

# Sun Java™ System Access Manager

## 릴리스 노트

버전 6 2005Q1

2005년 2월 25일

부품 번호 : 819-1947

---

이 릴리스 노트에는 Sun Java System Access Manager 6 2005Q1( 이전 명칭 Sun Java System Identity Server) 의 릴리스 당시에 사용 가능한 중요한 정보가 포함되어 있습니다. 여기에서는 새로운 기능과 향상된 기능, 알려진 제한 사항과 문제점 및 기타 정보에 대해 다룹니다. 이 릴리스의 설치 및 사용 전에 이 문서를 읽으시기 바랍니다.

이 릴리스 노트의 최신 버전은 다음 Sun Java System 설명서 웹 사이트에서 찾을 수 있습니다.

<http://docs.sun.com/prod/entsys.05q1> 와

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

소프트웨어를 설치 및 설정하기 전에, 그리고 그 후에도 정기적으로 이 웹 사이트를 확인하여 최신 릴리스 노트와 설명서를 참조하시기 바랍니다.

이 릴리스 노트는 다음 절로 구성되어 있습니다.

- [릴리스 노트 개정 내역](#)
- [Access Manager 6 2005Q1 정보](#)
- [이 릴리스의 새로운 기능](#)
- [이 릴리스에서 해결된 버그](#)
- [설치 정보](#)
- [알려진 문제점 및 제한 사항](#)
- [재배포 가능 파일](#)
- [문제점 보고 및 사용자 의견 제공 방법](#)
- [Sun 의 추가 자원](#)

본 문서에는 관련된 추가 정보를 제공하는 타사 URL 을 참조합니다.

---

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

---

---

## 릴리스 노트 개정 내역

**표 1** 개정 내역

날짜	변경 사항 설명
2005 년 2 월 25 일	개정된 표 2 의 Red Hat ™ Linux 에서 지원되는 버전 목록에 " 하드웨어 및 소프트웨어 요구 사항 " 을 추가함 .
2005 년 2 월 2 일	2005Q1 릴리스 . 릴리스 노트 첫 발행 .

---

---

## Access Manager 6 2005Q1 정보

Sun Java System Access Manager 는 급격히 늘어나고 있는 기업의 요구를 충족시키기 위해 설계된 Identity 관리 솔루션입니다 . Access Manager 를 사용하면 직원 , 파트너 및 공급자의 아이디를 하나의 온라인 디렉토리에 통합할 수 있습니다 . 그런 다음 기업 내의 어떤 정보에 누가 액세스할 수 있는지에 대한 정책 및 권한을 구축할 수 있습니다 . Access Manager 는 모든 데이터 , 서비스 그리고 어떤 정보에 누가 액세스 권한을 갖고 있는지에 대한 핵심 요소이며 이는 내부 및 외부 비즈니스 관계에 있어 매우 중요합니다 .

# 이 릴리스의 새로운 기능

Access Manager 2005Q1 에는 다음과 같은 기능이 포함됩니다 . 이 기능에 대한 자세한 내용은 *Sun Java System Access Manager Technical Overview* 를 참조하십시오 .

- Identity Server 에서 Access Manager 로 제품 이름 변경
- Solaris 10 지원
- 새로운 웹 컨테이너 지원 : Sun Java System Application Server Enterprise Edition 8 2005Q1 (8.1)
- 신규 또는 개정된 인증 모듈 :
  - Java Database Connectivity (JDBC)
  - Mobile Station ISDN (MSISDN)
  - 활성 디렉토리
  - SAML (Security Assertion Markup Language): SAML 인증 지원이 인증 모듈로 릴리스 되어 SAML 인증이 인증 스택의 한 부분으로 됨 .
- 세션 페일오버
  - 각기 다른 호스트 서버의 지원되는 웹 컨테이너에서 실행되는 각 인스턴스를 가진 둘 이상의 Access Manager 6 2005Q1 인스턴스
  - Access Manager 인스턴스와 세션 저장소 데이터베이스 간의 세션 메시지를 관리하는 메시지 대기열 브로커 클러스터
  - 세션 저장소 데이터베이스로 Sleepycat Software, Inc. (<http://www.sleepycat.com/>) 의 Berkeley DB 이용 . Berkeley DB 클라이언트 데몬은 amsessiondb 입니다 .
- 정책 관리에 포함되는 새로운 자원 이름 플러그인 : `HttpURLResourceName`.
- 향상된 콘솔 기능 :
  - 객체 속성을 하나 이상 표시하여 탐색 창에서 각 객체 유형 보기를 사용자 정의할 수 있음.
  - 탐색 창 드롭다운 메뉴에 새로운 객체 유형을 추가할 수 있음 ( 예 : 프린터나 빌딩에 대한 입력 항목 추가 ).
- 클라이언트 SDK:
  - SDK 패키지 ( 인증 , 서비스 관리 , 사용자 관리 , SAML , 정책 클라이언트 , 세션 구성 요소 ) 를 재구성하여 Java 응용 프로그램 개발자들이 Access Manager 와 쉽게 통합할 수 있음 .
  - `serverconfig.xml` 파일에 대한 종속성이 제거되고 jar 파일의 풋프린트가 최소화됨 .

- 연합 관리
  - LAP (Liberty Alliance Project) 이름 식별자 매핑 프로토콜 지원
  - LAP Identity Web Services Framework (ID-WSF) 검색 서비스 사양 , 버전 1.1 지원
  - LAP ID-WSF 인증 서비스 사양 지원
  - LAP 메타데이터 설명 및 검색 사양 지원
  - LAP Liberty Identity Federation Framework (ID-FF) 확장 프로필 지원 :
    - 동적 Identity 공급자 프록시 처리
    - 계열사 연합
    - 일회성 연합
    - 이름 식별자 매핑 프로필
    - 이름 식별자 암호화 프로필
- Application Server Enterprise Edition 8 2005Q1 (8.1) 을 웹 컨테이너로 조정하는 데 성능 조정 스크립트 사용 가능

---

## 하드웨어 및 소프트웨어 요구 사항

이 릴리스의 Access Manager 에 대한 하드웨어 및 소프트웨어 요구 사항은 다음과 같습니다.

**표 2** 하드웨어 및 소프트웨어 요구 사항

구성 요소	요구 사항
운영 체제	Solaris™ Operating System (OS), SPARC® Platform Edition, 버전 8, 9, 10  Solaris™ OS, x86 Platform Edition, 버전 9 및 10 Red Hat™ Linux, WS/AS/ES 2.1 Update 2 Red Hat™ Linux, WS/AS/ES 3.0, 3.0 Update 1
RAM	512MB
디스크 공간	Access Manager 및 관련 응용 프로그램은 250MB

## 지원하는 브라우저

Access Manager 의 본 릴리스는 다음 브라우저를 지원합니다 .

브라우저	플랫폼
Microsoft Internet Explorer™ 5.5 SP2	Windows™ 2000, Sun Linux, Red Hat™ Linux 8.0
Microsoft Internet Explorer 6.0	Windows 2000, Windows™ XP, Sun Linux, Red Hat Linux 8.0
Mozilla 1.7.1	Windows 2000, Sun Linux, Red Hat Linux 8.0, Solaris™ 9 및 10, Solaris™ OS, x86 Platform Edition, 버전 9 및 10
Netscape™ 4.79	Windows NT, Solaris 8 및 9
Netscape™ 6.2.1	Windows NT, Windows 98, Sun Linux, Red Hat™ Linux Advanced Server 2.1, Solaris™ OS, x86 Platform Edition, 버전 9 및 10
Netscape™ 7.0	Windows 2000, Sun Linux, Red Hat Linux 8.0, Solaris 9 및 10, Solaris™ OS, x86 Platform Edition, 버전 9 및 10

## 이 릴리스에서 해결된 버그

아래 표에서는 Access Manager 2005Q1 에서 해결된 버그에 대해 설명합니다 .

