CA SiteMinder Federation Standalone

설치 및 업그레이드 안내서

r12.52 SP1

CA Technologies 제품 참조

이 문서는 다음 CA Technologies 제품을 참조합니다 :

- SiteMinder

CA 에 문의

기술 지원팀에 문의

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

설명서 변경 사항

SiteMinder 의 이전 릴리스에서 발견된 문제점으로 인해 다음과 같은 내용이 12.52 설명서에서 업데이트되었습니다.

- SiteMinder 커넥터 라이브러리에 대한 고려 사항 (페이지 22) - 이 항목에서는 CA SiteMinder® Federation Standalone 이 SiteMinder 와 호환될 수 있도록 정책 서버에 복사할 올바른 라이브러리를 설명합니다. CQ 177513 을 해결합니다.
- JCE(Java Cryptographic Extension)를 위해 패치 필요 (페이지 11) - 이 항목에서는 Java 에서 제공하는 암호화 알고리즘을 사용하기 위해 업데이트가 필요한 파일을 설명합니다. CQ 174929 를 해결합니다.
- 기존 SAML 파트너 관계에 동일한 백 채널 사용자 이름이 없는지 확인 (페이지 68) - 기존 파트너 관계에서 사용하는 수신 백 채널 사용자 이름이 동일한 SSO 프로필 내에서 서로 달라야 한다는 업그레이드 요건을 설명하는 항목이 추가되었습니다. CQ 177179 를 해결합니다.
- 시스템 및 설치 사전 요구 사항, (페이지 11) UNIX 시스템에 CA SiteMinder® Federation Standalone 설치 (페이지 19), UNIX 시스템에서 구성 마법사 실행 (페이지 46) - 여러 가지 설치 및 구성 문제가 해결되었습니다. CQ 176815(STAR 문제 21189977 및 1+21182925-1)를 해결합니다.
- Windows 에서 Federation Standalone 12.52 로 업그레이드 (페이지 70) 및 UNIX 에서 Federation Standalone 12.52 로 업그레이드 (페이지 73) - AssertionGeneratorFramework.properties 파일을 업데이트하는 단계가 추가되었습니다. CQ 176623 을 해결합니다.
- 구성 내보내기 (페이지 83) - 구성을 내보내기 전에 파트너 관계를 비활성화하고 SSL 을 사용하지 않도록 설정하는 단계가 제거되었습니다. 이러한 단계는 필요하지 않습니다. CQ 165316 을 해결합니다.

목차

제 1 장: CA SiteMinder® Federation Standalone 설치 11

시스템 및 설치 사전 요구 사항 11
CA SiteMinder® Federation Standalone 설치 실행 15
설치에 필요한 정보 15
사용할 설치 모드 결정 16
r12.52 SP1 의 설치 실행 파일 17
Windows 시스템에 CA SiteMinder® Federation Standalone 설치 17
UNIX 시스템에 CA SiteMinder® Federation Standalone 설치 19
Solaris 10 보안 속성 파일 수정 필요 21
SiteMinder 커넥터 라이브러리에 대한 고려 사항 22
페더레이션 시스템과 백엔드 서버 사이에 SSL 사용 24
Windows 또는 UNIX 플랫폼에서 페더레이션 시스템 재설치 25
CA SiteMinder® Federation Standalone 구성 마법사 실행 25
구성 전 배포 모드 결정 26
SiteMinder 와 함께 CA SiteMinder® Federation Standalone 배포 31
구성 마법사에 필요한 정보 39
구성 실행 파일 44
Windows 에서 구성 마법사 실행 44
UNIX 시스템에서 구성 마법사 실행 46
CA SiteMinder® Federation Standalone 에 대한 가상 호스트 구성 48
CA SiteMinder® Federation Standalone 무인 설치 50
설치 속성 파일 설정 50
CA SiteMinder® Federation Standalone 무인 설치 실행 53
무인 CA SiteMinder® Federation Standalone 구성 53
구성 속성 파일 설정 54
무인 구성을 실행합니다. 58
Administrative UI 에 로그인합니다. 59

제 2 장: CA SiteMinder® Federation Standalone 제거 61

Windows 에서 페더레이션 시스템 제거 61
UNIX 시스템에서 CA SiteMinder® Federation Standalone 제거 62

제 3 장: 12.x 시스템을 CA SiteMinder® Federation Standalone r12.52 SP1 로 업그레이드 63

CA SiteMinder® Federation Standalone 의 업그레이드 및 마이그레이션 경로 63
CA SiteMinder® Federation Standalone r12.52 SP1 로 업그레이드하는 방법 65
키 데이터베이스 동기화 67
기존 파트너 관계에 고유 백 채널 사용자 이름이 있는지 확인 68
기존 구성 백업 69
Windows 에서 CA SiteMinder® Federation Standalone r12.52 SP1 로 업그레이드 70
UNIX 에서 CA SiteMinder® Federation Standalone r12.52 SP1 로 업그레이드 73

제 4 장: CA SiteMinder® Federation Standalone r12.52 SP1 로 마이그레이션 77

CA SiteMinder® Federation Standalone 의 업그레이드 및 마이그레이션 경로 77
r12.52 SP1 로 마이그레이션하는 방법 79
키 데이터베이스 동기화 81
구성을 XML 파일로 내보내기 83
CA SiteMinder® Federation Standalone 설치 프로그램 실행 84
기존 구성을 새 시스템으로 가져오기 85
키 데이터베이스를 인증서 데이터 저장소로 마이그레이션 87
SSL 키 및 인증서 마이그레이션(선택 사항) 90
장애 조치 배포를 마이그레이션하는 방법 96
r12 장애 조치 배포를 r12.52 SP1 로 마이그레이션 97
프록시 서버 또는 부하 분산 장치에서 장애 조치 설정 98

제 5 장: FIPS 암호화를 사용하기 위해 페더레이션 시스템 마이그레이션 99

고려해야 할 FIPS 마이그레이션 문제 100
FIPS_COMPAT 모드에서 FIPS_Only 모드로 마이그레이션하는 방법 100
SSL 구성 비활성화 102
기존 구성 백업 103
OPENSSL_FIPS 환경 변수 설정 104
정책 엔진을 FIPS_MIGRATE 모드로 설정 105
정책 저장소 암호화 키 다시 암호화 106
데이터베이스 관리자 암호 다시 암호화 107
슈퍼 사용자 암호 다시 암호화 108
프록시 엔진 에이전트 공유 암호 다시 암호화 108
정책 저장소 및 키 저장소 데이터 다시 암호화 110
CA SiteMinder® Federation Standalone UI 를 FIPS_Only 모드로 설정 112

보안 프록시 엔진을 FIPS_Only 모드로 설정 114
정책 엔진을 FIPS_Only 모드로 설정 115
FIPS 호환 SSL 인증서 가져오기(선택 사항) 116

제 6 장: CA SiteMinder® Federation Standalone 문제 해결 121

설치 문제 해결 121
CA SiteMinder® Federation Standalone 라이선스를 받거나 소프트웨어를 다운로드할 때 문제 발생 121
CA SiteMinder® Federation Standalone UI 또는 구성 요소 서비스가 시작되지 않음 122
구성 관리자를 실행할 때 설치가 실패함 122
키 데이터베이스 마이그레이션 문제 해결 123
SiteMinder 키 데이터베이스 마이그레이션의 상태를 알 수 없음 123
마이그레이션 실패 오류 발생 124
인증서 데이터 저장소 오류 발생 125
SiteMinder 키 데이터베이스 수동 마이그레이션 125
XML 서명 래핑 공격 방지 128
기존 시스템의 JDK 업그레이드 128

제 7 장: 키 도구 참조 129

개인 키 및 인증서 쌍 추가 130
인증서 추가 132
해지 정보 추가 133
해지 정보 삭제 134
인증서 데이터 제거 134
인증서 삭제 135
인증서 또는 개인 키 내보내기 135
별칭 찾기 136
기본 CA 인증서 가져오기 137
모든 인증서의 메타데이터 나열 137
해지 정보 나열 138
인증서 메타데이터 표시 139
별칭 이름 변경 139
인증서 유효성 검사 140

제 1 장: CA SiteMinder® Federation Standalone 설치

시스템 및 설치 사전 요구 사항

CA SiteMinder?Federation Standalone 의 최소 시스템 요구 사항:

메모리

2 GB(최소)

디스크 공간

최소 3 GB(디스크 공간 1 GB, 임시 파일 위치 2 GB)

브라우저

Windows Internet Explorer, Mozilla FireFox

지원되는 운영 체제

Windows, Solaris, Linux

버전별 상세 내용은 기술 지원 사이트의 "CA SiteMinder® Federation Standalone Platform Support Matrix"(CA SiteMinder® Federation Standalone 플랫폼 지원표)를 참조하십시오.

설치 요구 사항

설치에 필요한 사전 요구 사항은 다음과 같습니다.

참고: 특정 플랫폼에 대한 자세한 내용은 *CA SiteMinder® Federation Standalone 릴리스 정보*를 참조하십시오.

Oracle 또는 SQL Server 데이터베이스

정책, 키 및 세션 저장소는 서버 데이터베이스를 사용합니다. 데이터베이스를 설치하고 데이터베이스 인스턴스 이름을 지정하십시오. 이 인스턴스 이름은 나중에 구성 마법사를 실행할 때 사용됩니다.

중요! 여러 서버가 한 데이터베이스 인스턴스를 공유할 수 있지만 데이터베이스 인스턴스는 해당 페더레이션 환경 전용이어야 합니다. 데이터베이스 인스턴스를 SiteMinder 서버와 같은 다른 응용 프로그램용 서버와 공유하지 마십시오. 시스템에는 전용 데이터베이스 인스턴스가 필요하지만 전용 데이터베이스 서버는 필요하지 않습니다.

데이터베이스 관리자는 데이터베이스에서 테이블을 만들고 데이터베이스에 데이터를 입력할 수 있는 권한이 있어야 합니다.

버전별 상세 내용은 기술 지원 사이트의 "Platform Support Matrix"(플랫폼 지원표)를 참조하십시오.

Java

- 지원되는 JDK 가 필요합니다. 버전별 상세 내용은 기술 지원 사이트의 "Platform Support Matrix"(플랫폼 지원표)를 참조하십시오.
- Java 암호화 알고리즘을 사용하려면 최신 JCE(Java Cryptography Extension) Unlimited Strength Jurisdiction 패치가 필요합니다. 운영 플랫폼에 맞는 JCE 패키지를 찾으려면 Oracle 웹 사이트를 방문하십시오.

  패치를 시스템의 다음 파일에 적용하십시오.

  - local_policy.jar
  - US_export_policy.jar

  이러한 파일은 다음 디렉터리에 있습니다.

  Windows: *jre_home*\lib\security

  UNIX: *jre_home*/lib/security

  jre_home

  이 변수는 Java Runtime Environment 설치 위치를 지정합니다.

Javascript

JavaScript 는 활성화되어 있어야 합니다.

Windows

관리자로 설치를 실행하고 관리자로 페더레이션 서비스를 중지하거나 시작하십시오.

Solaris 및 Linux

- 루트 사용자로 CA SiteMinder® Federation Standalone 을 설치하지 마십시오. 루트 사용자로 설치하려고 하면 설치가 취소되고 오류 메시지가 나타납니다. 대신 CA SiteMinder® Federation Standalone 을 설치할 사용자 계정을 만드십시오.
- 1024 미만의 포트를 사용하는 UNIX 플랫폼에서 CA SiteMinder® Federation Standalone 을 실행하지 않는 것이 좋습니다. 이 권장 사항에는 기본 Apache HTTP 포트(80)와 기본 Apache SSL 포트(443)가 포함됩니다.
- 64 비트 시스템에 설치하는 경우라도 설치 프로그램에는 32 비트 시스템 라이브러리가 필요합니다. 설치를 실행하기 전에 64 비트 시스템에 32 비트 라이브러리를 설치하십시오.

  Linux 시스템에서는 32 비트 라이브러리를 설치한 후 **updatedb** 명령을 실행하십시오. updatedb 명령을 사용하면 운영 체제가 새 라이브러리를 인식하게 됩니다.
- xterminal 에서 GUI 모드 설치를 실행하려면 X11(32 비트) 라이브러리 패키지를 설치하십시오. 이 패키지는 필수입니다.

Linux 에만 해당

- **Linux 관련 Java 요구 사항:**
  - JDK 의 필요한 버전이 시스템 경로에 있는지 확인하십시오.
  - 필요한 버전 이외의 다른 Java 버전이 설치되지 않도록 하십시오. (Red Hat 에서 때때로 OpenJDK 가 설치됨) OpenJDK 가 있는 경우 다음 명령을 실행하여 OpenJDK 를 제거하십시오.

    ```
    yum erase openjdk
    ```
  - Java 기반 GUI 를 실행하려면 시스템에 libXsts 와 같은 필수 패키지가 있어야 합니다. 필수 패키지는 일반적으로 시스템에서 기본적으로 사용할 수 있습니다.

- **/dev/urandom 과 /dev/random 사이에 심볼 링크가 필요함:**

  재부팅하면 /dev/urandom 및 /dev/random 사이에 필요한 심볼 링크가 제거될 수 있습니다. 이 심볼 링크가 없으면 CA SiteMinder® Federation Standalone 서비스가 시작되지 못할 수 있습니다.

  심볼 링크를 복구하려면 다음 명령을 입력하십시오.

  ```
  rm dev/random;ln -s /dev/urandom /dev/random
  ```

- **방화벽**

  방화벽은 비활성화되어야 합니다.

  방화벽을 비활성화하려면 다음 명령을 실행하십시오.

  ```
  /etc/init.d/iptables stop
  chkconfig iptables off
  ```

- **라이브러리 종속성:**
  - mlocate.86_64
  - glibc.i686
  - libstdc++.i686
  - compat-expat1.i686
  - libuuid.i686
  - ksh.86_64
  - X-Windows 의 경우:
    - libXext.i686
    - libXi.686
    - libXtst.686

CA SiteMinder® Federation Standalone 설치 실행

CA SiteMinder?Federation Standalone 을 설치하려면 다음 프로세스를 완료하십시오.

1. 설치 마법사에 필요한 정보를 수집합니다.
2. 사용할 설치 모드를 결정합니다.
3. 설치 마법사를 실행합니다.

중요! 다음의 설치 제한을 확인하십시오.

- 정책 서버 또는 SPS(보안 프록시 서버)가 이미 설치된 시스템에는 CA SiteMinder® Federation Standalone 을 설치하지 마십시오. 이러한 다른 구성 요소가 있는 시스템에 CA SiteMinder® Federation Standalone 을 설치하면 기존 SiteMinder 설치에 부정적인 영향을 미칠 수 있습니다.
- 기존 Apache 웹 서버 또는 Apache Tomcat 서버가 있는 시스템에는 제품을 설치하지 마십시오.

설치에 필요한 정보

CA SiteMinder?Federation Standalone 을 설치하기 전에 다음 정보를 준비하십시오. 설치할 때 이러한 정보를 묻는 메시지가 나타납니다.

설치된 JDK 의 경로

CA SiteMinder® Federation Standalone 을 설치하기 전에 JDK 를 설치하고 설치 위치를 알아둡니다.

CA SiteMinder® Federation Standalone 관리자 암호

CA SiteMinder® Federation Standalone 설치 중 암호를 입력해야 합니다. CA SiteMinder® Federation Standalone UI 에 로그인할 때 이 암호를 사용하게 됩니다.

참고: CA SiteMinder® Federation Standalone 관리자 암호에는 영어(ASCII) 문자만 사용할 수 있습니다.

FIPS 모드

CA SiteMinder?Federation Standalone 은 다음의 FIPS 작동 모드 중 하나로 설치할 수 있습니다.

FIPS_COMPAT

FIPS_COMPAT(호환성) 모드는 설치 중에 사용되는 기본 FIPS 모드입니다. FIPS_COMPAT 모드에서 페더레이션 시스템은 현재의 비 FIPS 알고리즘뿐 아니라 지원되는 FIPS 호환 알고리즘도 함께 지원합니다.

FIPS_COMPAT 모드는 페더레이션의 이전 버전과도 호환됩니다. 이와 같은 호환성 기능 때문에 r12.52 SP1 이전 버전을 사용하는 환경도 r12.52 SP1 와 상호 작용할 수 있습니다. IPS_COMPAT 모드는 현재 구현되어 있는 페더레이션의 보안 수준에 만족하는 클라이언트에게도 적합합니다.

조직에서 FIPS 를 사용할 필요가 없는 경우에는 CA SiteMinder® Federation Standalone 을 FIPS_COMPAT 모드에서 설치하십시오. 추가 구성이 필요하지 않습니다.

FIPS_ONLY

FIPS_ONLY 모드의 환경에서는 FIPS 호환 알고리즘만 사용하여 중요한 데이터가 암호화됩니다.

새 설치에서 FIPS 호환 알고리즘만 사용하려는 경우에는 CA SiteMinder® Federation Standalone 을 FIPS_ONLY 모드로 설치하십시오.

중요! FIPS 모드를 변경할 때마다 CA SiteMinder® Federation Standalone 을 다시 시작하십시오.

사용할 설치 모드 결정

다음 모드 중 하나를 사용하여 CA SiteMinder?Federation Standalone 를 Windows 또는 UNIX 플랫폼에 설치할 수 있습니다.

- GUI 모드 - 그래픽 사용자 인터페이스 설치를 사용할 수 있습니다.
- 콘솔 모드 - 명령줄 설치를 사용할 수 있습니다.
- 무인 모드 - 사용자 개입이 필요 없는 파일 기반 설치가 가능합니다. 다른 시스템에서 무인 모드를 사용하려면 시스템에서 한 번의 GUI 또는 콘솔 모드 설치를 완료해야 합니다.

r12.52 SP1 의 설치 실행 파일

다음 표에는 CA SiteMinder?Federation Standalone 의 설치 실행 파일이 나와 있습니다. 표는 플랫폼별로 구성되어 있습니다.

플랫폼	설치 실행 파일
Linux	ca-fedmgr-r12.52 SP1-rhel30.bin
Solaris	ca-fedmgr-r12.52 SP1-sol.bin
Windows	ca-fedmgr-r12.52 SP1-win32.exe

지원되는 운영 체제에 대한 자세한 내용은 기술 지원 사이트의 "CA SiteMinder?Federation Standalone Platform Support Matrix"(CA SiteMinder?Federation Standalone 플랫폼 지원표)를 참조하십시오.

Windows 시스템에 CA SiteMinder® Federation Standalone 설치

이 지침은 Windows 시스템의 GUI 및 콘솔 모드 설치에 적용됩니다. 두 모드의 단계는 동일하지만 콘솔 모드에는 다음의 예외가 있습니다.

- 해당 번호를 입력하면 옵션을 선택하라는 메시지가 나타날 수 있습니다.
- 각 단계가 끝나면 Enter 키를 눌러 계속 진행합니다.
- 각 모드의 프롬프트에 따라 과정을 진행할 수 있습니다.
- 이전 단계로 가려면 BACK 을 입력합니다.

중요! 다음의 설치 제한을 확인하십시오.

- 정책 서버 또는 SPS(보안 프록시 서버)가 이미 설치된 시스템에는 CA SiteMinder® Federation Standalone 을 설치하지 마십시오. 이러한 다른 구성 요소가 있는 시스템에 CA SiteMinder® Federation Standalone 을 설치하면 기존 SiteMinder 설치에 부정적인 영향을 미칠 수 있습니다.
- 기존 Apache 웹 서버 또는 Apache Tomcat 서버가 있는 시스템에는 제품을 설치하지 마십시오.

설치 키트를 찾으려면

1. 기술 지원 사이트로 이동합니다.
2. 사이트에 로그온합니다.
3. "Download Center"(다운로드 센터)를 클릭합니다.

"Download Center"(다운로드 센터)에서 필요한 설치 키트를 검색하고 로컬 시스템으로 다운로드합니다.

Windows 에 CA SiteMinder® Federation Standalone 을 설치하려면

1. 실행 중인 모든 응용 프로그램을 종료하고 바이러스 백신 소프트웨어를 모두 중지합니다.
2. 설치를 실행합니다.

   설치를 실행하는 방법은 로컬 관리자로 로그인하는지, 네트워크 사용자로 로그인하는지에 따라 달라집니다. 네트워크 사용자인 경우 설치를 실행하려면 관리자 그룹의 구성원이어야 합니다.

   - **GUI 모드**

     로컬 관리자: *installation_executable* 을 두 번 클릭

     네트워크 사용자: *installation_executable* 을 마우스 오른쪽 단추로 클릭하고 "관리자 권한으로 실행" 선택

   - **콘솔 모드:** 명령 창을 열고 *installation_executable* -i console 입력

   CA SiteMinder® Federation Standalone 설치 마법사가 시작됩니다.

   참고: 설치 실행 파일의 목록을 확인하십시오.
3. 설치 전에 수집한 정보를 사용하여 각 설치 대화 상자의 프롬프트에 응답합니다.

   "사용권 계약" 대화 상자에서 계약서를 읽습니다. 사용권 계약의 끝까지 스크롤해야 계약을 수락하거나 수락하지 않을 수 있습니다.

4. "Install Summary"(설치 요약)에서 설치 설정을 검토하고 "설치"(GUI 모드)를 클릭하거나 Y 를 입력하여 설치(콘솔 모드)합니다.

   설치가 실행됩니다.

   설치 도중 문제가 발생하면 디렉터리 *federation_install_dir*\install_config_info 에 있는 설치 로그 파일 CA_Federation_Standalone_Install_*date_time*.log 를 검토하십시오.

5. 설치가 완료되면 시스템을 다시 시작합니다.

시스템이 다시 시작되면 구성 마법사를 실행하여 계속 진행합니다.

UNIX 시스템에 CA SiteMinder® Federation Standalone 설치

이 지침은 UNIX 시스템의 GUI 및 콘솔 모드 설치에 적용됩니다. 두 모드의 단계는 동일하지만 콘솔 모드에는 다음의 예외가 있습니다.

- 해당 번호를 입력하면 옵션을 선택하라는 메시지가 나타납니다.
- 각 단계가 끝나면 Enter 키를 눌러 계속 진행합니다.
- 각 모드의 프롬프트에 따라 과정을 진행할 수 있습니다.
- 이전 단계로 가려면 BACK 을 입력합니다.

참고: CA SiteMinder?Federation Standalone 을 설치하려는 UNIX 시스템이 IPv6 주소를 사용하는 경우에는 설치를 콘솔 모드에서만 실행하십시오. GUI 모드에서 설치하려고 하면 설치 프로그램은 타사 제한으로 인해 기본적으로 콘솔 모드를 사용합니다.

중요! 다음의 설치 제한을 확인하십시오.

