Access Manager 인스턴스를 재배포하는 데 사용할 수 있습니다.

모든 Access Manager 인스턴스 제거

이 시나리오는 모든 Access Manager 2005Q1 인스턴스와 패키지를 시스템에서 완전히 제거합니다.

컴퓨터에서 Access Manager 2005Q1 완전히 제거

1. 슈퍼유저 (루트) 로 로그인하거나 슈퍼유저가 됩니다.
2. 인스턴스를 배포하는 데 사용한 입력 파일에서 DEPLOY_LEVEL 변수를 제거 (구성 해제) 작업에 대해 설명된 값 중 하나로 설정합니다. 예를 들어, 전체 설치를 제거하거나 구성 해제하려면 DEPLOY_LEVEL=11 로 설정합니다.
3. 단계 2 에서 편집한 파일을 사용하여 amconfig 스크립트를 실행합니다. 예를 들어, Solaris 시스템에서는 다음과 같이 합니다.

```
cd AccessManager-base/SUNWam/bin/
./amconfig -s /newinstances/amnews6instance
```

amconfig 스크립트는 자동 설치 모드로 실행되어 인스턴스를 제거합니다.

Java Enterprise System 설치 프로그램을 사용하여 설치한 첫 번째 인스턴스를 제외하고 제거하려는 다른 Access Manager 인스턴스에 대해 이러한 단계를 반복합니다.

4. 첫 번째 인스턴스를 제거하고 모든 Access Manager 패키지를 시스템에서 제거하려면 Java Enterprise System 제거 프로그램을 실행합니다. 제거 프로그램에 대한 내용은 *Sun Java Enterprise System 설치 설명서*를 참조하십시오.

SSL 모드에서 Access Manager 구성

단순 인증에서 SSL(Secure Socket Layer) 을 사용하면 기밀성과 데이터 무결성이 보장됩니다 . Access Manager 를 SSL 모드에서 사용하려면 일반적으로 다음을 수행해야 합니다 .

1. 보안 웹 컨테이너를 사용하여 Access Manager 구성
2. Access Manager 를 보안 Directory Server 로 구성

다음 절에서 설명할 단계는 아래와 같습니다 .

- 54 페이지의 " 보안 Sun Java System Web Server 를 사용하여 Access Manager 구성 "
- 57 페이지의 " 보안 Sun Java System Application Server 를 사용하여 Access Manager 구성 "
- 62 페이지의 " 보안 BEA WebLogic Server 로 AMSDK 구성 "
- 65 페이지의 " 보안 IBM WebSphere Application Server 로 AMSDK 구성 "
- 66 페이지의 "SSL 모드에서 Access Manager 를 Directory Server 로 구성 "

보안 Sun Java System Web Server 를 사용하여 Access Manager 구성

Sun Java System Web Server 를 사용하여 SSL 모드에서 Access Manager 를 구성하려면 다음 단계를 참조하십시오 .

1. Access Manager 콘솔에서 서비스 구성 모듈로 이동하여 플랫폼 서비스를 선택합니다 . 서버 목록 속성에서 `http://` 프로토콜을 제거하고 `https://` 프로토콜을 추가합니다 . 저장을 누릅니다 .

주 저장을 눌러야 합니다 . 저장을 누르지 않더라도 다음 단계를 계속할 수 있지만 모든 구성 변경 내용이 손실되며 관리자로 로그인하여 해당 문제를 해결할 수 없습니다 .

단계 2 부터 단계 25까지는 Sun Java System Web Server 에 대한 설명입니다 .

2. WebServer 콘솔에 로그인합니다 . 기본 포트는 58888 입니다 .
3. Access Manager 가 실행 중인 Web Server 인스턴스를 선택하고 Manage(관리) 를 누릅니다 .
구성이 변경되었다는 메시지가 있는 팝업 창이 표시됩니다 . OK(확인) 를 누릅니다 .
4. 화면의 오른쪽 위 모서리에 있는 Apply(적용) 버튼을 누릅니다 .
5. Apply Settings(설정 적용) 를 누릅니다 .
Web Server 가 자동으로 다시 시작되어야 합니다 . 확인을 눌러 계속합니다 .
6. Web Server 인스턴스 선택을 중지합니다 .
7. Security Tab(보안탭) 을 누릅니다 .
8. Create Database(데이터베이스 만들기) 를 누릅니다 .
9. 새 데이터베이스 비밀번호를 입력하고 확인을 누릅니다 .
나중에 사용할 수 있도록 데이터베이스 비밀번호를 기록해 두십시오 .
10. 인증서 데이터베이스를 작성한 후 Request a Certificate(인증서 요청) 을 누릅니다 .

- 11.** 화면에 제공된 필드에 데이터를 입력합니다.

키 쌍 필드 비밀번호 필드는 **단계 9**에 입력한 것과 동일합니다. 위치 필드에 위치를 정확하게 입력해야 합니다. CA 와 같은 약어는 사용할 수 없습니다. 모든 필드를 정의해야 합니다. 공통 이름 필드에 Web Server 의 호스트 이름을 입력합니다.

- 12.** 양식이 제출되면 다음과 같은 메시지가 표시됩니다.

```
--BEGIN CERTIFICATE REQUEST--
afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdfasdf
alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwferoiqeroijeprwprwl
--END CERTIFICATE REQUEST--
```

- 13.** 이 텍스트를 복사하여 인증서를 요청할 때 제출합니다.

루트 CA 인증서를 가져와야 합니다.

- 14.** 인증서가 포함된 다음과 같은 인증서 응답을 받게 됩니다.

```
--BEGIN CERTIFICATE--
afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdfasdf
alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwferoiqeroijeprwprwl
--END CERTIFICATE--
```

- 15.** 이 텍스트를 클립보드에 복사하거나 텍스트를 파일로 저장합니다.

- 16.** Web Server 콘솔로 이동하여 Install Certificate(인증서 설치) 를 누릅니다.

- 17.** 이 서버의 인증서를 클릭합니다.

- 18.** 키 쌍 파일 비밀번호 필드에 인증서 데이터베이스 비밀번호를 입력합니다.

19. 인증서를 제공된 텍스트 필드에 붙여 넣거나 라디오 버튼을 누르고 텍스트 상자에 파일 이름을 입력합니다. 제출을 클릭합니다.
브라우저에 인증서가 표시되고 인증서를 추가하기 위한 버튼이 제공됩니다.
20. 인증서 설치를 클릭합니다.
21. 신뢰할 수 있는 인증 기관에 대한 인증서를 누릅니다.
22. 단계 16 부터 단계 21 까지 설명된 것과 동일한 방법으로 루트 CA 인증서를 설치합니다.
23. 두 인증서가 모두 설치되면 Web Server 콘솔의 Preferences tab(기본 설정 탭)을 누릅니다.
24. SSL 을 다른 포트에서 사용 가능하게 하려면 수신 소켓 추가를 선택합니다. 그런 다음 Edit Listen Socket(수신 소켓 편집) 을 선택합니다.
25. 보안 상태를 사용 불가능에서 사용 가능으로 변경하고 OK(확인)를 눌러 변경 내용을 제출합니다.

단계 26 부터 단계 28 까지는 Access Manager 를 설명합니다.

26. AMConfig.properties 파일을 엽니다. 기본적으로 이 파일의 위치는 /etc/opt/SUNWam/config 입니다.
27. Web Server 인스턴스 디렉토리를 제외하고 http:// 의 모든 프로토콜 항목을 https:// 로 교체합니다. Web Server 인스턴스 디렉토리도 AMConfig.properties 에 지정되어 있지만 그대로 유지되어야 합니다.
28. AMConfig.properties 파일을 저장합니다.
29. Web Server 콘솔에서 Web Server 인스턴스를 호스트하는 Access Manager에 대한 ON/OFF(설정 / 해제) 버튼을 누릅니다.
Web Server 의 Start/Stop(시작 / 중지) 페이지에 입력란이 표시됩니다.
30. 텍스트 필드에 인증서 데이터베이스 비밀번호를 입력하고 시작을 선택합니다.

보안 Sun Java System Application Server 를 사용하여 Access Manager 구성

SSL 사용 가능 Sun Java System Application Server 에서 실행하도록 Access Manager 를 설정하려면 두 단계를 거칩니다 . 먼저 설치된 Access Manager 에 대한 Application Server 인스턴스에 보안을 설정한 다음 Access Manager 를 구성합니다 .

SSL 을 사용하여 Application Server 6.2 설정

Application Server 인스턴스에 보안을 설정하려면 다음을 수행합니다 .

1. 브라우저에 다음 주소를 입력하여 Sun Java System Application Server 콘솔에 관리자로 로그인합니다 .
`http://fullservername:port`
기본 포트는 4848 입니다 .
2. 설치하는 동안 입력한 아이디와 비밀번호를 입력합니다 .
3. Access Manager 를 설치했거나 설치할 Application Server 인스턴스를 선택합니다 . 오른쪽 프레임에 구성이 변경되었다는 메시지가 표시됩니다 .
4. 변경 내용 적용을 클릭합니다 .
5. 재시작을 클릭합니다 . Application Server 가 자동으로 다시 시작되어야 합니다 .
6. 왼쪽 프레임에서 보안을 누릅니다 .
7. 데이터베이스 관리 탭을 누릅니다 .
8. 데이터베이스 만들기를 누릅니다 (선택하지 않은 경우) .
9. 새 데이터베이스 비밀번호를 입력하고 확인한 다음 확인 버튼을 누릅니다 . 나중에 사용할 수 있도록 데이터베이스 비밀번호를 기록해 두십시오 .
10. 인증서 데이터베이스를 작성한 후 인증서 관리 탭을 누릅니다 .
11. 요청 링크를 누릅니다 (선택하지 않은 경우) .

12. 인증서에 대해 다음 요청 데이터를 입력합니다.

- a. 새 인증서인지 인증서 업데이트인지를 선택합니다. 특정 기간이 경과하면 많은 인증서가 만료되고 일부 인증 기관 (CA) 에서는 업데이트 알림을 자동으로 보냅니다.
- b. 인증서에 대한 요청을 제출할 방법을 지정합니다.

CA 가 전자 메일 메시지로 요청을 받는 경우 CA 전자 메일을 선택하고 CA 의 전자 메일 주소를 입력합니다. CA 목록에서 사용 가능한 인증 기관 목록을 누릅니다.

Sun Java System Certificate Server 를 사용하는 내부 CA 로부터 인증서를 요청할 경우 CA URL 을 누르고 Certificate Server 에 대한 URL 을 입력합니다. 이 URL 은 인증서 요청을 처리하는 인증서 서버의 프로그램을 가리켜야 합니다.

- c. 키 쌍 파일에 대한 비밀번호 (단계 9 에서 지정한 비밀번호) 를 입력합니다.
- d. 다음 식별 정보를 입력합니다.

공통 이름. 포트 번호를 포함하여 서버의 성명입니다.

요청자 이름. 요청자의 이름입니다.

전화 번호. 요청자의 전화 번호입니다.

공통 이름. 디지털 인증서를 설치할 Sun Java System Application Server 의 정규화된 이름입니다.

전자 메일 주소. 관리자의 전자 메일 주소입니다.

조직 이름. 조직의 이름입니다. 인증 기관은 이 조직에 등록된 도메인에 속하는 이 속성에 입력된 호스트 이름을 요구할 수 있습니다.

조직 구성 단위 이름. 과, 부서 및 기타 조직 운영 단위의 이름입니다.

구/군/시 이름. 사용자의 구 / 군 / 시 이름입니다.

시/도 이름. 조직이 미국 또는 캐나다에 있는 경우 각각 조직이 운영되는 시 또는 도의 이름입니다. 약어를 사용하지 마십시오.

국가 코드. 국가에 대한 2 문자 ISO 코드입니다. 예를 들어, 미국의 국가 코드는 us 입니다.

13. 확인 버튼을 누릅니다. 메시지가 표시됩니다. 예를 들면 다음과 같습니다.

```
--BEGIN NEW CERTIFICATE REQUEST--

afajsdllwqeroisdaoi234r1kqwelkasjlasnvdknbslajowijalsdkjfalsdflla

alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwepwoiqreroijepwprfwl

--END NEW CERTIFICATE REQUEST--
```

14. 이 텍스트를 모두 파일에 복사하고 확인을 누릅니다. 루트 CA 인증서를 가져와야 합니다.
15. CA를 선택하고 해당 기관의 웹 사이트 지시에 따라 디지털 인증서를 가져옵니다. CMS, Verisign 또는 Entrust.net 에서 인증서를 가져올 수 있습니다.
16. 인증 기관으로부터 디지털 인증서를 받은 후 텍스트를 클립보드에 복사하거나 파일로 저장할 수 있습니다.
17. Sun Java System Application Server 콘솔로 이동하여 설치 링크를 누릅니다.
18. 이 서버에 대한 인증서를 선택합니다.
19. 키 쌍 파일 비밀번호 필드에 인증서 데이터베이스 비밀번호를 입력합니다 (단계 9 에 입력한 비밀번호).
20. 인증서를 제공된 텍스트 필드인 메시지 텍스트 (헤더 있음) 에 붙여 넣거나 이 파일 입력란에 있는 메시지에 파일 이름을 입력합니다. 해당 라디오 버튼을 선택합니다.
21. 확인 버튼을 누릅니다. 브라우저에 인증서가 표시되고 인증서를 추가할 수 있는 버튼이 제공됩니다.
22. 서버 인증서 추가를 누릅니다.
23. 단계 10 부터 단계 22 까지 설명된 것과 동일한 방법으로 루트 CA 인증서를 설치합니다. 그러나 단계 18 에서는 신뢰할 수 있는 인증 기관에 대한 인증서를 선택합니다.
24. 인증서 설치가 완료된 경우 왼쪽 프레임에서 HTTP Server 노드를 확장합니다.
25. HTTP Server 에서 HTTP Listeners 를 선택합니다.
26. http-listener-1 을 선택합니다. 브라우저에 소켓 정보가 표시됩니다.

27. http-listener-1 에 사용되는 포트 값을 응용 프로그램 서버를 설치하는 동안 입력한 값에서 해당 값 (예 : 443) 으로 변경합니다 .
28. SSL/TLS 사용 기능을 선택합니다 .
29. 인증서 별명을 선택합니다 .
30. 반환 서버를 지정합니다 . 이 이름은 단계 12에 지정된 공통 이름과 일치해야 합니다 .
31. 저장을 누릅니다 .
32. Sun Java System Access Manager 소프트웨어를 설치할 Application Server 인스턴스를 선택합니다 . 오른쪽 프레임에 구성이 변경되었다는 메시지가 표시됩니다 .
33. 변경 내용 적용을 클릭합니다 .
34. 재시작을 클릭합니다 . 응용프로그램 서버가 자동으로 다시 시작됩니다 .

SSL 을 사용하여 Application Server 8.1 설정

Application Server 인스턴스에 보안을 설정하려면 다음을 수행합니다 .

1. Application Server 인스턴스가 중지되었는지 확인합니다 .
2. asadmin>change-master-password 명령을 사용하여 토큰 비밀번호를 변경합니다 .
3. Application Server 콘솔로 이동하여 구성> HTTP 서비스> HTTP Listeners를 선택합니다 .
4. 사용할 수신기를 누르고 오른쪽 창에서 Security:Enabled 를 선택합니다 .
5. certutil 이 설치되어 있는지 확인합니다 .
 - a. /usr/sfw/bin 으로 이동합니다 .
 - b. 설치되어 있지 않으면 다음 디렉토리에서 SUNWt1su 패키지를 설치합니다 .
/share/builds/integration/security/SECURITY_3_9_3_03B4/packages/
~platform~
 - c. 셸 환경 변수 LD_LIBRARY_PATH
LD_LIBRARY_PATH has to have /usr/lib/mps/secv1

6. certutil 을 사용하여 certdb 에 설치된 인증서를 확인합니다.
 - a. /var/opt/SUNWappserver/domains/domain1/config 로 이동합니다.
 - b. certutil -L -d
 - c. 다음 출력이 나타납니다.


```
/var/opt/SUNWappserver/domains/domain1/config/% certutil -L -d
```

Application Server 8.1 은 설치 시 자체 서명된 서버 인증서 (별명 slas) 를 설치하고 ssl 사용 포트 4848, 8181 에 이를 사용합니다.
7. 인증서 요청을 생성합니다. 구문은 다음과 같습니다.


```
certutil -R -s subj -o cert-request-file [-d certdir] [-P dbprefix] [-p phone] [-a]
```

예를 들면 다음과 같습니다.

```
certutil -R -s "CN=test.company1.com, O=company1.com, C=US" -o cert.req -d . -a
```
8. 다음 명령을 사용하여 CA 로부터 인증서를 검색합니다.


```
certutil -A -n cert-name -t trustargs [-d certdir] [-P dbprefix] [-a] [-i input]
```
9. 서버 인증서를 파일로 저장합니다.
10. 다음 명령 구문을 사용하여 신뢰할 수 있는 CA 인증서를 설치합니다.


```
certutil -A -n cert-name -t trustargs [-d certdir] [-P dbprefix] [-a] [-i input]
```

신뢰할 수 있는 CA 인증서를 파일 (예 : cacert.txt) 로 저장합니다.
11. certdb 를 나열하여 설치가 성공했는지 확인합니다. 다음 명령을 입력합니다.


```
/var/opt/SUNWappserver/domains/domain1/config/% certutil -L -d
```
12. Application Server 관리 콘솔로 이동하여 HTTP Listeners 를 선택합니다. 일반 설정에서 새 서버 인증서로 HTTP Listener 를 구성합니다.
13. Application Server 를 다시 시작합니다.

SSL 모드에서 Access Manager 구성

SSL 모드에서 Access Manager 를 구성하려면 다음을 수행합니다 .

1. Access Manager 콘솔에서 서비스 구성 모듈로 이동하여 플랫폼 서비스를 선택합니다 . 서버 목록 속성에서 HTTPS 프로토콜과 동일한 URL 및 SSL 사용 가능 포트 번호를 추가합니다 . 저장을 누릅니다 .

주 단일 Access Manager 인스턴스가 HTTP 와 HTTPS 각각 하나씩 두 개의 포트를 수신하고 있고 쿠키를 사용하여 Access Manager 에 액세스하려고 시도할 경우 Access Manager 는 응답하지 않는 상태가 됩니다 . 이러한 구성은 지원되지 않습니다 .

2. 다음 기본 위치에서 `AMConfig.properties` 파일을 엽니다 .
`/etc/opt/SUNWam/config`
3. `http://`의 모든 프로토콜 항목을 `https://`로 교체하고 포트 번호를 SSL 사용 가능 포트 번호로 변경합니다 .
4. `AMConfig.properties` 파일을 저장합니다 .
5. Application Server 를 다시 시작합니다 .

보안 BEA WebLogic Server 로 AMSDK 구성

SSL 에서 AMSDK 로 BEA WebLogic Server 를 구성하기 전에 먼저 웹 컨테이너로서 BEA WebLogic Server 를 설치해야 합니다 . 설치 지침을 보려면 BEA WebLogic Server 설명서를 참조하십시오 . Access Manager 에 대한 웹 컨테이너로서 WebLogic 을 구성하려면 1 장 , 31 페이지의 "Access Manager 2005Q1 구성 스크립트" 를 참조하십시오 .

보안 WebLogic 인스턴스를 구성하려면 다음을 수행합니다 .

1. 즉석 시동 메뉴를 사용하여 도메인을 만듭니다 .
2. WebLogic 설치 디렉토리로 이동하여 인증서 요청을 생성합니다 .
3. `vetri_csr.txt` CSR 을 사용하여 이 서버 인증서를 CA 에 제출합니다 .

4. 승인된 인증서를 텍스트 파일로 저장합니다. 예를 들면 `approvedcert.txt` 입니다.
5. 다음 명령을 사용하여 루트 CA 를 `cacerts` 에 로드합니다.

```
cd jdk141_03/jre/lib/security/

jdk141_03/jre/bin/keytool -keystore cacerts -keyalg RSA -import
-trustcacerts -alias "Greenday CA" -storepass changeit -file
/opt/boa81/cacert.txt
```
6. 다음 명령을 사용하여 서버 인증서를 로드합니다.

```
jdk141_03/jre/bin/keytool -import -keystore keystore -keyalg RSA
-import -trustcacerts -file approvedcert.txt -alias "mykey"
```
7. 사용자 이름과 비밀번호를 사용하여 WebLogic 콘솔에 로그인합니다.
8. 다음 위치로 이동합니다.

```
yourdomain> Servers> myserver> Configure Keystores
```
9. 사용자 정의 ID 를 선택한 다음 Java Standard Trust 를 선택합니다.
10. 키 저장소 위치를 입력합니다. 예를 들면 `/opt/boa81/keystore` 입니다.
11. 키 저장소 비밀번호와 키 저장소 비밀 문구를 입력합니다. 예를 들면 다음과 같습니다.

```
키 저장소 비밀번호: JKS/Java Standard Trust(WL 8.1 의 경우 JKS 만 사용)
키 저장소 비밀 문구: changeit
```
12. 이 단계에서는 SSL 개인 키 설정 개인 키 별칭: `mykey` 및 비밀번호: `secret12`를 검토합니다.

주 가장 강도가 높은 SSL 라이선스를 사용해야 합니다. 그렇지 않으면 SSL 시작이 실패합니다.

13. Access Manager의 경우 설치 시 `AmConfig.properties`의 다음 매개 변수가 자동으로 구성됩니다. 자동 구성되지 않을 경우에는 사용자가 적절하게 편집할 수 있습니다.

```
com.sun.identity.jss.donotInstallAtHighestPriority=true [ this is not
required for AM 6.3 and above]
```

```
com.ipanet.security.SecureRandomFactoryImpl=com.ipanet.am.util.Secure
RandomFactoryImpl
```

```
com.ipanet.security.SSLSocketFactoryImpl=netscape.ldap.factory.JSSESoc
ketFactory
```

```
com.ipanet.security.encryptor=com.ipanet.services.util.JCEEncryption2
```

JDK 경로가 다음과 같은 경우

```
com.ipanet.am.jdk.path=/usr/jdk/entsys-j2se
```

키 도구 유틸리티를 사용하여 루트 CA 를 인증서 데이터베이스로 가져와야 합니다. 예를 들면 다음과 같습니다.

```
/usr/jdk/entsys-j2se/jre/lib/security
```

```
/usr/jdk/entsys-j2se/jre/bin/keytool -keystore cacerts -keyalg RSA
-import -trustcacerts -alias "machinename" -storepass changeit -file
```

```
/opt/bea81/cacert.txt
```

키 도구 유틸리티는 다음 디렉토리에 있습니다.

```
/usr/jdk/entsys-j2se/jre/bin/keytool
```

14. Access Manager `amadmin` 명령줄 유틸리티에서 `-D"java.protocol.handler.pkgs=com.ipanet.services.comm"` 을 제거합니다.
15. SSL 모드에서 Access Manager 를 구성합니다. 세부 사항에 대해서는 [62 페이지](#)의 "SSL 모드에서 Access Manager 구성" 을 참조하십시오.

보안 IBM WebSphere Application Server 로 AMSDK 구성

SSL 에서 AMSDK 를 사용하여 IBM WebSphere Server 를 구성하기 전에 먼저 IBM WebSphere Server 를 설치하고 웹 컨테이너로서 구성해야 합니다 . 자세한 내용은 WebSphere Server 설명서를 참조하십시오 . Access Manager 의 웹 컨테이너로서 WebLogic 를 구성하려면 1 장 , 31 페이지의 "Access Manager 2005Q1 구성 스크립트 " 를 참조하십시오 .

보안 WebSphere 인스턴스를 구성하려면 다음을 수행합니다 .

1. Websphere /bin 디렉토리에 있는 ikeyman.sh 를 시작합니다 .
2. 서명자 메뉴에서 인증 기관 (CA) 의 인증서를 가져옵니다 .
3. 개인 인증서 메뉴에서 CSR 을 생성합니다 .
4. 이전 단계에서 만든 인증서를 검토합니다 .
5. 개인 인증서를 선택하고 서버 인증서를 가져옵니다 .
6. WebSphere 콘솔에서 기본 SSL 설정을 바꾸고 암호화를 선택합니다 .
7. 기본 IBMJSSE SSL 공급자를 설정합니다 .
8. 다음 명령을 입력하여 방금 만든 파일에서 CA 인증서를 응용 프로그램 서버 JVM 키 저장소로 가져옵니다 .


```
$ appserver_root-dir/java/bin/ keytool -import -trustcacerts
-alias cmscacert -keystore ../jre/lib/security/cacerts -file
/full_path_cacert_filename.txt
```

app-server-root-dir 는 응용 프로그램 서버의 루트 디렉토리이며 *full_path_cacert_filename.txt* 는 인증서가 있는 파일의 전체 경로입니다 .
9. Access Manager 에서 JSSE 를 사용하도록 AmConfig.properties 의 다음 매개 변수를 업데이트합니다 .

```
com.sun.identity.jss.donotInstallAtHighestPriority=true
```

```
com.iplanet.security.SecureRandomFactoryImpl=com.iplanet.am.util.SecureRandomFactoryImpl
```

```
com.iplanet.security.SSLSocketFactorImpl=netscape.ldap.factory.JSSESocketFactory
```

```
com.iplanet.security.encryptor=com.iplanet.services.unil.JCEEncryption
```

10. SSL 모드에서 Access Manager 를 구성합니다 . 세부 사항에 대해서는 62 페이지의 "SSL 모드에서 Access Manager 구성 " 을 참조하십시오 .

SSL 모드에서 Access Manager 를 Directory Server 로 구성

네트워크를 통한 보안 통신을 제공하기 위해 Access Manager 에는 LDAPS 통신 프로토콜이 포함되어 있습니다. LDAPS 는 표준 LDAP 프로토콜이지만 SSL(Secure Sockets Layer) 의 상위에서 실행됩니다. SSL 통신을 사용하려면 먼저 Directory Server 를 SSL 모드에서 구성한 다음 Access Manager 를 Directory Server 로 연결합니다. 기본적인 단계는 다음과 같습니다.

1. Directory Server 의 인증서를 구하여 설치하고 인증 기관 (CA) 의 인증서를 신뢰하도록 Directory Server 를 구성합니다.
2. 디렉토리에서 SSL 을 활성화합니다.
3. 인증, 정책 및 플랫폼 서비스를 구성하여 SSL 사용 Directory Server 로 연결합니다.
4. Access Manager 를 Directory Server 백엔드에 안전하게 연결되도록 구성합니다.

SSL 모드에서 Directory Server 구성

Directory Server 를 SSL 모드에서 구성하려면 서버 인증서를 구하여 설치하고 인증 기관의 인증서를 신뢰하도록 Directory Server 를 구성한 다음 SSL 을 활성화해야 합니다. 자세한 내용은 *Directory Server 관리 설명서*의 11 장 "인증 및 암호화 관리" 에 있습니다. 이 문서는 다음 위치에 있습니다.

<http://docs.sun.com/doc/819-2012>

또한 다음 위치에서 PDF 형태의 설명서를 다운로드할 수 있습니다.

http://docs.sun.com/coll/DirectoryServer_04q2 및
http://docs.sun.com/coll/DirectoryServer_04q2?l=ko

Directory Server 가 이미 SSL 사용 가능 상태이면 Access Manager 를 Directory Server 로 연결하는 방법을 자세히 설명하는 다음 절로 이동합니다.

Access Manager 를 SSL 사용 Directory Server 로 연결

일단 SSL 모드로 Directory Server 가 구성된 다음에는 Access Manager 를 Directory Server 백엔드로 연결해야 합니다. 수행 방법은 다음과 같습니다.

1. Access Manager 콘솔에서 서비스 구성 모듈의 LDAP 인증 서비스로 이동합니다.
 - a. Directory Server 포트를 SSL 포트로 변경합니다.
 - b. LDAP 서버에 대한 SSL 액세스 가능 속성을 선택합니다.
2. 서비스 구성 모듈의 구성원 인증 서비스로 이동합니다.
 - a. Directory Server 포트를 SSL 포트로 변경합니다.
 - b. LDAP 서버에 대한 SSL 액세스 가능 속성을 선택합니다.
3. 서비스 구성에 있는 정책 구성 서비스로 이동합니다.
 - a. Directory Server 포트를 SSL 포트로 변경합니다.
 - b. LDAP 서버에 대한 SSL 액세스 가능 속성을 선택합니다.
4. 텍스트 편집기에서 `serverconfig.xml` 파일을 엽니다. 이 파일은 다음 위치에 있습니다.


```
/etc/opt/SUNWam/config
```

 - a. <Server> 요소에서 다음 값을 변경합니다.
 - port - Access Manager가 수신하는 보안 포트의 포트 번호를 입력합니다(기본값 : 636).
 - type- SIMPLE 을 SSL 로 변경합니다.
 - b. `serverconfig.xml` 파일을 저장한 다음 닫습니다.
5. 다음 기본 위치에서 `AMConfig.properties` 파일을 엽니다.


```
AcessManager-base/SUNWam/config
```

 다음 등록 정보를 변경합니다.
 - a. Directory Port = 636(기본값을 사용할 경우)
 - b. `ssl.enabled = true`
 - c. `AMConfig.properties` 를 저장합니다.
6. 서버를 다시 시작합니다.

SSL 모드에서 Access Manager 를 Directory Server 로 구성

콘솔을 통한 Access Manager 관리

*Sun Java™ System Access Manager 6 2005Q1 관리 설명서*의 2 부입니다. 여기에서는 Access Manager 그래픽 사용자 인터페이스와 항목 이동 방법을 설명하며 이 부분은 다음 내용으로 구성되어 있습니다.

- 71 페이지의 "Identity 관리 "
- 101 페이지의 " 현재 세션 "
- 105 페이지의 " 정책 관리 "
- 131 페이지의 " 인증 관리 "
- 175 페이지의 " 인증 옵션 "
- 207 페이지의 " 비밀번호 재설정 서비스 "

Identity 관리

이 장에서는 Sun Java™ System Access Manager 6 2005Q1 의 아이디 관리 기능에 대해 설명합니다. Identity 관리 모듈 인터페이스를 사용하면 모든 Access Manager 객체와 아이디를 보고, 관리하고, 구성할 수 있습니다. 이번 장은 다음 절로 구성됩니다.

- 71 페이지의 "Access Manager 콘솔 "
- 74 페이지의 "Identity 관리 인터페이스 "
- 74 페이지의 "Access Manager 객체 관리 "

Access Manager 콘솔

Access Manager 콘솔은 위치 창, 이동 창, 데이터 창의 세 섹션으로 구분됩니다. 관리자는 세 창을 모두 사용하여 디렉토리를 이동하고, 사용자 및 서비스 구성을 수행하고, 정책을 만들 수 있습니다.

헤더 창

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

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

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

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

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

도움말 링크는 이 설명서 [속성 참조 설명서](#)의 아이디 관리, 현재 세션, 연합 관리 및 4부에 대한 정보가 포함된 브라우저 창을 엽니다.

로그아웃 링크를 사용하여 Access Manager 에서 로그아웃할 수 있습니다.

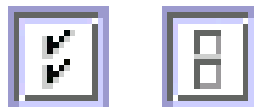
탐색 표시 영역

이동 창은 Access Manager 콘솔의 왼쪽 부분입니다. *디렉토리 객체* 부분 (회색 상자 내)에는 현재 열려 있는 디렉토리 객체의 이름과 해당 *등록 정보* 링크가 표시됩니다. 이동 창에 표시되는 대부분의 객체에는 해당 *등록 정보* 링크가 있습니다. 이 링크를 선택하면 오른쪽의 데이터 창에 항목의 속성이 표시됩니다. 보기 메뉴는 선택한 디렉토리 객체 아래에 있는 디렉토리를 나열합니다. 하위 디렉토리의 수에 따라 페이지 매김 메커니즘이 결정됩니다.

데이터 표시 영역

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

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



Access Manager 그래픽 사용자 인터페이스에는 두 가지 기본 보기가 있습니다. 로그인하는 사용자의 역할에 따라 Identity 관리 보기 또는 사용자 프로필 보기에 액세스할 수 있습니다.

Identity 관리 보기

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

사용자 프로필 보기

관리 역할이 할당되지 않은 사용자가 Access Manager 에 대해 인증을 수행할 때는 사용자 자신의 사용자 프로필이 기본 보기가 됩니다. 이 보기에서 사용자는 개인 프로필 특성의 속성 값을 수정할 수 있습니다. 여기에는 이름, 주소 (집), 비밀번호 등이 포함될 수 있지만 이에 제한되지는 않습니다. 사용자 프로필 보기에 표시되는 속성은 확장할 수 있습니다. 객체 및 아이디에 대한 사용자 정의된 속성을 추가하는 방법에 대한 자세한 내용은 *Access Manager Developer's Guide* 를 참조하십시오.

등록 정보 기능

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

항목의 등록 정보를 확장하는 방법은 *Access Manager Developer's Guide* 를 참조하십시오.

Identity 관리 인터페이스

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

Access Manager 객체 관리

사용자 관리 인터페이스에는 Access Manager 객체 (조직, 그룹, 사용자, 서비스, 역할, 정책, 컨테이너 객체, 에이전트)를 보거나 관리하는 데 필요한 모든 구성 요소가 포함되어 있습니다. 이 절에서는 객체 유형과 객체 유형을 구성하는 방법에 대해 설명합니다.

대부분의 Access Manager 객체 유형에서는 표시 옵션과 사용 가능한 작업을 선택적으로 구성함으로써 Access Manager 콘솔에 웹 인터페이스가 표시되는 방법을 표시하거나 숨길 수 있습니다. 구성은 조직 및 역할 수준에서 이루어지며 사용자는 자신이 상주하며 역할이 지정된 조직으로부터 구성을 상속합니다. 이 설정에 대해서는 이 장의 끝에서 설명합니다.

조직

조직은 기업에서 부서와 자원을 관리하는 데 사용되는 최상위 수준의 계층 구조를 나타냅니다. 설치 시 Access Manager는 Access Manager 엔터프라이즈 구성을 관리하기 위해 최상위 수준 조직 (설치하는 동안 정의됨)을 동적으로 만듭니다. 설치 후에 추가 조직을 만들어 별도 엔터프라이즈를 관리할 수 있습니다. 생성되는 모든 조직은 최상위 조직 아래에 놓입니다.

조직 만들기

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

3. 필드에 대한 값을 입력합니다. 이름 필드만 필수입니다. 필드는 다음과 같습니다.

이름. 조직의 이름 값을 입력합니다.

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

조직 상태. 활성 또는 비활성 상태를 선택합니다.

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

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

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

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

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

조직 별칭 이름은 조직 전체에서 고유해야 합니다. 고유 속성 목록을 사용하여 고유성을 강제로 적용할 수 있습니다.

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

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

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

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

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

```
PreferredDomain, AssociatedDomain
```

PreferredDomain 이 특정 사용자에게 대한 <http://www.example.com> 으로 정의 되는 경우 전체 섹트로 구분된 목록이 해당 URL에 대한 고유성으로 정의됩니다.

고유성은 모든 하위 조직에 적용됩니다 .

4. 확인을 누릅니다 .

새 조직이 이동 창에 표시됩니다 . 조직을 만드는 동안에 정의한 등록 정보를 편집하려면 편집할 조직의 등록 정보 화살표를 누르고 데이터 창의 보기 메뉴에서 일반을 선택한 다음 등록 정보를 편집하고 확인을 누릅니다 . [디스플레이 옵션](#) 및 [사용 가능한 작업](#) 보기를 사용하여 Access Manager 콘솔의 모양을 사용자 정의 하고 이 조직에 대해 인증된 모든 사용자의 동작을 지정할 수 있습니다 .

조직 삭제

1. Identity 관리의 보기 메뉴에서 조직을 선택합니다 .

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

2. 삭제할 조직의 이름 옆에 있는 확인란을 선택합니다 .

3. 삭제를 누릅니다 .

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

정책에 조직 추가

Access Manager 객체는 정책의 주제 정의를 통해 정책에 추가됩니다 . 정책을 작성하거나 수정할 때 정책의 주제 페이지에서 조직 , 역할 , 그룹 및 사용자를 주제로 정의할 수 있습니다 . 주제가 정의되고 나면 정책이 객체에 적용됩니다 . 세부 사항에 대해서는 [120 페이지의 "정책 관리"](#) 를 참조하십시오 .

그룹

그룹은 공통된 기능 , 특징 또는 관심사를 가진 사용자 모음을 나타냅니다 . 일반적으로 이 그룹에는 연관된 권한이 없습니다 . 그룹은 두 가지 수준 즉 , 조직 내에서와 다른 관리 대상 그룹 내에서 존재할 수 있습니다 . 다른 그룹 내에서 존재하는 그룹을 *하위 그룹*이라고 부릅니다 . 하위 그룹은 상위 그룹 내에서 물리적으로 존재하는 하위 노드입니다 .

Access Manager 는 또한 단일 그룹에 포함된 기존 그룹의 " 표현 " 인 **중첩 그룹**을 지원합니다. 하위 그룹과 반대로 중첩 그룹은 DIT 의 임의 위치에 존재할 수 있습니다. 중첩 그룹은 다수의 사용자에 대한 액세스 권한을 신속하게 설정할 수 있게 합니다.

그룹을 만들 경우 가입에 의한 구성원 (**정적 그룹**) 또는 필터링에 의한 구성원 (**필터링된 그룹**) 을 사용하는 그룹을 만들 수 있습니다. 이는 사용자가 그룹에 추가되는 방법을 제어합니다. 사용자는 정적 그룹에만 추가할 수 있습니다. 동적 그룹은 필터를 통해 사용자의 추가를 제어합니다. 그러나 중첩 또는 하위 그룹은 두 그룹 모두에 추가할 수 있습니다.

정적 그룹 (가입에 의한 구성원)

가입에 의한 그룹 구성원을 지정할 경우 지정된 관리 대상 그룹 유형에 기초하여 정적 그룹이 만들어집니다. 관리 대상 그룹 유형 값이 static 이면 groupOfNames 또는 groupOfUniqueNames 객체 클래스를 사용하여 그룹 구성원을 그룹 항목에 추가합니다. 관리 대상 그룹 유형 값이 dynamic 인 경우 특정 LDAP 필터를 사용하여 memberof 속성을 포함하는 사용자 항목만 검색하여 반환합니다. 세부 사항에 대해서는 [245 페이지의 " 관리 대상 그룹 유형 "](#) 을 참조하십시오.

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

필터링된 그룹 (필터링에 의한 구성원)

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

주 참조 무결성 플러그 인을 사용하도록 Directory Server 를 통해 Access Manager 를 구성해야 합니다. 참조 무결성 플러그 인을 사용 가능하게 하면 삭제 또는 이름 바꾸기 작업이 수행된 경우 지정된 속성에서 무결성 업데이트를 바로 수행합니다. 따라서 관련된 항목 간의 관계가 데이터베이스 전체에서 유지됩니다. 데이터베이스 색인은 Directory Server 에서 검색 성능을 향상시킵니다. 플러그 인 사용에 대한 자세한 내용은 [Sun Java System Access Manager Migration Guide](#) 를 참조하십시오.

정적 그룹 만들기

1. 그룹을 만들 조직, 그룹 또는 그룹 컨테이너로 이동합니다.
2. 보기 메뉴에서 그룹을 선택합니다.

3. 새로 만들기를 누릅니다.
4. 데이터 창에서 그룹 유형으로 가입에 의한 구성원을 선택합니다.
5. 이름 필드에 그룹의 이름을 입력합니다. 다음을 누릅니다.
6. 사용자가 이 그룹에 가입할 수 있음 속성을 선택하여 사용자가 그룹에 직접 가입할 수 있게 합니다.
7. DIT 에서 여러 그룹 컨테이너를 정의했고 관리 서비스에서 그룹 컨테이너 표시 속성을 사용 가능하게 하지 않은 경우 정적 그룹이 속할 상위 그룹 컨테이너를 선택할 수 있습니다. 그렇지 않은 경우에는 이 필드가 표시되지 않습니다.
8. 마침을 누릅니다.
그룹이 만들어지면 데이터 창의 보기 메뉴에서 일반을 선택하여 사용자가 이 그룹에 가입할 수 있음 속성을 편집할 수 있습니다.

정적 그룹에서 구성원 추가 또는 제거

1. 구성원을 추가할 그룹 옆에 있는 등록 정보 화살표를 누릅니다.
2. 데이터 창의 보기 메뉴에서 구성원을 선택합니다.

작업 선택 메뉴에서 수행할 작업을 선택합니다. 수행할 수 있는 작업은 다음과 같습니다.

새 사용자. 이 작업은 새 사용자를 만들며 사용자 정보를 저장할 때 사용자를 자동으로 그룹에 추가합니다.

사용자 추가. 이 작업은 기존 사용자를 그룹에 추가합니다. 이 작업을 선택할 경우 추가할 사용자를 지정하는 검색 조건을 만듭니다. 검색 조건을 생성하는 데 사용되는 필드는 ANY 또는 ALL 연산자를 사용합니다. ALL 은 지정된 모든 필드에 해당하는 사용자를 반환합니다. ALL 은 지정된 필드 중 하나 이상에 해당하는 사용자를 반환합니다. 필드를 비워두면 해당 특정 속성과 일치하는 가능한 모든 항목을 반환합니다.

검색 기준을 작성하고 나서 다음을 누릅니다. 반환된 사용자 목록에서 추가할 사용자를 선택하고 마침을 누릅니다.

팁 경로 표시 버튼을 눌러 사용자의 전체 조직 경로를 볼 수 있습니다.

그룹 추가. 이 작업은 중첩 그룹을 현재 그룹에 추가합니다. 이 작업을 선택할 경우 검색 범위와 그룹 이름 ("*" 와일드카드 사용 가능) 을 포함하는 검색 조건을 만들어 사용자가 그룹에 직접 가입할 수 있는지 여부를 지정할 수 있습니다. 정보를 입력하고 다음을 누릅니다. 반환된 그룹 목록에서 추가할 그룹을 선택하고 마침을 누릅니다.

구성원 제거. 이 작업은 그룹에서 구성원 (사용자 및 그룹 포함) 을 제거하지만 삭제하지는 않습니다. 제거할 구성원을 선택하고 사용 가능한 작업 목록에서 구성원 제거를 선택합니다.

구성원 삭제. 이 작업은 선택한 구성원을 영구적으로 삭제합니다. 삭제할 구성원을 선택하고 사용 가능한 작업 목록에서 구성원 삭제를 선택합니다.

필터링된 그룹 만들기

1. 그룹을 만들 조직 또는 그룹으로 이동합니다.
2. 보기 메뉴에서 그룹을 선택합니다.
3. 새로 만들기를 누릅니다.
4. 데이터 창에서 그룹 유형으로 필터링에 의한 구성원을 선택합니다.
5. 이름 필드에 그룹의 이름을 입력합니다. 다음을 누릅니다.
6. LDAP 검색 필터를 생성합니다.

기본적으로 Access Manager 는 기본 검색 필터 인터페이스를 표시합니다. 필터를 생성하는 데 사용되는 기본 필드는 ANY 또는 ALL 연산자를 사용합니다. ALL 은 지정된 모든 필드에 해당하는 사용자를 반환합니다. ALL 은 지정된 필드 중 하나 이상에 해당하는 사용자를 반환합니다. 필드를 비워두면 해당 특정 속성과 일치하는 가능한 모든 항목을 반환합니다.

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

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

마침을 누르면 검색 조건과 일치하는 모든 사용자가 자동으로 그룹에 추가됩니다.

필터링된 그룹에서 구성원 추가 또는 제거

1. 구성원을 추가할 그룹 옆에 있는 등록 정보 화살표를 누릅니다.

2. 데이터 창의 보기 메뉴에서 구성원을 선택합니다.

작업 선택 메뉴에서 수행할 작업을 선택합니다. 수행할 수 있는 작업은 다음과 같습니다.

그룹 추가. 이 작업은 중첩 그룹을 현재 그룹에 추가합니다. 이 작업을 선택할 경우 검색 범위와 그룹 이름 ("*" 와일드카드 사용 가능) 을 포함하는 검색 조건을 만들며 사용자가 그룹에 직접 가입할 수 있는지 여부를 지정할 수 있습니다. 정보를 입력하고 다음을 누릅니다. 반환된 그룹 목록에서 추가할 그룹을 선택하고 마침을 누릅니다.

구성원 제거. 이 작업은 그룹에서 구성원 (사용자 및 그룹 포함) 을 제거하지만 삭제하지는 않습니다. 제거할 구성원을 선택하고 사용 가능한 작업 목록에서 구성원 제거를 선택합니다.

구성원 삭제. 이 작업은 선택한 구성원을 영구적으로 삭제합니다. 삭제할 구성원을 선택하고 사용 가능한 작업 목록에서 구성원 삭제를 선택합니다.

정책에 그룹 추가

Access Manager 객체는 정책의 주제 정의를 통해 정책에 추가됩니다. 정책을 작성하거나 수정할 때 정책의 주제 페이지에서 조직, 역할, 그룹 및 사용자를 주제로 정의할 수 있습니다. 주제가 정의되고 나면 정책이 객체에 적용됩니다. 세부 사항에 대해서는 [120 페이지의 "정책 관리"](#) 를 참조하십시오.

사용자

*사용자*는 개인의 ID 를 나타냅니다. Access Manager Identity 관리 모듈을 통해 사용자를 조직, 컨테이너 및 그룹에서 만들고 삭제할 수 있으며 역할 및 / 또는 그룹에서 추가 또는 제거할 수 있습니다. 또한 서비스를 사용자에게 할당할 수도 있습니다.

주	하위 조직의 사용자가 amadmin 과 동일한 사용자 아이디를 사용하여 생성될 경우 amadmin 에 대한 로그인은 실패하게 됩니다. 그런 문제가 발생하면 관리자는 Directory Server 콘솔을 통해 사용자의 아이디를 변경해야 합니다. 이렇게 하면 관리자는 기본 조직에 로그인할 수 있습니다. 또한 인증 서비스에서 사용자 검색을 시작할 DN 을 사용자 컨테이너 DN 으로 설정하여 로그인 프로세스 도중 고유한 일치가 반환되도록 할 수 있습니다.
----------	--

사용자 만들기

1. 사용자를 만들 조직, 컨테이너 또는 사용자 컨테이너로 이동합니다.
2. 보기 메뉴에서 사용자를 선택합니다.

3. 새로 만들기를 누릅니다.

데이터 창에 새 사용자 페이지가 표시됩니다.

4. 사용자에게 사용 가능한 서비스가 있을 경우 사용 가능한 서비스 페이지에서 사용자가 등록한 서비스를 선택합니다. 이 페이지를 건너 뛰려면 다음을 누르십시오.

5. 다음 기본 필수 값에 대한 데이터를 입력합니다.

사용자 아이디. 이 필드에는 사용자가 Access Manager 에 로그인할 때 사용하는 이름을 입력합니다. 이 등록 정보는 비 DN 값입니다.

이름. 이 필드에는 사용자의 이름을 입력합니다. 이름 값과 성 값은 Access Manager 콘솔의 오른쪽 위 모서리에 있는 현재 로그인 필드의 사용자를 식별합니다. 이 값은 필수 값이 아닙니다.

성. 이 필드는 사용자의 성을 가집니다. 이름 값과 성 값은 Access Manager 콘솔의 오른쪽 위 모서리에 있는 현재 로그인 필드의 사용자를 식별합니다.

성명. 이 필드에는 사용자의 성명을 입력합니다.

비밀번호. 이 필드에는 사용자 아이디 필드에 지정된 이름의 비밀번호를 입력합니다.

비밀번호 (확인). 비밀번호를 확인합니다.

사용자 상태. 이 옵션은 사용자가 Access Manager 를 통해 인증될 수 있는지 여부를 지정합니다. 활성 사용자만 Access Manager 를 통해 인증될 수 있습니다. 기본값은 활성입니다.

6. 마침을 누릅니다.

역할 및 그룹에 사용자 추가

1. 수정할 사용자의 조직으로 이동합니다.

2. 보기 메뉴에서 사용자를 선택합니다.

3. 이동 창에서 수정할 사용자를 선택하고 등록 정보 화살표를 누릅니다.

4. 데이터 창의 보기 메뉴에서 역할 또는 그룹을 선택합니다. 이미 사용자에게 할당된 역할과 그룹만 표시됩니다. 추가를 눌러 선택할 수 있는 역할 및 그룹 목록을 표시합니다.

5. 사용자를 추가할 역할이나 그룹을 선택하고 저장을 누릅니다.

사용자에게 서비스를 추가하려면

1. 수정할 사용자의 조직으로 이동합니다.
2. 이동 창의 보기 메뉴에서 사용자를 선택합니다.
3. 이동 창에서 수정할 사용자를 선택하고 등록 정보 화살표를 누릅니다.
4. 데이터 창의 보기 메뉴에서 서비스를 선택합니다. 서비스 추가 페이지에 사용자가 사용할 수 있는 서비스 목록이 표시됩니다.
5. 사용자에게 지정할 서비스를 선택합니다.
6. 확인을 누릅니다.

서비스 속성을 편집하려면 서비스 이름 옆의 편집 링크를 누릅니다. 편집 링크는 편집할 수 있는 서비스에만 표시됩니다.

사용자 제거

1. 데이터 창의 보기 메뉴에서 역할 또는 그룹을 선택합니다.
2. 선택된 목록에서 사용자를 제거할 역할 또는 그룹을 선택한 다음 제거를 누릅니다. 또한 모두 제거를 누르면 사용자를 사용 가능한 모든 역할 및 그룹에서 제거할 수 있습니다.
3. 저장을 눌러 사용자를 제거합니다.

주 삭제 작업 전에 경고 메시지가 표시되지 않으며 삭제 작업을 실행 취소할 수도 없습니다.

정책에 사용자 추가

Access Manager 객체는 정책의 주제 정의를 통해 정책에 추가됩니다. 정책을 작성하거나 수정할 때 정책의 주제 페이지에서 조직, 역할, 그룹 및 사용자를 주제로 정의할 수 있습니다. 주제가 정의되고 나면 정책이 객체에 적용됩니다. 세부 사항에 대해서는 [120 페이지의 "정책 관리"](#)를 참조하십시오.

서비스

조직 또는 컨테이너 (컨테이너의 동작은 조직의 동작과 동일)에 대해 *서비스*를 활성화하는 과정은 두 단계로 이루어집니다. 첫 번째 단계에서는 서비스를 조직에 추가해야 합니다. 서비스를 추가한 후 해당 조직에 대해 특별히 구성된 템플릿을 구성해야 합니다. 자세한 내용은 "제 4 장, 현재 세션"을 참조하십시오.

주 우선 명령줄의 `amadmin`을 통해 새 서비스를 Access Manager로 가져와야 합니다. 서비스의 XML 스키마를 가져오는 방법에 대한 자세한 내용은 *Access Manager Developer's Guide*에서 확인할 수 있습니다.

서비스 추가

1. 서비스를 추가할 조직으로 이동합니다.
2. 보기 메뉴에서 서비스를 선택합니다.
3. 추가를 누릅니다.

이 조직에 추가할 수 있는 서비스 목록이 데이터 창에 표시됩니다.

4. 추가할 각 서비스 옆의 확인란을 선택합니다.
5. 확인을 누릅니다. 추가된 서비스가 이동 창에 표시됩니다.

주 상위 조직에 추가된 서비스만 하위 조직 수준에서 표시됩니다.

서비스의 템플릿 만들기

1. 추가된 서비스가 있는 조직이나 역할로 이동합니다.

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

2. 보기 메뉴에서 서비스를 선택합니다.
3. 활성화할 서비스 이름 옆에 있는 등록 정보 아이콘을 누릅니다.

데이터 창에 *이 서비스에 대한 템플릿이 현재 없습니다. 지금 템플릿을 만드시겠습니까?* 라는 메시지가 표시됩니다.

4. 예를 누릅니다.

이 서비스에 대해 부모 조직 또는 역할에 대한 템플릿이 만들어집니다. 데이터 창에 이 서비스의 기본 속성과 값이 표시됩니다. 기본 서비스의 속성은 [241 페이지의 "속성 참조 설명서"](#)에 설명되어 있습니다.

5. 기본값을 그대로 사용하거나 수정하고 저장을 누릅니다.

서비스 제거

1. 서비스를 제거할 조직으로 이동합니다.

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

2. 보기 메뉴에서 서비스를 선택합니다.
3. 제거할 서비스의 확인란을 선택합니다.
4. 제거를 클릭합니다.

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

역할

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

주 다른 Directory Server 역할 유형도 디렉토리 배포에 사용할 수 있지만, Access Manager 콘솔에 의해 관리되지는 않습니다. 정책의 주제 정의에 다른 Directory Server 유형을 사용할 수 있습니다. 정책 주제에 대한 자세한 내용은 [117 페이지의 "정책 만들기"](#)를 참조하십시오.

사용자는 하나 이상의 역할을 소유할 수 있습니다. 예를 들어, 세션 서비스 및 비밀번호 재설정 서비스의 속성을 갖는 계약자 역할을 만들 수 있습니다. 새 계약자가 시작되면 관리자는 계약자 항목에 개별 속성을 설정하는 대신 이 역할을 할당할 수 있습니다. 계약자가 엔지니어링 부서에서 일하며, 엔지니어링 직원이 사용할 수 있는 서비스와 액세스 권한을 요구하는 경우, 관리자는 계약자를 계약자 역할 외에 엔지니어링 역할에도 지정할 수 있습니다.

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

사용자는 관리 서비스에서 사용자 역할 표시 속성이 사용 가능하게 된 경우에만 할당된 역할을 볼 수 있습니다 . 세부 사항에 대해서는 [254 페이지의 " 사용자 프로필 페이지에 역할 표시 "](#) 를 참조하십시오 .

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

그룹과 마찬가지로 역할을 필터를 통해 만들거나 정적으로 만들 수 있습니다 .

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

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

정적 역할 만들기

1. 이동 창에서 역할을 만들 조직으로 이동합니다 .
2. 보기 메뉴에서 역할을 선택합니다 .

기본 역할 집합은 조직을 구성할 때 만들어지며 이동 창에 표시됩니다 . 기본 역할은 다음과 같습니다 .

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

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

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

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

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

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

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

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

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

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

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

3. 이동 창에서 새로 만들기를 누릅니다 . 새 역할 템플릿이 데이터 창에 나타납니다 .
4. 정적 역할을 선택하고 이름을 입력합니다 . 다음을 누릅니다 .

5. 역할에 대한 설명을 입력합니다.

6. 유형 메뉴에서 역할 유형을 선택합니다.

역할은 관리 역할 또는 서비스 역할이 될 수 있습니다. 역할 유형은 Access Manager 콘솔에서 사용자를 시작할 위치를 파악하기 위해 사용됩니다. 관리 역할은 역할 소유자가 관리 권한을 갖고 있다는 것을 콘솔에 알리고 서비스 역할은 역할 소유자가 최종 사용자라는 것을 콘솔에 알립니다.

7. 액세스 권한 메뉴에서 역할에 적용할 기본 사용 권한 집합을 선택합니다. 이러한 사용 권한은 조직 내의 항목에 대한 액세스를 제공합니다. 기본 사용 권한은 특별한 순서 없이 표시됩니다. 다음과 같은 권한이 있습니다.

사용 권한 없음. 역할에 사용 권한이 설정되지 않습니다.

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

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

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

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

8. 마침을 누릅니다.

만들어진 역할이 이동 창에 표시되고 역할에 대한 상태 정보가 데이터 창에 표시됩니다.

원하는 경우 보기 메뉴에서 표시 옵션과 사용 가능한 작업을 선택하여 구성할 수 있습니다. 자세한 내용은 이 장의 끝에 있는 [디스플레이 옵션과 사용 가능한 작업을 참조하십시오](#).

정적 역할에 사용자 추가

1. 수정할 역할을 선택하고 등록 정보 화살표를 누릅니다.

2. 데이터 창의 보기 메뉴에서 사용자를 선택합니다.

3. 추가를 누릅니다.

4. 검색 조건에 대한 정보를 입력합니다. 하나 이상의 표시된 필드에 기초하여 사용자를 검색할 수 있습니다. 이러한 필드는 다음과 같습니다.

일치. 필터에 포함할 임의의 필드에 대한 연산자를 포함할 수 있습니다. ALL 은 지정된 모든 필드에 해당하는 사용자를 반환합니다. ALL 은 지정된 필드 중 하나 이상에 해당하는 사용자를 반환합니다.

이름. 이름을 기준으로 사용자를 검색합니다.

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

사용자 아이디. 사용자 아이디를 기준으로 사용자를 검색합니다.

성. 성을 기준으로 사용자를 검색합니다.

성명. 성명을 기준으로 사용자를 검색합니다.

5. 다음을 눌러 검색을 시작합니다. 검색 결과가 표시됩니다.
6. 아이디 옆에 있는 확인란을 선택하여 반환된 이름에서 사용자를 선택합니다.
7. 마침을 누릅니다.
사용자가 이제 역할에 할당됩니다.

필터링된 역할 만들기

1. 이동 창에서 역할을 만들 조직으로 이동합니다.
2. 보기 메뉴에서 역할을 선택합니다.

기본 역할 집합은 조직을 구성할 때 만들어지며 이동 창에 표시됩니다. 기본 역할은 다음과 같습니다.

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

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

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

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

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

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

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

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

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

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

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

3. 이동 창에서 새로 만들기를 누릅니다. 새 역할 템플릿이 데이터 창에 나타납니다.
4. 필터링된 역할을 선택하고 이름을 입력합니다. 다음을 누릅니다.

5. 역할에 대한 설명을 입력합니다.
6. 유형 메뉴에서 역할 유형을 선택합니다.
역할은 관리 역할 또는 서비스 역할이 될 수 있습니다. 역할 유형은 Access Manager 콘솔에서 사용자를 시작할 위치를 파악하기 위해 사용됩니다. 관리 역할은 역할 소유자가 관리 권한을 갖고 있다는 것을 콘솔에 알리고 서비스 역할은 역할 소유자가 최종 사용자라는 것을 콘솔에 알립니다.
7. 액세스 권한 메뉴에서 역할에 적용할 기본 사용 권한 집합을 선택합니다.
8. 이러한 사용 권한은 조직 내의 항목에 대한 액세스를 제공합니다. 기본 사용 권한은 특별한 순서 없이 표시됩니다. 다음과 같은 권한이 있습니다.

사용 권한 없음. 역할에 사용 권한이 설정되지 않습니다.

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

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

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

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

9. 검색 조건에 대한 정보를 입력합니다. 필드는 다음과 같습니다.
일치. 필터에 포함할 임의의 필드에 대한 연산자를 포함할 수 있습니다. ALL은 지정된 모든 필드에 해당하는 사용자를 반환합니다. ALL은 지정된 필드 중 하나 이상에 해당하는 사용자를 반환합니다.
이름. 이름을 기준으로 사용자를 검색합니다.
사용자 상태. 상태 (활성 또는 비활성)를 기준으로 사용자를 검색합니다.
사용자 아이디. 사용자 아이디를 기준으로 사용자를 검색합니다.
성. 성을 기준으로 사용자를 검색합니다.
성명. 성명을 기준으로 사용자를 검색합니다.
또한 고급 버튼을 선택하여 필터 속성을 직접 정의할 수 있습니다. 예를 들면 다음과 같습니다.

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

필터를 비워두면 기본적으로 다음 역할이 만들어집니다.

```
(objectclass = inetorgperson)
```

역할 만들기 프로세스를 취소하려면 취소를 누릅니다.

10. 마침을 눌러 필터 조건을 기준으로 검색을 시작합니다. 필터 조건에서 정의된 사용자가 자동으로 역할에 할당됩니다.

원하는 경우 보기 메뉴에서 표시 옵션과 사용 가능한 작업을 선택하여 구성할 수 있습니다. 자세한 내용은 이 장의 끝에 있는 [디스플레이 옵션과 사용 가능한 작업](#)을 참조하십시오.

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

역할에서 사용자 제거

1. 수정할 역할을 포함하는 조직으로 이동합니다.

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

2. 보기 메뉴에서 역할을 선택합니다.
3. 수정할 역할을 선택합니다.
4. 보기 메뉴에서 사용자를 선택합니다.
5. 제거할 각 사용자 옆에 있는 확인란을 선택합니다.
6. 제거를 클릭합니다.

사용자가 이제 역할에서 제거됩니다.

정책에 역할 추가

Access Manager 객체는 정책의 주제 정의를 통해 정책에 추가됩니다. 정책을 작성하거나 수정할 때 정책의 주제 페이지에서 조직, 역할, 그룹 및 사용자를 주제로 정의할 수 있습니다. 주제가 정의되고 나면 정책이 객체에 적용됩니다. 세부 사항에 대해서는 [120 페이지의 "정책 관리"](#)를 참조하십시오.

역할에 대한 서비스 사용자 정의

역할에 사용할 수 있는 서비스를 사용자 정의하고 역할별로 서비스 속성의 액세스 수준을 사용자 정의할 수 있습니다. 속성에 대한 역할별 값을 설정하여 사용 가능한 각 서비스를 역할에 대해 사용자 정의할 수 있습니다. 또한 각 서비스와 서비스의 속성에 대해 액세스를 허용할 수 있습니다. 일부 서비스에 대해서는 특정 유형의 사용자(예: 관리자)만 액세스하도록 만들 수 있습니다. 이를 위해서 모든 사용자에게 서비스를 할당하되 특정 역할에 속하는 관리자 유형에게만 특정 서비스의 액세스 권한을 허용합니다.

동일한 논리가 서비스 속성에도 적용됩니다. 사용자의 계정은 여러 속성으로 구성되며 그 중 일부는 사용자의 액세스가 허용되지 않을 수 있습니다(예: 계정 만료 날짜). 계정의 관리자에게는 이 속성에 대한 액세스가 허용될 수 있지만 사용자(계정 소유자)는 이러한 액세스가 허용되지 않습니다. 서비스 및 속성 액세스를 사용자 정의하는 작업은 이동 창에서 역할의 서비스 보기를 통해 수행합니다.

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

서비스 구성

1. 역할의 서비스 보기에서 이 역할의 서비스 구성이라는 레이블이 붙은 섹션으로 이동합니다.
2. 서비스 이름 옆에 있는 편집 링크를 눌러 역할에 허용할 서비스를 선택합니다.
서비스 템플릿을 만들지 않은 경우 지금 만들 것인지 묻는 메시지가 나타납니다. 예를 누릅니다.
3. 서비스 속성을 수정합니다. 특정 서비스 속성에 대한 자세한 내용은 이 설명서의 3부, *속성 참조 설명서*를 참조하십시오.
4. 저장을 누릅니다.

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

속성 액세스 사용자 정의

1. 역할의 서비스 보기에서 이 역할의 서비스 액세스라는 레이블이 붙은 섹션으로 이동합니다.

2. 수정할 서비스에 대한 사용 가능 또는 사용 불가 상태를 선택합니다. 사용 가능을 선택하면 액세스 수정이 허용되고 사용 불가를 선택하면 액세스 수정이 허용되지 않습니다.
3. 액세스 수정 링크를 누릅니다.
4. 읽기 / 쓰기 또는 읽기 전용 확인란을 선택하여 액세스 수준을 속성에 할당합니다.
5. 확인을 누른 다음 저장을 누릅니다.

특정 서비스 속성에 대한 자세한 내용은 이 설명서의 4 부, [속성 참조 설명서](#)를 참조하십시오.

정책에 역할 추가

Access Manager 객체는 정책의 주제 정의를 통해 정책에 추가됩니다. 정책을 작성하거나 수정할 때 정책의 주제 페이지에서 조직, 역할, 그룹 및 사용자를 주제로 정의할 수 있습니다. 주제가 정의되고 나면 정책이 객체에 적용됩니다. 세부 사항에 대해서는 [120 페이지의 "정책 관리"](#)를 참조하십시오.

역할 삭제

1. 삭제할 역할을 포함하는 조직으로 이동합니다.
2. Identity 관리의 보기 메뉴에서 조직을 선택하고 이동 창에서 조직을 선택합니다. 위치 경로는 기본 최상위 수준 조직과 선택된 조직을 표시합니다.
3. 보기 메뉴에서 역할을 선택합니다.
4. 역할의 이름 옆에 있는 확인란을 선택합니다.
5. 삭제를 누릅니다.

정책

정책은 조직의 웹 자원을 보호하는 데 도움이 되는 규칙을 정의합니다. 정책 작성, 수정 및 삭제는 Identity 관리 모듈을 통해 수행되지만 그 절차는 [117 페이지의 "정책 만들기"](#)에 설명되어 있습니다.

에이전트

Access Manager 정책 에이전트는 웹 서버 및 웹 프록시 서버의 내용을 무단 침입으로부터 보호합니다. 정책 에이전트는 관리자가 구성한 정책에 기초하여 서비스 및 웹 자원에 대한 액세스를 제어합니다.

에이전트 객체는 정책 에이전트 프로필을 정의하고 Access Manager 자원을 보호하고 있는 특정 에이전트에 대한 인증 및 기타 프로필 정보를 Access Manager 에서 저장할 수 있게 합니다. 관리자는 Access Manager 콘솔을 통해 에이전트 프로필을 확인, 작성, 수정 및 삭제할 수 있습니다.

에이전트 만들기

1. 만들려는 에이전트를 포함하는 조직으로 이동합니다.
2. 보기 메뉴에서 에이전트를 선택합니다.
3. 새로 만들기를 누릅니다.
4. 필드에 대한 값을 입력합니다. 이름 필드만 필수입니다. 필드는 다음과 같습니다.

이름. 에이전트의 이름이나 아이디를 입력합니다. 에이전트는 Access Manager 에 로그인할 때 이 이름을 사용합니다. 멀티바이트 이름은 사용할 수 없습니다.

비밀번호. 에이전트의 비밀번호를 입력합니다. 이 비밀번호는 LDAP 인증 도중에 에이전트가 사용하는 비밀번호와 일치해야 합니다.

비밀번호 확인. 비밀번호를 확인합니다.

설명. 에이전트에 대한 간단한 설명을 입력합니다. 예를 들어, 에이전트 인스턴스 이름이나 에이전트가 보호하는 응용 프로그램의 이름을 입력할 수 있습니다.

에이전트 키 값. 키 / 값 쌍을 사용하여 에이전트 등록 정보를 설정합니다. Access Manager 는 이 등록 정보를 사용하여 사용자의 자격 증명 명제에 대한 에이전트 요청을 받습니다. 현재로는 하나의 등록 정보만 유효하며 다른 모든 등록 정보는 무시됩니다. 다음 형식을 사용합니다.

`agentRootURL=http://server_name:port/`

장치 상태. 에이전트의 장치 상태를 입력합니다. 활성화로 설정된 경우 에이전트는 Access Manager 에 대해 인증되어 Access Manager 와 통신할 수 있습니다. 비활성으로 설정된 경우 에이전트는 Access Manager 에 대해 인증될 수 없습니다.

5. 확인을 누릅니다.

에이전트 삭제

1. 삭제할 에이전트를 포함하는 조직으로 이동합니다.

2. 보기 메뉴에서 에이전트를 선택합니다.
3. 에이전트의 이름 옆에 있는 확인란을 선택합니다.
4. 삭제를 누릅니다.

컨테이너

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

주 컨테이너 표시는 선택 사항입니다. 컨테이너를 보려면 서비스 구성 모듈의 보기 메뉴에서 컨테이너 표시를 선택해야 합니다. 세부 사항에 대해서는 [245 페이지의 "보기 메뉴에 컨테이너 표시"](#) 를 참조하십시오.

컨테이너 만들기

1. 새 컨테이너가 만들어지는 조직이나 컨테이너로 이동합니다.
보기 메뉴에서 컨테이너를 선택합니다.
2. 새로 만들기를 누릅니다.
컨테이너 템플릿가 데이터 창에 표시됩니다.
3. 만들려는 컨테이너의 이름을 입력합니다.
4. 확인을 누릅니다.
원하는 경우 보기 메뉴에서 표시 옵션과 사용 가능한 작업을 선택하여 구성할 수 있습니다. 자세한 내용은 이 장의 끝에 있는 [디스플레이 옵션과 사용 가능한 작업을](#) 참조하십시오.

컨테이너 삭제

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

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

사용자 컨테이너

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

주 사용자 컨테이너의 표시는 선택 사항입니다. 사용자 컨테이너를 보려면 서비스 구성 모듈에서 사용자 컨테이너 표시를 선택해야 합니다. 세부 사항에 대해서는 [244 페이지의 "사용자 컨테이너 표시"](#)를 참조하십시오.

사용자 컨테이너 만들기

1. 새 사용자 컨테이너를 만들려는 조직이나 사용자 컨테이너로 이동합니다.
보기 메뉴에서 사용자 컨테이너를 선택합니다.
2. 새로 만들기를 누릅니다.
사용자 컨테이너 템플릿가 데이터 창에 표시됩니다.
3. 만들려는 사용자 컨테이너의 이름을 입력합니다.
4. 확인을 누릅니다.

사용자 컨테이너 삭제

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

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

그룹 컨테이너

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

주 그룹 컨테이너의 표시는 선택 사항입니다. 그룹 컨테이너를 표시하려면 서비스 구성 모듈에서 그룹 컨테이너 표시를 선택해야 합니다. 세부 사항에 대해서는 [245 페이지의 "그룹 컨테이너 표시"](#)를 참조하십시오.

그룹 컨테이너 만들기

1. 만들려는 그룹 컨테이너를 포함하는 조직 또는 그룹 컨테이너로 이동합니다.
2. 보기 메뉴에서 그룹 컨테이너를 선택합니다.
기본 그룹은 조직을 만드는 동안 만들어집니다.
3. 새로 만들기를 누릅니다.
4. 이름 필드에 값을 입력하고 확인을 누릅니다. 새 그룹 컨테이너가 이동 창에 표시됩니다.

그룹 컨테이너 삭제

1. 삭제할 그룹 컨테이너가 포함된 조직으로 이동합니다.
2. 보기 메뉴에서 그룹 컨테이너를 선택합니다.
기본 그룹 및 만들어진 모든 그룹 컨테이너가 이동 창에 표시됩니다.
3. 삭제할 그룹 컨테이너 옆의 확인란을 선택합니다.
4. 삭제를 누릅니다.