**표 3** Access Manager 2005Q1 에서 해결된 버그

버그 번호	설명
5050332	Linux 시스템의 경우 amserver 정지가 amunixd 프로세스를 중단하지 않음
5049218	사용자 관리가 사용 불가능한 경우 사용자를 검색하는 동안 콘솔에 오류가 발생함
5048378	smtp 서버 포트 등록 정보가 AMConfig.properties 에서 잘못된
5043752	am2bak 실행 시 실패 메시지가 나타남
5042100	정책 관리자가 자체 프로필을 수정할 수 없음
5041529	BasicEntitySearch 필터가 uid 에 하드 코드됨
5038600	SAML 서비스를 사용하여 사용자를 만들 수 없음
5037978	조직 관리자가 정의된 액세스 권한으로 역할을 만드는 경우 오류가 발생함
5026635	콘솔 샘플이 컴파일되지 않음
5016725	참조 정책 규칙의 수정 사항이 하위 조직에 영향을 주지 않음

**표 3** Access Manager 2005Q1 에서 해결된 버그 ( 계속 )

버그 번호	설명
5013994	일본어 브라우저에서 인증 수준 로그인을 할 수 없음
5008960	amadmin 이 잘못된 오류 메시지를 반환함
4996479	정책 스키마를 가진 서비스가 사용자에게 대해 " 추가 가능 " 으로 표시됨
4961370	**** 검색 마스크가 작동하지 않음
4959895	엔티티 설명자 검색 필터가 제대로 작동하지 않음
4959071	유휴 세션이 정리되지 않음
4931907	서비스 유형 역할 사용자가 로그인하면 서비스가 사라짐
4931163	이름 지정 속성이 소문자여야 함
4930610	am2bak 및 bak2am 버전 메시지가 영어로만 표시됨
4922030	고정된 로컬에서의 충돌 해결 수준
4916683	backup_restore.po 의 msgid-msgstr 쌍에 대한 메시지가 현지화되어 있지 않음
4853809	서비스 등록 문제
4853809	모든 서비스를 등록하는 경우 사용 가능한 모든 서비스가 등록되지 않음

## 설치 정보

Java Enterprise System 설치 프로그램을 사용하여 첫 번째 인스턴스를 설치한 다음에는 amconfig 스크립트가 Application Server Enterprise Edition 8 2005Q1 (8.1) 을 웹 컨테이너로 사용하는 추가 Access Manager 인스턴스 배포를 지원합니다 .

구성 스크립트 실행에 대한 자세한 내용은 *Access Manager 6 2005Q1 관리자 설명서* 를 참조하십시오 .

또한 [알려진 문제점 및 제한 사항](#) 에서 **설치** 부분을 참조하십시오 .

---

# 알려진 문제점 및 제한 사항

이 절에는 Access Manager 2005Q1 릴리스 당시에 알려진 중요한 문제점이 나열되어 있습니다. 이 절은 다음 내용으로 구성되어 있습니다.

- [설치](#)
- [인증](#)
- [Access Manager 샘플](#)
- [명령줄 도구](#)
- [구성](#)
- [Access Manager 콘솔](#)
- [연합](#)
- [로그 서비스](#)
- [정책](#)
- [단일 사인 온 \(SSO\)](#)
- [Access Manager SDK](#)
- [국제화 \(i18n\)](#)
- [쿠키](#)
- [쿠키 하이재킹](#)

## 설치

### Secure Server 를 이용한 SDK 설치에서 amadmin 이 예외 발생 (#5107584)

Access Manager 2005Q1 에서 보안 Access Manager 를 전체 설치한 후 SDK 를 전체 설치하면 예외가 발생할 수 있습니다. 이것은 com.ipplanet.am.admin.sli.cerdb.prefix 등록 정보가 웹 서버에서 잘못된 값을 가지기 때문입니다.

### 해결 방법

1. AMConfig.properties 를 편집합니다 .
2. 등록 정보 com.ipplanet.am.admin.cli.certdb.prefix 를 https-<ws-instance-name>-<ws-hostname>- 으로 변경합니다 .
3. 웹 서버를 다시 시작합니다 .

### Linux 에서 웹 컨테이너를 사용하여 AMSDK 를 설치할 경우 공유 구성 요소에 대한 잘못된 링크 포함 (#6199933)

Linux 플랫폼에서 웹 컨테이너에 Access Manager SDK 를 설치하면 여러 공유 구성 요소 링크가 깨집니다 .

### 해결 방법

잘못된 링크를 제거하고 올바른 링크를 만듭니다 .

링크를 제거하려면 :

```
cd ${AM_INSTALL_DIR}/identity/lib
rm -rf jaxrpc-spi.jar relaxngDatatype.jar xsdlib.jar
```

새 링크를 만들려면 :

```
ln -s /opt/sun/private/share/lib/jaxrpc-spi.jar
ln -s /opt/sun/private/share/lib/relaxngDatatype.jar
ln -s /opt/sun/private/share/lib/xsdlib.jar
```

### 참조 무결성 플러그인에 대한 인수의 오자가 성능에 영향을 줌 (#5029256)

Access Manager 가 Directory Server 에 대한 참조 무결성 플러그인을 사용 가능하게 한 경우 , 플러그인의 인수 11 에서 속성 이름에 오자가 있습니다 . 해당 속성 이름은 ipplanet-am-modifiable-by 입니다 . 조직이 삭제된 경우에는 이로 인해 디렉토리 오류 로그에 search not indexed 경고가 표시됩니다 .

참조 무결성 플러그인은 인수에서 언급된 모든 속성의 색인을 필요로 하며 , 색인이 붙은 속성은 ipplanet-am-modifiable-by 입니다 . 이 속성이 Access Manager 성능에 영향을 미칠 수 있습니다 .

### Application Server xercesImpl.jar 이 JVM 과 충돌을 일으킴 (#6223676)

Application Server 8.1 EE 에서 RedHat Linux 의 경우 /opt/sun/appserver/lib (Solaris 의 경우 /opt/SUNWappserver/appserver/lib) 안의 xercesImpl.jar 은 /opt/sun/share/lib (Solaris 의 경우 /usr/share/lib) 의 공유 구성 요소 버전 xercesImpl.jar 보다 먼저 로드됩니다 .



Application Server 버전은 클래스 로더에 의해 공유 구성 요소 버전보다 먼저 로드됩니다. 이런 경우 Application Server의 구 버전은 대기하고 있는 수천 개의 JSP를 처리할 수 없습니다. 따라서 JVM은 멈추거나 충돌합니다.

### 해결 방법

SPARC와 x86에서 Solaris 9 및 10의 경우 `/opt/SUNWappserver/appserver/lib`, Red Hat AS 2.1 및 3.0의 경우 `/opt/sun/appserver/lib` 안의 `xercesImpl.jar` 이름을 바꿉니다. 그렇게 하면 JVM 클래스 로더는 Red Hat AS 2.1 및 3.0의 경우 `/opt/sun/share/lib`, Solaris 9 및 10의 경우 `/usr/share/lib` 안의 공유 구성 요소 `xercesImpl.jar`를 강제로 사용하게 됩니다.