- 정책 서버 또는 SPS(보안 프록시 서버)가 이미 설치된 시스템에는 CA SiteMinder® Federation Standalone 을 설치하지 마십시오. 이러한 다른 구성 요소가 있는 시스템에 CA SiteMinder® Federation Standalone 을 설치하면 기존 SiteMinder 설치에 부정적인 영향을 미칠 수 있습니다.
- 기존 Apache 웹 서버 또는 Apache Tomcat 서버가 있는 시스템에는 제품을 설치하지 마십시오.
- 루트 사용자로 CA SiteMinder® Federation Standalone 을 설치하지 마십시오. 루트 사용자로 설치하려고 하면 설치가 취소되고 오류 메시지가 나타납니다. 대신 CA SiteMinder® Federation Standalone 을 설치할 사용자 계정을 만드십시오.
- 1024 미만의 포트를 사용하는 UNIX 플랫폼에서 CA SiteMinder® Federation Standalone 을 실행하지 않는 것이 좋습니다. 이 권장 사항에는 기본 Apache HTTP 포트(80)와 기본 Apache SSL 포트(443)가 포함됩니다.
- Linux 에서는 KornShell(ksh)을 사용하여 설치를 실행하십시오.

설치 키트를 찾으려면

1. 기술 지원 사이트로 이동합니다.
2. 사이트에 로그온합니다.
3. "Download Center"(다운로드 센터)를 클릭합니다.
4. "Download Center"(다운로드 센터)에서 필요한 설치 키트를 검색하고 로컬 시스템으로 다운로드합니다.

UNIX 시스템에 CA SiteMinder® Federation Standalone 을 설치하려면

1. 실행 중인 모든 응용 프로그램을 종료하고 바이러스 백신 소프트웨어를 모두 중지합니다.
2. 필요한 권한이 없는 경우 chmod 명령을 실행하여 설치 파일에 실행 권한을 추가합니다. 예를 들어 다음과 같습니다.

   Linux: chmod +x ca-fedmgr-r12.52 SP1-rhel30.bin

3. 명령 창에서 다음 명령 중 하나를 입력합니다.
   - **GUI 모드:** *./installation_executable*
   - **콘솔 모드:** *./installation_executable* -i console

   CA SiteMinder® Federation Standalone 설치 마법사가 시작됩니다.

   참고: 설치 실행 파일의 목록은 본 안내서에 나와 있습니다.
4. 설치 전에 수집한 정보를 사용하여 설치 프롬프트에 응답합니다.

   "사용권 계약" 대화 상자에서 계약서를 읽습니다. 계약서의 끝까지 이동해야 사용권 계약을 수락 여부를 선택할 수 있습니다.
5. 설치 설정을 검토하고 "설치"(GUI 모드)를 클릭하거나 Y 를 입력하여 설치(콘솔 모드)합니다.

   CA SiteMinder® Federation Standalone 설치 프로그램이 실행됩니다.

   설치 도중 문제가 발생하면 *federation_install_dir*\install_config_info 디렉터리에 있는 설치 로그 파일 CA_Federation_Standalone_Install_date_time.log 를 검토하십시오.

설치가 완료되면 계속해서 구성 마법사를 실행하십시오.

Solaris 10 보안 속성 파일 수정 필요

기본 보안 공급자 구성이 적용되는 경우 CA SiteMinder?Federation Standalone 은 Solaris 10 시스템에서 암호화 및 암호 해독을 올바르게 실행할 수 없습니다.

이 문제를 해결하려면 java.security 속성 파일에서 PKCS11 공급자(sun.security.pkcs11.SunPKCS11) 앞에 Sun 공급자(sun.security.provider.Sun)를 나열하십시오. 이 파일은 JDK 설치의 lib/security 디렉터리에 있습니다.

java.security 파일을 다음과 같이 수정하십시오.

security.provider.1=sun.security.provider.Sun

security.provider.2=sun.security.pkcs11.SunPKCS11
${java.home}/lib/security/sunpkcs11-solaris.cfg

security.provider.3=sun.security.rsa.SunRsaSign

security.provider.4=com.sun.net.ssl.internal.ssl.Provider

security.provider.5=com.sun.crypto.provider.SunJCE

security.provider.6=sun.security.jgss.SunProvider

security.provider.7=com.sun.security.sasl.Provider

SiteMinder 커넥터 라이브러리에 대한 고려 사항

CA SiteMinder?Federation Standalone 설치에는 페더레이션 제품이 사용자 아이덴티티 정보를 SiteMinder 로 보호된 응용 프로그램과 공유할 수 있도록 해 주는 SiteMinder 커넥터가 포함되어 있습니다. 이 커넥터는 프록시 또는 독립 실행형 배포 모드에서 사용할 수 있습니다.

커넥터와 작동할 수 있도록 smauthconnectors.zip 파일이 제품 설치에 포함되어 있습니다. 아카이브에서 라이브러리를 추출하는 경우 다음 두 가지 버전의 커넥터 라이브러리가 제공됩니다.

Windows

smauthsmconnector.dll

smauthsmconnectorI18n.dll

Solaris/Linux:

libsmauthsmconnector.so

libsmauthsmconnectorI18n.so

smauthsmconnector.dll 및 libsmauthsmconnector.so 파일은 12.52 이전 라이브러리입니다. smauthsmconnectorI18n.dll 및 libsmauthsmconnectorI18n.so 파일은 새로운 라이브러리이며 다국어 문자를 처리할 수 있습니다.

CA SiteMinder?Federation Standalone 과 SiteMinder 가 함께 작동하도록 하려면 해당 라이브러리를 SiteMinder 정책 서버에 복사하십시오. 라이브러리는 다음 정책 서버 디렉터리 중 하나에 있습니다.

- **Windows:** *policy_server_home*\siteminder\bin
- **Solaris/Linux:** *policy_server_home*/siteminder/lib

복사하는 라이브러리는 몇 가지 고려 사항에 따라 달라집니다.

새로운 페더레이션 설치의 경우 다음 지침을 따르십시오.

- r12.51 이전 정책 서버와 연결을 설정하려면 12.52 이전 라이브러리를 정책 서버에 복사합니다. 새 라이브러리를 사용하지 마십시오.

  다국어 문자를 처리해야 하는 r12.51 정책 서버와 연결을 설정하려면 새 라이브러리를 정책 서버에 복사합니다. 라이브러리의 이름을 12.52 이전 버전의 이름(smauthsmconnector.dll 또는 libsmauthsmconnector.so)으로 바꿉니다.
- r12.52 이상의 정책 서버와 연결을 설정하려면 라이브러리를 복사하지 마십시오. r12.52 이상의 정책 서버에는 해당 운영 환경에 맞게 설치되는 관련 라이브러리가 있습니다.

기존의 12.52 이전 구성에서 다국어 문자를 처리하려면 다음 지침을 따르십시오.

- r12.51 이전 정책 서버의 경우 시스템에서 새 라이브러리를 사용할 수 없습니다. r12.51 이전 배포 환경에서는 국제화를 관리할 수 없습니다.
- r12.51 정책 서버의 경우 기존 라이브러리를 백업하고 새 라이브러리를 복사합니다.

  다음 단계를 수행하십시오.

  a. 정책 서버를 중지합니다.

  b. 기존 라이브러리의 백업 복사본을 만들고 고유한 이름(예: smauthsmconnector_bkup.dll)을 지정합니다.

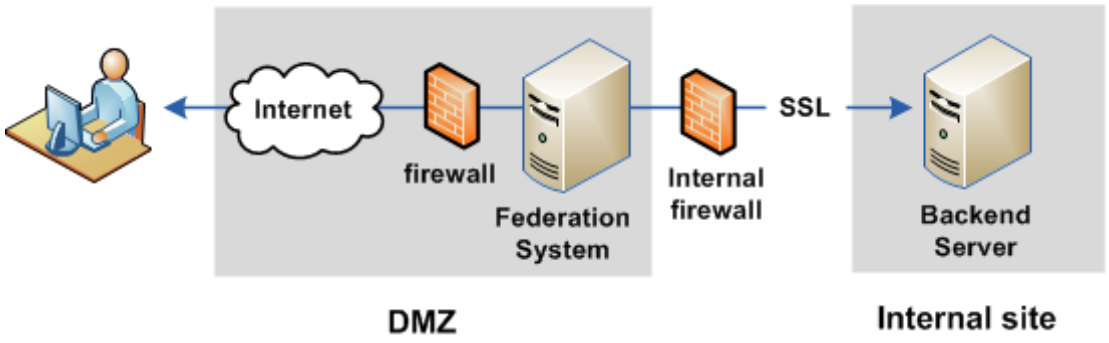
  c. 새 라이브러리를 정책 서버에 복사합니다.

  d. 12.52 이전 이름(smauthsmconnector.dll 또는 libsmauthsmconnector.so)으로 다시 이름을 바꿉니다.

  e. 정책 서버를 다시 시작합니다.

페더레이션 시스템과 백엔드 서버 사이에 SSL 사용

페더레이션된 네트워크에는 SSL 연결을 통해 백엔드 서버로 통신하는 페더레이션 시스템이 있을 수 있습니다. 네트워크 구성은 다음 그림에 나와 있습니다.



다음 단계를 수행하십시오.

1. SSL 을 사용하도록 백엔드 서버를 구성합니다.

   이에 대한 지침은 서버 설명서를 참조하십시오.

2. 페더레이션 시스템에서 서버 인증서에 서명한 CA 인증서를 ca-bundle.cert 파일에 추가합니다. 서버 인증서는 백엔드 서버가 SSL 을 활성화하기 위해 사용하는 인증서입니다.

   ca-bundle.cert 파일은 *federation_install_dir*\secure-proxy\SSL\certs 디렉터리에 있습니다.

   federation_install_dir 은 제품의 설치 위치입니다.

   이 인증서는 백엔드 서버의 관리자가 제공합니다.

Windows 또는 UNIX 플랫폼에서 페더레이션 시스템 재설치

동일한 버전의 CA SiteMinder?Federation Standalone 을 기존 설치 위에 다시 설치할 수 있습니다. 다시 설치하면 손실된 응용 프로그램 파일을 복원하거나 기본 설치 설정을 복원할 수 있습니다.

참고: 제품을 제거하지 않고 다시 설치할 수 있습니다.

다음 단계를 수행하십시오.

1. UNIX 플랫폼에서 환경 스크립트 ca_federation_env.ksh 의 경로를 수정합니다.
2. 초기 설치에 사용한 것과 동일한 프로그램을 사용하여 설치 프로그램을 다시 실행합니다.
3. 메시지가 나타나면 시스템을 다시 시작합니다.
4. 구성 마법사를 다시 실행합니다. (페이지 25)

   다시 설치 후 구성 마법사를 다시 실행합니다. 이 단계는 원래의 설치 및 구성과 동일한 설정을 사용하는지 여부에 관계없이 필요합니다.
5. 메시지가 나타나면 시스템을 다시 시작합니다.

참고: 다시 설치된 페더레이션 시스템에 Agent for Windows Authentication 을 설치한 경우에는 에이전트를 다시 구성해야 합니다. 그렇지 않으면 제대로 작동하지 않습니다.

다시 설치가 완료되었습니다.

CA SiteMinder® Federation Standalone 구성 마법사 실행

페더레이션 제품을 설치한 후 구성 마법사를 실행하십시오.

구성 마법사는 정책 저장소로 사용되는 데이터베이스, 페더레이션 서버에 대한 포트 및 Apache 웹 서버 구성을 설정합니다.

언제든지 구성 마법사를 다시 실행하여 기존 구성을 변경할 수 있지만, 다시 실행하면 기존 구성이 손실됩니다. 구성을 보존하려면 백업하십시오.

참고: SSL 이 사용되도록 설정한 상태로 Windows 시스템을 다시 구성하려면 시스템을 다시 구성하기 전에 SSL 구성을 비활성화하십시오. 재구성이 완료되면 SSL 을 다시 활성화하십시오.

다음 구성 프로세스를 완료하십시오.

1. 구성 마법사에 필요한 정보를 수집합니다.
2. 구성 마법사를 실행합니다.

구성 전 배포 모드 결정

구성 마법사를 실행할 때는 다음 배포 모드 중 하나를 선택할 수 있습니다.

- 프록시 모드
- 독립 실행형 모드

신뢰 당사자로서 페더레이션 시스템의 요청 처리 방식을 기준으로 배포 모드를 결정하십시오. 신뢰 당사자는 모드가 페더레이션 구현 방식에 큰 영향을 미치는 페더레이션된 통신의 당사자입니다.

배포 모드를 수정하려면 구성 마법사를 다시 실행하십시오.

각각의 모드는 사용자가 선택한 SAML 호환 페더레이션 제품과 함께 작동할 수 있습니다. 또한 필요한 경우 CA SiteMinder?Federation Standalone 은 SiteMinder 커넥터와 함께 작동하여 기존 SiteMinder 배포에 통합될 수 있습니다.

프록시 모드

프록시 모드 배포에서는 DMZ 의 페더레이션 시스템을 사용하여 페더레이션된 응용 프로그램을 호스트하는 백엔드 웹 서버로 요청을 전달합니다. 이러한 백엔드 시스템은 방화벽 뒤에 있으며 직접 액세스할 수 없습니다.

프록시 모드를 사용하면 다음과 같은 이점이 있습니다.

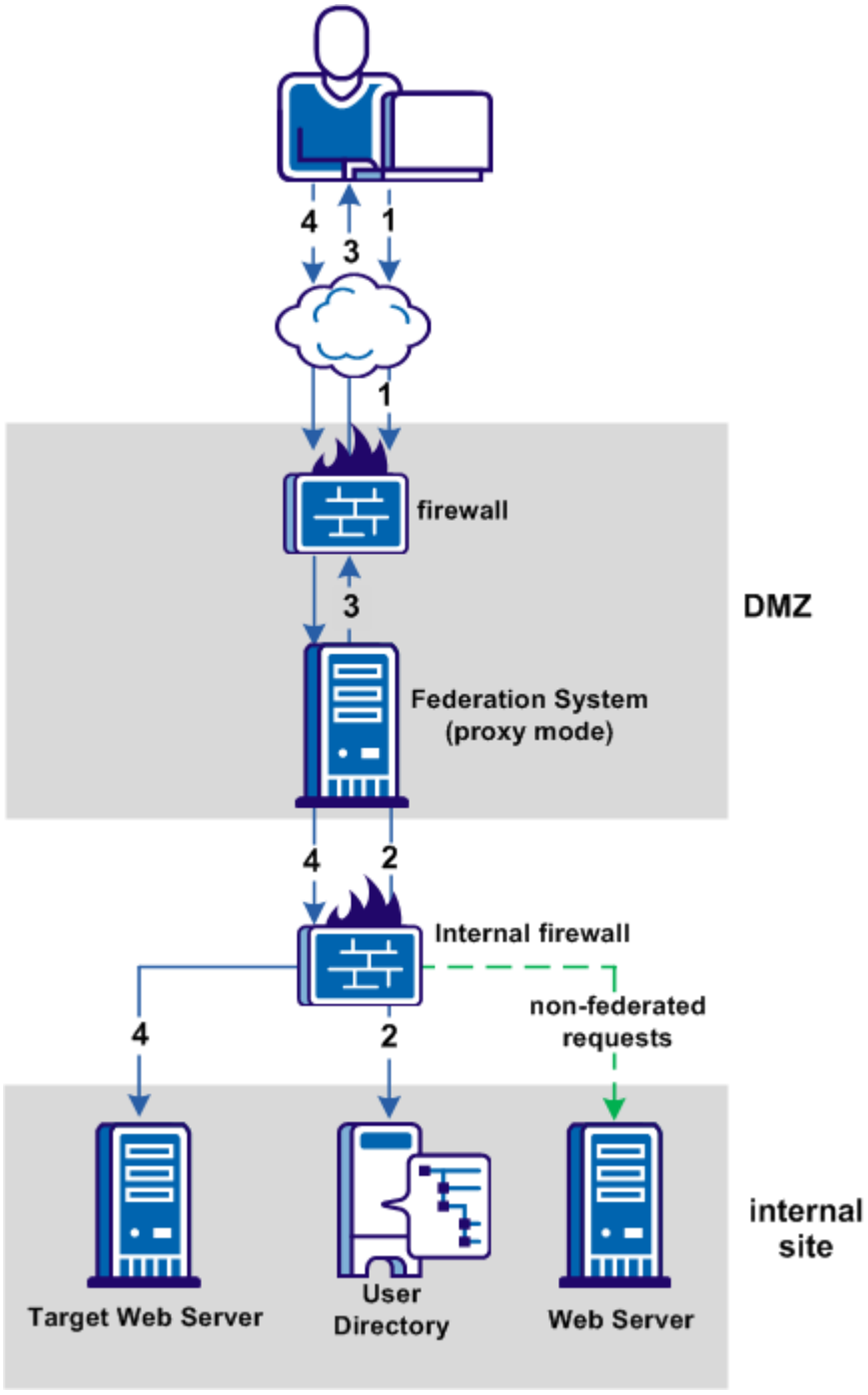
- 네트워크에 대한 하나의 액세스 지점을 제공합니다.
- 페더레이션 시스템이 SAML 어설션의 HTTP 헤더를 사용하여 백엔드 응용 프로그램에 아이덴티티 특성을 제공할 수 있습니다. 그러면 응용 프로그램을 사용자 지정하여 더 개인화된 사용자 환경을 제공할 수 있습니다.

참고: HTTP 헤더 접두사를 설정하여 권한 없는 사용자가 HTTP 헤더를 수정하는 것을 방지할 수 있습니다. 프록시 모드에서 HTTP 헤더를 보호하는 방법에 대한 자세한 정보를 확인할 수 있습니다.

프록시 모드에서 페더레이션 시스템은 *모든* 요청을 백엔드 네트워크로 전달합니다. 백엔드 웹 서버의 모든 리소스가 SiteMinder 또는 다른 액세스 제어 제품에 의해 보호되는지 확인하십시오.

예를 들어 백엔드 웹 서버가 페더레이션된 응용 프로그램 및 방화벽 뒤에서 보호되지 않는 리소스를 호스트할 수 있습니다. 관리자가 페더레이션된 응용 프로그램을 노출하면 페더레이션 시스템은 권한 부여를 확인하지 않고 백엔드 웹 서버에 대한 전체 액세스를 허용하므로 보호되지 않는 리소스도 노출됩니다. 여기에서는 페더레이션되지 않은 리소스가 URL 주소 지정이 가능한 리소스라고 가정합니다.

다음 그림에서는 신뢰 당사자의 관점에서 일반적인 프록시 모드 배포를 보여 줍니다.



위의 그림에 나타난 신뢰 당사자의 통신 흐름은 다음과 같습니다.

1. 사용자가 페더레이션된 리소스에 대한 초기 요청을 수행합니다.
2. 페더레이션 시스템은 어설션의 데이터에 기반하여 사용자를 인증하고 내부 사이트의 사용자 디렉터리에 연결하여 사용자 명확성 프로세스를 완료합니다.
3. 인증에 성공하면 리디렉션 응답이 사용자의 브라우저로 반환됩니다.
4. 페더레이션 시스템은 요청을 대상 웹 서버로 프록시하고 사용자는 리소스에 액세스합니다.

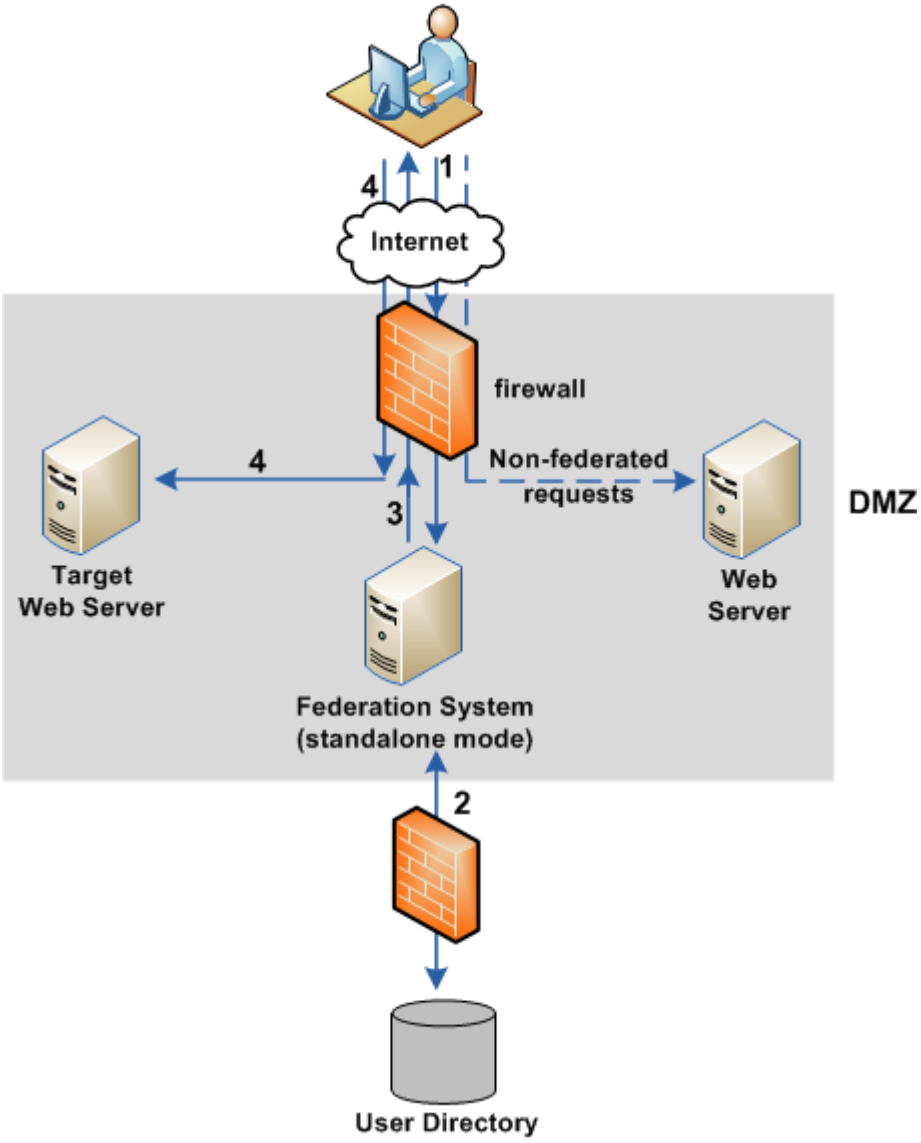
독립 실행형 모드

독립 실행형 모드 배포에서 CA SiteMinder® Federation Standalone 은 페더레이션된 요청만 처리하며 이러한 요청을 대상 웹 서버로 리디렉션합니다. 페더레이션되지 않은 요청은 CA SiteMinder® Federation Standalone 에 독립적으로 적절한 웹 서버로 직접 이동합니다.