디스플레이 옵션

조직, 역할 및 컨테이너의 경우 표시 옵션 보기를 사용하여 Access Manager 객체가 Access Manager 콘솔에서 표시되는 방법을 사용자 정의할 수 있습니다. 모든 객체 유형에 대해 모든 표시 옵션을 사용할 수 있는 것은 아닙니다.

표시 옵션 변경

1. 표시 옵션을 변경할 조직의 등록 정보 화살표를 누릅니다.

2. 데이터 창의 보기 메뉴에서 표시 옵션을 선택합니다.
3. 일반 섹션에서 등록 정보를 편집합니다. 등록 정보는 다음과 같습니다.
성명 생성 속성. 사용자 프로필의 이름 및 성 값으로 구성되는 사용자의 성명을 Access Manager 에서 항상 생성하도록 하려면 이 속성을 선택합니다.
항상 첫 번째 항목 선택. 검색 시에 이동 창에서 지정된 Identity 객체 유형의 첫 번째 항목을 자동으로 선택하여 데이터 창에서 표시하게 하려면 이 속성을 선택합니다.
사용자 프로필 페이지 제목. 사용자 프로필 페이지의 제목으로 사용할 속성을 이 폴다운 메뉴에서 선택합니다.
초기 검색 사용 불가. 이 값을 사용하면 하나 이상의 Identity 객체 유형에 대한 초기 Access Manager 검색이 사용 불가능하게 됩니다. 초기 검색을 사용 불가능하게 하면 성능이 향상되고 시간 초과 오류가 발생할 가능성이 줄어듭니다.
4. Access Manager 디렉토리 객체 섹션의 표시 구성에서 표시 옵션을 변경합니다. 이 섹션에서는 Access Manager 컨테이너와 객체가 표시되는 방법을 사용자 정의할 수 있습니다. Access Manager 컨테이너 옵션을 사용하면 이동 창의 보기 메뉴에 표시되는 객체 보기를 지정할 수 있습니다. Access Manager 객체 필드를 사용하면 데이터 창의 보기 메뉴에 표시되는 객체 보기를 지정할 수 있습니다.
5. 저장을 누릅니다.

사용 가능한 작업

일부 Access Manager 객체 유형의 경우 사용 가능한 작업 보기를 통해 사용자 액세스 권한을 정의할 수 있습니다.

사용자에 대한 사용 가능한 작업 설정

1. 사용 가능한 작업을 설정할 Identity 객체의 등록 정보 화살표를 누릅니다.
2. 데이터 창의 보기 메뉴에서 사용 가능한 작업을 선택합니다.

3. Access Manager 객체에 사용할 수 있는 작업 유형을 선택합니다. 작업 유형은 각 객체에 대한 사용자의 액세스를 정의합니다. 작업 유형은 다음과 같습니다.
 - 액세스 없음**. 사용자가 이 객체에 액세스할 수 없습니다.
 - 보기**. 사용자가 이 객체에 대한 읽기 전용 액세스를 가집니다.
 - 수정**. 사용자가 이 객체를 수정 및 확인할 수 있습니다.
 - 삭제**. 사용자가 이 객체를 수정, 확인 및 삭제할 수 있습니다.
 - 전체 액세스**. 사용자가 이 객체를 작성, 수정, 확인 및 삭제할 수 있습니다.
4. 저장을 누릅니다. 이전에 저장했던 상태로 값을 변경하려면 재설정을 누릅니다.

현재 세션

이 장에서는 Sun Java™ System Access Manager 6 2005Q1 의 세션 관리 기능에 대해 설명합니다. 세션 관리 모듈은 사용자 세션 정보 확인 및 사용자 세션 관리를 위한 솔루션을 제공합니다. 세션 관리 모듈은 다양한 세션 시간을 추적하고 관리자가 세션을 종료할 수 있도록 허용합니다. 시스템 관리자는 플랫폼 서버 목록에 있는 로드 밸런서 서버를 무시해야 합니다.

현재 세션 인터페이스

현재 세션 모듈 인터페이스를 사용하면 적절한 사용 권한이 있는 관리자가 현재 Access Manager 에 로그인한 사용자의 세션 정보를 볼 수 있습니다.

세션 관리 프레임

세션 관리 프레임은 현재 관리되고 있는 Access Manager 의 이름을 표시합니다.

세션 정보 창

세션 정보 창은 현재 Access Manager 에 로그인한 모든 사용자 및 각 사용자의 세션 시간을 표시합니다. 표시 필드는 다음과 같습니다.

사용자 아이디. 현재 로그인되어 있는 사용자의 사용자 아이디를 표시합니다.

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

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

유휴 시간. 사용자가 유휴 상태인 시간 (분) 을 표시합니다 .

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

시간 제한은 관리자가 세션 관리 서비스에서 정의합니다 . 자세한 내용은 [385 페이지의 " 세션 서비스 속성 "](#) 을 참조하십시오 .

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

[갱신] 버튼을 누르면 사용자 세션 표시가 업데이트됩니다 .

세션 종료

적절한 사용 권한을 가진 관리자가 언제든지 사용자 세션을 종료할 수 있습니다.
수행 방법은 다음과 같습니다.

1. 종료하려는 사용자 세션을 선택합니다.
2. [종료]를 누릅니다.

현재 세션 인터페이스

정책 관리

이 장에서는 Sun Java™ System Access Manager 6 2005Q1 의 정책 관리 기능에 대해 설명합니다. Access Manager 의 정책 관리 기능을 사용하면 최상위 관리자 또는 최상위 정책 관리자가 모든 조직에서 사용될 수 있는 특정 서비스에 대한 정책을 보고, 만들고, 삭제 및 수정할 수 있습니다. 조직 또는 하위 조직 관리자나 정책 관리자가 조직에서의 특정 사용을 위해 정책을 보고, 만들고, 삭제 및 수정할 수 있습니다.

이번 장은 다음 절로 구성됩니다.

- 106 페이지의 " 개요 "
- 106 페이지의 " 정책 관리 기능 "
- 109 페이지의 " 정책 유형 "
- 112 페이지의 " 정책 정의 유형 문서 "
- 117 페이지의 " 정책 만들기 "
- 120 페이지의 " 정책 관리 "
- 127 페이지의 " 정책 구성 서비스 "
- 129 페이지의 " 정책 기반 자원 관리 "

개요

정책은 조직의 보호 대상 자원에 대한 액세스 권한을 지정하는 규칙을 정의합니다. 보호하고 관리하고 모니터링해야 하는 자원, 응용 프로그램 및 서비스가 있습니다. 정책은 주어진 자원에 대한 작업을 사용자가 언제 어떤 방법으로 수행할 수 있는지 정의하여 이러한 자원에 대한 액세스 권한과 용도를 제어합니다. 정책을 객체에 적용할 때 특정 객체가 액세스할 수 있는 자원을 정의합니다.

주 객체는 기본입니다. 기본은 개인, 회사, 역할 또는 그룹 등 아이디를 가질 수 있는 모든 것일 수 있습니다. 자세한 내용은 Java™ 2 Platform Standard Edition Javadocs 를 참조하십시오.

단일 정책은 이진 또는 비 이진 결정 중 하나를 정의할 수 있습니다. 이진 결정은 *예/아니오*, *true/false* 또는 *허용/거부*입니다. 비 이진 결정은 속성의 값을 나타냅니다. 예를 들어, 메일 서비스에는 각 사용자에 대한 최대 저장 값이 설정된 mailboxQuota 속성이 포함될 수 있습니다. 일반적으로 정책은 한 객체가 어떤 자원에 대해 어떤 조건 하에서 어떤 작업을 수행할 수 있는지 정의하도록 구성됩니다.

정책 관리 기능

정책 관리 기능은 정책을 만들고 관리하기 위한 **정책 서비스**를 제공합니다. 정책 서비스는 관리자가 Access Manager 배포 내에서 자원을 보호하기 위해 권한을 정의, 수정, 부여, 철회 및 삭제할 수 있도록 합니다. 일반적으로 정책 서비스에는 데이터 저장소, 정책을 만들고 관리하며 평가하도록 해주는 인터페이스 라이브러리 및 정책 집행자 또는 **정책 에이전트**가 포함됩니다. Access Manager 는 데이터 저장을 위해 Sun Java System Directory Server 를 사용하며 정책 평가 및 정책 서비스 사용자 정의를 위해 Java 및 C API 를 제공합니다. 자세한 내용은 *Access Manager Developer's Guide* 를 참조하십시오. 또한 정책 서비스는 관리자가 정책 관리를 위해 Access Manager 콘솔을 사용할 수 있도록 합니다. Access Manager 는 다운로드할 수 있는 정책 에이전트를 사용하여 정책을 집행하는 URL 정책 에이전트 서비스를 제공합니다.

URL 정책 에이전트 서비스

Access Manager 는 정책 집행을 위해 URL 정책 에이전트 서비스를 제공합니다. 이 서비스를 사용하여 관리자는 정책 집행자 또는 **정책 에이전트**를 통해 정책을 만들고 관리할 수 있습니다.

정책 에이전트

정책 에이전트는 회사의 자원이 저장된 서버에 대한 정책 적용 지점 (PEP) 입니다. 정책 에이전트는 웹 서버에 Access Manager 와 별도로 설치되며 사용자가 보호를 받는 웹 서버에 있는 웹 자원에 대한 요청을 보낼 때 추가 인증 단계 역할을 합니다. 이 인증 단계는 자원에서 수행하는 사용자 인증 요청에 추가로 이루어집니다. 에이전트는 웹 서버를 보호하고 자원은 인증 플러그 인에 의해 보호됩니다.

예를 들어, 원격 설치된 Access Manager 에 의해 보호되는 인력 자원 웹 서버에는 에이전트가 설치되어 있을 수 있습니다. 이 에이전트는 제대로된 정책 없이 기밀 정보 인 봉급 정보나 기타 민감한 데이터를 보지 못하도록 방지합니다. 정책은 Access Manager 관리자가 정의하여 Access Manager 배포 내에 저장하며 정책 에이전트가 원격 웹 서버의 내용에 대한 사용자 액세스를 허용 또는 거부하는 데 사용됩니다.

최신 Sun Java System Access Manager 정책 에이전트는 Sun Microsystems 다운로드 센터에서 다운로드할 수 있습니다.

정책 에이전트 설치 및 관리에 대한 자세한 내용은 *Sun Java System Access Manager J2EE Policy Agents Guide* 또는 *Web Policy Agents Guide* 를 참조하십시오.

주 정책은 특별한 순서로 평가되지 않습니다. 그러나 정책을 평가할 때 한 가지 작업 값이 *거부*로 평가되는 경우 정책 구성 서비스에서 거부 결정에 대한 평가 계속 속성이 활성화되지 않으면 후속 정책은 평가되지 않습니다. 세부 사항에 대해서는 [367 페이지의 "정책 구성 서비스 속성"](#) 을 참조하십시오.

정책 에이전트는 웹 URL (<http://...>) 에서만 결정을 실행합니다. 그러나 Java 및 C 정책 평가 API 를 사용하여 다른 자원에서 정책을 실행하는 에이전트를 작성할 수 있습니다.

또한 정책 구성 서비스의 자원 비교기 속성도 기본 구성에서 다음과 같은 구성으로 변경해야 합니다.

```
serviceType=Name_of_LDAPService|class=com.sun.identity.policy.plugins.SuffixResourceName|wildcard=*|delimiter=,|caseSensitive=false
```

또는 LDAPResourceName 과 같은 구현을 제공하여 com.sun.identity.policy.interfaces.ResourceName 을 구현하고 자원 비교기를 구성하는 방법도 사용할 수 있습니다.

주 자원 비교기 속성의 필드는 [367 페이지의 "정책 구성 서비스 속성"](#) 에 설명되어 있습니다.

정책 에이전트 프로세스

보호 대상 웹 자원을 위한 프로세스는 정책 에이전트에 의해 보호를 받는 서버에 상주하는 URL 을 웹 브라우저에서 요청할 때 시작됩니다. 서버의 설치된 정책 에이전트는 요청을 인터셉트하여 기존 인증 자격 증명 (세션 토큰) 을 확인합니다.

에이전트가 요청을 인터셉트하고 기존 세션 토큰을 확인하면 다음 프로세스가 이어집니다.

1. 세션 토큰이 유효하면 사용자에게 권한이 부여 또는 거부됩니다. 유효한 토큰이 아닐 경우 사용자는 다음과 같은 단계를 거쳐 인증 서비스로 리디렉션됩니다.
2. 인증 서비스는 자격 증명이 유효한지 확인하고 토큰을 발급합니다.
3. 일단 사용자의 자격 증명에 제대로 인증을 받으면 에이전트는 Access Manager 의 내부 서비스에 액세스하는 데 사용되는 URL 을 정의하는 이름 지정 서비스에 대해 요청을 발급합니다.
4. 이름 지정 서비스는 정책 서비스에 대한 로케이터를 반환하고 에이전트는 사용자에게 적용할 수 있는 정책 결정을 얻기 위해 정책 서비스에 요청을 보냅니다.
5. 액세스 대상 자원에 대한 정책 결정에 따라 사용자는 액세스 권한이 부여되거나 거부됩니다. 정책 결정에 대한 조언에 다른 인증 수준 또는 방법이 제시되면 에이전트는 모든 검색 조건이 확인될 때까지 요청을 인증 서비스로 다시 보냅니다.

에이전트가 기존 세션 토큰이 없는 요청을 인터셉트했다면 다른 인증 방법을 사용하여 자원을 보호하더라도 사용자를 기본 로그인 페이지로 리디렉션합니다.

주 정책 기반 자원 인증 및 사용자 인증은 서로 다른 유형의 인증입니다. 자세한 내용은 [129 페이지의 "정책 기반 자원 관리"](#) 를 참조하십시오.

정책 유형

Access Manager 를 사용하여 구성할 수 있는 정책 유형에는 *일반정책*과 *참조정책*의 두 가지 유형이 있습니다. 일반 정책은 *규칙*, *주제* 및 *조건*으로 구성됩니다. 참조 정책은 *규칙* 및 조직에 대한 *참조*로 구성됩니다.

일반 정책

Access Manager 에서 액세스 권한을 정의하는 정책을 *일반정책*이라고 합니다. 일반 정책은 *규칙*, *주제* 및 *조건*으로 구성됩니다.

규칙

하나의 *규칙*에는 하나의 자원, 하나 이상의 작업 및 하나의 값이 포함됩니다. 기본적으로 규칙이 정책을 정의합니다.

- *자원*은 인적 자원 서비스를 사용하여 액세스되는 HTML 페이지 또는 사용자의 발급 정보 등 보호 대상인 특정 객체를 정의합니다.
- *작업*은 자원에 대해 수행될 수 있는 작업의 이름입니다. 예를 들어, 웹 서버 작업으로는 POST 또는 GET 등이 있습니다. 인적 자원에 대해 허용되는 작업 중 한 가지를 예로 들면 canChangeHomeTelephone 가 있습니다.
- *값*은 작업에 대한 권한 (예 : 허용 또는 거부) 을 정의합니다.

주

자원 없이 작업을 정의할 수 있습니다.

주제

*주제*는 정책이 영향을 주는 사용자 또는 사용자 집합 (예 : 그룹 또는 특정 역할 소유자들) 을 정의합니다. 주제는 정책에 지정됩니다. 사용자가 적어도 정책의 한 주제의 구성원일 경우에만 정책이 적용되는 것이 일반적인 규칙입니다. 기본 주제는 다음과 같습니다.

- 인증된 사용자
- Access Manager 역할
- LDAP 그룹
- LDAP 역할
- LDAP 사용자

- 조직
- 웹 서비스 클라이언트

Access Manager 역할 대 LDAP 역할

Access Manager 역할은 Access Manager 를 사용하여 생성됩니다. 이러한 역할은 Access Manager 에 의해 위임되는 객체 클래스를 가집니다. LDAP 역할은 Directory Server 역할 기능을 사용하는 역할 정의입니다. 이러한 역할은 Directory Server 역할 정의에 의해 위임되는 객체 클래스를 가집니다. 모든 Access Manager 역할은 Directory Server 역할로 사용될 수 있습니다. 그러나, 모든 Directory Server 역할이 반드시 Access Manager 역할인 것은 아닙니다. LDAP 역할은 정책 구성 서비스를 구성하여 기존 디렉토리에서 활용될 수 있습니다. Access Manager 역할은 호스팅 Access Manager 정책 서비스를 통해서만 액세스할 수 있습니다. Access Manager 역할의 구성원을 평가하는 작업은 Access Manager SDK 및 캐시에 액세스하기 때문에 더 빨라질 것입니다. 정책 구성 서비스에서 LDAP 역할 검색 필터를 수정하여 범위를 좁히고 성능을 향상시킬 수 있습니다.

중첩된 역할

중첩된 역할은 정책 정의의 주제에서 LDAP 역할로 올바르게 평가될 수 있습니다.

조건

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

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

주

참조, 규칙, 자원, 주제, 조건, 작업 및 값이라는 용어는 `policy.dtd` 에서 *Referral*, *Rule*, *ResourceName*, *Subject*, *Condition*, *Attribute* 및 *Value* 요소에 해당합니다.

정책 권고

조건에 따라 결정한 대로 정책을 적용할 수 없을 때는 그 조건에서 해당 정책을 요청에 적용할 수 없는 이유를 나타내는 권고 메시지를 만듭니다. 이러한 권고 메시지는 정책 적용 지점에 대한 정책 결정에 전달됩니다. 정책 적용 지점은 이 권고를 검색하고 더 높은 수준으로 인증하는 인증 메커니즘으로 사용자를 리디렉션하는 등의 적당한 조치를 취하게 됩니다. 적합한 조치가 취해진 후 정책이 적용 가능하게 되면 사용자에게 더 높은 수준의 인증에 관한 프롬프트가 나타나 자원에 액세스할 수 있게 됩니다.

자세한 내용은 다음 클래스를 참조하십시오.

```
com.sun.identity.policy.ConditionDecision.getAdvices()
```

해당 조건이 충족되지 않으면 `AuthLevelCondition` 및 `AuthSchemeCondition` 에서 권고를 제공합니다.

`AuthLevelCondition` 권고는 다음 키와 관련되어 있습니다.

```
com.sun.identity.policy.plugin.AuthLevelCondition.AUTH_LEVEL_CONDITION_ADVICE
```

`AuthSchemeCondition` 권고는 다음 키와 관련되어 있습니다.

```
com.sun.identity.policy.plugin.AuthLevelCondition.AUTH_SCHEME_CONDITION_ADVICE
```

사용자 정의한 조건도 권고를 만들 수 있습니다. 그러나 `Access Manager` 정책 에이전트는 인증 수준 권고와 인증 스키마 권고에만 응답합니다. 사용자 정의 에이전트를 작성하고 기존 `Access Manager` 에이전트를 확장하여 더 많은 권고를 이해하고 응답할 수 있습니다. 자세한 내용은 다음 위치에서 정책 에이전트 설명서를 참조하십시오.

http://docs.sun.com/app/docs/coll/S1_IdServPolicyAgent_21

참조 정책

관리자가 한 조직의 정책 정의와 결정을 다른 조직에 위임해야 하는 경우가 있습니다. 또는 자원에 대한 정책 결정을 다른 정책 제품에 위임할 수 있습니다. 참조 정책은 정책 작성과 평가를 위해 이 정책 위임을 제어합니다. 이 정책은 하나 이상의 규칙과 하나 이상의 참조로 구성됩니다.

규칙

규칙은 정책 정의와 평가가 참조되는 자원을 정의합니다.

참조

참조는 정책 평가가 참조되는 조직을 정의합니다. 기본적으로 참조에는 피어 조직과 하위 조직의 두 가지 유형이 있습니다. 이러한 참조는 각각 동일한 수준의 조직과 하위 수준의 조직에 위임됩니다. 자세한 내용은 [119 페이지의 " 피어 및 하위 조직에 대한 정책 만들기 "](#) 를 참조하십시오 .

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

정책 정의 유형 문서

일단 작성하여 구성한 정책은 Directory Server 에 XML 파일로 저장됩니다 . Directory Server 에서 XML 로 인코딩된 데이터는 한 곳에 저장됩니다 . amadmin.dtd (또는 콘솔) 를 사용하여 정책을 정의하고 구성하지만 실제로 Directory Server 에는 policy.dtd 를 기반으로 한 XML 로 저장됩니다 . policy.dtd 에는 정책 작성 태그가 없고 amadmin.dtd 에서 추출한 정책 요소 태그가 포함됩니다 . 그러므로 정책 서비스는 Directory Server 에서 정책을 로드할 때 policy.dtd 를 기반으로 XML 의 구문을 분석합니다 . amadmin.dtd 는 명령줄을 사용하여 정책을 만들 때만 사용됩니다 . 이 절에서는 policy.dtd 의 구조에 대해 설명합니다 . policy.dtd 는 다음 위치에 있습니다 .

AccessManager-base/SUNWam/dtd (Solairs)

AccessManager-base/identity/dtd (Linux)

주 이 장에서는 Solaris 디렉토리에 대한 내용만 설명합니다 . Linux 를 위한 디렉토리 구조는 다릅니다 . 자세한 내용은 [21 페이지의 " 설명서 소개 "](#) 를 참조하십시오 .

Policy 요소

Policy 요소는 정책의 권한 또는 *규칙*과 규칙 적용 대상 또는 *주제*를 정의하는 루트 요소입니다. 또한 정책이 *참조* (위임) 정책인지 아닌지 여부와 제한 (또는 *조건*) 이 있는지 여부도 정의합니다. *Policy* 요소에는 다음과 같은 하위 요소가 한 가지 이상 포함될 수 있습니다. *Rule, Conditions, Subjects* 또는 *Referrals*. 필수 XML 속성은 정책의 이름을 지정하는 *name* 속성입니다. *referralPolicy* 속성은 정책이 참조 정책인지 여부를 나타내며 정의하지 않을 경우 기본값은 일반 정책입니다. 선택 XML 속성은 *name* 속성과 *description* 속성입니다.

주 정책에 *참조*라는 태그를 붙이면 정책 평가 시 주제와 조건은 무시됩니다. 반대로 *일부*이라는 태그를 붙이면 정책을 평가할 때 참조가 무시됩니다.

Rule 요소

Rule 요소는 정책에 대한 구체적인 사항을 정의하며 3 가지 하위 요소를 취할 수 있습니다. *ServiceName, ResourceName* 또는 *AttributeValuePair*. *Rule* 요소는 정책이 만들어졌던 서비스 또는 응용 프로그램의 유형과 자원 이름, 수행되는 작업을 정의합니다. 작업이 없는 규칙을 정의할 수도 있습니다. 예를 들어, 참조 정책 규칙에는 작업이 포함되지 않습니다.

주 *ResourceName* 요소가 정의되지 않은 정책을 정의할 수도 있습니다.

ServiceName 요소

ServiceName 요소는 정책이 적용되는 서비스의 이름을 정의합니다. 이 요소는 서비스 유형을 나타내며 이 요소에는 다른 요소가 포함되지 않습니다. 이 요소의 값은 *sms.dtd*를 기반으로 서비스의 XML 파일에 정의된 것과 같습니다. *ServiceName* 요소의 XML 서비스 속성은 문자열 값을 취하는 서비스의 이름입니다.

ResourceName 요소

ResourceName 요소는 작업 수행 대상인 객체를 정의합니다. 정책은 이 객체를 보호하도록 특별히 구성되었습니다. 이 요소에는 다른 요소가 포함되지 않습니다.

ResourceName 요소의 XML 서비스 속성은 객체의 이름입니다. *ResourceName*의 예로는 웹 서버의 `http://www.sunone.com:8080/images` 또는 디렉토리 서버의 `ldap://sunone.com:389/dc=example,dc=com` 등이 있을 수 있습니다. 보다 구체적인 예를 들면 `salary://uid=jsmith,ou=people,dc=example,dc=com` 자원이 있을 수 있습니다. 이 예에서 작업이 수행되는 객체는 John Smith의 봉급 정보입니다.

AttributeValuePair 요소

AttributeValuePair 요소는 작업과 그 작업의 값을 정의합니다. 이 요소는 [Subject 요소](#), [Referral 요소](#) 및 [Condition 요소](#)의 하위 요소로 사용됩니다. *Attribute* 요소와 *Value* 요소가 모두 포함되며 XML 서비스 속성은 포함되지 않습니다.

Attribute 요소

Attribute 요소는 작업의 이름을 정의합니다. 작업은 자원에 대해 수행되는 작업 또는 이벤트입니다. POST 또는 GET는 웹 서버 자원에 대해 수행되는 작업이며 READ 또는 SEARCH는 디렉토리 서버 자원에 대해 수행되는 작업입니다. *Attribute* 요소는 *Value* 요소와 함께 사용되어야 합니다. *Attribute* 요소 자체는 다른 요소를 포함하지 않습니다. *Attribute* 요소의 XML 서비스 속성은 작업의 이름입니다.

Value 요소

Value 요소는 작업 값을 정의합니다. 작업 값으로는 허용 / 거부 또는 예 / 아니요 등이 있습니다. 그 밖의 작업 값은 부울, 숫자 또는 문자열일 수 있습니다. 작업 값은 sms.dtd를 기반으로 서비스의 XML 파일에 정의됩니다. *Value* 요소는 다른 요소를 포함하지 않으며 XML 서비스 속성도 포함하지 않습니다.

주의

거부 규칙은 허용 규칙보다 항상 우선됩니다. 예를 들어 한 정책이 액세스를 거부하고 다른 정책은 허용할 경우, 두 정책에 대한 다른 모든 조건은 충족된다고 가정할 때 정책 간에 잠재적인 충돌이 일어날 수 있으므로 거부 정책을 사용할 때는 매우 주의해야 합니다. 명시적인 거부 규칙이 사용될 경우 역할이나 그룹 구성원처럼 다른 주제를 통해 사용자에게 할당된 정책 때문에 액세스가 거부될 수 있습니다. 일반적으로 정책 정의 프로세스에서는 허용 규칙만 사용해야 합니다. 기본 거부는 다른 정책이 적용되지 않을 때 사용될 수 있습니다.

Subjects 요소

Subjects 하위 요소는 정책이 적용되는 객체의 집합을 식별합니다. 이 집합은 그룹의 구성원, 역할의 소유자 또는 개인 사용자에게 따라 선택됩니다. 이 요소의 하위 요소는 *Subject* 입니다. 정의될 수 있는 XML 속성은 다음과 같습니다.

name. 이 속성은 Subject 요소의 이름입니다.

description. 이 속성은 주제에 대한 설명입니다.

includeType. 이 속성은 현재 사용되지 않습니다.

Subject 요소

Subject 하위 요소는 정책이 적용되는 객체의 집합을 식별합니다. 이 집합은 *Subjects* 요소에 의해 정의되는 집합에서 보다 구체적인 객체들의 집합을 가려낸 것입니다. 이 집합의 구성원은 역할, 그룹 구성원 또는 개별 사용자를 기반으로 할 수 있습니다. 이 요소의 하위 요소는 [AttributeValuePair 요소](#)입니다. 필수 XML 속성은 *type* 입니다. 이 속성은 정의된 *Subjects* 가 취해지는 객체의 집합을 식별합니다. 다른 XML 속성으로는 집합의 이름을 정의하는 *name* 속성과 집합이 정의된 대로인지 정책이 *Subject* 의 구성원이 아닌 사용자에게 적용되는지 여부를 정의하는 *includeType* 속성이 있습니다.

주 다수의 *Subjects* 를 정의할 때는 최소한 그 중 하나가 정책이 적용될 사용자에게 적용되어야 합니다. *false* 로 설정된 *includeType* 속성을 사용하여 하나의 *Subject* 를 정의할 때는 사용자가 그 *Subject* 의 구성원이 아니어야 합니다.

Referrals 요소

Referrals 하위 요소는 정책 참조 집합을 식별합니다. 이 요소는 *Referral* 하위 요소를 취합니다. 정의될 수 있는 XML 속성은 집합의 이름을 정의하는 *name* 속성과 설명을 취하는 *description* 속성입니다.

Referral 요소

Referral 하위 요소는 특정 정책 참조를 식별합니다. 이 요소는 [AttributeValuePair 요소](#)를 하위 요소로 취합니다. 필수 XML 속성은 구체적으로 정의된 참조를 취하는 할당의 집합을 식별하는 *type* 속성입니다. 집합의 이름을 정의하는 *name* 속성도 포함될 수 있습니다.

Conditions 요소

Conditions 하위 요소는 정책 제한 사항 (시간 범위, 인증 수준 등)의 집합을 식별합니다. 이 요소는 하나 이상의 *Condition* 하위 요소를 포함해야 합니다. 정의될 수 있는 XML 속성은 집합의 이름을 정의하는 *name* 속성과 설명을 취하는 *description* 속성입니다.

주 Conditions 요소는 정책의 선택 요소입니다.

Condition 요소

Condition 하위 요소는 특정 정책 제한 사항 (시간 범위, 인증 수준 등)을 식별합니다. 이 요소는 **AttributeValuePair** 요소를 하위 요소로 취합니다. 필수 XML 속성은 구체적으로 정의된 조건을 취하는 제한 사항의 집합을 식별하는 *type* 속성입니다. 집합의 이름을 정의하는 *name* 속성도 포함될 수 있습니다.

정책 서비스 추가

기본적으로, Access Manager 는 URL 정책 에이전트 서비스 (iPlanetAMWebAgentService) 를 제공합니다. 이 서비스는 다음 디렉토리에 있는 XML 파일에 정의됩니다.

```
/etc/opt/SUNWam/config/xml/
```

그러나 Access Manager 에 정책 서비스를 추가할 수 있습니다. 일단 정책 서비스가 만들어지면 `amadmin` 명령줄 유틸리티를 통해 Access Manager 에 추가합니다.

새 정책 서비스 추가

1. `sms.dtd` 를 기반으로 XML 파일에 새 정책 서비스를 개발합니다. Access Manager 는 새 정책 서비스 파일을 위한 기반으로 사용 가능한 두 가지 정책 서비스 XML 파일을 제공합니다.

`amWebAgent.xml` - 기본 URL 정책 에이전트 서비스를 위한 XML 파일로
 /etc/opt/SUNWam/config/xml/ 에 있습니다.

`SampleWebService.xml` - 샘플 정책 서비스 파일로
 /opt/SUNWam/samples/policy 에 있습니다.

2. 새 정책 서비스를 로드할 디렉토리에 XML 파일을 저장합니다. 예를 들면 다음과 같습니다.

```
/etc/opt/SUNWam/config/xml/newPolicyService.xml
```

3. amadmin 명령줄 유틸리티를 사용하여 새 정책 서비스를 로드합니다. 예를 들면 다음과 같습니다.

```
AccessManager-base/SUNWam/bin/amadmin
--runasdn "uid=amAdmin,ou=People,default_org,root_suffix
--password password
--schema /etc/opt/SUNWam/config/xml/newPolicyService.xml
```

4. 새 정책 서비스를 로드한 후 amadmin 을 통해 새 정책을 로드하거나 Access Manager 콘솔을 통해 정책 정의 규칙을 정의할 수 있습니다.

정책 만들기

정책 API 와 Access Manager 콘솔을 통해 정책을 만들고 수정하고 삭제할 수 있으며 amadmin 명령줄 도구를 통해 정책을 만들고 삭제할 수 있습니다. 이 절에서는 amadmin 명령줄 유틸리티와 Access Manager 콘솔을 통해 정책을 만드는 방법에 대해 설명합니다. 정책 API 에 대한 자세한 내용은 *Access Manager Developer's Guide* 를 참조하십시오.

정책은 일반적으로 XML 파일을 통해 만들어지며 amadmin 명령줄 유틸리티를 통해 Access Manager 에 추가된 후 Access Manager 콘솔을 통해 관리됩니다 (콘솔을 통해 정책을 만들 수도 있음). amadmin 을 사용하여 직접 정책을 수정할 수 없기 때문입니다. 정책을 수정하려면 Access Manager 에서 정책을 삭제한 다음 amadmin 을 사용하여 수정된 정책을 추가해야 합니다.

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

amadmin 으로 정책 만들기

1. policy.dtd 를 기반으로 정책의 XML 파일을 만듭니다. 이 파일은 다음 디렉토리에 있습니다.

```
AccessManager-base/SUNWam/dtd
```

2. 일단 정책의 XML 파일이 만들어지면 다음 명령을 사용하여 로드할 수 있습니다.

```
AccessManager-base/SUNWam/bin/amadmin
```

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

```
--password password
```

```
--data policy.xml
```

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

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

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

Access Manager 콘솔을 사용하여 정책 생성

1. Identity 관리 인터페이스로 이동합니다.

2. 정책을 만들려는 조직을 선택합니다.

정책 관리 창의 위치가 조직에 맞게 올바른지 확인합니다.

3. 보기 메뉴에서 정책을 선택합니다.

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

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

5. 만들려는 정책 유형 (일반 또는 참조) 을 선택합니다.

하위 조직을 참조하는 참조 정책이 존재하지 않을 경우 해당 하위 조직에 대한 정책을 만들 수 없습니다.

이 시점에서 일반 또는 참조 정책에 대한 모든 필드를 정의할 필요는 없습니다. 정책을 만든 다음 나중에 규칙, 주제, 참조 등을 추가할 수 있습니다.

6. 정책의 이름을 입력하고 확인을 누릅니다.

7. 기본적으로 일반 보기가 표시됩니다.

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

8. 저장을 눌러 정책 구성을 완료합니다.

피어 및 하위 조직에 대한 정책 만들기

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

이 예에서 `o=isp` 는 상위 조직이고, `o=example.com` 은 하위 조직으로 `http://www.example.com` 의 자원과 하위 자원을 관리합니다.

하위 조직에 대한 정책을 만들려면

1. `o=isp`에 참조 정책을 만듭니다. 참조 정책에 대한 자세한 내용은 [126페이지의 "참조 정책 수정"](#) 절차를 참조하십시오.

참조 정책은 `http://www.example.com` 을 규칙의 자원으로 정의하고, `example.com` 을 갖는 `SubOrgReferral` 을 참조의 값으로 포함해야 합니다.

2. 조직 보기로 이동한 다음 `example.com` 하위 조직으로 이동합니다.
3. 정책 구성 서비스가 하위 조직 수준 `example.com`에 등록되어 있는지 확인합니다. 자세한 내용은 [128 페이지의 "정책 구성 서비스 추가"](#) 을 참조하십시오.

- 이제 자원이 isp 에 의해 sun.com 을 참조하므로 자원 `http://www.example.com` 또는 `http://www.example.com` 으로 시작하는 모든 자원에 대한 일반 정책을 만들 수 있습니다.

일반 정책 만들기에 대한 자세한 내용은 [120 페이지의 "일반 정책 수정"](#) 절차를 참조하십시오.

`example.com` 에 의해 관리되는 다른 자원에 대한 정책을 정의하려면 `o=isp` 에 추가 참조 정책을 만들어야 합니다.

정책 관리

일단 일반 또는 참조 정책을 만들어 Access Manager 에 추가하면 Access Manager 콘솔을 통해 규칙, 주제, 조건 및 참조를 수정하여 정책을 관리할 수 있습니다.

일반 정책 수정

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

규칙을 수정하려면

- Identity 관리 인터페이스의 보기 메뉴에서 정책을 선택합니다.

해당 조직에 대해 작성된 정책이 표시됩니다.

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

기본적으로 일반 보기가 표시됩니다. 일반 보기에 표시되는 속성은 [117 페이지의 "정책 만들기"](#)에 설명되어 있습니다.

- 보기 메뉴에서 규칙을 선택하고 새로 만들기를 누릅니다.

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

4. 규칙 필드에서 자원, 작업 및 작업 값을 정의합니다. 필드는 다음과 같습니다.

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

규칙 이름. 규칙의 이름을 입력합니다.

자원 이름. 자원의 이름을 입력합니다. 예를 들면 다음과 같습니다.

`http://www.example.com`

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

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

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

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

특정 시스템에 설치된 모든 서버에 대해 자원을 관리할 수 있도록 하려면 자원을 `http://host*:*` 로 정의합니다. 또는 다음 자원을 정의하여 특정 조직의 관리자에게 해당 조직의 모든 서비스에 대한 권한을 부여할 수 있습니다.

`http://*.subdomain.domain.topleveldomain`

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

- GET
- POST

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

- 허용 규칙에 정의된 자원과 일치하는 자원에 액세스할 수 있게 합니다.
- 거부 규칙에 정의된 자원과 일치하는 자원에 대한 액세스를 거부합니다.

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

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

이러한 문제를 해결하는 한 가지 방법은 조건 플러그 인을 사용하여 정책을 설계하는 것입니다. 위의 경우에 직원 역할에 인증된 사용자에게 거부 정책을 적용하고 관리자 역할에 인증된 사용자에게 허용 정책을 적용하는 " 역할 조건 " 을 지정하여 두 정책을 차별화할 수 있습니다. 다른 방법은 authentication level 조건을 사용하는 것입니다. 이 조건에서는 관리자 역할이 더 높은 인증 수준으로 인증됩니다. 자세한 내용은 [124 페이지의 " 조건 추가 또는 수정 "](#) 을 참조하십시오.

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

5. 마침을 눌러 규칙을 저장합니다. 이 경우에 구성만 메모리에 저장됩니다. 프로세스를 완료하려면 단계 7 을 수행합니다.

6. 단계 1 에서 단계 5 까지 반복하여 추가 규칙을 만듭니다.

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

정책에서 규칙을 제거하려면 규칙을 선택하고 제거를 누릅니다.

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

주제를 수정하려면

1. 정책의 주제를 정의하려면 보기 메뉴에서 주제를 선택하고 새로 만들기를 누릅니다.

2. 다음 기본 주제 유형 중 하나를 선택합니다.

인증된 사용자. 이 주제 유형은 유효한 SSO 토큰을 가진 사용자가 이 주제의 구성원이라는 것을 나타냅니다.

인증된 사용자는 정책이 정의된 조직과 다른 조직에 인증한 경우에도 모두 이 주제의 구성원이 됩니다. 이는 자원 소유자가 관리되는 자원에 대한 액세스 권한을 다른 조직의 사용자에게 제공하는 경우에 유용합니다. 보호되는 자원에 대한 액세스 권한을 특정 조직의 구성원에게만 제한하려면 조직 주제를 사용하십시오.

Access Manager 역할. 이 주제 유형은 Access Manager 역할의 구성원이 이 주제의 구성원이라는 것을 나타냅니다. Access Manager 역할은 Access Manager를 사용하여 작성됩니다. 이러한 역할은 Access Manager에 의해 위임되는 객체 클래스를 가집니다. Access Manager 역할은 Access Manager 정책 서비스를 호스팅하는 방법으로만 액세스할 수 있습니다.

LDAP 그룹. 이 주제 유형은 LDAP 그룹의 구성원이 이 주제의 구성원이라는 것을 나타냅니다.

LDAP 역할. 이 주제 유형은 LDAP 역할의 구성원이 이 주제의 구성원이라는 것을 나타냅니다. LDAP 역할은 Directory Server 역할 기능을 사용하는 임의의 역할 정의입니다. 이러한 역할은 Directory Server 역할 정의에 의해 위임되는 객체 클래스를 가집니다. 정책 구성 서비스에서 LDAP 역할 검색 필터를 수정하여 범위를 좁히고 성능을 향상시킬 수 있습니다.

LDAP 사용자. 이 주제 유형은 LDAP 사용자가 이 주제의 구성원이라는 것을 나타냅니다.

조직. 이 주제 유형은 조직의 구성원이 이 주제의 구성원이라는 것을 나타냅니다.

웹 서비스 클라이언트. 이 주제 유형은 SSO 토큰에 포함된 기본 DN이 이 주제의 선택된 임의 값과 일치할 경우 SSO 토큰으로 식별된 웹 서비스 클라이언트 (WSC)가 이 주제의 구성원이라는 것을 나타냅니다. 유효한 값은 로컬 JKS 키 저장소에 있는 신뢰할 수 있는 인증서 (신뢰할 수 있는 WSC의 인증서에 해당)의 DN입니다. 이 주제는 리버티 웹 서비스 프레임워크에 대해 종속성을 가지며 리버티 서비스 공급자가 WSC를 인증하기 위해서만 사용해야 합니다.

이 주제를 정책에 추가하기 전에 키 저장소를 만들어야 합니다. 키 저장소 설정에 대한 내용은 다음 사이트를 참조하십시오.

`AccessManager-base/SUNWam/samples/saml/xmlsig/keytool.html`

다음을 눌러 계속합니다.

3. 주제의 이름을 입력합니다.

4. 단독 필드를 선택하거나 선택 취소합니다.

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

정책에 여러 주제가 존재하는 경우, 최소한 하나 이상의 주제에서 정책이 주어진 Identity 에 적용된다는 것을 나타내면 정책이 Identity 에 적용됩니다.

5. 주제에 추가할 Identity 를 표시하기 위해 검색을 수행합니다. 이 단계는 인증된 사용자 주제 또는 웹 서비스 클라이언트 주제에는 적용되지 않습니다.

기본 (*) 검색 패턴은 모든 정규화된 항목을 표시합니다.

6. 주제에 대해 추가할 개별 Identity 를 선택하거나 모두 추가를 눌러 모든 Identity 를 한번에 추가합니다. 추가를 눌러 Identity 를 선택 목록 상자로 이동합니다. 이 단계는 인증된 사용자 주제 또는 웹 서비스 클라이언트 주제에는 적용되지 않습니다.

7. 마침을 누릅니다.

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

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

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

조건 추가 또는 수정

1. 보기 메뉴에서 조건을 선택합니다. 새로 만들기를 눌러 새 조건을 추가하거나 편집 링크를 눌러 기존 조건을 편집합니다.
2. 다음 기본 조건 중 하나를 선택합니다.

- 인증 수준
- 인증 방법
- IP 주소
- LE 인증 수준
- 세션
- 시간

인증 수준의 경우 사용자의 인증 수준이 조건에 설정된 인증 수준보다 크거나 같은 경우에 정책이 적용됩니다. LE 인증 수준의 경우 사용자의 인증 수준이 조건에 설정된 인증 수준보다 작거나 같을 경우에 정책이 적용됩니다.

3. 다음을 누릅니다.
4. 주어진 조건의 값을 정의합니다. 필드는 다음과 같습니다.

이름. 조건의 이름을 입력합니다.

인증 수준

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

인증 수준 조건은 해당 조직의 등록된 인증 모듈 수준이 아닌 다른 수준을 지정하는데 사용됩니다. 이는 다른 조직에서 인증된 사용자에게 정책을 적용할 때 유용합니다.

인증 방법

인증 방법. 폴다운 메뉴에서 조건에 대한 인증 방법을 선택합니다. 이러한 인증 방법은 조직 인증 모듈의 핵심 서비스 템플릿에서 가져옵니다.

IP 주소

보내는 / 받는 IP 주소. IP 주소의 범위를 지정합니다.

DNS 이름. DNS 이름을 지정합니다. 이 필드는 정규화된 호스트 이름이나 다음 형식의 문자열이 될 수 있습니다.

domainname

**.domainname*

시간

시작 / 끝 날짜. 날짜의 범위를 지정합니다.

시간. 하루 중 시간의 범위를 지정합니다.

요일. 요일의 범위를 지정합니다.

표준 시간대. 표준 또는 사용자 정의 표준 시간대를 지정합니다. 사용자 정의 표준 시간대는 Java 에서 구성한 표준 시간대 아이디 (예 : PST) 만 될 수 있습니다. 지정된 값이 없을 경우 기본값은 Access Manager JVM 에 설정된 표준 시간대입니다.

세션

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

세션 종료. 선택된 경우 세션 시간이 최대 세션 시간 필드에 정의된 허용되는 최대 시간을 초과하면 사용자 세션이 종료됩니다.

5. 조건을 정의한 후 마침을 누릅니다.

해당 정책에 대해 만든 모든 조건이 조건 보기의 테이블에 표시됩니다.

6. 저장을 누릅니다.

정책에서 조건을 제거하려면 조건을 선택하고 삭제를 누릅니다.

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

참조 정책 수정

Identity 관리 인터페이스를 통해 조직의 정책 정의 및 결정을 다른 조직에 위임할 수 있습니다. 또한 자원에 대한 정책 결정을 다른 정책 제품에 위임할 수도 있습니다. 참조정책은 정책 작성과 평가를 위해 이 정책 위임을 제어합니다. 참조 정책은 *규칙* 및 *참조*로 구성됩니다.

규칙을 수정하려면

1. 보기 메뉴에서 서비스를 선택합니다. 새로 만들기를 눌러 새 규칙을 추가하거나 편집 링크를 눌러 기존 규칙을 편집합니다.
2. 서비스 유형을 선택합니다. 새 규칙을 만드는 경우에는 다음을 누릅니다.
3. 규칙 필드에서 자원을 정의합니다. 필드는 다음과 같습니다.

유형. 작성할 정책의 정책 서비스를 표시합니다.

규칙 이름. 규칙의 이름을 입력합니다.

자원 이름. 자원의 이름을 입력합니다. 예를 들면 다음과 같습니다.

`http://www.sunone.com`

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

자원 이름, 포트 번호 및 프로토콜에 와일드카드가 지원됩니다.

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

특정 시스템에 설치된 모든 서버에 대해 자원을 관리할 수 있도록 하려면 자원을 `http://host*:*` 로 정의합니다. 또는 다음 자원을 정의하여 특정 조직의 관리자에게 해당 조직의 모든 서비스에 대한 권한을 부여할 수 있습니다.

`http://*.subdomain.domain.topleveldomain`

4. 마침을 누릅니다.

5. 단계 1-4 를 반복하여 추가 규칙을 만듭니다.

해당 정책에 대해 작성된 모든 규칙이 규칙 보기의 테이블에 표시됩니다.

6. 저장을 누릅니다.

정책에서 규칙을 제거하려면 규칙을 선택하고 삭제를 누릅니다.

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

참조 추가

1. 보기 메뉴에서 참조를 선택합니다. 새로 만들기를 눌러 새 참조를 추가하거나 편집 링크를 눌러 기존 참조를 편집합니다.
2. 규칙 필드에서 자원을 정의합니다. 필드는 다음과 같습니다.

참조. 현재 참조 유형을 표시합니다.

이름. 참조의 이름을 입력합니다.

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

값. 참조의 조직 이름을 선택합니다.

3. 확인을 누르고 저장을 누릅니다.

정책에서 참조를 제거하려면 참조를 선택하고 삭제를 누릅니다.

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

정책 구성 서비스

정책 구성 서비스는 Access Manager 콘솔을 통해 각 조직에 대한 정책 관련 속성을 구성하는 데 사용됩니다. 또한 Access Manager 인증 서비스와 함께 사용하기 위해 자원 이름 구현 및 Directory Server 데이터 저장소를 정의할 수 있습니다.

주제 평가 캐싱

정책 평가 성능을 향상시키려면 정책 구성 서비스의 주제 결과 수명 속성에 정의된 시간(분) 동안 주제 평가를 캐시에 저장합니다. 이렇게 캐시에 저장된 정책 결정은 주제 결과 수명 속성에 정의된 시간이 다 지날 때까지 참조됩니다. 일단 시간이 지나면 다음 번에 정책을 평가할 때 그 결정이 사용자의 변경된 상태를 반영할 것입니다(예: 사용자가 그룹에서 제거된 경우).

amldapuser 정의

amldapuser 는 LDAP 및 구성원 인증 도중 Directory Server 를 바인드하고 검색하는 데 사용되는 설치 도중 생성된 사용자이며 정책 구성 서비스에서도 사용됩니다. LDAP, 구성원 또는 정책 구성 서비스가 조직에 등록되고 나면 이 사용자의 비밀번호 (설치 도중 구성) 를 입력해야 합니다 . 자세한 내용은 *Sun Java System Access Manager Migration Guide* 를 참조하십시오 .

정책 구성 서비스 추가

정책 구성 서비스 추가는 일반적인 서비스 추가와 동일하며 Identity 관리 인터페이스 내에서 수행됩니다 . 기본적으로 정책 구성 서비스는 최상위 조직에 자동으로 추가됩니다 . 사용자가 만드는 모든 정책 서비스는 모든 조직에 추가되어야 합니다 . 정책 구성 서비스를 추가할 때마다 LDAP 바인드 비밀번호를 템플릿에 입력해야 합니다 .

정책 구성 서비스를 추가하려면

1. Identity 관리 인터페이스로 이동합니다 .

콘솔이 열릴 때 기본 인터페이스는 Identity 관리입니다 .

2. 정책을 만들려는 조직을 선택합니다 .

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

3. 보기 메뉴에서 서비스를 선택합니다 .

조직에 서비스가 이미 등록된 경우 서비스가 이동 프레임에 표시됩니다 .

4. 이동 프레임에서 추가를 누릅니다 .

이 조직에 아직 등록되지 않은 서비스 목록이 데이터 프레임에 표시됩니다 .

5. 데이터 프레임에서 열리는 서비스 추가 창에서 정책 구성을 선택하고 확인을 누릅니다 .

정책 구성 서비스가 이동 프레임의 서비스 목록에 추가됩니다 .

6. 등록 정보 화살표를 눌러 정책 서비스를 구성합니다 .

- a. 정책 템플릿이 아직 구성되지 않은 경우 새로 등록된 정책 서비스에 대한 서비스 템플릿을 만들어야 합니다 .

- b. 정책 서비스를 구성하려면 만들기를 누릅니다.
 - c. 정책 구성 속성을 수정합니다. 이러한 속성에 대한 설명은 [367 페이지의 "정책 구성 서비스 속성"](#) 을 참조하십시오.
7. 저장을 누릅니다.
- 정책 구성 서비스가 선택한 조직에 추가됩니다.

주 하위 조직은 상위 조직과 독립적으로 정책 서비스를 등록해야 합니다. 즉 하위 조직 `o=suborg, dc=sun, dc=com` 은 상위 조직 `dc=sun, dc=com` 으로부터 정책 서비스 구성을 상속 받지 않습니다.

정책 기반 자원 관리

일부 조직에서는 사용자가 액세스를 시도하는 자원에 따라 특정 모듈에 대해 인증하는 고급 인증 시나리오를 요구합니다. 정책 기반 자원 관리는 사용자가 웹 자원에 액세스하기 위해 기본 인증 모듈을 통과할 필요가 없는 Access Manager 기능입니다.

제한 사항

정책 기반 자원 관리에는 다음과 같은 제한 사항이 포함됩니다.

1. 자원에 적용할 수 있는 모든 정책은 동일한 인증 방법 또는 인증 수준을 필요로 합니다. 예를 들어, `abc.html` 이 LDAP 인증 모듈에 대한 정책에 정의되면 인증서 기반 인증 모듈에 대한 정책에는 정의될 수 없습니다.
2. 이 정책에 대해 정의될 수 있는 조건은 수준과 방법뿐입니다.
3. 이 기능은 서로 다른 DNS 도메인 사이에서는 사용할 수 없습니다.

정책 기반 자원 관리를 구성하려면

일단 Access Manager 와 정책을 설치한 후에는 정책 기반 자원 관리를 구성할 수 있습니다. 정책 기반 자원 관리를 구성하려면 Access Manager 가 게이트웨이 서버릿을 가리켜야 합니다.

1. `AMAgent.properties` 를 엽니다.
`AMAgent.properties` 는 Solaris 환경에서 `/etc/opt/SUNWam/agents/config/` 에 있습니다.

2. 다음 행을 주석으로 처리합니다 .
#com.sun.am.policy.am.loginURL =
http://identity_server_host.domain_name:port/amserver/UI/Login.
3. 다음 행을 추가합니다 .
com.sun.am.policy.am.loginURL =
http://identity_server_host.domain_name:port/amserver/gateway
4. 에이전트를 다시 시작합니다 .

인증 관리

인증 서비스는 Access Manager 배포 시 설치되는 모든 인증 모듈에 사용할 웹 기반의 사용자 인터페이스를 제공합니다. 이 인터페이스는 액세스 요청한 사용자에게 (호출된 인증 모듈에 따라) 로그인 요구 사항 화면을 표시함으로써 인증 자격 증명을 수집하는 동적 / 사용자 정의 가능 수단을 제공합니다. 이러한 인터페이스는 (경우에 따라 JATO 라고 불리는) Sun Java System™ Application Framework 를 사용하여 구축되는데 , 이는 개발자들이 기능적 웹 응용 프로그램 구축 시 사용하는 J2EE(Java 2 Enterprise Edition) 표현 프레임워크입니다 .

- [132 페이지의 " 사용자 인터페이스 로그인 URL "](#)
- [138 페이지의 " 인증 유형 "](#)
- [157 페이지의 " 인증 구성 "](#)
- [163 페이지의 " 계정 잠금 "](#)
- [165 페이지의 " 인증 서비스 페일오버 "](#)
- [166 페이지의 " 정규화된 도메인 이름 \(FQDN\) 매핑 "](#)
- [167 페이지의 " 영구 쿠키 "](#)
- [168 페이지의 " 다중 LDAP 인증 모듈 구성 "](#)
- [171 페이지의 " 세션 업그레이드 "](#)
- [171 페이지의 " 플러그 인 인터페이스 검증 "](#)
- [172 페이지의 " JAAS 공유 상태 "](#)

사용자 인터페이스 로그인 URL

인증 서비스 사용자 인터페이스는 웹 브라우저의 위치 표시줄에 로그인 URL 을 입력하는 방법으로 액세스할 수 있습니다. 다음과 같이 URL 을 입력합니다.

`http://identity_server_host.domain_name:port/service_deploy_uri/UI/Login`

주 설치 도중 `service_deploy_uri` 가 `amserver` 로 구성됩니다. 이러한 기본 서비스 배포 URL 은 이 설명서 전반에 걸쳐 사용됩니다.

사용자 인터페이스 로그인 URL 에 로그인 URL 매개 변수가 추가되어 특정 인증 방법이나 성공 또는 실패한 인증 리디렉션 URL 을 정의합니다. 리디렉션 URL 에 대한 자세한 내용은 [138 페이지의 "인증 유형"](#) 을 참조하십시오.

로그인 URL 매개 변수

URL 매개 변수는 URL 의 끝에 추가되는 이름 / 값 쌍입니다. 이 매개 변수는 물음표 (?) 로 시작되며 `name=value` 의 형식을 갖습니다. 다음과 같이 여러 개의 매개 변수를 하나의 로그인 URL 로 조합할 수 있습니다.

`http://server_name.domain_name:port/amserver/UI/Login?module=LDAP&locale=ja&goto=http://www.sun.com`

매개 변수가 둘 이상 있을 때는 앰퍼샌드 (&) 기호로 구분됩니다. 그러나 매개 변수 조합은 다음 지침을 지켜야 합니다.

- 각 매개 변수는 하나의 URL 에서 한 번만 사용되어야 합니다. 예를 들어 `module=LDAP&module=NT` 는 사용할 수 없습니다.
- `org` 매개 변수와 `domain` 매개 변수는 모두 로그인 조직을 결정합니다. 이 경우에는 로그인 URL 에서 두 매개 변수 중 하나만 사용해야 합니다. 두 매개 변수를 모두 사용하면서 우선 순위를 지정하지 않으면 하나만 적용됩니다.
- `user`, `role`, `service`, `module` 및 `authlevel` 매개 변수는 각각의 기준에 따라 인증 모듈을 정의하는 매개 변수입니다. 따라서 로그인 URL 에는 이들 중 하나만 사용해야 합니다. 매개 변수를 두 개 이상 사용하면서 우선 순위를 지정하지 않으면 하나만 적용됩니다.

다음 절에서는 사용자 인터페이스 로그인 URL 에 붙고 웹 브라우저의 위치 표시줄에 입력될 때 여러 가지 인증 기능을 수행하는 매개 변수를 설명합니다.

팁 전사적으로 배포할 인증 URL 및 매개 변수를 간소화하기 위해 관리자는 간단한 URL 을 사용하여 HTML 페이지를 구성할 수 있는데, 이 페이지에는 구성된 모든 인증 방법에서 사용할 복잡한 로그인 URL 링크가 포함됩니다.

goto 매개 변수

`goto=successful_authentication_URL` 매개 변수는 인증 구성 서비스의 로그인 성공 URL 에 정의된 값 대신 사용됩니다. 이 매개 변수는 인증이 성공하면 지정된 URL 로 연결됩니다. 마찬가지로 `goto=logout_URL` 매개 변수는 사용자 로그아웃 시 지정된 URL 로 연결하기 위해 사용됩니다. 성공적인 인증 URL 의 예는 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?goto=http://www.sun.com/homepage.html
```

`goto` 로그아웃 URL 의 예는 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Logout?goto=http://www.sun.com/logout.html
```

주 Access Manager 에서 성공적인 인증 리디렉션 URL 을 찾을 때 적용하는 우선 순위가 있습니다. 이러한 리디렉션 URL 과 그 순서는 인증 방법에 따라 다르므로 이 순서 (및 관련 정보) 에 대한 자세한 내용은 [138 페이지의 "인증 유형"](#) 을 참조하십시오.

gotoOnFail 매개 변수

`gotoOnFail=failed_authentication_URL` 매개 변수는 인증 구성 서비스의 로그인 실패 URL 에 정의된 값 대신 사용됩니다. 이 매개 변수는 사용자 인증 실패 시 지정된 URL 로 연결됩니다. `gotoOnFail` URL 의 예로

```
http://server_name.domain_name:port/amserver/UI/Login?gotoOnFail=http://www.sun.com/auth_fail.html
```

이 있습니다.

주 Access Manager 에서 실패한 인증 리디렉션 URL 을 찾을 때 적용하는 우선 순위가 있습니다. 이러한 리디렉션 URL 과 그 순서는 인증 방법에 따라 다르므로 이 순서 (및 관련 정보) 에 대한 자세한 내용은 [138 페이지의 "인증 유형"](#) 을 참조하십시오.

org 매개 변수

`org=orgName` 매개 변수를 사용하면 사용자가 지정된 조직의 사용자로서 인증할 수 있습니다.

팁	<p>아직 지정된 조직의 구성원이 아닌 사용자가 <code>org</code> 매개 변수를 사용하여 인증하려고 하면 오류 메시지가 나타납니다. 그러나 다음 사항이 모두 해당되면 Directory Server에서 사용자 프로필을 동적으로 작성할 수 있습니다.</p> <ul style="list-style-type: none">• 핵심 인증 서비스의 사용자 프로필 속성은 Dynamic 또는 Dynamic with User Alias로 설정되어야 합니다.• 사용자는 필수 모듈에 성공적으로 인증해야 합니다.• 사용자가 아직 Directory Server에 프로필이 없습니다.
----------	--

이 매개 변수를 통해 (조직 및 로케일 설정에 따라) 정확한 로그인 페이지가 표시됩니다. 이 매개 변수를 설정하지 않은 경우 기본값은 최상위 조직입니다. 예를 들어, 다음은 `org URL`이 될 수 있습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?org=sun
```

user 매개 변수

`user=userName` 매개 변수는 사용자 프로필의 사용자 인증 구성 속성에 구성된 모듈에 따라 인증을 강제 설정합니다. 예를 들어, 한 사용자의 프로필은 인증 모듈을 사용하여 인증하도록 구성하는 반면 다른 사용자는 LDAP 모듈을 사용하여 인증하도록 구성할 수 있습니다. 이 매개 변수를 추가하면 사용자의 조직에 구성된 방법이 아닌 사용자 자신이 구성한 인증 프로세스를 따르게 됩니다. 예를 들면 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?user=jsmith
```

role 매개 변수

`role=roleName` 매개 변수는 지정된 역할을 위해 구성된 인증 프로세스를 따르게 합니다. 아직 지정된 역할의 구성원이 아닌 사용자가 이 매개 변수를 사용하여 인증하려고 하면 오류 메시지가 나타납니다. 예를 들면 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?role=manager
```


locale 매개 변수

Access Manager에는 콘솔 자체는 물론 인증 프로세스에서도 현지화된 화면 (영어가 아닌 다른 언어로 번역된 화면) 을 표시하는 기능이 있습니다. `locale=localeName` 매개 변수를 사용하면 지정된 로캘이 다른 정의된 로캘보다 우선하여 적용됩니다. 로그인 로캘은 다음 위치에서 순서에 따라 구성을 검색한 후 클라이언트에 표시됩니다.

1. 로그인 URL 에서 locale 매개 변수의 값

`locale=localeName` 매개 변수의 값은 정의된 다른 로캘보다 우선하여 적용됩니다.

2. 사용자 프로필에 정의된 로캘

URL 매개 변수가 없을 때는 사용자 프로필의 사용자 기본 언어 속성에 설정된 값에 따라 로캘이 표시됩니다.

3. HTTP 헤더에 정의된 로캘

이 로캘은 웹 브라우저에서 설정합니다.

4. 핵심 인증 서비스에 정의된 로캘

이 로캘은 핵심 인증 모듈의 기본 인증 로캘 속성의 값입니다.

5. 플랫폼 서비스에 정의된 로캘

이 로캘은 플랫폼 서비스에서 플랫폼 로캘 속성의 값입니다.

6. 운영 체제 로캘

여기서 파생된 로캘은 사용자의 세션 토큰에 저장되며 Access Manager에서는 현지화된 인증 모듈을 로드할 때만 이를 사용합니다. 인증이 성공적으로 수행되면 사용자 프로필의 기본 언어 속성에 정의된 로캘이 사용됩니다. 아무 것도 설정되어 있지 않을 때는 인증에 사용된 로캘이 적용됩니다. 예를 들면 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?locale=ja
```

주

화면 텍스트와 오류 메시지를 현지화하는 방법에 대한 자세한 내용은 **Access Manager Developer's Guide** 를 참조하십시오.

module 매개 변수

`module=moduleName` 매개 변수를 사용하면 지정된 인증 모듈을 통해 인증할 수 있습니다. 모든 인증 모듈은 먼저 사용자가 속한 조직에서 등록되고 핵심 인증 모듈에서 해당 조직의 인증 모듈 중 하나로 선택되어야 지정될 수 있습니다. 예를 들면 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?module=Unix
```

주 URL 매개 변수에서 사용되는 인증 모듈 이름은 대소문자를 구분합니다.

service 매개 변수

`service=serviceName` 매개 변수를 사용하면 서비스의 구성된 인증 스키마를 통해 인증할 수 있습니다. 인증 구성 서비스를 사용하여 서비스마다 인증 스키마를 달리 구성할 수 있습니다. 예를 들어, 조직의 직원 디렉토리 응용 프로그램은 LDAP 인증 모듈만 필요한 반면 온라인 급여 응용 프로그램은 더 안전한 인증서 인증 모듈을 사용하여 인증해야 합니다. 이러한 서비스마다 인증 스키마를 구성하고 이름을 지정할 수 있습니다. 예를 들면 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?service=sv1
```

주 인증 구성 서비스는 서비스 기반의 인증을 위한 스키마 정의에 사용됩니다.

arg 매개 변수

`arg=newsession` 매개 변수는 사용자의 현재 세션을 끝내고 새 세션을 시작할 때 사용됩니다. 인증 서비스는 하나의 요청으로 사용자의 기존 세션 토큰을 삭제하고 새 로그인을 수행합니다. 이 옵션은 일반적으로 익명 인증 모듈에서 사용됩니다. 사용자는 먼저 익명 세션으로 인증한 다음 등록이나 로그인 링크를 누릅니다. 예를 들면 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?arg=newsession
```

authlevel 매개 변수

authlevel=*value* 매개 변수는 인증 수준이 인증 서비스에게 지정된 인증 수준 값보다 크거나 같은 모듈을 호출하도록 명령합니다. 각 인증 모듈은 고정된 정수 인증 수준으로 정의됩니다. 예를 들면 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?authlevel=1
```

주 인증 수준은 모듈별 프로필에 설정되어 있습니다. 이 모듈에 대한 자세한 내용은 *Sun Java System Access Manager 관리 설명서*를 참조하십시오.

domain 매개 변수

이 매개 변수를 사용하면 지정된 도메인으로 식별된 조직에 로그인할 수 있습니다. 지정된 도메인은 조직 프로필의 도메인 이름 속성에 정의된 값과 일치해야 합니다. 예를 들면 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?domain=sun.com
```

팁 아직 지정된 도메인 / 조직의 구성원이 아닌 사용자는 org 매개 변수를 사용하여 인증하려고 하는 경우 오류 메시지가 나타납니다. 그러나 다음 사항이 모두 해당되면 Directory Server에서 사용자 프로필을 동적으로 작성할 수 있습니다.

- 핵심 인증 서비스의 사용자 프로필 속성은 Dynamic 또는 Dynamic With User Alias. 로 설정되어야 합니다.
- 사용자는 필수 모듈에 성공적으로 인증해야 합니다.
- 사용자가 아직 Directory Server에 프로필이 없습니다.

iPSPCookie 매개 변수

iPSPCookie=yes 매개 변수를 사용하면 영구 쿠키를 사용하여 로그인할 수 있습니다. 영구 쿠키는 브라우저 창을 닫은 후에도 계속 존재하는 쿠키를 말합니다. 이 매개 변수를 사용하기 위해서는 사용자가 로그인한 조직의 영구 쿠키가 핵심 인증 모듈에서 활성화되어 있어야 합니다. 사용자가 인증하고 브라우저를 닫은 후에는 다시 인증할 필요 없이 새 브라우저 세션으로 로그인할 수 있고 콘솔로 직접 이동합니다. 이러한 작업은 핵심 서비스에 지정된 영구 쿠키 최대 시간의 값이 경과할 때까지 가능합니다. 예를 들면 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?org=example&iPSPCookie=yes
```

IDTokenN 매개 변수

이 매개 변수 옵션을 사용하면 URL 또는 HTML 형식으로 인증 자격 증명을 통과할 수 있습니다. IDTokenN=*value* 매개 변수를 사용하는 경우 **인증 서비스 사용자 인터페이스**에 액세스하지 않고도 인증할 수 있습니다. 이러한 프로세스를 *0 페이지 로그인*이라고 합니다. 0 페이지 로그인 은 하나의 로그인 페이지를 사용하는 인증 모듈에서만 작동합니다. IDToken0, IDToken1, ..., IDTokenN 값은 인증 모듈의 로그인 페이지에 있는 필드에 매핑됩니다. 예를 들어 LDAP 인증 모듈은 userID 정보에 IDToken1 을 사용하고 비밀번호 정보에 IDToken2 를 사용할 수 있습니다. 이 경우 LDAP 모듈 IDTokenN URL 은 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?module=LDAP&IDToken1
=userID&IDToken2=password
```

LDAP 가 기본 인증 모듈인 경우 module=LDAP 는 생략될 수 있습니다.

익명 인증의 경우 로그인 URL 매개 변수는 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?module=Anonymous&IDT
oken1=anonymousUserID
```

주 (이전 릴리스에서 사용하던) 토큰 이름 Login.Token0, Login.Token1, ..., Login.TokenN은 아직 지원되고 있지만, 향후 릴리스에서는 지원되지 않을 것입니다. 새로 제공되는 IDTokenN 매개 변수를 사용하는 것이 좋습니다.

인증 유형

인증 서비스는 여러 가지 인증 적용 방법을 제공합니다. 이러한 여러 가지 인증 방법은 로그인 URL 매개 변수를 지정하거나 인증 프로그래밍 인터페이스를 통해 적용할 수 있습니다. 인증 모듈을 구성하기 전에 특정 인증 모듈 이름을 포함하도록 핵심 인증 서비스 속성인 조직 인증 모듈을 수정해야 합니다.

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

- 141 페이지의 "조직 기반 인증"
- 143 페이지의 "역할 기반 인증"
- 147 페이지의 "서비스 기반 인증"
- 150 페이지의 "사용자 기반 인증"
- 152 페이지의 "인증 수준 기반 인증"
- 155 페이지의 "모듈 기반 인증"

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

인증 유형에 따른 액세스 결정 방법

이러한 방법마다 사용자 인증이 성공하기도하고, 실패하기도 합니다. 그러나 방법이 결정된 다음에는 다음 절차를 따르게 됩니다. 단계 1 부터 단계 3 까지는 인증 성공 후, 단계 4 는 인증 성공 및 실패 후에 모두 나타납니다.

1. Access Manager 에서는 인증된 사용자가 Directory Server 데이터 저장소에 정의되었는지 그리고 프로필이 활성화 상태인지를 확인합니다.

핵심 인증 모듈의 사용자 프로필 속성은 Required, Dynamic, Dynamic with User Alias 또는 Ignored 중 하나로 정의될 수 있습니다. 성공적인 인증에 따라 Access Manager 는 인증된 사용자가 Directory Server 데이터 저장소에 정의되어 있는지를 확인하고 사용자 프로필 값이 Required 인 경우에는 해당 프로필이 활성화 상태인지 확인합니다 (기본적인 경우). 사용자 프로필이 Dynamically Configured 인 경우에는 인증 서비스에서 Directory Server 데이터 저장소에 사용자 프로필을 작성합니다. 사용자 프로필이 Ignore 로 설정되어 있으면 사용자 검증이 수행되지 않습니다.

2. 인증 사후 처리 SPI 의 실행이 완료되었습니다.

핵심 인증 모듈에는 인증 사후 처리 클래스 이름이 그 값으로서 포함되는 인증 사후 처리 클래스 속성이 들어 있습니다. AMPostAuthProcessInterface 는 사후 처리 인터페이스로서 인증 성공 / 실패 시 또는 로그아웃 시 실행될 수 있습니다.

3. 다음 등록 정보가 세션 토큰에 추가되거나 세션 토큰에서 업데이트된 후 사용자의 세션이 활성화됩니다.

Organization. 사용자가 속한 조직의 DN 입니다.

Principal. 사용자의 DN 입니다.

Principals. 사용자가 인증한 이름의 목록입니다 (둘 이상의 값이 세로줄 (|) 로 구분된 목록 포함 가능).

UserId. 모듈에서 반환하는 사용자의 DN 이거나 LDAP 또는 구성원 이외의 모듈의 경우 사용자 이름입니다. 모든 Principal 은 같은 사용자로 매핑되어야 합니다. UserID 는 Principal 이 매핑되는 사용자 DN 입니다.

주 이 등록 정보는 DN 이 아닌 값이 될 수 있습니다 .