### AM SDK 설치 중에 사용자가 프로토콜을 입력할 수 없음 (#6180090)

Access Manager SDK를 설치하면 “Access Manager: Web Container for running Sun Java System Access Manager Services” 창에서 Access Manager 서비스를 실행하는 웹 컨테이너의 프로토콜을 묻지 않습니다. 설치 프로그램은 웹 컨테이너가 http 프로토콜을 사용한다고 가정하지만 https 프로토콜을 지정해야 SSL 사용 가능 Access Manager 설치를 사용하는 SDK 설치에 액세스할 수 있습니다.

### 해결 방법

AMConfig.properties 파일에서 Access Manager 서버 설치 관련 프로토콜을 https로 설정합니다. 예를 들면 다음과 같습니다.

```
com.ipplanet.am.server.protocol=https
com.ipplanet.am.console.protocol=https
```

### Access Manager가 서버 CLASSPATH에 servlet.jar를 추가함 (#5016348)

Access Manager는 지원되는 웹 컨테이너에 대해 `servlet.jar`를 서버 CLASSPATH에 배치합니다. 각 웹 컨테이너가 구현에서 `servlet.jar` 파일을 번들로 제공하기 때문에 이 파일은 예상치 못한 결과를 가져올 수 있습니다.

### 해결 방법

CLASSPATH에서 `servlet.jar`를 제거합니다.

## Access Manager 샘플

### JDK 1.5와 함께 샘플을 컴파일할 때 경고 반환 (#5102149)

Access Manager와 함께 포함된 샘플이 JDK 1.5와 컴파일되면 경고를 반환합니다.

### 해결 방법

다음과 같은 방법으로 경고를 방지합니다.

- JDK 1.5 를 사용하는 경우 컴파일 명령줄에 `encoding="ISO-8859-1"` 을 추가합니다.  
또는
- 샘플을 컴파일할 때 JDK 1.4 를 사용합니다.

### **SAML xmlsig 샘플에서 생략된 부분으로 인해 컴파일 실패함 (#5090925)**

JDK 1.5 로 컴파일하는 경우 SAML xmlsig 샘플에서 생략된 부분 때문에 컴파일이 실패합니다. 이 문제는 JDK 1.4.2 로 컴파일하면 발생하지 않습니다.

#### *해결 방법*

JDK 1.5 로 컴파일하는 경우 다음 단계에 따라 LD\_LIBRARY\_PATH 를 설정하십시오.

1. xmlsig 디렉토리에서 SAML 샘플에 대한 Readme.html 또는 Readme.txt 파일을 찾습니다.
2. 3 절 “Solaris 에서 XMLSIG 샘플을 설정하기 위한 지침 “ 의 4 단계에 따라 LD\_LIBRARY\_PATH 를 `web-server-install-directory/bin/https/lib` 로 설정합니다.
3. LD\_LIBRARY\_PATH 에 `/usr/lib/mps/secv1` 을 추가하여 JSS 라이브러리와 그 종속성을 선택합니다.

## 인증

### **전자 메일을 통한 사용자 수정 알림이 작동하지 않음 (#6212964)**

관리 서비스에 있는 전자 메일을 통한 사용자 수정 알림 기능은 현재 작동하지 않습니다.

### **SafeWord 연결이 닫히지 않음 (#5073718)**

Access Manager 에 로그인하려는 경우 SafeWord 시도 응답 페이지로 이동한 후 비밀번호를 입력하지 않아도 연결 시간 초과로 인한 연결 종료가 발생하지 않습니다. 브라우저를 닫아도 SafeWord 서버와의 연결은 종료되지 않습니다.

### **LDAP Directory Server 연결에서 LDAP 인증이 익명으로 바인딩됨 (#5090018)**

LDAP 연결에서 Access Manager 가 바인드 DN 및 비밀번호를 Directory Server 로 전달하지 않아 LDAP Directory Server 내의 익명 바인드가 사용 불가능한 경우 인증에 영향을 줍니다.

#### *해결 방법*

사용자의 Directory Server 내의 익명 바인드를 사용 가능하도록 합니다.

**지속성 쿠키 모드 등록 정보가 일치하지 않음 (#5038544)**

지속성 쿠키 모드에서 토큰의 사용자 아이디 등록 정보 집합이 일치하지 않습니다. 따라서 사용자 아이디 등록 정보에 따라 정책 에이전트가 실패할 수 있습니다.

**해결 방법**

DN 이외의 값인 경우 UserToken 을 사용하고 DN 값인 경우 Principal 을 사용하십시오.

**세션 시간 초과 페이지를 재로드하면 유효한 사용자 이름과 비밀번호로 사용자를 인증함 (#4697120)**

로그인 페이지에서 시간이 초과될 때까지 기다린 다음 유효한 사용자 이름과 비밀번호를 입력하면 세션 시간 초과 페이지가 나타납니다. 사용자가 사용자 이름과 비밀번호를 다시 입력하지 않고 페이지를 재로드하면 Access Manager 로 인증됩니다.

**여러 SafeWord 서버에 대해 각기 다른 디렉토리를 지정해야 함 (#4756295)**

개별적인 SafeWord 서버를 사용하는 여러 조직에 대해 구성하는 경우 각각의 SafeWord 인증 서비스 템플릿에 고유한 .../serverVerification 디렉토리를 지정해야 합니다. 기본값을 그대로 유지하고 모든 서버가 동일한 디렉토리를 사용하면 해당 SafeWord 서버로 인증하는 첫 번째 조직만 제대로 작동합니다.

## 명령줄 도구

**/opt/SUNWam/bin 디렉토리 내 Idapsearch 및 Idapmodify 유틸리티가 올바르게 작동하지 않음 (#4954779)**

/opt/SUNWam/bin 디렉토리 내 Idapsearch 및 Idapmodify 유틸리티가 치명적 오류를 반환합니다.

**해결 방법**

LD\_LIBRARY\_PATH 환경 변수에 DirectoryServer-base/lib/ 경로를 추가합니다.

**am2bak 및 bak2am 스크립트가 Linux 에서 작동하지 않음 (#5053866)**

Access Manager 를 Linux 시스템에서 실행할 경우 am2bak 및 bak2am 복원 스크립트가 작동하지 않습니다.

**해결 방법**

1. 다음 명령의 경로를 수정하십시오.
  - ECHO=/usr/bin/echo 는 ECHO=/bin/echo 로 바꿉니다.
  - uid='/usr/xpg4/bin/id -un' 는 uid='/usr/bin/id -un' 으로 바꿉니다.
  - /usr/bin/tar 는 /bin/tar 로 바꿉니다.

- /usr/bin/rm 는 /bin/rm 으로 바꿉니다.
- /usr/bin/grep 는 /bin/grep 으로 바꿉니다.
- /usr/bin/ps 는 /bin/ps 로 바꿉니다.
- /usr/bin/ls 는 /bin/ls 로 바꿉니다.

2. check\_for\_invalid\_chars() 함수를 수정합니다. 예를 들면 다음과 같습니다.

```
check_for_invalid_chars() {  
echo "$1" | grep '[^/_.-a-zA-Z0-9a-]' > /dev/null  
if [ $? = 0 ]; then  
return 1  
else  
return 0  
fi  
}
```

#### **amadmin 이 잘못된 오류 메시지를 반환함 (#5008960)**

amadmin 의 import 옵션이 모든 관련 오류에 대해 동일한 오류 메시지를 반환합니다.