독립 실행형 모드의 장점은 페더레이션 트래픽이 CA SiteMinder?Federation Standalone 으로 제한되며 다른 콘텐츠의 처리가 다른 웹 서버로 오프로드된다는 점입니다. 또한 사이트에서 기존 인프라의 중단 없이 네트워크에 페더레이션을 추가하는 것도 가능합니다.

독립 실행형 모드에서는 응답에 HTTP 헤더를 추가하기 위한 프록시가 웹 서버와 브라우저 사이에 없기 때문에 HTTP 헤더를 사용하여 어설션의 사용자 특성을 전달할 수 없습니다.

다음 그림에서는 신뢰 당사자의 관점에서 일반적인 독립 실행형 모드 배포를 보여 줍니다.



위의 그림에 나타난 신뢰 당사자의 통신 흐름은 다음과 같습니다.

1. 사용자가 페더레이션된 리소스를 요청합니다.
2. CA SiteMinder® Federation Standalone 은 어설션의 데이터에 기반하여 사용자를 인증하며 여기에는 사용자 명확성 프로세스를 완료하기 위한 사용자 디렉터리와의 통신이 포함됩니다.
3. CA SiteMinder® Federation Standalone 이 리디렉션 응답을 다시 사용자의 브라우저로 반환합니다.
4. 브라우저는 CA SiteMinder® Federation Standalone 을 통하지 않고도 사용자를 대상 웹 서버의 대상 리소스로 리디렉션합니다.

SiteMinder 와 함께 CA SiteMinder® Federation Standalone 배포

CA SiteMinder?Federation Standalone 에서는 사용자 아이덴티티 정보를 SiteMinder 로 보호되는 응용 프로그램과 공유할 수 있게 해 주는 SiteMinder 커넥터가 기본 제공됩니다. CA SiteMinder?Federation Standalone 과 SiteMinder 간의 이러한 통합으로 원활한 싱글 사인온이 가능합니다. SiteMinder 커넥터는 프록시 또는 독립 실행형 배포 모드에서 사용할 수 있습니다.

파트너 관계를 기준으로 SiteMinder 커넥터를 사용하도록 설정하여, 일부 파트너 관계는 커넥터를 사용할 수 있고 나머지는 사용하지 않도록 설정할 수 있습니다. 전역 SiteMinder 커넥터 개체는 하나뿐입니다. 파트너 관계에 대해 커넥터를 사용하도록 설정하면 파트너 관계는 전역 커넥터 구성을 사용합니다.

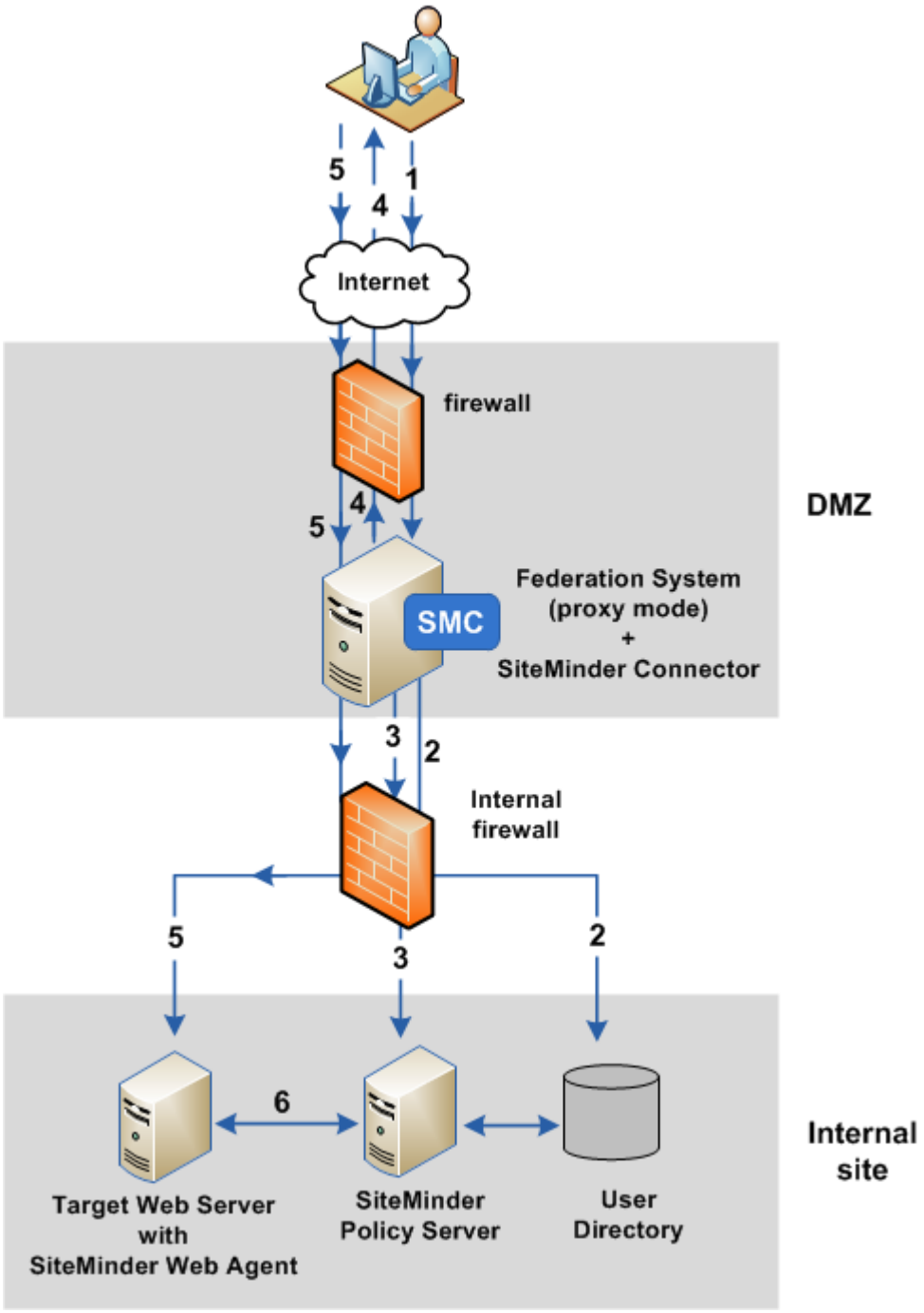
중요! SiteMinder 커넥터는 독립적 SiteMinder 설치에 연결하는 용도로 사용됩니다. SiteMinder 정책 서버 또는 SPS(보안 프록시 서버)가 이미 설치된 시스템에는 CA SiteMinder® Federation Standalone 을 설치하지 마십시오.

SiteMinder 커넥터 사용에 대한 자세한 내용은 *CA SiteMinder® Federation Standalone 안내서*를 참조하십시오.

SiteMinder 커넥터가 신뢰 당사자에 있는 프록시 모드

CA SiteMinder® Federation Standalone 이 프록시 모드에서 SiteMinder 와 통신하는 경우에도 모든 요청은 CA SiteMinder® Federation Standalone 을 통과합니다. 하지만 CA SiteMinder® Federation Standalone 은 사용자가 SiteMinder 로 보호된 리소스를 요청할 때 재인증을 받지 않도록 하기 위해 정책 서버와의 SiteMinder 세션을 설정해야 합니다. 요청은 SiteMinder 웹 에이전트로 보호되는 대상 웹 서버로 리디렉션됩니다.

다음 그림에서는 SiteMinder 커넥터가 있는 프록시 모드 아키텍처를 보여 줍니다. 이 그림은 신뢰 당사자의 관점에서 작성된 것입니다.



위의 그림에 나타난 신뢰 당사자의 통신 흐름은 다음과 같습니다.

1. 사용자가 페더레이션된 리소스를 요청하고 신뢰 당사자의 어설션 소비자 서비스로 리디렉션됩니다.
2. CA SiteMinder® Federation Standalone 은 어설션에서 받은 데이터를 기반으로 사용자를 인증하며 여기에는 사용자 명확성 프로세스를 완료하기 위한 사용자 디렉터리와의 통신이 포함됩니다.
3. CA SiteMinder® Federation Standalone 의 일부인 SiteMinder 커넥터는 SiteMinder 정책 서버의 사용자 지정 인증 스키마에 연결합니다. 정책 서버는 SiteMinder 세션 티켓을 생성하고 이를 CA SiteMinder® Federation Standalone 으로 보냅니다. 그러면 CA SiteMinder® Federation Standalone 은 티켓이 포함된 세션 쿠키를 생성합니다. SiteMinder 세션을 설정하면 나중에 대상 리소스에 액세스할 때 사용자에게 인증을 요청하지 않습니다.
4. CA SiteMinder® Federation Standalone 이 리디렉션 응답을 다시 사용자의 브라우저로 반환합니다.
5. 브라우저는 사용자를 CA SiteMinder® Federation Standalone 으로 리디렉션하고 CA SiteMinder® Federation Standalone 은 대상 리소스가 있는 웹 서버로 요청을 프록시하며, 이는 SiteMinder 웹 에이전트로 보호됩니다.
6. SiteMinder 웹 에이전트 및 정책 서버가 권한 부여 프로세스를 수행합니다.

   권한 부여에 성공하면 대상 리소스가 사용자 브라우저에 표시됩니다.

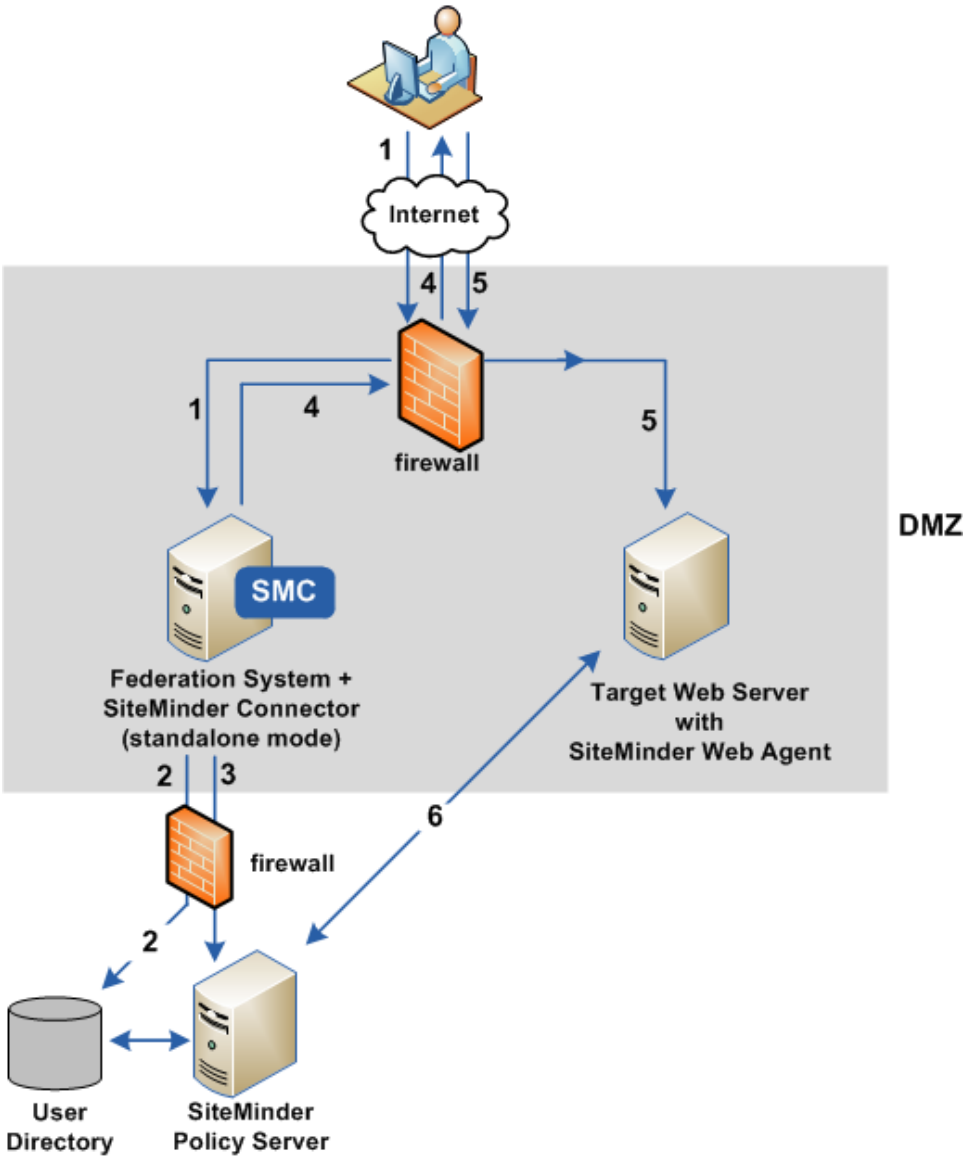
SiteMinder 커넥터가 신뢰 당사자에 있는 독립 실행형 모드

CA SiteMinder?Federation Standalone 이 독립 실행형 모드에서 기존 SiteMinder 환경과 통신하는 경우 CA SiteMinder?Federation Standalone 은 페더레이션된 요청만 처리합니다.

SiteMinder 와 함께 작동하려면 CA SiteMinder?Federation Standalone 은 사용자가 SiteMinder 로 보호되는 리소스를 요청할 때 재인증을 받지 않도록 정책 서버와의 SiteMinder 세션을 설정해야 합니다. 페더레이션된 요청은 최종적으로 대상 웹 서버로 리디렉션되며 이는 SiteMinder 웹 에이전트로 보호됩니다.

참고: CA SiteMinder® Federation Standalone 및 SiteMinder 웹 에이전트는 독립 실행형 모드에서 동일한 쿠키 도메인을 공유해야 합니다.

다음 그림에서는 SiteMinder 커넥터를 사용하는 독립 실행형 모드 아키텍처를 보여 줍니다. 이 그림은 신뢰 당사자의 관점에서 작성된 것입니다.



위의 그림에 나타난 신뢰 당사자의 통신 흐름은 다음과 같습니다.

1. 사용자가 페더레이션된 리소스를 요청하고 신뢰 당사자의 어설션 소비자 서비스로 리디렉션됩니다.
2. CA SiteMinder® Federation Standalone 은 어설션의 데이터를 기반으로 사용자를 인증하며 여기에는 사용자 명확성 프로세스를 완료하기 위한 사용자 디렉터리와의 통신이 포함됩니다.
3. CA SiteMinder® Federation Standalone 의 일부인 SiteMinder 커넥터는 SiteMinder 정책 서버의 사용자 지정 인증 스키마에 연결합니다. 정책 서버는 SiteMinder 세션 티켓을 생성하고 이를 CA SiteMinder® Federation Standalone 으로 보냅니다. 그러면 CA SiteMinder® Federation Standalone 은 티켓이 포함된 세션 쿠키를 생성합니다. SiteMinder 세션을 설정하면 나중에 대상 리소스에 액세스할 때 사용자에게 인증을 요청하지 않습니다.
4. CA SiteMinder® Federation Standalone 이 리디렉션 응답을 다시 사용자의 브라우저로 반환합니다.
5. 브라우저는 사용자를 대상 리소스가 있는 웹 서버로 리디렉션하며 이는 SiteMinder 웹 에이전트로 보호됩니다.
6. SiteMinder 웹 에이전트 및 정책 서버가 권한 부여 프로세스를 완료합니다.

   권한 부여에 성공하면 대상 리소스가 사용자 브라우저에 표시됩니다.

어설션 당사자 측에서 SiteMinder 커넥터를 사용하여 배포

어설션 당사자 측에서 SiteMinder 커넥터와 함께 구성된 CA SiteMinder?Federation Standalone 은 사용자 인증을 위해 SiteMinder 를 사용할 수 있습니다. 인증에 성공하면 사용자는 어설션을 발급하는 CA SiteMinder?Federation Standalone 으로 다시 리디렉션되어야 합니다.

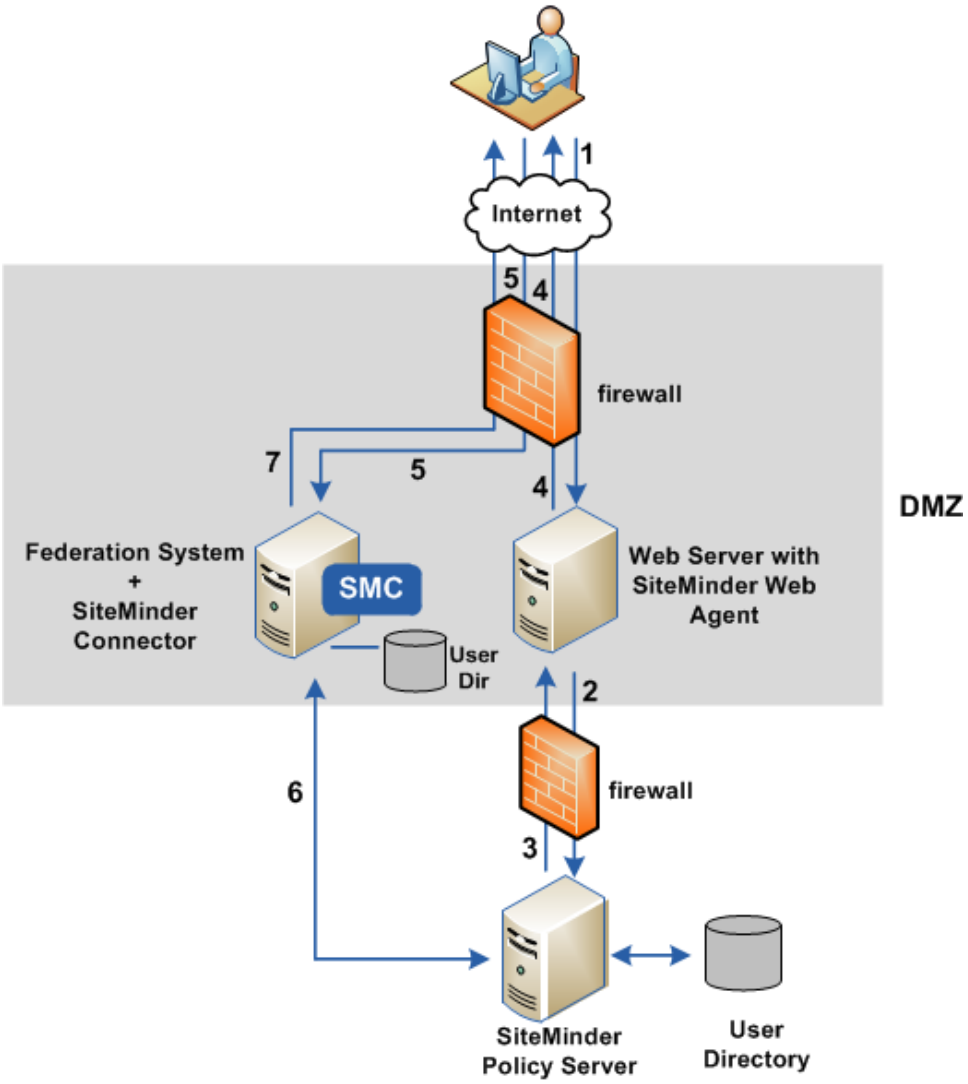
어설션 당사자 측에서 SiteMinder 는 사용자를 인증한 다음 SMSESSION 쿠키를 발급합니다. 사용자가 다시 CA SiteMinder?Federation Standalone 으로 보내질 때 SMSESSION 쿠키가 있으면 FEDSESSION 쿠키의 생성이 트리거됩니다. 이 경우 배포 모드(프록시 또는 독립 실행형)는 관련이 없습니다.

참고: CA SiteMinder?Federation Standalone 이 독립 실행형 모드에서 작동 중일 경우 CA SiteMinder?Federation Standalone 및 SiteMinder 웹 에이전트는 동일한 쿠키 도메인을 공유해야 합니다.

SiteMinder 를 사용한 배포에서 사용자는 인증을 위해 먼저 SiteMinder 에 방문해야 합니다. 인증이 성공하면 SiteMinder 로 보호되는 웹 리소스가 사용자를 다시 CA SiteMinder?Federation Standalone 으로 보내야 합니다. SiteMinder 커넥터를 사용한 배포는 위임된 인증이라고 하는 CA SiteMinder?Federation Standalone 기능과 동일하지 않습니다. 이 기능의 경우 SiteMinder 와 같은 웹 액세스 관리 시스템이 사용자 인증을 처리하도록 허용합니다. 위임된 인증이 없는 SiteMinder 커넥터 배포와 위임된 인증 간의 차이점은 위임된 인증의 경우 사용자가 SiteMinder 에서 인증을 시작할 필요가 없다는 점입니다.

위임된 인증을 사용하면 CA SiteMinder?Federation Standalone 은 인증 요청을 시작한 다음 사용자를 SiteMinder 로 리디렉션할 수 있기 때문에 기능이 적절하게 구성된 경우 리디렉션이 자동으로 수행될 수 있습니다. 사용자 인증이 성공한 후 사용자를 다시 CA SiteMinder?Federation Standalone 으로 리디렉션하려면 SiteMinder 가 보호하는 리소스는 사용자를 다시 CA SiteMinder?Federation Standalone 으로 리디렉션하기 위한 메커니즘으로 구성되어야 합니다. 리디렉션에는 보호되는 리소스가 수신한 모든 데이터가 포함되어야 합니다. 예를 들어 SiteMinder 로 보호된 리소스가 초기 인증 요청에서 몇 개의 쿼리 매개 변수를 수신한 경우에는 이 동일한 쿼리 매개 변수를 사용하여 사용자를 다시 CA SiteMinder?Federation Standalone 으로 리디렉션해야 합니다.

다음 그림에서는 어설션 당사자 측에서 SiteMinder 커넥터를 사용하는 아키텍처를 보여 줍니다.



위의 그림에 나타난 어설션 당사자의 통신 흐름은 다음과 같습니다.

1. 사용자가 페더레이션된 리소스를 요청하면 어설션 당사자에 있는 SiteMinder 웹 에이전트에 대해 인증 요청이 트리거됩니다.
2. 인증 요청은 SiteMinder 정책 서버로 전달됩니다.
3. 정책 서버는 사용자를 인증하고 SiteMinder 세션 티켓을 생성합니다. 티켓은 SiteMinder 웹 에이전트로 반환되며 여기에서 이 티켓이 포함된 SMSESSION 쿠키가 생성됩니다.

4. 웹 에이전트는 CA SiteMinder® Federation Standalone 에 대한 리디렉션 응답과 함께 SMSESSION 쿠키를 사용자 브라우저로 전달합니다.
5. 사용자 브라우저는 SMSESSION 쿠키와 함께 CA SiteMinder® Federation Standalone 으로 리디렉션됩니다.
6. CA SiteMinder® Federation Standalone 은 SiteMinder 정책 서버에 연결하여 SMESSION 쿠키의 유효성을 검사합니다.
7. SMSESSION 쿠키의 유효성 검사에 성공하면 CA SiteMinder® Federation Standalone 세션이 생성됩니다. 그러면 CA SiteMinder® Federation Standalone 은 대상 리소스가 있는 신뢰 당사자에 대한 나머지 페더레이션 통신을 처리합니다.