UserToken. 사용자 이름입니다 . 모든 Principal 은 같은 사용자로 매핑되어야 합니다 . UserToken 은 Principal 이 매핑된 사용자 이름입니다 .

Host. 클라이언트의 호스트 이름이나 IP 주소입니다 .

authLevel. 사용자의 최고 인증 수준입니다 .

AuthType. 사용자가 인증한 인증 모듈을 세로줄 (|) 로 구분한 목록 (예 : module1|module2|module3) 입니다 .

clientType. 클라이언트 브라우저의 장치 유형입니다 .

Locale. 클라이언트의 로캘입니다 .

CharSet. 클라이언트에 대해 결정된 문자 집합입니다 .

Role. 역할 기반의 인증에만 적용될 수 있으며 사용자가 속한 역할입니다 .

Service. 서비스 기반의 인증에만 적용될 수 있으며 사용자가 속한 서비스입니다 .

loginURL. 클라이언트의 로그인 URL 입니다 .

4. Access Manager 에서는 인증 성공 또는 실패 후 사용자를 리디렉션할 위치에 대한 정보를 찾습니다 .

URL 리디렉션은 Access Manager 페이지나 URL 로 수행할 수 있습니다 . 리디렉션은 Access Manager 가 인증 방법을 기준으로 찾은 리디렉션의 우선 순위 순서와 해당 인증이 성공 또는 실패했는지 여부에 따라 달라집니다 . 이러한 순서는 다음 인증 방법 절에서 URL 리디렉션 부분에 자세히 설명되어 있습니다 .

URL 리디렉션

인증 구성 서비스에서 성공적인 인증 또는 실패한 인증에 대한 URL 리디렉션을 할당할 수 있습니다 . URL 은 이 서비스의 로그인 성공 URL 및 로그인 실패 URL 속성에 자동으로 정의됩니다 . URL 리디렉션을 사용 가능하게 하려면 조직에 인증 구성 서비스를 추가하여 해당 서비스를 역할 , 조직 또는 사용자에게 대해 구성 가능하게 만들어야 합니다 . 인증 구성 서비스를 추가할 경우 LDAP - 필수와 같은 인증 모듈을 추가해야 합니다 . 세부 사항에 대해서는 [157 페이지의 " 인증 구성 "](#) 을 참조하십시오 .

조직 기반 인증

이 인증 방법을 사용하면 조직 또는 하위 조직에 인증할 수 있습니다. 이는 Access Manager의 기본 인증 방법입니다. 조직 인증 방법은 핵심 인증 모듈을 조직에 등록하고 조직 인증 구성 속성을 정의함으로써 설정됩니다.

조직 기반 인증 로그인 URL

인증 조직은 사용자 인터페이스 로그인 URL에서 org 매개 변수나 domain 매개 변수를 정의하는 방법으로 지정할 수 있습니다. 인증 요청 조직은 (여기에 표시된 순서대로) 다음 매개 변수 / 속성에 의해 결정됩니다.

1. domain 매개 변수
2. org 매개 변수
3. 관리 서비스의 DNS Alias Names(조직 별칭 이름) 속성

조직을 정확하게 호출한 다음에는 사용자가 인증할 인증 모듈을 핵심 인증 서비스의 조직 인증 구성 속성에서 검색합니다. 조직 기반 인증을 지정하고 초기화하는 데 사용되는 URL은 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login
```

```
http://server_name.domain_name:port/amserver/UI/Login?domain=domain_name
```

```
http://server_name.domain_name:port/amserver/UI/Login?org=org_name
```

정의된 매개 변수가 없을 때는 로그인 URL에 지정된 서버 호스트와 도메인으로부터 조직이 결정됩니다.

조직 기반 인증 리디렉션 URL

조직 기반 인증이 성공 / 실패했다면 Access Manager는 사용자를 리디렉션할 위치 정보를 찾습니다. 응용 프로그램에서 이러한 정보를 찾는 순서는 다음과 같습니다.

성공한 조직 기반 인증 리디렉션 URL

성공한 조직 기반 인증의 리디렉션 URL은 다음 정보를 순서대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL
2. goto 로그인 URL 매개 변수에서 설정한 URL
3. 사용자 프로필 (amUser.xml)의 iplanet-am-user-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL

4. 사용자의 역할 항목의 `iplanet-am-auth-login-success-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
5. 사용자 조직 항목의 `iplanet-am-auth-login-success-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
6. `iplanet-am-auth-login-success-url` 속성에 대해 전역 기본값으로 `clientType` 사용자 정의 파일에서 설정된 URL
7. 사용자 프로필 (`amUser.xml`)의 `iplanet-am-user-success-url` 속성에 설정된 URL
8. 사용자 역할 항목의 `iplanet-am-auth-login-success-url` 속성에 설정된 URL
9. 사용자 조직 항목의 `iplanet-am-auth-login-success-url` 속성에 설정된 URL
10. 전역 기본값으로서 `iplanet-am-auth-login-success-url` 속성에 설정된 URL

실패한 조직 기반 인증 리디렉션 URL

실패한 조직 기반 인증의 리디렉션 URL 은 다음 장소를 순서대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL
2. `gotoOnFail` 로그인 URL 매개 변수에서 설정한 URL
3. 사용자 항목 (`amUser.xml`)의 `iplanet-am-user-failure-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
4. 사용자 역할 항목의 `iplanet-am-auth-login-failure-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
5. 사용자 조직 항목의 `iplanet-am-auth-login-failure-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
6. `iplanet-am-auth-login-failure-url` 속성에 대해 전역 기본값으로서 `clientType` 사용자 정의 파일에서 설정된 URL
7. 사용자 항목 (`amUser.xml`)의 `iplanet-am-user-failure-url` 속성에 설정된 URL
8. 사용자 역할 항목의 `iplanet-am-auth-login-failure-url` 속성에 설정된 URL
9. 사용자 조직 항목의 `iplanet-am-auth-login-failure-url` 속성에 설정된 URL
10. `iplanet-am-auth-login-failure-url` 속성에서 전역 기본값으로서 설정된 URL

조직 기반 인증 구성

먼저 핵심 인증 서비스를 조직에 추가하여 조직에 인증 모듈을 설정합니다.

조직의 인증 속성을 구성하려면 다음을 수행합니다.

1. 인증 속성을 구성할 조직으로 이동합니다.
2. 보기 메뉴에서 서비스를 선택합니다.
3. 서비스 목록에서 핵심 등록 정보 화살표를 누릅니다.
핵심 인증 속성이 데이터 창에 표시됩니다.
4. 관리자 인증자 속성 옆에 있는 편집을 누릅니다. 여기서는 관리자에 대해서만 인증 서비스를 정의할 수 있습니다. 관리자의 인증 모듈이 최종 사용자의 모듈과 달라야 하는 경우 이 속성을 사용할 수 있습니다. 기본 인증 모듈은 LDAP입니다.

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

5. 조직 인증 구성 속성 옆에 있는 편집 링크를 누릅니다. 여기서는 조직 내의 모든 사용자에게 대한 인증 모듈을 정의할 수 있습니다. 기본 인증 모듈은 LDAP입니다.
6. 인증 서비스를 정의했으면 저장을 눌러 변경 내용을 저장한 다음 단기를 눌러 조직의 핵심 인증 속성으로 돌아갑니다.

역할 기반 인증

이 인증 방법을 사용하면 조직이나 하위 조직 내의 (정적 또는 필터링된) 역할에 인증할 수 있습니다.

주 인증 구성 서비스를 역할의 인스턴스로 등록하기 전에 먼저 조직에 등록해야 합니다.

인증이 성공하려면 사용자는 해당 역할에 속하고 이 역할에 구성된 인증 구성 서비스 인스턴스에 정의된 모듈마다 인증해야 합니다. 역할 기반 인증의 인스턴스마다 다음 속성을 지정할 수 있습니다.

충돌 해결 수준. 같은 사용자의 서로 다른 역할에 정의된 인증 구성 서비스 인스턴스에 대해 우선 순위 수준을 설정합니다. 예를 들어, User1 이 Role1 및 Role2에 모두 지정되고 Role1에 더 높은 충돌 해결 수준이 설정될 경우 사용자가 인증을 시도할 때 성공 또는 실패 리디렉션과 인증 사후 프로세스에 대해 Role1에 더 높은 우선 순위가 적용됩니다.

인증 구성 . 역할의 인증 프로세스에 구성된 인증 모듈을 정의합니다 .

로그인 성공 URL . 성공한 인증에서 사용자가 리디렉션될 URL 을 정의합니다 .

로그인 실패 URL . 실패한 인증에서 사용자가 리디렉션될 URL 을 정의합니다 .

인증 사후 처리 클래스 . 인증 사후 인터페이스를 정의합니다 .

역할 기반 인증 로그인 URL

역할 기반 인증은 role 매개 변수를 정의하는 방법으로 사용자 인터페이스 로그인 URL 에서 지정할 수 있습니다 . 역할을 정확하게 호출한 다음에는 사용자가 인증할 인증 모듈을 해당 역할에 대해 정의된 인증 구성 서비스 인스턴스에서 검색합니다 .

이 역할 기반 인증을 지정하고 초기화하는 데 사용되는 URL 은 다음과 같습니다 .

```
http://server_name.domain_name:port/amserver/UI/Login?role=role_name
```

```
http://server_name.domain_name:port/amserver/UI/Login?org=org_name&role=role_name
```

org 매개 변수가 구성되어 있지 않은 경우 , 역할이 속한 조직은 로그인 URL 자체에 지정된 서버 호스트와 도메인으로 결정됩니다 .

역할 기반 인증 리디렉션 URL

역할 기반 인증 성공 / 실패 시 Access Manager 에서 사용자를 리디렉션할 위치에 대한 정보를 찾습니다. 응용 프로그램에서 이러한 정보를 찾는 순서는 다음과 같습니다.

성공한 역할 기반 인증 리디렉션 URL

성공한 역할 기반 인증의 리디렉션 URL 은 다음 장소를 순서대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL
2. goto 로그인 URL 매개 변수에서 설정한 URL
3. 사용자 프로필 (amUser.xml) 의 iplanet-am-user-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
4. 사용자가 인증한 역할의 iplanet-am-auth-login-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
5. 인증된 사용자의 다른 역할 항목의 iplanet-am-auth-login-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL(이전 리디렉션 URL 이 실패할 경우 이 옵션은 폴백임)
6. 사용자 조직 항목의 iplanet-am-auth-login-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
7. iplanet-am-auth-login-success-url 속성에 대해 전역 기본값으로서 clientType 사용자 정의 파일에서 설정된 URL
8. 사용자 프로필 (amUser.xml) 의 iplanet-am-user-success-url 속성에 설정된 URL
9. 사용자가 인증한 역할의 iplanet-am-auth-login-success-url 속성에 설정된 URL
10. 인증된 사용자의 다른 역할 항목의 iplanet-am-auth-login-success-url 속성에 설정된 URL(이전 리디렉션 URL 이 실패할 경우 이 옵션은 폴백임)
11. 사용자 조직 항목의 iplanet-am-auth-login-success-url 속성에 설정된 URL
12. 전역 기본값으로서 iplanet-am-auth-login-success-url 속성에 설정된 URL

실패한 역할 기반 인증 리디렉션 URL

실패한 역할 기반 인증의 리디렉션 URL 은 다음 장소를 순서대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL
2. goto 로그인 URL 매개 변수에서 설정한 URL
3. 사용자 프로필 (amUser.xml) 의 iplanet-am-user-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
4. 사용자가 인증한 역할의 iplanet-am-auth-login-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
5. 인증된 사용자의 다른 역할 항목의 iplanet-am-auth-login-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL(이전 리디렉션 URL 이 실패할 경우 이 옵션은 폴백임)
6. 사용자 조직 항목의 iplanet-am-auth-login-failure-url 에 대해 clientType 사용자 정의 파일에서 설정된 URL
7. iplanet-am-auth-login-failure-url 속성에 대해 전역 기본값으로서 clientType 사용자 정의 파일에서 설정된 URL
8. 사용자 프로필 (amUser.xml) 의 iplanet-am-user-failure-url 속성에 설정된 URL
9. 사용자가 인증한 역할의 iplanet-am-auth-login-failure-url 속성에 설정된 URL
10. 인증된 사용자의 다른 역할 항목의 iplanet-am-auth-login-failure-url 속성에 설정된 URL(이전 리디렉션 URL 이 실패할 경우 이 옵션은 폴백임)
11. 사용자 조직 항목의 iplanet-am-auth-login-failure-url 속성에 설정된 URL
12. 전역 기본값으로서 iplanet-am-auth-login-failure-url 속성에 설정된 URL

역할 기본 인증 구성

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

1. 인증 속성을 구성할 조직으로 이동합니다.
2. 보기 메뉴에서 역할을 선택합니다.
3. 인증 구성을 설정할 역할을 선택하고 등록 정보 화살표를 누릅니다.
역할의 등록 정보가 데이터 창에 표시됩니다.
4. 데이터 창의 보기 메뉴에서 서비스를 선택합니다.

5. 필요한 경우 인증 구성 속성을 수정합니다. 이러한 속성에 대한 설명은 33 장, **“[확실히 구성 서비스 속성](#)”**에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다.
6. 저장을 누릅니다.

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

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

서비스 기반 인증

이 인증 방법을 사용하면 조직 또는 하위 조직에 등록된 특정 서비스나 응용 프로그램에 인증할 수 있습니다. 이러한 서비스는 인증 구성 서비스 내에 서비스 인스턴스로 구성되고 인스턴스 이름과 연관됩니다. 인증이 성공하려면 사용자는 해당 서비스에 구성된 인증 구성 서비스 인스턴스에 정의된 모듈마다 인증해야 합니다. 서비스 기반 인증의 인스턴스마다 다음 속성을 지정할 수 있습니다.

인증 구성. 서비스의 프로세스에 구성된 인증 모듈을 정의합니다.

로그인 성공 URL. 성공한 인증에서 사용자가 리디렉션될 URL 을 정의합니다.

로그인 실패 URL. 실패한 인증에서 사용자가 리디렉션될 URL 을 정의합니다.

인증 사후 처리 클래스. 인증 사후 인터페이스를 정의합니다.

서비스 기반 인증 로그인 URL

서비스 기반 인증은 `service` 매개 변수를 정의하는 방법으로 사용자 인터페이스 로그인 URL 에서 지정할 수 있습니다. 서비스를 호출한 다음에는 해당 서비스에 대해 정의된 인증 구성 서비스로부터 사용자가 인증할 인증 모듈을 검색합니다.

서비스 기반 인증을 지정하고 초기화하는 데 사용되는 URL 은 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?service=service_name
```

및

```
http://server_name.domain_name:port/amserver/UI/Login?org=org_name&service=service_name
```

`org` 매개 변수를 지정하지 않은 경우에는 로그인 URL 자체에 지정된 서버 호스트와 도메인으로부터 조직이 결정됩니다.

서비스 기반 인증 리디렉션 URL

서비스 기반 인증 성공 / 실패 시 Access Manager 에서 사용자를 리디렉션할 위치에 대한 정보를 찾습니다. 응용 프로그램에서 이 정보를 찾는 순서는 다음과 같습니다.

성공한 서비스 기반 인증 리디렉션 URL

성공한 서비스 기반 인증의 리디렉션 URL 은 다음 장소를 순서대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL
2. goto 로그인 URL 매개 변수에서 설정한 URL
3. 사용자 프로필 (amUser.xml) 의 iplanet-am-user-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
4. 사용자가 인증한 서비스의 iplanet-am-auth-login-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
5. 사용자 역할 항목의 iplanet-am-auth-login-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
6. 사용자 조직 항목의 iplanet-am-auth-login-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
7. iplanet-am-auth-login-success-url 속성에 대해 전역 기본값으로서 clientType 사용자 정의 파일에서 설정된 URL
8. 사용자 프로필 (amUser.xml) 의 iplanet-am-user-success-url 속성에 설정된 URL
9. 사용자가 인증한 서비스의 iplanet-am-auth-login-success-url 속성에 설정된 URL
10. 사용자 역할 항목의 iplanet-am-auth-login-success-url 속성에 설정된 URL
11. 사용자 조직 항목의 iplanet-am-auth-login-success-url 속성에 설정된 URL
12. 전역 기본값으로서 iplanet-am-auth-login-success-url 속성에 설정된 URL

실패한 서비스 기반 인증 리디렉션 URL

실패한 서비스 기반 인증의 리디렉션 URL 은 다음 장소를 순서대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL
2. goto 로그인 URL 매개 변수에서 설정한 URL

3. 사용자 프로필 (amUser.xml) 의 iplanet-am-user-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
4. 사용자가 인증한 서비스의 iplanet-am-auth-login-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
5. 사용자 역할 항목의 iplanet-am-auth-login-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
6. 사용자 조직 항목의 iplanet-am-auth-login-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
7. iplanet-am-auth-login-failure-url 속성에 대해 전역 기본값으로서 clientType 사용자 정의 파일에서 설정된 URL
8. 사용자 프로필 (amUser.xml) 의 iplanet-am-user-failure-url 속성에 설정된 URL
9. 사용자가 인증한 서비스의 iplanet-am-auth-login-failure-url 속성에 설정된 URL
10. 사용자 역할 항목의 iplanet-am-auth-login-failure-url 속성에 설정된 URL
11. 사용자 조직 항목의 iplanet-am-auth-login-failure-url 속성에 설정된 URL
12. 전역 기본값으로서 iplanet-am-auth-login-failure-url 속성에 설정된 URL

서비스 기반 인증을 구성하려면

인증 구성 서비스를 추가한 다음 서비스에 대한 인증 모듈을 설정합니다. 수행 방법은 다음과 같습니다.

1. Identity 관리 모듈의 보기 메뉴에서 서비스를 선택합니다.
 추가된 서비스 목록이 표시됩니다. 인증 구성 서비스가 추가되지 않으면 아래 단계를 계속합니다. 서비스가 추가되면 단계 4 로 이동합니다.
2. 이동 창에서 추가를 누릅니다.
 사용 가능한 서비스 목록이 데이터 창에 표시됩니다.
3. 인증 구성 확인란을 선택하고 추가를 누릅니다.
 인증 구성 서비스가 이동 창에 표시되며 관리자는 이를 통해 해당 서비스가 추가되었음을 확인할 수 있습니다.
4. 인증 구성 등록 정보 화살표를 누릅니다.
 서비스 인스턴스 목록이 데이터 창에 표시됩니다.
5. 인증 모듈을 구성할 서비스 인스턴스를 누릅니다.

- 인증 구성 속성을 수정하고 저장을 누릅니다. 이러한 속성에 대한 설명은 33 장, **확정 구성 서비스 속성**에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다.

사용자 기반 인증

이 인증 방법을 사용하면 사용자에게 대해 특별히 구성된 인증 프로세스를 인증할 수 있습니다. 이 프로세스는 사용자 프로필의 사용자 인증 구성 속성 값으로 구성됩니다. 인증이 성공하려면 정의된 모듈마다 인증해야 합니다.

사용자 기반 인증 로그인 URL

사용자 기반 인증은 사용자 인터페이스 로그인 URL에서 `user` 매개 변수를 정의하는 방법으로 지정할 수 있습니다. 사용자를 정확하게 호출한 다음에는 사용자가 인증할 인증 모듈을 정의된 사용자 인증 구성 인스턴스에서 검색합니다.

이 사용자 기반 인증을 지정하고 초기화하는 데 사용되는 URL 은 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?user=user_name
```

```
http://server_name.domain_name:port/amserver/UI/Login?org=org_name&user=user_name
```

`org` 매개 변수를 지정하지 않은 경우, 역할이 속한 조직은 로그인 URL 자체에 지정된 서버 호스트와 도메인에서 결정됩니다.

사용자 별칭 목록 속성

사용자 기반 인증에 대한 요청을 받으면 인증 서비스에서는 먼저 사용자가 유효한 사용자인지 확인하고 그에 대한 인증 구성 데이터를 검색합니다. 사용자 로그인 URL 매개 변수 값과 관련하여 유효한 사용자 프로필이 둘 이상 있는 경우에는 모든 프로필이 지정된 사용자에게 매핑되어야 합니다. 사용자 프로필의 사용자 별칭 속성 (`iplanet-am-user-alias-list`)은 해당 사용자에게 속한 다른 프로필을 정의할 수 있는 위치입니다. 매핑이 실패하면 사용자는 유효한 세션에서 거부됩니다. 사용자 중 하나가 최상위 관리자이기 때문에 사용자 매핑 검증이 수행되지 않고 사용자가 슈퍼 관리자 권한을 가진 경우는 예외가 될 수 있습니다.

사용자 기반 인증 리디렉션 URL

사용자 기반 인증 성공 / 실패 시 **Access Manager**에서 사용자를 리디렉션할 위치에 대한 정보를 찾습니다. 응용 프로그램에서 이 정보를 찾는 순서는 다음과 같습니다.

성공한 사용자 기반 인증 리디렉션 URL

성공한 사용자 기반 인증의 리디렉션 URL 은 다음 장소를 순서대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL
2. goto 로그인 URL 매개 변수에서 설정한 URL
3. 사용자 프로필 (amUser.xml) 의 iplanet-am-user-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
4. 사용자의 역할 항목의 iplanet-am-auth-login-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
5. 사용자 조직 항목의 iplanet-am-auth-login-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
6. iplanet-am-auth-login-success-url 속성에 대해 전역 기본값으로서 clientType 사용자 정의 파일에서 설정된 URL
7. 사용자 프로필 (amUser.xml) 의 iplanet-am-user-success-url 속성에 설정된 URL
8. 사용자 역할 항목의 iplanet-am-auth-login-success-url 속성에 설정된 URL
9. 사용자 조직 항목의 iplanet-am-auth-login-success-url 속성에 설정된 URL
10. 전역 기본값으로서 iplanet-am-auth-login-success-url 속성에 설정된 URL

실패한 사용자 기반 인증 리디렉션 URL

실패한 사용자 기반 인증의 리디렉션 URL 은 다음 장소를 순서대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL
2. gotoOnFail 로그인 URL 매개 변수에서 설정한 URL
3. 사용자 항목 (amUser.xml) 의 iplanet-am-user-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
4. 사용자 역할 항목의 iplanet-am-auth-login-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
5. 사용자 조직 항목의 iplanet-am-auth-login-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
6. iplanet-am-auth-login-failure-url 속성에 대해 전역 기본값으로서 clientType 사용자 정의 파일에서 설정된 URL

7. 사용자 항목 (amUser.xml) 의 iplanet-am-user-failure-url 속성에 설정된 URL
8. 사용자 역할 항목의 iplanet-am-auth-login-failure-url 속성에 설정된 URL
9. 사용자 조직 항목의 iplanet-am-auth-login-failure-url 속성에 설정된 URL
10. 전역 기본값으로서 iplanet-am-auth-login-failure-url 속성에 설정된 URL

사용자 기반 인증을 구성하려면

1. Identity 관리 모듈의 보기 메뉴에서 사용자를 선택합니다.
사용자 목록이 이동 창에 표시됩니다.
2. 수정할 사용자를 선택하고 등록 정보 화살표를 누릅니다.
사용자 프로필이 데이터 창에 표시됩니다.

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

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

인증 수준 기반 인증

각 인증 모듈에 해당 인증 수준에 대한 정수 값을 연결할 수 있습니다. 서비스 구성에서 인증 모듈의 등록 정보 화살표를 누르고 모듈의 인증 수준 속성에 해당하는 값을 변경하여 인증 수준을 할당할 수 있습니다. 높은 인증 수준은 사용자가 하나 또는 여러 인증 모듈에 인증을 얻은 후에 사용자에게 높은 신뢰도를 정의합니다.

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

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

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

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

인증 수준이 `auth_level_value`보다 크거나 같은 모든 모듈은 사용자가 선택할 인증 메뉴로 표시됩니다. 일치하는 모듈이 하나이면 이 인증 모듈에 대한 인증 페이지가 직접 표시됩니다.

이 인증 방법을 사용하면 관리자가 ID 로 인증할 수 있는 모듈의 보안 수준을 지정할 수 있습니다. 인증 모듈마다 별도의 인증 수준 속성이 있고 이 속성의 값은 유효한 정수로 정의될 수 있습니다. 인증 수준 기반 인증을 사용하면 인증 서비스에서 인증 모듈을 포함하는 메뉴가 있는 모듈 로그인 페이지를 표시하는데, 이 인증 모듈의 인증 수준은 로그인 URL 매개 변수에서 지정한 값보다 크거나 같습니다. 사용자는 제시된 목록에서 모듈을 선택할 수 있습니다. 모듈을 선택하면 나머지 프로세스는 모듈 기반 인증에 따라 진행됩니다.

인증 수준 기반 인증 로그인 URL

인증 수준 기반 인증은 `authlevel` 매개 변수를 정의하는 방법으로 사용자 인터페이스 로그인 URL 에서 지정할 수 있습니다. 관련된 모듈 목록이 있는 로그인 화면을 호출한 후 사용자는 인증할 모듈을 하나 선택해야 합니다. 인증 수준 기반 인증을 지정하고 초기화하는 데 사용되는 URL 은 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?authlevel=authentication_level
```

및

```
http://server_name.domain_name:port/amserver/UI/Login?org=org_name&authlevel=authentication_level
```

`org` 매개 변수를 지정하지 않은 경우, 사용자가 속한 조직은 로그인 URL 자체에 지정된 서버 호스트와 도메인으로부터 결정됩니다.

인증 수준 기반 인증 리디렉션 URL

인증 수준 기반 인증 성공 / 실패 시 Access Manager 에서 사용자를 리디렉션할 위치에 대한 정보를 찾습니다. 응용 프로그램에서 이 정보를 찾는 순서는 다음과 같습니다.

성공한 인증 수준 기반 인증 리디렉션 URL

성공한 인증 수준 기반 인증의 리디렉션 URL 은 다음 장소를 순서대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL
2. goto 로그인 URL 매개 변수에서 설정한 URL
3. 사용자 프로필 (amUser.xml) 의 iplanet-am-user-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
4. 사용자 역할 항목의 iplanet-am-auth-login-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
5. 사용자 조직 항목의 iplanet-am-auth-login-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
6. iplanet-am-auth-login-success-url 속성에 대해 전역 기본값으로서 clientType 사용자 정의 파일에서 설정된 URL
7. 사용자 프로필 (amUser.xml) 의 iplanet-am-user-success-url 속성에 설정된 URL
8. 사용자 역할 항목의 iplanet-am-auth-login-success-url 속성에 설정된 URL
9. 사용자 조직 항목의 iplanet-am-auth-login-success-url 속성에 설정된 URL
10. 전역 기본값으로서 iplanet-am-auth-login-success-url 속성에 설정된 URL

실패한 인증 수준 인증 리디렉션 URL

실패한 인증 수준 기반 인증의 리디렉션 URL 은 다음 장소를 순서대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL
2. gotoOnFail 로그인 URL 매개 변수에서 설정한 URL
3. 사용자 항목 (amUser.xml) 의 iplanet-am-user-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
4. 사용자 역할 항목의 iplanet-am-auth-login-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
5. 사용자 조직 항목의 iplanet-am-auth-login-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
6. iplanet-am-auth-login-failure-url 속성에 대해 전역 기본값으로서 clientType 사용자 정의 파일에서 설정된 URL

7. 사용자 항목 (amUser.xml) 의 `iplanet-am-user-failure-url` 속성에 설정된 URL
8. 사용자 역할 항목의 `iplanet-am-auth-login-failure-url` 속성에 설정된 URL
9. 사용자 조직 항목의 `iplanet-am-auth-login-failure-url` 속성에 설정된 URL
10. 전역 기본값으로서 `iplanet-am-auth-login-failure-url` 속성에 설정된 URL

모듈 기반 인증

다음 구문을 사용하여 특정 인증 모듈에 액세스할 수 있습니다.

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

인증 모듈에 액세스하기 전에 인증 모듈 이름을 포함하도록 핵심 인증 서비스 속성인 조직 인증 모듈을 수정해야 합니다. 인증 모듈 이름이 이 속성에 없으면 사용자가 인증하려고 시도할 때 "인증 모듈이 거부되었습니다" 라는 페이지가 표시됩니다.

이 인증 방법을 사용하면 사용자가 인증할 모듈을 지정할 수 있습니다. 지정된 모듈은 사용자가 액세스하는 조직 또는 하위 조직에 등록되어야 합니다. 이는 조직의 핵심 인증 서비스의 조직 인증 모듈 속성에서 구성됩니다. 이러한 모듈 기반 인증 요청을 받으면 인증 서비스에서 모듈이 정확하게 구성되었는지 확인하고 모듈이 정의되지 않은 경우에는 사용자 액세스가 거부됩니다.

주 Access Manager 콘솔을 사용하여 인증 모듈을 등록하는 방법에 대한 자세한 내용은 [7 장, **꺆适 옵션**](#) 을 참조하십시오.

모듈 기반 인증 로그인 URL

모듈 기반 인증은 사용자 인터페이스 로그인 URL 에서 `module` 매개 변수를 정의하는 방법으로 지정할 수 있습니다. 모듈 기반 인증을 지정하고 초기화하는 데 사용되는 URL 은 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?module=authentication_module_name
```

```
http://server_name.domain_name:port/amserver/UI/Login?org=org_name&module=authentication_module_name
```

`org` 매개 변수를 지정하지 않은 경우, 사용자가 속한 조직은 로그인 URL 자체에 지정된 서버 호스트와 도메인으로부터 결정됩니다.

모듈 기반 인증 리디렉션 URL

모듈 기반 인증 성공 / 실패 시 Access Manager 에서 사용자를 리디렉션할 위치에 대한 정보를 찾습니다. 응용 프로그램에서 이 정보를 찾는 순서는 다음과 같습니다.

성공한 모듈 기반 인증 리디렉션 URL

성공한 모듈 기반 인증의 리디렉션 URL 은 다음 장소를 순서대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL
2. goto 로그인 URL 매개 변수에서 설정한 URL
3. 사용자 프로필 (amUser.xml) 의 iplanet-am-user-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
4. 사용자의 역할 항목의 iplanet-am-auth-login-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
5. 사용자 조직 항목의 iplanet-am-auth-login-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
6. iplanet-am-auth-login-success-url 속성에 대해 전역 기본값으로서 clientType 사용자 정의 파일에서 설정된 URL
7. 사용자 프로필 (amUser.xml) 의 iplanet-am-user-success-url 속성에 설정된 URL
8. 사용자 역할 항목의 iplanet-am-auth-login-success-url 속성에 설정된 URL
9. 사용자 조직 항목의 iplanet-am-auth-login-success-url 속성에 설정된 URL
10. 전역 기본값으로서 iplanet-am-auth-login-success-url 속성에 설정된 URL

실패한 모듈 기반 인증 리디렉션 URL

실패한 모듈 기반 인증의 리디렉션 URL 은 다음 장소를 순서대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL
2. gotoOnFail 로그인 URL 매개 변수에서 설정한 URL
3. 사용자 항목 (amUser.xml) 의 iplanet-am-user-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
4. 사용자 역할 항목의 iplanet-am-auth-login-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL

5. 사용자 조직 항목의 `iplanet-am-auth-login-failure-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
6. `iplanet-am-auth-login-failure-url` 속성에 대해 전역 기본값으로서 `clientType` 사용자 정의 파일에서 설정된 URL
7. 사용자 항목 (`amUser.xml`)의 `iplanet-am-user-failure-url` 속성에 설정된 URL
8. 사용자 역할 항목의 `iplanet-am-auth-login-failure-url` 속성에 설정된 URL
9. 사용자 조직 항목의 `iplanet-am-auth-login-failure-url` 속성에 설정된 URL
10. 전역 기본값으로서 `iplanet-am-auth-login-failure-url` 속성에 설정된 URL

인증 구성

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

- 조직
- 역할
- 서비스
- 사용자

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

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

인증 구성 사용자 인터페이스

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

1. 객체의 인증 구성 속성 옆에 있는 편집 링크를 눌러 모듈 목록 창을 표시합니다.

2. 이 창에는 객체에 할당된 인증 모듈이 나열됩니다. 모듈이 없는 경우 추가를 눌러 모듈 추가 창을 표시합니다.

모듈 추가 창에는 정의할 다음과 같은 세 파일이 포함되어 있습니다.

모듈 이름. 이 풀다운 목록을 사용하면 핵심 인증 모듈의 조직 인증 모듈 속성에서 활성화된 인증 모듈 (추가한 사용자 정의 모듈 포함) 을 선택할 수 있습니다.

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

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

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

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

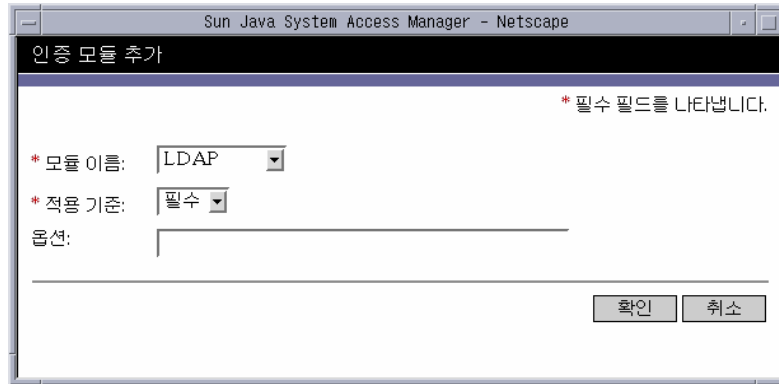
여러 인증 모듈을 추가하고 각 모듈에 대해 플래그를 필수로 설정한 경우 사용자는 모든 인증 요구 사항을 통과해야만 액세스가 허가됩니다.

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

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

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

그림 6-1 사용자에 대한 모듈 목록 추가 창



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

이 목록에 원하는 수의 인증 모듈을 추가할 수 있습니다. 여러 인증 모듈을 추가하는 것을 *인증 체이닝*이라고 합니다. 인증 모듈을 체이닝할 경우 모듈이 나열되는 순서에 따라 적용 계층의 순서가 정의된다는 점에 유의하십시오. 인증 체이닝에 대한 자세한 내용은 [160 페이지의 "인증 모듈 체이닝"](#) 을 참조하십시오.

인증 모듈의 순서를 변경하려면 다음을 수행합니다.

- a. 다시 정렬 버튼을 누릅니다.
- b. 다시 정렬할 모듈을 선택합니다.
- c. 위로 및 아래로 버튼을 사용하여 모듈을 원하는 위치에 놓습니다.

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

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

인증 모듈 체이닝

인증을 하나 이상 구성할 수 있으므로 사용자는 모든 인증에 인증 자격 증명을 전달해야 합니다. 이를 *인증 체이닝*이라고 합니다. Access Manager의 인증 체이닝은 인증 서비스에 통합된 JAAS 프레임워크를 사용하여 수행됩니다. 모듈 체이닝은 인증 구성 서비스 아래에 구성되어 있습니다. 등록된 각 모듈에는 다음 네 가지 값 중 하나가 할당됩니다.

- 필수
- 필요
- 충분
- 옵션

플래그에 따라 정의된 대로 모듈 인증이 연쇄적으로 성공하면 (JAAS 프레임워크에서) 인증에 사용한 모든 사용자 아이디를 검증하고 이를 한 사용자에게 매핑하는 인증 서비스로 제어가 반환됩니다. 매핑은 사용자 프로필의 User Alias List 속성을 구성하는 방법으로 수행됩니다. 유효한 세션 토큰은 모든 매핑이 정확히 이루어질 경우에만 실행되며, 이러한 매핑이 정확하지 않으면 사용자는 유효한 세션 토큰이 거부됩니다. 다음 등록 정보는 다른 사용자가 별칭으로 표시되는 단일 인증된 사용자를 나타냅니다.

- Principal(사용자가 하나만 갖고 있는 경우 해당 사용자의 DN 포함)
- UserToken
- UserId

모든 사용자 아이디가 동일한 사용자로 매핑되지 않고 사용자 아이디 중 하나가 로컬 디렉토리 서버에 있는 경우 동적 프로필 작성을 가능하게 하면 다른 사용자 아이디가 기존 사용자의 사용자 별칭 목록 속성에 추가됩니다.

주

- 인증 체이닝에서 모든 사용자 아이디가 단일 사용자로 매핑되지 않으면 마지막으로 실패한 인증 모듈에서 실패 리디렉션 URL이 선택됩니다. 또한 개별 모듈이 서로 다른 사용자 아이디를 사용하여 모두 성공하는 경우 아무 것도 선택되지 않습니다. 사용자 기반 인증의 경우에는 인증 페이지에 어떤 사용자 아이디가 제공되든지 관계 없이 항상 로그인 URL의 사용자 매개 변수에서 실패 리디렉션 URL이 선택됩니다.
 - 모든 사용자 아이디가 동일한 사용자로 매핑되지 않고 사용자 아이디 중 하나가 로컬 디렉토리 서버에 있는 경우 동적 프로필 작성을 가능하게 하면 다른 사용자 아이디가 기존 사용자의 사용자 별칭 목록 속성에 추가됩니다.
-

조직에 대한 인증 구성

먼저 핵심 인증 서비스를 조직에 추가하여 조직에 인증 모듈을 설정합니다.

조직의 인증 속성을 구성하려면 다음을 수행합니다.

1. 인증 속성을 구성할 조직으로 이동합니다.
2. 보기 메뉴에서 서비스를 선택합니다.
3. 서비스 목록에서 핵심 등록 정보 화살표를 누릅니다.
핵심 인증 속성이 데이터 창에 표시됩니다.
4. 관리자 인증자 속성 옆에 있는 편집 링크를 누릅니다. 여기서는 관리자에 대해서만 인증 서비스를 정의할 수 있습니다. 관리자의 인증 모듈이 최종 사용자의 모듈과 달라야 하는 경우 이 속성을 사용할 수 있습니다. 기본 인증 모듈은 LDAP입니다.
인증 서비스를 정의했으면 저장을 눌러 변경 내용을 저장한 다음 단기를 눌러 조직의 핵심 인증 속성으로 돌아갑니다.
5. 조직 인증 구성 속성 옆에 있는 편집 링크를 누릅니다. 여기서는 조직 내의 모든 사용자에게 대한 인증 모듈을 정의할 수 있습니다. 기본 인증 모듈은 LDAP입니다.
6. 인증 서비스를 정의했으면 저장을 눌러 변경 내용을 저장한 다음 단기를 눌러 조직의 핵심 인증 속성으로 돌아갑니다.

역할에 대한 인증 구성

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

1. 인증 속성을 구성할 조직으로 이동합니다.
2. 보기 메뉴에서 역할을 선택합니다.
3. 인증 구성을 설정할 역할을 선택하고 등록 정보 화살표를 누릅니다.
역할의 등록 정보가 데이터 창에 표시됩니다.
4. 데이터 창의 보기 메뉴에서 서비스를 선택합니다.
5. 필요한 경우 인증 구성 속성을 수정합니다. 이러한 속성에 대한 설명은 [33 장, **확장 구성 서비스 속성**](#)에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다.
6. 저장을 누릅니다.

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

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

서비스에 대한 인증 구성

인증 구성 서비스를 추가한 다음 서비스에 대한 인증 모듈을 설정합니다. 수행 방법은 다음과 같습니다.

1. Identity 관리 모듈의 보기 메뉴에서 서비스를 선택합니다.
추가된 서비스 목록이 표시됩니다. 인증 구성 서비스가 추가되지 않으면 아래 단계를 계속합니다. 서비스가 추가되면 [단계 4](#)로 이동합니다.
2. 이동 창에서 추가를 누릅니다.
사용 가능한 서비스 목록이 데이터 창에 표시됩니다.
3. 인증 구성 확인란을 선택하고 추가를 누릅니다.
인증 구성 서비스가 이동 창에 표시되며 관리자는 이를 통해 해당 서비스가 추가되었음을 확인할 수 있습니다.
4. 인증 구성 등록 정보 화살표를 누릅니다.
서비스 인스턴스 목록이 데이터 창에 표시됩니다.
5. 인증 모듈을 구성할 서비스 인스턴스를 누릅니다.
6. 인증 구성 속성을 수정하고 저장을 누릅니다. 이러한 속성에 대한 설명은 [33 장, 髡适 구성 서비스 속성](#)에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다.

사용자에 대한 인증 구성

1. Identity 관리 모듈의 보기 메뉴에서 사용자를 선택합니다.
사용자 목록이 이동 창에 표시됩니다.
2. 수정할 사용자를 선택하고 등록 정보 화살표를 누릅니다.
사용자 프로필이 데이터 창에 표시됩니다.

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

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

계정 잠금

인증 서비스는 사용자 인증이 n 회 실패하면 사용자 인증을 **잠금**하는 기능을 제공합니다. 이 기능은 기본적으로 꺼져 있지만 Access Manager 콘솔을 사용하여 활성화할 수 있습니다.

주 잘못된 비밀번호 예외가 발생하는 모듈만 계정 잠금 기능을 사용할 수 있습니다.

핵심 인증 서비스에는 다음을 포함하여 이 기능을 활성화 / 사용자 정의하는 속성이 들어 있습니다.

- **로그인 실패 잠금 모드** 계정 잠금을 활성화합니다.

- **로그인 실패 잠금 수** 사용자가 잠기기 전에 인증을 시도할 수 있는 횟수를 정의합니다. 이 값은 사용자 아이디에 대해서만 적용됩니다. 동일한 사용자 아이디가 지정된 횟수만큼 실패하면 그 사용자 아이디는 잠겨집니다.
- **로그인 실패 잠금 간격** 사용자 잠금이 적용되기 전 얼마 동안 로그인 실패 잠금 수의 값이 완료되어야 하는지 분 단위로 정의합니다.
- **잠금 알림을 보낼 전자 메일 주소** 사용자 잠금 알림을 보낼 전자 메일 주소를 지정합니다.
- **N 회 실패 후 사용자에게 경고** 몇 차례 인증이 실패하면 경고 메시지가 사용자에게 표시되는지 지정합니다. 관리자는 사용자에게 잠금이 임박했음을 경고한 이후의 추가 로그인 시도를 설정할 수 있습니다.
- **로그인 실패 잠금 기간** 잠금 후 얼마나 대기한 후 다시 인증을 시도할 수 있는지 분 단위로 정의합니다.
- **잠금 속성 이름** 물리적 잠금에 대해 사용자 프로필 중 어떤 LDAP 속성이 inactive로 설정될 것인지 정의합니다.
- **잠금 속성 값** 잠금 속성 이름에 지정된 LDAP 속성 중 어떤 속성이 inactive 또는 active로 설정될 것인지 정의합니다.

계정 잠금에 관하여 전자 메일 알림이 관리자에게 보내집니다 (계정 잠금 활동도 기록). 계정 잠금 속성에 대한 자세한 내용은 [20 장, 老母 ... 인증 속성](#) 을 참조하십시오.

주 Microsoft® Windows 2000 운영 체제에서의 이 기능 사용에 대한 자세한 내용은 *Access Manager Developer's Guide* 의 부록 A "AMConfig.properties File" 에서 "Simple Mail Transfer Protocol(SMTP)" 을 참조하십시오.

Access Manager에서는 다음 절에서 정의하는 물리적 잠금과 메모리 잠금의 두 가지 계정 잠금 유형을 지원합니다.

물리적 잠금

이 잠금은 Access Manager 의 기본 잠금 동작입니다. 사용자 프로필에서 LDAP 속성의 상태를 inactive 로 바꾸면 이 잠금이 초기화됩니다. Lockout Attribute Name 은 잠금 목적에 따라 사용되는 LDAP 속성을 정의합니다. 물리적 잠금을 구성하는 방법에 대한 자세한 내용은 *Sun Java System Access Manager 관리 설명서*를 참조하십시오.

주	<p>별칭 사용자는 LDAP 프로필에서 사용자 별칭 목록 속성 (iplanet-am-user-alias-list in amUser.xml) 을 구성하는 방법으로 기존의 LDAP 사용자 프로필에 매핑된 사용자입니다. 별칭 사용자는 핵심 인증 서비스의 별칭 검색 속성 이름 필드에 iplanet-am-user-alias-list 를 추가함으로써 검증할 수 있습니다. 즉 별칭 사용자가 잠긴 경우 해당 사용자가 별칭 처리된 실제 LDAP 프로필도 잠기게 됩니다. 이는 LDAP 및 구성원이 아닌 인증 모듈을 사용하는 물리적 잠금에만 적용됩니다.</p>
----------	---

메모리 잠금

메모리 잠금은 Login Failure Lockout Duration 속성을 0 보다 큰 값으로 변경하는 방법으로 사용할 수 있습니다. 그러면 사용자 계정은 지정된 분 수 동안 메모리에서 잠깁니다. 시간이 모두 경과한 후에는 계정의 잠금이 해제됩니다. 메모리 잠금 기능을 사용할 때는 몇 가지 사항에 특별히 주의해야 합니다.

- Access Manager 가 다시 시작하는 경우에는 메모리에서 잠긴 모든 계정이 잠금 해제됩니다.
- 사용자 계정이 메모리에서 잠겨 있고 관리자가 (잠금 기간을 0 으로 되돌려) 계정 잠금 기법을 물리적 잠금으로 변경할 경우 사용자 계정이 메모리에서 잠금 해제되고 잠금 수가 다시 설정됩니다.
- 메모리 잠금 후 LDAP 및 구성원이 아닌 인증 모듈을 사용할 때 사용자가 정확한 비밀번호로 로그인하려고 하면 *사용자가 활성 상태가 아닙니다* 오류 대신 *사용자에게 이 조직 프로필이 없습니다* 오류 메시지가 반환됩니다.

주	<p>실패 URL 속성이 사용자 프로필에 설정되어 있는 경우에는 사용자 계정이 잠겨 있다는 메시지나 잠금 경고 메시지가 표시되지 않으며 사용자는 정의된 URL 로 리디렉션됩니다.</p>
----------	---

인증 서비스 페일오버

인증 서비스 페일오버는 하드웨어나 소프트웨어 문제 때문에 주 서버에 장애가 발생하거나 서버가 일시적으로 다운될 경우 자동으로 인증 요청을 보조 서버로 리디렉션합니다.

인증 서비스를 사용할 수 있는 Access Manager 인스턴스에서 인증 컨텍스트가 먼저 생성되어야 합니다. 이 Access Manager 인스턴스를 사용할 수 없는 경우 인증 페일오버를 통해 다른 Access Manager 인스턴스에서 인증 컨텍스트를 생성할 수 있습니다. 인증 컨텍스트는 다음 순서로 서버 가용성을 확인합니다.

1. 인증 서비스 URL 이 AuthContext API 로 전달됩니다. 예를 들면 다음과 같습니다.

```
AuthContext(orgName, url)
```

이 API 가 사용될 경우 URL 에 의해 참조되는 서버만 사용합니다. 해당 서버에서 인증 서비스를 사용할 수 있는 경우라도 페일오버는 이루어지지 않습니다.

2. 인증 컨텍스트는 AMConfig.properties 파일의 com.ipplanet.am.server* 속성에 정의된 서버를 검사합니다.
3. 단계 2 가 실패할 경우 인증 컨텍스트는 이름 지정 서비스를 사용할 수 있는 서버에서 플랫폼 목록을 조회합니다. 이 플랫폼 목록은 하나의 Directory Server 인스턴스를 공유하는 다수의 Access Manager 인스턴스 (일반적으로 페일오버 목적)가 설치될 때 자동으로 작성됩니다.

예를 들어, 플랫폼 목록에 Server1, Server2 및 Server3 을 위한 URL 이 포함되면 인증 컨텍스트는 그 중 하나에서 인증이 성공할 때까지 Server1, Server2, Server3 를 차례로 순환합니다.

플랫폼 목록은 이름 지정 서비스의 가용성에 따라 다르므로 항상 동일한 서버에서 얻어질 수 있는 것은 아닙니다. 더욱이 이름 지정 서비스 페일오버가 먼저 일어날 수도 있습니다. AMConfig.properties 의 com.ipplanet.am.naming.url property 에 다수의 이름 지정 서비스 URL 이 지정됩니다. 사용할 수 있는 첫 번째 이름 지정 서비스 URL 은 인증 페일오버가 이루어지는 서버 목록이 포함된 서버를 식별하는 데 사용됩니다.

정규화된 도메인 이름 (FQDN) 매핑

정규화된 도메인 이름 (FQDN) 매핑을 사용하면 사용자가 잘못된 URL 을 입력하더라도 (예 : 보호된 자원에 액세스할 때 부분 호스트 이름이나 IP 주소 지정) 인증 서비스에서 수정할 수 있습니다. FQDN 매핑은 AMConfig.properties 파일의 com.sun.identity.server.fqdnMap 속성을 수정하여 활성화합니다. 이 등록 정보를 지정하는 형식은 다음과 같습니다.

```
com.sun.identity.server.fqdnMap[invalid-name]=valid-name
```


invalid-name 값은 사용자가 잘못 입력한 FQDN 호스트 이름이 되고 *valid-name* 은 필터에서 사용자를 리디렉션할 실제 호스트 이름이 됩니다. 명시된 요구 사항에 부합한다면 횡수 제한 없이 매핑 지정이 가능합니다 (코드 예 1-1 참조). 이 등록 정보를 설정하지 않으면 사용자는 AMConfig.properties 파일에서도 확인 가능한 `com.ipplanet.am.server.host=server_name` 등록 정보에 구성된 기본 서버 이름으로 보내집니다.

코드 예 6-1 AMConfig.properties 의 FQDN 매핑 속성

```
com.sun.identity.server.fqdnMap[issserver]=issserver.mydomain.com
com.sun.identity.server.fqdnMap[issserver.mydomain]=issserver.mydomain.com
com.sun.identity.server.fqdnMap[IP address]=issserver.mydomain.com
```

FQDN 매핑의 용도

이 등록 정보는 서버에 호스트된 응용 프로그램이 둘 이상의 호스트 이름으로 액세스 가능할 경우 둘 이상의 호스트 이름에 대해 하나의 매핑을 작성하는 데 사용할 수 있습니다. 또한 Access Manager 에서 특정 URL 에 대해 수정 조치를 취하지 않게 할 때에도 사용할 수 있습니다. 예를 들어, IP 주소를 사용하여 응용 프로그램에 액세스하는 사용자에게 리디렉션이 필요하지 않다면 이 기능은 다음과 같이 매핑 항목을 지정하여 구현할 수 있습니다.

```
com.sun.identity.server.fqdnMap[IP address]=IP address.
```

주의 매핑이 둘 이상 정의되어 있을 때는 잘못된 FQDN 이름으로 값이 겹치지 않아야 합니다. 응용 프로그램 액세스가 불가능해질 수도 있습니다.

영구 쿠키

영구 쿠키는 웹 브라우저를 닫은 후에도 계속 존재하는 쿠키로서, 사용자가 이 영구 쿠키를 사용하면 다시 인증할 필요 없이 새 브라우저 세션으로 로그인할 수 있습니다. 이 쿠키의 이름은 AMConfig.properties 의 `com.ipplanet.am.pcookie.name` 등록 정보에서 정의되며 그 기본값은 DProPCookie 입니다. 쿠키 값은 3DES 암호화된 문자열로서 사용자 DN, 조직 이름, 인증 모듈 이름, 최대 세션 시간, 유효 시간 및 캐시 시간으로 구성됩니다. 영구 쿠키를 활성화하려면 다음을 수행합니다.

1. 핵심 인증 모듈에서 Persistent Cookie Mode 를 켭니다.

2. 핵심 인증 모듈에서 Persistent Cookie Maximum Time 속성에 대한 시간 값을 구성합니다.
3. 값이 yes 인 iPSPCookie 매개 변수를 사용자 인터페이스 로그인 URL 에 추가합니다.

사용자가 이 URL 을 사용하여 인증하고 나면 브라우저를 닫아도 다시 인증할 필요 없이 새 브라우저 창을 열 수 있고 콘솔로 리디렉션하게 됩니다. 이러한 작업은 단계 2 에서 정의한 시간이 경과할 때까지 가능합니다.

영구 쿠키 모드는 다음 인증 SPI 방법을 사용하여 켤 수 있습니다.

```
AMLoginModule.setPersistentCookieOn()
```

다중 LDAP 인증 모듈 구성

파일오버의 한 형식으로 또는 Access Manager 콘솔에 값 필드가 하나만 제공되는 경우 하나의 속성에 여러 값을 구성하기 위해 관리자는 하나의 조직에 여러 LDAP 인증 모듈 구성을 정의할 수 있습니다. 이러한 추가 구성은 콘솔에 표시되지 않더라도 사용자의 인증 요청에 대한 초기 검색이 없는 경우에 기본 구성과 함께 사용됩니다. 예를 들어 한 조직에서 두 가지 서로 다른 도메인에 인증용 LDAP 서버를 통한 검색을 정의하거나 한 도메인에 사용자 이름 지정 속성을 여러 개 구성할 수도 있습니다. 후자는 콘솔에 텍스트 필드를 하나만 갖는 경우이며, 기본 검색 기준을 사용하여 사용자를 찾지 못하면 LDAP 모듈에서 2 차 범위를 사용하여 검색하게 됩니다. 다음은 추가 LDAP 구성을 구성하는 단계입니다.

추가 LDAP 구성 추가

1. 2 차 (또는 3 차) LDAP 인증 구성에 필요한 새 값과 전체 속성 세트를 포함하여 XML 파일을 작성합니다.

/etc/opt/SUNWam/config/xml에 있는 amAuthLDAP.xml을 확인하면서 사용 가능한 속성을 참조할 수 있습니다. 그러나 이 단계에서 만든 XML 파일은 amAuthLDAP.xml과 달리 amadmin.dtd 구조를 기반으로 합니다. 이 파일에 대해 속성을 하나 또는 전부 정의할 수 있습니다. 코드 예 1-2 는 하위 구성 파일의 예로서 LDAP 인증 구성에 사용할 수 있는 모든 속성의 값이 포함되어 있습니다.

코드 예 6-2

LDAP 하위 구성 파일을 추가하는 샘플 XML 파일

```

<?xml version="1.0" encoding="ISO-8859-1"?>
<!--
Copyright (c) 2002 Sun Microsystems, Inc. All rights reserved.
Use is subject to license terms.
-->
<!DOCTYPE Requests
PUBLIC "-//iPlanet/Sun ONE Identity Server 6.0 Admin CLI DTD//EN"
"jar://com/iplanet/am/admin/cli/amAdmin.dtd"
>
<!--
Before adding subConfiguration load the schema with
GlobalConfiguration defined and replace corresponding
serviceName and subConfigID in this sample file OR load
serviceConfigurationRequests.xml before loading this sample
-->
<Requests>
<OrganizationRequests DN="dc=iplanet,dc=com">
<AddSubConfiguration subConfigName = "ssc"
subConfigId = "serverconfig"
priority = "0" serviceName="iPlanetAMAuthLDAPService">

<AttributeValuePair>
<Attribute name="iplanet-am-auth-ldap-server"/>
<Value>newvalue</Value>
</AttributeValuePair>
<AttributeValuePair>
<Attribute name="iplanet-am-auth-ldap-server"/>
<Value>vbrao.red.iplanet.com:389</Value>
</AttributeValuePair>
<AttributeValuePair>
<Attribute name="iplanet-am-auth-ldap-base-dn"/>
<Value>dc=iplanet,dc=com</Value>
</AttributeValuePair>
<AttributeValuePair>
<Attribute name="iplanet-am-auth-ldap-bind-dn"/>
<Value>cn=amldapuser,ou=DSAME Users,dc=iplanet,dc=com</Value>
</AttributeValuePair>
<AttributeValuePair>
<Attribute name="iplanet-am-auth-ldap-bind-passwd"/>
<Value>plain text password</Value>
</AttributeValuePair>
<AttributeValuePair>
<Attribute name="iplanet-am-auth-ldap-user-naming-attribute"/>
<Value>uid</Value>
</AttributeValuePair>
<AttributeValuePair>
<Attribute name="iplanet-am-auth-ldap-user-search-attributes"/>
<Value>uid</Value>
</AttributeValuePair>
<AttributeValuePair>
<Attribute name="iplanet-am-auth-ldap-search-scope"/>
<Value>SUBTREE</Value>
</AttributeValuePair>
<AttributeValuePair>
<Attribute name="iplanet-am-auth-ldap-ssl-enabled"/>

```

코드 예 6-2 LDAP 하위 구성 파일을 추가하는 샘플 XML 파일 (계속)

```

    <Value>false</Value>
  </AttributeValuePair>
</AttributeValuePair>
  <Attribute name="iplanet-am-auth-ldap-return-user-dn"/>
  <Value>true</Value>
</AttributeValuePair>
</AttributeValuePair>
  <Attribute name="iplanet-am-auth-ldap-auth-level"/>
  <Value>0</Value>
</AttributeValuePair>
</AttributeValuePair>
  <Attribute name="iplanet-am-auth-ldap-server-check"/>
  <Value>15</Value>
</AttributeValuePair>

</AddSubConfiguration>

</OrganizationRequests>
</Requests>

```

2. 단계 1 에서 작성한 XML 파일에서 iplanet-am-auth-ldap-bind-passwd 의 값으로서 일반 텍스트 비밀번호를 복사합니다.

이 속성의 값은 41 페이지의 코드 예 1-2 에 굵은 서식으로 표시되어 있습니다.

3. amadmin 명령줄 도구를 사용하여 XML 파일을 로드합니다.

```
./amadmin -u amadmin -w administrator_password -v -t name_of_XML_file
```

이 2 차 LDAP 구성은 Access Manager 콘솔에서 보거나 수정할 수 없습니다.

팁 다중 LDAP 구성에 사용할 수 있는 샘플이 있습니다.

/AccessManager-base/SUNWam/samples/admin/cli/bulk-ops/ 에서 **serviceAddMultipleLDAPConfigurationRequests.xml** 명령줄 템플릿을 참조하십시오. 지침은 */AccessManager-base/SUNWam/samples/admin/cli/* 의 **Readme.html** 에서 볼 수 있습니다.

세션 업그레이드

인증 서비스를 사용하면 한 조직에서 동일한 사용자가 수행한 2 차 인증 성공을 기반으로 유효한 세션 토큰을 업그레이드할 수 있습니다. 유효한 세션 토큰을 가진 사용자가 현재 조직에서 보호한 자원에 인증을 시도하고 이 2 차 인증 요청이 성공하면 해당 세션은 새 인증을 기반으로 한 새 등록 정보로 업데이트됩니다. 인증이 실패하면 사용자의 현재 세션이 업그레이드 되지 않은 채 그대로 반환됩니다. 유효한 세션을 가진 사용자가 다른 조직에서 보호한 자원에 인증을 시도하는 경우 새 조직에 인증할 것인지 묻는 메시지를 받게 됩니다. 이때 사용자는 현재 세션을 유지하거나 새 조직에 인증을 시도할 수도 있습니다. 인증이 성공하면 옛 세션이 삭제되고 새 세션이 작성됩니다.

세션 업그레이드 중 로그인 페이지가 시간 초과되면 원래의 성공 URL 로 리디렉션됩니다. 시간 초과 값은 다음에 따라 결정됩니다.

- 각 모듈에 설정한 페이지 시간 초과 값 (기본값 : 1 분)
- AMConfig.properties 의 com.ipplanet.am.invalidMaxSessionTime 등록 정보 (기본값 : 10 분)
- ipplanet-am-max-session-time(기본값 : 120 분)

com.ipplanet.am.invalidMaxSessionTimeout 값 및 ipplanet-am-max-session-time 값은 페이지 시간 초과 값보다 커야 합니다. 그렇지 않으면 세션 업그레이드 중 유효한 세션 정보가 손실되고 이전의 성공 URL 에 대한 리디렉션이 실패하게 됩니다.

플러그 인 인터페이스 검증

관리자는 조직에 맞게 사용자 이름 또는 비밀번호 검증 논리를 작성하고 이를 인증 서비스에 플러그 인할 수 있습니다 (이 기능은 LDAP 및 구성원 인증 모듈에서만 지원됨) 사용자를 인증하거나 비밀번호를 변경하기 전에 Access Manager 에서는 이 플러그 인을 호출합니다. 검증이 성공하면 인증이 계속되지만, 실패하면 인증 실패 페이지가 나타납니다. 이 플러그 인은 서비스 관리 SDK 의 일부인

com.ipplanet.am.sdk.AMUserPasswordValidation 클래스를 확장합니다. 이 SDK 에 대한 내용은 Access Manager Javadocs 의 com.ipplanet.am.sdk 패키지를 참조하십시오. 다음은 Access Manager 의 검증 플러그 인을 작성 및 구성하는 단계입니다.

1. 새 플러그 인 클래스는 com.ipplanet.am.sdk.AMUserPasswordValidation 클래스를 확장하고 validateUserID() 및 validatePassword() 메소드를 구현합니다. AMException 은 검증이 실패할 때 나타납니다.

2. 플러그인 클래스를 컴파일하고 원하는 위치에 .class 파일을 놓습니다. 런타임 동안 Access Manager 에서 액세스할 수 있도록 클래스 경로를 업데이트합니다.
3. 최상위 관리자로서 Access Manager 콘솔에 로그인합니다. 서비스 관리 탭을 누르고 관리 서비스에 대한 속성을 확인하십시오. UserID & Password Validation Plugin Class 필드에 플러그인 클래스의 이름(패키지 이름 포함)을 입력합니다.
4. 로그아웃했다가 다시 로그인합니다.

JAAS 공유 상태

JAAS 공유 상태는 인증 모듈들이 사용자 아이디와 비밀번호를 공유하게 합니다. 다음 인증 모듈에 옵션이 정의되어 있습니다.

- 조직
- 사용자
- 서비스
- 역할

실패할 때 모듈에는 필수 자격 증명에 대한 메시지가 나타납니다. 인증이 실패하고 나면 모듈의 실행이 중지되거나 로그아웃 공유 상태가 지워집니다.

JAAS 공유 상태 활성화

JAAS 공유 상태를 구성하려면 다음을 수행합니다.

- `iplanet-am-auth-sharedstate-enabled` 옵션을 사용합니다.
- 공유 상태 옵션은 다음의 경우에 사용됩니다.
`iplanet-am-auth-shared-state-enabled=true`
- 이 옵션의 기본값은 `true` 입니다.

실패하면 인증 모듈에는 필수 자격 증명 프롬프트가 JAAS 사양에 제시된 `tryFirstPass` 옵션 동작에 따라 나타납니다.

JAAS 공유 상태 저장소 옵션

JAAS 공유 상태 저장소 옵션을 구성하려면 다음을 수행합니다.

- `iplanet-amauth-store-shared-state-enabled` 옵션을 사용합니다.
- 저장소 공유 상태 옵션은 다음과 같은 경우에 사용됩니다.
`iplanet-am-auth-shared-state-enabled=true`
- 이 옵션의 기본값은 `false` 입니다.

완결, 종단 또는 로그아웃 후에는 공유 상태가 지워집니다.

JAAS 공유 상태

인증 옵션

Sun Java™ System Access Manager 6 2005Q1 은 인증을 위한 프레임워크를 제공합니다. 인증은 회사 내에서 응용 프로그램에 액세스하는 사용자의 아이디를 확인하는 프로세스입니다. 사용자는 Access Manager 콘솔이나 기타 Access Manager 보호 자원에 액세스하기 전에 인증 프로세스를 통과해야 합니다. 인증은 사용자의 아이디를 검증하는 플러그 인을 통해 구현됩니다. 이 플러그 인 구조에 대한 자세한 내용은 *Access Manager Developer's Guide* 를 참조하십시오.

Access Manager 콘솔을 사용하여 기본값을 설정하고 인증 모듈을 추가하며 인증 템플릿을 만들고 관련된 인증 모듈을 사용 가능하게 할 수 있습니다. 이 장에서는 인증 모듈에 대한 개요와 추가에 관한 지침을 제공하며 다음 내용으로 구성되어 있습니다.

- 176 페이지의 "핵심 인증"
- 177 페이지의 "활성 디렉토리 인증"
- 178 페이지의 "익명 인증"
- 180 페이지의 "인증서 기반 인증"
- 182 페이지의 "HTTP 기본 인증"
- 183 페이지의 "JDBC 인증"
- 185 페이지의 "LDAP 디렉토리 인증"
- 187 페이지의 "구성원 인증"
- 188 페이지의 "MSISDN 인증"
- 190 페이지의 "Windows NT 인증"
- 192 페이지의 "RADIUS 서버 인증"
- 194 페이지의 "SafeWord 인증"

- 197 페이지의 "SAML 인증 "
- 198 페이지의 "SecurID 인증 "
- 200 페이지의 "Unix 인증 "
- 202 페이지의 "Windows 데스크탑 SSO 인증 "

핵심 인증

Access Manager 는 기본적으로 핵심 인증 모듈과 15 개의 다른 인증 모듈을 제공합니다 . 핵심 인증 모듈은 인증 모듈에 대한 전체 구성을 제공합니다 . 활성 디렉토리 , 익명 , 인증서 기반 , HTTP 기본 , JDBC, LDAP 및 인증 모듈을 추가하고 활성화하기 전에 먼저 핵심 인증을 추가하고 활성화해야 합니다 . 기본 조직에서는 핵심 및 LDAP 인증 모듈을 자동으로 사용할 수 있게 됩니다 . 20 장 , "핵심 인증 속성 "에는 핵심 속성의 자세한 목록이 나와 있습니다 .

핵심 모듈 추가 및 활성화

1. 핵심 모듈을 추가할 조직으로 이동합니다 .
2. 보기 메뉴에서 서비스를 선택합니다 .
3. 이동 창에서 추가를 누릅니다 .

사용 가능한 모듈 목록이 데이터 창에 표시됩니다 .

4. 핵심 인증 확인란을 선택하고 추가를 누릅니다 .

핵심 인증 모듈이 이동 창에 표시되며 관리자는 이를 통해 해당 모듈이 추가되었음을 확인할 수 있습니다 .

5. 핵심 인증 등록 정보 화살표를 누릅니다 .

이 서비스에 대한 템플릿이 현재 없습니다 . 지금 템플릿을 만드시겠습니까? 라는 메시지가 데이터 창에 표시됩니다 .

6. 예를 누릅니다 .

핵심 속성이 데이터 창에 표시됩니다 . 필요에 따라 속성을 수정합니다 . 핵심 속성에 대한 설명은 20 장 , "핵심 인증 속성 "에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다 .

활성 디렉토리 인증

활성 디렉토리 인증 모듈은 **LDAP 디렉토리 인증** 모듈과 비슷한 방법으로 인증을 수행하지만 (LDAP 인증 모듈의 Directory Server 와 반대되는) Microsoft 의 Active Directory™ 서버를 사용합니다 . 활성 디렉토리 서버에 대해 LDAP 인증 모듈을 구성할 수는 있지만 , 이 모듈을 사용하면 LDAP 및 활성 디렉토리 인증이 모두 같은 조직 아래에 있게 됩니다 .

주 이 릴리스의 경우 활성 디렉토리 인증 모듈만 사용자 인증을 지원합니다 . 비밀번호 정책은 LDAP 인증 모듈에서만 지원됩니다 .

활성 디렉토리 인증 추가 및 활성화

Access Manager 에 조직 관리자 또는 최상위 관리자로 로그인해야 합니다 .

1. 구성원 인증을 추가할 조직으로 이동합니다 .
2. 보기 메뉴에서 서비스를 선택합니다 .
 핵심 모듈을 이미 추가한 경우 이 내용이 이동 창에 표시됩니다 . 핵심 모듈을 아직 추가하지 않은 경우 활성 디렉토리 인증 모듈과 동시에 추가할 수 있습니다 .
3. 이동 창에서 추가를 누릅니다 .
 사용 가능한 모듈 목록이 데이터 창에 표시됩니다 .
4. 활성 디렉토리 인증 확인란을 선택하고 추가를 누릅니다 .
 활성 디렉토리 인증 모듈이 이동 창에 표시되며 관리자는 이를 통해 해당 모듈이 추가되었음을 확인할 수 있습니다 .
5. 활성 디렉토리 인증 등록 정보 화살표를 누릅니다 .
이 모듈에 대한 템플릿이 현재 없습니다 . 지금 템플릿을 만드시겠습니까?
 라는 메시지가 데이터 창에 표시됩니다 .
6. 예를 누릅니다 .
 활성 디렉토리 인증 속성이 데이터 창에 표시됩니다 . 필요에 따라 속성을 수정합니다 .
7. 저장을 누릅니다 .
 활성 디렉토리 인증 모듈을 사용할 수 있습니다 .

활성 디렉토리 인증을 사용하여 로그인

활성 디렉토리 인증을 사용하여 로그인하려면 [280 페이지의 "조직 인증 모듈"](#) 핵심 인증 모듈 속성을 수정하여 활성 디렉토리 인증을 활성화하고 선택해야 합니다. 이렇게 하면 사용자가 `http://hostname:port/deploy_URI/UI/Login?module=AD` (대소문자 구분)를 사용하여 로그인할 때 활성 디렉토리 인증 로그인 창이 표시됩니다. 사용 중인 인증 유형 (예: 서비스, 역할, 사용자, 조직)에 따라 인증 모듈을 기본값으로 구성할 경우 URL에 모듈 이름을 지정할 필요가 없습니다.

익명 인증

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

익명 인증 추가 및 활성화

Access Manager에 조직 관리자 또는 최상위 관리자로 로그인해야 합니다.

1. 익명 인증을 추가할 조직으로 이동합니다.
2. 보기 메뉴에서 서비스를 선택합니다.

핵심 모듈을 이미 추가한 경우 이 내용이 이동 창에 표시됩니다. 핵심 모듈을 아직 추가하지 않은 경우 익명 인증 모듈과 함께 추가할 수 있습니다.

3. 이동 창에서 추가를 누릅니다.

사용 가능한 모듈 목록이 데이터 창에 표시됩니다.

4. 익명 인증 확인란을 선택하고 추가를 누릅니다.

익명 인증 모듈이 이동 창에 표시되며 관리자는 이를 통해 해당 모듈이 추가되었음을 확인할 수 있습니다.

5. 익명 인증 등록 정보 화살표를 누릅니다.

이 서비스에 대한 템플릿이 현재 없습니다. 지금 템플릿을 만드시겠습니까? 라는 메시지가 데이터 창에 표시됩니다.

6. 예를 누릅니다.

익명 인증 속성이 데이터 창에 표시됩니다. 필요에 따라 속성을 수정합니다. 이러한 속성에 대한 설명은 18 장, "익명 인증 속성"에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다.

7. 저장을 누릅니다.

익명 인증 모듈이 활성화되었습니다.

익명 인증을 사용하여 로그인

익명 인증을 사용하여 로그인하려면 280 페이지의 "조직 인증 모듈" 핵심 인증 모듈 속성을 수정하여 익명 인증을 활성화 및 선택해야 합니다. 이렇게 하면 사용자가 `http(s)://hostname:port/SERVER_DEPLOY_URI/UI/Login?module=Anonymous&org=org_name` 을 사용하여 로그인할 수 있습니다. 익명 인증 로그인 창을 사용하지 않고 로그인하려면 다음 구문을 사용합니다.