#### **콘솔 전용 설치에서 amverifyarchive 가 스왑되지 않은 태그를 가짐 (#4993375)**

Access Manager 콘솔 전용 설치를 수행하는 경우 amverifyarchive 유틸리티가 이 스크립트에서 다음 태그를 스왑하지 않습니다. JSSHOME, JDK\_HOME, BASEDIR, PRODUCT\_DIR.

## 구성

#### **Linux 에서 WebSphere Application Server 5.1 구성에 성공한 후 시작 실패 (#6204646)**

Linux 상에 WebSphere 용 Access Manager SDK 구성 요소를 설치한 후 amwas51config 를 올바른 amsamplesilent 파일과 함께 실행하면 WebSphere 가 시작되지 않습니다.

#### *해결 방법*

다음과 같이 LD\_LIBRARY\_PATH 안에 /opt/sun/private/lib 를 추가합니다 :

```
LD_LIBRARY_PATH="$WAS_LIBPATH":$LD_LIBRARY_PATH:/opt/sun/private/lib  
export LD_LIBRARY_PATH ;;
```

server.xml 에서 -Djava.util.logging.config.class 옵션 앞에 있는 **"/:** 를 제거합니다.

**웹 서버에서 certdb 별칭이 올바르게 설정되지 않음 (#6212532)**

웹 서버에서 SSL 을 Access Manager 와 사용 가능하게 한 후 amadmin 을 실행하면 " 이름 지정 서비스 사용 불가 " 오류가 발생합니다 . 브라우저를 통해서 는 예상대로 작동합니다 .

**색인이 백엔드 이름과 관계 없이 사용자 루트에 대해 항상 생성됨 (#5002886)**

index.ldif 가 속성에 대한 색인 생성 시 사용자 루트를 하드 코드합니다 . 모든 임의 백엔드 데이터베이스 이름에 상주하는 루트 접미어에 대해 Access Manager 를 설치할 수 있습니다 . 백엔드 이름은 nsslapd-suffix=SUFFIX\_NAME 을 필터로 사용하여 기본 cn=config 상태의 ldapsearch 를 통해 얻을 수 있습니다 .

## 연합

**연합 관리 연락 담당자 예외 발생 (#6213102)**

새 공급자를 만든 후 그 공급자에게 새로운 연락 담당자를 추가할 경우 , 다음과 같은 오류 메시지를 받을 수 있습니다 .

```
The server encountered an internal error () that prevented it from fulfilling this request
```

**amFederation.access 로그에 원격 로깅 안 됨 (#6197608)**

원격 로깅이 구성되면 amFederation.access 를 제외한 모든 로그가 원격 Access Manager 인스턴스에 제대로 작성됩니다 . 로그 레코드는 작성되지 않습니다 .

**해결 방법**

LogUtils의 AccessController.doPrivileged(AdminTokenAction.getInstance()); 를 사용합니다.

**fedCookie 상태가 변경되지 않음 (#6202574)**

SP 및 IDP 상의 연합 사용자들을 연합 종료할 경우 , fedCookie 상태는 계속 YES 로 나타납니다 . 상태 표시가 NO 로 되어야 합니다 .

**쿼리/수정에 대한 개인 프로필 컨테이너 실패(#6189808)**

다음 개인 프로필 컨테이너는 쿼리 또는 수정 작업에서 실패합니다 :

```
LegalIdentity/Gender
```

```
EmploymentIdentity/AltO
```

### 속성 값이 비어 있는 경우 PP Modify 에 대해 예외가 발생함 (#5047103)

속성 값이 비어 있는 상태에서 PP Modify 를 수행하면 Access Manager 에서 예외가 발생합니다. 예를 들어 sis-ep 샘플을 테스트하기 위해 설치를 생성하고 EP Modify 페이지를 보낸 다음 어떤 속성 값도 입력하지 않고 버튼을 누르면 예외가 잘못 발생합니다.

### 정책을 적용하려면 서버를 다시 시작해야 함 (#5045036)

연합 정책 구현을 적용하려면 서버를 다시 시작해야 합니다. 이것은 Application Server 및 Web Server 모두에 적용됩니다. 처음 설치하거나 정책을 처음 구현하는 경우에만 서버를 다시 시작해야 합니다.

## Access Manager 콘솔

### DIT 에 다수의 사용자 컨테이너가 있는 경우 사용자 생성 불가 (#5079609)

다수 ( 천 개 이상 ) 의 사용자 컨테이너를 만들 경우 사용자 컨테이너를 찾을 수 없으므로 Access Manager 콘솔에 로그인하여 새 사용자를 만들 수 없습니다.

이는 시간 제한 전에 Directory Server 가 다수의 사용자 컨테이너를 찾는다 할지라도 UMCreatUserModelImpl.getPeopleContainers() 에서 검색 시간 제한 오류가 발생하기 때문입니다.

#### 해결 방법

Access Manager 콘솔에서 사용자 컨테이너 보기를 사용 가능하게 한 후 특정 사용자 컨테이너로 이동하여 사용자를 만듭니다.

### 읽기 전용으로 액세스하는 최상위 도움말 데스크 관리자 역할로 새 사용자를 만들 수 있음 (#5109348)

현재 도움말 데스크 관리자 역할의 기본값은 전체 액세스로 설정되어 있습니다. 수정으로 변경하면 이동 프레임에서 새로 만들기와 삭제 버튼은 사용할 수 없지만 관리자가 사용자 항목 등록 정보를 수정하는 것은 여전히 가능합니다.

#### 해결 방법

도움말 데스크 관리자 등록 정보 페이지를 불러와 사용 가능한 작업으로 보기를 변경합니다. 사용자 행으로 이동하여 전체 액세스에서 수정으로 설정을 변경합니다.

### 계열사 엔티티의 계열사 옵션을 선택하면 예외가 발생함 (#6203563)

연합 관리 모듈에서 계열사 엔티티 페이지의 보기 > 계열사를 선택하면 예외가 발생합니다.

### 해결 방법

높이 속성이 닫는 JATO 태그 밖으로 나오도록 JSP 를 수정합니다. FSAffiliateProfile.jsp 에서 , 104 째 줄을 다음과 같이 바꿉니다 :

```
<td width="1%"> height="1" alt=""></td>
```

높이 속성 앞에 /> 가 오도록 하십시오 .

### 계열사 디스플레이 옵션에서 오류 발생 (#6194139)

연합 관리 모듈에서 계열사 디스플레이 옵션이 메뉴의 유일한 옵션이며 기본값으로 설정되어 있는 경우 Access Manager 는 오류 페이지를 표시합니다 .

### 관리자 역할에서 사용자 서비스를 수정할 수 없음 (#6174652)

최상위 관리자 역할로 로그인했을 때 사용자에게 새로운 서비스를 추가할 수 있지만 서비스를 수정할 수는 없습니다 .

### 해결 방법

관리자 역할에 대한 디스플레이 프로필을 편집하고 필요한 보기 메뉴 및 가능한 작업을 부여합니다 .

### 뒤로 버튼을 누를 때 Cvalues 값이 유지되지 않음 (#4992972)

그룹이나 역할 생성 또는 정책에 조건 추가와 같이 여러 페이지 프로세스가 있는 경우 뒤로 버튼을 누르면 이전 페이지의 값이 복원되지 않습니다 .