구성 마법사에 필요한 정보

구성 마법사를 실행하기 전에 다음 정보를 준비하십시오.

데이터베이스 유형

정책 저장소에 사용할 데이터베이스 유형(SQL 또는 Oracle)을 지정합니다.

데이터베이스 정보

CA SiteMinder® Federation Standalone 이 사용하는 데이터베이스를 식별합니다.

데이터베이스 서버

데이터베이스가 설치된 서버의 IP 주소 또는 호스트 이름을 지정합니다. 데이터베이스는 데이터 저장소 리포지토리입니다.

운영 환경 및 데이터베이스 유형에 따라 다음 항목이 허용됩니다.

Windows(Oracle 및 SQL): IPv4 주소, IPv6 주소, 호스트 이름

UNIX(Oracle): IPv4 주소, 호스트 이름

UNIX(SQL): IPv4 주소, IPv6 주소, 호스트 이름

중요! 이 필드의 IPv6 주소 앞뒤에 대괄호를 사용하지 마십시오. 괄호의 생략은 이 설정에만 적용됩니다. 예: 3ff3:1900:4545:3:200:f8ff:fe25:67(대괄호 없음)

SQL 데이터베이스 명명된 인스턴스를 사용하려면 운영 환경에 대해 다음 값을 입력하십시오.

Windows: *server_name**named_instance*

예: server01-w3s-t1\federation1

이 예에서 server01-w3s-t1 은 서버 이름이고 federation1 은 인스턴스 이름입니다.

UNIX: *server_name*

SQL 명명된 인스턴스가 아니라 데이터베이스 서버 이름을 이 필드에 지정하십시오. 또한 SQL 명명된 인스턴스의 포트 번호를 "데이터베이스 포트" 필드에 입력하십시오.

예: server01-w3s-t1

데이터베이스 이름

데이터베이스 인스턴스의 이름을 지정합니다.

제한

SQL: 데이터베이스 이름

Oracle: CA SiteMinder® Federation Standalone 이 데이터베이스 테이블을 만들고 관리하는 테이블스페이스에 대해 CONNECT 및 RESOURCE 역할을 가진 Oracle 사용자의 이름입니다.

데이터베이스 포트

데이터베이스가 수신 대기하는 포트를 식별합니다. 데이터베이스가 기본 포트에서 실행되고 있지 않은 경우 포트 번호를 변경하십시오. 예를 들어 데이터베이스 서버에 대해 SQL 명명된 인스턴스를 지정한 경우 이 데이터베이스 인스턴스의 포트를 입력하십시오.

기본값

SQL:1433

Oracle: 1521

데이터베이스 사용자 이름

데이터베이스에 액세스하고, 데이터베이스 테이블을 만들고 관리할 수 있는 슈퍼 관리 권한을 가진 관리자의 이름을 지정합니다.

사용자 이름에는 슬래시(/)를 제외한 모든 인쇄 가능 문자를 사용할 수 있습니다. 슬래시를 사용하면 데이터베이스 연결이 실패하므로 Oracle 데이터베이스에는 슬래시를 사용할 수 없습니다.

데이터베이스 암호

데이터베이스 관리자 계정의 암호를 지정합니다. 암호에는 슬래시(/)를 제외한 모든 인쇄 가능 문자를 사용할 수 있습니다. 슬래시를 사용하면 데이터베이스 연결이 실패하므로 Oracle 데이터베이스에는 슬래시를 사용할 수 없습니다.

CA SiteMinder® Federation Standalone 서버 포트

CA SiteMinder® Federation Standalone 이 수신 대기하는 TCP 포트 번호를 지정합니다.

기본값: 44442

제한: 44443, 44444, 44445 를 제외한 숫자 값. 포트 번호 44443, 44444, 44445 는 허용되지 않습니다.

배포 모드

사용자 환경에서 CA SiteMinder® Federation Standalone 을 구현할 방법을 결정합니다.

배포 모드 옵션은 다음과 같습니다.

프록시 모드

프록시 모드 배포에서는 CA SiteMinder® Federation Standalone 이 모든 백엔드 리소스에 대한 기본 진입점입니다.

다음의 경우에 이 모드를 선택합니다.

- 네트워크에 대한 하나의 액세스 지점이 필요한 경우
- 개인화된 사용자 환경을 제공하기 위해 백엔드 응용 프로그램에 SAML 어설션의 특성이 필요한 경우. SAML 어설션 특성은 헤더로 전달될 수 있습니다.

참고: HTTP 헤더 접두사를 설정하여 권한 없는 사용자가 HTPP 헤더를 수정하는 것을 방지할 수 있습니다. 프록시 모드에서 HTTP 헤더를 보호하는 방법에 대한 자세한 정보를 확인할 수 있습니다.

독립 실행형 모드

독립 실행형 모드 배포에서는 CA SiteMinder® Federation Standalone 이 SiteMinder 웹 에이전트 또는 타사 웹 서버와 함께 배포됩니다. 이 경우 CA SiteMinder® Federation Standalone 은 페더레이션 요청만 처리하고 다른 모든 요청은 웹 서버가 처리합니다.

페더레이션 트래픽을 CA SiteMinder® Federation Standalone 으로 제한하고 일반적인 웹 트래픽의 처리는 다른 웹 서버로 오프로드하려는 경우에 이 모드를 선택하십시오.

독립 실행형 모드에서는 HTTP 헤더를 사용하여 어설션의 사용자 특성을 전달할 수 없습니다. HTTP 헤더를 응답에 추가할 수 없습니다. 웹 서버와 브라우저 사이에는 이러한 수정을 수행할 메커니즘이 없습니다.

서버 호스트 이름(프록시 모드에만 해당)

CA SiteMinder® Federation Standalone 이 페더레이션된 리소스에 대한 요청을 전달하는 백엔드 서버의 정규화된 도메인 이름을 식별합니다.

Apache 구성

CA SiteMinder® Federation Standalone 은 오픈 소스 Apache 웹 서버를 들어오는 요청의 HTTP 수신기로 사용합니다.

서버 이름

CA SiteMinder® Federation Standalone 배포의 정규화된 도메인 이름을 식별합니다. 이 서버 이름은 반드시 CA SiteMinder® Federation Standalone 이 설치된 시스템에 매핑되지 않아도 됩니다. 서버를 가상 호스트로 간주할 수 있습니다.

관리자 전자 메일 주소

데이터베이스 관리자의 전자 메일 주소를 지정합니다.

CA SiteMinder® Federation Standalone 과 함께 설치된 Apache 서버에 이 설정이 필요합니다. Apache 서버는 문제 발생 시 기본 오류 메시지에 관리자의 전자 메일 주소를 사용합니다. 전자 메일 주소는 ServerAdmin 지시문으로 설정되며 모든 유효한 전자 메일 주소가 될 수 있습니다.

참고: 이 주소로 전달되는 이벤트는 Apache 서버에 대한 서버별 오류 및 경고입니다. 메시지는 페더레이션과 관련이 없습니다.

Apache HTTP 포트

HTTP 요청을 수신 대기하는 포트를 지정합니다.

기본값: 80

참고: 시스템에 포트 80 을 사용하는 다른 웹 서버가 있는 경우 Apache 웹 서버의 기본 포트를 변경하십시오.

Apache SSL 포트

SSL 요청을 수신 대기하는 Apache 포트를 지정합니다.

기본값: 443

참고: 시스템에 포트 443 을 사용하는 다른 웹 서버가 있는 경우 Apache 웹 서버의 기본 SSL 포트를 변경하십시오.

관리 UI HTTP 포트

CA SiteMinder® Federation Standalone UI HTTP 요청을 수신 대기하는 포트를 지정합니다.

이 포트를 변경하는 경우 포트는 내부를 향해야 하며 인터넷에서 액세스할 수 없어야 합니다.

기본값: 8888

관리 UI SSL 포트

CA SiteMinder® Federation Standalone UI SSL 요청을 수신 대기하는 포트를 지정합니다.

이 포트를 변경하는 경우 포트는 내부를 향해야 하며 인터넷에서 액세스할 수 없어야 합니다.

기본값: 8889

중요! 포트 번호는 다음 설정에 대해 고유해야 합니다.

- CA SiteMinder® Federation Standalone 서버 포트
- Apache HTTP 포트
- Apache SSL 포트
- 관리 UI HTTP 포트
- 관리 UI SSL 포트

구성 실행 파일

다음 표에는 CA SiteMinder?Federation Standalone 의 구성 실행 파일이 나와 있습니다. 표는 플랫폼별로 구성되어 있습니다.

플랫폼	구성 실행 파일
Linux	ca-Federation-config.sh
Solaris	ca-Federation-config.sh
Windows	ca-federation-config.exe

지원되는 운영 체제에 대한 자세한 내용은 기술 지원 사이트의 "CA SiteMinder?Federation Standalone Platform Support Matrix"(CA SiteMinder?Federation Standalone 플랫폼 지원표)를 참조하십시오.

Windows 에서 구성 마법사 실행

구성 마법사를 실행하기 전에 먼저 CA SiteMinder?Federation Standalone 을 설치하고 구성 마법사에 필요한 모든 정보를 수집하십시오. CA SiteMinder?Federation Standalone 을 다시 설치할 때 항상 구성 마법사를 실행하십시오.

이 지침은 Windows 시스템의 GUI 및 콘솔 모드 구성에 적용됩니다. 두 모드의 단계는 동일하지만 콘솔 모드에는 다음의 예외가 있습니다.

- 해당 번호를 입력하여 옵션을 선택할 수 있습니다.
- 각 단계가 끝나면 Enter 키를 눌러 계속 진행합니다.
- 이전 단계로 가려면 BACK 을 입력합니다.

각 모드의 프롬프트에 따라 과정을 진행할 수 있습니다.

다음 단계를 수행하십시오.

1. 구성 마법사를 실행합니다.

   마법사를 실행하는 방법은 로컬 관리자로 로그인하는지, 네트워크 사용자로 로그인하는지에 따라 달라집니다. 네트워크 사용자인 경우 마법사를 실행하려면 관리자 그룹의 구성원이어야 합니다.

   - **GUI 모드**

     로컬 관리자: "시작" 메뉴에서 바로 가기를 선택하거나 "시작", "모든 프로그램", "CA", "Federation Standalone", "CA SiteMinder® Federation Standalone 구성 마법사"를 선택합니다.

     네트워크 사용자: "시작" 메뉴에서 바로 가기를 마우스 오른쪽 단추로 클릭하거나 "시작", "모든 프로그램", "CA", "Federation Standalone"을 선택한 다음 "CA SiteMinder® Federation Standalone 구성 마법사"를 마우스 오른쪽 단추로 클릭하고 "관리자 권한으로 실행"을 선택합니다.

   - **콘솔 모드:** 명령 창을 열고 *federation_install_dir*\install_config_info 로 이동한 후 다음 명령을 입력합니다.

     ca-federation-config.exe -i -console

     경로가 자동으로 설정되지 않으므로 올바른 위치에서 이 명령을 실행하십시오.

2. 마법사를 실행하기 전에 수집한 정보를 사용하여 구성 마법사 프롬프트에 응답합니다.

3. 구성 설정을 검토하고 "설치"(GUI 모드)를 클릭하거나 Y 를 입력(콘솔 모드)하여 구성을 실행합니다.

   CA SiteMinder® Federation Standalone 구성이 실행됩니다.

   구성 도중 문제가 발생하면 *federation_install_dir*\install_config_info 에 있는 구성 로그 파일 CA_SiteMinder_Federation_Standalone_Configuration.log 를 검토하십시오.

4. CA SiteMinder® Federation Standalone 시스템을 재부팅합니다.

CA SiteMinder?Federation Standalone 의 설치와 구성이 완료됩니다.

중요! 배포 모드 전환 등의 작업을 위해 구성을 변경하려면 구성 마법사를 다시 실행하십시오. 마법사를 다시 실행할 때 CA SiteMinder® Federation Standalone 서비스가 실행되고 있어야 합니다. 구성 마법사는 언제라도 다시 실행할 수 있지만 다시 실행하면 기존 구성이 손실됩니다. 구성 마법사를 다시 실행하기 전에 SSL 연결을 보존할 수 있도록 기존 구성을 백업하십시오.

UNIX 시스템에서 구성 마법사 실행

구성 마법사를 실행하기 전에 먼저 CA SiteMinder?Federation Standalone 을 설치하고 구성 마법사에 필요한 모든 정보를 수집하십시오. CA SiteMinder?Federation Standalone 을 다시 설치할 때 항상 구성 마법사를 실행하십시오.

중요! CA SiteMinder® Federation Standalone 를 재설치하는 경우 구성 마법사를 다시 실행하십시오. 구성 마법사를 다시 실행하기 전에 SSL 및 데이터베이스 연결을 보존할 수 있도록 기존 구성을 백업하십시오. ODBC 사용자 디렉터리를 사용하는 경우에는 system_odbc.ini 파일도 백업하십시오. 이 파일은 *federation_install_dir*/siteminder/db/ 디렉터리에 있습니다.

이 지침은 UNIX 시스템의 GUI 및 콘솔 모드 설치에 적용됩니다. 두 모드의 단계는 동일하지만 콘솔 모드에는 다음의 예외가 있습니다.

- 해당 번호를 입력하여 옵션을 선택할 수 있습니다.
- 각 단계가 끝나면 Enter 키를 눌러 계속 진행합니다.
- 이전 단계로 가려면 BACK 을 입력합니다.

각 모드의 프롬프트에 따라 과정을 진행할 수 있습니다.

참고: CA SiteMinder?Federation Standalone 을 구성하려는 UNIX 시스템이 IPv6 주소를 사용하는 경우에는 구성 마법사를 콘솔 모드에서만 실행하십시오. GUI 모드를 사용하려고 하면 프로그램은 타사 제한으로 인해 기본적으로 콘솔 모드를 사용합니다.

중요! 루트 사용자로 구성 마법사를 실행하지 마십시오. 루트로 실행하려고 하면 마법사가 취소되고 오류 메시지가 나타납니다. 설치를 실행한 것과 동일한 사용자로 구성 마법사를 실행하십시오.

구성 마법사를 실행하려면

1. 콘솔 창을 엽니다.
2. *federation_install_dir* 디렉터리로 이동합니다.
3. 환경 스크립트 ca_federation_env.ksh 의 경로를 수정합니다.
4. 명령 창(Linux 의 경우 ksh 창 사용)에 다음 명령 중 하나를 입력합니다.
   - **GUI 모드:** ./ca-Federation-config.sh
   - **콘솔 모드:** ./ca-Federation-config.sh -i console

   구성 마법사가 시작됩니다.
5. 마법사를 실행하기 전에 수집한 정보를 사용하여 구성 마법사 프롬프트에 응답합니다.

6. 구성 설정을 검토하고 "설치"(GUI 모드)를 클릭하거나 Y 를 입력하여 설치(콘솔 모드)합니다.

   CA SiteMinder® Federation Standalone 이 구성됩니다.

   구성 도중 문제가 발생하면 *federation_install_dir*/install_config_info 에 있는 구성 로그 파일 CA_Federation_Manager_ConfigLog.log 를 검토하십시오.

   CA SiteMinder® Federation Standalone 의 설치와 구성이 완료됩니다.

7. 다음 스크립트를 실행하여 CA SiteMinder® Federation Standalone 을 시작합니다.

   federation_install_dir/fedmanager.sh start

중요! 배포 모드 전환 등의 작업을 위해 구성을 변경하려면 구성 마법사를 다시 실행하십시오. 마법사를 다시 실행할 때 CA SiteMinder?Federation Standalone 서비스가 실행되고 있어야 합니다. 구성 마법사는 언제라도 다시 실행할 수 있지만 다시 실행하면 기존 구성이 손실됩니다. 구성 마법사를 다시 실행하기 전에 SSL 연결을 보존할 수 있도록 기존 구성을 백업하십시오.

CA SiteMinder® Federation Standalone 에 대한 가상 호스트 구성

CA SiteMinder?Federation Standalone 에 대해 여러 가상 호스트를 정의할 수 있습니다. 가상 호스트를 사용하면 어설션 당사자와 신뢰 당사자를 동일한 시스템에 설치할 수 있으므로 테스트 용도로 유용할 수 있습니다. 또한 여러 가상 호스트를 정의하면 검색 서비스에 별도의 호스트 이름 및 도메인을 사용하여 SAML 2.0 IdP 검색 프로필을 구성할 수 있습니다.

여러 가상 호스트를 정의할 때 CA SiteMinder?Federation Standalone 에 필요한 구성 설정은 다음과 같습니다.

- server.conf 파일의 hostnames 매개 변수에 호스트를 추가합니다. server.conf 파일은 다음 디렉터리에 있습니다.

  federation_install_dir\secure-proxy\proxy-engine\conf

- CA SiteMinder® Federation Standalone 이 CA SiteMinder® Federation Standalone UI 에 액세스하는 데 사용하는 것과 동일한 시스템에서 작동 중이거나, 페더레이션 트랜잭션을 실행하는 시스템과 동일한 시스템에서 작동 중인 경우에는 httpd.conf 파일을 업데이트합니다. httpd.conf 파일은 *federation_install_dir*\secure-proxy\httpd\conf 디렉터리에 있습니다.

  참고: 포함된 웹 서버에 대해 SSL 이 사용되도록 설정한 경우 httpd-ssl.conf 파일을 다음과 같이 변경하십시오. httpd-ssl.conf 파일은 *federation_install_dir*\secure-proxy\httpd\conf\extra folder 디렉터리에 있습니다.

  사용하는 시스템 유형에 기반하여 httpd.conf 파일을 다음과 같이 업데이트하십시오.

  - IPV4 기반 시스템의 경우 다음과 같이 LISTEN 지시문을 추가합니다.

    LISTEN 127.0.0.1:*port*

  - IPv4 및 IPv6 을 지원하는 이중 스택 시스템의 경우 다음과 같이 LISTEN 지시문을 추가합니다.

    LISTEN 127.0.0.1:*port*

    LISTEN [::1]:*port*

  - IPv6 시스템의 경우 다음과 같이 LISTEN 지시문을 추가합니다.

    LISTEN [::1]:*port*

  또한 시스템의 호스트 파일에서 새 호스트 이름이 추가되도록 루프백 주소 항목을 업데이트합니다. 값은 다음과 같습니다.

  - IPv4: 127.0.0.1
  - IPv6: [::1]

CA SiteMinder® Federation Standalone 무인 설치

CA SiteMinder?Federation Standalone 을 설치하는 방법 중 하나로 무인 설치가 있습니다. 무인 설치를 사용하면 사용자 개입 없이 제품을 설치할 수 있습니다.

무인 설치를 실행하려면 먼저 수동 설치를 실행해야 합니다. 수동 설치에서는 수동 설치 중 입력한 모든 매개 변수, 경로 및 암호가 포함된 *ca-federation-installer.properties* 라는 파일이 생성됩니다. 무인 설치를 수행하면 일반적으로 사용자가 수동으로 입력해야 하는 설정이 이 속성 파일을 통해 제공됩니다.

기본 속성 파일을 사용하여 초기 설치와 동일한 설정으로 설치를 실행하거나, 이 파일을 사용자 환경에 맞게 수정하는 템플릿으로 사용할 수 있습니다. 속성 파일의 내용은 대/소문자가 구분되므로 수정할 때 주의해야 합니다.

중요! CA SiteMinder® Federation Standalone 을 처음 설치한 시스템과 동일한 플랫폼의 시스템에서만 무인 설치를 실행할 수 있습니다. 예를 들어 Solaris 시스템에 제품을 설치한 다음 이 속성 파일을 사용하여 Windows 시스템에서 무인 설치를 실행할 수 없습니다.

설치 속성 파일 설정

네트워크의 다른 시스템에 설치 설정을 전파하려면 ca-federation-installer.properties 파일을 사용하십시오.

중요! 속성 파일을 생성하려면 먼저 수동 설치를 실행해야 합니다.

이 속성 파일로 다음을 수행할 수 있습니다.

- 파일에서 설치 매개 변수를 정의합니다.
- 네트워크에서 CA SiteMinder® Federation Standalone 을 설치하려는 시스템에 속성 파일 및 설치 실행 파일을 복사합니다.

ca-federation-installer.properties 파일은 다음 위치에 생성됩니다.

Windows: *federation_install_dir*\install-config-info

UNIX: *federation_install_dir*/install-config-info

파일의 기본 매개 변수 및 경로에는 초기 설치 시 입력한 정보가 반영됩니다.

설치 속성 파일을 수정하려면

1. ca-federation-installer.properties 파일을 열고 파일의 매개 변수를 수정합니다.

   참고: 속성 파일은 대/소문자를 구분합니다.

2. 파일을 저장합니다.

매개 변수는 다음과 같습니다.

매개 변수	정의
DEFAULT_PRODUCT_INSTALL_TYPE	설치가 새 설치인지, 업그레이드인지 아니면 재설치인지를 정의합니다. **기본값:** INSTALL
DEFAULT_INSTALL_DIR	기본값(Windows): C:\\Program Files\\CA\\FederationManager (이중 백슬래시에 주의) 기본값(UNIX): 시스템의 계정 예: /home/myacct/CA/FederationManager
서버별 항목	
DEFAULT_JRE_ROOT	JRE 의 위치를 나타냅니다.
JDK_ROOT	JDK 의 위치를 나타냅니다.

매개 변수	정의
#FEDADMIN_PW	CA SiteMinder® Federation Standalone 의 암호를 정의합니다. 이 매개 변수는 주석 처리를 제거해야 하며 암호를 일반 텍스트로 입력해야 합니다. 보안을 강화하려면 ENCRYPTED_FEDADMIN_PASSWORD 설정을 사용하십시오. **참고:** CA SiteMinder® Federation Standalone 관리자 암호에는 영어(ASCII) 문자만 사용할 수 있습니다.
ENCRYPTED_FEDADMIN_PASSWORD	CA SiteMinder® Federation Standalone 암호를 암호화된 형식으로 표시합니다. 보안을 강화하려면 이 암호화된 암호를 사용하는 것이 좋습니다. 모든 시스템에서 동일한 관리자 암호를 사용하려면 이 암호를 그대로 두고 FEDADMIN_PW 속성의 주석 처리를 제거하지 마십시오.
FIPS 모드 설정	
FED_FIPS_VALUE	FIPS 140-2 작동 모드를 지정합니다. **제한:** ■ ONLY ■ COMPAT
LGPL 라이선스 설정	
ACCEPT_LGPL_EULA	LGPL 사용권 계약에 동의할지 여부를 지정합니다. *federation_install_dir*/install_config_info 디렉터리의 사용권 계약 내용(httpclient-EULA.txt)을 검토하십시오. 사용권 계약에 동의하려면 이 변수를 YES 로 설정하십시오. **기본값:** NO

CA SiteMinder® Federation Standalone 무인 설치 실행

무인 설치를 실행하여 사용자 개입 없이 CA SiteMinder?Federation Standalone 을 설치할 수 있습니다.