```
http(s)://hostname:port/SERVER_DEPLOY_URI/UI/Login?module=Anonymous&org=org_name&Login.Token1=user_id
```

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

주

익명 인증 모듈의 기본 익명 사용자 이름 속성 값은 `anonymous` 입니다. 이 속성 값은 사용자가 로그인할 때 사용하는 이름입니다. 따라서 조직 내에서 기본 익명 사용자를 만들어야 합니다. 사용자 아이디는 익명 인증 속성에 지정된 아이디와 동일해야 합니다. 이 속성 값을 대소문자가 구분되도록 선택할 수 있습니다.

인증서 기반 인증

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

인증서 기반 인증 모듈을 조직에 추가하기 전에 여러 가지 작업을 수행해야 합니다. 먼저, Access Manager 와 함께 설치되는 웹 컨테이너를 보호하고 인증서 기반 인증에 맞게 구성해야 합니다. 인증서 기반 모듈을 활성화하기 전에 이 초기 Web Server 구성 단계에 대한 내용을 보려면 *Sun ONE Web Server 6.1 관리자 설명서*의 6 장 "인증서 및 키 사용" 을 참조하십시오. 이 문서는 다음 위치에서 확인할 수 있습니다.

<http://docs.sun.com/db/prod/slwebsrv#hic>

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

<http://docs.sun.com/db/prod/slappsrv#hic>

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

인증서 기반 인증 추가 및 활성화

Access Manager 에 조직 관리자로 로그인해야 합니다.

1. 인증서 기반 인증을 추가할 조직으로 이동합니다.

2. 보기 메뉴에서 서비스를 선택합니다.

핵심 모듈을 이미 추가한 경우 이 내용이 이동 창에 표시됩니다. 핵심 모듈을 아직 추가하지 않은 경우 인증서 기반 인증 모듈과 함께 추가할 수 있습니다.

3. 이동 창에서 추가를 누릅니다.

사용 가능한 모듈 목록이 데이터 창에 표시됩니다.

4. 인증서 기반 인증 확인란을 선택하고 추가를 누릅니다.

인증서 기반 인증 모듈이 이동 창에 표시되며 관리자는 이를 통해 해당 모듈이 추가되었음을 확인할 수 있습니다.

5. 인증서 기반 인증 등록 정보 화살표를 누릅니다.

이 서비스에 대한 템플릿이 현재 없습니다. 지금 템플릿을 만드시겠습니까?
라는 메시지가 데이터 창에 표시됩니다.

6. 예를 누릅니다.

인증서 기반 인증 속성이 데이터 창에 표시됩니다. 필요에 따라 속성을 수정합니다. 이러한 속성에 대한 설명은 [19 장](#), "[인증서 인증 속성](#)"에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다.

7. 저장을 누릅니다.

인증서 기반 인증의 플랫폼 서버 목록에 서버 URL 추가

이 모듈을 추가하려면 Access Manager 에 조직 관리자로 로그인해야 하며 Access Manager 와 웹 컨테이너에서 SSL 을 구성하고 클라이언트 인증을 활성화해야 합니다. 세부 사항에 대해서는 [53 페이지](#)의 "[SSL 모드에서 Access Manager 구성](#)" 을 참조하십시오.

인증서 기반 인증을 사용하여 로그인

인증서 기반 인증을 기본 인증 방법으로 만들려면 핵심 인증 모듈 속성 [조직 인증 모듈](#) ([페이지 280](#) 참조) 을 수정해야 합니다. 이렇게 하면 사용자가 `https://hostname:port/deploy_URI/UI/Login?module=Cert` 를 사용하여 로그인할 때 인증서 기반 인증 로그인 창이 표시됩니다. 사용 중인 인증 유형 (예 : 역할, 사용자, 조직) 에 따라 인증 모듈을 기본값으로 구성할 경우 URL 에 모듈 이름을 지정할 필요가 없습니다.

HTTP 기본 인증

이 모듈은 HTTP 프로토콜에서 기본적으로 제공하는 기본 인증을 사용합니다. Web Server 는 아이디 및 비밀번호에 대한 클라이언트 요청을 발급하고, 해당 정보를 인증된 요청에 포함하여 서버로 다시 보냅니다. Access Manager 는 사용자 아이디와 비밀번호를 수신한 다음 LDAP 인증 모듈에 대해 사용자를 내부적으로 인증합니다. HTTP 기본이 제대로 작동하게 하려면 LDAP 인증 모듈을 추가해야 합니다 (HTTP 기본 모듈만 추가하면 작동되지 않음). 세부 사항에 대해서는 [185 페이지의 "LDAP 인증 추가 및 활성화"](#) 를 참조하십시오. 성공적으로 인증한 사용자는 사용자 아이디와 비밀번호를 묻는 메시지를 표시하지 않고 다시 인증할 수 있습니다.

HTTP 기본 인증 추가 및 활성화

Access Manager 에 조직 관리자 또는 최상위 관리자로 로그인하고 LDAP 인증 모듈이 이미 등록되어 있어야 합니다.

1. HTTP 기본 인증을 추가할 조직으로 이동합니다.
2. 보기 메뉴에서 서비스를 선택합니다.

핵심 모듈을 이미 추가한 경우 이 내용이 이동 창에 표시됩니다. 핵심 모듈을 아직 추가하지 않은 경우 HTTP 기본 인증 모듈과 함께 추가할 수 있습니다.

3. 이동 창에서 추가를 누릅니다.
사용 가능한 모듈 목록이 데이터 창에 표시됩니다.
4. HTTP 기본 인증 확인란을 선택하고 추가를 누릅니다.

HTTP 기본 인증 모듈이 이동 창에 표시되며 관리자는 이를 통해 해당 모듈이 추가되었음을 확인할 수 있습니다.

5. HTTP 기본 인증 등록 정보 화살표를 누릅니다.

이 서비스에 대한 템플릿이 현재 없습니다. 지금 템플릿을 만드시겠습니까?
라는 메시지가 데이터 창에 표시됩니다.

6. 예를 누릅니다.

HTTP 기본 인증 속성이 데이터 창에 표시됩니다. 필요에 따라 속성을 수정합니다. 이러한 속성에 대한 설명은 [21 장](#), "["HTTP 기본 인증 속성"](#) 에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다.

7. 저장을 누릅니다.

HTTP 기본 인증 모듈이 활성화되었습니다.

HTTP 기본 인증을 사용하여 로그인

LDAP 인증을 사용하여 로그인하려면 [280 페이지의 "조직 인증 모듈"](#) 핵심 인증 모듈 속성을 수정하여 HTTP 기본 인증을 활성화하고 선택해야 합니다. 이렇게 하면 사용자가

`http://hostname:port/server_deploy_URI/UI/Login?module=HTTPBasic` 를 사용하여 로그인할 때 인증 로그인 창이 표시됩니다. 사용 중인 인증 유형 (예: 서비스, 역할, 사용자, 조직)에 따라 인증 모듈을 기본값으로 구성할 경우 URL에 모듈 이름을 지정할 필요가 없습니다. 인증이 실패하면 새 인스턴스가 열리고 사용자가 다시 로그인해야 합니다. HTTP 기본 인증을 사용한 후에 완전히 로그아웃하려면 기존 브라우저 인스턴스를 모두 닫고 새 브라우저 인스턴스를 시작해야 합니다.

JDBC 인증

JDBC(Java Database Connectivity) 인증 모듈은 Access Manager가 JDBC 기술 사용 드라이버를 제공하는 SQL 데이터베이스를 통해 사용자를 인증하는 기법을 지원합니다. SQL 데이터베이스에 대한 연결은 JDBC 드라이버를 통해 또는 JNDI 연결 풀을 통해 수행될 수 있습니다.

주 이 모듈은 MySQL 4.0 및 Oracle 8i에서 테스트 완료되었습니다.

JDBC 인증 추가 및 활성화

Access Server에 조직 관리자나 최상위 관리자로 로그인해야 합니다.

1. JDBC 인증을 추가할 조직으로 이동합니다.
2. 보기 메뉴에서 서비스를 선택합니다.

핵심 모듈을 이미 추가한 경우 이 내용이 이동 창에 표시됩니다. 핵심 모듈을 아직 추가하지 않은 경우 JDBC 인증 모듈과 함께 추가할 수 있습니다.

3. 이동 창에서 추가를 누릅니다.

사용 가능한 모듈 목록이 데이터 창에 표시됩니다.

4. JDBC 인증 확인란을 선택하고 추가를 누릅니다.

JDBC 인증 모듈이 이동 창에 표시되며 관리자는 이를 통해 해당 모듈이 추가되었음을 확인할 수 있습니다.

5. JDBC 인증 등록 정보 화살표를 누릅니다.

이 서비스에 대한 템플릿이 현재 없습니다. 지금 템플릿을 만드시겠습니까?
라는 메시지가 데이터 창에 표시됩니다.

6. 예를 누릅니다.

JDBC 인증 속성이 데이터 창에 표시됩니다. 필요에 따라 속성을 수정합니다.

7. 저장을 누릅니다.

JDBC 인증 모듈이 활성화되었습니다.

JDBC 인증을 사용하여 로그인

JDBC 인증을 사용하여 로그인하려면 280 페이지의 "조직 인증 모듈" 핵심 인증 모듈 속성을 수정하여 JDBC 인증을 활성화하고 선택해야 합니다. 이렇게 하면 사용자가 `http://hostname:port/deploy_URI/UI/Login?module=JDBC`(대소문자 구분)를 사용하여 로그인할 때 JDBC 인증 로그인 창이 표시됩니다. 사용 중인 인증 유형(예: 서비스, 역할, 사용자, 조직)에 따라 인증 모듈을 기본값으로 구성할 경우 URL에 모듈 이름을 지정할 필요가 없습니다.

LDAP 디렉토리 인증

LDAP 인증 모듈에서는 사용자가 로그인할 때 특정 사용자 DN 및 비밀번호를 사용하여 LDAP 디렉토리 서버에 바인드해야 합니다. 이것은 모든 조직 기반 인증에 대한 기본 인증 모듈입니다. 사용자는 Directory Server 에 있는 사용자 아이디와 비밀번호를 입력하여 유효한 Access Manager 세션에 액세스할 수 있으며, 해당 세션을 사용하여 사용자를 설정할 수 있습니다. 기본 조직에서는 핵심 및 LDAP 인증 모듈을 모두 자동으로 사용할 수 있게 됩니다. 다음 지침은 모듈을 사용할 수 없는 경우를 위해 제공되었습니다.

LDAP 인증 추가 및 활성화

Access Manager 에 조직 관리자 또는 최상위 관리자로 로그인해야 합니다.

1. LDAP 인증을 추가할 조직으로 이동합니다.

2. 보기 메뉴에서 서비스를 선택합니다.

핵심 모듈을 이미 추가한 경우 이 내용이 이동 창에 표시됩니다. 핵심 모듈을 아직 추가하지 않은 경우 LDAP 인증 모듈과 함께 추가할 수 있습니다.

3. 이동 창에서 추가를 누릅니다.

사용 가능한 모듈 목록이 데이터 창에 표시됩니다.

4. LDAP 인증 확인란을 선택하고 추가를 누릅니다.

LDAP 인증 모듈이 이동 창에 표시되며 관리자는 이를 통해 해당 모듈이 추가되었음을 확인할 수 있습니다.

5. LDAP 인증 등록 정보 화살표를 누릅니다.

이 서비스에 대한 템플릿이 현재 없습니다. 지금 템플릿을 만드시겠습니까? 라는 메시지가 데이터 창에 표시됩니다.

6. 예를 누릅니다.

LDAP 인증 속성이 데이터 창에 표시됩니다. 필요에 따라 속성을 수정합니다. 이러한 속성에 대한 설명은 [23 장](#), "[LDAP 인증 속성](#)" 에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다.

7. 사용자 바인드용 비밀번호 속성에 비밀번호를 입력합니다. 기본적으로 설치하는 동안 입력된 `amldapuser` 비밀번호가 바인드 사용자로 사용됩니다. Directory Server 에서 익명 액세스를 통해 사용자 항목을 읽을수 있으면 이 단계를 생략할 수 있습니다.

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

8. 저장을 누릅니다.

LDAP 인증 모듈이 활성화되었습니다.

LDAP 인증을 사용하여 로그인

LDAP 인증을 사용하여 로그인하려면 [280 페이지의 "조직 인증 모듈"](#) 핵심 인증 모듈 속성을 수정하여 LDAP 인증을 활성화하고 선택해야 합니다. 이렇게 하면 사용자가 `http://hostname:port/server_deploy_URI/UI/Login?module=LDAP` 를 사용하여 로그인할 때 LDAP 인증 로그인 창이 표시됩니다. 사용 중인 인증 유형 (예 : 서비스 , 역할 , 사용자 , 조직)에 따라 인증 모듈을 기본값으로 구성할 경우 URL 에 모듈 이름을 지정할 필요가 없습니다.

LDAP 인증 페일오버 사용

LDAP 인증 속성은 주 Directory Server 와 보조 Directory Server 모두에 대한 값 필드를 포함합니다. Access Manager 는 주 서버가 사용 불가능할 경우 보조 서버를 통해 인증을 시도합니다. 자세한 내용은 LDAP 속성 [298 페이지의 "주 LDAP 서버"](#) 및 [298 페이지의 "보조 LDAP 서버"](#) 를 참조하십시오.

다중 LDAP 구성

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

구성원 인증

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

구성원 인증 추가 및 활성화

Access Manager 에 조직 관리자 또는 최상위 관리자로 로그인해야 합니다.

1. 구성원 인증을 추가할 조직으로 이동합니다.

2. 보기 메뉴에서 서비스를 선택합니다.

핵심 모듈을 이미 추가한 경우 이 내용이 이동 창에 표시됩니다. 핵심 모듈을 아직 추가하지 않은 경우 구성원 인증 모듈과 함께 추가할 수 있습니다.

3. 이동 창에서 추가를 누릅니다.

사용 가능한 모듈 목록이 데이터 창에 표시됩니다.

4. 구성원 인증 확인란을 선택하고 추가를 누릅니다.

구성원 인증 모듈이 이동 창에 표시되며 관리자는 이를 통해 해당 모듈이 추가되었음을 확인할 수 있습니다.

5. 구성원 인증 등록 정보 화살표를 누릅니다.

이 서비스에 대한 템플릿이 현재 없습니다. 지금 템플릿을 만드시겠습니까? 라는 메시지가 데이터 창에 표시됩니다.

6. 예를 누릅니다.

구성원 인증 속성이 데이터 창에 표시됩니다. 필요에 따라 속성을 수정합니다. 이러한 속성에 대한 설명은 [24 장](#), "[구성원 인증 속성](#)" 에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 선택하여 확인할 수 있습니다.

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

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

8. 저장을 누릅니다.

구성원 인증 모듈이 활성화되었습니다.

구성원 인증을 사용하여 로그인

구성원 인증을 사용하여 로그인하려면 280 페이지의 "조직 인증 모듈" 핵심 인증 모듈 속성을 수정하여 구성원 인증을 활성화하고 선택해야 합니다. 이렇게 하면 사용자가 `http://hostname:port/deploy_URI/UI/Login?module=Membership` 을 사용하여 로그인할 때 (대소문자 구분) 구성원 인증 로그인 (자동 등록) 창이 표시됩니다. 사용 중인 인증 유형 (예: 역할, 사용자, 조직)에 따라 인증 모듈을 기본값으로 구성할 경우 URL에 모듈 이름을 지정할 필요가 없습니다.

MSISDN 인증

MSISDN(Mobile Station Integrated Services Digital Network) 인증 모듈을 사용하면 휴대 전화와 같은 장치의 이동 가입자 ISDN 을 사용하여 인증할 수 있습니다. 이 모듈은 비대화식 모듈입니다. 가입자 ISDN 을 검색하고 이를 Directory Server 에서 검증하여 번호에 맞는 사용자를 찾습니다.

MSISDN 인증 추가 및 활성화

Access Server 에 조직 관리자나 최상위 관리자로 로그인해야 합니다.

1. MSISDN 인증을 추가할 조직으로 이동합니다.
2. 보기 메뉴에서 서비스를 선택합니다.

핵심 모듈을 이미 추가한 경우 이 내용이 이동 창에 표시됩니다. 핵심 모듈을 아직 추가하지 않은 경우 MSISDN 인증 모듈과 함께 추가할 수 있습니다.

3. 이동 창에서 추가를 누릅니다.
사용 가능한 모듈 목록이 데이터 창에 표시됩니다.
4. MSISDN 인증 확인란을 선택하고 추가를 누릅니다.

MSISDN 인증 모듈이 이동 창에 표시되며 관리자는 이를 통해 해당 모듈이 추가되었음을 확인할 수 있습니다.

5. MSISDN 인증 등록 정보 화살표를 누릅니다.

이 서비스에 대한 템플릿이 현재 없습니다. 지금 템플릿을 만드시겠습니까?
라는 메시지가 데이터 창에 표시됩니다.

6. 예를 누릅니다.

MSISDN 인증 속성이 데이터 창에 표시됩니다. 필요에 따라 속성을 수정합니다.

7. 저장을 누릅니다.

MSISDN 인증 모듈이 활성화되었습니다.

MSISDN 인증을 사용하여 로그인

MSISDN 인증을 사용하여 로그인하려면 [280 페이지](#)의 "조직 인증 모듈" 핵심 인증 모듈 속성을 수정하여 MSISDN 인증을 활성화하고 선택해야 합니다. 이렇게 하면 사용자가 `http://hostname:port/deploy_URI/UI/Login?module=MSISDN(대소문자 구분)` 을 사용하여 로그인할 때 MSISDN 인증 로그인 창이 표시됩니다. 사용 중인 인증 유형 (예: 서비스, 역할, 사용자, 조직)에 따라 인증 모듈을 기본값으로 구성할 경우 URL에 모듈 이름을 지정할 필요가 없습니다.

Windows NT 인증

Access Manager 를 구성하여 이미 설치된 NT/Windows 2000 서버에서 작업할 수 있습니다. Access Manager 는 NT 인증의 클라이언트 부분을 제공합니다.

1. Windows NT 서버를 구성합니다. 자세한 내용은 Windows NT 서버 설명서를 참조하십시오.
2. Windows NT 인증 모듈을 추가하여 사용 가능하게 하려면 Solaris 시스템의 Access Manager 와 통신하도록 Samba 클라이언트를 설치해야 합니다. 세부 사항에 대해서는 [313 페이지의 "Windows NT 인증 속성"](#) 을 참조하십시오.
3. Windows NT 인증 모듈을 추가하여 활성화합니다.

Samba 클라이언트 설치

Windows NT 인증 모듈을 활성화하려면 Samba Client 2.2.2 를 다운로드하여 다음 디렉토리에 설치해야 합니다.

```
AccessManager-base/SUNWam/bin
```

Samba Client 는 별도의 Windows NT/2000 Server 를 필요로 하지 않고 Windows 시스템과 UNIX 시스템을 블렌딩하는 파일 및 인쇄 서버입니다. 자세한 내용을 보거나 Samba Client 를 다운로드하려면

<http://www.sun.com/software/download/products/3e3af224.html> 에 액세스하십시오.

Red Hat Linux 는 Samba 클라이언트와 함께 제공됩니다. 이 클라이언트는 다음 디렉토리에 있습니다.

```
/usr/bin
```

Linux 용 Windows NT 인증 모듈을 사용하여 인증하려면 다음 Access Manager 디렉토리에 클라이언트 이진을 복사합니다.

```
AccessManager-base/sun/identity/bin
```

주 인터페이스가 여러 개인 경우에는 추가 구성이 필요합니다. smb.conf 파일에서 구성에 의해 다수의 인터페이스가 설정될 수 있으므로 mbclient 로 전달됩니다.

Windows NT 인증 추가 및 활성화

Access Manager 에 조직 관리자 또는 최상위 관리자로 로그인해야 합니다.

1. Windows NT 인증을 추가할 조직으로 이동합니다.

2. 보기 메뉴에서 서비스를 선택합니다.

핵심 모듈을 이미 추가한 경우 이 내용이 이동 창에 표시됩니다. 핵심 모듈을 아직 추가하지 않은 경우 Windows NT 인증 모듈과 함께 추가할 수 있습니다.

3. 이동 창에서 추가를 누릅니다.

사용 가능한 모듈 목록이 데이터 창에 표시됩니다.

4. Windows NT 인증 확인란을 선택하고 추가를 누릅니다.

Windows NT 인증 모듈이 이동 창에 표시되며 관리자는 이를 통해 해당 모듈이 추가되었음을 확인할 수 있습니다.

5. Windows NT 인증 등록 정보 화살표를 누릅니다.

이 서비스에 대한 템플릿이 현재 없습니다. 지금 템플릿을 만드시겠습니까? 라는 메시지가 데이터 창에 표시됩니다.

6. 예를 누릅니다.

Windows NT 인증 속성이 데이터 창에 표시됩니다. 필요에 따라 속성을 수정합니다. 이러한 속성에 대한 설명은 [26 장](#), "[Windows NT 인증 속성](#)" 에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 선택하여 확인할 수 있습니다.

7. 저장을 누릅니다.

Windows NT 인증 모듈이 활성화되었습니다.

Windows NT 인증을 사용하여 로그인

Windows NT 인증을 사용하여 로그인하려면 [280페이지의 "조직 인증 모듈"](#) 핵심 인증 모듈 속성을 수정하여 NT 인증을 활성화하고 선택해야 합니다. 이렇게 하면 사용자가 `http://hostname:port/deploy_URI/UI/Login?module=NT` 를 사용하여 로그인할 때 Windows NT 인증 로그인 창이 표시됩니다. 사용 중인 인증 유형 (예: 서비스, 역할, 사용자, 조직)에 따라 인증 모듈을 기본값으로 구성할 경우 URL에 모듈 이름을 지정할 필요가 없습니다.

RADIUS 서버 인증

Access Manager 를 구성하여 이미 설치된 RADIUS 서버에서 작업할 수 있습니다. 이렇게 하면 회사에서 레거시 RADIUS 서버를 사용하여 인증하는 경우에 유용합니다. RADIUS 인증 모듈을 활성화하려면 단계 2 프로세스를 거쳐야 합니다.

1. RADIUS 서버를 구성합니다.
자세한 내용은 RADIUS 서버 설명서를 참조하십시오.
2. RADIUS 인증 모듈을 등록하여 사용 가능하게 합니다.

RADIUS 인증 추가 및 활성화

Access Manager 에 조직 관리자로 로그인해야 합니다.

1. RADIUS 인증을 추가할 조직으로 이동합니다.
2. 보기 메뉴에서 서비스를 선택합니다.
핵심 모듈을 이미 추가한 경우 이 내용이 이동 창에 표시됩니다. 핵심 모듈을 아직 추가하지 않은 경우 RADIUS 인증 모듈과 함께 추가할 수 있습니다.
3. 이동 창에서 추가를 누릅니다.
사용 가능한 모듈 목록이 데이터 창에 표시됩니다.
4. RADIUS 인증 확인란을 선택하고 추가를 누릅니다.
RADIUS 인증 모듈이 이동 창에 표시되며 관리자는 이를 통해 해당 모듈이 추가되었음을 확인할 수 있습니다.
5. RADIUS 인증 등록 정보 화살표를 누릅니다.
이 서비스에 대한 템플릿이 현재 없습니다. 지금 템플릿을 만드시겠습니까?
라는 메시지가 데이터 창에 표시됩니다.
6. 예를 누릅니다.
RADIUS 인증 속성이 데이터 창에 표시됩니다. 필요에 따라 속성을 수정합니다. 이러한 속성에 대한 설명은 [27 장](#), "[RADIUS 인증 속성](#)" 에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 선택하여 확인할 수 있습니다.
7. 저장을 누릅니다.
RADIUS 인증 모듈이 활성화되었습니다.

RADIUS 인증을 사용하여 로그인

RADIUS 인증을 사용하여 로그인하려면 280 페이지의 "조직 인증 모듈" 핵심 인증 모듈 속성을 수정하여 RADIUS 인증을 활성화하고 선택해야 합니다. 이렇게 하면 사용자가 `http://hostname:port/deploy_URI/UI/Login?module=RADIUS` 를 사용하여 로그인할 때 RADIUS 인증 로그인 창이 표시됩니다. 사용 중인 인증 유형 (예: 서비스, 역할, 사용자, 조직)에 따라 인증 모듈을 기본값으로 구성할 경우 URL에 모듈 이름을 지정할 필요가 없습니다.

Sun ONE Application Server 에서 RADUIS 구성

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

- 적용
- 연결
- 수신
- 결정

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

```
host = hostname | IPaddress:portrange:portrange = portnumber |
-portnumberportnumber-portnumber
```

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

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

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

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

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

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

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

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

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

SafeWord 인증

Access Manager 를 구성하여 Secure Computing 의 SafeWord™ 또는 SafeWord PremierAccess™ 인증 서버에 대한 SafeWord 인증 요청을 처리할 수 있습니다. Access Manager 는 SafeWord 인증의 클라이언트 부분을 제공합니다. SafeWord 서버는 Access Manager 가 설치되는 시스템이나 별도의 시스템에 위치할 수 있습니다.

SafeWord 인증 추가 및 활성화

Access Manager 에 조직 관리자 또는 최상위 관리자로 로그인해야 합니다.

1. SafeWord 인증을 추가할 조직으로 이동합니다.
2. 보기 메뉴에서 서비스를 선택합니다.

핵심 모듈을 이미 추가한 경우 이 내용이 이동 창에 표시됩니다. 핵심 모듈을 아직 추가하지 않은 경우 SafeWord 인증 모듈과 함께 추가할 수 있습니다.

3. 이동 창에서 추가를 누릅니다.

사용 가능한 모듈 목록이 데이터 창에 표시됩니다.

4. SafeWord 인증 확인란을 선택하고 추가를 누릅니다.

SafeWord 인증 모듈이 이동 창에 표시되며 관리자는 이를 통해 해당 모듈이 추가되었음을 확인할 수 있습니다.

5. SafeWord 인증 등록 정보 화살표를 누릅니다.

이 서비스에 대한 템플릿이 현재 없습니다. 지금 템플릿을 만드시겠습니까? 라는 메시지가 데이터 창에 표시됩니다.

6. 예를 누릅니다.

SafeWord 인증 속성이 데이터 창에 표시됩니다. 필요에 따라 속성을 수정합니다. 이러한 속성에 대한 설명은 28 장, "SafeWord 인증 속성"에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다.

7. 저장을 누릅니다.

SafeWord 인증 모듈이 활성화되었습니다.

SafeWord 인증을 사용하여 로그인

SafeWord 인증을 사용하여 로그인하려면 280 페이지의 "조직 인증 모듈" 핵심 인증 모듈 속성을 수정하여 SafeWord 인증을 활성화하고 선택해야 합니다. 이렇게 하면 사용자가 `http://hostname:port/deploy_URI/UI/Login?module=SafeWord` 를 사용하여 로그인할 때 SafeWord 인증 로그인 창이 표시됩니다. 사용 중인 인증 유형 (예: 역할, 사용자, 조직)에 따라 인증 모듈을 기본값으로 구성할 경우 URL에 모듈 이름을 지정할 필요가 없습니다.

Sun ONE Application Server에서 SafeWord 구성

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

- 적용
- 연결
- 수신
- 결정

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

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

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

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

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

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

```
permission java.net.SocketPermission machine1.example.com:5030,
"connect,accept";
```

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

```
permission java.net.SocketPermission "machine1.example.com:5030",
"connect,accept";
```

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

주

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

SAML 인증

SAML(Security Assertion Markup Language) 인증 모듈은 대상 서버에서 SAML 명제를 받아 검증합니다. SAML SSO 는 업그레이드 (예 : Access Manager 2004Q2 를 Access Manager 2005Q1 로) 이후를 포함하여 이 모듈을 대상 컴퓨터에 구성한 경우에만 작동됩니다.

SAML 인증 추가 및 활성화

Access Manager 에 조직 관리자 또는 최상위 관리자로 로그인해야 하며 LDAP 인증 모듈이 이미 등록되어 있어야 합니다.

1. SAML 인증을 추가할 조직으로 이동합니다.

2. 보기 메뉴에서 서비스를 선택합니다.

핵심 모듈을 이미 추가한 경우 이 내용이 이동 창에 표시됩니다. 핵심 모듈을 아직 추가하지 않은 경우 SAML 인증 모듈과 함께 추가할 수 있습니다.

3. 이동 창에서 추가를 누릅니다.

사용 가능한 모듈 목록이 데이터 창에 표시됩니다.

4. SAML 인증 확인란을 선택하고 추가를 누릅니다.

SAML 인증 모듈이 이동 창에 표시되며 관리자는 이를 통해 해당 모듈이 추가되었음을 확인할 수 있습니다.

5. SAML 인증 등록 정보 화살표를 누릅니다.

이 서비스에 대한 템플릿이 현재 없습니다. 지금 템플릿을 만드시겠습니까? 라는 메시지가 데이터 창에 표시됩니다.

6. 만들기를 누릅니다.

SAML 인증 속성이 데이터 창에 표시됩니다. 필요에 따라 속성을 수정합니다. 이러한 속성에 대한 설명은 21 장, "[HTTP 기본 인증 속성](#)" 에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다.

7. 저장을 누릅니다.

SAML 인증 모듈이 활성화되었습니다.

SAML 인증을 사용하여 로그인

SAML 인증을 사용하여 로그인하려면 [280 페이지](#)의 "조직 인증 모듈" 핵심 인증 모듈 속성을 수정하여 HTTP 기본 인증을 활성화하고 선택해야 합니다. 이렇게 하면 사용자가 `http://hostname:port/server_deploy_URI/UI/Login?module=SAML` 를 사용하여 로그인할 때 인증 로그인 창이 표시됩니다. 사용 중인 인증 유형 (예: 서비스, 역할, 사용자, 조직)에 따라 인증 모듈을 기본값으로 구성할 경우 URL에 모듈 이름을 지정할 필요가 없습니다.

SecurID 인증

Access Manager 를 구성하여 RSA 의 ACE/Server 인증 서버에 대한 SecureID 인증 요청을 처리할 수 있습니다. Access Manager 는 SecurID 인증의 클라이언트 부분을 제공합니다. ACE/Server 는 Access Manager 가 설치되는 시스템이나 별도의 시스템에 위치할 수 있습니다. 로컬로 관리되는 사용자 아이디 (admintool(1M) 참조) 를 인증하려면 루트로 액세스해야 합니다.

Unix 인증에서는 인증 `도우미/amsecuridd` 가 사용됩니다. 이 프로세스는 메인 Access Manager 프로세스와 별도의 프로세스입니다. 시작 시에 이 도우미는 하나의 포트에서 구성 정보를 수신합니다. Access Manager 를 설치하여 nobody 또는 루트가 아닌 사용자 아이디로 실행할 경우에도

`AccessManager-base/SUNWam/share/bin/amsecuridd` 프로세스는 여전히 루트로 실행되어야 합니다. amsecuridd 도우미에 대한 자세한 내용은 [237 페이지](#)의 "amsecuridd 도우미" 를 참조하십시오.

주 이번 Access Manager 릴리스에서 SecurID 인증 모듈은 Linux 또는 Solaris x86 플랫폼을 지원하지 않으므로 이 두 플랫폼에서 등록, 구성 및 활성화할 수 없습니다. 오직 Solaris 에만 사용할 수 있습니다.

SecurID 인증 추가 및 활성화

Access Manager 에 조직 관리자 또는 최상위 관리자로 로그인해야 합니다.

1. SecurID 인증을 추가할 조직으로 이동합니다.

2. 보기 메뉴에서 서비스를 선택합니다.

핵심 모듈을 이미 추가한 경우 이 내용이 이동 창에 표시됩니다. 핵심 모듈을 아직 추가하지 않은 경우 SecurID 인증 모듈과 함께 추가할 수 있습니다.

3. 이동 창에서 추가를 누릅니다.

사용 가능한 모듈 목록이 데이터 창에 표시됩니다.

4. SecurID 인증 확인란을 선택하고 추가를 누릅니다.

SecurID 인증 모듈이 이동 창에 표시되며 관리자는 이를 통해 해당 모듈이 추가되었음을 확인할 수 있습니다.

5. SecurID 인증 등록 정보 화살표를 누릅니다.

이 서비스에 대한 템플릿이 현재 없습니다. 지금 템플릿을 만드시겠습니까? 라는 메시지가 데이터 창에 표시됩니다.

6. 예를 누릅니다.

SecurID 인증 속성이 데이터 창에 표시됩니다. 필요에 따라 속성을 수정합니다. 이러한 속성에 대한 설명은 30 장, "SecurID 인증 속성" 에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다.

7. 저장을 누릅니다.

SecurID 인증 모듈이 활성화되었습니다.

SecurID 인증을 사용하여 로그인

SecurID 인증을 사용하여 로그인하려면 280 페이지의 "조직 인증 모듈" 핵심 인증 모듈 속성을 수정하여 SecurID 인증을 활성화하고 선택해야 합니다. 이렇게 하면 사용자가 `http://hostname:port/deploy_URI/UI/Login?module=SecurID` 를 사용하여 로그인할 때 SecurID 인증 로그인 창이 표시됩니다. 사용 중인 인증 유형 (예 : 역할, 사용자, 조직) 에 따라 인증 모듈을 기본값으로 구성할 경우 URL 에 모듈 이름을 지정할 필요가 없습니다.

Unix 인증

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

Unix 인증에서는 인증 도우미/amunixd가 사용됩니다. 이 프로세스는 메인 Access Manager 프로세스와 별도의 프로세스입니다. 시작 시에 이 도우미는 하나의 포트에서 구성 정보를 수신합니다. 각 Access Manager 에는 모든 조직에 서비스를 제공하는 Unix 도우미가 하나씩만 있습니다.

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

```
./amunixd
```

기본 포트가 아닌 포트에서 amunixd 를 실행하려면 다음 명령을 입력합니다.

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

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

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

Unix 인증 추가 및 활성화

Access Manager 에 최상위 관리자로 로그인하여 다음 단계를 수행합니다 .

1. 서비스 구성 모듈을 선택합니다 .

2. 서비스 이름 목록에서 Unix 인증 등록 정보 화살표를 누릅니다 .

여러 전역 속성과 하나의 조직 속성이 표시됩니다 . 하나의 Unix 도우미가 모든 Access Manager 서버 조직에 서비스를 제공하기 때문에 대부분의 Unix 속성은 전역입니다 . 이러한 속성에 대한 설명은 31 장 , "Unix 인증 속성 " 에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다 .

3. 저장을 눌러 새 속성 값을 저장합니다 .

Access Manager 에 조직 관리자로 로그인하여 조직에 대한 Unix 인증을 사용 가능하게 할 수도 있습니다 .

4. Unix 인증을 추가할 조직으로 이동합니다 .

5. 보기 메뉴에서 서비스를 선택합니다 .

핵심 모듈을 이미 추가한 경우 이 내용이 이동 창에 표시됩니다 . 핵심 모듈을 아직 추가하지 않은 경우 Unix 인증 모듈과 함께 추가할 수 있습니다 .

6. 이동 창에서 추가를 누릅니다 .

사용 가능한 모듈 목록이 데이터 창에 표시됩니다 .

7. Unix 인증 확인란을 선택하고 추가를 누릅니다 .

Unix 인증 모듈이 이동 창에 표시되며 관리자는 이를 통해 해당 모듈이 추가되었음을 확인할 수 있습니다 .

8. Unix 인증 등록 정보 화살표를 누릅니다 .

이 서비스에 대한 템플릿이 현재 없습니다 . 지금 템플릿을 만드시겠습니까? 라는 메시지가 데이터 창에 표시됩니다 .

9. 예를 누릅니다 .

Unix 인증 조직 속성이 데이터 창에 표시됩니다 . 필요한 경우 인증 수준 속성을 수정합니다 . 이 속성에 대한 설명은 31 장 , "Unix 인증 속성 " 에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다 .

10. 저장을 누릅니다 . Unix 인증 모듈이 활성화되었습니다 .

Unix 인증을 사용하여 로그인

Unix 인증을 사용하여 로그인하려면 280 페이지의 "조직 인증 모듈" 핵심 인증 모듈 속성을 수정하여 Unix 인증을 활성화하고 선택해야 합니다. 이렇게 하면 사용자가 `http://hostname:port/deploy_URI/UI/Login?module=Unix` 를 사용하여 로그인할 때 Unix 인증 로그인 창이 표시됩니다. 사용 중인 인증 유형 (예: 서비스, 역할, 사용자, 조직)에 따라 인증 모듈을 기본값으로 구성할 경우 URL에 모듈 이름을 지정할 필요가 없습니다.

Windows 데스크탑 SSO 인증

Windows 데스크탑 SSO 인증 모듈은 Windows 2000™에 사용되는 커버로스 기반 인증 플러그인 모듈입니다. 여기서는 Kerberos Distribution Center(KDC)에 대해 이미 인증된 사용자가 로그인 조건을 제출하지 않고 Identity Sever에서 인증될 수 있습니다 (단일 사인 온).

사용자는 SPNEGO(Simple and Protected GSS-API Negotiation Mechanism) 프로토콜을 통해 Access Manager에 커버로스 토큰을 제공합니다. 이 인증 모듈을 통해 Access Manager에 커버로스 기반 싱글 사인 온을 수행하려면 사용자는 클라이언트 측에서 자신을 인증하도록 SPNEGO 프로토콜을 지원해야 합니다. 일반적으로 이 프로토콜을 지원하는 사용자는 이 모듈을 사용하여 Access Manager에 인증할 수 있습니다. 클라이언트측의 토큰 가용성에 따라 이 모듈은 SPENGO 토큰을 제공하거나 커버로스 토큰 (두 경우 모두 프로토콜 동일)을 제공하게 됩니다. 현재 Windows 2000 이상 버전에서 실행되는 Microsoft Internet Explorer(5.01 이상)에서 이러한 프로토콜을 지원합니다. 또한 Solaris(9 10) Mozilla 1.4도 SPNEGO 지원 기능이 있으나 Solaris에서 SPNEGO를 지원하지 않으므로 반환되는 토큰은 커버로스 토큰뿐입니다.

주 커버로스 V5 인증 모듈의 새 기능을 활용하려면 JDK 1.4 이상을 사용하고 이 SPNEGO 모듈에서 커버로스 기반 SSO를 수행하려면 Java GSS API를 사용해야 합니다.

Internet Explorer 의 알려진 제한 사항

WindowsDesktopSSO 인증에 Microsoft Internet Explorer 6.x 를 사용하는 중 이 브라우저에 WindowsDesktopSSO 모듈에 구성된 (KDC) 영역에 일치하는 사용자의 커버로스 /SPNEGO 토크에 대한 액세스 권한이 없는 경우, 해당 브라우저는 WindowsDesktopSSO 모듈 인증 실패 후 다른 모듈에 대해 제대로 작동되지 않습니다. 이 문제의 직접적인 원인은 Internet Explorer 에서 WindowsDesktopSSO 모듈 실패 후 다른 모듈의 콜백이 프롬프트에 표시되는 경우에도 브라우저에서 이를 Access Manager 에 전달할 수 없기 때문이며, 이러한 불능 상태는 브라우저를 다시 시작할 때까지 계속됩니다. 즉 null 사용자 자격 증명 때문에 WindowsDesktopSSO 실패 후 수신한 모든 모듈도 실패합니다.

자세한 내용은 다음 설명서를 참조하십시오.

<http://support.microsoft.com/default.aspx?scid=kb;en-us;308074>

<http://www.wedgetail.com/jcsi/sso/doc/guide/troubleshooting.html#ieNTLM>

Windows 데스크탑 SSO 인증 추가 및 활성화

Windows 데스크탑 SSO 인증을 사용 가능하게 하는 단계 3 프로세스는 다음과 같습니다.

1. Windows 2000 도메인 제어기에서 사용자를 생성합니다.
2. Internet Explorer 를 설정합니다.
3. Windows 데스크탑 SSO 인증 모듈을 추가하고 구성합니다.

Windows 2000 도메인 제어기에서 사용자를 생성하려면

1. 도메인 제어기에서 Access Manager 인증 모듈에 사용할 사용자 계정을 만듭니다.
 - a. 시작 메뉴에서 프로그램 > 관리 도구로 이동합니다.
 - b. 활성 디렉토리 및 컴퓨터를 선택합니다.
 - c. 사용자 아이디(로그인 이름)가 Access Manager 호스트 이름인 새 사용자를 만듭니다. Access Manager 호스트 이름에는 도메인 이름이 포함되지 않아야 합니다.

2. 사용자 계정을 서비스 공급자 이름과 연결하고 Access Manager 가 설치된 시스템으로 키탭 파일을 내보냅니다. 그러려면 다음 명령을 실행합니다.

```
ktpass -princ host/hostname.domainname@DCDOMAIN -pass password -mapuser  
userName-out hostname.host.keytab
```

```
ktpass -princ HTTP/hostname.domainname@DCDOMAIN -pass password -mapuser  
userName-out hostname.host.keytab
```

ktpass 명령에는 다음과 같은 매개 변수가 사용됩니다.

hostname. Access Manager 를 실행하는 호스트 이름 (도메인 이름 없음)입니다.

domainname. Access Manager 도메인 이름

DCDOMAIN. 도메인 제어기의 도메인 이름입니다. Access Manager 도메인 이름과 다를 수도 있습니다.

password. 사용자 계정의 비밀번호입니다. ktpass 에서는 비밀번호를 확인하지 않으므로 비밀번호가 정확한지 확인합니다.

userName. 사용자 계정 아이디입니다. 호스트 이름과 같아야 합니다.

주 두 키탭 파일이 모두 안전하게 보존되는지 확인합니다.

3. 서버를 다시 시작합니다.

Internet Explorer 를 설정하려면

이 단계는 Microsoft Internet Explorer™ 6 이상에 적용됩니다. 이전 버전을 사용하는 경우에는 Access Manager 가 브라우저의 인터넷 영역에 있는지 확인한 다음 고유 Windows 인증을 활성화합니다.

1. 도구 메뉴에서 인터넷 옵션 > 고급 / 보안 > 보안으로 갑니다.
2. 통합된 Windows 인증 사용 옵션을 선택합니다.
3. 보안 > 로컬 인터넷으로 갑니다.
 - a. 사용자 지정 수준을 선택합니다. 사용자 인증 / 로그인 창에서 인터넷 영역에서만 자동으로 로그인 옵션을 선택합니다.
 - b. 사이트로 가서 옵션을 모두 선택합니다.
 - c. 고급을 누르고 로컬 영역에 Access Manager 를 추가합니다 (아직 추가되지 않은 경우).

Internet Explorer 의 알려진 제한 사항

WindowsDesktopSSO 인증에 Microsoft Internet Explorer 6.x 를 사용하는데 이 브라우저에 WindowsDesktopSSO 모듈에 구성된 (KDC) 영역에 일치하는 사용자의 커버로스 /SPNEGO 토큰에 대한 액세스 권한이 없는 경우, 해당 브라우저는 WindowsDesktopSSO 모듈 인증 실패 후 다른 모듈에 대해 제대로 작동되지 않습니다. 이 문제의 직접적인 원인은 Internet Explorer 에서 WindowsDesktopSSO 모듈 실패 후 다른 모듈의 콜백이 프롬프트에 표시되는 경우에도 브라우저에서 이를 Access Manager 에 전달할 수 없기 때문이며, 이러한 불능 상태는 브라우저를 다시 시작할 때까지 계속됩니다. 즉 null 사용자 자격 증명 때문에 WindowsDesktopSSO 실패 후 수신한 모든 모듈도 실패합니다.

자세한 내용은 다음 설명서를 참조하십시오.

<http://support.microsoft.com/default.aspx?scid=kb;en-us;308074>

<http://www.wedgetail.com/jcsi/sso/doc/guide/troubleshooting.html#ieNTLM>

Windows 데스크탑 SSO 인증을 추가하고 구성하려면

Access Manager 에 조직 관리자 또는 최상위 관리자로 로그인해야 합니다.

1. Windows 데스크탑 SSO 인증을 추가할 조직으로 이동합니다.
2. 보기 메뉴에서 서비스를 선택합니다.

핵심 모듈을 이미 추가한 경우 이 내용이 이동 창에 표시됩니다. 핵심 모듈을 아직 추가하지 않은 경우에는 Windows Desktop SSO 인증 모듈과 함께 추가할 수 있습니다.

3. 이동 창에서 추가를 누릅니다.

사용 가능한 모듈 목록이 데이터 창에 표시됩니다.

4. Windows 데스크탑 SSO 인증 확인란을 선택하고 추가를 누릅니다.

Windows 데스크탑 SSO 인증 모듈이 이동 창에 표시되며 관리자는 이를 통해 해당 모듈이 추가되었음을 확인할 수 있습니다.

5. Windows 데스크탑 SSO 인증 등록 정보 화살표를 누릅니다.

이 서비스에 대한 템플릿이 현재 없습니다. 지금 템플릿을 만드시겠습니까? 라는 메시지가 데이터 창에 표시됩니다.

6. 예를 누릅니다 .

Windows 데스크탑 SSO 인증 속성이 데이터 창에 표시됩니다 . 필요에 따라 속성을 수정합니다 . 이러한 속성에 대한 설명은 32 장 , "Windows 데스크탑 SSO 인증 속성 " 에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 선택하여 확인할 수 있습니다 .

7. 저장을 누릅니다 . Windows Desktop SSO 인증 모듈을 사용할 수 있게 됩니다 .

Windows 데스크탑 SSO 인증을 사용하여 로그인

Windows 데스크탑 SSO 인증을 사용하여 로그인하려면 280 페이지의 " 조직 인증 모듈 " 핵심 인증 모듈을 수정하여 Windows 데스크탑 SSO 인증을 활성화하고 선택해야 합니다 . 이렇게 하면 Windows 2000 도메인 제어기의 일부이고

`http://hostname:port/deploy_URI/UI/Login?module=WindowsDesktopSSO`를 사용하여 도메인 사용자로 로그인한 호스트에서 로그인하는 사용자가 인증을 받을 수 있습니다 . 사용 중인 인증 유형 (예 : 서비스 , 역할 , 사용자 , 조직) 에 따라 인증 모듈을 기본값으로 구성할 경우 URL 에 모듈 이름을 지정할 필요가 없습니다 .

비밀번호 재설정 서비스

Sun Java™ System Access Manager 6 2005Q1 는 사용자가 Access Manager 에 의해 보호되는 지정된 서비스 또는 응용 프로그램에 액세스하기 위한 비밀번호를 재설정할 수 있도록 비밀번호 재설정 서비스를 제공합니다. 최상위 수준 관리자에 의해 정의되는 비밀번호 재설정 서비스 속성은 사용자 검증 자격 증명 (*비밀 문제* 형식) 을 제어하고 , 새 비밀번호 알림 또는 기존 비밀번호 알림에 대한 메커니즘을 제어하며 , 잘못된 사용자 검증에 대한 가능한 잠금 간격을 설정합니다 .

이번 장은 다음 절로 구성됩니다 .

- 207 페이지의 " 비밀번호 재설정 서비스 등록 "
- 208 페이지의 " 비밀번호 재설정 서비스 구성 "
- 210 페이지의 " 최종 사용자에게 대한 비밀번호 재설정 "

비밀번호 재설정 서비스 등록

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

다른 조직의 사용자에게 대해 비밀번호 재설정을 등록하려면

1. [아이디 관리] 모듈에서 [조직]을 선택하고 서비스를 등록할 조직을 선택합니다.
2. 이동 프레임에서 등록을 누릅니다 .

사용 가능한 서비스 목록이 데이터 프레임에 표시됩니다 .

3. [비밀번호 재설정] 확인란을 선택하고 [등록] 을 누릅니다.

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

비밀번호 재설정 서비스 구성

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

서비스를 구성하려면

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

데이터 프레임에 " 이 서비스에 사용 가능한 템플릿이 없습니다 " 라는 메시지가 표시됩니다. [만들기] 를 누릅니다.

3. 비밀번호 재설정 속성이 데이터 프레임에 표시되고 사용자는 이 속성을 사용하여 비밀번호 재설정 서비스에 대한 요구 사항을 정의할 수 있습니다. 비밀번호 재설정 서비스가 사용 가능 (기본값) 한지 확인합니다. 최소한 다음 속성을 정의해야 합니다.

- 사용자 검증
- 비밀 문제
- 바인드 DN
- 바인드 비밀번호

바인드 DN 속성은 비밀번호 재설정 권한이 있는 사용자 (예 : 도움말 데스크 관리자) 를 포함해야 합니다. Directory Server 의 제한 때문에 바인드 DN 이 cn=directory manager 인 경우에는 비밀번호 재설정이 실행되지 않습니다.

나머지 속성은 선택 사항입니다. 비밀번호 재설정 속성에 대한 설명은 357 페이지의 " 비밀번호 재설정 서비스 속성 " 에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 [도움말] 링크를 눌러 확인할 수 있습니다.

주 Access Manager 는 임의의 비밀번호 생성을 위한 비밀번호 재설정 웹 응용 프로그램을 자동으로 설치합니다 . 그러나 비밀번호 생성 및 비밀번호 알림을 위한 사용자 플러그인 클래스를 작성할 수 있습니다 . 이러한 플러그인 클래스에 대해서는 다음 위치에 있는 다음 `Readme.html` 파일을 참조하십시오 .

PasswordGenerator:

AccessManager-base/SUNWam/samples/console/PasswordGenerator

NotifyPassword:

AccessManager-base/SUNWam/samples/console/NotifyPassword

4. 사용자가 고유 개인 문제를 직접 정의해야 하는 경우 [개인 문제 사용 가능] 속성을 선택합니다 . 속성을 정의한 다음 [저장] 을 누릅니다 .

비밀번호 재설정 잠금

비밀번호 재설정 서비스에는 사용자가 비밀 문제에 올바르게 응답하기 위해 시도할 수 있는 횟수를 제한하는 잠금 기능이 포함됩니다 . 잠금 기능은 비밀번호 재설정 서비스 속성을 통해 구성됩니다 . 이러한 속성에 대한 설명은 [357 페이지의 " 비밀번호 재설정 서비스 속성 "](#)에서 확인할 수 있습니다 . 비밀번호 재설정은 메모리 잠금과 물리적 잠금이라는 두 가지 유형의 잠금을 지원합니다 .

메모리 잠금

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

물리적 잠금

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

최종 사용자에게 대한 비밀번호 재설정

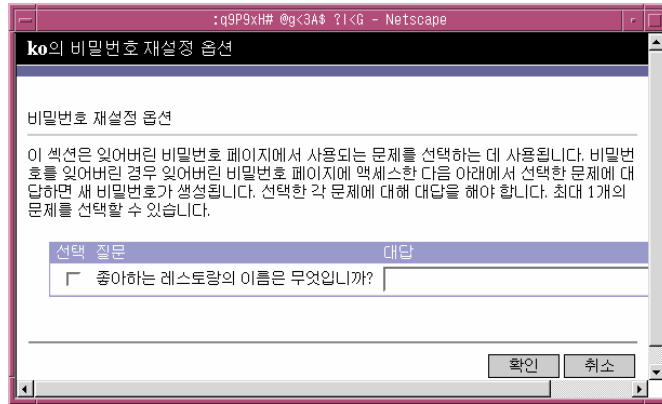
다음 절에서는 비밀번호 재설정 서비스에 대한 사용자 경험을 설명합니다.

비밀번호 재설정 사용자 정의

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

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

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



5. [저장] 을 누릅니다.

잊어버린 비밀번호 재설정

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

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

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

또는

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

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

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

2. 사용자 아이디를 입력합니다 .

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

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

비밀번호 정책

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

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

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

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

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

명령줄 참조 설명서

Sun Java™ System Access Manager 6 2005Q1 관리 설명서의 3 부 명령줄 참조 설명서입니다. 이 부분은 다음 내용으로 구성되어 있습니다.

- 215 페이지의 "amadmin 명령줄 도구 "
- 223 페이지의 "amserver 명령줄 도구 "
- 231 페이지의 "ampassword 명령줄 도구 "
- 225 페이지의 "am2bak 명령줄 도구 "
- 229 페이지의 "bak2am 명령줄 도구 "
- 235 페이지의 "VerifyArchive 명령줄 도구 "
- 237 페이지의 "amsecuridd 도우미 "

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

AccessManager-base/SUNWam/bin (Solaris)

AccessManager-base/identity/bin (Linux)

amadmin 명령줄 도구

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

- [215 페이지의 "amadmin 명령줄 도구"](#)

amadmin 명령줄 실행 파일

명령줄 실행 파일 amadmin 의 주 목적은 XML 서비스 파일을 Directory Server 로 로드하고 DIT 에서 일괄 관리 작업을 수행하는 것입니다. amadmin 은 AccessManager-base/SUNWam/bin 에 위치하며 다음 작업을 수행하는 데 사용됩니다.

- XML 서비스 파일 로드 - 관리자가 sms.dtd 에 정의된 XML 서비스 파일 형식을 사용하는 Access Manager 로 서비스를 로드합니다. 모든 서비스는 amadmin 을 사용하여 로드해야 하며, Access Manager 콘솔을 통해 가져올 수 없습니다.

주 XML 서비스 파일은 Access Manager 에서 참조하는 XML 데이터의 정적 blob 으로 Directory Server 에 저장됩니다. 이 정보는 LDAP 만 이해하는 Directory Server 에서는 사용되지 않습니다.

- DIT 에 대한 identity 객체 일괄 업데이트 수행 - 관리자는 amadmin.dtd 에 정의된 일괄 처리 XML 파일 형식을 사용하여 Directory Server DIT 를 일괄적으로 업데이트할 수 있습니다. 예를 들어, 관리자가 10 개의 조직, 100 명의 사용자 및 100 개의 그룹을 만들고자 할 경우 하나 이상의 일괄 처리 XML 파일에 요청을 입력한 다음 amadmin 을 사용하여 로드하여 해당 작업을 한 번에 수행할 수 있습니다. 이 작업에 관한 자세한 내용은 *Access Manager Developer's Guide* 의 "Service Management" 장을 참조하십시오.

주 amadmin 은 Access Manager 콘솔에서 지원하고 교체할 필요가 없는 일부 기능만 지원 합니다. 소량의 관리 작업에는 콘솔을 사용하고 대용량의 관리 작업에는 amadmin 을 사용하는 것이 좋습니다.

amadmin 구문

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

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

주 구문에 표시된 것처럼 두 개의 하이픈을 정확하게 입력해야 합니다.

amadmin 옵션

amadmin 명령줄 매개 변수 옵션의 정의는 다음과 같습니다.

--runasdn (-u)

--runasdn 은 LDAP 서버에 사용자를 인증하는 데 사용됩니다. 인자는 amadmin 을 실행하도록 인증된 사용자의 고유 이름 (DN) 인수와 동일한 값입니다. 예를 들면 다음과 같습니다.

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

각 도메인 구성 요소 사이에 공백을 삽입하고 전체 DN 을 큰 따옴표로 묶어 (예 : --runasdn "uid=amAdmin, ou=People, o=iplanet.com, o=isp") DN 서식을 지정할 수도 있습니다.

--password (-w)

--password 는 필수 옵션이며 --runasdn 옵션으로 지정한 DN 의 비밀번호와 동일한 값을 가집니다.

--locale (-l)

--locale 은 로케일 이름과 동일한 값을 갖는 옵션입니다. 이 옵션은 메시지 언어 사용자 정의에 사용될 수 있습니다. 이 옵션을 지정하지 않으면 기본 로케일 en_US 가 사용됩니다.

--continue (-c)

--continue 는 오류가 발생하더라도 XML 파일 처리를 계속하라는 옵션입니다. 예를 들어, 세 XML 파일을 동시에 로드할 때 첫 번째 XML 파일이 실패할 경우 amadmin 은 나머지 파일을 계속해서 로드합니다. 계속 옵션은 별도 요청에만 적용됩니다.

--session (-m)

--session (-m) 은 세션을 관리하거나 현재 세션을 표시하는 옵션입니다.

--runasdn 을 지정할 경우 AMConfig.properties 에 있는 슈퍼유저의 DN 또는 최상위 관리자의 아이디와 같아야 합니다.

다음 예에서는 특정 서비스 호스트 이름에 대한 모든 세션을 표시합니다.

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

다음 예에서는 특정 사용자 세션을 표시합니다.

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

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

다음 옵션을 사용하는 경우 :

```
amadmin -m | --session servername pattern
```

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

--debug (-d)

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

```
CLASSPATH=$CLASSPATH:/opt/IS61/SUNWam/lib/mysql-connector-java-3.0.6-stable-bin.jar
export CLASSPATH
```

--verbose (-v)

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

--data (-t)

--data는 가져올 일괄 처리 XML 파일 이름을 값으로 갖는 옵션입니다 . XML 파일을 하나 이상 지정할 수 있습니다 . 이 XML 파일은 서비스를 등록 및 등록 취소할 수 있을 뿐만 아니라 다양한 디렉토리 객체를 만들고 , 삭제하고 , 읽을 수 있습니다 . 이 옵션에 전달될 수 있는 XML 파일 유형에 대한 자세한 내용은 *Access Manager Developer's Guide* 의 "Servic Management" 장을 참조하십시오 .

--schema (-s)

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

주 DIT 에 대한 일괄 업데이트를 구성하는지 서비스 스키마 및 구성 데이터를 로드하는 지에 따라 --data 또는 --schema 옵션을 지정해야 합니다 .

--deleteservice (-r)

--deleteservice 는 서비스와 해당 스키마만 삭제하는 옵션입니다.

--serviceName

--serviceName은 XML 서비스 파일의 Service name=... 태그에 정의되는 서비스 이름과 같은 값을 갖는 옵션입니다. 해당 내용이 [219 페이지의 코드 예 9-1](#)에 표시되어 있습니다.

코드 예 9-1 sampleMailService.xml 의 부분

```

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

```

--help (-h)

--help 는 amadmin 명령에 대한 구문을 표시하는 인수입니다.

--version (-n)

--version은 유틸리티 이름, 제품 이름, 제품 버전 및 사용권에 대한 고지 사항을 표시하는 인수입니다.

연합 관리를 위해 amadmin 사용

이 절에서는 연합 관리와 함께 사용하는 amadmin 매개 변수를 나열합니다. 연합 관리에 대한 자세한 내용은 *Access Manager Federation Management Guide* 를 참조하십시오.

Directory Server 에 Liberty 메타 호환 XML 로드

```

amadmin -u|--runasdn <user's DN>
    -w|--password <password> or -f|--passwordfile <passwordfile>
    -e|--entityname <entity name>
    -g|--import <xmlfile>

```

--runasdn (-u)

사용자의 DN

--password (-w)

사용자의 비밀번호 .

--passwordfile (-f)

사용자의 비밀번호가 포함된 파일의 이름 .

--entityname (-e)

엔티티 이름 . 예 : <http://www.example.com>

하나의 엔티티는 하나의 조직에만 소속되어야 합니다 .

--import (-g)

메타 정보가 포함된 XML 파일의 이름 . 이 파일은 Liberty 메타 사양과 XSD 를 준수해야 합니다 .

XML 파일에 엔티티 내보내기 (XML 디지털 서명 사용 안 함)

amadmin -u|--runasdn <user's DN>

-w|--password <password> or -f|--passwordfile <passwordfile>

-e|--entityname <entity name>

-o|--export <filename>

--runasdn (-u)

사용자의 DN

--password (-w)

사용자의 비밀번호 .

--passwordfile (-f)

사용자의 비밀번호가 포함된 파일의 이름 .

--entityname (-e)

Directory Server 에 상주하는 엔티티의 이름

--export (-o)

엔티티의 XML 이 포함된 파일의 이름 . XML 은 Liberty 메타 XSD 를 준수합니다 .

XML 파일에 엔티티 내보내기 (XML 디지털 서명 사용)

```
amadmin -u|--runasdn <user's DN>
    -w|--password <password> or -f|--passwordfile <passwordfile>
    -e|--entityname <entity name>
    -q|--exportwithsig <filename>
```

--runasdn (-u)

사용자의 DN

--password (-w)

사용자의 비밀번호.

--passwordfile (-f)

사용자의 비밀번호가 포함된 파일의 이름.

--entityname (--e)

Directory Server 에 상주하는 엔티티의 이름

--exportwithsig (-o)

엔티티의 XML 이 포함된 파일의 이름 . 이 파일에는 디지털 서명이 추가됩니다 .
XML 은 Liberty 메타 XSD 호환이어야 합니다 .

자원 번들에 대해 amadmin 사용

다음 절에서는 자원 번들을 추가 , 위치 파악 및 제거하기 위한 amadmin 구문을 보여줍니다 .

자원 번들 추가

```
amadmin -u|--runasdn <user-dn> -w|--password <user-password>
    -b|--addresourcebundle <name-of-resource-bundle>
    -i|--resourcebundlefilename <resource-bundle-file-name>
    [-R|--resourcelocale] <locale>
```

자원 문자열 가져오기

```
amadmin -u|--runasdn <user-dn> -w|--password <user-password>  
        -z|--getresourcestrings <name-of-resource-bundle>  
        [-R|--resourcelocale] <locale>
```

자원 번들 제거

```
amadmin -u|--runasdn <user-dn> -w|--password <user-password>  
        -j|--deleteresourcebundle <name-of-resource-bundle>  
        [-R|--resourcelocale] <locale>
```


amserver 명령줄 도구

이 장에서는 amserver 명령줄 도구에 대해 설명하며 이번 장은 다음 절로 구성됩니다.

- [223 페이지의 "amserver 명령줄 실행 파일"](#)

amserver 명령줄 실행 파일

명령줄 실행 파일 amserver 는 , Unix 와 SecurID 인증 모듈과 연관된 amunixd 와 amsercuridd 도우미를 각각 시작 및 중지합니다.

amserver 구문

이 도구에 대한 일반 구문은 다음과 같습니다.

```
./amserver { start | stop }
```

start

start 는 도우미를 시작하는 명령입니다.

stop

stop 은 도우미를 중지하는 명령입니다.

amserver 명령줄 실행 파일

am2bak 명령줄 도구

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

- 225 페이지의 "am2bak 명령줄 실행 파일"

am2bak 명령줄 실행 파일

Access Manager 에는 AccessManager-base/SUNWam/bin 아래에 am2bak 유틸리티가 포함되어 있습니다. 이 유틸리티는 Access Manager 의 모든 구성 요소 또는 선택 구성 요소에 대한 백업을 수행합니다. 로그 백업을 가져오는 동안 Directory Server 가 실행되고 있어야 합니다.

am2bak S 구문

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

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

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

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

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

주 구문에 표시된 것처럼 두 개의 하이픈을 정확하게 입력해야 합니다.

am2bak 옵션

--verbose (-v)

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

--backup backup-name (-k)

--backup *backup-name* 은 백업 파일의 이름을 지정합니다. 기본값은 ambak 입니다.

--location (-l)

--location 은 백업의 디렉토리 위치를 지정합니다. 기본 위치는 AccessManager-base/backup 입니다.

--config (-c)

--config 는 구성 파일에 대해서만 백업을 지정합니다.

--debug (-b)

--debug 는 디버그 파일에 대해서만 백업을 지정합니다.

--log (-g)

--log 는 로그 파일에 대해서만 백업을 지정합니다.

--cert (-t)

--cert 는 인증서 데이터베이스 파일에 대해서만 백업을 지정합니다.

--ds (-d)

--ds 는 Directory Server 에 대해서만 백업을 지정합니다.

--all (-a)

--all 은 전체 Access Manager 에 대한 전체 백업을 지정합니다.

--help (-h)

--help 는 am2bak 명령에 대한 구문을 표시하는 인수입니다.

--version (-n)

--version은 유틸리티 이름, 제품 이름, 제품 버전 및 사용권에 대한 고지 사항을 표시하는 인수입니다.

백업 절차**1. 루트로 로그인합니다.**

이 스크립트를 실행하는 사용자는 루트로 액세스해야 합니다.

2. 필요한 경우 스크립트를 실행하여 올바른 경로가 사용되는지 확인합니다.

이 스크립트가 백업하는 Solaris™ 운영 환경 파일은 다음과 같습니다.

○ 구성 및 사용자 정의 파일 :

- *AcessManager-base/SUNWam/config/*
- *AcessManager-base/SUNWam/locale/*
- *AcessManager-base/SUNWam/servers/httpacl*
- *AcessManager-base/SUNWam/lib/*.properties* (Java 등록 정보 파일)
- *AcessManager-base/SUNWam/bin/amserver.instance-name*
- *AcessManager-base/SUNWam/servers/https-all_instances*
- *AcessManager-base/SUNWam/servers/web-apps-all_instances*
- *AcessManager-base/SUNWam/web-apps/services/WEB-INF/config*
- *AcessManager-base/SUNWam/web-apps/services/config*
- *AcessManager-base/SUNWam/web-apps/applications/WEB-INF/classes*
- *AcessManager-base/SUNWam/web-apps/applications/console*
- */etc/rc3.d/K55amserver.all_instances*
- */etc/rc3.d/S55amserver.all_instances*
- *DirectoryServer_base/slapd-host/config/schema/*
- *DirectoryServer_base/slapd-host/config/slapd-collations.conf*
- *DirectoryServer_base/slapd-host/config/dse.ldif*

○ 로그 및 디버그 파일 :

- *var/opt/SUNWam/logs* (Access Manager 로그 파일)
- *var/opt/SUNWam/install* (Access Manager 설치 로그 파일)

- `var/opt/SUNWam/debug` (Access Manager 디버그 파일)
- 인증서 :
 - `AcessManager-base/SUNWam/servers/alias`
 - `DirectoryServer_base/alias`

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

- 구성 및 사용자 정의 파일 :
 - `AcessManager-base/web-apps/services/WEB-INF/config/*`
 - `AcessManager-base/locale/*`
 - `AcessManager-base/web-apps/applications/WEB-INF/classes/*.properties` (java 등록 정보 파일)
 - `AcessManager-base/servers/https-host/config/jvm12.conf`
 - `AcessManager-base/servers/https-host/config/magnus.conf`
 - `AcessManager-base/servers/https-host/config/obj.conf`
 - `DirectoryServer_base/slapd-host/config/schema/*.ldif`
 - `DirectoryServer_base/slapd-host/config/slapd-collations.conf`
 - `DirectoryServer_base/slapd-host/config/dse.ldif`
- 로그 및 디버그 파일 :
 - `var/opt/logs` (Access Manager 로그 파일)
 - `var/opt/debug` (Access Manager 디버그 파일)
- 인증서 :
 - `AcessManager-base/servers/alias`
 - `AcessManager-base/alias`

bak2am 명령줄 도구

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

- 229 페이지의 "bak2am 명령줄 실행 파일"

bak2am 명령줄 실행 파일

Access Manager 에는 AccessManager-base/SUNWam/bin 아래에 bak2am 유틸리티가 포함되어 있습니다. 이 유틸리티는 am2back 유틸리티에 의해 백업된 Access Manager 구성 요소의 복원을 수행합니다.

bak2am 구문

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

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

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

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

주 구문에 표시된 것처럼 두 개의 하이픈을 정확하게 입력해야 합니다.

bak2am 옵션

--gzip backup-name

--gzip 은 백업 파일의 전체 경로와 파일 이름을 tar.gz 형식으로 지정합니다. 기본적으로 경로는 AccessManager-base/backup입니다. 이 옵션은 Solaris 전용입니다.

--tar backup-name

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

--verbose

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

--directory

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

--help

--help 는 bak2am 명령에 대한 구문을 표시하는 인수입니다.

--version

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

1. 루트로 로그인합니다.

이 스크립트를 실행하는 사용자는 루트로 액세스해야 합니다.

2. 입력 tar 파일의 압축을 해제합니다.

이 파일은 백업 스크립트를 실행할 때 생성되었습니다.

ampassword 명령줄 도구

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

- 231 페이지의 "ampassword 명령줄 실행 파일"
- 232 페이지의 "SSL 에서 ampassword 실행"

ampassword 명령줄 실행 파일

Access Manager 에는 /etc/opt/SUNWam/bin 에 ampassword 유틸리티가 포함되어 있습니다. 이 유틸리티를 사용하여 관리자 또는 사용자에게 대한 Access Manager 비밀번호를 변경할 수 있습니다.

ampassword 구문

ampassword 도구 사용을 위한 일반 구문은 다음과 같습니다.

```
ampassword -a | --admin [ -o | --old oldPassword -n | --new newPassword ]
```

```
ampassword -p | --proxy [ -o | --old oldPassword -n | --new newPassword ]
```

```
ampassword -e | --encrypt [ password ]
```

주 구문에 표시된 것처럼 두 개의 하이픈을 정확하게 입력해야 합니다.

ampasword 옵션

--admin (-a)

--admin 은 관리 비밀번호를 변경하는 데 사용됩니다.

--proxy (-p)

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

--version

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

--encrypt (-e)

--encrypt 는 비밀번호를 암호화하는 데 사용됩니다. 명령줄에 인쇄됩니다. 예를 들어 새 dsamuser 비밀번호를 암호화하려면 다음 명령을 사용합니다.

```
ampasword -e newPassword
```

그리고 나서 새 dsamuser 비밀번호를 serverconfig.xml 에 넣은 후 웹 컨테이너 (Web Server 또는 Application Server) 를 다시 시작합니다.

SSL 에서 ampasword 실행

SSL (Secure-Socket Layer) 모드로 실행 중인 Access Manager 에서 ampasword 를 실행하려면 다음을 수행합니다.

1. 다음 디렉토리에 있는 serverconfig.xml 파일을 수정합니다.