### 연합 관리 모듈의 호스트 공급자에 대해 새로 고침 문제가 발생함 (#4915894)

연합 관리 모듈에서는 호스트 공급자의 Identity 공급자 보기에서 속성을 수정하고 저장하면 변경 사항은 저장되지만 디스플레이가 자동으로 새로 고쳐지지 않습니다 .

### 해결 방법

다른 모듈 ( 예 : 서비스 구성 ) 을 선택하여 연합 관리 모듈을 종료한 다음 연합 관리 모듈로 돌아갑니다 . 이렇게 하면 디스플레이가 새로 고쳐집니다 .

### 콘솔이 사용자 속성 변경 사항을 새로 고치지 않음 (#4931455)

Access Manager 콘솔 이동 프레임이 데이터 프레임에서 지정한 사용자 속성 값의 변경 사항을 나타내도록 새로 고쳐지지 않습니다 . 변경된 값을 볼 수 있도록 페이지를 수동으로 새로 고칩니다 .

### Internet Explorer 에서의 포트 문제 (#4864133)

Internet Explorer 와의 비호환성 때문에 http 를 실행할 때 포트 번호 80 및 https 를 실행할 때 포트 443 을 Access Manager 포트 번호로 사용할 수 없습니다 .

## 로깅 서비스

### 자바 보안이 활성화되면 로깅 문제가 발생함 (#4926520)

자바 보안이 활성화되면 `jdk_logging.jar` 가 작동하지 않을 수 있습니다.

#### 해결 방법

자바 보안이 사용 가능하며 JDK 1.4 이전 버전이 있을 경우 자바 보안 파일에 다음 권한을 포함시킵니다.

```
permission java.lang.RuntimePermission shutdownHooks
```

## 정책

### nslookthrough 제한에 도달했을 때 일치하는 항목이 반환되지 않음 (#5013538)

nslookthrough 에 정의된 관리자 제한에 도달하여도 일치하는 항목이 Access Manager 콘솔에 반환되지 않습니다.

#### 해결 방법

nslookthroughlimit 매개 변수를 조정하여 항목 수를 보상합니다.

### 정책이 별칭 토큰에 적용되지 않음 (#4985823)

LDAP 와 구성원 이외의 인증 모듈에 대한 Access Manager 에 사용자 별칭을 사용하여 로그인한 다음 보호된 자원에 액세스하면 액세스가 거부됩니다.

### 정책 샘플 문제 (#4923898)

정책 샘플에 있는 `Readme.html` 은 해당 샘플을 실행할 수 없도록 만드는 정보를 제외시킵니다.

#### 해결 방법

샘플을 실행하려면 `LD_LIBRARY_PATH` 환경 변수에 `NSPR`, `NSS`, 및 `JSS` 공유 라이브러리에 대한 경로를 포함해야 합니다. Solaris 시스템의 경우 `/usr/lib/mps/secv1`, Linux 시스템의 경우 `/opt/sun/private/lib` 를 포함하도록 `LD_LIBRARY_PATH` 를 설정합니다.



# Access Manager SDK

## 이름 지정 속성의 최상위 조직에서 속성 고유성이 잘못됨 (#6204537)

최상위 조직에서 이름 지정 속성에 대한 속성 고유성이 제대로 작동하지 않습니다. 그러나 사용자 및 조직 속성 고유성은 올바르게 적용됩니다.

## 영구 검색 연결이 되지 않을 경우 EventService 가 루프에 빠짐 (#6205443)

영구 검색이 연결되어 있어도 EventService (ES) 스레드가 listener 를 성공적으로 추가 (LDAP JDK 가 listener 를 성공적으로 추가) 합니다. ES 스레드가 반응을 얻으려 하는 경우에는 LDAPResponse 가 영구 검색 연결을 사용할 수 없다고 보고합니다 (오류 코드 51). 그런 경우 ES 는 listener 재구축을 시도합니다. 이렇게 해서 타이트한 루프에 빠지게 됩니다.

## SSL 서버를 사용하는 Access Manager SDK 설치에 대한 certutil 의 CDocument 사용 (#5027614)

사용자가 SSL 사용 가능 Access Manager 서버에 SDK 전용 시스템을 사용하여 통신을 시도할 때 보안 관련 오류 및 예외가 발생합니다. 이 시나리오에서 Access Manager SDK 는 어떤 웹 컨테이너에도 배포되지 않았거나 BEA WebLogic Server 또는 IBM WebSphere Application Server 와 같은 타사 웹 컨테이너에 배포된 경우에 해당합니다.

### 해결 방법

SDK 전용 시스템에 인증서 데이터베이스를 만들고 Access Manager 서버에 대한 루트 CA 인증서를 이 데이터베이스에 설치합니다.

1. SDK 전용 시스템에 슈퍼 유저 (root) 로 로그인합니다.
2. 필요한 Netscape Security Services (NSS) 패키지가 설치되었는지 확인합니다.
  - Solaris 시스템의 경우 SUNWtlsu
  - Linux 시스템의 경우 sun-nss RPM
3. 패키지가 설치되지 않았다면 설치합니다. 예를 들면 다음과 같습니다.

Solaris 시스템의 경우

```
cd JavaEnterpriseSystem_base/Solaris_arch/Product/shared_components/Packages
pkgadd -d . SUNWtlsu
```

Linux 시스템의 경우

```
cd JavaEnterpriseSystem_base/Linux_x86/Product/shared_components/Packages
rpm -Uvh sun-nss-3.3.10-1.i386.rpm
```

- 해당 인증서 데이터베이스의 토큰 비밀번호에 대한 비밀번호 파일을 만듭니다. 예를 들면 다음과 같습니다.

Solaris 시스템의 경우

```
echo "cert-database-password" > /etc/opt/SUNWam/config/.wtpass
chmod 700 /etc/opt/SUNWam/config/.wtpass
```

Linux 시스템의 경우

```
echo "cert-database-password" > /etc/opt/sun/identity/config/.wtpass
chmod 700 /etc/opt/sun/identity/config/.wtpass
```

여기서 *cert-database-password* 가 토큰 비밀번호입니다.

- LD\_LIBRARY\_PATH 변수를 확인합니다.

Solaris 시스템의 경우 LD\_LIBRARY\_PATH 에 /usr/lib, /usr/lib/mps/secv1 및 /usr/lib/mps 디렉토리가 존재하는지 확인합니다. 빠진 디렉토리가 있으면 추가합니다.

Linux 시스템의 경우 LD\_LIBRARY\_PATH 에 /opt/sun/private/lib 디렉토리가 존재하는지 확인합니다. 없다면 이 디렉토리를 추가합니다.

- 인증서 데이터베이스 도구 (certutil) 를 사용하여 인증서 및 키 데이터베이스를 만듭니다. certutil 에 대한 자세한 내용은 다음 웹 사이트를 참조하십시오.

<http://mozilla.org/projects/security/pki/nss/tools/certutil.html>

예를 들면 다음과 같습니다.

```
certutil-home/certutil -N -d cert-database-dir -f config-home/.wtpass
```

여기서

*certutil-home* 은 certutil 의 위치입니다.

- Solaris 시스템의 경우 /usr/sfw/bin
- Linux 시스템의 경우 /opt/sun/private/bin

*cert-database-dir* 은 인증서 및 키 데이터베이스용 데이터베이스 디렉토리입니다.

*config-home* 은 Access Manager 구성 파일의 위치입니다.