참고: 무인 설치를 실행하기 전에 수동 설치를 실행하여 ca-Federation-installer.properties 파일을 만드십시오. 다른 시스템에서 무인 설치를 실행하려면 이 파일이 필요합니다. 이 파일은 설치에 필요한 대로 수정할 수 있습니다.

다음 단계를 수행하십시오.

1. CA SiteMinder® Federation Standalone 이 이미 설치된 시스템에서 다음 두 개의 파일을 임시 위치로 복사합니다.
   - 설치 실행 파일 또는 바이너리
   - ca-Federation-installer.properties 파일
2. 설치 및 속성 파일을 복사한 위치에서 다음 명령을 실행합니다.

   installation_executable -f ca-federation-installer.properties -i silent

무인 모드에서 설치가 시작되고 속성 파일의 매개 변수를 사용하여 CA SiteMinder?Federation Standalone 을 설치합니다.

참고: Windows 에서 무인 설치를 확인하려면 *federation_install_dir*\install_config_info 디렉터리에 있는 설치 로그 파일 CA_Federation_Standalone_Install_date_time.log 를 검토하십시오.

무인 CA SiteMinder® Federation Standalone 구성

CA SiteMinder?Federation Standalone 을 구성하는 방법 중 하나로 무인 구성이 있습니다. 무인 구성을 사용하면 사용자 개입 없이 CA SiteMinder?Federation Standalone 을 구성할 수 있습니다.

무인 구성을 실행하려면 먼저 컴퓨터에서 CA SiteMinder?Federation Standalone 을 수동으로 구성해야 합니다. 수동으로 구성하면 *ca-federation-config.properties* 라는 파일이 생성되며 이 파일을 사용하여 다른 컴퓨터에서 무인 구성을 실행합니다. 기본적으로 ca-federation-config.properties 에는 초기 구성의 설정이 포함됩니다.

ca-federation-config.properties 파일에는 초기 구성 중 입력한 모든 매개 변수, 경로 및 암호가 포함됩니다. 무인 구성을 수행하면 일반적으로 사용자가 수동으로 입력해야 하는 설정이 이 속성 파일을 통해 제공됩니다.

기본 속성 파일을 사용하여 초기 구성과 동일한 설정으로 구성을 실행하거나, 이 파일을 사용자 환경에 맞게 수정하는 템플릿으로 사용할 수 있습니다.

속성 파일을 네트워크에 있는 둘 이상의 시스템에서 사용하려는 경우에는 APACHE_SERVER_NAME 설정을 무인 구성을 실행하는 각 시스템마다 고유한 값으로 설정해야 합니다. 둘 이상의 시스템에 동일한 서버 이름을 사용하면 충돌이 발생합니다.

중요! CA SiteMinder® Federation Standalone 을 처음 설치한 시스템과 동일한 플랫폼의 시스템에서만 무인 구성을 실행할 수 있습니다. 예를 들어 Solaris 시스템에서 제품을 구성한 다음 이 속성 파일을 사용하여 Linux 시스템에서 무인 구성을 실행할 수 없습니다.

구성 속성 파일 설정

무인 구성은 ca-federation-config.properties 파일을 사용하여 CA SiteMinder?Federation Standalone 구성을 네트워크의 다른 시스템에 전파합니다.

이 속성 파일로 다음을 수행할 수 있습니다.

- 파일에서 구성 매개 변수를 정의합니다.
- 네트워크에서 CA SiteMinder® Federation Standalone 을 구성하려는 모든 시스템에 속성 파일 및 구성 실행 파일을 복사합니다.

ca-federation-config.properties 파일은 다음 위치에 설치됩니다.

Windows: *federation_install_dir*\install-config-info

UNIX: *federation_install_dir*/install-config-info

파일의 기본 매개 변수 및 경로에는 초기 구성 시 입력한 정보가 반영됩니다.

중요! 구성 속성 파일은 대/소문자를 구분합니다.

구성 속성 파일을 수정하려면

1. ca-federation-config.properties 파일을 열고 파일의 매개 변수를 수정합니다.
2. 파일을 저장합니다.

매개 변수는 다음과 같습니다.

매개 변수	설명
데이터베이스 정보	
PARAM_DBTYPE	데이터베이스의 유형(SQL 또는 Oracle)을 나타냅니다.
PARAM_UID	데이터베이스 관리자 사용자 이름을 표시합니다.
#PARAM_PWD	UI 에 로그인하는 데 사용되는 CA SiteMinder® Federation Standalone 관리자 암호를 일반 텍스트로 식별합니다. 값을 입력하기 전에 이 행의 주석 처리를 제거하십시오. 보안을 강화하려면 ENCRYPTED_PARAM_PWD 설정을 사용하십시오.
ENCRYPTED_PARAM_PWD	암호화된 CA SiteMinder® Federation Standalone 관리자 암호를 지정합니다. 보안을 강화하려면 이 암호화된 암호를 사용하는 것이 좋습니다.
PARAM_DB_SERVER	데이터베이스 서버의 IP 주소를 식별합니다.
PARAM_DB_PORT	데이터베이스가 수신 대기하는 포트를 표시합니다. **기본값:** ■ SQL: 1433 ■ Oracle: 1521
MSSQL 특정	
PARAM_DB	MS-SQL 특정 매개 변수입니다. SQL 데이터베이스 이름을 지정합니다.
Oracle 특정	

매개 변수	설명
ORACLE_SID	Oracle 특정 매개 변수입니다. Oracle 데이터베이스의 **서비스 이름**(SID 가 아님)을 지정합니다.
RECONFIGURE	CA SiteMinder® Federation Standalone 이 기존 데이터베이스 스키마를 사용하는지 아니면 새 스키마를 만드는지를 지정합니다. **제한:** true(기존 스키마 사용), false(새 스키마 만들기)
서버 포트	
PARAM_PORT	CA SiteMinder® Federation Standalone 이 수신 대기하는 포트를 정의합니다. **기본값:** 44442 **중요!** 이 포트에 44445 값을 할당하지 마십시오.
배포 모드	
DEPLOYMENT_MODE	CA SiteMinder® Federation Standalone 배포 모드를 지정합니다. **제한:** ■ 프록시(대문자 P) ■ 독립 실행형(대문자 S)
PROXY_HOST_NAME	(프록시 모드에만 해당) CA SiteMinder® Federation Standalone 이 페더레이션된 리소스에 대한 요청을 전달하는 백엔드 서버의 정규화된 도메인 이름을 식별합니다. *server_name.domain:port* 구문을 사용하여 이 설정을 정의합니다. 예: myserver.mycompany.ca.com:5555 이 속성 파일을 둘 이상의 CA SiteMinder® Federation Standalone 시스템에서 사용하고 이들 시스템이 동일한 프록시를 사용하는 경우에는 각 시스템에 대해 이 호스트 이름을 동일한 값으로 설정하십시오. CA SiteMinder® Federation Standalone 및 프록시 호스트는 동일한 도메인에 있어야 합니다.

매개 변수	설명
Apache 서버 정보	
APACHE_SERVER_NAME	Apache 웹 서버의 이름을 지정합니다. 속성 파일을 네트워크에 있는 둘 이상의 시스템에서 사용하려는 경우에는 이 값을 무인 구성을 실행하는 각 시스템마다 고유한 값으로 설정하십시오. 둘 이상의 시스템에 동일한 서버 이름을 사용하면 충돌이 발생합니다.
APACHE_ADMIN_EMAIL	CA SiteMinder® Federation Standalone 관리자의 전자 메일 주소를 나타냅니다. 이 설정은 CA SiteMinder® Federation Standalone 의 일부로 설치된 Apache 서버에 필요합니다. Apache 는 문제가 발생했을 때 기본 오류 메시지에 관리자의 전자 메일 주소를 사용합니다. 전자 메일 주소는 ServerAdmin 지시문으로 설정되며 모든 유효한 전자 메일 주소가 될 수 있습니다. 이 주소로 전달되는 이벤트는 Apache 서버에 대한 서버별 오류 및 경고입니다. 메시지는 페더레이션과 관련이 없습니다. **기본값:** admin@mycompany.com
APACHE_HTTP_PORT	Apache 웹 서버가 수신 대기하는 기본 포트를 지정합니다. **기본값:** 80
APACHE_SSL_PORT	Apache 웹 서버가 수신 대기하는 기본 SSL 포트를 지정합니다. **기본값:** 443
UI_HTTP_PORT	Administrative UI 가 수신 대기하는 기본 HTTP 포트를 지정합니다. **기본값:** 8888
UI_SSL_PORT	Administrative UI 가 수신 대기하는 기본 SSL 포트를 지정합니다. **기본값:** 8889

중요! 포트 번호는 다음 설정에 대해 고유해야 합니다.

- CA SiteMinder® Federation Standalone 서버 포트
- Apache HTTP 포트
- Apache SSL 포트
- 관리 UI HTTP 포트
- 관리 UI SSL 포트

무인 구성을 실행합니다.

사용자 개입 없이 CA SiteMinder?Federation Standalone 을 구성할 수 있습니다.

참고: ca-Federation-config.properties 파일을 만들려면 먼저 시스템을 수동으로 구성해야 합니다. 이 파일을 네트워크에 맞게 수정할 수 있습니다.

다음 단계를 수행하십시오.

1. CA SiteMinder® Federation Standalone 이 이미 설치된 시스템에서 다음 두 개의 파일을 임시 위치로 복사합니다.
   - 구성 실행 파일 또는 바이너리 (페이지 44)
   - ca-Federation-config.properties
2. 설치 및 속성 파일을 복사한 위치에서 다음 명령을 실행합니다.

   configuration_executable -f ca-federation-config.properties -i silent

   설정용 속성 파일의 매개 변수를 사용하여 무인 모드에서 구성이 시작됩니다.
3. Windows 에서는 구성이 끝나면 시스템을 재부팅합니다.

   참고: Windows 에서 무인 설치를 확인하려면 *federation_install_dir*\install_config_info 디렉터리에 있는 설치 로그 파일 CA_Federation_Standalone_Install_*date_time*.log 를 검토하십시오.

Administrative UI 에 로그인합니다.

Administrative UI 를 통해 페더레이션 시스템을 구성할 수 있습니다.

중요! 한 번에 한 명의 관리자만 Administrative UI 에 로그온할 수 있습니다. 또한 관리자는 하나의 브라우저 인스턴스만 열 수 있습니다.

다음 단계를 수행하십시오.

1. 브라우저에서 Java 스크립트가 사용되도록 설정되어 있는지 확인합니다. 이 설정은 Administrative UI 를 여는 데 필요합니다.
2. 사용하는 플랫폼에 대한 지침을 따르십시오.

   Windows

   "시작", "모든 프로그램", "CA", "Federation Standalone", "Federation Standalone 관리 UI"를 차례로 선택합니다.

   UNIX

   웹 브라우저를 열고 URL 로 http://*fed_server:ui_port*/ca/federation/adminui 를 입력합니다.

   fed_server:ui_port

   Administrative UI 의 포트를 포함하여 CA SiteMinder® Federation Standalone 가 설치되어 있는 서버의 정규화된 도메인 이름을 지정합니다. 기본 포트는 8888 입니다.

   예:

   http://fed1.ca.com:8888/ca/federation/adminui

   로그인 창이 나타납니다.
3. 사용자 이름과 암호를 입력하고 "로그인"을 클릭합니다.

   중요! 사용자 이름은 항상 **admin** 입니다. 이 이름은 변경할 수 없습니다. 관리자 암호는 설치할 때 설정됩니다.

Administrative UI 가 시작됩니다.

제 2 장: CA SiteMinder® Federation Standalone 제거

Windows 에서 페더레이션 시스템 제거

시스템에서 더 이상 필요하지 않을 경우 CA SiteMinder?Federation Standalone 을 제거하십시오.

다음 단계를 수행하십시오.

1. "시작", "모든 프로그램", "CA", "Federation Standalone", "CA SiteMinder® Federation Standalone 제거"를 차례로 선택합니다.

   제거 마법사가 실행됩니다.
2. 마법사의 지시를 따릅니다.
3. 제거가 완료되면 필요에 따라 *federation_install_dir* 로 이동하여 FederationManager 폴더와 해당 하위 폴더를 삭제합니다.
4. 시스템을 재부팅합니다.

제품이 제거되었습니다.

UNIX 시스템에서 CA SiteMinder® Federation Standalone 제거

시스템에서 더 이상 필요하지 않을 경우 CA SiteMinder?Federation Standalone 을 제거하십시오.

다음 단계를 수행하십시오.

1. 명령 창을 엽니다.
2. *federation_install_dir* 디렉터리로 이동합니다.
3. 환경 스크립트 ca_federation_env.ksh 의 경로를 수정합니다.
4. 다음 명령을 입력하여 제거 스크립트를 실행합니다.

   ./ca-Federation-uninstall.sh
5. 필요한 경우 *federation_install_dir* 디렉터리로 이동하여 CA SiteMinder® Federation Standalone 폴더 및 모든 하위 폴더를 삭제합니다.

제품이 제거되었습니다.

제 3 장: 12.x 시스템을 CA SiteMinder® Federation Standalone r12.52 SP1 로 업그레이드

이 섹션은 다음 항목을 포함하고 있습니다.

CA SiteMinder® Federation Standalone 의 업그레이드 및 마이그레이션 경로 (페이지 63)
CA SiteMinder® Federation Standalone r12.52 SP1 로 업그레이드하는 방법 (페이지 65)

CA SiteMinder® Federation Standalone 의 업그레이드 및 마이그레이션 경로

업그레이드는 기존 12.x 버전을 실행하는 시스템에서 새 버전의 CA SiteMinder?Federation Standalone 으로 업데이트하는 것입니다.
업그레이드하려면 기존 시스템은 새 버전의 제품이 지원하는 운영 체제, 데이터베이스 및 JDK 를 실행해야 합니다.

마이그레이션은 기존 시스템의 구성을 r12.52 SP1 가 새로 설치된 시스템으로 복제하는 것입니다. 새 페더레이션 시스템은 지원되는 데이터베이스 버전과 통신해야 합니다.

참고:

- r12.52 SP1 환경으로 마이그레이션할 경우 지원되는 데이터베이스가 포함되어야 합니다. r12.52 SP1 가 지원하지 않는 데이터베이스가 사용자 환경에서 사용되고 있는 경우에는 지원되는 데이터베이스 서버를 설치하고 데이터를 새 데이터베이스로 이동하십시오. 마지막으로 r12.52 SP1 로 마이그레이션합니다.
- r12.52 SP1 로 업그레이드할 때 Federation Agent for Windows Authentication 이 설치된 경우에는 에이전트를 페더레이션 시스템과 동일한 버전으로 업그레이드하십시오. 그렇지 않으면 에이전트가 제대로 작동하지 않습니다.

버전별 상세 내용은 기술 지원 사이트의 "Platform Support Matrix"(플랫폼 지원표)를 참조하십시오.

사용 가능한 다음 경로에 기반하여 r12.52 SP1 로 업그레이드하거나 마이그레이션할 수 있습니다.

Windows

기존 페더레이션 버전	데이터베이스가 r12.52 SP1 에서 작동하는지 여부	업그레이드 또는 마이그레이션
모든 SP 를 포함한 r12.0	아니요	r12.52 SP1 로 마이그레이션
모든 SP 를 포함한 r12.1	아니요	r12.52 SP1 로 마이그레이션
r12.1 SP3	예	r12.52 SP1 로 업그레이드

Solaris/Linux

기존 페더레이션 버전	데이터베이스가 r12.52 SP1 에서 작동하는지 여부	업그레이드 또는 마이그레이션
모든 SP 를 포함한 r12.0	아니요	r12.52 SP1 로 마이그레이션

기존 페더레이션 버전	데이터베이스가 r12.52 SP1 에서 작동하는지 여부	업그레이드 또는 마이그레이션
모든 SP 를 포함한 r12.1	아니요	r12.52 SP1 로 마이그레이션
r12.1 SP3	예	r12.52 SP1 로 업그레이드

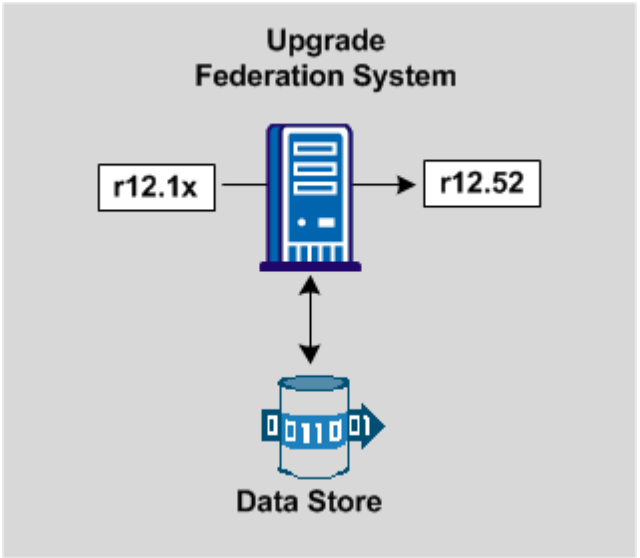
FIPS 마이그레이션

CA SiteMinder?Federation Standalone 은 비 FIPS 에서 FIPS 전용 환경으로의 마이그레이션을 지원하지만 마이그레이션 프로세스가 복잡합니다. 비 FIPS 에서 FIPS 전용 환경으로 마이그레이션하려면 먼저 r12.52 SP1 로의 업그레이드를 완료하십시오. 업그레이드가 성공적으로 수행되면 FIPS 마이그레이션 프로세스를 수행합니다.

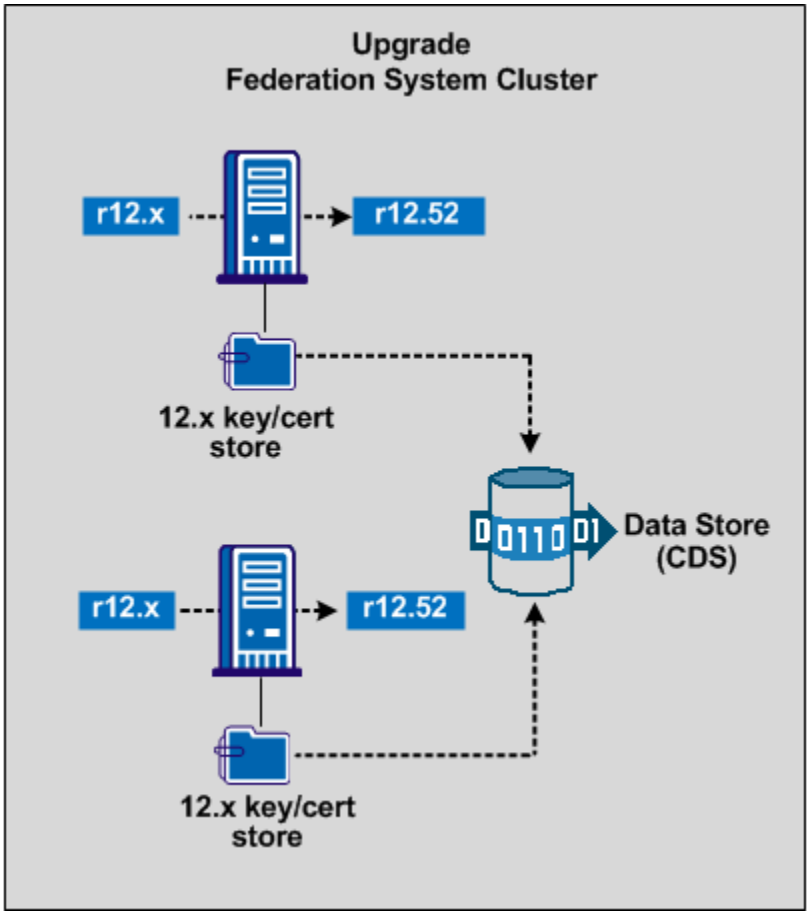
CA SiteMinder® Federation Standalone r12.52 SP1 로 업그레이드하는 방법

Windows 및 UNIX(Solaris 및 Linux) 시스템의 CA SiteMinder?Federation Standalone 을 r12.52 SP1 로 업그레이드할 수 있습니다. 기존 시스템은 r12.52 SP1 를 지원하는 운영 플랫폼 및 데이터베이스를 실행해야 합니다.

다음 그림에서는 단일 시스템의 업그레이드 경로를 보여 줍니다.



다음 그림에서는 클러스터 환경의 업그레이드를 보여 줍니다.



장애 조치를 지원하도록 CA SiteMinder?Federation Standalone 클러스터를 설정할 수 있습니다. 기존 r12.x 클러스터에서 새 클러스터로 업그레이드하려면 비클러스터 업그레이드와 비슷한 절차를 따르십시오. 현재 운영 플랫폼이 r12.52 SP1 를 지원하는 것으로 가정하고 기존 클러스터의 각 시스템을 r12.52 SP1 로 업그레이드합니다.

클러스터의 시스템은 하나의 데이터 저장소를 공유합니다. 업그레이드를 감지하는 r12.52 SP1 설치 프로그램을 실행하면 키 및 인증서 정보가 자동으로 CDS(인증서 데이터 저장소)로 이동합니다. CDS 는 기본 데이터 저장소와 같은 곳에 있습니다.

업그레이드 프로세스는 다음과 같습니다.

1. 여러 개의 키 데이터베이스를 동기화합니다(클러스터를 업그레이드하는 경우에만).
2. 파트너 관계에 고유 백 채널 사용자 이름이 있는지 확인합니다.
3. 데이터 저장소와 키 저장소를 포함하여 기존 구성을 백업합니다.
4. 설치 프로그램을 실행하여 r12.52 SP1 로 업그레이드합니다. 설치 프로그램은 업그레이드를 감지할 수 있습니다.

각 절차는 다음 단원에서 자세히 설명합니다.

키 데이터베이스 동기화

12.5 이전 시스템에서는 개인 키 및 인증서 데이터를 smkeydatabase 라고 하는 키 저장소에 저장했습니다. 이제 이 데이터는 데이터 저장소와 함께 있는 인증서 데이터 저장소에 저장됩니다. 인증서 데이터 저장소를 사용하면 환경의 각 페더레이션 시스템이 로컬 smkeydatabase 에 액세스할 필요가 없습니다.

설치 관리자는 업그레이드 도중 로컬 smkeydatabase 를 자동으로 백업하고 모든 콘텐츠를 인증서 데이터 저장소로 마이그레이션하려고 시도합니다. 이 프로세스에서는 마이그레이션을 시작하기 전에 smkeydatabase 와 CDS 를 비교합니다. 이렇게 비교하는 목적은 마이그레이션 실패를 초래할 수 있는 데이터 불일치(예: 서로 다른 인증서에 동일한 별칭이 매핑된 경우)를 식별하는 것입니다.