```
AccessManager-base/SUNWam/config/
```

2. port 서버 속성을 Access Manager 가 실행 중인 SSL 포트 로 변경합니다.
3. type 속성을 SSL 로 변경합니다.

예를 들면 다음과 같습니다.

```
<iPlanetDataAccessLayer>  
  
<ServerGroup name="default" minConnPool="1" maxConnPool="10">
```

```
<Server name="Server1" host="sun.com" port="636" type="SSL" />

<User name="User1" type="proxy">

    <DirDN>

        cn=puser,ou=DSAME Users,dc=iplanet,dc=com

    </DirDN>

    <DirPassword>

        AQIC5wM2LY4Sfcy+AQBQxghVwhBE92i78cqf

    </DirPassword>

</User> ...
```

ampassword 는 Directory Server 에서만 비밀번호를 변경합니다 . Access Manager 의 ServerConfig.xml 및 모든 인증 템플릿에서는 비밀번호를 수동으로 변경해야 합니다 .

SSL 에서 ampasword 실행

VerifyArchive 명령줄 도구

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

- [235 페이지의 "VerifyArchive 명령줄 실행 파일"](#)

VerifyArchive 명령줄 실행 파일

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

VerifyArchive 는 지정된 logName 에 대해 모든 아카이브 집합과 각 아카이브 집합에 속하는 모든 파일을 추출합니다. VerifyArchive 를 실행하면 각 로그 레코드에서 손상을 검색하여 손상이 있을 경우 손상된 파일 및 레코드 수를 지정하는 메시지를 인쇄합니다.

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

주 관리자 권한이 없는 사용자로 amverifyarchive 를 실행하면 오류가 발생할 수 있습니다.

VerifyArchive 구문

모든 매개 변수 옵션은 필수입니다. 구문은 다음과 같습니다.

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

VerifyArchive 옵션

logName

logName 은 확인할 로그 이름 (예 : amConsole, amAuthentication 등) 입니다. VerifyArchive 는 지정된 *logName* 에 대한 액세스 로그와 오류 로그를 모두 확인합니다. 예를 들어 , amConsole 이 지정된 경우 검증기는 amConsole.access 및 amConsole.error 파일을 확인합니다. 또는 *logName* 을 amConsole.access 또는 amConsole.error 로 지정하여 이러한 로그만 확인하도록 제한할 수 있습니다.

path

path 는 로그 파일이 저장되는 전체 디렉토리 경로입니다.

uname

uname 은 Access Manager 관리자의 사용자 아이디입니다.

password

password 는 Access Manager 관리자의 비밀번호입니다.

amsecuridd 도우미

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

- 237 페이지의 "amsecuridd 도우미 명령줄 실행 파일 "
- 238 페이지의 "amsecuridd 도우미 실행 "

amsecuridd 도우미 명령줄 실행 파일

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

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

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

amsecuridd 도우미는 포트 번호 58943(기본값)에서 구성 정보를 수신합니다. 이 포트가 이미 사용되고 있는 경우 `AMConfig.properties` 파일 (기본적으로 `AccessManager-base/SUNWam/config/`에 있음)의 `securidHelper.ports` 속성에서 포트 번호를 변경할 수 있습니다. `securidHelper.ports` 속성에는 각 amsecuridd 도우미 인스턴스에 대한 공백으로 구분된 포트 목록이 포함되어 있습니다. `AMConfig.properties`에 대한 변경 내용을 저장하고 Identity Sever 를 다시 시작합니다.

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

amsecuridd 구문

구문은 다음과 같습니다.

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

amsecuridd 옵션

verbose (-v)

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

configure portnumber (-c portnm)

수신 포트 번호를 구성합니다. 기본값은 58943 입니다.

amsecuridd 도우미 실행

amsecuridd는 기본적으로 `AccessManager-base/SUNWam/share/bin`에 있습니다. 기본 포트에서 도우미를 실행하려면 다음 명령 (옵션 없이) 을 입력합니다.

```
./amsecuridd
```

기본 포트가 아닌 포트에서 도우미를 실행하려면 다음 명령을 입력합니다.

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

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

필수 라이브러리

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

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

주 libaceclnt.so 를 찾으려면 LD_LIBRARY_PATH 를
AccessManager-base/Sunwam/lib/ 로 설정합니다.

amsecuridd 도우미 명령줄 실행 파일

속성 참조 설명서

Sun Java System Access Manager 관리 설명서의 4 부 속성 참조 설명서입니다. 여기에서는 Access Manager의 기본 서비스 내에 구성된 속성에 대해 설명하며 다음 내용으로 구성되어 있습니다.

- 243 페이지의 " 관리 서비스 속성 "
- 267 페이지의 " 익명 인증 속성 "
- 271 페이지의 " 인증서 인증 속성 "
- 277 페이지의 " 핵심 인증 속성 "
- 289 페이지의 "HTTP 기본 인증 속성 "
- 297 페이지의 "LDAP 인증 속성 "
- 303 페이지의 " 구성원 인증 속성 "
- 313 페이지의 "Windows NT 인증 속성 "
- 317 페이지의 "RADIUS 인증 속성 "
- 321 페이지의 "SafeWord 인증 속성 "
- 327 페이지의 "SecurID 인증 속성 "
- 329 페이지의 "Unix 인증 속성 "
- 337 페이지의 " 인증 구성 서비스 속성 "
- 341 페이지의 " 클라이언트 검색 서비스 속성 "
- 345 페이지의 " 국제화 설정 서비스 속성 "
- 347 페이지의 " 로깅 서비스 속성 "
- 353 페이지의 " 이름 지정 서비스 속성 "

- 207 페이지의 "비밀번호 재설정 서비스 "
- 363 페이지의 "플랫폼 서비스 속성 "
- 367 페이지의 "정책 구성 서비스 속성 "
- 377 페이지의 "SAML 서비스 속성 "
- 385 페이지의 "세션 서비스 속성 "
- 391 페이지의 "사용자 속성 "

관리 서비스 속성

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

- [243 페이지의 "전역 속성"](#)
- [252 페이지의 "조직 속성"](#)

전역 속성

관리 서비스의 전역 속성은 다음과 같습니다.

- [244 페이지의 "연합 관리 사용"](#)
- [244 페이지의 "사용자 관리 사용"](#)
- [244 페이지의 "사용자 컨테이너 표시"](#)
- [245 페이지의 "보기 메뉴에 컨테이너 표시"](#)
- [245 페이지의 "그룹 컨테이너 표시"](#)
- 관리 대상 그룹 유형
- 기본 역할 권한
- 도메인 구성 요소 트리 사용 가능
- [248 페이지의 "관리 그룹 사용 가능"](#)

- 248 페이지의 " 호환 사용자 삭제 사용 가능 "
- 248 페이지의 " 동적 관리 역할 ACI "
- 250 페이지의 " 사용자 프로필 서비스 클래스 "
- 251 페이지의 " DC 노드 속성 목록 "
- 251 페이지의 " 삭제된 객체에 대한 필터 검색 "
- 251 페이지의 " 기본 사용자 컨테이너 "
- 252 페이지의 " 기본 그룹 컨테이너 "
- 252 페이지의 " 기본 에이전트 컨테이너 "

연합 관리 사용

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

사용자 관리 사용

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

사용자 컨테이너 표시

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

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

보기 메뉴에 컨테이너 표시

이 속성은 Access Manager 콘솔의 보기 메뉴에 있는 컨테이너를 표시할지 여부를 지정합니다. 기본값은 `false` 입니다. 관리자는 선택적으로 다음 중 하나를 선택할 수 있습니다.

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

그룹 컨테이너 표시

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

관리 대상 그룹 유형

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

- 정적 그룹은 `groupOfNames` 또는 `groupOfUniqueNames` 객체 클래스를 사용하여 각 그룹 구성원을 명시적으로 나열합니다. 그룹 항목은 그룹의 각 구성원에 대해 `uniqueMember` 속성을 포함합니다. 정적 그룹의 구성원은 수동으로 추가되므로 사용자 항목 자체가 바뀌지 않습니다. 정적 그룹은 구성원이 거의 없는 그룹에 적합합니다.
- 동적 그룹은 각 그룹 구성원의 항목에서 `memberOf` 속성을 사용합니다. 동적 그룹의 구성원은 `memberOf` 속성을 포함하는 모든 항목을 검색 및 반환하는 LDAP 필터를 사용하여 생성됩니다. 동적 그룹은 구성원 수가 많은 그룹에 적합합니다.
- 필터링된 그룹은 LDAP 필터를 사용하여 필터의 요구 사항을 충족하는 구성원을 검색 및 반환합니다. 예를 들어, 필터는 특정 `uid(uid=g*)` 나 전자 메일 주소 (`email=*@sun.com`) 를 가진 구성원을 생성할 수 있습니다. 이러한 예에서 LDAP 필터는 각각 `uid` 가 `g` 로 시작하거나 전자 메일 주소가 `sun.com` 으로 끝나는 모든 사용자를 반환합니다. 필터링된 그룹은 필터링에 의한 구성원을 선택하여 사용자 관리 보기 내에서만 만들 수 있습니다.

관리자는 다음 중 하나를 선택할 수 있습니다.

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

기본 역할 권한

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

사용 권한 없음

역할에 사용 권한이 설정되지 않습니다.

조직 관리

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

조직 지원 안내 관리

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

조직 정책 관리자

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

-
- 주** 역할은 `aci_name | aci_desc | dn:aci ## dn:aci ## dn:aci` 형식을 사용하여 정의합니다. 이를 살펴보면 다음과 같습니다.
- `aci_name` 은 **ACI** 의 이름입니다.
 - `aci_desc` 는 이러한 **ACI** 가 허용하는 액세스에 대한 설명입니다. 최대한의 유용성을 위해 이 설명을 읽는 사람이 **ACI** 나 다른 디렉토리 개념을 알지 못한다고 가정합니다.
- `aci_name` 및 `aci_desc` 는 `amAdminUserMsgs.properties` 파일에 포함된 `i18n` 키입니다. 콘솔에 표시되는 값은 `.properties` 파일로부터 가져오며 키는 이러한 값을 검색하는 데 사용됩니다.
- `dn:aci` 는 `##` 으로 분리된 **DN** 과 **ACI** 의 쌍을 나타냅니다. **Access Manager** 는 관련 **DN** 항목에서 각 **ACI** 를 설정합니다. 이 형식은 또한 값으로 대체할 수 있는 태그를 지원하며 이러한 태그는 값으로 대체할 수 없는 경우 **ACI** 에서 문자 그대로 지정해야 합니다 (**ROLENAME**, **ORGANIZATION**, **GROUPNAME** 및 **PCNAME**). 이러한 태그를 사용하여 기본으로 사용하기에 충분히 유연한 역할을 정의할 수 있습니다. 기본 역할 중 하나를 바탕으로 역할이 만들어지면 **ACI** 의 태그가 새 역할의 **DN** 에서 취해진 값을 확인합니다.
-

도메인 구성 요소 트리 사용 가능

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

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

조직 트리에서 **Access Manager SDK** 를 통해 `inetdomainstatus` 속성의 상태를 변경하면 해당하는 DC 트리 항목의 상태가 업데이트됩니다. **Access Manager SDK** 를 통해 이루어지지 않은 상태 업데이트는 동기화되지 않습니다. 예를 들어, DNS 이름 속성 `sun.com` 을 사용하여 새 조직 `sun` 을 만들 경우 DC 트리에 다음 항목이 만들어집니다.

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

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

관리 그룹 사용 가능

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

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

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

호환 사용자 삭제 사용 가능

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

동적 관리 역할 ACI

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

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

컨테이너 지원 안내 관리

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

조직 지원 안내 관리

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

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

컨테이너 관리

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

조직 정책 관리자

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

사용자 컨테이너 관리

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

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

그룹 관리

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

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

최상위 수준 관리자

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

조직 관리

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

사용자 프로필 서비스 클래스

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

서비스 이름 | 상대 url

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

DC 노드 속성 목록

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

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

삭제된 객체에 대한 필터 검색

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

기본 사용자 컨테이너

이 속성은 사용자가 만들어지는 기본 사용자 컨테이너를 지정합니다.

기본 그룹 컨테이너

이 속성은 그룹이 만들어지는 기본 그룹 컨테이너를 지정합니다.

기본 에이전트 컨테이너

이 속성은 에이전트가 만들어지는 기본 에이전트 컨테이너를 지정합니다.

조직 속성

관리 서비스의 조직 속성은 다음과 같습니다.

- 253 페이지의 " 그룹 기본 사용자 컨테이너 "
- 253 페이지의 " 그룹 사용자 컨테이너 목록 "
- 253 페이지의 " 사용자 프로필 디스플레이 클래스 "
- 254 페이지의 " 사용자 프로필 페이지에 역할 표시 "
- 254 페이지의 " 사용자 프로필 페이지에 그룹 표시 "
- 254 페이지의 " 사용자 그룹 자동 가입 사용 가능 "
- 254 페이지의 " 사용자 프로필 디스플레이 옵션 "
- 255 페이지의 " 사용자 작성 기본 역할 "
- 255 페이지의 " 관리 콘솔 탭 "
- 255 페이지의 " 검색에서 반환되는 최대 결과 수 "
- 255 페이지의 " 검색 시간 초과 "
- 256 페이지의 " JSP 디렉토리 이름 "
- 256 페이지의 " 온라인 도움말 문서 "
- 256 페이지의 " 필수 서비스 "
- 256 페이지의 " 사용자 검색 키 "
- 257 페이지의 " 사용자 검색 반환 속성 "
- 257 페이지의 " 사용자 작성 알림 목록 "
- 258 페이지의 " 사용자 삭제 알림 목록 "

- 258 페이지의 " 사용자 수정 알림 목록 "
- 259 페이지의 " 페이지당 표시되는 최대 항목 "
- 259 페이지의 "Event Listener 클래스 "
- 259 페이지의 " 사전 처리 및 사후 처리 클래스 "
- 260 페이지의 " 외부 속성 불러오기 사용 가능 "
- 260 페이지의 " 잘못된 사용자 아이디 문자 "
- 260 페이지의 " 사용자 아이디 및 비밀번호 검증 플러그 인 클래스 "

그룹 기본 사용자 컨테이너

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

그룹 사용자 컨테이너 목록

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

그룹의 dn | 사용자 컨테이너의 dn

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

사용자 프로필 디스플레이 클래스

이 속성은 사용자 프로필 페이지를 표시할 때 Access Manager 콘솔에서 사용하는 Java 클래스를 지정합니다.

최종 사용자 프로필 디스플레이 클래스

이 속성은 Access Manager 콘솔에서 최종 사용자 프로필 페이지를 표시할 때 사용하는 Java 클래스를 지정합니다.

사용자 프로필 페이지에 역할 표시

이 옵션은 사용자 프로필 페이지의 일부로 사용자에게 할당된 역할 목록을 표시할지 여부를 지정합니다. 값이 `false`(선택되지 않음)인 경우 사용자 프로필 페이지는 관리자에 대해서만 사용자 역할을 표시합니다. 기본값은 `false`입니다.

사용자 프로필 페이지에 그룹 표시

이 옵션은 사용자 프로필 페이지의 일부로 사용자에게 할당된 그룹 목록을 표시할지 여부를 지정합니다. 값이 `false`(선택되지 않음)인 경우 사용자 프로필 페이지는 관리자에 대해서만 사용자 그룹을 표시합니다. 기본값은 `false`입니다.

사용자 그룹 자동 가입 사용 가능

이 옵션은 사용자가 가입이 허용된 그룹에 자신을 추가할 수 있는지 여부를 지정합니다. 값이 `false`인 경우 사용자 프로필 페이지는 관리자만 사용자의 그룹 구성원을 수정할 수 있게 허용합니다. 기본값은 `false`입니다.

주 이 옵션은 사용자 프로필 페이지에 그룹 표시 옵션이 선택된 경우에만 적용됩니다.

사용자 프로필 디스플레이 옵션

이 메뉴는 사용자 프로필 페이지에 표시되는 서비스 속성을 지정합니다. 관리자는 다음을 선택할 수 있습니다.

- `UserOnly` - 사용자에게 할당된 서비스에 대한 보기 가능한 사용자 스키마 속성을 표시합니다.

속성에 `Display` 키워드가 포함된 경우 사용자 서비스 속성 값을 사용자가 볼 수 있습니다. 자세한 내용은 *Access Manager Developer's Guide* 를 참조하십시오.

- Combined - 사용자에게 할당된 서비스에 대한 보기 가능한 사용자 및 동적 스키마 속성을 표시합니다.

사용자 작성 기본 역할

이 목록은 새로 만든 사용자에게 자동으로 할당되는 역할을 정의합니다. 기본값은 없습니다. 관리자는 하나 이상의 역할 DN 을 입력할 수 있습니다.

주 이 필드에는 역할 이름이 아니라 완전한 고유 이름 (DN) 주소만 입력해야 합니다. 역할은 LDAP(Directory Server) 역할이 아닌 Access Manager 역할만 사용할 수 있습니다.

관리 콘솔 탭

이 필드는 콘솔의 맨 위에 표시되는 모듈의 Java 클래스를 나열합니다. 구문은 `i18N key | java class name` 입니다. `i18N` 키는 보기 메뉴의 현지화된 항목 이름에 사용됩니다.

검색에서 반환되는 최대 결과 수

이 필드는 검색에서 반환되는 최대 결과 수를 정의합니다. 기본값은 100 입니다.

주의 이 값을 큰 값으로 설정할 경우 주의하십시오. 크기 제한은 다음 위치에 있는 *Sun Java System Directory Server 설치 및 조정 설명서*를 참조하십시오.

<http://docs.sun.com/db/doc/816-6850-10>

LDAPModify 를 통해 이 속성에 수행된 수정 사항은 Access Manager 콘솔을 통해 수행된 수정 사항보다 우선하여 적용됩니다. LDAPModify 를 사용한 속성 변경에 대한 자세한 내용은 *Access Manager Developer's Guide* 를 참조하십시오.

검색 시간 초과

이 필드는 시간이 초과되기 전에 검색이 수행되는 시간 (초) 을 정의합니다. 이 필드는 너무 오래 수행되는 검색을 정지하는 데 사용되며 최대 검색 시간에 도달하면 오류가 반환됩니다. 기본값은 5 초입니다.

JSP 디렉토리 이름

이 필드는 콘솔을 구성하여 다른 모양으로 변경 (사용자 정의) 하는 데 사용되는 .jsp 파일을 포함하는 디렉토리의 이름을 지정합니다. 이 필드에 지정된 디렉토리에 .jsp 파일을 복사해야 합니다.

온라인 도움말 문서

이 필드는 주 Access Manager 도움말 페이지에서 만들어지는 온라인 도움말 링크를 나열합니다. 이를 통해 다른 응용 프로그램에서 자체 온라인 도움말 링크를 Access Manager 페이지에 추가할 수 있습니다. 이 속성의 형식은 다음과 같습니다.

linki18nkey | 눌렀을 때 로드할html 페이지 | i18n 등록정보 파일 | 원격 서버

주 *원격 서버*는 온라인 도움말 문서가 위치하는 원격 서버를 지정할 수 있는 선택적 인수입니다.

예를 들면 다음과 같습니다.

`IdentityServer Help | /AMAdminHelp.html | amAdminModuleMsgs`

필수 서비스

이 필드는 사용자 항목이 만들어질 때 사용자 항목에 동적으로 추가되는 서비스를 나열합니다. 관리자는 작성 시에 어떤 서비스를 추가할 것인지 선택할 수 있습니다.

이 속성은 콘솔이 아니라 Access Manager SDK 에서 사용합니다. 동적으로 만들어진 사용자 및 amadmin 명령줄 유틸리티에 의해 만들어진 사용자에게 이 속성에 나열된 서비스가 할당됩니다.

사용자 검색 키

이 속성은 이동 페이지에서 단순 검색을 수행할 때 검색되는 속성 이름을 정의합니다. 이 속성의 기본값은 cn 입니다. 예를 들어, 이 속성에서 기본값을 사용할 경우에는 다음과 같습니다.

이동 프레임의 이름 필드에 j* 를 입력할 경우 이름이 "j" 또는 "J" 로 시작되는 사용자가 표시됩니다.

사용자 검색 반환 속성

이 필드는 단순 검색에서 반환된 사용자를 표시하는 데 사용되는 속성 이름을 정의합니다. 이 속성의 기본값은 uid.cn 입니다. 이 속성은 사용자 아이디와 사용자의 성명을 표시합니다.

처음 나열되는 속성 이름은 반환되는 사용자 집합을 정렬하기 위한 키로도 사용됩니다. 성능 감소를 방지하려면 사용자 항목에 값이 설정되는 속성을 사용합니다.

사용자 작성 알림 목록

이 필드는 새 사용자를 만들 때 알림이 보내지는 전자 메일 주소의 목록을 정의합니다. 다음 구문과 같이 여러 전자 메일 주소를 지정할 수 있습니다.

```
e-mail|locale|charset
```

```
e-mail|locale|charset
```

```
e-mail|locale|charset
```

또한 알림 목록에서 |locale 옵션을 사용하여 다른 로케일을 적용합니다. 예를 들어, 프랑스에 있는 관리자에게 알림을 보내려는 경우는 다음과 같습니다.

```
someuser@example.com|fr|fr
```

로케일 목록은 [283 페이지의 표 20-1](#) 을 참조하십시오.

주

보낸 사람의 전자 메일 아이디는 기본적으로 AccessManager-base/SUNWam/locale. 에 있는 amProfile.properties 의 등록 정보 497 을 수정하여 변경할 수 있습니다.

사용자 삭제 알림 목록

이 필드는 사용자를 삭제할 때 알림이 보내지는 전자 메일 주소의 목록을 정의합니다. 다음 구문과 같이 여러 전자 메일 주소를 지정할 수 있습니다.

```
e-mail|locale|charset
```

```
e-mail|locale|charset
```

```
e-mail|locale|charset
```

또한 알림 목록에서 |locale 옵션을 사용하여 다른 로케일을 적용합니다. 예를 들어, 프랑스에 있는 관리자에게 알림을 보내려는 경우는 다음과 같습니다.

```
someuser@example.com|fr|fr
```

로케일 목록은 [283 페이지의 표 20-1](#) 을 참조하십시오.

주	보낸 사람의 전자 메일 아이디는 기본적으로 AccessManager-base/SUNWam/locale.에 있는 amProfile.properties의 등록 정보 497을 수정하여 변경할 수 있습니다. 보낸 사람 아이디의 기본값은 DSAME입니다.
----------	---

사용자 수정 알림 목록

이 필드는 속성 목록 및 속성과 연관된 전자 메일 주소의 목록을 정의합니다. 목록에 정의된 속성에서 사용자 수정이 발생하면 해당 속성과 연관된 전자 메일 주소로 알림이 보내집니다. 각 속성에는 여러 주소 집합이 연관되어 있을 수 있습니다. 다음 구문과 같이 여러 전자 메일 주소를 지정할 수 있습니다.

```
attrName e-mail|locale|charset e-mail|locale|charset .....
```

```
attrName e-mail|locale|charset e-mail|locale|charset .....
```

주소 중 하나 대신에 self 키워드를 사용할 수 있습니다. 이 키워드는 프로필이 수정된 사용자에게 전자 메일을 보냅니다.

예를 들면 다음과 같습니다.

```
manager someuser@sun.com|self|admin@sun.com
```

전자 메일은 manager 속성에 지정된 주소인 someuser@sun.com, admin@sun 및 사용자를 수정한 사람 (self)에게 보내집니다.

또한 알림 목록에서 |locale 옵션을 사용하여 다른 로케일을 적용합니다. 예를 들어, 프랑스에 있는 관리자에게 알림을 보내려는 경우는 다음과 같습니다.

```
manager someuser@sun.com|self|admin@sun.com|fr
```

로케일 목록은 [283 페이지의 표 20-1](#) 을 참조하십시오 .

주 속성 이름은 콘솔의 디스플레이 이름이 아니라 Directory Server 스키마에 나타나는 이름과 동일합니다.

페이지당 표시되는 최대 항목

이 속성을 사용하면 페이지당 표시할 수 있는 최대 행을 정의할 수 있습니다. 기본값은 25 입니다. 예를 들어, 검색 결과 100 개의 행이 반환될 경우 4 개의 페이지에 각각 25 개의 행이 표시됩니다.

Event Listener 클래스

이 속성은 Access Manager 콘솔에서 작성, 수정 및 삭제 이벤트를 받는 수신기 목록을 포함합니다.

사전 처리 및 사후 처리 클래스

이 필드는 사용자, 조직, 역할 및 그룹에 대한 사전 처리 및 사후 처리 작업 중에 콜백을 받도록 com.ipplanet.am.sdk.AMCallback 클래스를 확장하는 플러그인을 통한 구현 클래스 목록을 정의합니다. 작업은 다음과 같습니다.

- 만들기
- 삭제
- 수정
- 역할 / 그룹에 사용자 추가
- 역할 / 그룹에서 사용자 삭제

플러그인 인의 전체 클래스 이름을 입력해야 합니다. 예를 들면 다음과 같습니다.

```
com.ipplanet.am.sdk.AMCallbacSample
```

그런 다음 플러그인 클래스 위치에 대한 전체 경로를 포함하도록 (Access Manager 설치 기본에서) 웹 컨테이너의 클래스 경로를 변경해야 합니다.

외부 속성 불러오기 사용 가능

이 옵션을 사용하면 플러그인에 대한 콜백에서 외부 속성 (모든 외부 응용 프로그램 특정 속성) 을 검색할 수 있습니다. 외부 속성은 Access Manager SDK 에 캐시되지 않기 때문에 이 속성을 사용하면 조직 수준별 속성 검색이 가능합니다. 기본적으로 이 옵션은 사용 불가능합니다.

잘못된 사용자 아이디 문자

이 속성은 사용자 이름에 사용할 수 없는 문자 목록을 정의합니다.

각 문자는 | 문자로 구분되어야 합니다. 예를 들면 다음과 같습니다.

*|(|)|&|!

사용자 아이디 및 비밀번호 검증 플러그인 클래스

이 클래스는 사용자 아이디 및 비밀번호 검증 플러그인 기법을 제공합니다.

사용자의 사용자 아이디 및 / 또는 비밀번호를 검증하는 구현 플러그인 모듈이 이 클래스의 메소드를 대체해야 합니다. 구현 플러그인 모듈은 Access Manager 콘솔, amadmin 명령줄 인터페이스 또는 SDK 를 사용하여 사용자 아이디 또는 비밀번호 값을 추가하거나 수정할 때마다 호출됩니다.

이 클래스를 확장하는 플러그인은 조직별로 구성할 수 있습니다. 조직에 대해 플러그인이 구성되지 않은 경우 전역 수준에서 구성된 플러그인이 사용됩니다.

플러그인 검증이 실패할 경우 사용자가 제공한 사용자 아이디 또는 비밀번호에 오류가 있다는 것을 응용 프로그램에 알리기 위해 플러그인 모듈에서 예외가 발생할 수 있습니다.

활성 디렉토리 인증 속성

활성 디렉토리 인증 속성은 조직 속성입니다. 서비스 구성에서 이러한 속성에 적용되는 값이 활성 디렉토리 인증 템플릿의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플릿을 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 항목은 조직 속성을 상속하지 않습니다. 활성 디렉토리 인증 속성은 다음과 같습니다.

- 262 페이지의 " 주 활성 Directory Server"
- 262 페이지의 " 보조 활성 Directory Server"
- 263 페이지의 " 사용자 검색을 시작할 DN"
- 263 페이지의 " 루트 사용자 바인드용 DN"
- 263 페이지의 " 루트 사용자 바인드용 비밀번호 "
- 264 페이지의 " 루트 사용자 바인드용 비밀번호 (확인)"
- 264 페이지의 " 사용자 프로필 검색 시 사용되는 활성 디렉토리 속성 "
- 264 페이지의 " 인증될 사용자 검색 시 사용되는 활성 디렉토리 속성 "
- 264 페이지의 " 사용자 검색 필터 "
- 265 페이지의 " 검색 범위 "
- 265 페이지의 "SSL 이 활성 Directory Server 에 액세스 가능 "
- 265 페이지의 " 인증할 사용자 DN 반환 "
- 266 페이지의 " 활성 Directory Server 확인 간격 "
- 266 페이지의 " 사용자 작성 속성 목록 "
- 266 페이지의 " 인증 수준 "

주 활성 Directory Server

이 필드는 Access Manager 설치 도중 지정된 주 활성 Directory Server 의 호스트 이름과 포트 번호를 지정합니다. 이 서버는 활성 디렉토리 인증을 위해 연결되는 첫 번째 서버입니다. 형식은 hostname:port 입니다. 포트 번호가 없을 경우 포트 번호를 389 라고 가정합니다.

Access Manager 를 여러 도메인으로 배포한 경우 Access Manager 의 특정 인스턴스와 Directory Server 의 특정 인스턴스 간의 통신 링크를 다음 형식으로 지정할 수 있습니다 (여러 항목에서 로컬 서버 이름을 접두어로 사용해야 함).

```
local_servername|server:port local_servername2|server2:port2 ...
```

예를 들어, Directory Server 의 서로 다른 인스턴스 (L1-machine1-DS 및 L2-machine2-DS) 와 통신하는 두 Access Manager 를 서로 다른 위치 (L1-machine1-IS 및 L2-machine2-IS) 에 배포한 경우 형식은 다음과 같습니다.

```
L1-machine1-IS.example.com|L1-machine1-DS.example.com:389  
L2-machine2-IS.example.com|L2-machine2-DS.example.com:389
```

보조 활성 Directory Server

이 필드는 Access Manager 플랫폼에 사용할 수 있는 보조 활성 Directory Server 의 호스트 이름과 포트 번호를 지정합니다. 주 활성 Directory Server 가 인증 요청에 응답하지 않을 경우 이 서버에 연결됩니다. 주 서버가 실행 중인 경우 Access Manager 는 주 서버로 다시 전환합니다. 형식은 hostname:port 입니다. 여러 항목이 있을 경우 로컬 서버 이름을 접두어로 지정해야 합니다.

주의	Access Manager 엔터프라이즈와 떨어져 있는 원격 Directory Server 에서 사용자를 인증하는 경우 주 활성 Directory Server 포트와 보조 활성 Directory Server 포트 모두에 값이 있어야 합니다. 하나의 Directory Server 위치에 대한 값을 두 필드 모두에 사용할 수 있습니다.
-----------	---

사용자 검색을 시작할 DN

이 필드는 사용자 검색이 시작되는 노드의 DN 을 지정합니다. 성능상의 이유 때문에 이 DN 은 가능한 구체적이어야 합니다. 기본값은 디렉토리 트리의 루트입니다. 유효한 모든 DN 이 인식됩니다. **검색 범위** 속성에서 OBJECT 를 선택한 경우에는 DN 에서 프로필이 있는 수준보다 한 수준 위를 지정해야 합니다.

여러 항목이 있을 경우 로컬 서버 이름을 접두어로 지정해야 합니다. 형식은 다음과 같습니다.

```
servername|search dn
```

여러 항목이 있는 경우

```
servername1|search dn servername2|search dn servername3|search dn...
```

동일한 검색에서 여러 사용자가 발견될 경우 인증은 실패합니다.

루트 사용자 바인드용 DN

이 필드는 관리자로서 주 활성 Directory Server 및 포트 필드에 지정된 Directory Server 에 바인딩하는 데 사용되는 사용자의 DN 을 지정합니다. 사용자 로그인 아이디에 기초하여 일치하는 사용자 DN 을 검색하려면 인증 서비스가 이 DN 으로 바인드되어야 합니다. 기본값은 amLDAPuser 입니다. 유효한 모든 DN 이 인식됩니다.

비밀번호가 잘못된 경우 사용자가 잠기기 때문에 로그아웃하기 전에 비밀번호가 올바른지 확인합니다. 사용자가 잠길 경우에는 AMConfig.Properties 파일의 com.ipplanet.authentication.super.user 등록 정보에 있는 슈퍼유저 DN 을 사용하여 로그인할 수 있습니다. 기본적으로 전체 DN 을 사용하더라도 이 amAdmin 계정을 사용하여 로그인하게 됩니다. 예를 들면 다음과 같습니다.

```
uid_amAdmin,ou=People,AccessManager-base
```

루트 사용자 바인드용 비밀번호

이 필드는 루트 사용자 바인드용 DN 필드에 지정된 관리자 프로필의 비밀번호를 포함합니다. 기본값은 없습니다. 관리자의 유효한 활성 디렉토리 비밀번호만 인식됩니다.

루트 사용자 바인드용 비밀번호 (확인)

비밀번호를 확인합니다.

사용자 프로필 검색 시 사용되는 활성 디렉토리 속성

사용자에 의한 인증이 성공한 후 사용자의 프로필이 검색됩니다. 이 속성의 값은 검색을 수행하는 데 사용됩니다. 이 필드는 사용할 활성 디렉토리 속성을 지정합니다. 기본적으로 Access Manager 는 사용자 항목이 uid 속성에 의해 식별된다고 가정합니다. Directory Server 가 다른 속성 (예 : givenname) 을 사용할 경우 이 필드에 속성 이름을 지정합니다.

주 사용자 검색 필터는 검색 필터 속성과 사용자 프로필 검색 시 사용되는 활성 디렉토리 속성을 결합한 것이 됩니다.

인증될 사용자 검색 시 사용되는 활성 디렉토리 속성

이 필드에서는 인증될 사용자에 대한 검색 필터 구성에 사용되는 속성을 나열하며, 사용자가 사용자 항목의 여러 속성으로 인증될 수 있게 합니다. 예를 들어, 이 필드를 uid, employeenumber 및 mail 로 설정한 경우 이러한 이름 중 하나로 사용자가 인증될 수 있습니다.

사용자 검색 필터

이 필드는 사용자 검색을 시작할 DN 필드에서 사용자를 찾는 데 사용될 속성을 지정하며 사용자 항목 이름 지정 속성과 함께 작동합니다. 기본값은 없습니다. 유효한 모든 사용자 항목 속성이 인식됩니다.

검색 범위

이 메뉴는 일치하는 사용자 프로필을 검색할 Directory Server 의 수준 수를 나타냅니다. 검색은 263 페이지의 " 사용자 검색을 시작할 DN" 속성에 지정된 노드에서 시작됩니다. 기본값은 SUBTREE 입니다. 다음 항목 중 하나를 목록에서 선택할 수 있습니다.

- 객체 - 지정된 노드만 검색합니다.
- 한 수준 - 지정된 노드 수준과 한 수준 아래에서 검색합니다.
- 하위 트리 - 지정된 노드와 그 아래 수준에 있는 모든 항목을 검색합니다.

주의 하위 조직의 사용자는 하위 조직이 비활성 상태인 경우에도 로그인할 수 있습니다. 이렇게 하지 못하도록 하려면 검색 범위와 기본 DN 이 해당 사용자가 속하는 특정 조직으로 설정해야 합니다.

SSL 이 활성화 Directory Server 에 액세스 가능

이 옵션은 주 및 보조 활성화 Directory Server 및 포트 필드에 지정된 Directory Server 에 대한 SSL 액세스를 사용 가능하게 합니다. 기본적으로 이 옵션은 사용 불가능하므로 Directory Server 에 액세스하는 데 SSL 프로토콜이 사용되지 않습니다. 그러나 이 속성이 사용 가능한 경우 비 SSL 서버에 바인드할 수 있습니다.

SSL 이 활성화된 상태에서 LDAP 서버가 실행되는 경우 (LDAPS), Access Manager 가 LDAPS 프로토콜을 통해 디렉토리 서버와 연결할 수 있도록 신뢰할 수 있는 SSL 인증서가 Access Manager 에서 구성되어야 합니다.

인증할 사용자 DN 반환

Access Manager 디렉토리가 활성화 디렉토리용으로 구성된 디렉토리와 동일한 경우 이 옵션을 사용할 수 있습니다. 이 옵션을 사용 가능하게 한 경우 활성화 디렉토리 인증 모듈은 userId 대신 DN 을 반환할 수 있으며 검색이 필요하지 않습니다. 일반적으로 인증 모듈은 userId 만 반환하며 인증 서비스는 로컬 Access Manager 활성화 디렉토리에서 사용자를 검색합니다. 외부 활성화 디렉토리가 사용될 경우 일반적으로 이 옵션은 대개 사용 가능하지 않습니다.

활성 Directory Server 확인 간격

이 속성은 활성 Directory Server 파일백에 사용됩니다. 이 속성은 활성 디렉토리 주 서버가 실행 중인지 확인하기 전에 스레드가 "일시 정지" 하는 시간 (분) 을 정의합니다.

사용자 작성 속성 목록

이 속성은 활성 Directory Server 가 외부 활성 Directory Server 로 구성된 경우에 활성 디렉토리 인증 모듈에서 사용됩니다. 이 속성은 로컬 Directory Server 와 외부 Directory Server 간의 속성 매핑을 포함합니다. 이 속성의 형식은 다음과 같습니다.

```
attr1|externalattr1
```

```
attr2|externalattr2
```

이 속성을 채우면 외부 Directory Server 에서 외부 속성 값을 읽은 다음 내부 Directory Server 속성 값을 설정합니다. 외부 속성 값은 **사용자 프로필** 속성 (핵심 인증 모듈에 있음) 이 "동적으로 작성" 으로 설정되고 사용자가 로컬 Directory Server 인스턴스에 없는 경우에만 내부 속성에 설정됩니다. 새로 작성된 사용자는 사용자 작성 속성 목록에 지정된 대로 매핑되는 외부 속성 값이 있는 내부 속성 값을 포함합니다.

인증 수준

인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 이 값은 인증을 어느 정도 신뢰할 수 있는지 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다. 기본값은 0 입니다.

주

지정된 인증 수준이 없을 경우 SSO 토큰은 핵심 인증 속성인 기본 인증 수준에 지정된 값을 저장합니다. 자세한 내용은 [288페이지의 "기본 인증 수준"](#)을 참조하십시오.

익명 인증 속성

익명 인증 속성은 조직 속성입니다. 서비스 구성에서 이러한 속성에 적용되는 값이 익명 인증 템플릿의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플릿을 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 하위 트리에 있는 항목은 조직 속성을 상속하지 않습니다. 익명 인증 속성은 다음과 같습니다.

- [267 페이지의 " 유효한 익명 사용자 목록 "](#)
- [268 페이지의 " 대소문자 구분 사용자 아이디 사용 "](#)
- [268 페이지의 " 기본 익명 아이디 "](#)
- [268 페이지의 " 인증 수준 "](#)

유효한 익명 사용자 목록

이 필드는 인증서를 제공하지 않고 로그인할 수 있는 사용 권한을 가진 사용자 아이디 목록을 포함합니다. 사용자의 로그인 이름이 이 목록의 사용자 아이디와 일치할 경우 액세스가 허가되며 지정된 사용자 아이디에 세션이 할당됩니다.

이 목록이 비어 있는 경우 다음 기본 모듈 로그인 URL 에 액세스하면 기본 익명 아이디로 인증됩니다.

```
protocol://server_host.server_domain:server_port/server_deploy_uri/UI/Login?module=Anonymous&org=org_name
```

이 목록이 비어 있지 않은 경우 기본 모듈 로그인 URL (위와 동일) 에 액세스하면 유효한 익명 아이디를 입력하라는 메시지가 표시됩니다.

이 목록이 비어 있지 않은 경우 다음 URL 에 액세스하여 로그인 페이지를 표시하지 않고 로그인할 수 있습니다.

```
protocol://server_host.server_domain:server_port/server_deploy_uri/UI/Login?module=Anonymous&org=org_name&IDToken1=<valid Anonymous username>
```

기본 익명 아이디

이 필드는 유효한 익명 사용자 목록이 비어 있고 다음 기본 모듈 로그인 URL 이 액세스되는 경우에 세션이 할당되는 사용자 아이디를 정의합니다.

```
protocol://server_host.server_domain:server_port/server_deploy_uri/UI/Login?module=Anonymous&org=org_name
```

기본값은 anonymous 입니다. 또한 조직에서 익명 사용자를 만들어야 합니다.

주 유효한 익명 사용자 목록이 비어 있지 않은 경우 기본 익명 아이디에 정의된 사용자를 사용하여 로그인 페이지에 액세스하지 않고 로그인할 수 있습니다. 그렇게 하려면 다음 URL 에 액세스합니다.

```
protocol://server_host.server_domain:server_port/server_deploy_uri/UI/Login?module=Anonymous&org=org_name&IDToken1=<DefaultAnonymous User Name>
```

대소문자 구분 사용자 아이디 사용

이 옵션을 사용하면 사용자 아이디에서 대소문자를 구분할 수 있습니다. 기본적으로 이 속성은 사용하지 않는 것으로 설정됩니다.

인증 수준

인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 이 값은 인증을 어느 정도 신뢰할 수 있는지 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다. 기본값은 0 입니다.

주

지정된 인증 수준이 없을 경우 SSO 토큰은 핵심 인증 속성인 기본 인증 수준에 지정된 값을 저장합니다. 자세한 내용은 [288 페이지의 "기본 인증 수준"](#) 을 참조하십시오. 2005Q1 릴리스에서는 이 기능이 제대로 수행되지 않지만 이전 릴리스에서는 제대로 수행됩니다.

인증서 인증 속성

인증서 인증 속성은 조직 속성입니다. 서비스 구성에서 이러한 속성에 적용되는 값이 인증서 인증 템플릿의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플릿을 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 하위 트리에 있는 항목은 조직 속성을 상속하지 않습니다. 인증서 인증 속성은 다음과 같습니다.

- 272 페이지의 "LDAP 에서 인증서 일치 "
- 272 페이지의 "LDAP 에서 인증서 검색 시 사용되는 주제 DN 속성 "
- 272 페이지의 "CRL 에 인증서 일치 "
- 272 페이지의 "LDAP 에서 CRL 검색 시 사용되는 발급자 DN 속성 "
- 273 페이지의 "OCSP 검증 사용 가능 "
- 273 페이지의 " 인증서가 저장되는 LDAP 서버 "
- 274 페이지의 "LDAP 검색 시작 DN"
- 274 페이지의 "LDAP 서버 기본 사용자 "
- 274 페이지의 "LDAP 서버 기본 비밀번호 "
- 274 페이지의 " 프로필 아이디의 LDAP 속성 "
- 275 페이지의 "LDAP 액세스에 SSL 사용 "
- 275 페이지의 " 사용자 프로필 액세스에 사용되는 인증서 필드 "
- 275 페이지의 " 사용자 프로필 액세스에 사용되는 기타 인증서 필드 "
- 276 페이지의 " 신뢰할 수 있는 원격 호스트 "
- 276 페이지의 "SSL 포트 번호 "
- 276 페이지의 " 인증 수준 "

LDAP 에서 인증서 일치

이 옵션은 로그인 시 제공되는 사용자 인증서가 LDAP 서버에 저장되어 있는지 검사할지 여부를 지정합니다. 일치하는 항목이 발견되지 않을 경우 사용자는 액세스가 거부됩니다. 일치하는 항목이 발견되고 다른 검증이 필요하지 않을 경우 사용자는 액세스가 허가됩니다. 기본값은 인증서 인증 서비스가 사용자 인증서를 검사하지 않는 것입니다.

주 Directory Server에 저장된 인증서는 반드시 유효할 필요는 없으며 인증서 해지 목록에 있어도 됩니다. [272 페이지의 "CRL 에 인증서 일치"](#) 을 참조하십시오. 그러나 웹 컨테이너는 로그인할 때 제공되는 사용자 인증서의 유효성을 확인할 수 있습니다.

LDAP 에서 인증서 검색 시 사용되는 주제 DN 속성

이 필드는 LDAP 에서 인증서를 검색하는 데 사용되는 인증서의 subjectDN 값 속성을 지정합니다. 이 속성은 사용자 항목을 고유하게 식별해야 합니다. 실제 값은 검색에 사용됩니다. 기본값은 cn 입니다.

CRL 에 인증서 일치

이 옵션은 LDAP 서버의 인증서 해지 목록 (CRL) 에 대해 사용자 인증서를 비교할지 여부를 지정합니다. CRL 은 발급자 subjectDN 의 속성 이름 중 하나로 찾습니다. 인증서가 CRL 에 있는 경우 사용자는 액세스가 거부되고 그렇지 않은 경우에는 액세스가 허용됩니다. 기본적으로 이 속성은 사용 불가능합니다.

주 인증서 소유자가 상태를 변경했고 더 이상 인증서 사용 권한을 갖고 있지 않거나, 인증서 소유자의 개인 키가 손상된 경우 인증서를 해지해야 합니다.

LDAP 에서 CRL 검색 시 사용되는 발급자 DN 속성

이 필드는 LDAP 에서 CRL 을 검색하는 데 사용되는 수신된 인증서의 발급자 subjectDN 값에 대한 속성을 지정합니다. 이 필드는 CRL 에 인증서 일치 속성이 사용 가능한 경우에만 사용됩니다. 실제 값은 검색에 사용됩니다. 기본값은 cn 입니다.

CRL 업데이트용 HTTP 매개 변수

이 필드는 CRL 업데이트를 위해 서버로부터 CRL 을 얻기 위한 HTTP 매개 변수를 지정합니다. 이러한 매개 변수에 대한 자세한 내용은 해당 CA 의 관리자에게 문의하십시오.

OCSP 검증 사용 가능

이 매개 변수를 사용하여 해당 OCSP 응답자에 연결하여 OCSP 검증을 수행할 수 있습니다. OCSP 응답자는 다음과 같이 런타임 도중에 결정됩니다.

- `com.sun.identity.authentication.ocspCheck` 가 `true` 이고 OCSP 응답자가 `com.sun.identity.authentication.ocsp.repsonder.url` 속성에 설정된 경우 이 속성 값이 OCSP 응답자로 사용됩니다.
- `com.sun.identity.authentication.ocspCheck` 가 `true` 로 설정되어 있는 경우 및 속성 값이 `AMConfig.properties` 파일에 설정되지 않은 경우 클라이언트 인증서에 제공된 OCSP 응답자가 OCSP 응답자로 사용됩니다.

`com.sun.identity.authentication.ocspCheck`가 `false`로 설정되어 있는 경우 또는 `com.sum.identity.authentication.ocspCheck`가 `true`로 설정되어 있지만 OCSP 응답자가 없는 경우 OCSP 검증이 수행되지 않습니다.

주	OCSP 검증을 사용할 수 있도록 하기 전에 Access Manager 시스템과 OCSP 응답자 시스템의 시간이 최대한 동기화되어 있는지 확인합니다. 또한 Access Manager 시스템의 시간이 OCSP 응답자의 시간보다 느려서는 안 됩니다. 예를 들면 다음과 같습니다. OCSP 응답자 시스템 - 오후 12:00:00 Access Manager 시스템 - 오후 12:00:30
----------	---

인증서가 저장되는 LDAP 서버

이 필드는 인증서가 저장되는 LDAP 서버의 이름과 포트 번호를 지정합니다. 기본값은 Access Manager 설치 시 지정된 호스트 이름과 포트입니다. 인증서가 저장되는 모든 LDAP 서버의 호스트 이름과 포트를 사용할 수 있습니다. 형식은 *hostname:port*입니다.

LDAP 검색 시작 DN

이 필드는 사용자 인증서에 대한 검색을 시작해야 하는 노드의 DN 을 지정합니다. 기본값은 없습니다. 이 필드는 모든 유효한 DN 을 인식합니다. 여러 항목이 있을 경우 로컬 서버 이름을 접두어로 지정해야 합니다. 형식은 다음과 같습니다.

```
servername|search dn
```

여러 항목이 있는 경우

```
servername1|search dn servername2|search dn servername3|search dn...
```

동일한 검색에서 여러 사용자가 발견될 경우 인증은 실패합니다.

LDAP 서버 기본 사용자

이 필드는 인증서가 저장되는 LDAP 서버에 대한 기본 사용자의 DN 을 지정합니다. 이 필드에는 기본값이 없으며 유효한 모든 DN 이 인식됩니다. Directory Server 에 저장된 인증서 정보를 읽고 검색할 수 있는 권한이 기본 사용자에게 허가되어야 합니다.

LDAP 서버 기본 비밀번호

이 필드는 [LDAP 서버 기본 사용자](#) 필드에 지정된 사용자와 연관된 LDAP 비밀번호 를 지정합니다. 이 필드에는 기본값이 없으며 지정된 기본 사용자에 대한 유효한 LDAP 비밀번호가 인식됩니다.

주 이 값은 읽을 수 있는 텍스트로 디렉토리에 저장됩니다.

프로필 아이디의 LDAP 속성

이 필드는 올바른 사용자 프로필을 식별하는 데 사용해야 하는 값을 가진 인증서와 일치하는 Directory Server 항목의 속성을 지정합니다. 이 필드에는 기본값이 없으며 사용자 아이디로 사용할 수 있는 사용자 항목의 모든 유효한 속성 (예 : cn, sn 등) 이 인식됩니다.

LDAP 액세스에 SSL 사용

이 옵션은 SSL 을 사용하여 LDAP 서버에 액세스할지 여부를 지정합니다. 기본값은 인증서 인증 서비스가 LDAP 액세스에 SSL 을 사용하지 않는 것입니다.

사용자 프로필 액세스에 사용되는 인증서 필드

이 메뉴는 일치하는 사용자 프로필을 검색하는 데 사용해야 할 인증서 주제 DN 의 필드를 지정합니다. 예를 들어, email address 를 선택할 경우 인증서 인증 서비스는 사용자 인증서의 email address 속성과 일치하는 사용자 프로필을 검색합니다. 그런 다음, 로그인하는 사용자는 일치하는 프로필을 사용하게 됩니다. 기본값은 subject CN 입니다. 목록에는 다음 항목이 포함되어 있습니다.

- 전자 메일 주소
- 주제 CN
- 주제 DN
- 주제 UID
- 기타

사용자 프로필 액세스에 사용되는 기타 인증서 필드

사용자 프로필 액세스에 사용되는 인증서 필드 속성 값을 other 로 설정할 경우 이 필드는 수신된 인증서의 subjectDN 값에서 선택할 속성을 지정합니다. 그런 다음, 인증 서비스는 해당 속성의 값과 일치하는 사용자 프로필을 검색합니다.

신뢰할 수 있는 원격 호스트

이 속성은 Access Manager 에 인증서를 보내도록 신뢰할 수 있는 호스트 목록을 정의합니다. Access Manager 는 인증서가 신뢰할 수 있는 호스트 중 하나에서 온 것인지 확인해야 합니다. 이 구성은 Sun Java System Portal Server 에만 사용됩니다.

이 속성은 다음 값을 가집니다.

- **없음**. 이 속성이 사용 불가능하게 됩니다. 기본적으로 이 값이 설정됩니다.
- **모두**. 모든 클라이언트 IP 주소로부터 Portal Server 게이트웨이 스타일의 인증서 인증을 허용합니다.
- **IP 주소**. Portal Server 게이트웨이 스타일의 인증서 인증 요청을 허용할 IP 주소를 나열합니다(게이트웨이의 IP 주소). 이 속성은 조직별로 구성할 수 있습니다.

SSL 포트 번호

이 속성은 Secure Socket Layer 의 포트 번호를 지정합니다. 현재 이 속성은 게이트웨이 서버릿에서만 사용됩니다. SSL 포트 번호를 추가하거나 변경하기 이전에 Access Manager Developer's Guide 에서 7 장의 "Policy-Based Resource Management" 절을 참조하십시오.

인증 수준

인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 이 값은 인증을 어느 정도 신뢰할 수 있는지 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다. 기본값은 0 입니다.

주

지정된 인증 수준이 없을 경우 SSO 토큰은 핵심 인증 속성인 기본 인증 수준에 지정된 값을 저장합니다. 자세한 내용은 [288 페이지의 "기본 인증 수준"](#) 을 참조하십시오. 2005Q1 릴리스에서는 이 기능이 제대로 수행되지 않지만 이전 릴리스에서는 제대로 수행됩니다.

핵심 인증 속성

핵심 인증 서비스는 모든 기본 인증 서비스뿐만 아니라 모든 사용자 정의 인증 모듈 속성에 대한 기본 서비스입니다. 핵심 인증은 모든 형태의 인증을 사용하려는 각 조직에 대해 서비스로 구성되어야 합니다. 핵심 인증 속성은 전역 속성과 조직 속성으로 구성됩니다. 전역 속성에 적용되는 값은 Sun Java System Access Manager 구성 전체에 걸쳐 적용되어 구성된 모든 조직이 상속합니다. 전역 속성의 목표는 Access Manager 응용 프로그램을 사용자 정의하는 것이므로 이러한 값은 역할이나 조직에 직접 적용할 수 없습니다. 서비스 구성에서 조직 속성에 적용되는 값이 핵심 인증 템플릿의 기본값이 됩니다. 조직의 서비스를 추가한 후 서비스 템플릿을 만들어야 합니다. 기본값은 조직의 관리자가 추가 후 변경할 수 있습니다. 조직의 항목은 조직 속성을 상속하지 않습니다. 핵심 인증 속성은 다음과 같이 구분됩니다.

- [277 페이지의 "전역 속성"](#)
- [279 페이지의 "조직 속성"](#)

전역 속성

핵심 인증 서비스의 전역 속성은 다음과 같습니다.

- [278 페이지의 "플러그 가능 인증 모듈 클래스"](#)
- [278 페이지의 "지원되는 클라이언트용 인증 모듈"](#)
- [278 페이지의 "LDAP 연결 풀 크기"](#)
- [278 페이지의 "기본 LDAP 연결 풀 크기"](#)

플러그 가능 인증 모듈 클래스

이 필드는 Access Manager 플랫폼 내에서 구성된 모든 조직에서 사용할 수 있는 인증 모듈의 Java 클래스를 지정합니다. 기본적으로 여기에는 LDAP, SafeWord, SecurID, 응용 프로그램, 익명, HTTP 기본, 구성원, Unix, 인증서, NT, RADIUS 및 Windows 데스크탑 SSO가 포함됩니다. 또한 AMLoginModule SPI 또는 JAAS LoginModule SPI를 구현하여 사용자 정의 인증 모듈을 작성할 수 있습니다. 자세한 내용은 Access Manager Developer's Guide를 참조하십시오. 새 서비스를 정의하려면 새로운 각 인증 서비스의 전체 클래스 이름 (패키지 이름 포함)을 지정하는 텍스트 문자열을 이 필드에 입력해야 합니다.

지원되는 클라이언트용 인증 모듈

이 속성은 특정 클라이언트에 대해 지원되는 인증 모듈 목록을 지정합니다. 형식은 다음과 같습니다.

```
clientType | module1,module2,module3
```

이 속성은 클라이언트 검색이 사용 가능한 경우에 적용됩니다.

LDAP 연결 풀 크기

이 속성은 특정 LDAP 서버와 포트에서 사용되는 최소 및 최대 연결 풀을 지정합니다. 이 속성은 LDAP 및 구성원 인증 서비스에만 사용됩니다. 형식은 다음과 같습니다.

```
host:port:min:max
```

주 이 연결 풀은 serverconfig.xml에 구성된 SDK 연결 풀과 다릅니다.

기본 LDAP 연결 풀 크기

이 속성은 모든 LDAP 인증 모듈 구성과 함께 사용되는 기본 최소 및 최대 연결 풀을 설정합니다. 호스트와 포트에 대한 항목이 [LDAP 연결 풀 크기](#) 속성에 존재할 경우 LDAP 연결 기본 풀 크기의 최소 및 최대 설정이 사용됩니다.

조직 속성

핵심 인증 서비스의 조직 속성은 다음과 같습니다.

- 280 페이지의 " 조직 인증 모듈 "
- 280 페이지의 " 사용자 프로필 "
- 280 페이지의 " 관리자 인증 구성 "
- 281 페이지의 " 사용자 프로필 동적 작성 기본 역할 "
- 281 페이지의 " 영구 쿠키 모드 사용 가능 "
- 281 페이지의 " 영구 쿠키 최대 시간 "
- 282 페이지의 " 모든 사용자를 위한 사용자 컨테이너 "
- 282 페이지의 " 별칭 검색 속성 이름 "
- 288 페이지의 " 기본 인증 수준 "
- 282 페이지의 " 아이디 지정 속성 "
- 283 페이지의 " 기본 인증 로컬 "
- 284 페이지의 " 조직 인증 구성 "
- 285 페이지의 " 로그인 실패 잠금 모드 사용 가능 "
- 285 페이지의 " 로그인 실패 잠금 수 "
- 285 페이지의 " 로그인 실패 잠금 간격 "
- 285 페이지의 " 잠금 알림을 보낼 전자 메일 주소 "
- 285 페이지의 "N 회 실패 후 사용자에게 경고 "
- 286 페이지의 " 로그인 실패 잠금 기간 "
- 286 페이지의 " 잠금 속성 이름 "
- 286 페이지의 " 잠금 속성 값 "
- 286 페이지의 " 기본 성공 로그인 URL "
- 287 페이지의 " 기본 실패 로그인 URL "
- 287 페이지의 " 인증 사후 처리 클래스 "
- 287 페이지의 " 사용자 아이디 생성 모드 사용 가능 "
- 287 페이지의 " 플러그 가능 아이디 생성기 클래스 "

조직 인증 모듈

이 목록에서는 조직에 등록되어 사용할 수 있는 인증 모듈을 지정합니다. 각 관리자는 각 특정 조직에 대한 인증 유형을 선택할 수 있습니다. 여러 인증 모듈이 유연성을 제공하지만 사용자는 자신의 로그인 설정이 선택된 인증 모듈에 적합한지 확인해야 합니다. 기본 인증은 LDAP 입니다. Access Manager 에 포함된 인증 서비스는 다음과 같습니다.

주 관리자가 핵심 및 인증 모듈 템플릿을 작성하고 작성된 조직에서 이러한 사실을 알려야만 해당 조직이 제대로 작동합니다.

사용자 프로필

이 옵션을 사용하면 사용자 프로필의 옵션을 지정할 수 있습니다.

- 필수 - 인증에 성공한 경우 Access Manager 와 함께 설치된 로컬 Directory Server 에 사용자의 프로필이 있어야만 인증 서비스가 SSO 토큰을 발급하도록 지정합니다.
- Dynamic - 인증에 성공한 경우 사용자 프로필이 아직 존재하지 않는다면 인증 서비스에서 이를 만들도록 지정합니다. 그런 다음 SSO 토큰이 발급됩니다. 사용자 프로필은 Access Manager 와 함께 설치된 로컬 Directory Server 에 만들어 집니다.
- Dynamic With User Alias - 인증에 성공한 경우 인증 서비스에서 사용자 별칭 목록 속성을 사용하여 사용자 프로필을 만듭니다.
- Ignore - 인증 서비스가 성공적인 인증을 위해 SSO 토큰을 발급하는 데 사용자 프로필이 필요하지 않도록 지정합니다.

관리자 인증 구성

편집 링크를 클릭하면 관리자에 대해서만 인증 서비스를 정의할 수 있습니다. 관리자의 인증 모듈이 최종 사용자의 모듈과 달라야 하는 경우 이 속성을 사용할 수 있습니다. 이 속성에 구성된 모듈은 Access Manager 콘솔에 액세스할 때 선택됩니다. 예를 들면 다음과 같습니다.

```
http://servername.port/console_deploy_uri
```

사용자 프로필 동적 작성 기본 역할

이 필드는 280 페이지의 "사용자 프로필" 기능을 통해 동적 작성을 선택한 경우 프로필이 작성되는 새 사용자에게 할당되는 역할을 지정합니다. 기본값은 없습니다. 관리자는 새 사용자에게 할당할 역할의 DN 을 지정해야 합니다.

주	지정된 역할은 인증이 구성되고 있는 조직 아래에 있어야 합니다. 이 역할은 Access Manager 또는 LDAP 역할 중 하나일 수 있지만 필터링된 역할일 수는 없습니다. 사용자에게 특정 서비스가 자동으로 할당되게 하려면 사용자 프로필에 필수 서비스를 구성해야 합니다.
----------	---

영구 쿠키 모드 사용 가능

이 옵션은 사용자가 브라우저를 다시 시작하고 자신의 인증된 세션으로 돌아갈 수 있는지 여부를 결정합니다. **영구 쿠키 모드 사용 가능**을 사용 가능하게 하여 사용자 세션을 유지할 수 있습니다. **영구 쿠키 모드 사용 가능**을 사용 가능하게 하면 영구 쿠키가 만료되거나 사용자가 명시적으로 로그아웃할 때까지 사용자 세션이 만료되지 않습니다. 만료 시간은 **영구 쿠키 최대 시간**에 지정됩니다. 기본값은 **영구 쿠키 모드**가 사용 가능하지 않고 인증 서비스가 메모리 쿠키만 사용하는 것입니다.

주	로그인 URL 에서 <code>iPSPCookie=yes</code> 매개 변수를 사용하여 클라이언트가 영구 쿠키를 명시적으로 요청해야 합니다.
----------	--

영구 쿠키 최대 시간

이 필드는 그 이후에 영구 쿠키가 만료되는 간격을 지정합니다. 해당 확인란을 선택하여 **영구 쿠키 모드 사용 가능**을 사용 가능하게 해야 합니다. 이 간격은 사용자의 세션이 성공적으로 인증되었을 때 시작됩니다. 기본값은 2147483 (초) 입니다. 이 필드는 0 에서 2147483 사이의 모든 정수 값을 가집니다.

모든 사용자를 위한 사용자 컨테이너

사용자별로 인증이 성공한 후 사용자의 프로필이 검색됩니다. 이 필드의 값은 프로필을 검색하는 위치를 지정합니다. 일반적으로 이 값은 기본 사용자 컨테이너의 DN이 됩니다. 조직에 추가되는 모든 사용자 항목은 조직의 기본 사용자 컨테이너에 자동으로 추가됩니다. 기본값은 `ou=People`이며 일반적으로 조직 이름과 루트 접두어로 완성됩니다. 이 필드는 모든 조직 구성 단위의 유효한 DN을 가집니다.

주

인증은 다음 작업을 차례로 수행하여 사용자 프로필을 검색합니다.

- 기본 사용자 컨테이너에서 검색
- 기본 조직에서 검색
- 별칭 검색 속성 이름 속성을 사용하여 기본 조직에서 사용자 검색

최종 검색은 인증에 사용되는 아이디가 프로필의 이름 지정 속성이 아닐 수 있는 SSO 경우에 대한 것입니다. 예를 들어, 사용자는 `jn10191`의 `Safeword` 아이디를 사용하여 인증할 수 있지만 해당 프로필은 `uid=jamie`일 수 있습니다.

별칭 검색 속성 이름

사용자별로 인증이 성공한 후 사용자의 프로필이 검색됩니다. 이 필드는 [282 페이지의 "아이디 지정 속성"](#)에 지정된 첫 번째 LDAP 속성에 대한 검색에서 일치하는 사용자 프로필을 찾지 못한 경우 검색할 두 번째 LDAP 속성을 지정합니다. 주로 이 속성은 인증 모듈에서 반환된 사용자 아이디가 아이디 지정 속성에 지정된 것과 다를 경우에 사용됩니다. 예를 들어, RADIUS 서버는 `abc1234`를 반환하지만 아이디는 `abc`일 수 있습니다. 이 필드에는 기본값이 없으며 유효한 모든 LDAP 속성(예: `cn`)이 사용될 수 있습니다.

아이디 지정 속성

사용자별로 인증이 성공한 후 사용자의 프로필이 검색됩니다. 이 속성 값은 검색에 사용할 LDAP 속성을 지정합니다. 기본적으로 Access Manager는 사용자 항목이 `uid` 속성에 의해 식별된다고 가정합니다. Directory Server가 다른 속성(예: `givenname`)을 사용할 경우 이 필드에 속성 이름을 지정합니다.

기본 인증 로케일

이 필드는 인증 서비스에 사용되는 기본 언어 서브 타입을 지정합니다. 기본값은 en_US입니다. 유효한 언어 서브 타입 목록은 [표 20-1](#)에서 확인할 수 있습니다.

다른 로케일을 사용하려면 해당 로케일에 대한 모든 인증 템플릿을 먼저 만들어야 합니다. 그런 다음 이러한 템플릿에 대해 새 디렉토리를 만들어야 합니다. 자세한 내용은 [132 페이지의 "로그인 URL 매개 변수"](#)를 참조하십시오.

표 20-1 지원되는 언어 로케일

언어 태그	언어
af	아프리카니어
be	벨로루시어
bg	불가리아어
ca	카탈로니아어
cs	체코어
da	덴마크어
de	독일어
el	그리스어
en	영어
es	스페인어
eu	바스크어
fi	핀란드어
fo	페로어
fr	프랑스어
ga	아일랜드어
gl	갈리시아어
hr	크로아티아어
hu	헝가리어
id	인도네시아어
is	아이슬란드어
it	이탈리아어
ja	일본어

표 20-1 지원되는 언어 로케일 (계속)

언어 태그	언어
ko	한국어
nl	네덜란드어
아니오	노르웨이어
pl	폴란드어
pt	포르투갈어
ro	루마니아어
ru	러시아어
sk	슬로바키아어
sl	슬로베니아어
sq	알바니아어
sr	세르비아어
sv	스웨덴어
tr	터키어
uk	우크라이나어
zh	중국어

조직 인증 구성

이 속성은 조직의 인증 모듈을 설정합니다. 기본 인증 모듈은 LDAP입니다. 편집 링크를 눌러 하나 이상의 인증 모듈을 선택할 수 있습니다. 여러 모듈을 선택할 경우 사용자는 선택된 모든 모듈 체인을 통과해야 합니다.

이 속성에 구성된 모듈은 사용자가 `/server_deploy_uri/UL/Login` 형식을 사용하여 인증 모듈에 액세스할 때 인증을 위해 사용됩니다. 자세한 내용은 *Access Manager Developer's Guide* 를 참조하십시오.

로그인 실패 잠금 모드 사용 가능

이 기능은 첫 번째 인증이 실패할 경우 사용자가 두 번째 인증을 시도할 수 있는지 여부를 지정합니다. 이 속성을 선택하면 잠금이 사용 가능하고 사용자는 한 번만 인증할 수 있습니다. 기본적으로 잠금 기능은 사용 불가능으로 설정되어 있습니다. 이 속성은 잠금 관련 및 알림 속성과 함께 사용됩니다.

로그인 실패 잠금 수

이 속성은 사용자가 잠기기 전에 **로그인 실패 잠금 간격**에 정의된 시간 간격 내에서 사용자가 인증을 시도할 수 있는 횟수를 정의합니다.

로그인 실패 잠금 간격

이 속성은 실패한 두 로그인 시도 사이의 간격 (분) 을 정의합니다. 로그인에 실패한 다음 잠금 간격 내에 다시 로그인에 실패할 경우 잠금 개수가 증가됩니다. 그렇지 않으면 잠금 개수가 재설정됩니다.

잠금 알림을 보낼 전자 메일 주소

이 속성은 사용자 잠금이 발생한 경우 알림을 받게 될 전자 메일 주소를 지정합니다. 여러 주소로 전자 메일 알림을 보내려면 각 전자 메일 주소를 공백으로 구분합니다. 영어가 아닌 로캘의 경우 다음과 같은 형식을 사용합니다.

```
email_address|locale|charset
```

N 회 실패 후 사용자에게 경고

이 속성은 사용자가 잠길 것이라는 경고 메시지를 Access Manager 가 보내기 전에 발생할 수 있는 인증 실패 수를 지정합니다.

로그인 실패 잠금 기간

이 속성은 메모리 잠금을 사용 가능하게 합니다. 기본적으로 잠금 기법은 잠금 속성 이름에 정의된 사용자 프로필 (로그인 실패 이후) 을 비활성화합니다. 로그인 실패 잠금 기간 값이 0 보다 큰 경우 메모리 잠금과 해당 사용자 계정이 지정된 기간 (분) 동안 잠깁니다.

잠금 속성 이름

이 속성은 잠금에 대해 설정할 LDAP 속성을 지정합니다. 잠금 속성 값에서 값을 변경하여 이 속성 이름에 대해 잠금을 사용 가능하게 할 수도 있습니다. 기본적으로 Access Manager 콘솔에서 잠금 속성 이름은 비어 있습니다. 기본 구현 값은 사용자가 잠기고 로그인 실패 잠금 기간이 0 으로 설정되어 있는 경우 `inetuserstatus` (LDAP 속성) 및 `inactive` 입니다.

잠금 속성 값

이 속성은 [잠금 속성 이름](#)에 정의된 속성에 대해 잠금이 사용 가능한지 사용 불가능한지 여부를 지정합니다. 기본적으로 `inetuserstatus`에 대해 값이 0 으로 설정됩니다.

기본 성공 로그인 URL

이 필드는 성공적인 인증 후 사용자가 리디렉션되는 URL 을 지정하는 다수의 값 목록을 허용합니다. 기본 HTML 유형을 가정하는 URL 의 값만 지정할 수 있지만 이 속성의 형식은 `clientType|URL` 입니다.

주 기본값은 `/amconsole` 입니다. 이번 릴리스에서는 *protocol*, *host* 및 *port* 값이 더 이상 필요 없습니다.

원격 콘솔의 경우 실제 원격 콘솔 호스트의 콘솔 페이지를 가리키도록 이 속성을 수동으로 수정해야 합니다.

기본 실패 로그인 URL

인증에 실패한 후 사용자가 리디렉션되는 URL 을 지정하는 다수의 값 목록을 허용합니다. 기본 HTML 유형을 가정하는 URL 의 값만 지정할 수 있지만 이 속성의 형식은 `clientType|URL` 입니다.

인증 사후 처리 클래스

이 필드는 성공 또는 실패 로그인에 대한 인증 사후 프로세스를 사용자 정의하는 데 사용되는 Java 클래스의 이름을 지정합니다. 예를 들면 다음과 같습니다.

```
com.abc.authentication.PostProcessClass
```

Java 클래스는 다음과 같은 Java 인터페이스를 구현해야 합니다.