- Solaris 시스템의 경우 /etc/opt/SUNWam/config
- Linux 시스템의 경우 /etc/opt/sun/identity/config

7. 새로 생성된 인증서 데이터베이스에서는 Access Manager 서버에 설치된 SSL 인증서에 대한 루트 CA 인증서를 추가합니다. 예를 들면 다음과 같습니다.

```
certutil-home/certutil -A -n "certificate-nickname" -t "TCu,TCu,TCuw" -d
cert-database-dir -a -i path-to-file-containing-cert -f config-home/.wtpass
```

8. 편집기를 사용하여 AMConfig.properties 파일을 확인하고 다음 값을 검증합니다.
  - 인증서 데이터베이스 디렉토리 : com.iplanet.am.admin.cli.certdb.dir
  - 접두어 : com.iplanet.am.admin.cli.certdb.prefix
  - 비밀번호 파일 : com.iplanet.am.admin.cli.certdb.passfile
 필요에 따라 설정을 편집합니다. 예를 들어, 접두어 설정은 비어 있어야 합니다( ""와 동일).
9. AMConfig.properties 가 변경되고 Access Manager SDK 가 웹 컨테이너에 배포된 후 , 웹 컨테이너를 다시 시작합니다 .

#### **JCE 공급자와 함께 DNSAlias 를 사용하는 경우 SSL 핸드셰이크가 실패함 (#5038876)**

JCE 공급자와 함께 subjectaltname 에 있는 유효한 DNSAlias 이름을 가진 인증서를 사용하는 경우 SSL 핸드셰이킹이 실패합니다 .

#### **필터의 Init() 에서 Identity 메소드로 인해 Weblogic 이 충돌함 (#5016283)**

필터의 init () 메소드가 Access Manager 관련 코드를 가지고 있는 경우 WebLogic 서버가 시작되지 않습니다 . Access Manager API 가 ServletFilter 서블릿의 init 메소드에 호출됩니다 .

Access Manager 는 보안 공급자로서 JSS 를 사용하지만 WebLogic 은 JCE 를 기본적으로 사용합니다 . init 메소드를 호출하면 WebLogic 은 JCE 를 사용하여 사용권을 검증하려고 시도하지만 JSS 는 초기화됩니다 .

#### *해결 방법*

JSEncryption 의 기본 보안 암호화를 AMConfig.properties 파일의 JCEEncryption 으로 변경하십시오 .

#### **"{SSHA}" 기호로 시작하는 모든 비밀번호를 사용할 수 없음 (#4966191)**

Access Manager 는 비밀번호에 해시 {SSHA} 기호 사용을 지원하지 않습니다 .

#### **그룹 만들기 옵션이 하나의 memberURL 속성만 추가함 (#4931958)**

여러 LDAP 필터 옵션 (-f) 으로 그룹을 만들면 memberURL 속성 하나만 생기면서 해당 그룹이 제대로 만들어지지 않습니다 .

## 조정

### **Solaris-x86 에서 amtune 및 연결된 파일을 전달하지 않음 (#6213019)**

이 릴리스에서는 amtune 스크립트 및 관련 파일들이 Solaris-x86 에서 적절한 디렉토리에 설치되지 않습니다.

#### *해결 방법*

Sparc-Solaris 에 제공하는 amtune 파일을 사용합니다.

### **비밀번호 파일에서 amtune-as8 스크립트에 오류가 있음 (#6212380)**

asadmin 비밀번호를 가진 임시 비밀번호 파일이 만들어지기 때문에 Application Server 8 (amtune-as8)에서는 amtune 스크립트를 이용한 자동 조정이 작동하지 않습니다. 현재 비밀번호만 파일에 입력됩니다.

#### *해결 방법*

amtune-as8 에서 다음 구문을 문자열에 입력합니다.

```
"TOKEN=Value"
```

예를 들면 다음과 같습니다.

```
"AS_ADMIN_PASSWORD=11111111"
```

amtune-env 변경 사항을 입력합니다.

```
#ASADMIN=$CONTAINER_BASE_DIR/bin/asadmin
```

```
ASADMIN=/opt/SUNWappserver/appserver/bin/asadmin
```

## 단일 사인 온 (SSO)

### **다른 배포 URI 로 SSO 를 수행할 수 없음 (#4770271)**

Access Manager 의 다른 두 인스턴스 간에 배포 URI 가 다르면 단일 사인 온 (SSO) 이 제대로 작동하지 않습니다.

## 국제화 (i18n)

그룹 이름이 멀티바이트인 경우 그룹 구성원이 나열되지 않음 (#6197041)

국제화된 버전의 Access Manager 6 2005Q1 에서 그룹 이름이 멀티바이트인 경우 Access Manager 콘솔에 그룹 구성원이 나열되지 않습니다 .

#### **Linux 에서 시작 및 중지 메시지를 읽을 수 없음 (#6207421)**

zh/zh\_TW 문자 집합에 대한 Access Manager 시작 및 종료 메시지를 읽을 수 없습니다 . 이 문제는 Linux 플랫폼에서 발생합니다 .

#### **비영어 로컬에서 HTTPBasic 및 WindowsDesktopSSO 을 사용하여 로그인할 수 없음 (#6209324)**

비영어 로컬에서 HTTPBasic 과 WindowsDesktopSSO 인증 모듈로 로그인할 수 없습니다 .

#### *해결 방법*

XML 파일에서 이 매개 변수를 영어로 되돌립니다 .

```
HTTPBasic.xml: <HTTPHeader>Authorization</HTTPHeader>
```

```
WindowsDesktopSSO.xml: <HTTPHeader>Authorization</HTTPHeader>
```

Access Manager 가 Application Server 에 배포될 경우 이 파일들은 다음 디렉토리 안에 설치됩니다 .

```
/var/opt/sun/appserver/domains/domain1/applications/j2ee-modules/amserver/config/auth/default_<lang>
```

Access Manager 가 Web Server 에 배포될 경우 이 파일들은 다음 디렉토리 안에 설치됩니다 .

```
/opt/sun/webserver/https-<host>/is-web-apps/services/config/auth/default_<lang>
```

#### **일본어 온라인 도움말이 잘못 표시됨 (#5024138)**

일본어 버전의 Access Manager 를 실행하고 언어를 en\_US 로 변경하는 경우 일본어 도움말 컨텍스트가 계속 표시됩니다 .

#### *해결 방법*

sym 링크를 docs\_en 에서 docs\_en\_US 로 변경하십시오 .

#### **클라이언트 검색 기능이 제대로 작동하지 않음 (#5028779)**

클라이언트 검색 서비스에서 UTF-8 제거가 제대로 작동하지 않습니다 .

#### *해결 방법*

UTF-8 문자 집합을 제거하는 경우 변경을 완료한 후 웹 컨테이너를 다시 시작합니다 .

#### **G11Nsetting 이 Q 요소의 공백을 처리하지 않음 (#5008860)**

클라이언트 데이터가 q 요소 주위에 공백을 가진 경우 G11NSettings 코드가 제대로 구문 분석하지 못하고 다음과 같은 오류를 반환합니다 .

오류 G11NSettings::Fetchcharset() Unable to parse charset entry invalid Q q

### URL 에 ja 문자 집합에 대한 멀티바이트 역할 매개 변수를 사용하면 로그인 페이지가 실패함 (#4905708)

멀티바이트 역할을 만든 다음 멀티바이트 역할에 등록된 사용자로 URL 로그인을 시도하면 로그인 페이지에 오류가 발생합니다.