클러스터 환경에는 smkeydatabase 의 인스턴스가 여러 개 있습니다. r12.52 SP1 로 업그레이드 또는 마이그레이션하기 전에 정보 일관성을 유지하기 위해 모든 smkeydatabase 인스턴스를 동기화하십시오. 데이터베이스를 동기화하면 각 인스턴스가 CDS 로 마이그레이션될 때 불일치가 발생하는 것을 방지할 수 있습니다.

Administrative UI 의 "인증서 및 키" 탭에서 smkeydatabase 인스턴스 간의 모든 데이터 불일치를 해결하십시오. 다음 데이터가 여러 키 데이터베이스 인스턴스 간에 일관성을 유지하는지 확인하십시오.

- 각 CA 인증서는 여러 인스턴스 간에 일관되게 인증서 해지 목록을 참조해야 합니다.
- **예:** CA 인증서는 LDAP 디렉터리 서비스의 인증서 해지 목록을 일관되게 참조합니다.
- defaultentpriseprivatekey 별칭이 모든 인스턴스에서 동일한 개인 키/인증서 쌍을 나타냅니다.
- 동일한 별칭이 동일한 인증서 또는 키/인증서 쌍에 매핑됩니다.
- 동일한 CA 인증서가 동일한 인증서 해지 목록에 매핑됩니다.
- 해지되거나 만료된 인증서가 없습니다.
- 모든 CRL 정보가 올바릅니다.

중요! 모든 데이터 불일치를 해결한 후에는 마이그레이션이 모두 완료되기 전까지 smkeydatabase 인스턴스를 변경하지 마십시오.

기존 파트너 관계에 고유 백 채널 사용자 이름이 있는지 확인

HTTP-아티팩트 싱글 사인온 트랜잭션 중에 어설션 당사자가 보안이 유지되는 백 채널을 통해 어설션을 신뢰 당사자에게 반환합니다. 엔터티가 백 채널에 액세스하려면 인증이 필요하도록 설정할 수 있습니다. 백 채널에 대한 인증 방법으로 "기본"을 선택하는 경우 사용자 이름이 필요합니다.

업그레이드하기 전에 동일한 SAML 프로필 내 각 페더레이션된 파트너 관계가 수신 백 채널에 대해 고유한 사용자 이름을 사용하는지 확인하십시오. 두 개의 SAML 2.0 또는 SAML 1.x 파트너 관계가 수신 백 채널 사용자 이름을 공유할 수 없습니다.

참고: SAML 1.x 및 SAML 2.0 파트너 관계는 수신 백 채널 사용자 이름을 공유할 수 있지만 권장되지는 않습니다.

수신 백 채널 사용자 이름을 공유하는 동일한 프로토콜의 파트너 관계가 있는 경우 업그레이드 전에 다음 단계를 수행하십시오.

1. 파트너 관계 중 하나를 비활성화합니다.
2. 파트너 관계에 정의된 백 채널 사용자 이름을 변경합니다.
3. 원격 파트너에게 이 변경 사항을 알립니다.

파트너 관계를 다시 활성화합니다.

기존 구성 백업

구성 및 키 데이터베이스의 백업은 시스템 복구나 마이그레이션에 유용합니다.

구성을 백업하려면 키 데이터베이스를 복사하고 구성 데이터를 내보내십시오. 제품에 포함되어 있는 XPSExport 도구를 사용하면 구성 데이터를 XML 파일로 내보낼 수 있습니다.

중요! 내보내기 프로세스 중에는 페더레이션 트랜잭션을 진행할 수 없습니다.

구성을 백업하려면

1. 키 데이터베이스를 복사하여 안전한 위치에 저장합니다. 키 데이터베이스는 다음 디렉터리에 있습니다.

   federation_install_dir/siteminder/smkeydatabase

2. 명령 창에서 다음 명령을 입력하여 CA SiteMinder® Federation Standalone 구성을 내보냅니다.

   XPSExport *export_file_name* -xa -passphrase *passphrase*

   export_file_name

   내보내기를 통해 생성되는 출력 파일의 이름을 지정합니다. XPSExport 에서 생성하는 출력은 XML 형식이기 때문에 파일 이름도 **.xml** 확장명으로 끝나야 합니다.

   passphrase

   중요한 데이터를 암호화하는 데 필요한 암호를 지정합니다. 암호는 8 자 이상이고 숫자, 대문자, 소문자를 각각 하나 이상 포함해야 합니다. 암호에 공백이 포함되어 있는 경우 암호를 따옴표로 묶어야 합니다.

   참고: 암호를 직접 입력하지 않으려면 명령에서 제외해도 됩니다. 그러면 XPSExport 도구가 화면에 표시되지 않게 암호와 암호 확인을 묻는 메시지를 표시합니다.

이제 키 데이터베이스 복사본 및 암호화된 구성 데이터가 포함된 XML 파일이 만들어졌습니다.

Windows 에서 CA SiteMinder® Federation Standalone r12.52 SP1 로 업그레이드

CA SiteMinder?Federation Standalone 을 지원하는 운영 플랫폼이 실행되고 있는 Windows 시스템에서는 동일한 운영 플랫폼에서 CA SiteMinder?Federation Standalone r12.52 SP1 로 직접 업그레이드할 수 있습니다.

r12.52 SP1 에서 지원되지 않는 운영 체제에서 기존 시스템을 실행하는 경우 직접 업그레이드할 수 없으므로 먼저 구성을 마이그레이션하십시오 (페이지 77).

참고: 업그레이드하기 전에 파트너 관계를 비활성화할 필요가 없습니다.

r12.52 SP1 CA SiteMinder?Federation Standalone 설치 관리자 실행 파일을 실행하여 업그레이드하십시오. 업그레이드하더라도 이전 CA SiteMinder?Federation Standalone 구성이 유지됩니다.

중요! 다음의 설치 제한을 확인하십시오.

- 정책 서버 또는 SPS(보안 프록시 서버)가 이미 설치된 시스템에는 CA SiteMinder® Federation Standalone 을 설치하지 마십시오. 이러한 다른 구성 요소가 있는 시스템에 CA SiteMinder® Federation Standalone 을 설치하면 기존 SiteMinder 설치에 부정적인 영향을 미칠 수 있습니다.
- 기존 Apache 웹 서버 또는 Apache Tomcat 서버가 있는 시스템에는 제품을 설치하지 마십시오.

설치 관리자가 smkeydatabase 파일을 발견하면 설치 관리자는 다음 작업을 수행합니다.

- smkeydatabase 를 백업합니다.
- 콘텐츠를 인증서 데이터 저장소로 마이그레이션하려고 시도합니다.

중요! smkeydatabase 마이그레이션에 실패할 경우 시스템을 원래 환경으로 되돌리지 마십시오. 이 경우 인증서 데이터를 필요로 하는 모든 트랜잭션이 실패하게 됩니다.

설치 키트를 찾으려면

1. CA 기술 지원 사이트에 로그온합니다.
2. "Download Center"(다운로드 센터)를 클릭합니다.
3. "Download Center"(다운로드 센터)에서 필요한 설치 키트를 검색합니다.

Windows 에서 CA SiteMinder® Federation Standalone 을 업그레이드하려면

1. 실행 중인 응용 프로그램을 모두 종료합니다.
2. 설치 프로그램을 실행할 폴더로 이동합니다.
3. 설치 실행 파일을 폴더로 복사합니다.

   참고: 설치 실행 파일의 목록을 확인하십시오.
4. *installation_executable* 를 두 번 클릭합니다.

   설치 마법사가 시작됩니다.
5. 설치를 진행합니다.
6. 설치 설정을 검토하고 "설치"를 클릭합니다.

7. 설치 프로그램이 실행되어 시스템을 업그레이드합니다.

   메시지가 나타나면 시스템을 다시 시작합니다.

8. 시스템이 업그레이드에 의해 생성된 새 파일을 사용하도록 AssertionGeneratorFramework.properties 파일의 이름을 변경합니다.

   a. *federation_install_dir*\siteminder\config\properties 로 이동합니다.

   b. 보존하기 위해 기존 AssertionGeneratorFramework.properties 파일의 이름을 AssertionGeneratorFramework.properties.old 등과 같이 변경합니다.

   c. 업그레이드에 의해 생성되는 AssertionGeneratorFramework.properties.new 파일에서 .new 확장명을 제거합니다.

9. 업그레이드가 완료되면 올바른 파일이 로드되도록 브라우저에서 모든 임시 파일을 지웁니다.

참고: SiteMinder 커넥터가 활성화된 환경에서 업그레이드하는 경우 커넥터를 사용하는 파트너 관계는 변경이 필요 없이 계속 작동합니다. 업그레이드가 완료된 후 개별 파트너 관계를 기준으로 커넥터를 활성화 또는 비활성화할 수 있습니다. 업그레이드 전에 커넥터가 활성화되지 않은 경우 지정된 파트너 관계와 사용할 수 있도록 활성화하고 구성하십시오.

업그레이드 오류 발생 시 수행할 작업

데이터베이스 업그레이드가 실패하면 CA SiteMinder?Federation Standalone 은 policy_store_upgrade 스크립트를 실행하라는 내용의 오류 메시지를 표시합니다. 업그레이드 스크립트(policy_store_upgrade.bat)는 *federation_install_dir*/install_config_info 에 있습니다.

설치 도중 다른 문제가 발생하면 설치 로그 파일 CA_Federation_Standalone_Install_*date_time*.log 및 업그레이드 로그 파일 CA_Federation_policy_store_upgrade.log 를 검토하십시오. 두 파일 모두 *federation_install_dir*/install_config_info 디렉터리에 있습니다.

UNIX 에서 CA SiteMinder® Federation Standalone r12.52 SP1 로 업그레이드

UNIX 시스템에서는 동일한 운영 플랫폼과 동일한 데이터베이스에서 CA SiteMinder?Federation Standalone r12.52 SP1 로 직접 업그레이드할 수 있습니다.

r12.52 SP1 에서 지원되지 않는 운영 체제에서 기존 시스템을 실행하는 경우 직접 업그레이드할 수 없으므로 먼저 구성을 마이그레이션하십시오 (페이지 77).

r12.52 SP1 CA SiteMinder® Federation Standalone 설치 관리자를 실행합니다. 업그레이드하더라도 이전 구성이 유지됩니다.

설치 관리자가 smkeydatabase 파일을 발견하면 설치 관리자는 다음 작업을 수행합니다.

- smkeydatabase 를 백업합니다.
- 콘텐츠를 인증서 데이터 저장소로 마이그레이션하려고 시도합니다.

중요! smkeydatabase 마이그레이션에 실패할 경우 시스템을 원래 환경으로 되돌리지 마십시오. 이 경우 인증서 데이터를 필요로 하는 모든 트랜잭션이 실패하게 됩니다.

이 지침은 UNIX 시스템의 GUI 및 콘솔 모드 설치에 적용됩니다. 두 모드의 단계는 동일하지만 콘솔 모드에는 다음의 예외가 있습니다.

- 해당 번호를 입력하면 옵션을 선택하라는 메시지가 나타날 수 있습니다.
- 각 단계가 끝나면 Enter 키를 눌러 계속 진행합니다.
- 각 모드의 프롬프트에 따라 과정을 진행할 수 있습니다.
- 이전 단계로 가려면 BACK 을 입력합니다.

중요! 다음의 설치 제한을 확인하십시오.

- 정책 서버 또는 SPS(보안 프록시 서버)가 이미 설치된 시스템에는 CA SiteMinder® Federation Standalone 을 설치하지 마십시오. 이러한 다른 구성 요소가 있는 시스템에 CA SiteMinder® Federation Standalone 을 설치하면 기존 SiteMinder 설치에 부정적인 영향을 미칠 수 있습니다.
- 기존 Apache 웹 서버 또는 Apache Tomcat 서버가 있는 시스템에는 제품을 설치하지 마십시오.

r12.52 SP1 CA SiteMinder?Federation Standalone 설치 관리자를 실행하여 CA SiteMinder?Federation Standalone 을 업그레이드하십시오. 플랫폼에 맞는 설치 관리자를 선택하십시오.

지원 사이트에서 설치 키트를 찾으려면

1. CA 기술 지원 사이트에 로그온합니다.
2. "Download Center"(다운로드 센터)를 클릭합니다.
3. "Download Center"(다운로드 센터)에서 필요한 설치 키트를 검색합니다.

CA SiteMinder® Federation Standalone 을 업그레이드하려면

중요! 루트 사용자로 업그레이드를 실행하지 마십시오. 루트로 설치하려고 하면 설치가 취소되고 오류 메시지가 나타납니다. 대신 CA SiteMinder?Federation Standalone 을 설치할 새 사용자 계정을 만드십시오.

1. 실행 중인 응용 프로그램을 모두 종료합니다.

   참고: 업그레이드하기 전에 파트너 관계를 비활성화할 필요가 없습니다.
2. 필요한 경우 chmod 명령을 실행하여 설치 파일에 실행 권한을 추가합니다. 예를 들어 다음과 같습니다.

   chmod +x *ca-fed-executable*-sol.bin
3. 설치 프로그램을 실행할 폴더로 이동합니다.
4. 설치 바이너리를 폴더로 복사합니다.
5. 명령 창에서 다음 명령 중 하나를 입력합니다.
   - **GUI 모드:** *./installation_binary*
   - **콘솔 모드:** *./installation_binary* -i console

   예(GUI 모드): *./ca-fed-executable*-sol.bin

   설치 마법사가 시작됩니다.
6. 설치를 진행합니다.
7. 설치 설정을 검토하고 "설치"(GUI 모드)를 클릭하거나 Y 를 입력하여 설치(콘솔 모드)합니다.

   CA SiteMinder® Federation Standalone 설치 프로그램이 실행되고 서비스가 다시 시작됩니다.

8. 시스템이 업그레이드에 의해 생성된 새 파일을 사용하도록 AssertionGeneratorFramework.properties 파일의 이름을 변경합니다.
   a. *federation_install_dir*\siteminder\config\properties 로 이동합니다.
   b. 보존하기 위해 기존 AssertionGeneratorFramework.properties 파일의 이름을 AssertionGeneratorFramework.properties.old 등과 같이 변경합니다.
   c. 업그레이드에 의해 생성되는 AssertionGeneratorFramework.properties.new 파일에서 .new 확장명을 제거합니다.
9. 업그레이드가 완료되면 올바른 CA SiteMinder® Federation Standalone 파일이 로드되도록 브라우저에서 모든 임시 파일을 지웁니다.

참고: SiteMinder 커넥터가 활성화된 환경에서 업그레이드하는 경우 커넥터를 사용하는 파트너 관계는 변경이 필요 없이 계속 작동합니다. 업그레이드가 완료된 후 개별 파트너 관계를 기준으로 커넥터를 활성화 또는 비활성화할 수 있습니다. 업그레이드 전에 커넥터가 활성화되지 않은 경우 지정된 파트너 관계와 사용할 수 있도록 활성화하고 구성하십시오.

업그레이드 오류 발생 시 수행할 작업

데이터베이스 업그레이드가 실패하면 CA SiteMinder?Federation Standalone 은 policy_store_upgrade 스크립트를 실행하라는 내용의 오류 메시지를 표시합니다. 업그레이드 스크립트(policy_store_upgrade.sh)는 *federation_install_dir*/install_config_info 에 있습니다.

설치 도중 다른 문제가 발생하면 설치 로그 파일 CA_Federation_Standalone_Install_*date_time*.log 및 업그레이드 로그 파일 CA_Federation_policy_store_upgrade.log 를 검토하십시오. 두 파일 모두 *federation_install_dir*/install_config_info 디렉터리에 있습니다.

중요! smkeydatabase 마이그레이션에 실패할 경우 시스템을 원래 환경으로 되돌리지 마십시오. 이 경우 인증서 데이터를 필요로 하는 모든 트랜잭션이 실패하게 됩니다.

제 4 장: CA SiteMinder® Federation Standalone r12.52 SP1 로 마이그레이션

이 섹션은 다음 항목을 포함하고 있습니다.

CA SiteMinder® Federation Standalone 의 업그레이드 및 마이그레이션 경로 (페이지 77)
r12.52 SP1 로 마이그레이션하는 방법 (페이지 79)
장애 조치 배포를 마이그레이션하는 방법 (페이지 96)

CA SiteMinder® Federation Standalone 의 업그레이드 및 마이그레이션 경로

업그레이드는 기존 12.x 버전을 실행하는 시스템에서 새 버전의 CA SiteMinder?Federation Standalone 으로 업데이트하는 것입니다. 업그레이드하려면 기존 시스템은 새 버전의 제품이 지원하는 운영 체제, 데이터베이스 및 JDK 를 실행해야 합니다.

마이그레이션은 기존 시스템의 구성을 r12.52 SP1 가 새로 설치된 시스템으로 복제하는 것입니다. 새 페더레이션 시스템은 지원되는 데이터베이스 버전과 통신해야 합니다.

참고:

- r12.52 SP1 환경으로 마이그레이션할 경우 지원되는 데이터베이스가 포함되어야 합니다. r12.52 SP1 가 지원하지 않는 데이터베이스가 사용자 환경에서 사용되고 있는 경우에는 지원되는 데이터베이스 서버를 설치하고 데이터를 새 데이터베이스로 이동하십시오. 마지막으로 r12.52 SP1 로 마이그레이션합니다.
- r12.52 SP1 로 업그레이드할 때 Federation Agent for Windows Authentication 이 설치된 경우에는 에이전트를 페더레이션 시스템과 동일한 버전으로 업그레이드하십시오. 그렇지 않으면 에이전트가 제대로 작동하지 않습니다.

버전별 상세 내용은 기술 지원 사이트의 "Platform Support Matrix"(플랫폼 지원표)를 참조하십시오.

사용 가능한 다음 경로에 기반하여 r12.52 SP1 로 업그레이드하거나 마이그레이션할 수 있습니다.

Windows

기존 페더레이션 버전	데이터베이스가 r12.52 SP1 에서 작동하는지 여부	업그레이드 또는 마이그레이션
모든 SP 를 포함한 r12.0	아니요	r12.52 SP1 로 마이그레이션
모든 SP 를 포함한 r12.1	아니요	r12.52 SP1 로 마이그레이션
r12.1 SP3	예	r12.52 SP1 로 업그레이드

Solaris/Linux

기존 페더레이션 버전	데이터베이스가 r12.52 SP1 에서 작동하는지 여부	업그레이드 또는 마이그레이션
모든 SP 를 포함한 r12.0	아니요	r12.52 SP1 로 마이그레이션
모든 SP 를 포함한 r12.1	아니요	r12.52 SP1 로 마이그레이션
r12.1 SP3	예	r12.52 SP1 로 업그레이드

FIPS 마이그레이션

CA SiteMinder?Federation Standalone 은 비 FIPS 에서 FIPS 전용 환경으로의 마이그레이션을 지원하지만 마이그레이션 프로세스가 복잡합니다. 비 FIPS 에서 FIPS 전용 환경으로 마이그레이션하려면 먼저 r12.52 SP1 로의 업그레이드를 완료하십시오. 업그레이드가 성공적으로 수행되면 FIPS 마이그레이션 프로세스를 수행합니다.

r12.52 SP1 로 마이그레이션하는 방법

r12.52 SP1 이전 배포는 r12.52 SP1 가 지원하지 않는 운영 플랫폼에서 실행되거나 r12.52 SP1 가 지원하지 않는 데이터베이스를 사용할 수 있습니다. 그에 따라 r12.52 SP1 이전 환경에서 r12.52 SP1 로 마이그레이션할 수 있습니다.

CA SiteMinder?Federation Standalone 구성을 새 시스템으로 마이그레이션하면 구성이 복제됩니다. 기존 구성을 복사하면 새 시스템에서 구성 프로세스 전체를 반복하지 않아도 됩니다.

r12.52 SP1 시스템으로 마이그레이션하려면 다음 태스크를 완료하십시오.

중요! 명시되어 있는 대로 가져오기 단계를 수행해야 합니다. 복사 절차가 완료되기 전까지는 CA SiteMinder?Federation Standalone UI 의 "인증서 및 키" 탭에 액세스하지 마십시오.

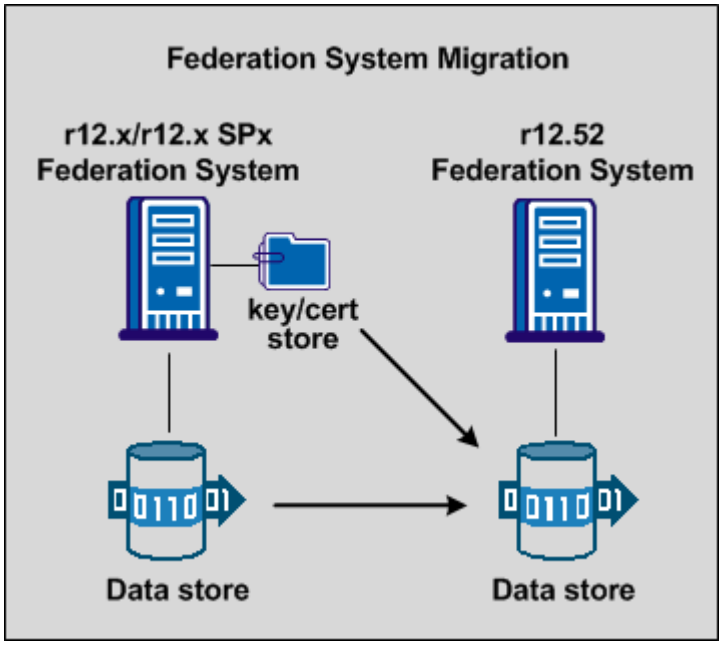
1. 여러 개의 키 데이터베이스를 동기화합니다(클러스터를 마이그레이션하는 경우). (페이지 67)
2. 기존 구성을 XML 파일로 내보냅니다 (페이지 83).
3. 새 시스템에서 설치 프로그램을 실행합니다. (페이지 84)
4. 기존 구성을 새 시스템으로 가져옵니다 (페이지 85).
5. 키 데이터베이스를 인증서 데이터 저장소로 마이그레이션합니다 (페이지 87).
6. SSL 키 및 인증서 데이터를 마이그레이션합니다 (페이지 90).

모든 데이터를 마이그레이션한 후 파트너 관계를 다시 활성화하십시오.