```
com.sun.identity.authentication.spi.AMPostAuthProcessInterface
```

또한, Web Server 의 Java Classpath 속성에 클래스를 찾을 경로를 추가해야 합니다.

사용자 아이디 생성 모드 사용 가능

이 속성은 구성원 인증 모듈에 사용됩니다. 이 속성 필드가 사용 가능하면 구성원 모듈은 사용자 아이디가 이미 존재할 경우 자동 등록 프로세스 중에 특정 사용자에게 대한 사용자 아이디를 생성할 수 있습니다. 사용자 아이디는 [플러그 가능 아이디 생성기 클래스](#)에 지정된 Java 클래스로부터 생성됩니다.

플러그 가능 아이디 생성기 클래스

이 필드는 [사용자 아이디 생성 모드 사용 가능](#)이 사용 가능한 경우 사용자 아이디를 생성하는 데 사용되는 Java 클래스의 이름을 지정합니다.

기본 인증 수준

이 인증 수준 값은 인증을 어느 정도 신뢰할 수 있는지를 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다.

인증 수준은 조직의 특정 인증 템플릿 내에서 설정해야 합니다. 여기서 설명한 기본 인증 수준 값은 특정 조직 인증 템플릿의 인증 수준 필드에서 인증 수준이 지정되지 않은 경우에만 적용됩니다. 기본 인증 수준의 기본값은 0입니다 (이 속성 값은 Access Manager 에서 사용되는 것이 아니라 이 값을 사용하도록 선택한 모든 외부 응용 프로그램에서 사용됨). 2005Q1 릴리스에서는 이 기능이 제대로 수행되지 않지만 이전 릴리스에서는 제대로 수행됩니다.

HTTP 기본 인증 속성

HTTP 기본 인증 속성은 조직 속성입니다. 서비스 구성에서 이러한 속성에 적용되는 값이 HTTP 기본 인증 템플릿의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플릿을 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 항목은 조직 속성을 상속하지 않습니다.

HTTP 기본 인증 속성은 다음과 같습니다.

인증 수준

인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 이 값은 인증을 어느 정도 신뢰할 수 있는지 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다. 기본값은 0입니다.

주

지정된 인증 수준이 없을 경우 SSO 토큰은 핵심 인증 속성인 기본 인증 수준에 지정된 값을 저장합니다. 자세한 내용은 [288 페이지의 "기본 인증 수준"](#)을 참조하십시오. 2005Q1 릴리스에서는 이 기능이 제대로 수행되지 않지만 이전 릴리스에서는 제대로 수행됩니다.

JDBC 인증 속성

JDBC (Java Database Connectivity) 인증 속성은 조직 속성입니다. 서비스 구성에서 이러한 속성에 적용되는 값이 JDBC 인증 템플릿의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플릿을 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 항목은 조직 속성을 상속하지 않습니다. JDBC 인증 속성은 다음과 같습니다.

- 291 페이지의 "연결 유형"
- 292 페이지의 "연결 풀 JNDI 이름"
- 293 페이지의 "JDBC 드라이버"
- 294 페이지의 "JDBC URL"
- 294 페이지의 "데이터베이스에 연결할 사용자"
- 294 페이지의 "데이터베이스에 연결할 비밀번호"
- 294 페이지의 "데이터베이스에 연결할 비밀번호 (확인)"
- 294 페이지의 "데이터베이스의 비밀번호 열"
- 294 페이지의 "준비된 명령문"
- 295 페이지의 "비밀번호 구문을 변환할 클래스"
- 295 페이지의 "인증 수준"

연결 유형

이 필드는 JNDI (Java Naming and Directory Interface) 연결 풀 또는 JDBC 드라이버를 사용하여 SQL 데이터베이스에 대한 연결 유형을 지정합니다. 옵션은 다음과 같습니다.

- Connection pool is retrieved via JDNI
- Non-persistent JDBC connection

JNDI 연결 풀은 기본 웹 컨테이너에서 구성을 사용합니다.

연결 풀 JNDI 이름

연결 유형에서 JNDI 를 선택하면 이 필드가 연결 풀 이름을 지정합니다. JDBC 인증에서 웹 컨테이너가 제공하는 JNDI 연결 풀을 사용하므로 JNDI 연결 풀의 설정이 다른 웹 컨테이너와 다를 수 있습니다.

다음은 Web Server 및 MySQL 4.0 용으로 연결 풀을 설정하는 예입니다.

1. Web Server 콘솔에서 다음 속성을 가진 JDBC 연결 풀을 만듭니다.

풀 이름 : samplePool

데이터 소스 클래스 이름 :

com.mysql.jdbc.jdbc2.optional.MysqlDataSource

서버 이름 : MySQL 서버의 서버 이름

포트 : MySQL 서버가 실행 중인 포트 번호

사용자 : 데이터베이스의 사용자 이름

비밀번호 : 사용자의 비밀번호

데이터베이스 이름 : 데이터베이스 이름

주 다음 단계에서 설명하는 데이터 소스 클래스 및 JDBC 드라이버 클래스를 포함하는 jar 파일을 응용 프로그램 클래스 경로에 추가해야 합니다.

2. JDBC 자원을 구성합니다. Web Server 콘솔에서 다음 속성을 가진 JDBC 자원을 만듭니다.

JNDI 이름 : jdbc/samplePool

풀 이름 : samplePool

데이터 자원 사용 : on

3. 응용 프로그램의 sun-web.xml 파일에 다음 행을 추가합니다.

```
<resource-ref>

  <res-ref-name>jdbc/mysql</res-ref-name>

  <jndi-name>jdbc/samplePool</jndi-name>

</resource-ref>
```

4. 응용 프로그램의 web.xml 파일에 다음 행을 추가합니다 .

```
<resource-ref>

  <description>mysql Database</description>

  <res-ref-name>jdbc/mysql</res-ref-name>

  <res-type>javax.sql.DataSource</res-type>

  <res-auth>Container</res-auth>

</resource-ref>
```

설정을 완료하면 이 속성 값이 다음과 같아야 합니다 .

```
java:comp/env/jdbc/mysql
```

JDBC 드라이버

연결 유형에서 JDBC 를 선택한 경우 이 필드에서 SQL 데이터베이스가 제공하는 JDBC 를 지정합니다 . 예를 들면 다음과 같습니다 .

```
com.mysql.jdbc.Driver
```

JDBC URL

연결 유형에서 JDBC 를 선택한 경우 이 필드에서 데이터베이스 URL 을 지정합니다. 예를 들어 , MySQL 의 URL 은 다음과 같습니다 .

```
jdbc:mysql://hostname:port/databaseName
```

데이터베이스에 연결할 사용자

이 필드에서는 JDBC 에 연결하기 위해 데이터베이스에 연결할 사용자 이름을 지정합니다 .

데이터베이스에 연결할 비밀번호

이 필드에서는 데이터베이스에 연결할 사용자에서 지정한 사용자의 비밀번호를 정의합니다 .

데이터베이스에 연결할 비밀번호 (확인)

비밀번호를 확인합니다 .

데이터베이스의 비밀번호 열

이 필드에서는 SQL 데이터베이스의 비밀번호 열 이름을 지정합니다 .

준비된 명령문

이 필드에서는 로그인한 사용자의 비밀번호를 검색하는 SQL 문을 지정합니다 . 예를 들어 , 다음과 같습니다 .

```
select Password from Employees where USERNAME = ?
```


비밀번호 구문을 변환할 클래스

이 속성은 비밀번호를 비교하기 위해 데이터베이스에서 검색한 비밀번호를 사용자 입력 형식으로 변환할 클래스 이름을 지정합니다. 이 클래스는 반드시 `JDBCPasswordSyntaxTransform` 인터페이스를 구현해야 합니다.

인증 수준

인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 이 값은 인증을 어느 정도 신뢰할 수 있는지 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다. 기본값은 0입니다.

LDAP 인증 속성

LDAP 인증 속성은 조직 속성입니다. 서비스 구성에서 이러한 속성에 적용되는 값이 LDAP 인증 템플릿의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플릿을 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 항목은 조직 속성을 상속하지 않습니다. LDAP 인증 속성은 다음과 같습니다.

- 298 페이지의 " 주 LDAP 서버 "
- 298 페이지의 " 보조 LDAP 서버 "
- 299 페이지의 " 사용자 검색을 시작할 DN"
- 299 페이지의 " 루트 사용자 바인드용 DN"
- 299 페이지의 " 루트 사용자 바인드용 비밀번호 "
- 300 페이지의 " 루트 사용자 바인드용 비밀번호 (확인)"
- 300 페이지의 " 사용자 프로필 검색 시 사용되는 LDAP 속성 "
- 300 페이지의 " 인증될 사용자 검색 시 사용되는 LDAP 속성 "
- 300 페이지의 " 사용자 검색 필터 "
- 300 페이지의 " 검색 범위 "
- 301 페이지의 "SSL 이 LDAP 서버에 액세스 가능 "
- 301 페이지의 " 인증할 사용자 DN 반환 "
- 301 페이지의 "LDAP 서버 확인 간격 "
- 302 페이지의 " 사용자 작성 속성 목록 "
- 302 페이지의 " 인증 수준 "

주 LDAP 서버

이 필드는 Access Manager 설치 도중 지정된 주 LDAP 서버의 호스트 이름과 포트 번호를 지정합니다. 이 LDAP 서버는 LDAP 인증을 위해 연결되는 첫 번째 서버입니다. 형식은 `hostname:port` 입니다. (포트 번호가 없을 경우 포트 번호를 389 라고 가정합니다.)

Access Manager 를 여러 도메인으로 배포한 경우 Access Manager 의 특정 인스턴스와 Directory Server 의 특정 인스턴스 간의 통신 링크를 다음 형식으로 지정할 수 있습니다 (여러 항목에서 로컬 서버 이름을 접두어로 사용해야 함).

```
local_servername|server:port local_servername2|server2:port2 ...
```

예를 들어 , Directory Server 의 서로 다른 인스턴스 (L1-machine1-DS 및 L2-machine2-DS) 와 통신하는 두 Access Manager 를 서로 다른 위치 (L1-machine1-IS 및 L2-machine2-IS) 에 배포한 경우 형식은 다음과 같습니다.

```
L1-machine1-IS.example.com|L1-machine1-DS.example.com:389  
L2-machine2-IS.example.com|L2-machine2-DS.example.com:389
```

보조 LDAP 서버

이 필드는 Access Manager 플랫폼에 사용할 수 있는 보조 LDAP 서버의 호스트 이름과 포트 번호를 지정합니다. 주 LDAP 서버가 인증 요청에 응답하지 않을 경우 이 서버에 연결됩니다. 주 서버가 실행 중인 경우 Access Manager 는 주 서버로 다시 전환합니다. 형식은 `hostname:port` 입니다. 여러 항목이 있을 경우 로컬 서버 이름을 접두어로 지정해야 합니다.

주의

Access Manager 엔터프라이즈와 떨어져 있는 원격 Directory Server 에서 사용자를 인증하는 경우 주 LDAP 서버 포트와 보조 LDAP 서버 포트 모두에 값이 있어야 합니다. 하나의 Directory Server 위치에 대한 값을 두 필드 모두에 사용할 수 있습니다.

사용자 검색을 시작할 DN

이 필드는 사용자 검색이 시작되는 노드의 DN 을 지정합니다. (성능상의 이유 때문에 이 DN 은 가능한 구체적이어야 합니다.) 기본값은 디렉토리 트리의 루트입니다. 유효한 모든 DN 이 인식됩니다. **검색 범위** 속성에서 OBJECT 를 선택한 경우에는 DN 에서 프로필이 있는 수준보다 한 수준 위를 지정해야 합니다.

여러 항목이 있을 경우 로컬 서버 이름을 접두어로 지정해야 합니다. 형식은 다음과 같습니다.

```
servername|search dn
```

여러 항목이 있는 경우

```
servername1|search dn servername2|search dn servername3|search dn...
```

동일한 검색에서 여러 사용자가 발견될 경우 인증은 실패합니다.

루트 사용자 바인드용 DN

이 필드는 관리자로서 주 LDAP 서버 및 포트 필드에 지정된 Directory Server 에 바인딩하는 데 사용되는 사용자의 DN 을 지정합니다. 사용자 로그인 아이디에 기초하여 일치하는 사용자 DN 을 검색하려면 인증 서비스가 이 DN 으로 바인드되어야 합니다. 기본값은 amldapuser 입니다. 유효한 모든 DN 이 인식됩니다.

비밀번호가 잘못된 경우 사용자가 잠기기 때문에 로그아웃하기 전에 비밀번호가 올바른지 확인합니다. 사용자가 잠길 경우에는 AMConfig.Properties 파일의 com.ipplanet.authentication.super.user 등록 정보에 있는 슈퍼유저 DN 을 사용하여 로그인할 수 있습니다. 기본적으로 전체 DN 을 사용하더라도 이 amAdmin 계정을 사용하여 로그인하게 됩니다. 예를 들면 다음과 같습니다.

```
uid_amAdmin,ou=People,AccessManager-base
```

루트 사용자 바인드용 비밀번호

이 필드는 루트 사용자 바인드용 DN 필드에 지정된 관리자 프로필의 비밀번호를 포함합니다. 기본값은 없습니다. 관리자의 유효한 LDAP 비밀번호만 인식됩니다.

루트 사용자 바인드용 비밀번호 (확인)

비밀번호를 확인합니다.

사용자 프로필 검색 시 사용되는 LDAP 속성

사용자별로 인증이 성공한 후 사용자의 프로필이 검색됩니다. 이 속성의 값은 검색을 수행하는 데 사용됩니다. 이 필드는 사용할 LDAP 속성을 지정합니다. 기본적으로 Access Manager 는 사용자 항목이 uid 속성에 의해 식별된다고 가정합니다. Directory Server 가 다른 속성 (예 : givenname) 을 사용할 경우 이 필드에 속성 이름을 지정합니다.

주 사용자 검색 필터는 검색 필터 속성과 사용자 프로필 검색 시 사용되는 LDAP 속성을 결합한 것이 됩니다.

인증될 사용자 검색 시 사용되는 LDAP 속성

이 필드는 인증될 사용자에 대한 검색 필터를 구성하는 데 사용되는 속성을 나열하며 사용자가 사용자 항목의 여러 속성으로 인증될 수 있게 합니다. 예를 들어, 이 필드를 uid, employeenumber 및 mail 로 설정한 경우 이러한 이름 중 하나로 사용자가 인증될 수 있습니다.

사용자 검색 필터

이 필드는 사용자 검색을 시작할 DN 필드에서 사용자를 찾는 데 사용될 속성을 지정하며 사용자 항목 이름 지정 속성과 함께 작동합니다. 기본값은 없습니다. 유효한 모든 사용자 항목 속성이 인식됩니다.

검색 범위

이 메뉴는 일치하는 사용자 프로필을 검색할 Directory Server 의 수준 수를 나타냅니다. 검색은 [299 페이지의 " 사용자 검색을 시작할 DN"](#) 속성에 지정된 노드에서 시작됩니다. 기본값은 SUBTREE 입니다. 다음 항목 중 하나를 목록에서 선택할 수 있습니다.

- 객체 - 지정된 노드만 검색합니다.

- 한 수준 - 지정된 노드 수준과 한 수준 아래에서 검색합니다.
- 하위 트리 - 지정된 노드와 그 아래 수준에 있는 모든 항목을 검색합니다.

주의 하위 조직의 사용자는 하위 조직이 비활성 상태인 경우에도 로그인할 수 있습니다. 이렇게 하지 못하도록 하려면 검색 범위와 기본 DN 이 해당 사용자가 속하는 특정 조직으로 설정해야 합니다.

SSL 이 LDAP 서버에 액세스 가능

이 옵션은 주 및 보조 LDAP 서버 및 포트 필드에 지정된 Directory Server 에 대한 SSL 액세스를 사용 가능하게 합니다. 기본적으로 이 옵션은 사용 불가능하므로 Directory Server 에 액세스하는 데 SSL 프로토콜이 사용되지 않습니다. 그러나 이 속성이 사용 가능한 경우 비 SSL 서버에 바인드할 수 있습니다.

LDAP 서버가 SSL 을 사용할 수 있는 상태에서 실행 중 (LDAPS) 이면, AM 이 LDAPS 프로토콜을 통해 디렉토리 서버에 연결될 수 있도록 Access Manager 가 적절한 SSL 로 신뢰된 인증서로 구성되었는지 확인해야만 합니다.

인증할 사용자 DN 반환

Access Manager 디렉토리가 LDAP 용으로 구성된 디렉토리와 동일한 경우 이 옵션을 사용 가능하게 할 수 있습니다. 이 옵션을 사용 가능하게 한 경우 LDAP 인증 모듈은 userId 대신 DN 을 반환할 수 있으며 검색이 필요하지 않습니다. 일반적으로 인증 모듈은 userId 만 반환하며 인증 서비스는 로컬 Access Manager LDAP 에서 사용자를 검색합니다. 외부 LDAP 디렉토리가 사용될 경우 일반적으로 이 옵션은 사용 가능하지 않습니다.

LDAP 서버 확인 간격

이 속성은 LDAP 서버 파일백에 사용됩니다. 이 속성은 LDAP 주 서버가 실행 중인지 확인하기 전에 스레드가 "일시 정지" 되는 시간 (분) 을 정의합니다.

사용자 작성 속성 목록

이 속성은 LDAP 서버가 외부 LDAP 서버로 구성된 경우에 LDAP 인증 모듈에서 사용됩니다. 이 속성은 로컬 Directory Server 와 외부 Directory Server 간의 속성 매핑을 포함합니다. 이 속성의 형식은 다음과 같습니다.

```
attr1|externalattr1
```

```
attr2|externalattr2
```

이 속성을 채우면 외부 Directory Server 에서 외부 속성 값을 읽은 다음 내부 Directory Server 속성 값을 설정합니다. 외부 속성 값은 **사용자 프로필** 속성 (핵심 인증 모듈에 있음) 이 "동적으로 작성" 으로 설정되고 사용자가 로컬 Directory Server 인스턴스에 없는 경우에만 내부 속성에 설정됩니다. 새로 작성된 사용자는 사용자 작성 속성 목록에 지정된 대로 매핑되는 외부 속성 값이 있는 내부 속성 값을 포함합니다.

인증 수준

인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 이 값은 인증을 어느 정도 신뢰할 수 있는지 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다. 기본값은 0 입니다.

주

지정된 인증 수준이 없을 경우 SSO 토큰은 핵심 인증 속성인 기본 인증 수준에 지정된 값을 저장합니다. 자세한 내용은 [288 페이지의 "기본 인증 수준"](#) 을 참조하십시오. 2005Q1 릴리스에서는 이 기능이 제대로 수행되지 않지만 이전 릴리스에서는 제대로 수행됩니다.

구성원 인증 속성

구성원 인증 속성은 조직 속성입니다. 서비스 구성에서 이러한 속성에 적용되는 값이 구성원 인증 템플릿의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플릿을 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 하위 트리에 있는 항목은 조직 속성을 상속하지 않습니다. 구성원 인증 속성은 다음과 같습니다.

- 304 페이지의 " 최소 비밀번호 길이 "
- 304 페이지의 " 기본 사용자 역할 "
- 304 페이지의 " 등록 후 사용자 상태 "
- 304 페이지의 " 주 LDAP 서버 "
- 305 페이지의 " 보조 LDAP 서버 "
- 305 페이지의 " 사용자 검색을 시작할 DN "
- 306 페이지의 " 루트 사용자 바인드용 DN "
- 306 페이지의 " 루트 사용자 바인드용 비밀번호 "
- 306 페이지의 " 루트 사용자 바인드용 비밀번호 (확인) "
- 306 페이지의 " 사용자 프로필 검색 시 사용되는 LDAP 속성 "
- 306 페이지의 " 인증될 사용자 검색 시 사용되는 LDAP 속성 "
- 306 페이지의 " 사용자 검색 필터 "
- 307 페이지의 " 검색 범위 "
- 307 페이지의 " SSL 이 LDAP 서버에 액세스 가능 "
- 307 페이지의 " 인증할 사용자 DN 반환 "
- 308 페이지의 " 인증 수준 "

최소 비밀번호 길이

이 필드는 자가 등록 동안 비밀번호 집합에 필요한 최소 문자 수를 지정합니다. 기본값은 8입니다.

이 값이 변경되면 다음 파일의 등록 및 오류 텍스트에서도 값을 변경해야 합니다.

```
AcessManager-base/locale/amAuthMembership.properties (PasswdMinChars  
entry)
```

기본 사용자 역할

이 필드는 자가 등록을 통해 프로필이 만들어지는 새 사용자에게 할당되는 역할을 지정합니다. 기본값은 없습니다. 관리자는 새 사용자에게 할당할 역할의 DN을 지정해야 합니다.

주 지정된 역할은 인증이 구성되고 있는 조직 아래에 있어야 합니다. 사용자에게 할당될 수 있는 역할만 자동 등록 중에 추가됩니다. 다른 DN은 모두 무시됩니다. 역할은 Access Manager 역할 또는 LDAP 역할 중 하나일 수 있지만 필터링된 역할은 허용되지 않습니다.

등록 후 사용자 상태

이 메뉴는 자가 등록한 사용자가 서비스를 즉시 사용할 수 있는지 여부를 지정합니다. 기본값은 Active이며 이 경우 새 사용자가 서비스를 사용할 수 있습니다. 관리자는 Inactive를 선택하여 새 사용자가 서비스를 사용할 수 없게 만들 수 있습니다.

주 LDAP 서버

이 필드는 Access Manager 설치 도중 지정된 주 LDAP 서버의 호스트 이름과 포트 번호를 지정합니다. 이 LDAP 서버는 LDAP 인증을 위해 연결되는 첫 번째 서버입니다. 형식은 hostname:port입니다. (포트 번호가 없을 경우 포트 번호를 389라고 가정합니다.)

Access Manager 를 여러 도메인으로 배포한 경우 Access Manager 의 특정 인스턴스와 Directory Server 의 특정 인스턴스 간의 통신 링크를 다음 형식으로 지정할 수 있습니다 (여러 항목에서 로컬 서버 이름을 접두어로 사용해야 함).

```
local_servername|server:port local_servername2|server:port ...
```

예를 들어 , Access Manager 의 서로 다른 인스턴스 (L1-machine1-DS 및 L2-machine2-DS) 와 통신하는 두 Access Manager 를 서로 다른 위치 (L1-machine1-IS 및 L2-machine2-IS) 에 배포한 경우 형식은 다음과 같습니다 .

```
L1-machine1-IS.example.com|L1-machine1-DS.example.com:389  
L2-machine2-IS.example.com|L2-machine2-DS.example.com:389
```

보조 LDAP 서버

이 필드는 Access Manager 플랫폼에 사용할 수 있는 보조 LDAP 서버의 호스트 이름과 포트 번호를 지정합니다 . 주 LDAP 서버가 인증 요청에 응답하지 않을 경우 이 서버에 연결됩니다 . 주 서버가 실행 중인 경우 Access Manager 는 주 서버로 다시 전환합니다 . 형식은 hostname:port 입니다 . 여러 항목이 있을 경우 로컬 서버 이름을 접두어로 지정해야 합니다 .

주의	Access Manager 엔터프라이즈와 떨어져 있는 원격 Directory Server 에서 사용자를 인증하는 경우 주 LDAP 서버 포트와 보조 LDAP 서버 포트 모두에 값이 있어야 합니다 . 하나의 Directory Server 위치에 대한 값을 두 필드 모두에 사용할 수 있습니다 .
-----------	---

사용자 검색을 시작할 DN

이 필드는 사용자 검색이 시작되는 노드의 DN 을 지정합니다 . (성능상의 이유 때문에 이 DN 은 가능한 구체적이어야 합니다 .) 기본값은 디렉토리 트리의 루트입니다 . 유효한 모든 DN 이 인식됩니다 . **검색 범위** 속성에서 객체를 선택한 경우에는 DN 에서 프로필이 있는 수준보다 한 수준 위를 지정해야 합니다 .

여러 항목을 사용할 경우 로컬 서버 이름을 접두어로 지정해야 합니다 . 형식은 다음과 같습니다 .

```
servername|search dn
```

여러 항목이 있는 경우

```
servername1|search dn servername2|search dn servername3|search dn...
```

동일한 검색에서 여러 사용자가 발견될 경우 인증은 실패합니다 .

루트 사용자 바인드용 DN

이 필드는 관리자로서 주 LDAP 서버 및 포트 필드에 지정된 Directory Server 에 바인딩하는 데 사용되는 사용자의 DN 을 지정합니다. 사용자 로그인 아이디에 기초하여 일치하는 사용자 DN 을 검색하려면 인증 서비스가 이 DN 으로 바인드되어야 합니다. 기본값은 amldapuser 입니다. 유효한 모든 DN 이 인식됩니다.

루트 사용자 바인드용 비밀번호

이 필드는 루트 사용자 바인드용 DN 필드에 지정된 관리자 프로필의 비밀번호를 포함합니다. 기본값은 없습니다. 관리자의 유효한 LDAP 비밀번호만 인식됩니다.

루트 사용자 바인드용 비밀번호 (확인)

비밀번호를 확인합니다.

사용자 프로필 검색 시 사용되는 LDAP 속성

이 필드는 사용자 항목의 이름 지정 규칙에 사용되는 속성을 지정합니다. 기본적으로 Access Manager 는 사용자 항목이 uid 속성에 의해 식별된다고 가정합니다. Directory Server 가 다른 속성 (예 : givenname) 을 사용할 경우 이 필드에 속성 이름을 지정합니다.

인증될 사용자 검색 시 사용되는 LDAP 속성

이 필드는 인증될 사용자에 대한 검색 필터를 구성하는 데 사용되는 속성을 나열하며 사용자가 사용자 항목의 여러 속성으로 인증될 수 있게 합니다. 예를 들어, 이 필드를 uid, employeenumber 및 mail 로 설정한 경우 이러한 이름 중 하나로 사용자가 인증될 수 있습니다.

사용자 검색 필터

이 필드는 사용자 검색을 시작할 DN 필드에서 사용자를 찾는 데 사용될 속성을 지정하며 아이디 지정 속성과 함께 작동합니다. 기본값은 없습니다. 유효한 모든 사용자 항목 속성이 인식됩니다.

검색 범위

이 메뉴는 일치하는 사용자 프로필을 검색할 Directory Server 의 수준 수를 나타냅니다. 검색은 305 페이지의 " 사용자 검색을 시작할 DN" 속성에 지정된 노드에서 시작됩니다. 기본값은 SUBTREE 입니다. 다음 항목 중 하나를 목록에서 선택할 수 있습니다.

- 객체 - 지정된 노드만 검색합니다.
- 한 수준 - 지정된 노드 수준과 한 수준 아래에서 검색합니다.
- 하위 트리 - 지정된 노드와 그 아래 수준에 있는 모든 항목을 검색합니다.

SSL 이 LDAP 서버에 액세스 가능

이 옵션은 주 LDAP 서버 및 보조 LDAP 서버 그리고 포트 필드에 지정된 Directory Server 에 대한 SSL 액세스를 사용 가능하게 합니다. 기본적으로 이 상자는 선택되어 있지 않으므로 Directory Server 에 액세스하는 데 SSL 프로토콜이 사용되지 않습니다.

LDAP 서버가 SSL 을 사용할 수 있는 상태에서 실행 중 (LDAPS) 이면 , AM 이 LDAPS 프로토콜을 통해 디렉토리 서버에 연결될 수 있도록 Access Manager 가 적절한 SSL 로 신뢰된 인증서로 구성되었는지 확인해야만 합니다 .

인증할 사용자 DN 반환

Access Manager 디렉토리가 LDAP 용으로 구성된 디렉토리인 경우 이 옵션을 사용 가능하게 할 수 있습니다. 이 옵션을 사용 가능하게 한 경우 LDAP 인증 모듈은 userId 대신 DN 을 반환할 수 있으며 검색이 필요하지 않습니다. 일반적으로 인증 모듈은 userId 만 반환하며 인증 서비스는 로컬 Access Manager LDAP 에서 사용자를 검색합니다. 외부 LDAP 디렉토리가 사용될 경우 일반적으로 이 옵션은 사용 가능하지 않습니다.

인증 수준

인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 이 값은 인증을 어느 정도 신뢰할 수 있는지 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다. 기본값은 0입니다.

주

지정된 인증 수준이 없을 경우 SSO 토큰은 핵심 인증 속성인 기본 인증 수준에 지정된 값을 저장합니다. 자세한 내용은 [288 페이지의 "기본 인증 수준"](#)을 참조하십시오. 2005Q1 릴리스에서는 이 기능이 제대로 수행되지 않지만 이전 릴리스에서는 제대로 수행됩니다.

MSISDN 인증 속성

MSISDN 인증 속성은 조직 속성입니다. 서비스 구성에서 이러한 속성에 적용되는 값이 MSISDN 인증 템플릿의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플릿을 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 항목은 조직 속성을 상속하지 않습니다. MSISDN 인증 속성은 다음과 같습니다.

신뢰할 수 있는 게이트웨이 IP 주소

이 속성은 MSISDN 모듈에 액세스할 수 있는 신뢰할 수 있는 클라이언트의 IP 주소 목록을 지정합니다. 입력 필드에 주소 (예 :123.456.123.111) 를 입력하고 추가를 눌러, 모든 클라이언트의 IP 주소를 MSISDN 모듈에 액세스할 수 있도록 설정할 수 있습니다. 기본적으로 이 목록은 비어 있습니다. 이 속성이 비어 있으면 모든 클라이언트가 MSISDN 모듈에 액세스할 수 있습니다. none 으로 지정하면 어떤 클라이언트도 MSISDN 모듈에 액세스할 수 없습니다.

MSISDN 번호 인수

이 필드에서는 MSISDN 번호에 대한 요청 헤더 또는 쿠키 헤더에서 어떤 매개 변수를 검색할 것인지 식별하는 매개 변수 이름 목록을 지정합니다. 예를 들어, x-Cookie-Param, AM_NUMBER 및 COOKIE-ID 를 지정하면 MSISDN 인증 서비스는 MSISDN 번호에 대해 해당 매개 변수를 검색합니다.

LDAP 서버 및 포트

이 필드에서는 MSISDN 번호를 가진 사용자에게 대한 검색을 수행할 대상이 되는 Directory Server 의 호스트 이름 및 포트 번호를 지정합니다. 형식은 `hostname:port` 입니다. 포트 번호가 없을 경우 포트 번호를 389 라고 가정합니다.

Access Manager 를 여러 도메인으로 배포한 경우 Access Manager 의 특정 인스턴스와 Directory Server 의 특정 인스턴스 간의 통신 링크를 다음 형식으로 지정할 수 있습니다 (여러 항목에서 로컬 서버 이름을 접두어로 사용해야 함).

```
local_servername|server:port local_servername2|server2:port2 ...
```

예를 들어, Directory Server 의 서로 다른 인스턴스 (L1-machine1-DS 및 L2-machine2-DS) 와 통신하는 두 Access Manager 를 서로 다른 위치 (L1-machine1-IS 및 L2-machine2-IS) 에 배포한 경우 형식은 다음과 같습니다.

```
L1-machine1-IS.example.com|L1-machine1-DS.example.com:389  
L2-machine2-IS.example.com|L2-machine2-DS.example.com:389
```

LDAP 시작 검색 DN

이 필드는 사용자의 MSISDN 번호에 대한 검색을 시작할 노드의 DN 을 지정합니다. 기본값은 없습니다. 이 필드는 모든 유효한 DN 을 인식합니다. 여러 항목이 있을 경우 로컬 서버 이름을 접두어로 지정해야 합니다. 형식은 다음과 같습니다.

```
servername|search dn
```

여러 항목이 있는 경우

```
servername1|search dn servername2|search dn servername3|search dn...
```

동일한 검색에서 여러 사용자가 발견될 경우 인증은 실패합니다.

LDAP 검색에 사용할 속성

이 필드에서는 특정 사용자에게 대해 검색할 MSISDN 번호를 포함하고 있는 사용자 프로필 내의 속성 이름을 지정합니다. 기본값은 `sunIdentityMSISDNNumber` 입니다. 사용자 프로필의 다른 속성이 동일한 MSISDN 번호를 포함하고 있는지 확실하지 않으면 이 값을 변경하지 마십시오.

LDAP 서버 기본 사용자

이 속성은 LDAP 바인드 DN 을 지정하여 Directory Server 내의 MSISDN 검색을 허용하도록 합니다. 기본 바인드 DN 은 `cn=amldapuser,ou=DSAME Users,dc=sun,dc=com` 입니다.

LDAP 서버 기본 비밀번호

이 속성은 LDAP 서버 기본 사용자에서 정의한 대로 바인드 DN 에 대한 LDAP 바인드 비밀번호를 지정합니다.

LDAP 서버 기본 비밀번호 (확인)

비밀번호를 확인합니다.

LDAP 액세스에 대해 SSL 설정

이 옵션은 LDAP 서버 및 포트 속성에서 지정된 Directory Server 에 대한 SSL 액세스를 사용 가능하게 합니다. 기본적으로 이 옵션은 사용 불가능하므로 Directory Server 에 액세스하는 데 SSL 프로토콜이 사용되지 않습니다. 그러나 이 속성이 사용 가능한 경우 비 SSL 서버에 바인드할 수 있습니다.

MSISDN 헤더 검색 속성

이 속성은 MSISDN 번호에 대한 요청을 검색할 때 사용할 헤더를 지정합니다. 지원되는 값은 다음과 같습니다.

- SearchCookieHeader - 쿠키에서 검색합니다.
- SearchRequestHeader - 요청 헤더에서 검색합니다.
- SearchRequestParameter - 요청 매개 변수에서 검색합니다.

기본적으로 모든 옵션이 선택되어 있습니다.

인증 수준

인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 이 값은 인증을 어느 정도 신뢰할 수 있는지 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다. 기본값은 0입니다.

주

지정된 인증 수준이 없을 경우 SSO 토큰은 핵심 인증 속성인 기본 인증 수준에 지정된 값을 저장합니다. 자세한 내용은 [288페이지의 "기본 인증 수준"](#)을 참조하십시오.

Windows NT 인증 속성

Windows NT 인증 속성은 조직 속성입니다. 서비스 구성에서 이러한 속성에 적용되는 값이 Windows NT 인증 템플릿의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플릿을 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 하위 트리에 있는 항목은 조직 속성을 상속하지 않습니다.

Windows NT 인증 모듈을 활성화하려면 Samba Client 2.2.2 를 다운로드하여 다음 디렉토리에 설치해야 합니다.

```
AccessManager-base/SUNWam/bin
```

Samba Client 는 별도의 Windows NT/2000 Server 를 필요로 하지 않고 Windows 시스템과 UNIX 시스템을 블렌딩하는 파일 및 인쇄 서버입니다. 자세한 내용을 보거나 Samba Client 를 다운로드하려면

<http://www.sun.com/software/download/products/3e3af224.html> 에 액세스하십시오.

Red Hat Linux 는 Samba 클라이언트와 함께 제공됩니다. 이 클라이언트는 다음 디렉토리에 있습니다.

```
/usr/bin
```

Linux 용 Windows NT 인증 서비스를 사용하여 인증하려면 다음 Access Manager 디렉토리에 클라이언트 이진을 복사합니다.

```
AccessManager-base/identity/bin
```

Windows NT 인증 속성은 다음과 같습니다.

- [314 페이지의 "Windows NT 인증 도메인 "](#)
- [314 페이지의 "Windows NT 인증 호스트 "](#)
- [314 페이지의 "Windows NT Samba 구성 파일 이름 "](#)

Windows NT 인증 도메인

이 속성은 사용자가 속하는 도메인 이름을 정의합니다.

Windows NT 인증 호스트

이 속성은 Windows NT 인증 호스트 이름을 정의합니다. 호스트 이름은 정규화된 도메인 이름 (FQDN) 이 아니라 netBIOS 이름이어야 합니다. 기본적으로 FQDN 의 첫 번째 부분은 netBIOS 이름입니다.

DHCP(동적 호스트 구성 프로토콜) 가 사용될 경우 Windows 2000 시스템에서 HOSTS 파일에 적절한 항목을 입력합니다.

netBIOS 이름에 기초하여 이름 확인이 수행됩니다. netBIOS 이름 확인을 제공하는 서버넷에 서버가 없을 경우 매핑을 하드 코드해야 합니다.

예를 들어, 호스트 이름은 example1.company1.com 이 아니라 example1 이어야 합니다.

Windows NT Samba 구성 파일 이름

이 속성은 smbclient 명령에서 Samba 구성 파일 이름을 정의하고 -s 옵션을 지원합니다. 값은 Samba 구성 파일이 있는 전체 디렉토리 경로여야 합니다. 예를 들면 다음과 같습니다.

```
/etc/opt/SUNWam/config/smb.conf
```

인증 수준

인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 이 값은 인증을 어느 정도 신뢰할 수 있는지 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다. 기본값은 0 입니다.

주

지정된 인증 수준이 없을 경우 SSO 토큰은 핵심 인증 속성인 기본 인증 수준에 지정된 값을 저장합니다. 자세한 내용은 [288 페이지의 "기본 인증 수준"](#)을 참조하십시오. 2005Q1 릴리스에서는 이 기능이 제대로 수행되지 않지만 이전 릴리스에서는 제대로 수행됩니다.

RADIUS 인증 속성

RADIUS 인증 속성은 조직 속성입니다. 서비스 구성에서 이러한 속성에 적용된 값이 RADIUS 인증 템플릿의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플릿을 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 항목은 조직 속성을 상속하지 않습니다. RADIUS 인증 속성은 다음과 같습니다.

- [317 페이지의 "RADIUS 서버 1"](#)
- [318 페이지의 "RADIUS 서버 2"](#)
- [318 페이지의 "RADIUS 공유 비밀"](#)
- [318 페이지의 "RADIUS 공유 비밀 \(확인\)"](#)
- [318 페이지의 "RADIUS 서버 포트"](#)
- [318 페이지의 "시간 초과"](#)
- [318 페이지의 "인증 수준"](#)

RADIUS 서버 1

이 필드는 주 RADIUS 서버의 IP 주소나 정규화된 호스트 이름을 표시합니다. 기본 IP 주소는 127.0.0.1입니다. 이 필드는 유효한 모든 IP 주소나 호스트 이름을 인식합니다. 여러 항목이 있는 경우 다음 구문과 같이 로컬 서버 이름을 사용하여 접두어를 지정해야 합니다.

```
local_servername|ip_address local_servername2|ip_address ...
```

RADIUS 서버 2

이 필드는 보조 RADIUS 서버의 IP 주소나 정규화된 도메인 이름 (FQDN) 을 표시합니다. 이 서버는 주 서버에 연결할 수 없는 경우 연결되는 페일오버 서버입니다. 기본 IP 주소는 127.0.0.1 입니다. 여러 항목이 있는 경우 다음 구문과 같이 로컬 서버 이름을 사용하여 접두어를 지정해야 합니다.

```
local_servername|ip_address local_servername2|ip_address ...
```

RADIUS 공유 비밀

이 필드는 RADIUS 인증을 위한 공유 비밀을 가집니다. 공유 비밀은 적절히 선택된 비밀번호와 동일한 자격을 가져야 합니다. 이 필드에는 기본값이 없습니다.

RADIUS 공유 비밀 (확인)

RADIUS 인증을 위한 공유 비밀을 확인합니다.

RADIUS 서버 포트

이 필드는 RADIUS 서버가 수신하는 포트를 지정합니다. 기본값은 1645 입니다.

시간 초과

이 필드는 RADIUS 서버의 응답을 대기하는 시간 간격 (초) 을 지정합니다. 기본값은 3 초입니다. 이 필드는 시간 초과를 지정하는 모든 숫자를 초 단위로 인식합니다.

인증 수준

인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 이 값은 인증을 어느 정도 신뢰할 수 있는지 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하

지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다. 기본값은 0입니다. 2005Q1 릴리스에서는 이 기능이 제대로 수행되지 않지만 이전 릴리스에서는 제대로 수행됩니다.

SafeWord 인증 속성

SafeWord 인증 속성은 조직 속성입니다. 서비스 구성에서 이러한 속성에 적용된 값이 SafeWord 인증 템플릿의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플릿을 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 하위 트리에 있는 항목은 조직 속성을 상속하지 않습니다.

이 서비스를 사용하면 Secure Computing 의 SafeWord 또는 SafeWord PremierAccess 인증 서버를 사용하여 사용자를 인증할 수 있습니다. SafeWord 인증 속성은 다음과 같습니다.

- [322 페이지의 "SafeWord 서버 "](#)
- [322 페이지의 "SafeWord 서버 검증 파일 디렉토리 "](#)
- [322 페이지의 "SafeWord 로깅 사용 "](#)
- [322 페이지의 "SafeWord 로깅 수준 "](#)
- [322 페이지의 "SafeWord 로그 파일 "](#)
- [323 페이지의 "SafeWord 인증 연결 시간 초과 "](#)
- [323 페이지의 "SafeWord 클라이언트 유형 "](#)
- [323 페이지의 "SafeWord eassp 버전 "](#)
- [323 페이지의 "SafeWord 최소 인증 강도 "](#)
- [324 페이지의 " 인증 수준 "](#)

SafeWord 서버

이 필드는 SafeWord 또는 SafeWord PremiereAccess 서버 이름과 포트를 지정합니다. 기본 포트 번호는 SafeWord 서버의 경우 7482 이고 SafeWord PremierAccess 서버의 경우 5030 입니다.

SafeWord 서버 검증 파일 디렉토리

이 필드는 SafeWord 클라이언트 라이브러리가 확인 파일을 두는 디렉토리를 지정합니다. 기본값은 다음과 같습니다.

```
/var/opt/SUNWam/auth/safeword/serverVerification
```

이 필드에 다른 디렉토리가 지정된 경우 SafeWord 인증을 시도하기 전에 해당 디렉토리가 존재해야 합니다.

SafeWord 로깅 사용

이 속성을 선택하면 SafeWord 로깅을 사용할 수 있습니다. 기본적으로 SafeWord 로깅이 사용됩니다.

SafeWord 로깅 수준

이 필드에서는 SafeWord 로깅 수준을 지정합니다. 풀다운 메뉴에서 수준을 선택합니다. 수준은 DEBUG, ERROR, INFO 및 NONE 입니다.

SafeWord 로그 파일

이 속성은 SafeWord 클라이언트 로깅의 디렉토리 경로와 로그 파일 이름을 지정합니다. 기본 경로는 다음과 같습니다.

```
/var/opt/SUNWam/auth/safeword/safe.log
```

다른 경로나 파일 이름을 지정할 경우 SafeWord 인증을 시도하기 전에 해당 경로나 파일 이름이 존재해야 합니다.

여러 조직이 SafeWord 인증을 사용하도록 구성되어 있고 다른 SafeWord 서버가 사용될 경우에는 다른 경로를 지정해야 합니다. 그렇지 않을 경우 SafeWord 인증이 수행되는 첫 번째 조직만 작동합니다. 마찬가지로 조직에서 SafeWord 서버를 변경할 경우 새로 구성한 SafeWord 서버에 대한 인증이 수행되기 전에 지정된 디렉토리의 swec.dat 파일을 삭제해야 합니다.

SafeWord 인증 연결 시간 초과

이 속성은 SafeWord 클라이언트 (Access Manager) 와 SafeWord 서버 간의 시간 초과 기간 (초 단위) 을 정의합니다. 기본값은 120 초입니다.

SafeWord 클라이언트 유형

이 속성은 SafeWord 서버가 다른 클라이언트와 통신하기 위해 사용하는 클라이언트 유형 (모바일 클라이언트, VPN, 비밀번호, 시도 / 응답 등) 을 정의합니다.

SafeWord eassp 버전

이 속성은 EASSP(Extended Authentication and Single Sign-on Protocol) 버전을 지정합니다. 이 필드에서는 표준 (101) 또는 Premier Access(201) 프로토콜 버전을 사용합니다.

SafeWord 최소 인증 강도

이 속성은 클라이언트 /SafeWord 서버 인증에 필요한 최소 인증 강도를 정의합니다. 각 클라이언트 유형은 다른 인증 값을 가지며 값이 클수록 인증 강도가 강해집니다. 20 이 가장 큰 값이며 0 이 가장 작은 값입니다.

인증 수준

인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 이 값은 인증을 어느 정도 신뢰할 수 있는지 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다. 기본값은 0입니다.

주

지정된 인증 수준이 없을 경우 SSO 토큰은 핵심 인증 속성인 기본 인증 수준에 지정된 값을 저장합니다. 자세한 내용은 [288 페이지의 "기본 인증 수준"](#)을 참조하십시오. 2005Q1 릴리스에서는 이 기능이 제대로 수행되지 않지만 이전 릴리스에서는 제대로 수행됩니다.

SAML 인증 속성

SAML 인증 속성은 조직 속성입니다. 서비스 구성에서 이러한 속성에 적용된 값이 SAML 인증 템플릿의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플릿을 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 항목은 조직 속성을 상속하지 않습니다.

SAML 인증 속성은 다음과 같습니다.

인증 수준

인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 이 값은 인증을 어느 정도 신뢰할 수 있는지 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다. 기본값은 0입니다.

주

지정된 인증 수준이 없을 경우 SSO 토큰은 핵심 인증 속성인 기본 인증 수준에 지정된 값을 저장합니다. 자세한 내용은 [288 페이지의 "기본 인증 수준"](#)을 참조하십시오. 2005Q1 릴리스에서는 이 기능이 제대로 수행되지 않지만 이전 릴리스에서는 제대로 수행됩니다.

SecurID 인증 속성

SecurID 인증 속성은 조직 속성입니다. 서비스 구성에서 이러한 속성에 적용된 값이 SecurID 인증 템플릿의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플릿을 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 하위 트리에 있는 항목은 조직 속성을 상속하지 않습니다.

이 서비스는 RSA의 ACE/ 서버 인증 서버를 사용하여 사용자를 인증할 수 있게 합니다. SecurID 인증 속성은 다음과 같습니다.

- [327 페이지의 "SecurID ACE/ 서버 구성 경로"](#)
- [328 페이지의 "SecurID 도우미 구성 포트"](#)
- [328 페이지의 "SecurID 도우미 인증 포트"](#)
- [328 페이지의 "인증 수준"](#)
-

주

이 릴리스의 Access Manager에서는 Linux 또는 Solaris x86 플랫폼에 대해 SecurID 인증 모듈을 사용할 수 없으며, 이 두 플랫폼에서 등록, 구성 및 사용해서는 안됩니다. SecurID 인증 모듈은 Solaris에서만 사용할 수 있습니다.

SecurID ACE/ 서버 구성 경로

이 필드는 SecurID ACE/ 서버 `sdconf.rec` 파일이 위치하는 디렉토리를 지정합니다. 기본값은 다음과 같습니다.

```
/opt/ace/data
```

이 필드에 다른 디렉토리를 지정할 경우 SecurID 인증을 시도하기 전에 해당 디렉토리가 존재해야 합니다.

SecurID 도우미 구성 포트

이 속성은 SecurID 도우미가 시작될 때 SecurID 도우미 인증 포트 속성에 포함된 구성 정보를 '수신' 하는 포트를 지정합니다. 기본값은 58943입니다.

이 속성이 변경될 경우 `AMConfig.properties` 파일에서 `securidHelper.ports` 항목을 변경하고 Access Manager 를 다시 시작해야 합니다. `AMConfig.properties` 파일의 항목은 SecurID 도우미 인스턴스에 대한 포트 목록입니다. 각 포트는 공백으로 구분되어 있습니다. 다른 `sdconf.rec` 파일을 가진 다른 ACE/ 서버와 통신하는 각 조직에 대해 별도의 SecurID 도우미가 있어야 합니다.

SecurID 도우미 인증 포트

이 속성은 조직의 SecurID 인증 모듈이 SecurID 도우미 인스턴스를 구성하여 인증 요청을 '수신' 하는 포트를 지정합니다. 이 포트 번호는 SecurID 또는 Unix 인증을 사용하는 모든 조직에서 고유해야 합니다. 기본 포트는 57943입니다.

인증 수준

인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 이 값은 인증을 어느 정도 신뢰할 수 있는지 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다. 기본값은 0입니다.

주 지정된 인증 수준이 없을 경우 SSO 토큰은 핵심 인증 속성인 기본 인증 수준에 지정된 값을 저장합니다. 자세한 내용은 [288 페이지의 "기본 인증 수준"](#)을 참조하십시오. 2005Q1 릴리스에서는 이 기능이 제대로 수행되지 않지만 이전 릴리스에서는 제대로 수행됩니다.

Unix 인증 속성

Unix 인증 서비스는 전역 및 조직 속성으로 구성됩니다. 전역 변수에 적용되는 값은 Sun Java System Access Manager 구성에서 적용되며 구성된 모든 조직이 상속합니다. 전역 속성의 목표가 Access Manager 응용 프로그램을 사용자 정의하는 것이므로 이러한 값은 역할이나 조직에 직접 적용할 수 없습니다. 조직 속성에 적용되는 값은 구성된 각 조직에 대해 기본값이며 서비스가 조직에 등록될 때 변경할 수 있습니다. 조직의 항목은 조직 속성을 상속하지 않습니다. Unix 인증 속성은 다음과 같이 구분됩니다.

- [329 페이지의 "전역 속성"](#)
- [330 페이지의 "조직 속성"](#)

주 임의의 Unix 인증 속성이 수정된 경우 Access Manager 와 amunixd 도우미를 모두 다시 시작해야 합니다.

전역 속성

Unix 인증 서비스의 전역 속성은 다음과 같습니다.

- [330 페이지의 "Unix 도우미 구성 포트"](#)
- [330 페이지의 "Unix 도우미 인증 포트"](#)
- [330 페이지의 "Unix 도우미 시간 초과"](#)
- [330 페이지의 "Unix 도우미 스레드"](#)

Unix 도우미 구성 포트

이 속성은 Unix 도우미가 시작될 때 [Unix 도우미 인증 포트](#), [Unix 도우미 시간 초과](#) 및 [Unix 도우미 스레드](#) 속성에 포함된 구성 정보를 '수신' 하는 포트를 지정합니다. 기본값은 58946 입니다.

이 속성이 변경될 경우 `AMConfig.properties` 파일에서 `unixHelper.port` 항목을 변경하고 Access Manager 를 다시 시작해야 합니다.

Unix 도우미 인증 포트

이 속성은 구성 후 Unix 도우미가 인증 요청을 '수신' 하는 포트를 지정합니다. 기본 포트는 57946 입니다.

Unix 도우미 시간 초과

이 속성은 사용자가 인증을 완료해야 하는 시간 (분) 을 지정합니다. 할당된 시간을 초과할 경우 인증이 자동으로 실패합니다. 기본 시간은 3 분으로 설정됩니다.

Unix 도우미 스레드

이 속성은 허용되는 동시 Unix 인증 세션의 최대 개수를 지정합니다. 특정 시점에 최대값에 도달하면 세션이 해제될 때까지 후속 인증 시도가 허용되지 않습니다. 기본 값은 5 로 설정됩니다.

조직 속성

Unix 인증 서비스의 조직 속성은 다음과 같습니다.

인증 수준

인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 값 인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 이 값은 인증을 어느 정도 신뢰할 수 있는지 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을

사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다. 기본값은 0 입니다.

주

지정된 인증 수준이 없을 경우 SSO 토큰은 핵심 인증 속성인 기본 인증 수준에 지정된 값을 저장합니다. 자세한 내용은 [288 페이지의 "기본 인증 수준"](#) 을 참조하십시오. 2005Q1 릴리스에서는 이 기능이 제대로 수행되지 않지만 이전 릴리스에서는 제대로 수행됩니다.

조직 속성

Windows 데스크탑 SSO 인증 속성

Windows 데스크탑 SSO 인증 속성은 조직 속성입니다. 서비스 구성에서 이러한 속성에 적용되는 값이 Windows 데스크탑 SSO 인증 템플릿의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플릿을 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 하위 트리에 있는 항목은 조직 속성을 상속하지 않습니다.

이 인증 모듈에는 도메인 제어기로 실행되는 Windows 2000 서버에서 제공하는 커버로스 인증 서비스가 필요합니다.

Windows 데스크탑 SSO 인증 속성은 다음과 같습니다.

- 333 페이지의 " 서비스 기본 "
- 334 페이지의 " 키값 파일 이름 "
- 334 페이지의 " 커버로스 영역 "
- 334 페이지의 " 커버로스 서버 이름 "
- 334 페이지의 " 도메인 이름과 함께 기본 반환 "
- 334 페이지의 " 인증 수준 "

서비스 기본

이 속성은 인증에 사용되는 커버로스 기본을 지정합니다. 다음 형식을 사용합니다.

`HTTP/hostname.domainname@dc_domain_name`

hostname 및 *domainname* 은 Access Manager 인스턴스의 호스트 이름과 도메인 이름을 나타냅니다. *dc_domain_name* 은 Windows 2000 커버로스 서버 (도메인 제어기)가 상주하는 커버로스 도메인입니다. 이 이름은 Access Manager 의 도메인 이름과 다를 수 있습니다.

키텡 파일 이름

이 속성은 인증에 사용되는 커버로스 키텡 파일을 지정합니다. 다음 형식을 사용합니다 (반드시 따라야 하는 형식은 아님).

```
hostname.HTTP.keytab
```

hostname 은 Access Manager 인스턴스의 호스트 이름입니다.

커버로스 영역

이 속성은 커버로스 배포 센터 (도메인 제어기) 의 도메인 이름을 지정합니다. 구성에 따라 도메인 제어기의 도메인 이름은 Access Manager 도메인 이름과 다를 수 있습니다.

커버로스 서버 이름

이 속성은 커버로스 배포 센터 (도메인 제어기) 의 호스트 이름을 지정합니다. 도메인 제어기의 정규화된 도메인 이름 (FQDN) 을 입력해야 합니다.

도메인 이름과 함께 기본 반환

사용 가능하게 설정된 경우 이 속성은 Access Manager 가 인증 도중에 도메인 제어기의 도메인 이름과 함께 커버로스 기본을 자동으로 반환할 수 있게 합니다.

인증 수준

인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 이 값은 인증을 어느 정도 신뢰할 수 있는지 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다. 기본값은 0 입니다.

주

지정된 인증 수준이 없을 경우 SSO 토큰은 핵심 인증 속성인 기본 인증 수준에 지정된 값을 저장합니다. 자세한 내용은 [288 페이지의 "기본 인증 수준"](#) 을 참조하십시오. 2005Q1 릴리스에서는 이 기능이 제대로 수행되지 않지만 이전 릴리스에서는 제대로 수행됩니다.

인증 구성 서비스 속성

인증 구성 서비스 속성은 동적이며 조직 속성입니다. 이러한 속성은 조직, 서비스 또는 역할에 대해 정의할 수 있습니다. 조직 속성은 핵심 인증 모듈에 정의됩니다.

사용자에게 역할이 할당되거나 사용자가 조직에 할당될 경우 해당 사용자는 기본적으로 이러한 속성을 상속합니다. 인증 구성 속성은 다음과 같습니다.

- 337 페이지의 "인증 구성"
- 338 페이지의 "로그인 성공 URL"
- 338 페이지의 "로그인 실패 URL"
- 339 페이지의 "인증 사후 처리 클래스"

인증 구성

편집 링크를 누르면 인증 구성 인터페이스가 표시됩니다. 이 인터페이스를 사용하면 역할 기반 또는 조직 기반 인증을 위한 인증 모듈을 구성할 수 있습니다.

다음 표에는 인증 모듈 구성 옵션이 나열되어 있습니다.

모듈 이름	이 옵션을 사용하면 Access Manager 에서 사용할 수 있는 기본 인증 모듈 목록으로부터 모듈을 선택할 수 있습니다.
-------	--

플래그	<p>이 폴다운 메뉴를 사용하면 인증 모듈 요구 사항을 다음 중 하나로 지정할 수 있습니다.</p> <ul style="list-style-type: none"> 필수 - 인증 모듈이 성공적이어야 합니다. 성공 또는 실패한 경우 인증 모듈 목록의 그 다음 항목에 대해 인증이 계속 진행됩니다. 필요 - 인증 모듈이 성공적이어야 합니다. 성공한 경우 인증 모듈 목록의 그 다음 항목에 대해 인증이 계속됩니다. 실패한 경우 컨트롤이 응용 프로그램에 반환됩니다 (인증 모듈 목록의 그 다음 항목에 대해 인증이 진행되지 않음). 충분 - 인증 모듈이 반드시 성공적이지 않아도 됩니다. 성공한 경우 컨트롤이 즉시 응용 프로그램에 반환됩니다 (인증 모듈 목록의 그 다음 항목에 대해 인증이 진행되지 않음). 실패한 경우 목록의 그 다음 항목에 대해 인증이 계속됩니다. 옵션 - 인증 모듈이 반드시 성공적이지 않아도 됩니다. 성공 또는 실패한 경우 목록의 그 다음 항목에 대해 인증이 계속됩니다. <p>이러한 플래그는 플래그가 정의된 인증 모듈에 대한 적용 기준을 설정하며 필수가 가장 높고 옵션이 가장 낮은 단계입니다.</p> <p>예를 들어, 관리자가 필수 플래그로 LDAP 모듈을 정의하면 사용자의 인증서는 주어진 자원에 액세스하기 위해 LDAP 인증 요구 사항을 통과해야 합니다.</p> <p>여러 인증 모듈을 추가하고 각 모듈에 대해 플래그를 필수로 설정한 경우 사용자는 모든 인증 요구 사항을 통과해야만 액세스가 허가됩니다.</p> <p>플래그 정의에 대한 자세한 내용은 다음 위치에 있는 JAAS (Java Authentication and Authorization Service) 를 참조하십시오. http://java.sun.com/security/jaas/doc/module.html</p>
옵션	<p>키 = 값 쌍으로 모듈에 대한 추가 옵션을 허용합니다. 여러 옵션을 사용할 경우 공백으로 구분합니다.</p>

로그인 성공 URL

이 속성은 인증 성공 시 사용자가 리디렉션되는 URL 을 지정합니다.

로그인 실패 URL

이 속성은 인증 실패 시 사용자가 리디렉션되는 URL 을 지정합니다.

인증 사후 처리 클래스

이 속성은 로그인 성공 또는 실패 후에 인증 사후 처리를 사용자 정의하는 데 사용되는 Java 클래스의 이름을 정의합니다.

확인 수준 충돌

이 속성은 역할에만 적용됩니다. 충돌 해결 수준은 동일한 사용자를 포함할 수 있는 역할의 인증 구성 속성에 대한 우선 순위 수준을 설정합니다. 예를 들어, User1 이 Role1 및 Role2 에 할당된 경우 Role1 에 더 높은 우선 순위 수준을 정의할 수 있으며 이 경우 사용자가 인증을 시도할 때 Role1 이 성공 또는 실패 리디렉션과 인증 사후 처리에 대해 가장 높은 우선 순위를 갖게 됩니다.

클라이언트 검색 서비스 속성

클라이언트 검색 서비스 속성은 전역 속성입니다. 이러한 속성에 적용되는 값은 Access Manager 구성 전체에 걸쳐 적용되며 구성된 모든 조직이 상속합니다. 전역 속성의 목적은 Access Manager 응용 프로그램을 사용자 정의하는 것이므로 이러한 값을 역할이나 조직에 직접 적용할 수는 없습니다. 클라이언트 검색 속성은 다음과 같습니다.

- [341 페이지의 "클라이언트 유형"](#)
- [344 페이지의 "기본 클라이언트 유형"](#)
- [344 페이지의 "클라이언트 검색 클래스"](#)
- [344 페이지의 "클라이언트 검색 사용 가능"](#)

클라이언트 유형

클라이언트 유형을 검색하려면 Access Manager가 해당 식별 특징을 인식해야 합니다. 이러한 특징은 지원되는 모든 유형의 등록 정보를 클라이언트 데이터 형식으로 식별합니다. 이 속성을 사용하면 클라이언트 관리자 인터페이스를 통해 클라이언트 데이터를 수정할 수 있습니다. 클라이언트 관리자에 액세스하려면 편집 링크를 누릅니다.

Access Manager에는 다음 클라이언트 유형이 포함되어 있습니다.

- HDML
- HTML
- JHTML
- VoiceX
- WML

- XHTML
- cHTML
- iHTML
- 이러한 클라이언트 유형에 대한 자세한 내용은 다음 위치에서 Sun Java System Portal Server, Mobile Access 2005Q1 관리 설명서를 참조하십시오 .
http://docs.sun.com/app/docs/coll/PortalServer_05q1 및
http://docs.sun.com/app/docs/coll/PortalServer_05q1_ko

클라이언트 관리자

클라이언트 관리자는 기본 클라이언트 , 스타일 및 연결된 등록 정보를 나열하는 인터페이스이며 장치를 추가 및 구성하는 데 사용할 수 있습니다 .

기본 클라이언트 유형

기본 클라이언트 유형은 클라이언트 관리자의 위쪽에 나열됩니다 . 이러한 클라이언트 유형에는 해당 클라이언트 유형에 속하는 모든 장치가 상속할 수 있는 기본 등록 정보가 포함됩니다 .

스타일 프로필

클라이언트 관리자는 기본 클라이언트 유형을 포함하여 사용 가능한 모든 클라이언트를 스타일 풀다운 메뉴에 그룹화합니다 . 선택한 스타일 (또는 상위 프로필) 은 구성된 하위 장치에 공통되는 등록 정보를 정의합니다 . 장치는 상위 프로필의 등록 정보를 동적으로 상속합니다 .

현재 스타일 등록 정보 링크를 누르면 스타일 등록 정보를 볼 수 있는 읽기 전용 클라이언트 편집기 창이 시작됩니다 .

장치 프로필

스타일을 선택하면 클라이언트 관리자가 해당 스타일에 대해 구성된 장치 프로필을 표시합니다 . 장치는 사용자 에이전트 (장치 이름) 별로 정렬되며 필터 필드에 사용자 에이전트 문자열 (와일드카드 허용) 을 입력하여 장치를 필터링할 수 있습니다 .

각 장치에 대해 각 장치 이름 옆에 있는 편집 링크를 눌러 클라이언트 등록 정보를 수정할 수 있습니다 . 그러면 등록 정보가 클라이언트 편집기 창에 표시됩니다 . 등록 정보를 편집하려면 풀다운 목록에서 다음 분류를 선택합니다 .

하드웨어 플랫폼 . 디스플레이 크기 , 지원되는 문자 집합 등과 같은 장치 하드웨어 등록 정보를 포함합니다 .

소프트웨어 플랫폼. 장치의 응용 프로그램 환경, 운영 체제 및 설치된 소프트웨어의 등록 정보를 포함합니다.

네트워크 특징. 지원되는 베어를 포함하여 네트워크 환경을 설명하는 등록 정보를 포함합니다.

BrowserUA. 장치에서 실행 중인 브라우저 사용자 에이전트 관련 속성을 포함합니다.

WapCharacteristics. 장치에서 지원하는 WAP(Wireless Application Protocol) 환경의 등록 정보를 포함합니다.

PushCharacteristicsNames. 장치에서 지원하는 WAP 환경의 등록 정보를 포함합니다.

추가 등록 정보. 장치에 대한 등록 정보를 추가하는 데 사용할 수 있습니다.

특정 등록 정보에 대한 정의는 다음 위치에 있는 Open Mobile Alliance Ltd. (OMA) *Wireless Application Protocol, Version 20-Oct-2001* 을 참조하십시오.

<http://www1.wapforum.org/tech/terms.asp?doc=WAP-248-UAProf-20011020-a.pdf>

주 설명서를 보려면 먼저 WAP Forum™ 에 등록해야 합니다. 자세한 내용은 <http://www.wapforum.org/faqs/index.htm> 을 참조하십시오.

등록 정보를 수정한 경우 저장을 누릅니다. 장치는 "***" 문자를 표시하여 해당 장치가 사용자 정의되었음을 나타냅니다. 사용자 정의된 등록 정보를 제거하고 장치를 다시 기본 설정으로 재설정하려면 기본 링크를 사용합니다.

스타일에 대해 새 장치를 추가하려면 새 장치 버튼을 누릅니다. 다음과 같은 필드가 있는 새 장치 만들기 창이 표시됩니다.

스타일. 장치에 대한 기본 스타일 (예 : HTML) 을 표시합니다.

장치 사용자 에이전트. 장치에 대한 이름을 지정합니다.

다음 필드를 표시하려면 다음을 누르십시오.

클라이언트 유형 이름. 클라이언트 유형 (예 : HTML) 을 표시합니다. 클라이언트 유형 이름은 모든 장치에서 고유해야 합니다.

이 장치의 바로 상위. 장치의 상위 (기본) 클라이언트 유형을 지정합니다.
예 : HTML

HTTP 사용자 에이전트 문자열. HTTP 요청 헤더에 사용자 에이전트를 정의합니다.
예 : Mozilla/4.0

확인을 누르고 장치 등록 정보를 사용자 정의합니다. 특정 등록 정보에 대한 정의는 다음 위치에 있는 Open Mobile Alliance Ltd. (OMA) *Wireless Application Protocol, Version 20-Oct-2001* 을 참조하십시오.

<http://www1.wapforum.org/tech/>

장치와 장치 등록 정보를 복제하려면 복제 링크를 누릅니다. 장치 이름은 고유해야 합니다. 기본적으로 Access Manager 는 장치의 이름을 `copy_of_devicename` 으로 변경합니다.

장치를 삭제하려면 장치와 함께 나열된 삭제 링크를 누릅니다.

기본 클라이언트 유형

이 속성은 클라이언트 유형 속성의 클라이언트 유형 목록에서 파생된 기본 클라이언트 유형을 정의합니다. 기본값은 `genericHTML` 입니다.

클라이언트 검색 클래스

이 속성은 모든 클라이언트 검색 요청이 라우팅되는 클라이언트 검색 클래스를 정의합니다. 이 속성이 반환하는 문자열은 클라이언트 유형 속성에 나열된 클라이언트 유형 중 하나와 일치해야 합니다. 기본 클라이언트 검색 클래스는 `com.sun.mobile.cdm.FEDIClientDetector` 입니다. 또한 Access Manager 에는 `com.ipplanet.services.cdm.ClientDetectionDefaultImpl` 이 포함되어 있습니다.

클라이언트 검색 사용 가능

이 속성을 사용하면 클라이언트 검색을 사용 가능하게 할 수 있습니다. 클라이언트 검색이 사용 가능하면 (선택되면) 클라이언트 검색 클래스 속성에 지정된 클래스를 통해 모든 요청이 라우팅됩니다.

기본적으로 클라이언트 검색 기능은 사용 가능합니다. 이 속성을 선택하지 않은 경우 Access Manager 는 클라이언트가 `genericHTML` 이고 HTML 브라우저를 통해 액세스된다고 가정합니다.

국제화 설정 서비스 속성

국제화 설정 서비스 속성은 전역 속성입니다. 이러한 속성에 적용되는 값은 Access Manager 구성 전체에 걸쳐 적용되며 구성된 모든 조직이 상속합니다. 전역 속성의 목적은 Access Manager 응용 프로그램을 사용자 정의하는 것이므로 이러한 값을 역할이나 조직에 직접 적용할 수는 없습니다. 국제화 설정 속성은 다음과 같습니다.

- 345 페이지의 " 각 로케일이 지원하는 문자 집합 "
- 345 페이지의 " 문자 집합 별칭 "
- 346 페이지의 " 자동 생성된 공통 이름 형식 "

각 로케일이 지원하는 문자 집합

이 속성은 로케일 및 문자 집합 간의 매핑을 나타내는 각 로케일에 대한 문자 집합 지원을 나열합니다. 형식은 다음과 같습니다.

```
locale=localename | charset=charset1;charset2;charset3;...;charsetn
```

속성의 아래쪽에 있는 버튼을 사용하여 문자 집합을 추가, 편집, 복제 및 제거할 수 있습니다.

문자 집합 별칭

이 속성은 응답을 보내는 데 사용되는 코드 집합 이름 (IANA 이름에 매핑됨) 을 나열합니다. 이러한 코드 집합 이름은 java 코드 집합 이름과 일치할 필요가 없습니다. 현재는 java 문자 집합을 IANA 문자 집합으로 매핑하고 또한 그 반대로 매핑하기 위한 해시 테이블이 있습니다. 별칭 형식은 다음과 같습니다.

```
mimeName=charset | javaName=charset
```

예를 들면 다음과 같습니다.

```
mimeName=Shift_JIS|javaName=SJIS
```

이 예에서는 둘 다 동일한 문자 집합을 나타냅니다.

속성의 아래쪽에 있는 버튼을 사용하여 문자 집합 별칭을 추가, 편집, 복제 및 제거할 수 있습니다.

자동 생성된 공통 이름 형식

이 디스플레이 옵션을 사용하면 다른 로캘 및 문자 집합에 대한 이름 형식을 적용하여 이름을 자동으로 생성하는 방법을 정의할 수 있습니다. 기본 구문은 다음과 같습니다 (정의에 포함된 쉼표 및 / 또는 공백이 이름 형식에 표시됨).

```
en_us = {givenname} {initials} {sn}
```

예를 들어, 중국어 문자 집합의 uid(11111)인 사용자 (User One)에 대한 새 이름 형식을 표시할 경우 다음 표준을 사용합니다.

```
zh = {sn}{givenname}({uid})
```

이 형식을 사용하면 다음과 같이 표시됩니다.