#### 해결 방법

인증 프레임워크가 URL 에 지정된 멀티바이트 역할 값의 암호를 해독하려면 매개 변수와 함께 gx\_charset 를 지정해야 합니다. 예를 들면 다음과 같습니다.

```
http://hostname:port/amserver/UI/Login?role=manager?role=%E3%81%82%&gx_charset=utf-8
```

### 로그 파일의 문자가 Ja 로케에서 올바르게 표시되지 않음 (#4882286)

다음 로그 파일에 일본어 문자가 포함되어 있으며 열었을 때 일본어 문자가 올바르게 표시되지 않습니다. deploy.log 및 undeploy.log 를 제외한 /var/opt/SUNWam/debug 디렉토리 내의 모든 파일.

### URL 의 로케 매개 변수가 혼합된 로그인 페이지를 표시함 (#4915137)

WebServer 와 Access Manager 인스턴스가 함께 설치되어 있을 경우 비영어 기반 브라우저를 사용하여 http://host:port/amserver/UI/Login?locale=en 에 로그인하면 로그인 페이지에 영어와 비영어 문자가 섞여서 표시됩니다.

#### 해결 방법

다음 심볼릭 링크를

```
AccessManager-base/SUNWam/web-apps/services/config/auth/default
```

아래와 같이 변경합니다.

```
AccessManager-base/SUNWam/web-apps/services/config/auth/default_en
```

### Application Server 가 ja 이면 로그인 창에 혼합된 로케이 표시됨 (#4932089)

브라우저 언어 설정이 en 이고 Application Server 의 로케이 ja 로 설정된 경우 기본적으로 Access Manager 로그인 창은 다시 영어로 표시되지 않습니다.

#### 해결 방법

로케을 en 으로 설정하여 Application Server 를 실행합니다.

### 잠금 알림에서 읽을 수 없는 전자 메일을 보냄 (#4938511)

기본 로케이 c 이외의 로케로 설정된 웹 컨테이너로 Access Manager 를 실행하고 사용자가 서버에서 잠겨지면 잠금 알림 전자 메일이 보내지지만 읽을 수 없습니다.

### 해결 방법

잠금 알림을 보낼 전자 메일 주소 속성에 email 매개 변수 대신 email|local|charset 을 설정합니다. 예를 들면 다음과 같습니다.

```
user1@example.com|zh|GB2312
```

### 멀티바이트 이름이 자동 등록에서 작동하지 않음 (#4732470)

자동 등록 (구성원 인증 서비스) 모듈에서 중복된 사용자 아이디와 멀티바이트 성 및 이름으로 사용자를 만드는 경우 오류가 발생합니다. 멀티바이트 사용자 아이디는 지원되지 않습니다.

### 해결 방법

사용자가 멀티바이트 환경에서 자동 등록을 사용하여 로그인하는 경우 관리자는 핵심 인증에서 사용자 생성기 모드 속성이 선택되지 않았는지 확인해야 합니다.

또는

사용자가 자동 등록 로그인 페이지에서 자체 아이디 생성 옵션을 선택할 수 있습니다.

### Access Manager 의 일본어 버전이 Netscape 6.22, 6.23 에서 작동하지 않음 (#4902421)

Access Manager 의 일본어 버전에서는 Netscape 6.22 또는 6.23 을 사용하여 콘솔에 로그인할 수 없습니다.

### 시간 조건 형식이 변경되지 않음 (#4888416)

정책 정의에 대한 시간 조건에서 시간 표시는 현지화와 관계 없이 다음 형식에서 변경되지 않습니다.

```
Hour:Minute AM/PM
```

### 클라이언트 검색 화면이 현지화되어 있지 않음 (#4922013)

클라이언트 검색 인터페이스의 현재 스타일 등록 정보 화면 부분이 이 릴리스에서 현지화되지 않았습니다.

### 업데이트된 genericHTML 클라이언트 등록 정보가 적용되지 않음 (#4922348)

클라이언트 검색 서비스의 genericHTML 클라이언트 등록 정보에 있는 문자 집합 목록에서 UTF-8을 제거하고, 변경 사항을 저장하고 클라이언트 검색을 활성화한 다음 로그아웃했다가 다시 로그인하면 로그인 페이지가 여전히 UTF-8 문자 집합으로 표시됩니다.

### 해결 방법

amsrver 를 사용하여 서버를 수동으로 다시 시작합니다.

### 로그 파일 헤더가 현지화되어 있지 않음 (#4923536)

모든 로그 파일의 처음 두 행 즉, Version 섹션과 Fields 섹션 및 해당 필드 목록이 현지화되지 않았습니다.

### amSSO.access의 데이터 필드 값이 현지화되어 있지 않음 (#4923549)

amSSO.access 로그 파일에서 Data 필드의 모든 값이 현지화되지 않았습니다.

### Exception.jsp에 하드 코드된 메시지가 있음 (#4772313)

Exception.jsp가 현지화되어 있지 않으며 하드 코드된 제목, 오류 메시지 및 저작권 정보를 포함합니다. 이 예외 오류 jsp 페이지는 특별한 경우에만 호출됩니다. 예를 들면 Directory Server가 중단되거나 Access Manager 서비스를 가져올 수 없고 이 jsp 페이지에 대해 현지화되지 않은 경우입니다.

## 쿠키

### 쿠키 해제 모드가 작동하지 않음 (#4967866)

쿠키를 지원하는 브라우저가 Access Manager에 액세스한 다음 쿠키 지원을 해제한 경우 브라우저가 이전의 Access Manager 쿠키를 계속 보냅니다. 이 문제로 인해 Access Manager 자원에 대한 액세스가 거부됩니다.

#### 해결 방법

다음 해결 방법 중 하나를 선택하십시오.

- 모든 Access Manager 쿠키를 제거하려면 브라우저 쿠키 캐시를 지우십시오.
- 브라우저에서 쿠키를 비활성화하십시오.

## 쿠키 하이재킹

세션 쿠키를 사용하는 응용 프로그램을 신뢰할 수 없을 경우 보안이 손상될 수 있습니다.

단일 사인 온 (SSO) 또는 크로스 도메인 단일 사인 온 (CDSSO)을 해당 Access Manager 배포 시 사용할 수 있는 경우 http(s) 세션 쿠키가 사용자 브라우저에 설정됩니다. 이러한 쿠키는 여러 응용 프로그램에 걸쳐 검증됩니다. Access Manager가 여러 DNS 도메인에 걸쳐 배포되는 경우 Liberty 프로토콜은 인증된 DNS 도메인에서 웹 응용 프로그램의 대상 도메인으로 http(s) 세션 쿠키를 전송합니다.



사용자가 자동으로 웹 자원에 로그인했지만 세션 쿠키를 사용하여 응용 프로그램을 인증할 수 없는 경우 알려진 보안 취약점이 있습니다. 취약점은 Identity 공급자가 타사 또는 기업 내의 공인되지 않은 그룹에 의해 개발된 응용 프로그램 (또는 서비스 공급자)에 사용자의 인증, 권한 및 프로필 정보를 제공할 때 존재할 수 있습니다. 예상되는 보안 문제는 다음과 같습니다.