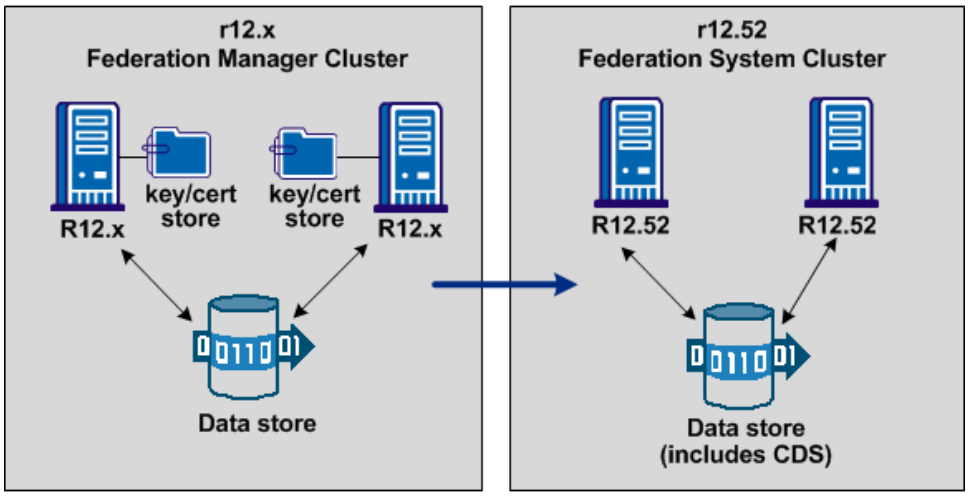
참고: XPSExport 및 XPSImport 도구는 제품과 함께 제공됩니다.

중요! 마이그레이션은 프로덕션 환경이 아니라 테스트 환경에서 수행하는 것이 좋습니다.

다음 그림에서는 단일 시스템의 마이그레이션 경로를 보여 줍니다.



다음 그림에서는 클러스터 환경에 대한 마이그레이션 경로를 보여 줍니다.



장애 조치를 지원하도록 클러스터를 설정할 수 있습니다. 비클러스터 마이그레이션과 비슷한 절차를 사용하여 기존 r12.x 클러스터에서 새 클러스터로 마이그레이션할 수 있습니다. 클러스터를 마이그레이션하려면 기존 클러스터의 각 시스템에 대해 새 r12.52 SP1 시스템을 설정합니다. 클러스터의 시스템은 하나의 데이터 저장소를 공유합니다. 모든 데이터를 새 r12.52 SP1 데이터 저장소로 마이그레이션합니다.

다음 단계를 수행하십시오.

1. 구성을 XML 파일로 내보내고 키 데이터베이스를 복사합니다. 내보낸 파일은 백업 구성으로 사용될 수 있습니다.
2. 키 데이터베이스 인스턴스를 동기화합니다.
3. 각각의 새 시스템에서 CA SiteMinder® Federation Standalone 을 설치하고 구성합니다.
4. 각각의 새 시스템을 구성합니다. 원본 시스템에 사용하던 것과 동일한 설정을 새 시스템에 사용합니다. 새 시스템에 대해 다음 설정이 일치해야 합니다.
   - **배포 모드**

     새 시스템에 동일한 배포 모드(프록시 또는 독립 실행형)를 사용합니다.
   - **SiteMinder 커넥터**

     원본 시스템에서 SiteMinder 가 사용되도록 설정된 경우 새 시스템에서도 활성화해야 합니다.
   - **포트 번호**

     구성 마법사를 실행할 때 원본 시스템이 사용하던 것과 동일한 포트를 새 시스템에 대해 지정합니다.
   - **가상 호스트 이름**

     원본 시스템이 가상 호스트를 사용한 경우 새 시스템에서도 동일한 가상 호스트 이름을 사용합니다. 또한 호스트 파일에서 새 시스템에 대한 적절한 항목을 만듭니다.
5. 내보낸 구성을 원본 시스템에서 새 시스템으로 가져옵니다.

이 프로세스는 다음 단원에서 자세히 설명합니다.

키 데이터베이스 동기화

12.5 이전 시스템에서는 개인 키 및 인증서 데이터를 smkeydatabase 라고 하는 키 저장소에 저장했습니다. 이제 이 데이터는 데이터 저장소와 함께 있는 인증서 데이터 저장소에 저장됩니다. 인증서 데이터 저장소를 사용하면 환경의 각 페더레이션 시스템이 로컬 smkeydatabase 에 액세스할 필요가 없습니다.

설치 관리자는 업그레이드 도중 로컬 smkeydatabase 를 자동으로 백업하고 모든 콘텐츠를 인증서 데이터 저장소로 마이그레이션하려고 시도합니다. 이 프로세스에서는 마이그레이션을 시작하기 전에 smkeydatabase 와 CDS 를 비교합니다. 이렇게 비교하는 목적은 마이그레이션 실패를 초래할 수 있는 데이터 불일치(예: 서로 다른 인증서에 동일한 별칭이 매핑된 경우)를 식별하는 것입니다.

클러스터 환경에는 smkeydatabase 의 인스턴스가 여러 개 있습니다. r12.52 SP1 로 업그레이드 또는 마이그레이션하기 전에 정보 일관성을 유지하기 위해 모든 smkeydatabase 인스턴스를 동기화하십시오. 데이터베이스를 동기화하면 각 인스턴스가 CDS 로 마이그레이션될 때 불일치가 발생하는 것을 방지할 수 있습니다.

Administrative UI 의 "인증서 및 키" 탭에서 smkeydatabase 인스턴스 간의 모든 데이터 불일치를 해결하십시오. 다음 데이터가 여러 키 데이터베이스 인스턴스 간에 일관성을 유지하는지 확인하십시오.

- 각 CA 인증서는 여러 인스턴스 간에 일관되게 인증서 해지 목록을 참조해야 합니다.
- **예:** CA 인증서는 LDAP 디렉터리 서비스의 인증서 해지 목록을 일관되게 참조합니다.
- defaultentpriseprivatekey 별칭이 모든 인스턴스에서 동일한 개인 키/인증서 쌍을 나타냅니다.
- 동일한 별칭이 동일한 인증서 또는 키/인증서 쌍에 매핑됩니다.
- 동일한 CA 인증서가 동일한 인증서 해지 목록에 매핑됩니다.
- 해지되거나 만료된 인증서가 없습니다.
- 모든 CRL 정보가 올바릅니다.

중요! 모든 데이터 불일치를 해결한 후에는 마이그레이션이 모두 완료되기 전까지 smkeydatabase 인스턴스를 변경하지 마십시오.

구성을 XML 파일로 내보내기

기존 시스템의 구성을 XML 파일로 내보내서 r12.5 이전 구성을 새 시스템으로 복제할 수 있습니다. 이 태스크를 완료하려면 XPSExport 도구를 사용하십시오.

CA SiteMinder?Federation Standalone 과 함께 제공되는 XPSExport 도구를 사용하면 데이터 저장소의 모든 데이터를 XML 파일로 내보낼 수 있습니다.

중요! 구성 백업이 진행 중일 때는 페더레이션 트랜잭션이 실패합니다.

구성을 내보내려면

1. 키 데이터베이스 디렉터리를 복사하여 안전한 위치에 저장합니다. 키 데이터베이스는 다음 디렉터리에 있습니다.

   federation_install_dir/siteminder/smkeydatabase

   마이그레이션 프로세스 도중 이 디렉터리를 다른 시스템으로 복사합니다.

2. 명령 창에서 다음 명령을 입력하여 구성을 내보냅니다.

   XPSExport *export_file_name* -xa -passphrase *passphrase*

   export_file_name

   내보내기를 통해 생성되는 출력 파일의 이름을 지정합니다. XPSExport 의 출력은 XML 형식이므로 파일 이름은 **.xml** 확장명으로 끝나야 합니다.

   passphrase

   중요한 데이터를 암호화하는 데 필요한 암호를 지정합니다. 이 암호는 8 자 이상이고 숫자, 대문자, 소문자를 각각 하나 이상 포함해야 합니다. 암호에 공백이 포함되어 있는 경우 암호를 따옴표로 묶어야 합니다.

   참고: 암호를 직접 입력하지 않으려면 명령에서 제외해도 됩니다. 그러면 XPSExport 도구가 화면에 표시되지 않게 암호와 암호 확인을 묻는 메시지를 표시합니다.

   이제 암호화된 구성 데이터가 포함된 XML 파일이 생성되었으며 이를 사용하여 다른 시스템에서 구성을 복제할 수 있습니다.

3. 구성을 성공적으로 백업한 후에는 설치 프로그램을 실행 (페이지 84)하십시오.

CA SiteMinder® Federation Standalone 설치 프로그램 실행

구성을 마이그레이션하기 전에 새 시스템에서 설치 프로그램을 실행합니다.

다음 단계를 수행하십시오.

1. 원본 시스템의 설치에 사용된 것과 동일한 설정을 새 설치에 사용하여 제품을 설치합니다.
2. 페더레이션 데이터 개체를 가져올 새 데이터베이스 인스턴스를 설정합니다.

   중요! 기존 데이터베이스를 사용하지 마십시오. 기존 데이터베이스를 사용하면 가져오기가 실패합니다.
3. "구성 마법사"를 실행하고 해당 메시지가 표시되면 새 데이터베이스 인스턴스를 지정합니다.

   원본 시스템에 사용한 것과 동일한 설정을 새 구성에 사용합니다. 다음과 같은 설정이 포함됩니다.

   - 배포 모드
   - 포트 번호
   - 가상 호스트 이름
   - SiteMinder 커넥터

기존 구성을 새 시스템으로 가져오기

1. XPSImport 명령을 사용하여 모든 구성 데이터를 가져옵니다. 해당 구문은 다음과 같습니다.

   XPSImport *export_file_name* -passphrase *passphrase*

   export_file_name

   원래 구성을 내보낼 때 생성된 XML 파일의 이름을 지정합니다. 파일 이름 확장명은 **.xml** 이어야 합니다.

   passphrase

   중요한 데이터를 암호 해독하는 데 필요한 암호를 지정합니다. 이 암호는 파일로 내보낼 데이터를 암호화하는 데 사용한 암호와 동일해야 합니다. XML 파일을 처음 만든 관리자로부터 암호를 받으십시오.

   암호는 8 자 이상이고 숫자, 대문자, 소문자를 각각 하나 이상 포함해야 합니다. 암호에 공백이 포함되어 있는 경우 암호를 따옴표로 묶어야 합니다.

2. 플랫폼에 따라 CA SiteMinder® Federation Standalone 서비스를 중지합니다.

   - Windows

     CA SiteMinder® Federation Standalone 중지 바로 가기를 사용합니다. 로컬 관리자가 아닌 네트워크 사용자로 로그인한 경우에는 바로 가기를 마우스 오른쪽 단추로 클릭하고 "관리자 권한으로 실행"을 선택하십시오.

     "시작", "모든 프로그램", "CA", "Federation Standalone", "서비스 중지"를 차례로 선택합니다.

   - UNIX

     a. 명령 창을 엽니다.

     b. *federation_install_dir*/fedmanager.sh stop 스크립트를 실행합니다.

   참고: 서비스를 중지했다가 루트 사용자로 시작하지 마십시오.

3. ODBC 데이터베이스(SQL 또는 Oracle)를 사용자 저장소로 사용하는 환경의 경우 데이터베이스에 대한 데이터 원본 이름을 지정해야 합니다.

   Windows:

   a. "관리 도구" 제어판에서 "데이터 원본(ODBC)"으로 이동합니다.

   b. 새 데이터 원본 항목을 추가하고 해당 항목에 대한 데이터 원본 이름을 지정합니다.

   데이터 원본을 추가하는 방법은 Windows 설명서를 참조하십시오.

   UNIX:

   데이터베이스의 DSN(데이터 원본 이름)을 포함하도록 system_odbc.ini 파일을 수정합니다. 이 DSN 은 마이그레이션하기 전 사용되고 있는 데이터베이스의 이름을 지정합니다. CA SiteMinder® Federation Standalone 시스템이 데이터베이스에 연결하고 트랜잭션을 완료하려면 이 DSN 항목이 필요합니다.

   a. *federation_install_dir*/siteminder/db 디렉터리로 이동합니다.

   b. 텍스트 편집기에서 system_odbc.ini 파일을 엽니다.

   c. DSN 를 추가합니다.

   d. 파일을 저장합니다.

   참고: 동일한 system_odbc.ini 파일에 SQL 및 Oracle 데이터 원본을 추가할 수 있습니다.

4. 원본 시스템의 CA SiteMinder® Federation Standalone 구성과 동일한 설정을 사용하여 구성 마법사를 다시 실행합니다. 다음과 같은 설정이 포함됩니다.

   - 배포 모드
   - 포트 번호
   - 가상 호스트 이름
   - SiteMinder 커넥터

   중요! Apache Tomcat http.conf 파일 또는 SPS server.conf 파일을 수동으로 변경한 경우에는 새 시스템에서도 해당 파일을 동일하게 변경하십시오.

5. 다음 태스크 중 하나를 수행하여 SSL 키 및 인증서를 마이그레이션합니다.
   - SSL 키 및 인증서를 새 시스템으로 마이그레이션합니다. SSL 마이그레이션 절차를 따릅니다. SSL 데이터를 마이그레이션하면 새로운 키나 인증서를 구입하지 않아도 됩니다.
   - 새로운 키/인증서 요청을 생성한 다음 인증서 서명을 받습니다. 가져온 구성 파일에는 SSL 인증서가 포함되어 있지 않습니다.

모든 데이터를 마이그레이션한 후 파트너 관계를 다시 활성화하십시오.

키 데이터베이스를 인증서 데이터 저장소로 마이그레이션

사용자 환경에 하나 이상의 키 데이터베이스(smkeydatabase)가 포함된 경우 내용을 r12.52 SP1 인증서 데이터 저장소로 마이그레이션하십시오.

참고: SSL 키 및 인증서를 마이그레이션하려면 SSL 마이그레이션 절차 (페이지 90)를 참조하십시오.

인증서 데이터 저장소는 키 데이터베이스를 대체합니다. 환경에 하나 이상의 smkeydatabase 를 배포한 경우에는 다음 사항을 고려하십시오.

- 인증서 데이터 저장소는 데이터 서버와 같은 곳에 배치됩니다. 인증서 데이터 저장소 하나가 있으면 각 호스트 시스템마다 개별적인 smkeydatabase 인스턴스가 있을 필요가 없습니다.
- 업그레이드의 일환으로 모든 smkeydatabase 콘텐츠가 자동으로 백업되고 인증서 데이터 저장소로 마이그레이션됩니다.
- 페더레이션 시스템은 인증서 데이터 저장소하고만 통신할 수 있습니다. smkeydatabase 는 호환성 모드에서 작동하지 않습니다.

  중요! smkeydatabase 의 마이그레이션이 실패한 경우 페더레이션 시스템을 환경으로 되돌리지 마십시오. 마이그레이션 실패 후 시스템을 되돌리면 인증서 데이터를 필요로 하는 모든 트랜잭션이 실패하게 됩니다.
- 마이그레이션을 시작하기 전에 모든 smkeydatabase 인스턴스를 동기화하십시오. 모든 인스턴스를 동기화하면 데이터 충돌을 방지할 수 있습니다. 데이터 충돌이 있으면 마이그레이션에 성공할 수 없습니다.
- 동일한 데이터베이스 서버에 대한 공통의 보기를 공유하는 모든 페더레이션 시스템은 동일한 키, 인증서 및 CRL(인증서 해지 목록)에 액세스할 수 있습니다.

- 인증서 데이터 저장소의 용도는 smkeydatabase 의 용도에서 변경되지 않고 유지됩니다. 이 저장소는 SiteMinder 환경에서 다음을 사용할 수 있게 합니다.
  - CA(인증 기관) 인증서
  - 공개 키 및 개인 키
  - 인증서 해지 목록
- CRL 이 LDAP 디렉터리 서비스에 저장된 경우 다음 사항을 고려하십시오.
  - 페더레이션 시스템은 더 이상 CRL 의 발급자가 해당 루트 인증서를 발행한 동일한 CA 일 것을 요구하지 않습니다.
  - 페더레이션 시스템은 더 이상 이 검사를 수행하지 않습니다. 이 동작은 텍스트 기반 CRL 에 대한 요구 사항과 일치합니다.

마이그레이션 유틸리티를 실행하여 데이터를 CDS 로 이동

키 데이터베이스를 CDS 로 마이그레이션할 때의 고려 사항을 검토한 후에는 마이그레이션 유틸리티인 smmigratecds 를 실행합니다.

다음 단계를 수행하십시오.

1. 모든 r12.x smkeydatabase 가 동기화 (페이지 67)되었는지 확인합니다.
2. r12.x 호스트 시스템에 로그인하고 다음 위치로 이동합니다.

   federation_install_dir\siteminder\config\properties

   federation_install_dir

   CA SiteMinder® Federation Standalone 설치 경로를 지정합니다.
3. 다음 파일을 복사합니다.

   smkeydatabase.properties
4. r12.52 SP1 호스트 시스템에 로그인하고 다음 단계를 완료하십시오.
   a. 다음 위치로 이동합니다.

      federation_install_dir\siteminder\config\properties
   b. smkeydatabase 속성 파일의 r12.52 SP1 버전의 이름을 다음 값으로 변경합니다.

      newsmkeydatabase.properties
   c. 디렉터리에 r12.x 버전의 속성 파일을 추가합니다.
   d. r12.52 SP1 및 r12.x 속성 파일을 텍스트 편집기에서 엽니다.

e. r12.x 버전의 데이터베이스 위치 경로를 r12.52 SP1 버전의 경로와 일치하도록 편집합니다.

Windows 예

```
DBLocation=C:\CA\FederationStandalone\siteminder\smkeydatab
ase
```

Solaris/Linux 예

```
DBLocation=export/fed/CA/FederationStandalone/siteminder/sm
keydatabase
```

f. r12.x 속성 파일을 저장하고 r12.52 SP1 속성 파일을 닫습니다.

g. CA SiteMinder® Federation Standalone 설치 루트에 다음 디렉터리를 생성합니다.

```
smkeydatabase
```

Windows 예:

```
C:\Program
Files\CA\FederationStandaloe\siteminder\smkeydatabase
```

Solaris/Linux 예

```
export/fed/CA/FederationStandalone/siteminder/smkeydatabase
```

5. r12.x 호스트 시스템으로 돌아가서 smkeydatabase 디렉터리의 내용을 복사합니다.

6. r12.52 SP1 호스트 시스템으로 돌아가서 다음 단계를 완료하십시오.

a. r12.x smkeydatabase 디렉터리의 내용을 앞에서 생성한 r12.52 SP1 smkeydatabase 디렉터리에 추가합니다.

b. 다음 명령을 입력하여 smkeydatabase 를 인증서 데이터 저장소로 마이그레이션합니다.

```
smmigratecds
```

c. 마이그레이션에 성공하면 smkeydatabase 속성 파일과 smkeydatabase 디렉터리를 제거합니다.

마이그레이션이 완료되었습니다.

키 데이터베이스 마이그레이션이 실패하면 수동으로 CDS 로 마이그레이션할 수 있습니다.

추가 정보:

키 데이터베이스 마이그레이션 문제 해결 (페이지 123)

SSL 키 및 인증서 마이그레이션(선택 사항)

CA SiteMinder?Federation Standalone r12.52 SP1 의 경우 포함된 Apache 및 Tomcat 서버에 대한 SSL 키와 인증서 파일이 암호화됩니다. 12.0 및 12.0 SP1 릴리스에서는 이러한 파일이 암호화되지 않습니다. 암호화된 파일에 대한 키/인증서 쌍을 새로 구매하는 것을 방지하려면 기존 키 또는 인증서 파일을 CA SiteMinder?Federation Standalone r12.0/r12.0 SP1 에서 r12.52 SP1 로 마이그레이션하십시오. 이러한 파일을 마이그레이션하지 않고 백업 용도로 내보낼 수도 있습니다.

중요! r12.1 이전 시스템에서는 포함된 Tomcat 서버가 자체 서명된 인증서를 사용합니다. r12.52 SP1 로의 마이그레이션에는 이 자체 서명된 인증서를 사용할 수 없습니다. 서명된 인증서를 구매하고 Tomcat SSL 구성을 서명된 인증서로 업그레이드하십시오.

Apache 의 경우 r12.0 부터 SSL 연결을 위한 파일을 마이그레이션할 수 있습니다. Tomcat 의 경우 r12.0 에서는 자체 서명된 인증서로 Tomcat 키 저장소를 보호하기 때문에 r12.1 이상의 파일만 마이그레이션할 수 있습니다. r12.1 부터 페더레이션 제품은 인증 기관이 인증서를 서명해야 합니다.

SSL 키 및 인증서 파일은 다음과 같은 경우에 유용합니다.

- 기존 시스템을 업그레이드하는 대신 새 시스템에 있는 다른 버전의 CA SiteMinder® Federation Standalone 으로 이동하는 경우. SSL 키 또는 인증서를 기존 시스템에서 새 시스템으로 마이그레이션합니다.
- SSL 키와 인증서를 클러스터의 한 시스템에서 다른 시스템으로 마이그레이션하는 경우. 마이그레이션을 수행하면 키와 인증서를 재사용할 수 있습니다. 예를 들어 부하 분산 장치가 SSL 요청을 클러스터의 페더레이션 시스템으로 전달하는 경우 각 시스템이 동일한 키와 인증서를 사용해야 합니다. 따라서 키와 인증서를 한 시스템에서 다른 시스템으로 마이그레이션합니다.

참고: 12.0 시스템을 r12.52 SP1 로 업그레이드하면 설치 관리자는 자동으로 Apache 및 Tomcat SSL 키와 인증서 파일을 암호화된 파일로 업그레이드합니다. 마이그레이션에는 이 자동화가 적용되지 않습니다.

인증서 및 개인 키 파일은 다음과 같습니다.

Apache

- server.key 파일에 개인 키가 포함되어 있습니다.
- server.cert 파일에 서버 인증서가 포함되어 있습니다.

Tomcat

- r12.0 의 경우 tomcat.keystore 파일에 자체 서명된 인증서가 포함되어 있습니다. r12.x 의 경우 tomcat.keystore 파일에 CA 서명된 인증서 및 개인 키 쌍이 포함되어 있습니다.

이러한 파일을 마이그레이션하거나 내보내려면 migratessl 이라는 SSL 유틸리티를 사용하십시오. 마이그레이션 유틸리티는 Windows 시스템의 경우 배치 파일로, UNIX 시스템의 경우 셸 스크립트의 형태로 CA SiteMinder?Federation Standalone r12.52 SP1 에 포함되어 있습니다. 이 도구는 *federation_install_dir*/bin 폴더에 있습니다.

SSL 파일을 마이그레이션하는 프로세스는 다음과 같습니다.

1. 키 및 인증서 파일을 기존 페더레이션 시스템에서 r12.52 SP1 시스템의 원하는 위치로 복사합니다.
2. 키와 인증서 파일을 복사한 위치로 migratessl 도구를 복사합니다.
3. 서명된 인증서를 마이그레이션하는 경우 SSL 인증서에 서명한 인증 기관 인증서를 내보냅니다. 마이그레이션을 계속하기 전에 먼저 CA 인증서를 가져옵니다.