```
OneUser 11111
```

로깅 서비스 속성

로깅 서비스 속성은 전역 속성입니다. 이러한 속성에 적용되는 값은 Sun Java System Access Manager 구성 전체에 걸쳐 적용되며 구성된 모든 조직이 상속합니다. 전역 속성의 목표는 Access Manager 응용 프로그램을 사용자 정의하는 것이므로 이러한 값은 역할이나 조직에 직접 적용할 수 없습니다. 로깅 속성은 다음과 같습니다.

- 348 페이지의 " 최대 로그 크기 "
- 348 페이지의 " 기록 파일 수 "
- 348 페이지의 " 로그 파일 위치 "
- 349 페이지의 " 로깅 유형 "
- 349 페이지의 " 데이터베이스 사용자 이름 "
- 349 페이지의 " 데이터베이스 사용자 비밀번호 "
- 349 페이지의 " 데이터베이스 사용자 비밀번호 (확인)"
- 349 페이지의 " 데이터베이스 드라이버 이름 "
- 349 페이지의 " 구성 가능한 로그 필드 "
- 350 페이지의 " 로그 확인 빈도 "
- 350 페이지의 " 로그 서명 시간 "
- 350 페이지의 " 보안 로깅 사용 가능 "
- 350 페이지의 " 최대 레코드 수 "
- 351 페이지의 " 아카이브당 파일 수 "
- 351 페이지의 " 버퍼 크기 "
- 351 페이지의 " DB 실패 메모리 버퍼 크기 "
- 351 페이지의 " 버퍼 시간 "

- 351 페이지의 "시간 버퍼링 사용 가능"

최대 로그 크기

이 속성은 Access Manager 로그 파일의 최대 크기 (바이트)에 대한 값을 가집니다. 기본값은 1000000입니다.

기록 파일 수

이 속성은 기록 분석을 위해 보유되는 백업 로그 파일의 수에 해당하는 값을 가집니다. 로컬 시스템의 분할 영역 크기와 사용 가능한 디스크 공간에 따라 임의의 정수를 입력할 수 있습니다. 기본값은 3입니다.

주 0을 입력하는 것은 1값과 같은 것으로 해석되며, 이는 0을 지정하면 백업 로그 파일이 만들어지는 것을 의미합니다.

로그 파일 위치

파일 기반 로깅 기능에는 로그 파일을 저장할 수 있는 위치가 필요합니다. 이 필드는 해당 위치에 대한 전체 디렉토리 경로를 가집니다. 기본 위치는 다음과 같습니다.

```
/var/opt/SUNWam/logs
```

기본값이 아닌 디렉토리가 사용될 경우 해당 디렉토리는 Access Manager를 실행 중인 사용자에 대한 쓰기 권한을 갖고 있어야 합니다.

DB(데이터베이스) 로깅을 위한 로그 위치 (예: Oracle 또는 MySQL)를 구성할 때 로그 위치 부분은 대소문자 구분이 있습니다.

예를 들어, Oracle 데이터베이스에 기록하는 경우 로그 위치는 다음과 같습니다.

```
jdbc:oracle:thin:@machine.domain:port:DBName
```

jdbc:oracle:thin은 소문자이어야 합니다.

주 DB에 로깅하도록 구성하려면 웹 컨테이너의 JVM 클래스 경로에 JDBC 드라이버 파일을 추가하십시오. `amadmin` 스크립트의 클래스 경로에 수동으로 JDBC 드라이버 파일을 추가해야 합니다. 그렇지 않으면 `amadmin` 로깅이 JDBC 드라이버를 로드할 수 없습니다.

로깅 속성 값을 변경한 경우 변경 사항을 활성화하기 전에 `Access Manager` 를 다시 시작해야 합니다.

로깅 유형

이 속성을 사용하면 플랫폼 파일 로깅을 위한 파일 또는 데이터베이스 로깅을 위한 DB 를 지정할 수 있습니다.

데이터베이스 사용자 이름

이 속성은 `로깅 유형` 속성이 DB 로 설정된 경우 데이터베이스에 연결하는 사용자의 이름을 가집니다.

데이터베이스 사용자 비밀번호

이 속성은 `로깅 유형` 속성이 DB 로 설정된 경우 데이터베이스 사용자 비밀번호를 가집니다.

데이터베이스 사용자 비밀번호 (확인)

데이터베이스 비밀번호를 확인합니다.

데이터베이스 드라이버 이름

이 속성을 사용하면 로깅 구현 클래스에 사용할 드라이버를 지정할 수 있습니다.

구성 가능한 로그 필드

이 매개 변수는 기록할 필드 목록을 나타냅니다. 기본적으로 다음 필드가 기록됩니다.

- 도메인
- 호스트 이름
- IP 주소
- 기록자
- 로그 수준
- 로그인 아이디
- 모듈 이름

로그 확인 빈도

이 속성은 서버가 손상을 감지하기 위해 로그를 확인해야 하는 빈도 (초) 를 설정합니다. 기본 시간은 3600 초입니다. 이 매개 변수는 보안 로깅에만 적용됩니다.

로그 서명 시간

이 매개 변수는 로그가 서명되는 빈도 (초) 를 설정합니다. 기본 시간은 900 초입니다. 이 매개 변수는 보안 로깅에만 적용됩니다.

보안 로깅 사용 가능

이 속성은 보안 로깅을 사용 가능하게 할지 여부를 지정합니다. 기본적으로 보안 로깅은 사용되지 않습니다. 보안 로깅은 보안 로그의 인증되지 않은 변경이나 손상을 감지할 수 있게 합니다.

최대 레코드 수

이 속성은 읽기 쿼리와 일치하는 레코드 수에 상관 없이 Java LogReader 인터페이스가 반환하는 최대 레코드 수를 설정합니다. 기본적으로 이 속성은 500 으로 설정되며 로깅 API 의 호출자가 LogQuery 매개 변수를 통해 이 속성을 대체할 수 있습니다.

아카이브당 파일 수

이 속성은 보안 로깅에만 적용됩니다. 이 속성은 로그 파일과 키 저장소를 아카이브해야 하는 시점과 후속 보안 로깅을 위해 보안 키 저장소를 다시 생성해야 하는 시점을 지정합니다. 기본값은 로거당 파일 5개입니다.

버퍼 크기

이 속성은 기록할 로깅 서비스에 보내지기 전에 메모리에서 버퍼되는 로그 레코드의 최대 크기를 지정합니다. 기본값은 레코드 한 개입니다.

DB 실패 메모리 버퍼 크기

이 속성은 데이터베이스(DB) 로깅이 실패하는 경우 메모리에 보존된 로그 레코드의 최대 수를 정의합니다. 이 속성은 DB 로깅이 지정되어 있을 때만 적용할 수 있습니다. Access Manager 로깅 서비스에서 DB에 대한 연결이 끊어지면 지정된 레코드 수만큼 버퍼링됩니다. 기본값은 **버퍼 크기** 속성에서 정의한 값의 두 배입니다.

버퍼 시간

이 속성은 기록할 로깅 서비스에 보내지기 전에 로그 레코드가 메모리에 버퍼되는 시간을 정의합니다. 기본값은 3600 초입니다.

시간 버퍼링 사용 가능

이 속성에서 ON을 선택하면 Access Manager가 로그 레코드를 메모리에 버퍼하는 시간 제한을 설정합니다. 시간은 **버퍼 시간** 속성에 설정됩니다.

이름 지정 서비스 속성

이름 지정 서비스 속성은 전역 속성입니다. 이러한 속성에 적용된 값은 Sun Java System Access Manager 구성 전체에 걸쳐 적용되며 구성된 모든 조직이 상속합니다. 전역 속성의 목표는 Access Manager 응용 프로그램을 사용자 정의하는 것이므로 이러한 값은 역할이나 조직에 직접 적용할 수 없습니다.

이름 지정 서비스를 사용하면 클라이언트는 플랫폼이 둘 이상의 Access Manager 를 실행하는 경우 올바른 서비스 URL 을 찾을 수 있습니다. 이름 지정 URL 이 발견되면 이름 지정 서비스는 사용자 세션을 해독하고 프로토콜, 호스트 및 포트를 세션의 매개 변수로 동적으로 대체합니다. 이는 서비스에 대해 반환된 URL 이 사용자 세션이 만들어진 호스트에 대한 URL 이 되도록 합니다. 이름 지정 속성은 다음과 같습니다.

- 354 페이지의 "프로필 서비스 URL"
- 354 페이지의 "세션 서비스 URL"
- 354 페이지의 "로그인 서비스 URL"
- 354 페이지의 "정책 서비스 URL"
- 354 페이지의 "인증 서비스 URL"
- 355 페이지의 "SAML 웹 프로필 / 아티팩트 서비스 URL"
- 355 페이지의 "SAML SOAP 서비스 URL"
- 355 페이지의 "SAML 웹 프로필 /POST 서비스 URL"
- 355 페이지의 "SAML 명제 관리자 서비스 URL"
- 356 페이지의 "연합 명제 관리자 서비스 URL"
- 356 페이지의 "Identity SDK 서비스 URL"
- 356 페이지의 "보안 토큰 관리자 URL"
- 356 페이지의 "JAXRPC 종점 URL"

프로필 서비스 URL

이 필드는 다음과 동일한 값을 가집니다.

```
%protocol://%host:%port/Server_DEPLOY_URI/profileservice
```

이 구문은 특정 세션 매개 변수에 기초하여 프로필 URL 을 동적으로 대체할 수 있게 합니다.

세션 서비스 URL

이 필드는 다음과 동일한 값을 가집니다.

```
%protocol://%host:%port/Server_DEPLOY_URI/sessionsservice
```

이 구문은 특정 세션 매개 변수에 기초하여 세션 URL 을 동적으로 대체할 수 있게 합니다.

로깅 서비스 URL

이 필드는 다음과 동일한 값을 가집니다.

```
%protocol://%host:%port/Server_DEPLOY_URI/loggingservice
```

이 구문은 특정 세션 매개 변수에 기초하여 로깅 URL 을 동적으로 대체할 수 있게 합니다.

정책 서비스 URL

이 필드는 다음과 동일한 값을 가집니다.

```
%protocol://%host:%port/Server_DEPLOY_URI/policyservice
```

이 구문은 특정 세션 매개 변수에 기초하여 정책 URL 을 동적으로 대체할 수 있게 합니다.

인증 서비스 URL

이 필드는 다음과 동일한 값을 가집니다.

```
%protocol://%host:%port/Server_DEPLOY_URI/authservice
```

이 구문은 특정 세션 매개 변수에 기초하여 인증 URL 을 동적으로 대체할 수 있게 합니다.

SAML 웹 프로파일 / 아티팩트 서비스 URL

이 필드는 다음과 동일한 값을 가집니다.

```
%protocol://%host:%port/Server_DEPLOY_URI/SAMLAwareServlet
```

이 구문은 특정 세션 매개 변수에 기초하여 SAML 웹 프로파일 / 아티팩트 URL 을 동적으로 대체할 수 있게 합니다.

SAML SOAP 서비스 URL

이 필드는 다음과 동일한 값을 가집니다.

```
%protocol://%host:%port/Server_DEPLOY_URI/SAMLSOAPReceiver
```

이 구문은 특정 세션 매개 변수에 기초하여 SAML SOAP URL 을 동적으로 대체할 수 있게 합니다.

SAML 웹 프로파일 /POST 서비스 URL

이 필드는 다음과 동일한 값을 가집니다.

```
%protocol://%host:%port/Server_DEPLOY_URI/SAMLPOSTProfileServlet
```

이 구문은 특정 세션 매개 변수에 기초하여 SAML 웹 프로파일 /POST URL 을 동적으로 대체할 수 있게 합니다.

SAML 명제 관리자 서비스 URL

이 필드는 다음과 동일한 값을 가집니다.

```
%protocol://%host:%port/Server_DEPLOY_URI/AssertionManagerServlet/AssertionManagerIF
```

이 구문은 특정 세션 매개 변수에 기초하여 SAML 명제 관리자 서비스 URL 을 동적으로 대체할 수 있게 합니다.

연합 명제 관리자 서비스 URL

이 필드는 다음과 동일한 값을 가집니다.

```
%protocol://%host:%port/amserver/FSAssertionManagerServlet/FSAssertionManagerIF
```

이 구문은 특정 세션 매개 변수에 기초하여 연합 명제 관리자 서비스 URL 을 동적으로 대체할 수 있게 합니다.

Identity SDK 서비스 URL

이 필드는 다음과 동일한 값을 가집니다.

```
%protocol://%host:%port/amserver/UserManagementServlet/
```

이 구문은 특정 세션 매개 변수에 기초하여 Identity SDK 서비스 URL 을 동적으로 대체할 수 있게 합니다.

보안 토큰 관리자 URL

이 필드는 다음과 동일한 값을 가집니다.

```
%protocol://%host:%port/amserver/SecurityTokenManagerServlet/SecurityTokenManagerIF/
```

이 구문은 특정 세션 매개 변수에 기초하여 보안 토큰 관리자 URL 을 동적으로 대체할 수 있게 합니다.

JAXRPC 종점 URL

이 필드는 다음과 동일한 값을 가집니다.

```
%protocol://%host:%port/amserver/jaxrpc/
```

이 구문은 특정 세션 매개 변수에 기초하여 JAXRPC 종점 URL 을 동적으로 대체할 수 있게 합니다.

비밀번호 재설정 서비스 속성

비밀번호 재설정 서비스 속성은 조직 속성입니다. 서비스 구성에서 이러한 속성에 적용된 값이 주어진 조직의 비밀번호 재설정 서비스의 기본값이 됩니다. 조직의 하위 트리에 있는 항목은 조직 속성을 상속하지 않습니다.

비밀번호 재설정 속성은 다음과 같습니다.

- 358 페이지의 " 사용자 검증 "
- 358 페이지의 " 비밀 문제 "
- 358 페이지의 " 검색 필터 "
- 358 페이지의 " 기본 DN "
- 358 페이지의 " 바인드 DN "
- 359 페이지의 " 바인드 비밀번호 "
- 359 페이지의 " 비밀번호 재설정 옵션 "
- 359 페이지의 " 비밀번호 변경 알림 옵션 "
- 359 페이지의 " 비밀번호 재설정 사용 가능 "
- 359 페이지의 " 개인 질문 사용 가능 "
- 360 페이지의 " 최대 질문 수 "
- 360 페이지의 " 다음 로그인 시 반드시 비밀번호 변경 "
- 360 페이지의 " 비밀번호 재설정 실패 잠금 사용 가능 "
- 360 페이지의 " 비밀번호 재설정 실패 잠금 수 "
- 360 페이지의 " 비밀번호 재설정 실패 잠금 간격 "
- 360 페이지의 " 잠금 알림을 보낼 전자 메일 주소 "

- 361 페이지의 "N 회 실패 후 사용자에게 경고 "
- 361 페이지의 " 비밀번호 재설정 실패 잠금 기간 "
- 361 페이지의 " 비밀번호 재설정 잠금 속성 이름 "
- 361 페이지의 " 비밀번호 재설정 잠금 속성 값 "

사용자 검증

이 속성은 비밀번호를 재설정할 사용자를 검색하는 데 사용되는 값을 지정합니다.

비밀 문제

이 필드를 사용하면 사용자가 비밀번호를 재설정하는 데 사용할 수 있는 문제 목록을 추가할 수 있습니다. 문제를 추가하려면 비밀 문제 필드에 문제를 입력하고 추가를 누릅니다. 선택된 문제가 사용자의 사용자 프로필 페이지에 나타납니다. 그런 다음 사용자는 비밀번호 재설정을 위한 문제를 선택할 수 있습니다.

사용자는 개인 문제 사용 가능 속성이 선택된 경우 고유한 문제를 만들 수 있습니다.

검색 필터

이 속성은 사용자 항목을 찾는 데 사용되는 검색 필터를 지정합니다.

기본 DN

이 속성은 사용자 검색이 시작되는 DN 을 지정합니다. DN 을 지정하지 않으면 검색은 조직 DN 에서 시작됩니다. cn=directorymanager 를 기본 DN 으로 사용하지 마십시오. 프록시 인증 충돌이 발생합니다.

바인드 DN

이 속성 값은 사용자 비밀번호를 재설정하기 위해 바인드 비밀번호와 함께 사용됩니다.

바인드 비밀번호

이 속성 값은 바인드 DN 과 함께 사용되어 사용자 비밀번호를 재설정합니다.

비밀번호 재설정 옵션

이 속성은 비밀번호 재설정을 위한 클래스 이름을 결정합니다. 기본 클래스 이름은 다음과 같습니다.

```
com.sun.identity.password.RandomPasswordGenerator
```

비밀번호 재설정 클래스는 플러그 인을 통해 사용자 정의할 수 있습니다. 이 클래스는 PasswordGenerator 인터페이스를 통해 구현해야 합니다. 자세한 내용은 *Access Manager Developer's Guide* 를 참조하십시오.

비밀번호 변경 알림 옵션

이 속성은 비밀번호가 재설정되었음을 사용자에게 알리는 방법을 결정합니다. 기본 클래스 이름은 다음과 같습니다.

```
com.sun.identity.password.EmailPassword
```

비밀번호 알림 클래스는 플러그 인을 통해 사용자 정의할 수 있습니다. 이 클래스는 NotifyPassword 인터페이스로 구현해야 합니다. 자세한 내용은 *Access Manager Developer's Guide* 를 참조하십시오.

비밀번호 재설정 사용 가능

이 속성을 선택하면 비밀번호 재설정 기능을 사용할 수 있습니다.

개인 질문 사용 가능

이 속성을 선택하면 사용자가 비밀번호 재설정을 위한 고유한 문제를 만들 수 있습니다.

최대 질문 수

이 값은 비밀번호 재설정 페이지에서 묻는 최대 문제 수를 지정합니다.

다음 로그인 시 반드시 비밀번호 변경

사용 가능하게 된 경우 이 옵션은 사용자가 다음 로그인 시에 반드시 비밀번호를 변경하게 합니다. 최상위 수준 관리자가 아니라 관리자가 비밀번호 재설정 강제 옵션을 설정할 수 있게 하려면 기본 권한 ACI를 수정하여 해당 속성에 대한 액세스를 허용해야 합니다.

비밀번호 재설정 실패 잠금 사용 가능

이 속성은 사용자가 처음으로 비밀번호 재설정 응용 프로그램을 사용하여 비밀번호 재설정에 실패한 경우 해당 사용자가 비밀번호를 재설정할 수 없게 할지 여부를 지정합니다. 기본적으로 이 기능은 사용 불가로 설정되어 있습니다.

비밀번호 재설정 실패 잠금 수

이 속성은 잠기기 전에 비밀번호 재설정 실패 잠금 간격에 정의된 시간 간격 내에서 사용자가 비밀번호 재설정을 시도할 수 있는 횟수를 정의합니다.

예를 들어, 비밀번호 재설정 실패 잠금 수가 5로 설정되고 로그인 실패 잠금 간격이 5분으로 설정된 경우 사용자는 잠기기 전에 5분 동안 5회에 걸쳐 비밀번호 재설정을 시도할 수 있습니다.

비밀번호 재설정 실패 잠금 간격

이 속성은 사용자가 잠기기 전에 비밀번호 재설정 시도 (비밀번호 재설정 실패 잠금 수에 정의됨)를 완료할 수 있는 시간 (분)을 정의합니다.

잠금 알림을 보낼 전자 메일 주소

이 속성은 사용자가 비밀번호 재설정 서비스로부터 잠길 경우 알림을 받을 전자 메일 주소를 지정합니다. 공백으로 구분된 목록에서 여러 전자 메일 주소를 지정합니다.

N 회 실패 후 사용자에게 경고

이 속성은 Access Manager에서 사용자가 잠길 것이라는 경고 메시지를 보내기 전에 발생할 수 있는 비밀번호 재설정 실패 수를 지정합니다.

비밀번호 재설정 실패 잠금 기간

이 속성은 잠금이 발생한 경우 사용자의 비밀번호 재설정 시도가 허용되지 않는 기간 (분)을 정의합니다.

비밀번호 재설정 잠금 속성 이름

이 속성은 비밀번호 재설정 잠금 속성 값에 설정되는 `inetuserstatus` 값을 포함합니다. 비밀번호 재설정 실패로 사용자가 잠겼으며 비밀번호 재설정 실패 잠금 기간 (분) 변수가 0으로 설정된 경우 `inetuserstatus`가 비활성으로 설정되어 사용자가 비밀번호 재설정을 시도하지 못하도록 합니다.

비밀번호 재설정 잠금 속성 값

이 속성은 사용자 상태의 `inetuserstatus` 값 (비밀번호 재설정 잠금 속성 이름에 포함됨)을 활성 또는 비활성으로 지정합니다. 비밀번호 재설정 실패로 사용자가 잠겼으며 비밀번호 재설정 실패 잠금 기간 (분) 변수가 0으로 설정된 경우 `inetuserstatus`가 비활성으로 설정되어 사용자가 비밀번호 재설정을 시도하지 못하도록 합니다.

플랫폼 서비스 속성

플랫폼 서비스 속성은 전역 속성입니다. 이러한 속성에 적용된 값은 Sun Java System Access Manager 구성 전체에 걸쳐 적용되며 구성된 모든 조직이 상속합니다. 전역 속성의 목표는 Access Manager 응용 프로그램을 사용자 정의하는 것이므로 이러한 값은 역할이나 조직에 직접 적용할 수 없습니다. 플랫폼 속성은 다음과 같습니다.

- 363 페이지의 " 서버 목록 "
- 364 페이지의 " 플랫폼 로컬 "
- 364 페이지의 " 쿠키 도메인 "
- 364 페이지의 " 로그인 서비스 URL "
- 364 페이지의 " 로그아웃 서비스 URL "
- 365 페이지의 " 사용 가능한 로컬 "
- 365 페이지의 " 클라이언트 문자 집합 "

서버 목록

이름 지정 서비스는 초기화 시점에 이 속성을 읽습니다. 이 목록에는 단일 Access Manager 구성의 여러 Access Manager 세션 서버가 있습니다. 예를 들어, 두 개의 Access Manager 가 설치되어 하나인 것처럼 작동해야 할 경우에는 이 목록에 두 서버를 모두 포함해야 합니다. 서비스 URL 에 대한 요청에서 지정된 호스트가 이 목록에 없으면 네임 서비스가 요청을 거부합니다. 목록의 첫 번째 값은 설치 중에 지정된 서버의 호스트 이름과 포트를 지정합니다. 목록의 끝에는 서버를 고유하게 식별하는 2 바이트 값이 있습니다. 로드 균형 조정 또는 페일오버에 참여하는 각 서버는 고유한 식별자를 가져야 합니다. 또한 이 식별자는 서버 URL 을 서버 아이디에 매핑하여 쿠키 길이를 줄이는 데 사용됩니다. 예를 들면 다음과 같습니다.

```
protocol://server_domain:port|01
```

추가 서버는 `protocol://server_domain:port|01|instance_name` 형식을 사용하여 추가할 수 있습니다.

이 속성에는 이름 지정 서비스 프로토콜만 사용되어야 합니다.

플랫폼 로케일

플랫폼 로케일 값은 Access Manager 설치 시 사용된 기본 언어 서브 타입입니다. 인증, 로깅 및 관리 서비스는 이 값의 언어로 관리됩니다. 기본값은 `en_us` 입니다. 지원되는 모든 언어 서브 타입 목록은 [283 페이지의 표 20-1](#) 을 참조하십시오.

쿠키 도메인

인증하는 동안 사용자의 브라우저에 쿠키를 설정한 경우 쿠키 헤더에서 반환되는 도메인 목록입니다. 이 목록이 비어 있으면 쿠키 도메인이 설정되지 않습니다. 다시 말해서 Access Manager 세션 쿠키는 Access Manager 자체에만 전달되며 도메인의 다른 서버에는 전달되지 않습니다. 도메인의 다른 서버에서 SSO가 필요할 경우 쿠키 도메인으로 이 속성을 설정해야 합니다. 하나의 Access Manager 에서 서로 다른 도메인에 두 개의 인터페이스가 있을 경우 이 속성에서 두 쿠키 도메인을 모두 설정해야 합니다. 로드 밸런서가 사용된 경우 쿠키 도메인은 로드 밸런서 뒤에 있는 서버가 아니라 로드 밸런서 도메인의 쿠키 도메인이어야 합니다. 이 필드의 기본값은 설치된 Access Manager 의 도메인입니다.

주 올바른 쿠키 도메인을 입력했는지 확인합니다. 쿠키 도메인이 올바르지 않으면 Access Manager 에 로그인할 수 없습니다.

로그인 서비스 URL

이 필드는 로그인 페이지의 URL 을 지정합니다. 이 속성의 기본값은 `/Service_DEPLOY_URI/UI/Login`. 입니다.

로그아웃 서비스 URL

이 필드는 로그아웃 페이지의 URL 을 지정합니다. 이 속성의 기본값은 `/Service_DEPLOY_URI/UI/Logout` 입니다.

사용 가능한 로케일

이 속성은 플랫폼용으로 구성된 사용 가능한 모든 로케일을 저장합니다. 사용자가 로케일을 선택할 수 있는 응용 프로그램이 있다고 가정합니다. 이 응용 프로그램은 플랫폼 프로필에서 이 속성을 가져와 로케일 목록을 사용자에게 제공합니다. 사용자는 로케일을 선택하고 응용 프로그램은 사용자 항목 `preferredLocale` 에서 이를 설정합니다.

클라이언트 문자 집합

이 속성은 플랫폼 수준에서 다른 클라이언트의 문자 집합을 지정합니다. 이 속성에는 클라이언트 유형과 해당 문자 집합의 목록이 포함됩니다. 형식은 다음과 같습니다.

```
clientType|charset
```

```
clientType2|charset
```

예를 들면 다음과 같습니다.

```
genericHTML|UTF-8
```


정책 구성 서비스 속성

정책 구성 서비스 속성은 전역 속성과 조직 속성으로 구성됩니다. 전역 속성에 적용되는 값은 Sun Java System Access Manager 구성 전체에 걸쳐 적용되며 구성된 모든 조직이 상속합니다. (전역 속성의 목표는 Access Manager 응용 프로그램을 사용자 정의하는 것이므로 이러한 값은 역할이나 조직에 직접 적용할 수 없습니다.) 서비스 관리에서 조직 속성에 적용된 값이 정책 구성의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플릿을 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 항목은 조직 속성을 상속하지 않습니다. 정책 구성 속성은 다음과 같이 구분됩니다.

- [367 페이지의 "전역 속성"](#)
- [368 페이지의 "조직 속성"](#)

전역 속성

정책 구성 서비스의 전역 속성은 다음과 같습니다.

- [368 페이지의 "자원 비교기"](#)
- [368 페이지의 "거부 결정에 대한 평가 계속"](#)

자원 비교기

이 속성은 정책 규칙 정의에 지정된 자원을 비교하는 데 사용되는 자원 비교기 정보를 지정합니다. 자원 비교는 정책 작성과 평가에 모두 사용됩니다. 이 속성은 다음 값을 포함합니다.

<code>serviceType</code>	비교기를 사용해야 하는 서비스를 지정합니다.
<code>class</code>	자원 비교 알고리즘을 구현하는 <code>java</code> 클래스를 정의합니다.
와일드카드	자원 이름에 정의할 수 있는 와일드카드를 지정합니다.
<code>delimiter</code>	자원 이름에 사용되는 분리자를 지정합니다.
<code>caseSensitivity</code>	두 자원의 비교에서 대소문자를 구분하는지 아니면 무시하는지 여부를 지정합니다. <code>False</code> 인 경우 대소문자를 무시하며 <code>True</code> 인 경우 대소문자를 구분합니다.

거부 결정에 대한 평가 계속

이 속성은 DENY 정책 결정이 존재하는 경우에도 정책 프레임워크가 계속해서 후속 정책을 평가해야 하는지 여부를 지정합니다. 선택되지 않은 경우 (기본값) DENY 결정이 인식되고 나면 정책 평가가 후속 정책을 건너뛴니다.

조직 속성

정책 구성 서비스의 조직 속성은 다음과 같습니다.

- [370 페이지의 "LDAP 서버 및 포트 "](#)
- [370 페이지의 "LDAP 기본 DN"](#)
- [370 페이지의 "LDAP 사용자 기본 DN"](#)
- [371 페이지의 "Access Manager 역할 기본 DN"](#)
- [371 페이지의 "LDAP 바인드 DN"](#)
- [371 페이지의 "LDAP 바인드 비밀번호 "](#)
- [371 페이지의 "LDAP 바인드 비밀번호 \(확인 \)"](#)
- [371 페이지의 "LDAP 조직 검색 필터 "](#)

- 371 페이지의 "LDAP 조직 검색 범위 "
- 372 페이지의 "LDAP 그룹 검색 필터 "
- 372 페이지의 "LDAP 그룹 검색 범위 "
- 372 페이지의 "LDAP 사용자 검색 필터 "
- 372 페이지의 "LDAP 사용자 검색 범위 "
- 372 페이지의 "LDAP 역할 검색 필터 "
- 373 페이지의 "LDAP 역할 검색 범위 "
- 373 페이지의 "Access Manager 역할 검색 범위 "
- 373 페이지의 "LDAP 조직 검색 속성 "
- 373 페이지의 "LDAP 그룹 검색 속성 "
- 373 페이지의 "LDAP 사용자 검색 속성 "
- 373 페이지의 "LDAP 역할 검색 속성 "
- 374 페이지의 " 검색에서 반환되는 최대 결과 수 "
- 374 페이지의 " 검색 시간 초과 "
- 374 페이지의 "LDAP SSL 사용 가능 "
- 374 페이지의 "LDAP 연결 풀 최소 크기 "
- 374 페이지의 "LDAP 연결 풀 최대 크기 "
- 374 페이지의 " 선택한 정책 주제 "
- 375 페이지의 " 선택한 정책 조건 "
- 375 페이지의 " 선택한 정책 참조 "
- 375 페이지의 " 주제 결과 수명 "
- 375 페이지의 " 사용자 별칭 사용 가능 "

LDAP 서버 및 포트

이 필드는 정책 주제 (예 : LDAP 사용자, LDAP 역할, LDAP 그룹 등) 를 검색하는데 사용할 Access Manager 를 설치하는 동안 지정된 기본 LDAP 서버의 호스트 이름과 포트 번호를 지정합니다. 형식은 *hostname:port*입니다. 예를 들면 다음과 같습니다.

```
machine1.example.com:389
```

여러 LDAP 서버 호스트에 대한 파일오버 구성의 경우 이 값은 공백으로 구분된 호스트 목록일 수 있습니다. 형식은 *hostname1:port1 hostname2:port2...* 입니다.

예를 들면 다음과 같습니다.

```
machine1.example1.com:389 machine2.example1.com:389
```

여러 항목이 있을 경우 로컬 서버 이름을 접두어로 지정해야 합니다. 이렇게 지정해야 특정 Access Manager가 특정 Directory Server와 통신하도록 구성할 수 있습니다.

형식은 *servername|hostname:port* 입니다.

예를 들면 다음과 같습니다.

```
machine1.example1.com|machine1.example1.com:389
```

```
machine1.example2.com|machine1.example2.com:389
```

파일오버 구성의 경우 :

```
IS_Server1.example1.com|machine1.example1.com:389 machine2.example.com:389
```

```
IS_Server2.example2.com|machine1.example2.com:389 machine2.example2.com:389
```

LDAP 기본 DN

이 필드는 검색이 시작되는 LDAP 서버의 기본 DN 을 지정합니다. 기본값은 Access Manager 설치의 최상위 수준 조직입니다.

LDAP 사용자 기본 DN

이 속성은 검색을 시작할 LDAP 서버의 LDAP 사용자 주제에 사용되는 기본 DN 을 지정합니다. 기본값은 Access Manager 설치 기본의 최상위 수준 조직입니다.

Access Manager 역할 기본 DN

이 속성은 검색을 시작할 LDAP 서버의 Access Manager 역할 주제에 사용되는 기본 DN을 지정합니다. 기본값은 Access Manager 설치 기본의 최상위 수준 조직입니다.

LDAP 바인드 DN

이 필드는 LDAP 서버의 바인드 DN 을 지정합니다.

LDAP 바인드 비밀번호

이 속성은 LDAP 서버에 바인드하는 데 사용되는 비밀번호를 정의합니다. 기본적으로 설치하는 동안 입력된 `amldapuser` 비밀번호가 바인드 사용자로 사용됩니다.

LDAP 바인드 비밀번호 (확인)

LDAP 바인드 비밀번호를 확인합니다.

LDAP 조직 검색 필터

조직 항목을 찾는 데 사용되는 검색 필터를 지정합니다. 기본값은 `(objectclass=sunMangagedOrganization)` 입니다.

LDAP 조직 검색 범위

이 속성은 조직 항목을 찾는 데 사용되는 범위를 정의합니다. 이 범위는 다음 중 하나가 되어야 합니다.

- `SCOPE_BASE`
- `SCOPE_ONE`
- `SCOPE_SUB` (기본값)

LDAP 그룹 검색 필터

그룹 항목을 찾는 데 사용되는 검색 필터를 지정합니다. 기본값은 (objectclass=groupOfUniqueNames) 입니다.

LDAP 그룹 검색 범위

이 속성은 그룹 항목을 찾는 데 사용되는 범위를 정의합니다. 이 범위는 다음 중 하나가 되어야 합니다.

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB (기본값)

LDAP 사용자 검색 필터

사용자 항목을 찾는 데 사용되는 검색 필터를 지정합니다. 기본값은 (objectclass=inetorgperson) 입니다.

LDAP 사용자 검색 범위

이 속성은 사용자 항목을 찾는 데 사용되는 범위를 정의합니다. 이 범위는 다음 중 하나가 되어야 합니다.

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB (기본값)

LDAP 역할 검색 필터

역할에 대한 항목을 찾는 데 사용되는 검색 필터를 지정합니다. 기본값은 (&(objectclass=ldapsubentry)(objectclass=nsroledefinitions)) 입니다.

LDAP 역할 검색 범위

이 속성은 역할에 대한 항목을 찾는 데 사용되는 범위를 정의합니다. 이 범위는 다음 중 하나가 되어야 합니다.

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB (기본값)

Access Manager 역할 검색 범위

이 속성은 Access Manager 역할 주제에 대한 항목을 찾는 데 사용되는 범위를 정의합니다. 이 범위는 다음 중 하나가 되어야 합니다.

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB (기본값)

LDAP 조직 검색 속성

이 필드는 조직에서 검색을 수행하는 속성 유형을 정의합니다. 기본값은 o입니다.

LDAP 그룹 검색 속성

이 필드는 그룹에서 검색을 수행하는 속성 유형을 정의합니다. 기본값은 cn입니다.

LDAP 사용자 검색 속성

이 필드는 사용자에서 검색을 수행하는 속성 유형을 정의합니다. 기본값은 uid입니다.

LDAP 역할 검색 속성

이 필드는 역할에서 검색을 수행하는 속성 유형을 정의합니다. 기본값은 cn입니다.

검색에서 반환되는 최대 결과 수

이 필드는 검색에서 반환되는 최대 결과 수를 정의합니다. 기본값은 100 입니다. 검색 제한이 지정된 양을 초과할 경우 해당 지점까지 발견된 항목이 반환됩니다.

검색 시간 초과

이 속성은 검색 시간 초과가 발생하기 전까지의 시간을 지정합니다. 검색이 지정된 시간을 초과할 경우 해당 시점까지 발견된 항목이 반환됩니다.

LDAP SSL 사용 가능

이 속성은 LDAP 서버가 SSL 을 실행 중인지 여부를 지정합니다. 선택할 경우 SSL 이 사용 가능하고 선택하지 않을 경우 (기본값) SSL 이 사용 불가능합니다.

LDAP 서버가 SSL 을 사용할 수 있는 상태에서 실행 중 (LDAPS) 이면 , Access Manager 가 LDAPS 프로토콜을 통해 디렉토리 서버에 연결될 수 있도록 Access Manager 가 적절한 SSL 로 신뢰된 인증서로 구성되었는지 확인해야만 합니다.

LDAP 연결 풀 최소 크기

이 속성은 LDAP 서버 속성에 지정된 대로 Directory Server에 연결하는 데 사용되는 연결 풀의 최소 크기를 지정합니다. 기본값은 1 입니다.

LDAP 연결 풀 최대 크기

이 속성은 LDAP 서버 속성에 지정된 대로 Directory Server에 연결하는 데 사용되는 연결 풀의 최대 크기를 지정합니다. 기본값은 10 입니다.

선택한 정책 주제

이 속성을 사용하면 조직의 정책 정의에 사용할 수 있는 주제 유형 집합을 선택할 수 있습니다.

선택한 정책 조건

이 속성을 사용하면 조직의 정책 정의에 사용할 수 있는 조건 유형 집합을 선택할 수 있습니다.

선택한 정책 참조

이 속성을 사용하면 조직의 정책 정의에 사용할 수 있는 참조 유형 집합을 선택할 수 있습니다.

주제 결과 수명

이 속성은 단일 사인 온 (SSO) 토큰에 기반한 동일한 정책 요청을 평가하기 위해 캐시된 주제 결과를 사용할 수 있는 시간 (분) 을 지정합니다.

초기에 SSO 토큰에 대해 정책을 평가할 때 주어진 사용자에게 정책을 적용할 수 있는지 여부를 확인하기 위해 해당 정책의 주제 인스턴스를 평가합니다. SSO 토큰 아이디가 키로 사용되는 주제 결과는 정책에 캐시됩니다. 주제 결과 수명 속성에 지정된 시간 내에 동일한 SSO 토큰 아이디의 동일한 정책에 대해 다른 평가가 수행되면 정책 프레임워크는 주제 인스턴스를 평가하는 대신 캐시된 주제 결과를 검색합니다. 따라서 정책 평가를 위한 시간이 크게 줄어듭니다.

사용자 별칭 사용 가능

이 속성은 원격 Directory Server 에서 자원 주제 구성원이 로컬 사용자의 별칭을 지정하는 자원을 보호하는 정책을 만들 경우에 사용 가능으로 지정해야 합니다.

예를 들어, 원격 Directory Server 에서 uid=rmuser 를 만든 다음 rmuser 를 Access Manager 의 로컬 사용자 (예 :uid=luser) 에 별칭으로 추가할 경우에 이 속성을 사용 가능으로 지정해야 합니다. rmuser 로 로그인하면 세션이 로컬 사용자 (luser) 에 만들어지고 정책이 성공적으로 적용됩니다.

조직 속성

SAML 서비스 속성

SAML (Security Assertion Markup Language) 서비스 속성은 전역 속성입니다. 이러한 속성에 적용된 값은 Sun Java System Access Manager 구성 전체에 걸쳐 적용되며 구성된 모든 조직이 상속합니다. (전역 속성의 목표는 Access Manager 응용 프로그램을 사용자 정의하는 것이므로 이러한 값은 역할이나 조직에 직접 적용할 수 없습니다.)

SAML 서비스 구조에 대한 자세한 내용은 *Access Manager Developer's Guide* 를 참조하십시오.

SAML 속성은 다음과 같습니다.

- 378 페이지의 " 사이트 아이디 및 사이트 발급자 이름 "
- 378 페이지의 "SAML 요청에 서명 "
- 378 페이지의 "SAML 응답에 서명 "
- 378 페이지의 " 서명 명제 "
- 378 페이지의 "SAML 아티팩트 이름 "
- 379 페이지의 " 대상 지정자 "
- 379 페이지의 " 아티팩트 시간 초과 "
- 379 페이지의 "notBefore 시간에 대한 명제 비대칭 요소 "
- 379 페이지의 " 명제 시간 초과 "
- 379 페이지의 " 신뢰할 수 있는 파트너 사이트 "
- 383 페이지의 " 대상 URL 에 POST"

사이트 아이디 및 사이트 발급자 이름

이 속성은 항목 목록을 포함하며 각 항목은 인스턴스 아이디, 사이트 아이디 및 사이트 발급자 이름을 포함합니다. 기본값은 설치하는 동안 할당됩니다. 형식은 다음과 같습니다.

```
instanceid=serverprotocol://servername:portnumber|siteid=site_id|issuerName=site_issuer_name
```

SSL에 대해 이 속성을 구성한 후 (소스 사이트와 대상 사이트 모두에서) instanceid 프로토콜이 HTTPS// 인지 확인합니다.

SAML 요청에 서명

이 속성은 모든 SAML 요청을 전달하기 전에 디지털 서명할 것인지 (XML DSIG) 여부를 지정합니다. 이 옵션을 누르면 이 기능을 사용할 수 있습니다.

SAML 응답에 서명

이 속성은 모든 SAML 응답을 전달하기 전에 디지털 서명할 것인지 (XML DSIG) 여부를 지정합니다. 이 옵션을 누르면 이 기능을 사용할 수 있습니다.

이 옵션의 사용 가능 여부에 상관 없이 SAML 웹 게시 프로파일 사용하는 모든 SAML 응답이 디지털 서명됩니다.

서명 명제

이 속성은 모든 SAML 명제를 전달하기 전에 디지털 서명할 것인지 (XML DSIG) 여부를 지정합니다. 이 옵션을 누르면 이 기능을 사용할 수 있습니다.

SAML 아티팩트 이름

이 속성은 SAML 서비스 구성에 정의된 SAML 아티팩트에 변수 이름을 할당합니다. SAML 아티팩트는 명제와 소스 사이트를 식별하는 바운드 크기 데이터입니다. SAML 아티팩트는 URL 쿼리 문자열의 일부로 보내지며 리디렉션에 의해 대상 사이트로 전달됩니다. 기본값은 SAMLart 입니다. 예를 들어, 기본 SAMLart 서비스 구성을 사용할 경우 리디렉션 쿼리 문자열이 다음과 같을 수 있습니다.

`http://host:port/deploy_URI/SamlAwareServlet?TARGET=http://URL/&SAMLart=artifact123`

대상 지정자

이 속성은 리디렉션에 사용되는 대상 사이트 URL 에 변수 이름을 할당합니다. 기본값은 Target 입니다.

아티팩트 시간 초과

이 속성은 아티팩트에 대해 작성된 명제의 시간 초과를 지정합니다. 기본값은 400 입니다.

notBefore 시간에 대한 명제 비대칭 요소

이 속성은 명제의 notBefore 시간을 계산하는 데 사용됩니다. 예를 들어, IssueInstant가 2002-09024T21:39:49Z 이고 명제 비대칭 요소 notBefore 시간 값이 300 초 (기본값: 180) 로 설정된 경우 명제에 대한 조건 요소의 notBefore 속성은 2002-09-24T21:34:49Z 입니다.

명제 시간 초과

이 속성은 명제에서 시간 초과가 발생하기까지의 시간 (초) 을 지정합니다. 기본값은 420 입니다.

주 명제의 총 유효 기간은 notBefore 시간에 대한 명제 비대칭 요소 속성과 명제 시간 초과 속성 모두에 설정된 값에 의해 정의됩니다.

신뢰할 수 있는 파트너 사이트

이 속성은 특정 사이트가 신뢰할 수 있는 관계를 설정하여 다른 파트너 사이트와 통신할 수 있도록 파트너의 정보를 저장합니다.

이 속성은 각각 키 / 값 쌍 ("|" 로 분리) 이 들어있는 항목의 목록을 포함합니다. 각 항목에는 소스 아이디가 필요합니다. 예를 들면 다음과 같습니다.

SourceID=siteid|SOAPURL=https://servername:portnumber/amserver/SAMLSOAPReceiver|AuthType=SSL|hostlist=ipaddress (또는 ,DNS 서버 이름 또는 인증서 별칭)

매개 변수는 다음과 같습니다.

표 41-1 신뢰할 수 있는 파트너 사이트 매개 변수

SourceID	사이트 아이디 및 발급자 이름에서처럼 20 바이트 시퀀스를 정의했습니다.
대상	<p>이 매개 변수는 포트 번호와 함께 또는 포트 번호 없이 특정 도메인에 정의됩니다. 해당 특정 도메인에서 호스트되는 웹 페이지에 연결하려는 경우 추가 처리를 위해 SAMLUrl 매개 변수 또는 POSTUrl 매개 변수로 정의되는 URL에 대한 리디렉션을 target 에서 지정합니다.</p> <p>신뢰할 수 있는 파트너 사이트 속성에 동일한 도메인이 지정된 두 개의 항목 (포트 번호를 포함하는 항목과 그렇지 않은 항목) 이 있는 경우 포트 번호를 가진 항목이 더 높은 우선 순위를 가집니다.</p> <p>예를 들어 , 다음과 같은 두 개의 신뢰할 수 있는 파트너 사이트 정의가 있고</p> <pre>target=sun.com SAMLUrl=http://machine1.sun.com:8080/amserver/SAMLAwareServlet</pre> <p>및</p> <pre>target=sun.com:8080 SAMLUrl=http://machine2.sun.com:80/amserver/SAMLAwareServlet</pre> <p>다음 페이지를 찾으려는 경우</p> <pre>http://sOMEMACHINE.sun.com:8080/index.html</pre> <p>두 번째 정의가 SAML 서비스 공급자로 선택되는데 그 이유는 일치하는 도메인과 포트가 target 매개 변수에 공존하기 때문입니다.</p>
SAMLUrl	SAML 서비스를 제공하는 URL 을 정의합니다 . 이 URL 에 지정된 서블릿은 OASIS-SAML 바인딩 및 프로파일 사양에 정의된 Web-browser SSO with Artifact 프로필을 구현합니다 .
POSTUrl	SAML 서비스를 제공하는 URL 을 정의합니다 . 이 URL 에 지정된 서블릿은 OASIS-SAML 바인딩 및 프로파일 사양에 정의된 Web-browser SSO with POST 프로필을 구현합니다 .
issuer	Access Manager 내에서 생성된 명제 작성자를 정의합니다 . 구문은 hostname:port 입니다 .

SOAPUrl	SOAP 수신기 서비스 URL 을 지정합니다 .
AuthType	<p>SAML 에 사용되는 인증 유형을 정의합니다 . 인증 유형은 다음 중 하나가 되어야 합니다 .</p> <ul style="list-style-type: none"> • NOAUTH • BASICAUTH • SSL • SSLWITHBASICAUTH <p>이 매개 변수는 선택 사항이며 지정하지 않을 경우 기본값은 NOAUTH 입니다 .</p> <p>BASICAUTH 또는 SSLWITHBASICAUTH 를 지정하는 경우 사용자 매개 변수가 필요하며 SOAPUrl 은 HTTPS 이어야 합니다 .</p>
User	파트너의 SOAP 수신기를 보호하는 데 사용되는 파트너의 uid 를 정의합니다 .
version	<p>SAML 요청을 보내는 데 사용되는 SAML 버전을 정의합니다 . SAML 버전으로 1.0 또는 1.1 을 지정합니다 . 이 매개 변수를 정의하지 않을 경우 AMConfig.properties 의 다음 기본값이 사용됩니다 .</p> <pre>com.example.identity.saml.assertion.version-1.1 com.example.identity.saml.protocol.version=1.1</pre>
hostlist	<p>이 속성은 지정된 파트너 사이트에 요청을 보낼 수 있는 해당 사이트 내의 모든 호스트에 대한 IP 주소 및 / 또는 certAlias 를 나열합니다 . 이것은 요청자가 실제로 SAML 아티팩트의 의도된 수신자가 되도록 합니다 .</p> <p>요청자의 호스트 또는 클라이언트 인증서가 수신자 사이트의 이 목록에 있는 경우 서비스가 계속됩니다 . 호스트 또는 클라이언트 인증서가 호스트 목록의 해당 호스트 또는 인증서와 일치하지 않는 경우 SAML 서비스가 요청을 거부합니다 .</p>
AccountMapper	<p>명제의 주제가 대상 사이트에서 아이디와 관련되는 방법을 정의하는 플러그 가능 클래스를 지정합니다 . 기본값은 다음과 같습니다 .</p> <pre>com.sun.identity.saml.plugins.DefaultAccountMapper</pre>
PartnerAccountMapper	PartnerAccountMapper 클래스는 파트너 계정을 Sun Java System Access Manager 의 사용자 계정으로 매핑하기 위해 구현되는 인터페이스입니다 .

<code>attributeMapper</code>	<code>attributeMapper</code> 가 위치하는 경로로 클래스를 지정합니다. 응용 프로그램은 <code>attributeMapper</code> 를 개발하여 SSO 토큰 아이디를 얻거나 쿼리의 <code>AuthenticationStatement</code> 를 포함하는 명제를 얻을 수 있습니다. 그런 다음 이 매핑은 주제의 속성을 검색하는 데 사용됩니다. <code>attributeMapper</code> 가 지정되지 않은 경우 <code>DefaultAttributeMapper</code> 가 사용됩니다.
<code>actionMapper</code>	<code>actionMapper</code> 가 위치하는 경로로 클래스를 지정합니다. 응용 프로그램은 <code>actionMapper</code> 를 개발하여 SSO 토큰 아이디를 얻거나 쿼리의 <code>AuthenticationStatement</code> 를 포함하는 명제를 얻을 수 있습니다. 그런 다음 이 매핑은 쿼리에 정의된 작업에 대한 권한 부여 결정을 검색하는 데 사용됩니다. <code>actionMapper</code> 가 지정되지 않은 경우 <code>DefaultActionMapper</code> 가 사용됩니다.
<code>siteAttributeMapper</code>	<code>siteAttributeMapper</code> 가 위치하는 경로로 클래스를 지정합니다. 응용 프로그램은 <code>siteAttributeMapper</code> 를 개발하여 SSO 동안 명제에 포함되는 속성을 얻습니다. <code>siteAttributeMapper</code> 를 찾을 수 없으면 SSO 동안 명제에 속성이 포함되지 않습니다.
<code>PartnerSiteAttributeMapper</code>	브라우저 아티팩트 및 POST 프로필의 SSO 시나리오 도중 파트너에게 반환되는 인증 명제의 일부로서, <code>AttributeStatements</code> 요소로 반환되도록 요청되는 속성 개체의 목록을 반환하려면 파트너 사이트에서 이 인터페이스를 구현해야 합니다.
<code>certAlias=aliasName</code>	파트너가 명제에 서명하고 파트너 인증서를 서명된 명제의 <code>KeyInfo</code> 부분에서 찾을 수 없을 경우 명제의 서명을 확인하는 데 사용되는 <code>certAlias</code> 이름을 지정합니다.

다음 표에는 신뢰할 수 있는 파트너 사이트의 구성 예가 나열되어 있습니다. 모든 매개 변수가 항상 필요한 것은 아니며 선택적 매개 변수는 대괄호로 묶여 있습니다.

	보낸 사람	수신자
아티팩트	<code>sourceid</code>	<code>sourceid</code>
	<code>target</code>	<code>SOAPUrl</code>
	<code>SAMLUrl</code>	<code>[accountMapper]</code>
	<code>hostlist</code>	<code>[AuthType]</code>
	<code>[siteAttributeMapper]</code>	<code>[User]</code>
		<code>[certAlias]</code>

	보낸 사람	수신자
POST 프로파일	sourceid	sourceid
	target	issuer
	POSTUrl	[accountMapper]
	[siteAttributeMapper]	[certAlias]
SOAP 요청		sourceid
		hostlist
		[attributeMapper]
		[actionMapper]
		[certAlias]
		[issuer]

대상 URL 에 POST

사이트에서 SSO (아티팩트 프로파일 또는 POST 프로파일) 를 통해 받은 대상 URL 이 이 속성에 나열된 경우 SSO 에서 받은 명제가 http: FORM POST 에 의해 대상 URL 로 보내집니다. POST 에 테스트 URL 또는 기타 추가 URL 을 사용하지 마십시오.

세션 서비스 속성

세션 서비스 속성은 전역 속성이자 동적 속성입니다. 전역 속성에 적용되는 값은 Access Manager 구성 전체에 걸쳐 적용되며 구성된 모든 조직에서 상속합니다. 전역 속성의 목적은 Access Manager 응용 프로그램을 사용자 정의하는 것이므로 이러한 값을 역할이나 조직에 직접 적용할 수는 없습니다.

동적 속성에 적용되는 값은 역할 또는 조직에 적용됩니다. 사용자에게 역할이 할당되거나 사용자가 조직에 할당될 경우 해당 사용자는 기본적으로 이러한 속성을 상속합니다. 기본 세션 값은 등록된 모든 Access Manager 조직에 대한 서비스 구성에 설정됩니다. 특정 조직에 대한 세션 서비스를 등록하고 템플릿을 만든 다음 기본값이 아닌 값을 입력하여 이러한 값을 개별 조직에 대해 다르게 설정할 수 있습니다.

보조 구성 인스턴스

인스턴스 이름

이 필드에서는 보조 인스턴스의 이름을 정의합니다.

세션 저장소 사용자

이 필드에서는 세션 데이터를 검색하고 저장하는 데 필요한 데이터베이스 사용자를 정의합니다.

세션 저장소 비밀번호

이 필드에서는 세션 저장소에서 정의된 데이터베이스 사용자의 비밀번호를 정의합니다.

세션 저장소 비밀번호 (확인)

비밀번호를 확인합니다.

세션 클러스터 서버 목록

이 속성은 동일한 세션 페일오버 클러스터에 참여하는 Access Manager 서버의 고유한 식별자 (2 바이트 값이며 플랫폼 서비스의 서버 목록 항목에 해당됨) 를 나열합니다.

최대 대기 시간

이 필드에서는 스레드가 JDBC 연결 객체를 얻기 위해 대기하는 총 시간을 정의합니다. 값은 밀리초 단위입니다.

JDBC 드라이버 구현 클래스

이 필드에서는 JDBC 연결 풀을 설정하는 데 필요한 저장소 종속 팩토리 클래스의 이름을 지정합니다. Access Manager 는 HADB 및 Oracle 둘 다에 사용할 수 있는 구현을 제공합니다.

JDBC URL

이 필드에서는 JDBC 의 URL 을 지정합니다.

최소 풀 크기

이 속성은 연결 풀에서 작성될 JDBC 연결의 최소 수를 정의합니다.

최대 풀 크기

이 속성은 연결 풀에서 작성될 JDBC 연결의 최대 수를 정의합니다.

전역 속성

전역 속성은 다음과 같습니다.

- 387 페이지의 " 최대 검색 결과 수 "
- 387 페이지의 " 검색 시간 초과 (초)"

최대 검색 결과 수

이 속성은 세션 검색에서 반환되는 최대 결과 수를 지정합니다. 기본값은 120입니다.

검색 시간 초과 (초)

이 속성은 세션 검색이 종료되기 이전의 최대 시간을 정의합니다. 기본값은 5 초입니다.

동적 속성

동적 속성은 다음과 같습니다.

- 388 페이지의 " 최대 세션 시간 (분)"
- 388 페이지의 " 최대 유휴 시간 (분)"
- 388 페이지의 " 최대 캐싱 시간 (분)"

최대 세션 시간 (분)

이 속성은 세션이 만료되고 사용자가 액세스 권한을 다시 얻기 위해 재인증을 수행하기 전까지의 최대 시간을 나타내는 값 (분) 을 가집니다. 1 이상의 값이 사용되며 기본값은 120 입니다. 보안과 편의에 대한 요구 사항 사이에서 균형을 이루려면 최대 세션 시간 간격을 더 높은 값으로 설정하고 최대 유휴 시간 간격을 상대적으로 낮은 값으로 설정하는 것을 고려합니다. 최대 세션 시간은 구성된 값 이상으로 확장되지 않도록 세션의 유효성을 제한합니다.

최대 유휴 시간 (분)

이 속성은 세션이 만료되고 사용자가 액세스 권한을 다시 얻기 위해 재인증을 수행하기 전까지 활동이 없는 최대 시간을 나타내는 값 (분) 을 가집니다. 1 이상의 값이 사용되며 기본값은 30 입니다. 보안과 편의에 대한 요구 사항 사이에서 균형을 이루려면 최대 세션 시간 간격을 더 높은 값으로 설정하고 최대 유휴 시간 간격을 상대적으로 낮은 값으로 설정하는 것을 고려합니다.

최대 캐싱 시간 (분)

이 속성은 클라이언트가 캐시된 세션 정보를 새로 고치기 위해 Access Manager 에 연결하기 전까지의 최대 간격 값 (분) 을 가집니다. 0 이상의 값이 사용되며 기본값은 3 입니다. 최대 캐싱 시간을 최대 유휴 시간보다 항상 짧게 지정해야 합니다.

SOAP 바인드 서비스 속성

SOAP 바인드 서비스 속성은 전역 속성입니다. 이러한 속성에 적용된 값은 Sun Java System Access Manager 구성 전체에 걸쳐 적용되며 구성된 모든 조직이 상속합니다. 전역 속성의 목표는 Access Manager 응용 프로그램을 사용자 정의하는 것이므로 이러한 값은 역할이나 조직에 직접 적용할 수 없습니다.

SOAP 바인드 서비스 속성은 다음과 같습니다.

- [389 페이지의 "요청 처리기 목록"](#)
- [390 페이지의 "웹 서비스 인증자"](#)
- [390 페이지의 "지원되는 인증 기법"](#)

요청 처리기 목록

이 속성은 Access Manager 에 배포된 웹 서비스 공급자 (WSP) 에 대한 정보를 저장합니다. 이 속성은 키 / 값 쌍 ("|" 으로 구분) 을 포함하는 항목을 나열합니다. 예를 들면 다음과 같습니다.

```
key=disco|class=com.example.identity.liberty.ws.disco.DiscoveryService|soa
pActions=sa1 sa2 sa2
```

새 요청 처리기를 추가하려면 추가 버튼을 누릅니다. 키 및 클래스 매개 변수는 필수 항목입니다. 매개 변수는 다음과 같습니다.

key. 이 매개 변수는 WSP 의 SOAP 종점에 대한 URI 경로의 두 번째 부분을 정의합니다. 첫 번째 부분은 SOAP 서비스의 리버티로 정의됩니다. 예를 들어, disco 를 key 매개 변수로 정의할 경우 검색 서비스에 대한 SOAP 종점은 다음과 같습니다.

```
protocol://hostname:port/deploy_uri/Liberty/disco
```

class. WSP 에 대한 구현 클래스의 이름을 지정합니다. 리버티 SOAP 계층은 요청된 메시지를 처리한 다음 응답을 반환하기 위해 각 WSP 에 의해 구현되는 처리기 인터페이스를 제공합니다.

soapActions. 지원되는 SOAPAction 을 지정하는 선택적 매개 변수입니다. 이 매개 변수를 지정하지 않을 경우 모든 SOAPAction 이 지원됩니다. 웹 서비스 사용자 (WSC) 가 지원되지 않는 SOAPAction 을 사용하여 요청을 보낼 경우 해당 요청은 SOAP 계층에 의해 거부되며 해당하는 WSP 로 전달되지 않습니다.

웹 서비스 인증자

이 속성은 요청에 기초하여 웹 서비스 사용자 (WSC) 에 대한 자격 증명을 인증 및 생성하는 `WebServiceAuthenticator` 인터페이스에 대한 구현 클래스를 정의합니다.

지원되는 인증 기법

이 속성은 SOAP 종점에 의해 지원되는 인증 기법을 지정합니다. 기본적으로 모든 기법이 선택됩니다. 인증 기법을 선택하지 않았으며 WSC 가 해당 인증 기법을 사용하여 요청을 보낼 경우 요청은 SOAP 계층에 의해 거부되며 해당하는 WSP 로 전달되지 않습니다.

사용자 속성

사용자 속성이 보관되는 위치는 서비스 구성 창과 사용자 관리 창입니다. 서비스 구성 창에는 등록된 조직에 대한 기본 속성이 포함되며 사용자 관리 창에는 사용자 항목 속성이 포함됩니다.

- [391 페이지의 " 사용자 서비스 속성 "](#)
- [393 페이지의 " 사용자 프로필 속성 "](#)
- [396 페이지의 " 고유 사용자 아이디 "](#)

사용자 서비스 속성

사용자 서비스 속성은 동적 속성입니다. 동적 속성에 적용된 값은 Access Manager 에서 구성된 역할이나 조직에 할당됩니다. 역할이 사용자에게 할당되거나 사용자가 조직에 할당되면 동적 속성이 해당 사용자의 특성이 됩니다. 사용자 속성은 다음과 같이 구분됩니다.

- [사용자 기본 언어](#)
- [사용자 기본 표준 시간대](#)
- [상속된 로캘](#)
- [관리자 DN 시작 보기](#)
- [기본 사용자 상태](#)

기본 사용자 값은 등록된 모든 Access Manager 조직에 대해 설정됩니다. 이러한 값은 특정 조직에 대한 사용자 서비스를 등록하고 템플리트를 만든 다음 기본값이 아닌 값을 입력하여 개별 조직에 대해 다르게 설정할 수 있습니다.

사용자 기본 언어

이 필드는 Access Manager 콘솔에 표시되는 텍스트 언어에 대해 사용자가 선택할 수 있는 항목을 지정합니다. 기본값은 en 입니다. 이 값은 화면 상의 텍스트가 사용자에게 적합한 언어로 표시되도록 현지화 키 집합을 사용자 세션에 매핑합니다.

사용자 기본 표준 시간대

이 필드는 사용자가 Access Manager 콘솔에 액세스하는 표준 시간대를 지정합니다. 기본값은 없습니다.

상속된 로캘

이 필드는 사용자의 로캘을 지정합니다. 기본값은 en_US 입니다. [283 페이지의 표 20-1](#)의 값을 사용할 수 있습니다.

관리자 DN 시작 보기

이 사용자가 Access Manager 관리자인 경우 이 필드는 이 사용자가 로그인했을 때 Access Manager 콘솔에 시작 지점으로 표시되는 노드를 지정합니다. 기본값은 없으며 사용자가 최소한 읽기 권한을 가진 유효한 DN 을 사용할 수 있습니다.

기본 사용자 상태

이 옵션은 새로 만든 사용자의 기본 상태를 나타냅니다. 이 상태는 사용자 항목 상태로 대체됩니다. 활성 사용자만 Access Manager 를 통해 인증될 수 있습니다. 기본값은 Active 입니다. 다음 중 하나를 풀다운 메뉴에서 선택할 수 있습니다.

- Active - 사용자가 Access Manager 를 통해 인증될 수 있습니다.
- Inactive - 사용자가 Access Manager 를 통해 인증될 수 없지만 사용자 프로파일은 디렉토리에 저장된 상태로 남습니다.

개별 사용자 상태는 사용자 서비스를 등록하고 값을 선택하여 역할에 적용한 다음 역할을 사용자 프로필에 추가하여 설정합니다.

사용자 프로필 속성

사용자 프로필 속성은 사용자 프로필의 기본 속성입니다. 이러한 값은 관리자나 사용자가 로그인 시 사용자 프로필 보기에서 설정합니다. 관리자는 고유한 사용자 속성을 사용자 프로필에 추가하거나 새 서비스를 만들 수 있습니다. 자세한 내용은 *Access Manager Developer's Guide* 를 참조하십시오.

주 Access Manager에서는 사용자 항목 내의 속성이 고유할 필요가 없습니다. 예를 들어, userA와 userB를 동일한 조직에서 만들어 둘 다에 대해 전자 메일 주소 속성을 jimbo@madisonparc.com으로 설정할 수 있습니다. 관리자는 Sun Java System Directory Server의 속성 고유성 플러그인을 구성하여 고유한 속성 값을 적용하도록 할 수 있습니다. 자세한 내용은 이 장의 끝에 있는 고유 사용자 아이디나 *Sun Java System Directory Server 관리자 설명서*를 참조하십시오.

이름

이 필드는 사용자의 이름을 가집니다. (이름 값과 성 값은 Access Manager 콘솔의 오른쪽 위 모서리에 있는 현재 로그인 필드의 사용자를 식별합니다.)

성

이 필드는 사용자의 성을 가집니다. 이름 값과 성 값은 Access Manager 콘솔의 오른쪽 위 모서리에 있는 현재 로그인 필드의 사용자를 식별합니다.

성명

이 필드는 사용자의 성명을 가집니다.

비밀번호

이 필드는 사용자 아이디 필드에 지정된 이름의 비밀번호를 가집니다.

비밀번호 (확인)

비밀번호를 확인합니다.

전자 메일 주소

이 필드는 사용자의 전자 메일 주소를 가집니다.

사원 번호

이 필드는 사용자의 사원 번호를 가집니다.

전화 번호

이 필드는 사용자의 전화 번호를 가집니다.

주소 (집)

이 필드는 사용자의 집 주소를 가질 수 있습니다.

사용자 상태

이 옵션은 사용자가 Access Manager 를 통해 인증될 수 있는지 여부를 나타냅니다. 활성화 사용자만 Access Manager 를 통해 인증될 수 있습니다. 기본값은 활성화 . 다음 중 하나를 풀다운 메뉴에서 선택할 수 있습니다 .

- 활성화 - 사용자가 Access Manager 를 통해 인증될 수 있습니다 .
- 비활성 - 사용자가 Access Manager 를 통해 인증될 수 없지만 사용자 프로필은 디렉토리에 저장된 상태로 남습니다 .

주 사용자 상태를 비활성으로 변경하는 것은 Access Manager 를 통한 인증에만 영향을 줍니다 . Directory Server 는 nsAccountLock 속성을 사용하여 사용자 계정 상태를 결정합니다 . Access Manager 인증에 대해 비활성화된 사용자 계정은 Access Manager 가 필요하지 않은 작업을 계속 수행할 수 있습니다 . 단순히 Access Manager 인증에 대해서가 아니라 디렉토리에서 사용자 계정을 비활성화하려면 nsAccountLock 값을 true 로 설정합니다 . 사이트의 위임된 관리자가 정기적으로 사용자를 비활성화할 경우 nsAccountLock 속성을 Access Manager 사용자 프로필 페이지에 추가하는 방법을 고려하십시오 . 자세한 내용은 *Access Manager Developer's Guide* 를 참조하십시오 .

계정 만료일

이 속성이 있으면 현재 날짜와 시간이 지정된 계정 만료일을 지난 경우 인증 서비스는 로그인을 허용하지 않습니다. 이 속성의 형식은 다음과 같습니다.

(yyyy/mm/dd hh:mm)

사용자 인증 구성

이 속성은 사용자의 인증 방법을 설정합니다. 기본 인증 방법은 LDAP입니다. 편집 링크를 눌러 하나 이상의 인증 방법을 선택할 수 있습니다. 여러 인증 방법을 선택할 경우 사용자는 선택된 모든 방법으로 성공적으로 인증되어야 할 수 있습니다.

사용자 별칭 목록

이 필드는 사용자에게 적용될 수 있는 별칭 목록을 정의합니다. 이 속성에 구성된 별칭을 사용하려면 LDAP 서비스의 사용자 항목 검색 속성 필드에 `iplanet-am-user-alias-list` 속성을 추가하여 LDAP 서비스를 수정해야 합니다.

기본 로케일

이 필드는 사용자의 로케일을 지정합니다. 기본값은 `en_us`입니다. [283 페이지의 표 20-1](#)의 값을 사용할 수 있습니다.

폴다운 메뉴에서 다음 속성 중 하나를 사용할 수 있습니다.

- 무시
- 사용자 정의
- 상속

성공 URL

이 필드는 성공적인 인증 후 사용자가 리디렉션되는 URL을 지정하는 다수의 값 목록을 허용합니다. 기본 HTML 유형을 가정하는 URL의 값만 지정할 수 있지만 이 속성의 형식은 `clientType|URL`입니다.

실패 URL

인증에 실패한 후 사용자가 리디렉션되는 URL 을 지정하는 다수의 값 목록을 허용합니다. 기본 HTML 유형을 가정한 URL 의 값만 지정할 수 있지만 이 속성의 형식은 `clientType|URL` 입니다.

고유 사용자 아이디

Access Manager 응용 프로그램 내에서 uid 고유성을 강제하려면 Directory Server 에서 사용할 수 있는 플러그 인을 다음과 같이 구성해야 합니다.

```
dn: cn=uid uniqueness,cn=plugins,cn=config
objectClass: top
objectClass: nsSlapdPlugin
objectClass: extensibleObject
cn: uid uniqueness
nsslapd-pluginPath: /ids908/lib/uid-plugin.so
nsslapd-pluginInitfunc: NSUniqueAttr_Init
nsslapd-pluginType: preoperation
nsslapd-pluginEnabled: on
nsslapd-pluginarg0: attribute=uid
nsslapd-pluginarg1: markerObjectClass=nsManagedDomain
nsslapd-plugin-depends-on-type: database
nsslapd-pluginId: NSUniqueAttr
nsslapd-pluginVersion: 6.1
nsslapd-pluginVendor: Sun | SunONE
nsslapd-pluginDescription: Enforce unique attribute values
```

`nsManagedDomain` 객체 클래스를 사용하여 uid 고유성을 강제하려는 조직을 표시하는 것이 좋습니다. 이 플러그 인은 기본적으로 사용 가능하지 않습니다.

조직별로 uid 의 고유성을 구성하려면 플러그 인 항목에서 각 조직에 대해 DN 을 추가하거나 표시자 객체 클래스 옵션을 사용하여 nsManagedDomain 을 각 최상위 수준 조직 항목에 추가합니다.