- 모든 응용 프로그램은 동일한 http 세션 쿠키를 공유합니다. 따라서 감염된 응용 프로그램이 세션 쿠키를 하이재킹하여 다른 응용 프로그램에 대해 사용자를 가장할 수 있습니다.
- 응용 프로그램이 https 프로토콜을 사용하지 않는 경우 세션 쿠키는 네트워크 도청에 취약합니다.
- 단 하나의 응용 프로그램을 해킹할 수 있으면 전체 인프라의 보안이 손상될 위험이 있습니다.
- 감염된 응용 프로그램은 세션 쿠키를 사용하여 사용자에게 대한 프로필 속성을 가져와서 수정할 수 있습니다. 사용자가 관리 권한을 가진 경우 응용 프로그램은 상당한 손상을 입을 수 있습니다.

## 해결 방법

다음 단계를 따르십시오.

1. Access Manager 관리 콘솔을 사용하여 각 에이전트에 대한 항목을 만듭니다.
  - a. 생성할 에이전트를 포함하는 조직에 대해 보기 메뉴에서 에이전트를 선택한 다음 새로 만들기를 누릅니다.
  - b. 다음과 같은 정보를 제공합니다.

**이름.** 에이전트의 이름이나 아이디를 입력합니다. 예: agent123

**비밀번호.** 에이전트의 비밀번호를 입력합니다. 예: agent123

**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 Manager는 이 등록 정보를 사용하여 사용자의 자격 증명에 대한 에이전트 요청을 받습니다.

agentRootURL에 대한 등록 정보 값을 포트 번호가 있는 에이전트 URL과 동일한 값으로 입력합니다. agentRootURL 값은 대소문자를 구분합니다.

예 : agentRootURL=http://server\_name:99/

**장치 상태.** 에이전트의 장치 상태를 입력합니다. 활성으로 설정된 경우 에이전트는 Access Manager에 대해 인증되어 Access Manager와 통신할 수 있습니다. 비활성으로 설정된 경우 에이전트는 Access Manager에 대해 인증될 수 없습니다.

c. 확인을 누릅니다.

2. 1b 단계에서 입력한 비밀번호에 대해 다음 명령을 실행하십시오.

```
AccessManager-base/SUNWam/agents/bin/crypt_util agent123
```

이렇게 하면 다음과 같은 출력이 표시됩니다.

```
WnmKUCg/y3l404ivWY6HPQ==
```

3. 새 값을 적용하기 위해 `AMAgent.properties` 를 변경한 다음 에이전트를 다시 시작합니다. 예를 들면 다음과 같습니다.

```
# The username and password to use for the Application authentication module.

com.sun.am.policy.am.username = agent123
com.sun.am.policy.am.password = WnmKUCg/y3l404ivWY6HPQ==

# Cross-Domain Single Sign On URL
# Is CDSSO enabled.
com.sun.am.policy.agents.cdsso-enabled=true

# This is the URL the user will be redirected to after successful login
# in a CDSSO Scenario.
com.sun.am.policy.agents.cdcservletURL =
http://server.example.com:port/amserver/cdcservlet
```

4. 새 값을 적용하기 위해 `AMConfig.properties` 를 변경한 다음 Access Manager 를 다시 시작합니다. 예를 들면 다음과 같습니다.

```
com.sun.identity.enableUniqueSSOTokenCookie=true
com.sun.identity.authentication.uniqueCookieName=sunIdentityServerAuthNServer

com.sun.identity.authentication.uniqueCookieDomain=example.com
```

5. Access Manager 관리 콘솔에서 서비스 구성 > 플랫폼을 선택합니다.
6. 쿠키 도메인 목록에서 쿠키 도메인 이름을 다음과 같이 변경합니다.
  - a. 기본 iplanet.com 도메인을 선택한 다음 제거를 누릅니다.
  - b. Access Manager 설치의 호스트 이름을 입력한 다음 추가를 누릅니다.

예 : server.example.com

다음과 같이 브라우저에 설정된 두 개의 쿠키가 표시됩니다.

쿠키	호스트 이름
iPlanetDirectoryPro	server.example.com
sunIdentityServerAuthNServer	example.com

---

## 재배포 가능 파일

Sun Java System Access Manager 2005Q1 의 모든 파일은 제품의 라이선스가 없는 사용자에게 재배포할 수 없습니다.

---

## 문제점 보고 및 사용자 의견 제공 방법

Sun Java System Access Manager 에 문제가 발생하면 다음 중 한 가지 방법으로 Sun 고객 지원 부서에 문의하십시오.

- Sun 소프트웨어 지원 서비스 (온라인)  
<http://www.sun.com/supporttraining>

이 사이트에는 기술 자료, 온라인 지원 센터 및 제품 추적에 대한 링크와 유지 보수 프로그램 및 지원 연락처 등이 있습니다.

- 유지 보수 계약 관련 긴급 전화 번호

문제 해결을 위해 최상의 지원을 제공할 수 있도록 지원 부서에 연락할 때는 다음 정보를 미리 준비해 두십시오.

- 문제가 발생한 상황 및 해당 문제가 작업에 미치는 영향 등을 비롯한 문제에 대한 설명
- 시스템 종류, 운영 체제 버전 및 제품 버전 ( 문제에 영향을 미치는 패치 및 기타 소프트웨어 )
- 문제를 재현하기 위해 사용한 방법에 대한 자세한 단계
- 오류 로그나 코어 덤프

## 사용자 의견 환영

Sun 은 설명서의 내용을 개선하기 위해 노력하고 있으며 사용자의 의견 및 제안을 환영합니다 . 다음 의 웹 기반 양식을 사용하여 Sun 으로 의견을 보내 주십시오 .

<http://www.sun.com/hwdocs/feedback/>

해당 필드에 전체 설명서 제목과 부품 번호를 기입해 주십시오 . 부품 번호는 해당 설명서의 제목 페이지나 문서 맨 위에 있으며 일반적으로 7 자리 또는 9 자리 숫자입니다 . 예를 들어 이 릴리스 노트의 부품 번호는 819-1947 입니다 .

---

## Sun 의 추가 자원

다음 인터넷 사이트에서 유용한 Sun Java System 관련 정보를 찾을 수 있습니다 .

Sun Java System 설명서

<http://docs.sun.com/prod/entsys.05q1> 와

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

- Sun Java System 전문가 서비스  
<http://www.sun.com/service/products/software/javaenterprisesystem/>
- Sun Java System 소프트웨어 제품 및 서비스  
<http://www.sun.com/software/>
- Sun Java System 소프트웨어 지원 서비스  
<http://www.sun.com/supporttraining>
- Sun Java System 지원 및 기술 자료  
<http://sunsolve.sun.com>
- Sun Java System 컨설팅 및 전문가 서비스  
<http://www.sun.com/service/products/software/javaenterprisesystem>

- Sun Java System 개발자 정보  
<http://developers.sun.com/>
- Sun 개발자 지원 서비스  
<http://www.sun.com/developers/support>

---

Copyright © 2005 Sun Microsystems, Inc. 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.

SUN PROPRIETARY/CONFIDENTIAL.

미국 정부의 권리 - 상용 소프트웨어. 정부 사용자는 Sun Microsystems, Inc. 표준 사용권 계약과 해당 FAR 규정 및 보충 규정을 준수해야 합니다.

본 제품의 사용은 사용권 조항의 적용을 받습니다.

이 배포에는 타사에서 개발한 자료가 포함되어 있을 수 있습니다.

제품 중에는 캘리포니아 대학에서 허가한 Berkeley BSD 시스템에서 파생된 부분이 포함되어 있을 수 있습니다.

Sun, Sun Microsystems, Sun 로고, Java 및 Solaris 는 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.