```
nsslapd-pluginEnabled: on  
nsslapd-pluginarg0: attribute=uid  
nsslapd-pluginarg1: markerObjectClass=nsManagedDomain
```

고유 사용자 아이디

오류 코드

이 부록은 Sun Java System Access Manager 에서 생성되는 오류 메시지의 목록을 제공합니다. 이 목록이 완벽하지는 않지만 이 장에 설명된 정보는 일반 문제의 해결을 위한 훌륭한 출발점으로서의 역할을 수행할 것입니다. 이 부록에 나열된 표에서는 오류 코드, 오류에 대한 설명 및 / 또는 가능한 원인을 제공하고 발생한 문제를 수정하기 위해 수행할 수 있는 작업에 대해 설명합니다.

이 부록에서는 기능적으로 다음과 같은 영역으로 구분하여 오류 코드를 나열합니다.

- [Access Manager 콘솔 오류](#)
- [인증 오류 코드](#)
- [정책 오류 코드](#)
- [amadmin 오류 코드](#)

오류 진단에 대한 도움이 필요한 경우 Sun 기술 지원부에 문의하십시오.

<http://www.sun.com/service/sunone/software/index.html>

Access Manager 콘솔 오류

다음 표에서는 Access Manager 콘솔에서 생성되고 표시되는 오류 코드에 대해 설명합니다.

표 A-1 Access Manager 콘솔 오류

오류 메시지	설명 / 가능한 원인	작업
다음을 삭제하는 중 오류가 발생했습니다.	현재 사용자가 객체를 제거하기 이전에 다른 사용자가 해당 객체를 제거할 수 있습니다.	삭제할 객체를 다시 표시하고 작업을 다시 수행하십시오.

표 A-1 Access Manager 콘솔 오류

오류 메시지	설명 / 가능한 원인	작업
잘못된 URL 을 입력했습니다 .	이 메시지는 Access Manager 콘솔 창에 대한 URL 을 잘못 입력한 경우에 발생합니다 .	
검색 기준과 일치하는 항목이 없습니다 .	검색 창 또는 필터 필드에 입력한 매개 변수가 디렉토리에 있는 객체와 일치하지 않습니다 .	다른 매개 변수 집합을 사용하여 검색을 다시 실행하십시오 .
표시할 속성이 없습니다 .	선택된 객체의 스키마에 편집 가능한 속성이 정의되어 있지 않습니다 .	
이 서비스에 대해 표시할 정보가 없습니다 .	서비스 구성 모듈에서 표시되는 서비스에 전역 또는 조직 기반 속성이 없습니다 .	
검색 크기 제한을 초과했습니다 . 검색 조건을 구체화하십시오 .	검색에 지정된 매개 변수가 허용된 것보다 더 많은 항목을 반환했습니다 .	관리 서비스의 검색에서 반환되는 최대 결과 수 속성을 더 큰 값으로 수정해야 합니다 . 검색 매개 변수를 보다 제한적으로 수정할 수도 있습니다 .
검색 시간 제한을 초과했습니다 . 검색 조건을 구체화하십시오 .	지정된 매개 변수에 대한 검색 작업이 허용된 검색 시간보다 더 오래 걸립니다 .	관리 서비스에서 검색 시간 초과 속성을 더 큰 값으로 수정해야 합니다 . 많은 값을 반환하도록 검색 매개 변수를 덜 제한적으로 수정할 수도 있습니다 .
사용자 시작 위치가 유효하지 않습니다 . 관리자에게 문의하십시오 .	사용자 항목의 시작 위치 DN 이 더 이상 유효하지 않습니다 .	사용자 프로필 페이지에서 시작 DN 값을 유효한 DN 으로 변경합니다 .
<i>identity</i> 객체를 만들지 못했습니다 . 사용자에게 충분한 액세스 권한이 없습니다 .	충분한 권한이 없는 사용자가 작업을 실행했습니다 . 사용자가 정의한 권한에 따라 해당 사용자가 수행할 수 있는 작업이 결정됩니다 .	

인증 오류 코드

다음 표에서는 인증 서비스에서 생성되는 오류 코드에 대해 설명합니다 . 이러한 오류는 인증 모듈에서 사용자 / 관리자에게 표시됩니다 .

표 A-2 인증 오류 코드

오류 메시지	설명 / 가능한 원인	작업
authentication.already.login.	사용자가 이미 로그인했고 유효한 세션이 있지만 성공 URL 리디렉션이 정의되어 있지 않습니다.	로그아웃을 수행하거나, Access Manager 콘솔을 통해 일부 로그인 성공 리디렉션 URL을 설정합니다. "goto" 쿼리 매개 변수를 해당 값과 함께 관리 콘솔 URL로 사용합니다.
logout.failure.	사용자가 Access Manager 에서 로그아웃할 수 없습니다.	서버를 다시 시작합니다.
uncaught_exception	처리가 잘못되어 인증 예외가 발생했습니다.	로그인 URL 에 잘못된 문자 또는 특수 문자가 있는지 확인합니다.
redirect.error	Access Manager 가 성공 또는 실패 리디렉션 URL 에 리디렉션할 수 없습니다.	웹 컨테이너의 오류 로그에서 오류가 있는지 확인합니다.
gotoLoginAfterFail	이 링크는 대부분의 오류가 발생할 때 생성됩니다. 이 링크를 누르면 원본 로그인 URL 페이지로 이동합니다.	
invalid.password	입력한 비밀번호가 잘못되었습니다.	비밀번호는 8 자 이상이어야 합니다. 비밀번호의 문자 수가 적절한지 확인하고 비밀번호가 만료되지 않았는지 확인합니다.
auth.failed	인증에 실패했습니다. 기본 로그인 실패 템플릿에 표시되는 일반적인 오류 메시지입니다. 가장 일반적인 원인은 유효하지 않은 / 잘못된 자격 증명입니다.	유효하며 올바른 아이디 / 비밀번호 (호출된 인증 모듈에 필요한 자격 증명) 를 입력합니다.
nouser.profile	지정된 조직에 입력한 아이디와 일치하는 사용자 프로필이 없습니다. 이 오류는 구성원 / 자동 등록 인증 모듈에 로그인할 때 표시됩니다.	로그인 정보를 다시 입력합니다. 첫 번째 로그인 시도인 경우 로그인 화면에서 새 사용자를 선택하십시오.
notenough.characters	입력한 비밀번호의 길이가 짧습니다. 이 오류는 구성원 / 자동 등록 인증 모듈에 로그인할 때 표시됩니다.	로그인 비밀번호는 기본적으로 8 자 이상이어야 합니다. 이 수는 구성원 인증 모듈을 통해 구성 가능합니다.
useralready.exists	지정된 조직에 이 이름을 사용하는 사용자가 이미 있습니다. 이 오류는 구성원 / 자동 등록 인증 모듈에 로그인할 때 표시됩니다.	사용자 아이디는 조직 내에서 고유해야 합니다.

표 A-2 인증 오류 코드

오류 메시지	설명 / 가능한 원인	작업
uidpasswd.same	사용자 이름 및 비밀번호 필드에 동일한 값을 사용할 수 없습니다. 이 오류는 구성원 / 자동 등록 인증 모듈에 로그인할 때 표시됩니다.	아이디 및 비밀번호가 다른지 확인합니다.
nouser.name	아이디를 입력하지 않았습니다. 이 오류는 구성원 / 자동 등록 인증 모듈에 로그인할 때 표시됩니다.	아이디를 입력하십시오.
no.password	비밀번호를 입력하지 않았습니다. 이 오류는 구성원 / 자동 등록 인증 모듈에 로그인할 때 표시됩니다.	비밀번호를 입력하십시오.
missing.confirm.passwd	비밀번호 확인 필드가 없습니다. 이 오류는 구성원 / 자동 등록 인증 모듈에 로그인할 때 표시됩니다.	비밀번호 확인 필드에 비밀번호를 입력하십시오.
password.mismatch	비밀번호와 확인용 비밀번호가 일치하지 않습니다. 이 오류는 구성원 / 자동 등록 인증 모듈에 로그인할 때 표시됩니다.	비밀번호와 확인용 비밀번호가 일치하는지 확인합니다.
사용자 프로필을 저장하는 중 오류가 발생했습니다.	사용자 프로필을 저장하는 중 오류가 발생했습니다. 이 오류는 구성원 / 자동 등록 인증 모듈에 로그인할 때 표시됩니다.	Membership.xml 파일에서 속성 및 요소가 자동 등록에 유효한지 확인합니다.
originative	이 조직이 활성 상태가 아닙니다.	Access Manager 콘솔을 통해 조직 상태를 inactive에서 active로 변경하여 조직을 활성화합니다.
internal.auth.error	내부 인증 오류입니다. 서로 다른 여러 환경 및 / 또는 구성 문제로 인해 발생할 수 있는 일반 인증 오류입니다.	
usernot.active	사용자가 더 이상 활성 상태가 아닙니다.	관리 콘솔을 통해 사용자 상태를 inactive에서 active로 변경하여 사용자를 활성화합니다. 메모리 잠금에 의해 사용자가 잠긴 경우 서버를 다시 시작하십시오.
user.not.inrole	사용자가 지정된 역할에 속하지 않습니다. 이 오류는 역할 기반 인증 중에 표시됩니다.	로그인 사용자가 역할 기반 인증에 지정된 역할에 속하는지 확인합니다.
session.timeout	사용자 세션이 시간 초과되었습니다.	다시 로그인합니다.

표 A-2 인증 오류 코드

오류 메시지	설명 / 가능한 원인	작업
authmodule.denied	지정한 인증 모듈이 거부되었습니다.	요청한 인증 모듈이 요구된 조직에 등록되어 있고, 모듈에 대한 템플릿이 생성 및 저장되어 있으며, 핵심 인증 모듈의 조직 인증 모듈 목록에서 해당 모듈이 선택되어 있는지 확인합니다.
noconfig.found	구성이 없습니다.	요청한 인증 방법에 대한 인증 구성 서비스를 확인합니다.
cookie.notpersistent	영구 쿠키 사용자 이름이 영구 쿠키 도메인에 없습니다.	
nosuch.domain	조직이 있습니다.	요청된 조직이 유효하고 올바른지 확인합니다.
userhasnoprofile.org	지정된 조직에 사용자의 프로필이 없습니다.	로컬 Directory Server에서 사용자가 있으며 지정된 조직에 유효한지 확인합니다.
reqfield.missing	필수 필드 중 하나를 입력하지 않았습니다. 모든 필수 필드에 입력했는지 확인하십시오.	모든 필수 필드를 입력하십시오.
session.max.limit	최대 세션 제한에 도달했습니다.	로그아웃한 다음 다시 로그인합니다.

정책 오류 코드

다음 표에서는 정책 프레임워크에서 생성되고 Access Manager 콘솔에 표시되는 오류 코드에 대해 설명합니다.

표 A-3 정책 오류 코드

오류 메시지	설명 / 가능한 원인	작업
illegal_character_in_name	정책 이름에 잘못된 문자 "/" 가 있습니다.	정책 이름에 "/" 문자가 있는지 확인합니다.
policy_already_exists_in_org	동일한 이름의 규칙이 이미 있습니다.	정책 작성에 다른 이름을 사용하십시오.

표 A-3 정책 오류 코드

오류 메시지	설명 / 가능한 원인	작업
rule_name_already_present	지정된 이름을 갖는 다른 규칙이 이미 있습니다 .	정책 작성에 다른 규칙 이름을 사용하십시오 .
rule_already_present	동일한 이름 값을 갖는 규칙이 이미 있습니다 .	다른 규칙 값을 사용하십시오 .
no_referral_can_not_create_policy	조직에 참조가 없습니다 .	하위 조직에서 정책을 만들려면 상위 조직에서 참조 정책을 만들어 이 하위 조직에서 참조할 수 있는 자원을 나타내야 합니다 .
ldap_search_exceed_size_limit	LDAP 검색 크기 제한을 초과했습니다 . 검색에서 최대 결과 수보다 더 많은 결과를 찾았기 때문에 오류가 발생했습니다 .	검색 제어 매개 변수에 대한 조직의 검색 패턴 또는 정책 구성을 변경하십시오 . 검색 크기 제한은 정책 구성 서비스에 있습니다 .
ldap_search_exceed_time_limit	LDAP 검색 시간 제한을 초과했습니다 . 검색에서 최대 결과 수보다 더 많은 결과를 찾았기 때문에 오류가 발생했습니다 .	검색 제어 매개 변수에 대한 조직의 검색 패턴 또는 정책 구성을 변경하십시오 . 검색 시간 제한은 정책 구성 서비스에 있습니다 .
ldap_invalid_password	LDAP 바인드 비밀번호가 잘못되었습니다 .	정책 구성에 정의된 LDAP 바인드 사용자에게 대한 비밀번호가 잘못되었습니다 . 인증된 LDAP 연결을 구성하여 정책 작업을 수행할 수 없습니다 .
app_sso_token_invalid	응용 프로그램 SSO 토큰이 잘못되었습니다 .	서버에서 응용 프로그램 SSO 토큰을 검증하지 못했습니다 . SSO 토큰이 만료되었을 수 있습니다 .
user_sso_token_invalid	사용자 SSO 토큰이 잘못되었습니다 .	서버에서 사용자 SSO 토큰을 검증하지 못했습니다 . SSO 토큰이 만료되었을 수 있습니다 .
property_is_not_an_Integer	등록 정보 값이 정수가 아닙니다 .	이 플러그 인 등록 정보 값은 정수이어야 합니다 .
property_value_not_defined	등록 정보 값을 정의해야 합니다 .	지정된 등록 정보에 대한 값을 제공하십시오 .
start_ip_can_not_be_greater_than_end_ip	시작 IP 가 끝 IP 보다 더 큼니다 .	끝 IP 주소를 IP 주소 조건의 시작 IP 주소보다 더 크게 설정하려고 시도했습니다 . 시작 IP 가 끝 IP 보다 크지 않아야 합니다 .
start_date_can_not_be_larger_than_end_date	시작 날짜가 종료 날짜보다 더 큼니다 .	종료 날짜를 정책 시간 조건의 시작 날짜보다 더 크게 설정하려고 시도했습니다 . 시작 날짜가 종료 날짜보다 크지 않아야 합니다 .

표 A-3 정책 오류 코드

오류 메시지	설명 / 가능한 원인	작업
policy_not_found_in_organization	조직에 정책이 없습니다. 조직에서 존재하지 않는 정책을 찾는 중 오류가 발생했습니다.	정책이 지정된 조직에 있는지 확인합니다.
insufficient_access_rights	사용자에게 충분한 액세스 권한이 없습니다. 사용자에게 정책 작업 수행을 위한 충분한 권한이 없습니다.	적절한 액세스 권한이 있는 사용자가 정책 작업을 수행합니다.
invalid_ldap_server_host	LDAP 서버 호스트가 잘못되었습니다.	정책 구성 서비스에 입력한 잘못된 LDAP 서버 호스트를 변경합니다.

amadmin 오류 코드

다음 표에서는 amadmin 명령줄 도구에 의해 Access Manager 의 디버그 파일에 생성되는 오류 코드를 설명합니다.

표 A-4 amadmin 오류 코드

오류 메시지	코드	설명 / 가능한 원인	작업
nocomptype	1	인수가 너무 적습니다.	필수 인수 (--runasdn, --password, --passwordfile, --schema, --data, 및 --addAttributes) 및 해당 값을 명령줄에 입력했는지 확인합니다.
파일	2	입력 XML 파일이 없습니다.	구문을 확인하고 입력 XML 이 유효한지 확인합니다.
nodnforadmin	3	--runasdn 값에 대한 사용자 DN 이 없습니다.	사용자 DN 을 --runasdn 에 대한 값으로 제공합니다.
noservicename	4	--deleteservice 값에 대한 서비스 이름이 없습니다.	서비스 이름을 --deleteservice 에 대한 값으로 제공합니다.
nopwdforadmin	5	--password 값에 대한 비밀번호가 없습니다.	비밀번호를 --password 에 대한 값으로 제공합니다.
nocalename	6	로컬 이름을 지정하지 않았습니다. 로컬은 en_US 를 기본값으로 사용합니다.	로컬 목록은 기본 인증 로컬을 참조하십시오.
nofile	7	XML 입력 파일이 없습니다.	처리할 입력 XML 파일 이름을 하나 이상 지정하십시오.

표 A-4 amadmin 오류 코드

오류 메시지	코드	설명 / 가능한 원인	작업
invopt	8	하나 이상의 인수가 잘못되었습니다.	모든 인수가 유효한지 확인합니다. 유효한 인수 집합을 보려면 <code>amadmin --help</code> 를 입력하십시오.
oprfailed	9	작업에 실패했습니다.	<code>amadmin</code> 이 실패할 경우 세부적인 오류 코드를 생성하여 특정 오류를 나타냅니다. 이러한 오류 코드를 참조하여 문제를 평가하십시오.
execfailed	10	요청을 처리할 수 없습니다.	<code>amadmin</code> 이 실패할 경우 세부적인 오류 코드를 생성하여 특정 오류를 나타냅니다. 이러한 오류 코드를 참조하여 문제를 평가하십시오.
policycreatexception	12	정책을 만들 수 없습니다.	<code>amadmin</code> 은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
policydelexception	13	정책을 삭제할 수 없습니다.	<code>amadmin</code> 은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
smsdelexception	14	서비스를 삭제할 수 없습니다.	<code>amadmin</code> 은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
ldapauthfail	15	사용자를 인증할 수 없습니다.	사용자 DN 및 비밀번호가 올바른지 확인합니다.
parsererror	16	입력 XML 파일을 구문 분석할 수 없습니다.	XML 이 올바르게 서식 지정되어 있고 <code>amAdmin.dtd</code> 를 준수하는지 확인합니다.
parseiniterror	17	응용 프로그램 오류 또는 구문 분석기 초기화 오류로 인해 구문 분석할 수 없습니다.	XML 이 올바르게 서식 지정되어 있고 <code>amAdmin.dtd</code> 를 준수하는지 확인합니다.
parsebuilterror	18	지정한 옵션으로 구문 분석기를 만들 수 없기 때문에 구문 분석할 수 없습니다.	<code>amadmin</code> 은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
ioexception	19	입력 XML 파일을 읽을 수 없습니다.	<code>amadmin</code> 은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.

표 A-4 amadmin 오류 코드

오류 메시지	코드	설명 / 가능한 원인	작업
fatalvalidationerror	20	XML 파일이 유효한 파일이 아니기 때문에 구문 분석할 수 없습니다.	구문을 확인하고 입력 XML 이 유효한지 확인합니다.
nonfatalvalidationerror	21	XML 파일이 유효한 파일이 아니기 때문에 구문 분석할 수 없습니다.	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
validwarn	22	파일에 대한 XML 파일 검증 경고	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
failedToProcessXML	23	XML 파일을 처리할 수 없습니다.	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
nodataschemawarning	24	--data 및 --schema 옵션이 명령에 없습니다.	모든 인수가 유효한지 확인합니다. 유효한 인수 집합을 보려면 amadmin --help를 입력하십시오.
doctyperror	25	XML 파일이 올바른 DTD를 따르지 않습니다.	XML 파일의 DOCTYPE 요소를 확인하십시오.
statusmsg9	26	DN, 비밀번호, 호스트 이름 또는 포트 번호가 잘못되었기 때문에 LDAP 인증에 실패했습니다.	사용자 DN 및 비밀번호가 올바른지 확인합니다.
statusmsg13	28	서비스 관리자 예외 (SSO 예외)	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
statusmsg14	29	서비스 관리자 예외	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
statusmsg15	30	스키마 파일 입력 스트림 예외	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
statusmsg30	31	정책 관리자 예외 (SSO 예외)	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.

표 A-4 amadmin 오류 코드

오류 메시지	코드	설명 / 가능한 원인	작업
statusmsg31	32	정책 관리자 예외	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
dbugerror	33	여러 디버그 옵션을 지정했습니다.	디버그 옵션은 하나만 지정해야 합니다.
loginFailed	34	로그인에 실패했습니다.	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
levelerr	36	속성 값이 잘못되었습니다.	LDAP 검색에 대한 수준 설정을 확인합니다. SCOPE_SUB 또는 SCOPE_ONE 이어야 합니다.
failToGetObjType	37	객체 유형을 가져오는 중 오류가 발생했습니다.	XML 파일의 DN 이 유효하며 올바른 객체 유형을 포함하는지 확인합니다.
invalidOrgDN	38	조직 DN 이 잘못되었습니다.	XML 파일의 DN 이 유효하고 조직 객체인지 확인합니다.
invalidRoleDN	39	역할 DN 이 잘못되었습니다.	XML 파일의 DN 이 유효하고 역할 객체인지 확인합니다.
invalidStaticGroupDN	40	정적 그룹 DN 이 잘못되었습니다.	XML 파일의 DN 이 유효하고 정적 그룹 객체인지 확인합니다.
invalidPeopleContainerDN	41	사용자 컨테이너 DN 이 잘못되었습니다.	XML 파일의 DN 이 유효하고 사용자 컨테이너 객체인지 확인합니다.
invalidOrgUnitDN	42	조직 구성 단위 DN 이 잘못되었습니다.	XML 파일의 DN 이 유효하고 컨테이너 객체인지 확인합니다.
invalidServiceHostName	43	서비스 호스트 이름이 잘못되었습니다.	유효한 세션 검색을 위한 호스트 이름이 올바른지 확인합니다.
subschemaexception	44	하위 스키마 오류	하위 스키마는 전역 및 조직 속성에만 지원됩니다.
serviceschemaexception	45	서비스에 대한 서비스 스키마를 찾을 수 없습니다.	XML 파일에서 하위 스키마가 유효한지 확인합니다.
roletemplateexception	46	역할 템플릿은 스키마가 동적 유형인 경우에만 true 일 수 있습니다.	XML 파일에서 역할 템플릿이 유효한지 확인합니다.
cannotAddusersToFilteredRole	47	필터링된 역할에 사용자를 추가할 수 없습니다.	XML 파일의 역할 DN 이 필터링된 역할이 아닌지 확인합니다.
templateDoesNotExist	48	템플릿이 없습니다.	XML 파일에서 서비스 템플릿이 유효한지 확인합니다.

표 A-4 amadmin 오류 코드

오류 메시지	코드	설명 / 가능한 원인	작업
cannotAddUsersToDynamicGroup	49	동적 그룹에 사용자를 추가할 수 없습니다.	XML 파일의 그룹 DN 이 동적 그룹이 아닌지 확인합니다.
cannotCreatePolicyUnderContainer	50	컨테이너의 하위 조직인 조직에서 정책을 만들 수 없습니다.	정책을 만들 조직이 컨테이너의 하위 조직이 아닌지 확인합니다.
defaultGroupContainerNotFound	51	그룹 컨테이너가 없습니다.	상위 조직 또는 컨테이너에 대해 그룹 컨테이너를 만듭니다.
cannotRemoveUserFromFilteredRole	52	필터링된 역할에서 사용자를 제거할 수 없습니다.	XML 파일의 역할 DN 이 필터링된 역할이 아닌지 확인합니다.
cannotRemoveUsersFromDynamicGroup	53	동적 그룹에서 사용자를 제거할 수 없습니다.	XML 파일의 그룹 DN 이 동적 그룹이 아닌지 확인합니다.
subSchemaStringDoesNotExist	54	하위 스키마 문자열이 없습니다.	XML 파일에 하위 스키마 문자열이 있는지 확인합니다.
defaultPeopleContainerNotFound	59	조직 또는 컨테이너에 사용자를 추가하려고 합니다. 그런데 기본 사용자 컨테이너가 조직 또는 컨테이너에 존재하지 않습니다.	기본 사용자 컨테이너가 존재하는지 확인해야 합니다.
nodefaulturlprefix	60	--defaultURLPrefix 인수 다음에 기본 URL 접두어가 없습니다.	기본 URL 접두어를 제공합니다.
nometaalias	61	--metaalias 인수 다음에 메타 별칭이 없습니다.	메타 별칭을 제공합니다.
missingEntityName	62	엔티티 이름이 지정되어 있지 않습니다.	엔티티 이름을 제공합니다.
missingLibertyMetaInputFile	63	메타 데이터를 가져오기 위한 파일 이름이 빠져 있습니다.	메타 데이터가 포함된 파일 이름을 제공합니다.
missingLibertyMetaOutputFile	64	내보낸 메타 데이터를 저장할 파일 이름이 빠져 있습니다.	메타 데이터를 저장할 파일 이름을 제공합니다.
cannotObtainMetaHandler	65	메타 속성에 대한 처리기를 가져올 수 없습니다. 지정된 사용자 이름과 비밀번호가 틀린 것일 수 있습니다.	사용자 이름과 비밀번호가 맞는지 확인합니다.
missingResourceBundleName	66	Directory Server 에 저장된 자원 번들을 추가하거나, 보거나 또는 삭제할 때 자원 번들 이름이 빠져 있습니다.	자원 번들 이름을 제공합니다.
missingResourceFileName	67	자원 번들을 Directory Server 에 추가할 때 자원 문자열이 포함된 파일의 이름이 빠져 있습니다.	유효한 파일 이름을 입력합니다.
failLoadLibertyMeta	68	Liberty 메타를 Directory Server 에 로드하는 데 실패했습니다.	다시 로드하기 전에 메타 데이터를 다시 확인합니다.

amadmin 오류 코드

용어집

이 설명서 세트에 사용된 용어 목록은 최신 *Sun Java™ Enterprise System 용어집*을 참조하십시오 .

<http://docs.sun.com/doc/819-1934>

A

am.encrypted.pwd 등록 정보 48

am2bak 명령줄 도구 225
구문 225
백업 절차 227

amadmin 명령줄 도구 215
구문 216

amconfig 스크립트
구문 46
배포 시나리오 47
작업 33

AMConfig.properties 파일 48

AM_ENC_PWD 변수 48

ampasssword 명령줄 도구 231
SSL 에서 실행 232
구문 231

amsamplesilent 파일 32

amsecuridd 도우미 46
구문 238

amserver 명령줄 도구 223
구문 223

amserver 스크립트 46

amserver.instance 스크립트 46

amunixd 도우미 46

Application Server
구성 변수 40, 41
지원 40, 41

arg 로그인 URL 매개 변수 136

authlevel 로그인 URL 매개 변수 137

B

bak2am 명령줄 도구 229
구문 229

BEA WebLogic Server
구성 변수 42
지원 33

C

CRL 업데이트용 HTTP 매개 변수 273

CRL 에 인증서 일치 272

D

DC 노드 속성 목록 251

DEPLOY_LEVEL 변수 35

domain 로그인 URL 매개 변수 137

DSAME 콘솔
데이터 표시 영역 72

DTD 파일
policy.dtd 112

E

Event Listener 클래스 259

F

FQDN 매핑
및 인증 166

G

- goto 로그인 URL 매개 변수 133
- gotoOnFail 로그인 URL 매개 변수 133

H

- HTTP 기본 인증 182
 - 등록 및 사용 182, 197
 - 로그인 183, 198
- HTTP 기본 인증 속성 289
 - 조직 속성
 - 인증 수준 289

I

- IBM WebSphere
 - 지원 33
- Identity Server
 - 설치 개요 32
 - 콘솔 71
- Identity Server SDK, 배포 33
- Identity Server 객체 관리 74
- Identity Server 인스턴스 구성 해제 50
- Identity Server 인스턴스 재구성 49
- Identity Server 인스턴스 제거 50
- Identity Server 콘솔
 - 위치 표시 영역
 - 검색 링크 72
 - 도움말 링크 72
 - 로그아웃 72
 - 모듈 71
 - 위치 필드 72
 - 환영합니다 72
- 탐색 표시 영역 72

- Identity 관리 71
 - Identity 관리 인터페이스 74
 - Identity 관리 보기 73
 - 사용자 프로필 보기 73
 - Properties 73
 - 그룹 76
 - 가입에 의한 구성원 77
 - 관리 대상 그룹 만들기 77
 - 동적 그룹 245
 - 정적 그룹 245
 - 정책에 추가 80
 - 필터링된 그룹 245
 - 필터링에 의한 구성원 77
 - 그룹 컨테이너 97
 - 만들기 97
 - 삭제 97
 - 사용자 80
 - 만들기 80
 - 삭제 82
 - 서비스, 역할 및 그룹에 추가 81
 - 정책에 추가 82
 - 사용자 컨테이너 96
 - 만들기 96
 - 삭제 96
 - 서비스 83
 - 등록 83
 - 제거 84
 - 템플릿 만들기 83
 - 에이전트 94
 - 삭제 94
 - 역할 84
 - 만들기 85
 - 사용자 제거 91
 - 사용자 추가 87
 - 삭제 93
 - 정책에 추가 91, 93
 - 정책 93
 - 조직 74
 - 만들기 74
 - 삭제 76
 - 정책에 추가 76
 - 컨테이너 95
 - 만들기 95

삭제 95
 IDTokenN 138
 IDTokenN 로그인 URL 매개 변수 138
 iPSPCookie 로그인 URL 매개 변수 137

J

Java Enterprise System 설치 프로그램 32, 47
 JDBC URL 294
 JDBC 드라이버 294
 JDBC 인증 속성
 조직 속성
 JDBC URL 294
 JDBC 드라이버 294
 데이터베이스에 연결할 사용자 294
 연결 유형 292
 연결 풀 JNDI 이름 292
 인증 수준 295
 JSP 디렉토리 이름 256

L

LDAP SSL 사용 가능 374
 LDAP 검색 시 사용되는 주제 DN 속성 272
 LDAP 그룹 검색 범위 372
 LDAP 그룹 검색 속성 373
 LDAP 그룹 검색 필터 372
 LDAP 기본 DN 371
 LDAP 디렉토리 인증 185
 등록 및 사용 185
 로그인 186
 파일오버 사용 186
 LDAP 바인드 DN 370
 LDAP 바인드 비밀번호 371

LDAP 사용자 검색 범위 372
 LDAP 사용자 검색 속성 373
 LDAP 사용자 검색 필터 372
 LDAP 서버 기본 비밀번호 274
 LDAP 서버 기본 사용자 274
 LDAP 서버 및 포트 370
 LDAP 시작 검색 DN 274
 LDAP 액세스에 SSL 사용 275
 LDAP 역할 검색 범위 373
 LDAP 역할 검색 속성 373
 LDAP 역할 검색 필터 372
 LDAP 연결 풀 최대 크기 374
 LDAP 연결 풀 최소 크기 374
 LDAP 연결 풀 크기 278
 LDAP 인증
 다중 구성 168
 LDAP 인증 속성 297
 조직 속성
 SSL 이 LDAP 서버에 액세스 가능 301
 검색 범위 300
 루트 사용자 바인드용 비밀번호 299, 306
 루트 사용자 바인드의 DN 299
 보조 LDAP 서버 298
 사용자 검색 필터 300
 사용자 검색을 시작할 DN 299
 사용자 프로필 검색 시 사용되는 LDAP 속성 300
 인증 수준 289, 302, 312, 325
 인증될 사용자 검색 시 사용되는 LDAP 속성 300
 인증할 사용자 DN 반환 301
 주 LDAP 서버 298
 LDAP 조직 검색 범위 371
 LDAP 조직 검색 속성 373
 LDAP 조직 검색 필터 371
 LDAP 에서 CRL 검색 시 사용되는 발급자 DN 속성 272

LDAP 에서 인증서 일치 [272](#)
Linux 시스템 , 기본 설치 디렉토리 [32](#)
locale 로그인 URL 매개 변수 [135](#)

M

module 로그인 URL 매개 변수 [136](#)
MSISDN 인증 속성 [309](#)

N

notBefore 시간에 대한 명제 비대칭 요소 [379](#)
NT Samba 구성 파일 이름 [314](#)
NT 모듈 인증 수준 [314](#), [334](#)
NT 인증 [190](#)

- 등록 및 사용 [191](#)
- 로그인 [191](#)
- 조직 속성
 - NT Samba 구성 파일 이름 [314](#)
 - NT 모듈 인증 수준 [314](#), [334](#)
 - NT 인증 도메인 [314](#)
 - NT 인증 호스트 [314](#)

NT 인증 도메인 [314](#)
NT 인증 속성 [313](#)
NT 인증 호스트 [314](#)
N 회 실패 후 사용자에게 경고 [285](#), [361](#)

O

OCSF 검증 사용 가능 [273](#)
org 로그인 URL 매개 변수 [134](#)

P

Policy [105](#)

- 일반 정책 [109](#)
 - 규칙 추가 [120](#)
 - 수정 [120](#)
 - 조건 추가 [124](#)
- 참조 정책 [111](#)
 - 수정 [126](#)
 - 참조 추가 [127](#)
- 피어 및 하위 조직에 대해 만들기 [119](#)

policy.dtd [112](#)
Properties [73](#)

R

RADIUS 공유 비밀 [318](#)
RADIUS 서버 1 [317](#)
RADIUS 서버 2 [318](#)
RADIUS 서버 인증 [192](#)

- 등록 및 사용 [192](#)
- 로그인 [193](#)

RADIUS 서버 포트 [318](#)
RADIUS 인증 속성 [317](#)

- 조직 속성
 - RADIUS 공유 비밀 [318](#)
 - RADIUS 서버 1 [317](#)
 - RADIUS 서버 2 [318](#)
 - RADIUS 서버 포트 [318](#)
 - 시간 초과 [318](#)
 - 인증 수준 [318](#)

role 로그인 URL 매개 변수 [134](#)

S

- SafeWord EASSP 버전 323
- SafeWord 로그 파일 322
- SafeWord 로깅 사용 가능 322
- SafeWord 로깅 수준 322
- SafeWord 모듈 인증 수준 324
- SafeWord 서버 322
- SafeWord 서버 검증 파일 디렉토리 322
- SafeWord 인증 194
 - 등록 및 사용 194
 - 로그인 195
- SafeWord 인증 속성
 - 조직 속성
 - SafeWord EASSP 버전 323
 - SafeWord 로그 파일 322
 - SafeWord 로깅 사용 가능 322
 - SafeWord 로깅 수준 322
 - SafeWord 모듈 인증 수준 324
 - SafeWord 서버 322
 - SafeWord 서버 검증 파일 디렉토리 조직 속성
 - SafeWord 서버 검증 파일 디렉토리 322**
 - SafeWord 인증 연결 시간 초과 323
 - SafeWord 최소 인증 강도 323
 - SafeWord 클라이언트 유형 323
- SafeWord 인증 연결 시간 초과 323
- SafeWord 최소 인증 강도 323
- SafeWord 클라이언트 유형 323
- SAML SOAP 서비스 URL 355
- SAML 명제 관리자 서비스 URL 355
- SAML 속성 377
 - 전역 속성
 - notBefore 시간에 대한 명제 비대칭 요소 379
 - SAML 아티팩트 이름 378
 - SAML 요청에 서명 378
 - SAML 응답에 서명 378
 - 대상 URL 에 POST 383
 - 대상 지정자 379
 - 명제 시간 초과 379
 - 사이트 아이디 및 사이트 발급자 이름 378
 - 서명 명제 378
 - 신뢰할 수 있는 파트너 사이트 379
 - 아티팩트 시간 초과 379
- SAML 아티팩트 이름 378
- SAML 요청에 서명 378
- SAML 웹 프로파일 /POST 서비스 URL 355
- SAML 웹 프로파일 / 아티팩트 서비스 URL 355
- SAML 응답에 서명 378
- SAML 인증 속성 325
 - 조직 속성
 - 인증 수준 325
- SecurID ACE/ 서버 구성 경로 327
- SecurID 도우미 구성 포트 328
- SecurID 도우미 인증 포트 328
- SecurID 인증 198
 - 등록 및 사용 199
 - 로그인 199
- SecurID 인증 속성 327
 - 조직 속성
 - SecurID ACE/ 서버 구성 경로 327
 - SecurID 도우미 구성 포트 328
 - SecurID 도우미 인증 포트 328
 - 인증 수준 328
- service 로그인 URL 매개 변수 136
- Solaris 시스템 , 기본 설치 디렉토리 32
- SSL
 - Identity Server 구성 53
- SSL 이 AD 서버에 액세스 가능
 - 활성 디렉토리 인증 265
- SSL 이 LDAP 서버에 액세스 가능
 - LDAP 인증 301
 - 회원 인증 307

U

- Unix 도우미 구성 포트 330
- Unix 도우미 스레드 330
- Unix 도우미 시간 초과 330
- Unix 도우미 인증 포트 330
- Unix 인증 200
 - 등록 및 사용 201
 - 로그인 202, 206
- Unix 인증 속성 329
 - 전역 속성
 - Unix 도우미 구성 포트 330
 - Unix 도우미 스레드 330
 - Unix 도우미 시간 초과 330
 - Unix 도우미 인증 포트 330
 - 조직 속성
 - Unix 모듈 인증 수준 330
- user 로그인 URL 매개 변수 134

V

- VerifyArchive 명령줄 도구 235, 237
 - 구문 236

W

- Web Server
 - 구성 변수 39
 - 지원 39
- WEB_CONTAINER 변수 38
- WebLogic Server
 - 구성 변수 42
 - 지원 33
- WebSphere
 - 구성 변수 44

지원 33

- Windows 데스크탑 SSO 인증 202
 - 등록 및 사용 203

ㄱ

- 개요
 - 사용자 인터페이스
 - 로그인 URL 매개 변수 132
 - 인증
 - 로그인 URL 132
 - 정책 106
 - 정책 에이전트 107
 - 정책 프로세스 108
- 개요, Identity Server 설치 32
- 개인 질문 사용 가능 359
- 검색 링크 72
- 검색 범위
 - LDAP 인증 300
 - 활성 디렉토리 인증 265
 - 회원 인증 307
- 검색 시간 초과 374
- 검색 시간 초과 (초) 255
- 검색 필터 358
- 검색에서 반환되는 최대 결과 수 255
- 계정 잠금 157
 - 메모리 165
 - 물리적 164
- 고유 사용자 아이디 396
- 관리 대상 그룹 유형 245
- 관리 속성 243
 - 전역 속성 243
 - DC 노드 속성 목록 251
 - 관리 그룹 사용 가능 248
 - 관리 대상 그룹 유형 245

- 그룹 컨테이너 표시 245
- 기본 그룹 컨테이너 252
- 기본 사용자 컨테이너 251
- 기본 에이전트 컨테이너 252
- 기본 역할 권한 (ACI) 246
- 도메인 구성 요소 트리 사용 가능 247
- 동적 관리 역할 ACI 248
- 보기 메뉴에 컨테이너 표시 245
- 사용자 컨테이너 표시 244
- 사용자 프로필 서비스 클래스 250
- 삭제된 객체의 검색 필터 251
- 호환 사용자 삭제 사용 가능 248
- 조직 속성 252
 - Event Listener 클래스 259
 - JSP 디렉토리 이름 256
 - 검색 시간 초과 (초) 255
 - 검색에서 반환되는 최대 결과 수 255
 - 그룹 기본 사용자 컨테이너 253
 - 그룹 사용자 컨테이너 목록 253
 - 메뉴 항목 보기 255
 - 사용자 검색 반환 속성 257
 - 사용자 검색 키 256
 - 사용자 그룹 자동 가입 254
 - 사용자 삭제 알림 목록 258
 - 사용자 수정 알림 목록 258
 - 사용자 아이디 및 비밀번호 검증 플러그인 클래스 260
 - 사용자 작성 기본 역할 255
 - 사용자 작성 알림 목록 257
 - 사용자 프로필 디스플레이 옵션 254
 - 사용자 프로필 디스플레이 클래스 253
 - 사용자 프로필 페이지에 그룹 표시 254
 - 사용자 프로필 페이지에 역할 표시 254
 - 사전 처리 및 사후 처리 클래스 259
 - 온라인 도움말 문서 256
 - 외부 속성 불러오기 사용 가능 260
 - 최종 사용자 프로필 디스플레이 클래스 254
 - 페이지당 표시되는 최대 항목 259
 - 필수 서비스 256
- 관리자 DN 시작 보기 392
- 관리자 인증 구성 280
- 구성 가능한 로그 필드 349
- 구성 변수
 - Application Server 40, 41
 - BEA WebLogic Server 42
 - IBM WebSphere Server 44
 - Identity Server 35
 - Web Server 39
- 구성원 인증 속성 303
 - 조직 속성
 - SSL 이 LDAP 서버에 액세스 가능 307
 - 검색 범위 307
 - 기본 사용자 역할 304
 - 등록 후 사용자 상태 304
 - 루트 사용자 바인드의 DN 306
 - 보조 LDAP 서버 305
 - 사용자 검색 필터 306
 - 사용자 검색을 시작할 DN 305
 - 사용자 프로필 검색 시 사용되는 LDAP 속성 306
 - 인증 수준 308
 - 인증될 사용자 검색 시 사용되는 LDAP 속성 306
 - 인증에 사용자 DN 반환 307
 - 주 LDAP 서버 304
 - 최소 비밀번호 길이 304
- 국제화 설정 서비스 속성 345
- 규칙 추가 120
- 그룹 76
 - 가입에 의한 구성원 77
 - 관리 대상 그룹 만들기 77
 - 동적 그룹 245
 - 정적 그룹 245
 - 정책에 추가 80
 - 필터링된 그룹 245
 - 필터링에 의한 구성원 77
- 그룹 기본 사용자 컨테이너 253
- 그룹 사용자 컨테이너 목록 253
- 그룹 컨테이너 97
 - 만들기 97
 - 삭제 97
- 그룹 컨테이너 표시 245
- 기본 DN 358

색션 L

기본 LDAP 연결 풀 크기 [278](#)
기본 그룹 컨테이너 [252](#)
기본 사용자 상태 [392](#)
기본 사용자 역할 [304](#)
기본 사용자 컨테이너 [251](#)
기본 성공 로그인 URL [286](#)
기본 실패 로그인 URL [287](#)
기본 에이전트 컨테이너 [252](#)
기본 역할 권한 (ACI) [246](#)
기본 익명 아이디 [268](#)
기본 인증 로컬 [283](#)
기본 인증 수준 [288](#)
기본 클라이언트 유형 [344](#)

L

나중에 구성 옵션 , Java Enterprise System 설치 프로
그램 [32](#)
내역 파일 수 [348](#)

L

다음 로그인 시 반드시 비밀번호 변경 [360](#)
대상 URL 에 POST [383](#)
대상 지정자 [379](#)
데이터베이스 드라이버 이름 [349](#)
데이터베이스 사용자 비밀번호 [349](#)
데이터베이스 사용자 이름 [349](#)
데이터베이스에 연결할 비밀번호 [294](#)
데이터베이스에 연결할 사용자 [294](#)
데이터베이스의 비밀번호 열 [294](#)

도움말 링크 [72](#)
동적 관리 역할 ACI [248](#)
동적 그룹 [245](#)
동적 속성
관리자 DN 시작 보기 [392](#)
기본 사용자 상태 [392](#)
사용자 기본 로컬 [392](#)
사용자 기본 언어 [392](#)
사용자 기본 표준 시간대 [392](#)
최대 세션 시간 (분) [388](#)
최대 유휴 시간 (분) [388](#)
최대 캐싱 시간 (분) [388](#)
등록 후 사용자 상태 [304](#)

로그인

로그 서명 시간 [350](#)
로그 파일 위치 [348](#)
로그 확인 빈도 [350](#)
로그아웃 [72](#)
로그아웃 서비스 URL [364](#)
로그인 [132](#)
로그인 URL
사용자 기반 [150](#)
서비스 기반 [147](#)
역할 기반 [144](#)
조직 기반 [141](#)
로그인 서비스 URL [364](#)
로그인 성공 URL [338](#)
로그인 실패 URL [338](#)
로그인 실패 잠금 간격 [285](#)
로그인 실패 잠금 기간 [286](#)
로그인 실패 잠금 모드 사용 가능 [285](#)

로그인 실패 잠금 수 285

로깅 서비스 URL 354

로깅 속성 347

전역 속성

구성 가능한 로그 필드 349

내역 파일 수 348

데이터베이스 드라이버 이름 349

데이터베이스 사용자 비밀번호 349

데이터베이스 사용자 이름 349

로그 서명 시간 350

로그 파일 위치 348

로그 확인 빈도 350

로깅 유형 349

보안 로깅 사용 가능 350

아카이브당 파일 수 351

최대 레코드 수 350

최대 로그 크기 348

로깅 유형 349

루트 사용자 바인드용 비밀번호

LDAP 인증 299

회원 인증 306

루트 사용자 바인드의 DN

LDAP 인증 299

회원 인증 306

리디렉션 URL

사용자 기반 150

서비스 기반 148

역할 기반 145

인증 수준 기반 153

조직 기반 141

□

메뉴 항목 보기 255

명령줄 도구

am2bak 225

구문 225

백업 절차 227

amadmin 215

구문 216

ampasssword 231

SSL에서 실행 232

구문 231

amsecridd 도우미

구문 238

amserver 223

구문 223

bak2am 229

구문 229

VerifyArchive 235, 237

구문 236

명제 시간 초과 379

모듈 체이닝

인증 160

모든 사용자를 위한 사용자 컨테이너 282

ㅂ

바인드 DN 358

바인드 비밀번호 359

방법

인증 138

사용자 기반 150

서비스 기반 147

역할 기반 143

정책 기반 129

조직 기반 141

배포 시나리오, Identity Server 47

별칭 검색 속성 이름 282

보기 메뉴에 컨테이너 표시 245

보안 로깅 사용 가능 350

보조 LDAP 서버 298, 305

보조 활성화 Directory Server 262

비밀 문제 358

비밀번호 393

- 비밀번호 구문 변환에 사용할 클래스 295
- 비밀번호 변경 알림 옵션 359
- 비밀번호 암호화 키 48
- 비밀번호 재설정 사용 가능 359
- 비밀번호 재설정 서비스 속성 357
 - 조직 속성
 - N 회 실패 후 사용자에게 경고 361
 - 개인 질문 사용 가능 359
 - 검색 필터 358
 - 기본 DN 358
 - 다음 로그인 시 반드시 비밀번호 변경 360
 - 바인드 DN 358
 - 바인드 비밀번호 359
 - 비밀 문제 358
 - 비밀번호 변경 알림 옵션 359
 - 비밀번호 재설정 사용 가능 359
 - 비밀번호 재설정 실패 잠금 간격 360, 361
 - 비밀번호 재설정 실패 잠금 사용 가능 360
 - 비밀번호 재설정 실패 잠금 수 360
 - 비밀번호 재설정 옵션 359
 - 비밀번호 재설정 잠금 속성 값 361
 - 비밀번호 재설정 잠금 속성 이름 361
 - 사용자 검증 358
 - 잠금 알림을 보낼 전자 메일 주소 360
 - 최대 질문 수 360
- 비밀번호 재설정 실패 잠금 간격 360, 361
- 비밀번호 재설정 실패 잠금 사용 가능 360
- 비밀번호 재설정 실패 잠금 수 360
- 비밀번호 재설정 옵션 359
- 비밀번호 재설정 잠금 속성 값 361
- 비밀번호 재설정 잠금 속성 이름 361
- 비밀번호 확인 393

人

- 사용 가능한 로컬 365
- 사용되는 기타 인증서 필드 275
- 사용자 80

- 만들기 80
- 삭제 82
- 서비스, 역할 및 그룹에 추가 81
- 정책에 추가 82
- 사용자 검색 반환 속성 257
- 사용자 검색 키 256
- 사용자 검색 필터
 - LDAP 인증 300
 - 회원 인증 306
- 사용자 검색을 시작할 DN
 - LDAP 인증 263, 299
 - 회원 인증 305
- 사용자 검증 358
- 사용자 그룹 자동 가입 254
- 사용자 기반 로그인 URL 150
- 사용자 기반 리디렉션 URL 150
- 사용자 기반 인증 150
- 사용자 기본 로컬 392
- 사용자 기본 언어 392
- 사용자 기본 표준 시간대 392
- 사용자 삭제 알림 목록 258
- 사용자 상태 394
- 사용자 속성 391
 - 사용자 프로필 속성 393
 - 고유 사용자 아이디 396
 - 비밀번호 393
 - 비밀번호 확인 393
 - 사용자 상태 394
 - 사원 번호 394
 - 성 393
 - 이름 393
 - 전자 메일 주소 394
 - 성명 393
 - 전화 번호 394
 - 주소 (집) 394

- 서비스 관리
 - 동적 속성
 - 관리자 DN 시작 보기 392
 - 기본 사용자 상태 392
 - 사용자 기본 로컬 392
 - 사용자 기본 언어 392
 - 사용자 기본 표준 시간대 392
- 사용자 수정 알림 목록 258
- 사용자 아이디 및 비밀번호 검증 플러그인 클래스 260
- 사용자 아이디 생성 모드 사용 가능 287
- 사용자 인터페이스
 - 사용자 정의 138
- 사용자 인터페이스 로그인 URL 132
- 사용자 인터페이스 로그인 URL 매개 변수 132
- 사용자 작성 기본 역할 255
- 사용자 작성 알림 목록 257
- 사용자 정의
 - 인증 사용자 인터페이스 138
- 사용자 컨테이너 96
 - 만들기 96
 - 삭제 96
- 사용자 컨테이너 표시 244
- 사용자 프로필 280
- 사용자 프로필 검색 시 사용되는 LDAP 속성 300, 306
- 사용자 프로필 검색 시 사용되는 활성 디렉토리 속성 264
- 사용자 프로필 동적 작성 기본 역할 281
- 사용자 프로필 디스플레이 옵션 254
- 사용자 프로필 디스플레이 클래스 253
- 사용자 프로필 속성 393
 - 고유 사용자 아이디 396
 - 비밀번호 393
 - 비밀번호 확인 393
 - 사용자 상태 394
 - 사원 번호 394
 - 성 393
 - 이름 393
 - 전자 메일 주소 394
 - 성명 393
 - 전화번호 394
 - 주소 (집) 394
- 사용자 프로필 액세스에 사용되는 인증서 필드 275
- 사용자 프로필 페이지에 그룹 표시 254
- 사용자 프로필 페이지에 역할 표시 254
- 사원 번호 394
- 사이트 아이디 및 사이트 발급자 이름 378
- 사전 처리 및 사후 처리 클래스 259
- 삭제된 객체의 검색 필터 251
- 상태 파일 , Java Enterprise System 설치 프로그램 33
- 새 설치 , Identity Server 32
- 서명 명제 378
- 서버 목록 363
- 서비스 83
 - 등록 83
 - 정책 106
 - 제거 84
 - 템플릿 만들기 83
- 서비스 기반 로그인 URL 147
- 서비스 기반 인증 147
- 서비스 기반 인증 리디렉션 URL 148
- 선택한 정책 조건 375
- 선택한 정책 주제 374
- 선택한 정책 참조 375
- 설치 디렉토리 , Identity Server 32
- 설치 프로그램 , Java Enterprise System 32
- 성 393
- 세션 서비스 URL 354

색션 ○

세션 속성 385

동적 속성

최대 세션 시간 (분) 388

최대 유희 시간 (분) 388

최대 캐싱 시간 (분) 388

세션 업그레이드

및 인증 171

세션 종료 103

소유자 및 그룹 , 변경 49

속성

데이터베이스에 연결할 비밀번호 294

데이터베이스의 비밀번호 열 294

비밀번호 구문 변환에 사용할 클래스 295

준비된 명령문 295

시간 초과 318

신뢰할 수 있는 파트너 사이트 379

○

아이디 지정 속성

핵심 인증 282

아카이브당 파일 수 351

아티팩트 시간 초과 379

에이전트

삭제 94

역할 84

만들기 85

사용자 제거 91

사용자 추가 87

삭제 93

정책에 추가 91, 93

역할 기반 로그인 URL 144

역할 기반 리디렉션 URL 145

역할 기반 인증 143

연결 유형 292

연결 풀 JNDI 이름 292

연합 관리 모듈 , 배포 34

영구 167

영구 쿠키

및 인증 167

영구 쿠키 모드 사용 가능 281

영구 쿠키 최대 시간 281

온라인 도움말 문서 256

외부 속성 불러오기 사용 가능 260

유효한 익명 사용자 목록 267

이름 393

이름 지정 서비스

및 정책 108

이름 지정 속성 353

전역 속성

SAML SOAP 서비스 URL 355

SAML 명제 관리자 서비스 URL 355

SAML 웹 프로파일 /POST 서비스 URL 355

SAML 웹 프로파일 / 아티팩트 서비스 URL 355

로그인 서비스 URL 354

세션 서비스 URL 354

인증 서비스 URL 354

정책 서비스 URL 354

프로파일 서비스 URL 354

익명 인증 178

등록 및 사용 178

로그인 179

익명 인증 속성 267

조직 속성

기본 익명 아이디 268

유효한 익명 사용자 목록 267

인증 수준 268

인스턴스 , 새 Identity Server 47

인증

FQDN 매핑 166

계정 잠금 157

메모리 165

물리적 164

- 다중 LDAP 구성 168
- 로그인 URL
 - 사용자 기반 150
 - 서비스 기반 147
 - 역할 기반 144
 - 조직 기반 141
- 리디렉션 URL
 - 사용자 기반 150
 - 서비스 기반 148
 - 역할 기반 145
 - 인증 수준 기반 153
 - 조직 기반 141
- 모듈 체이닝 160
- 모듈별 155
- 방법 138
 - 사용자 기반 150
 - 서비스 기반 147
 - 역할 기반 143
 - 정책 기반 129
 - 조직 기반 141
- 사용자 인터페이스
 - 로그인 URL 132
 - 로그인 URL 매개 변수 132
 - 사용자 정의 138
- 세션 업그레이드 171
- 영구 쿠키 167
- 플러그 인 인터페이스 검증 171
- 인증 구성 157, 337
 - 사용자 163
 - 사용자 인터페이스 157
 - 서비스에 대한 149, 162
 - 역할 146, 161
 - 조직 143, 161
- 인증 구성 속성 337
 - 조직 속성
 - 로그인 성공 URL 338
 - 로그인 실패 URL 338
 - 인증 구성 337
 - 인증 사후 처리 클래스 339
 - 충돌 해결 수준 339
- 인증 사후 처리 클래스 287, 339
- 인증 서비스 URL 354
- 인증 수준 289, 325, 328
 - JDBC 인증 295
 - LDAP 인증 289, 302, 312, 325
 - RADIUS 인증 318
 - SafeWord 모듈 인증 수준 324
 - Unix 모듈 인증 수준 330
 - 익명 인증 268
 - 활성 디렉토리 인증 266
 - 회원 인증 308
- 인증 수준 기반 인증 리디렉션 URL 153
- 인증될 사용자 검색 시 사용되는 LDAP 속성 300
- 인증서 기반 인증 180
 - 등록 및 사용 180
 - 로그인 181
- 인증서 인증 속성 271
 - 조직 속성
 - CRL 업데이트용 HTTP 매개 변수 273
 - CRL 에 인증서 일치 272
 - LDAP 서버 기본 비밀번호 274
 - LDAP 서버 기본 사용자 274
 - LDAP 시작 검색 DN 274
 - LDAP 액세스에 SSL 사용 275
 - LDAP 에서 CRL 검색 시 사용되는 발급자 DN 속성 272
 - LDAP 에서 인증서 검색 시 사용되는 주제 DN 속성 272
 - LDAP 에서 인증서 일치 272
 - OCSP 검증 사용 가능 273
 - 사용자 프로필 액세스에 사용되는 기타 인증서 필드 275
 - 사용자 프로필 액세스에 사용되는 인증서 필드 275
 - 인증서가 저장되는 LDAP 서버 273
 - 프로필 아이디의 LDAP 속성 274
- 인증서가 저장되는 LDAP 서버 273
- 인증에 사용자 DN 반환
 - 회원 인증 307
- 인증할 사용자 DN 반환 265, 301

일반 정책 109, 120, 124
수정 120

ㅈ

자동 설치 모드 입력 파일, amconfig 스크립트 32

자원 비교기 368

작업, amconfig 사용 33

잠금 속성 값 286

잠금 속성 이름 286

잠금 알림을 보낼 전자 메일 주소 285, 360

전역 속성 277

DC 노드 속성 목록 251

LDAP 연결 풀 크기 278

notBefore 시간에 대한 명제 비대칭 요소 379

SAML SOAP 서비스 URL 355

SAML 명제 관리자 서비스 URL 355

SAML 아티팩트 이름 378

SAML 요청에 서명 378

SAML 웹 프로파일 /POST 서비스 URL 355

SAML 웹 프로파일 / 아티팩트 서비스 URL 355

SAML 응답에 서명 378

Unix 도우미 구성 포트 330

Unix 도우미 스레드 330

Unix 도우미 시간 초과 330

Unix 도우미 인증 포트 330

관리 그룹 사용 가능 248

관리 대상 그룹 유형 245

구성 가능한 로그 필드 349

그룹 컨테이너 표시 245

기본 LDAP 연결 풀 크기 278

기본 그룹 컨테이너 252

기본 사용자 컨테이너 251

기본 에이전트 컨테이너 252

기본 역할 권한 (ACI) 246

기본 클라이언트 유형 344

내역 파일 수 348

대상 URL 에 POST 383

대상 지정자 379

데이터베이스 드라이버 이름 349

데이터베이스 사용자 비밀번호 349

데이터베이스 사용자 이름 349

도메인 구성 요소 트리 사용 가능 247

동적 관리 역할 ACI 248

로그 서명 시간 350

로그 파일 위치 348

로그 확인 빈도 350

로그아웃 서비스 URL 364

로그인 서비스 URL 364

로깅 서비스 URL 354

로깅 유형 349

명제 시간 초과 379

보기 메뉴에 컨테이너 표시 245

보안 로깅 사용 가능 350

사용 가능한 로컬 365

사용자 컨테이너 표시 244

사용자 프로필 서비스 클래스 250

사이트 아이디 및 사이트 발급자 이름 378

삭제된 객체의 검색 필터 251

서명 명제 378

서버 목록 363

세션 서비스 URL 354

신뢰할 수 있는 파트너 사이트 379

아카이브당 파일 수 351

아티팩트 시간 초과 379

인증 서비스 URL 354

자원 비교기 368

정책 서비스 URL 354

지원되는 클라이언트용 인증 모듈 278

- 최대 레코드 수 350
- 최대 로그 크기 348
- 쿠키 도메인 364
- 클라이언트 검색 사용 가능 344
- 클라이언트 검색 클래스 344
- 클라이언트 문자 세트 365
- 클라이언트 유형 341
- 프로필 서비스 URL 354
- 플랫폼 로컬 364
- 플러그 가능 인증 모듈 클래스 278
- 호환 사용자 삭제 사용 가능 248
- 전자 메일 주소 394
- 성명 393
- 전화 번호 394
- 정적 그룹 245
- 정책
 - DTD 파일
 - policy.dtd 112
 - 개요 106
 - 및 이름 지정 서비스 108
 - 정책 기반 자원 관리 (인증) 129
 - 프로세스 개요 108
- 정책 구성 서비스 127
- 정책 구성 속성 367
 - 전역 속성
 - 자원 비교기 368
 - 조직 속성
 - LDAP SSL 사용 가능 374
 - LDAP 그룹 검색 범위 372
 - LDAP 그룹 검색 속성 373
 - LDAP 그룹 검색 필터 372
 - LDAP 기본 DN 371
 - LDAP 바인드 DN 370
 - LDAP 바인드 비밀번호 371
 - LDAP 사용자 검색 범위 372
 - LDAP 사용자 검색 속성 373
 - LDAP 사용자 검색 필터 372
 - LDAP 서버 및 포트 370
 - LDAP 역할 검색 범위 373
 - LDAP 역할 검색 속성 373
 - LDAP 역할 검색 필터 372
 - LDAP 연결 풀 최대 크기 374
 - LDAP 연결 풀 최소 크기 374
 - LDAP 조직 검색 범위 371
 - LDAP 조직 검색 속성 373
 - LDAP 조직 검색 필터 371
 - 검색 시간 초과 374
 - 검색에서 반환되는 최대 결과 수 374
 - 선택한 정책 조건 375
 - 선택한 정책 주제 374
 - 선택한 정책 참조 375
 - 주제 결과 수명 375
- 정책 기반 자원 관리 (인증) 129
- 정책 서비스 URL 354
- 정책 에이전트
 - 개요 107
- 조건 추가 124
- 조직 74
 - 만들기 74
 - 삭제 76
 - 정책에 추가 76
- 조직 기반 로그인 URL 141
- 조직 기반 리디렉션 URL 141
- 조직 기반 인증 141
- 조직 속성 252
 - CRL 업데이트용 HTTP 매개 변수 273
 - CRL 에 인증서 일치 272
 - Event Listener 클래스 259
 - JDBC URL 294
 - JDBC 드라이버 294
 - JSP 디렉토리 이름 256
 - LDAP SSL 사용 가능 374
 - LDAP 그룹 검색 범위 372
 - LDAP 그룹 검색 속성 373
 - LDAP 그룹 검색 필터 372
 - LDAP 기본 DN 371
 - LDAP 바인드 DN 370

- LDAP 바인드 비밀번호 371
- LDAP 사용자 검색 범위 372
- LDAP 사용자 검색 속성 373
- LDAP 사용자 검색 필터 372
- LDAP 서버 기본 비밀번호 274
- LDAP 서버 기본 사용자 274
- LDAP 서버 및 포트 370
- LDAP 시작 검색 DN 274
- LDAP 액세스에 SSL 사용 275
- LDAP 역할 검색 범위 373
- LDAP 역할 검색 속성 373
- LDAP 역할 검색 필터 372
- LDAP 연결 풀 최대 크기 374
- LDAP 연결 풀 최소 크기 374
- LDAP 조직 검색 범위 371
- LDAP 조직 검색 속성 373
- LDAP 조직 검색 필터 371
- LDAP 에서 CRL 검색 시 사용되는 발급자 DN 속성 272
- LDAP 에서 인증서 검색 시 사용되는 주제 DN 속성 272
- LDAP 에서 인증서 일치 272
- NT Samba 구성 파일 이름 314
- NT 모듈 인증 수준 314, 334
- NT 인증 도메인 314
- NT 인증 호스트 314
- N 회 실패 후 사용자에게 경고 285, 361
- OCSP 검증 사용 가능 273
- RADIUS 공유 비밀 318
- RADIUS 서버 1 317
- RADIUS 서버 2 318
- RADIUS 서버 포트 318
- SafeWord EASSP 버전 323
- SafeWord 로그 파일 322
- SafeWord 로깅 사용 가능 322
- SafeWord 로깅 수준 322
- SafeWord 모듈 인증 수준 324
- SafeWord 서버 322
- SafeWord 인증 연결 시간 초과 323
- SafeWord 최소 인증 강도 323
- SafeWord 클라이언트 유형 323
- SecurID ACE/ 서버 구성 경로 327
- SecurID 도우미 구성 포트 328
- SecurID 도우미 인증 포트 328
- SSL 이 LDAP 서버에 액세스 가능
 - LDAP 인증 301
 - 회원 인증 307
- Unix 모듈 인증 수준
 - Unix 모듈 인증 수준 330
- 개인 질문 사용 가능 359
- 검색 범위
 - LDAP 인증 300
 - 활성 디렉토리 인증 265
 - 회원 인증 307
- 검색 시간 초과 374
- 검색 시간 초과 (초) 255
- 검색 필터 358
- 검색에서 반환되는 최대 결과 수 255, 374
- 관리자 인증 구성 280
- 그룹 기본 사용자 컨테이너 253
- 그룹 사용자 컨테이너 목록 253
- 기본 DN 358
- 기본 사용자 역할 304
- 기본 성공 로그인 URL 286
- 기본 실패 로그인 URL 287
- 기본 익명 아이디 268
- 기본 인증 로컬 283
- 기본 인증 수준 288
- 다음 로그인 시 반드시 비밀번호 변경 360
- 데이터베이스에 연결할 비밀번호 294
- 데이터베이스에 연결할 사용자 294
- 데이터베이스의 비밀번호 열 294
- 등록 후 사용자 상태 304

- 로그인 성공 URL 338
- 로그인 실패 URL 338
- 로그인 실패 잠금 간격 285
- 로그인 실패 잠금 기간 286
- 로그인 실패 잠금 모드 사용 가능 285
- 로그인 실패 잠금 수 285
- 루트 사용자 바인드용 비밀번호 263
 - LDAP 인증 299
 - 회원 인증 306
- 루트 사용자 바인드의 DN 263
 - LDAP 인증 299
 - 회원 인증 306
- 메뉴 항목 보기 255
- 모든 사용자를 위한 사용자 컨테이너 282
- 바인드 DN 358
- 바인드 비밀번호 359
- 별칭 검색 속성 이름 282
- 보조 LDAP 서버 298, 305
- 보조 활성화 Directory Server 262
- 비밀 문제 358
- 비밀번호 구문 변환에 사용할 클래스 295
- 비밀번호 변경 알림 옵션 359
- 비밀번호 재설정 사용 가능 359
- 비밀번호 재설정 실패 잠금 간격 360, 361
- 비밀번호 재설정 실패 잠금 사용 가능 360
- 비밀번호 재설정 실패 잠금 수 360
- 비밀번호 재설정 옵션 359
- 비밀번호 재설정 잠금 속성 값 361
- 비밀번호 재설정 잠금 속성 이름 361
- 사용자 검색 반환 속성 257
- 사용자 검색 키 256
- 사용자 검색 필터
 - LDAP 인증 300
 - 회원 인증 306
- 사용자 검색을 시작할 DN
 - LDAP 인증 299
 - 활성 디렉토리 인증 263
 - 회원 인증 305
- 사용자 검증 358
- 사용자 그룹 자동 가입 254
- 사용자 삭제 알림 목록 258
- 사용자 수정 알림 목록 258
- 사용자 아이디 및 비밀번호 검증 플러그인
 - 클래스 260
- 사용자 아이디 생성 모드 사용 가능 287
- 사용자 작성 기본 역할 255
- 사용자 작성 알림 목록 257
- 사용자 프로필 280
- 사용자 프로필 검색 시 사용되는 LDAP
 - 속성 300, 306
- 사용자 프로필 검색 시 사용되는 활성 디렉토리 속
 - 성 264
- 사용자 프로필 동적 작성 기본 역할 281
- 사용자 프로필 디스플레이 옵션 254
- 사용자 프로필 디스플레이 클래스 253
- 사용자 프로필 액세스에 사용되는 기타 인증서 필
 - 드 275
- 사용자 프로필 액세스에 사용되는 인증서
 - 필드 275
- 사용자 프로필 페이지에 그룹 표시 254
- 사용자 프로필 페이지에 역할 표시 254
- 사전 처리 및 사후 처리 클래스 259
- 선택한 정책 조건 375
- 선택한 정책 주제 374
- 선택한 정책 참조 375
- 시간 초과 318
- 아이디 지정 속성
 - 핵심 인증 282
- 연결 유형 292
- 연결 풀 JNDI 이름 292
- 영구 쿠키 모드 사용 가능 281
- 영구 쿠키 최대 시간 281
- 온라인 도움말 문서 256
- 외부 속성 불러오기 사용 가능 260
- 유효한 익명 사용자 목록 267

인증 구성 337
 인증 사후 처리 클래스 287, 339
 인증 수준 289, 325, 328
 JDBC 인증 295
 LDAP 인증 289, 302, 312, 325
 RADIUS 인증 318
 익명 인증 268
 활성 디렉토리 인증 266
 회원 인증 308
 인증될 사용자 검색 시 사용되는 LDAP 속성 300
 구성원 인증 306
 인증서가 저장되는 LDAP 서버 273
 인증에 사용자 DN 반환
 회원 인증 307
 인증할 사용자 DN 반환
 LDAP 인증 301
 활성 디렉토리 인증 265
 잠금 속성 값 286
 잠금 속성 이름 286
 잠금 알림을 보낼 전자 메일 주소 285, 360
 조직 인증 구성 284
 조직 인증 메뉴 280
 주 LDAP 서버 298, 304
 주 활성 Directory Server 262
 주제 결과 수명 375
 준비된 명령문 295
 최대 질문 수 360
 최소 비밀번호 길이 304
 최종 사용자 프로필 디스플레이 클래스 254
 충돌 해결 수준 339
 페이지당 표시되는 최대 항목 259
 프로필 아이디의 LDAP 속성 274
 필수 서비스 256
 활성 Directory Server 에 대한 SSL 액세스 사용
 LDAP 인증 265
 조직 인증 구성 284
 조직 인증 메뉴 280
 주 LDAP 서버 298, 304

주 활성 Directory Server 262
 주소 (집) 394
 주제 결과 수명 375
 준비된 명령문 295
 지급 구성 옵션 , Java Enterprise System 설치 프로그램
 램 32
 지원되는 언어 로컬 283
 지원되는 클라이언트용 인증 모듈 278

夫

참조 정책 111
 수정 126
 참조 추가 127
 최대 레코드 수 350
 최대 로그 크기 348
 최대 세션 시간 (분) 388
 최대 유휴 시간 (분) 388
 최대 질문 수 360
 최대 캐싱 시간 (분) 388
 최소 비밀번호 길이 304
 최종 사용자 프로필 디스플레이 클래스 254
 충돌 해결 수준 339

ㄱ

컨테이너 95
 만들기 95
 삭제 95
 콘솔
 사용자 인터페이스
 로그인 URL 132
 로그인 URL 매개 변수 132

콘솔 Identity Server 콘솔 참조

쿠키 도메인 364

클라이언트 검색 사용 가능 344

클라이언트 검색 속성 341

전역 속성

기본 클라이언트 유형 344

클라이언트 검색 사용 가능 344

클라이언트 검색 클래스 344

클라이언트 유형 341

클라이언트 검색 클래스 344

클라이언트 문자 세트 365

클라이언트 유형 341

Ⅱ

페이지당 표시되는 최대 항목 259

프로필 서비스 URL 354

프로필 아이디의 LDAP 속성 274

플랫폼 로컬 364

플랫폼 속성 363

전역 속성

로그아웃 서비스 URL 364

로그인 서비스 URL 364

사용 가능한 로컬 365

서버 목록 363

쿠키 도메인 364

클라이언트 문자 세트 365

플랫폼 로컬 364

플러그 가능 인증 모듈 클래스 278

플러그 인 인터페이스 검증

인증 171

필수 서비스 256

필터링된 그룹 245

ㅎ

핵심 인증

전역 속성 277

LDAP 연결 풀 크기 278

기본 LDAP 연결 풀 크기 278

지원되는 클라이언트용 인증 모듈 278

플러그 가능 인증 모듈 클래스 278

조직 속성 279

N 회 실패 후 사용자에게 경고 285

관리자 인증 구성 280

기본 성공 로그인 URL 286

기본 실패 로그인 URL 287

기본 인증 로컬 283

기본 인증 수준 288

로그인 실패 잠금 간격 285

로그인 실패 잠금 기간 286

로그인 실패 잠금 모드 사용 가능 285

로그인 실패 잠금 수 285

모든 사용자를 위한 사용자 컨테이너 282

별칭 검색 속성 이름 282

사용자 아이디 생성 모드 사용 가능 287

사용자 프로필 280

사용자 프로필 동적 작성 기본 역할 281

아이디 지정 속성 282

영구 쿠키 모드 사용 가능 281

영구 쿠키 최대 시간 281

인증 사후 처리 클래스 287

잠금 속성 값 286

잠금 속성 이름 286

잠금 알림을 보낼 전자 메일 주소 285

조직 인증 구성 284

조직 인증 메뉴 280

핵심 인증 서비스 176

등록 및 사용 176

핵심 인증 속성 277

헤더 프레임 71

현재 세션

세션 관리

세션 종료 103

세션 관리 창 101

인터페이스 101

활성 디렉토리 속성 인증될 사용자 검색 시

사용됨 264

활성 디렉토리 인증 속성 261

조직 속성

SSL 이 AD 서버에 액세스 가능 265

검색 범위 265

루트 사용자 바인드용 비밀번호 263

루트 사용자 바인드의 DN 263

보조 활성 Directory Server 262

사용자 검색 필터 264

사용자 검색을 시작할 DN 263

사용자 프로필 검색 시 사용되는 활성 디렉토리

속성 264

인증 수준 266

인증할 사용자 DN 반환 265

조직 속성을 인증할 사용자 검색 시 사용되는 활
성 디렉토리 속성

인증될 사용자 검색 시 사용되

는 활성 디렉토리

속성 264

주 활성 Directory Server 262

회원 인증 187

등록 및 사용 187

로그인 188