참고: 이 마이그레이션 프로세스를 건너뛰고, 새 키/인증서 요청을 생성한 다음 인증서 서명을 받을 수도 있습니다. 가져온 구성 파일에는 SSL 인증서가 포함되어 있지 않습니다.

r12 시스템에서 키 및 인증서 파일 복사

SSL 마이그레이션 도구를 사용하려면 먼저 마이그레이션하거나 내보낼 원본 CA SiteMinder?Federation Standalone 시스템의 키 및 인증서 파일을 수집한 후 복사하십시오.

SSL 키 및 인증서 파일을 복사하려면

1. 기존 CA SiteMinder® Federation Standalone 시스템에서 파일을 찾습니다.

   Apache SSL 키 및 인증서 파일은 다음 위치에 있습니다.

   - *federation_install_dir*/secure-proxy/SSL/keys/server.key
   - *federation_install_dir*/secure-proxy/SSL/certs/server.crt

   Tomcat SSL 키 저장소 파일의 위치는 다음과 같습니다.

   - *federation_install_dir*/secure-proxy/SSL/keys/tomcat.keystore
2. 키 및 인증서 파일을 새 CA SiteMinder® Federation Standalone 컴퓨터의 원하는 위치로 복사합니다.

SSL 마이그레이션 도구를 키/인증서 파일과 동일한 폴더에 복사

SSL 마이그레이션 도구에는 CA SiteMinder?Federation Standalone 12.1 SP3 과 함께 배포되는 소프트웨어가 필요합니다. CA SiteMinder?Federation Standalone 12.1 SP3 제품이 설치된 컴퓨터에서 도구를 실행하십시오. 도구는 마이그레이션될 파일을 복사한 폴더와 동일한 폴더에 있어야 합니다.

SSL 유틸리티 도구를 복사하려면

1. r12.52 SP1 시스템에서 *federation_install_dir*/bin 으로 이동합니다.
2. migratessl 파일(.bat 또는 .sh)을 키 및 인증서 파일을 복사한 r12.52 SP1 시스템의 위치로 복사합니다.

SSL 키 및 인증서 마이그레이션 또는 내보내기

migratessl 유틸리티를 실행하여 SSL 키 또는 인증서 파일 마이그레이션을 완료하십시오.

다음 단계를 수행하십시오.

1. 마이그레이션하려는 SSL 인증서에 원래 서명한 인증 기관 인증서를 가져옵니다.
   a. 마이그레이션하는 원본 시스템에서 CA SiteMinder® Federation Standalone UI 를 사용하여 CA 인증서를 내보냅니다.
   b. 마이그레이션하는 새 대상 시스템에서 CA SiteMinder® Federation Standalone UI 를 사용하여 CA 인증서를 가져옵니다.
2. 기존 키 또는 인증서 파일을 복사한 새 시스템에서 명령 창을 엽니다.
3. 구성 요소를 복사한 폴더로 이동합니다.
4. migratessl 명령을 필요한 명령 인수와 함께 지정합니다. 모든 옵션을 보려면 마이그레이션 도구 명령 인수 (페이지 94) 목록을 참조하십시오.

   예

   - Apache SSL 연결에 사용할 SSL server.key 를 마이그레이션하려면 다음을 입력하십시오.

   ```
   migratessl.bat -op migrate -keytype Apache
   -sourcefile server.key -certfile server.crt
   -sourcever 12.0 -sourceos Windows -oldpwd admin1
   -newpwd admin2 -issueralias trustedca
   ```

   - Tomcat SSL 연결에 사용되는 키/인증서 파일을 마이그레이션하려면 다음을 입력하십시오.

   ```
   migratessl.sh -op migrate -keytype Tomcat
   -sourcefile tomcat.keystore -sourcever 12.1
   -sourceos UNIX -issueralias trustedca
   -oldpwd admin1 -newpwd admin2
   ```

   - Tomcat SSL 연결에 사용되는 키/인증서 파일을 내보내려면 다음을 입력하십시오.

   ```
   migratessl.sh -op export -keytype Tomcat
   -sourcefile tomcat.keystore -sourcever 12.1
   -sourceos UNIX  -dest ca/federationmgr/secure-proxy/
   SSL/keys/ -oldpwd admin1 -newpwd admin2
   ```

전체 구성 마이그레이션의 일부로 SSL 키와 인증서를 마이그레이션하는 경우에는 파트너 관계를 다시 활성화하여 마이그레이션 프로세스를 완료하십시오.

SSL 마이그레이션 도구 명령 인수

명령줄에서 migratessl 도구가 호출됩니다. 명령을 입력할 때 다음 사항에 유의하십시오.

- 각 명령 인수에 값을 하나씩만 입력합니다(Help 플래그 제외).
- 디렉터리 경로처럼 공백이 있는 값은 큰따옴표로 묶습니다.

명령 인수	의미
-op	마이그레이션 또는 내보내기 기본값: Migrate -certfile 인수를 지정한 경우 도구는 Apache 용으로 내보낼 때 server.key 파일 및 server.crt 파일을 내보냅니다. Tomcat 의 경우 도구는 PKCS#12 키/인증서 파일인 tomcat.p12 파일을 내보냅니다.
-keytype	Apache 또는 Tomcat 기본값: Apache
-sourcefile	SSL 키가 포함된 파일(Apache) 또는 키와 인증서가 포함된 키 저장소(Tomcat)의 이름입니다.
-certfile	Apache SSL 서버 인증서가 포함된 파일의 이름입니다(Apache 에만 해당).
-sourcever	키 또는 인증서를 가져온 원본 CA SiteMinder® Federation Standalone 버전입니다(예: 12.0, 12.1). 기본값: 12.0
-sourceos	키를 가져온 원본 환경의 운영 체제입니다(예: Windows 또는 UNIX). **참고:** Linux 는 r12.1 SP3 부터 지원되었기 때문에 Linux 옵션은 없습니다. 기본값: 도구를 실행 중인 컴퓨터의 OS 입니다.
-dest	출력 파일에 대한 폴더의 경로입니다. 마이그레이션에서 이 옵션은 무시됩니다. 내보내기 기본값: 현재 폴더 **중요!** 대상 폴더를 지정하지 않으면 마이그레이션할 파일을 덮어쓰게 됩니다.

-issueralias	마이그레이션 중인 인증서에 서명한 CA 인증서의 별칭입니다. CA 인증서를 이 별칭을 사용하여 대상 CA SiteMinder® Federation Standalone 시스템으로 가져옵니다. 마이그레이션에만 사용되며 내보내기의 경우에는 무시됩니다.
-oldpwd	키가 있는 원본 시스템의 CA SiteMinder® Federation Standalone 관리 암호입니다.
-newpwd	키를 이동할 대상 시스템의 CA SiteMinder® Federation Standalone 관리 암호입니다.
-h	사용 지침을 표시합니다.
-help	사용 지침을 표시합니다.
-?	사용 지침을 표시합니다.

SSL 과 SiteMinder 커넥터 재구성(선택 사항)

이전 구성이 SSL 또는 SiteMinder 커넥터를 사용한 경우 마이그레이션을 완료한 후 다음 단계를 완료하십시오.

1. Administrative UI 에 로그인합니다.

   중요! 전체 절차가 완료되기 전까지는 Administrative UI 의 "인증서 및 키" 탭에 액세스하지 마십시오.

2. (선택 사항) 원래 시스템에서 커넥터가 활성화되어 있었으면 다음 단계를 따라 새 시스템에서 커넥터를 구성 및 활성화할 수 있습니다.

   a. "인프라" 탭을 클릭하고 "배포 설정"을 선택합니다.

   b. 원래 구성과 동일한 값을 사용하여 커넥터 설정을 다시 구성합니다.

   c. "호스트 등록"을 클릭하여 정책 서버에 페더레이션 시스템을 등록합니다.

   참고: 새 시스템에서 커넥터를 구성 및 활성화하는 경우 모든 파트너 관계가 기본적으로 커넥터를 사용하게 됩니다. 개별 파트너 관계에 대해 커넥터를 사용하지 않도록 설정하려면 특정 파트너 관계를 편집하십시오.

3. (선택 사항) SSL 이 원래 시스템에서 아티팩트 백 채널 또는 Administrative UI 에 대해 활성화되어 있었으면 새 시스템에서 SSL 을 재구성합니다. 페더레이션 트랜잭션을 처리하기 전에 SSL 을 활성화합니다.

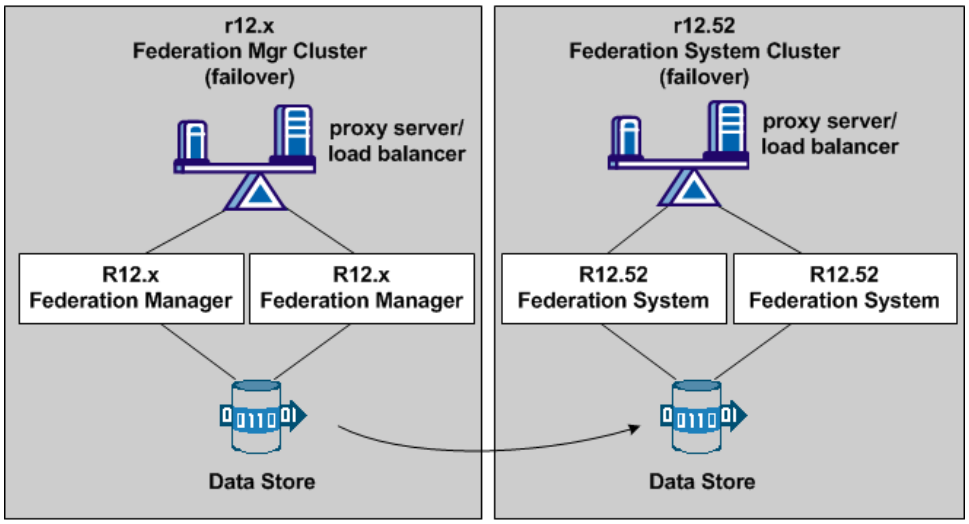
   포함된 웹 서버의 경우 기존 SSL 키 및 인증서를 마이그레이션하거나 새 키/인증서 요청을 생성하십시오. 마지막으로 인증서에 서명을 받습니다. 가져온 구성 파일에는 SSL 인증서가 포함되어 있지 않습니다.

이제 새 시스템은 원본 시스템과 동일한 구성으로 작동합니다.

장애 조치 배포를 마이그레이션하는 방법

기존 r12x 장애 조치 배포를 r12.52 SP1 장애 조치 배포로 마이그레이션할 수 있습니다.

다음 그림에서는 장애 조치를 지원하기 위한 클러스터 환경을 보여 줍니다.



장애 조치 배포를 r12.52 SP1 로 마이그레이션하려면 다음 단계를 수행해야 합니다.

1. 기존 구성을 새 r12.52 SP1 시스템으로 복사합니다.
2. 적절한 URL 을 새 r12.52 SP1 시스템으로 전달하도록 프록시 서버 또는 부하 분산 장치를 업데이트합니다.

r12 장애 조치 배포를 r12.52 SP1 로 마이그레이션

기존 r12.x 장애 조치 배포를 r12.52 SP1 CA SiteMinder?Federation Standalone 배포로 마이그레이션할 수 있습니다.

장애 조치 구성을 마이그레이션하려면

1. 배포 환경의 각 컴퓨터에 r12.52 SP1 를 설치합니다.
2. 처음 업그레이드된 컴퓨터에서 구성 마법사를 실행하고 이전 구성에 사용한 것과 동일한 정보를 입력합니다.

   기존 구성 설정을 확인하려면 r12.x 시스템에서 *federation_install_dir*\install_config_info\ca-Federation-Config.properties 파일로 이동합니다.
3. 두 번째 컴퓨터에서 r12.52 SP1 구성 마법사를 실행합니다. 다음 정보를 입력합니다.
   a. 첫 번째 컴퓨터의 데이터베이스 정보
   b. ca-Federation-Config.properties 파일의 다른 모든 항목
4. CA SiteMinder® Federation Standalone UI 에 로그인합니다.
5. "인프라" 탭에서 "시스템 설정"을 선택합니다.

   "시스템 설정 구성" 대화 상자가 나타납니다.
6. UI 에서 페더레이션된 네트워크에 있는 프록시 서버 또는 부하 분산 장치의 호스트와 포트를 포함하도록 "전역 기준 URL"을 변경합니다. 이 URL 을 제대로 설정해야 파트너 관계를 만드는 데 사용되는 모든 메타데이터의 기본 URL 이 올바르게 적용됩니다.
7. 페더레이션된 네트워크에 있는 프록시 서버 또는 부하 분산 장치의 호스트와 포트를 포함하도록 프록시 엔진의 기본 URL 을 변경합니다. 이 URL 을 제대로 설정해야 파트너 관계를 만드는 데 사용되는 모든 메타데이터의 기본 URL 이 올바르게 적용됩니다.

   기본 URL 은 server.conf 파일에서 정의됩니다.

   server.conf 파일을 수정하려면

   a. *federation_mgr_home*/secure-proxy/proxy-engine/conf 로 이동합니다.
   b. 편집기에서 server.conf 파일을 엽니다.

c. # Default Virtual Host 섹션으로 이동합니다.

d. 다음과 같이 정규화된 호스트 이름을 사용하여 **hostnames** 설정에 기본 URL 을 추가합니다.

```
<VirtualHost name="default">
hostnames="defaultbaseurl.ca.com:80, newbaseurl.ca.com:80"
</VirtualHost>
```

참고: hostnames 설정에 *host_name:port* 항목을 여러 개 지정하려면 각 항목을 쉼표로 구분하십시오.

8. r12x 시스템에서 장애 조치에 대해 SSL 을 사용하도록 설정한 경우 SSL 마이그레이션 단계 (페이지 90)의 지침에 따라 SSL 구성을 r12.52 SP1 기본 시스템 및 보조 시스템으로 마이그레이션해야 합니다.

그러면 두 CA SiteMinder?Federation Standalone 시스템 모두 동일한 데이터베이스 서버를 가리키며 프록시 서버 또는 부하 분산 장치에서 장애 조치되도록 구성될 수 있습니다.

프록시 서버 또는 부하 분산 장치에서 장애 조치 설정

이 안내서에서는 프록시 서버 또는 부하 분산 장치의 관리자가 해당 시스템에 대해 장애 조치를 설정하는 방법을 알고 있다고 가정합니다.

프록시 서버/부하 분산 장치 컴퓨터에서

1. 프록시 서버 구성에 대해 하나의 페더레이션 시스템을 기본 호스트로 식별하고 다른 시스템을 보조 호스트로 식별합니다.

   컴퓨터에 대해서는 부하 분산을 구성하지 마십시오.

2. 서버가 다음 URL 을 페더레이션 컴퓨터로 전달하도록 구성합니다.
   - /affwebservices/*
   - /siteminderagent/*

배포 모드(독립 실행형 또는 프록시)에 따라 페더레이션 시스템을 통해 다른 트래픽이 라우트될 수 있습니다.

이제 프록시 서버 또는 부하 분산 장치는 페더레이션 시스템으로 장애 조치될 수 있습니다.

제 5 장: FIPS 암호화를 사용하기 위해 페더레이션 시스템 마이그레이션

FIPS_Only 모드로 마이그레이션하기 전에 다음과 같은 문제에 유의하십시오.

- SiteMinder 커넥터를 활성화한 상태에서 페더레이션 제품을 FIPS_ONLY 모드로 배포하는 경우에는 백엔드 SiteMinder 시스템은 버전이 r12x 이고 FIPS_ONLY 모드에서 작동해야 합니다.

  SiteMinder 시스템이 r6.0 SP5 인 경우 이 시스템은 FIPS 호환 작업을 지원하지 않으므로 페더레이션 시스템이 FIPS_ONLY 모드에서 작동할 수 없습니다.

- r12.1 이전 릴리스의 CA SiteMinder® Federation Standalone 은 개인 키 생성에 대해 FIPS 승인 암호화 알고리즘을 지원하지 않습니다. 이러한 릴리스는 개인 키 생성을 위한 서명 알고리즘으로 MD5 만 지원하며 이는 승인된 FIPS 알고리즘이 아닙니다.

  서명 알고리즘으로 MD5 만 사용하는 개인 키가 있는 경우에는 파트너 관계의 양측 모두에서 다음 작업을 수행하십시오.

  - 새 개인 키 생성
  - 새 인증서 가져오기
  - 필요한 모든 파트너 관계를 새 공개 키로 업데이트합니다.

이 섹션은 다음 항목을 포함하고 있습니다.

고려해야 할 FIPS 마이그레이션 문제 (페이지 100)
FIPS_COMPAT 모드에서 FIPS_Only 모드로 마이그레이션하는 방법 (페이지 100)

고려해야 할 FIPS 마이그레이션 문제

FIPS_Only 모드로 마이그레이션하기 전에 다음과 같은 문제에 유의하십시오.

- SiteMinder 커넥터를 활성화한 상태에서 페더레이션 제품을 FIPS_ONLY 모드로 배포하는 경우에는 백엔드 SiteMinder 시스템은 버전이 r12x 이고 FIPS_ONLY 모드에서 작동해야 합니다.

  SiteMinder 시스템이 r6.0 SP5 인 경우 이 시스템은 FIPS 호환 작업을 지원하지 않으므로 CA SiteMinder® Federation Standalone 이 FIPS_ONLY 모드에서 작동할 수 없습니다.

- r12.1 이전 릴리스의 CA SiteMinder® Federation Standalone 은 개인 키 생성에 대해 FIPS 승인 암호화 알고리즘을 지원하지 않습니다. 이러한 릴리스는 개인 키 생성을 위한 서명 알고리즘으로 MD5 만 지원하며 이는 승인된 FIPS 알고리즘이 아닙니다.

  서명 알고리즘으로 MD5 만 사용하는 개인 키가 있는 경우에는 파트너 관계의 양측 모두에서 다음 작업을 수행하십시오.

  - 새 개인 키 생성
  - 새 인증서 가져오기
  - 필요한 모든 파트너 관계를 새 공개 키로 업데이트합니다.

FIPS_COMPAT 모드에서 FIPS_Only 모드로 마이그레이션하는 방법

FIPS 가 제공하는 강력한 암호화 알고리즘을 사용하여 중요한 데이터에 보안을 적용하면 보안 위반으로부터 데이터를 보호하고 페더레이션 시스템의 전반적인 보안을 강화하는 데 도움이 됩니다.

중요한 데이터를 보호하기 위해 FIPS 호환 암호화 알고리즘만 사용하여 작동하도록 페더레이션 시스템을 마이그레이션할 수 있습니다.

CA SiteMinder?Federation Standalone 은 다음의 FIPS 작동 모드 중 하나로 설치할 수 있습니다.

FIPS_COMPAT

FIPS_COMPAT(호환성) 모드는 설치 중에 사용되는 기본 FIPS 모드입니다. FIPS_COMPAT 모드에서 페더레이션 시스템은 현재의 비 FIPS 알고리즘뿐 아니라 지원되는 FIPS 호환 알고리즘도 함께 지원합니다.

FIPS_COMPAT 모드는 페더레이션의 이전 버전과도 호환됩니다. 이와 같은 호환성 기능 때문에 r12.52 SP1 이전 버전을 사용하는 환경도 r12.52 SP1 와 상호 작용할 수 있습니다. IPS_COMPAT 모드는 현재 구현되어 있는 페더레이션의 보안 수준에 만족하는 클라이언트에게도 적합합니다.

조직에서 FIPS 를 사용할 필요가 없는 경우에는 CA SiteMinder® Federation Standalone 을 FIPS_COMPAT 모드에서 설치하십시오. 추가 구성이 필요하지 않습니다.

FIPS_ONLY

FIPS_ONLY 모드의 환경에서는 FIPS 호환 알고리즘만 사용하여 중요한 데이터가 암호화됩니다.

새 설치에서 FIPS 호환 알고리즘만 사용하려는 경우에는 CA SiteMinder® Federation Standalone 을 FIPS_ONLY 모드로 설치하십시오.

제품은 FIPS_COMPAT 모드에서의 단방향 마이그레이션 경로만 허용하며 이는 MIGRATE 모드를 통해 FIPS_ONLY 모드로 전환하는 기본 모드입니다. FIPS_MIGRATE 모드에서는 FIPS_COMPAT 모드에서 실행 중인 페더레이션 환경을 FIPS_Only 모드로 전환할 수 있습니다. MIGRATE 모드에서는 환경을 FIPS_Only 모드로 마이그레이션할 때 페더레이션 시스템이 기존 데이터에 대해 기존 암호화 알고리즘을 계속 사용합니다. 하지만 암호화가 필요한 새 데이터는 모두 FIPS 호환 알고리즘만 사용하여 암호화됩니다.

중요! FIPS_ONLY 모드에서 작동 중인 환경은 이전 버전의 페더레이션과 상호 운용될 수 없으며 호환되지도 않습니다. 여기에는 이전 버전의 페더레이션 API 를 사용하는 사용자 지정 소프트웨어가 포함됩니다. 사용자 지정 소프트웨어가 r12.52 SP1 이전 SDK 로 빌드된 경우에는 r12.52 SP1 SDK 를 사용하여 이 소프트웨어를 다시 컴파일해야 FIPS_ONLY 모드가 지원됩니다.

페더레이션 시스템을 FIPS_ONLY 모드로 마이그레이션하려면:

1. 기존 구성을 백업합니다.
2. OPENSSL_FIPS 환경 변수를 설정합니다.
3. 정책 엔진을 FIPS_MIGRATE 모드로 설정합니다.
4. 정책 저장소 키를 다시 암호화합니다.
5. 정책 저장소 관리자 암호를 다시 암호화합니다.
6. SiteMinder 슈퍼 사용자 암호를 다시 암호화합니다.
7. 클라이언트 공유 암호를 다시 암호화합니다.
8. 정책 및 키 저장소 데이터를 다시 암호화합니다.
9. Administrative UI 를 FIPS_ONLY 모드로 설정합니다.
10. 포함된 보안 프록시 엔진을 FIPS_ONLY 모드로 설정합니다.
11. 포함된 정책 엔진을 FIPS_ONLY 모드로 설정합니다.

중요! FIPS_ONLY 모드로 마이그레이션한 후에는 비 FIPS 승인 인증서로 구성된 파트너 관계는 작동이 중지되며 이에 따라 파트너 관계의 작동이 중지됩니다. FIPS_ONLY 작업으로 마이그레이션하기 전에 FIPS 호환 알고리즘을 사용하여 파트너 관계 데이터를 다시 암호화하십시오.

다음 단원에서는 각 절차에 대해 자세히 설명합니다.

SSL 구성 비활성화

FIPS 전용 모드로 마이그레이션하기 위한 첫 번째 단계는 포함된 웹 서버 또는 관리 UI 섹션에 대해 SSL 을 비활성화하는 것입니다. 먼저 SSL 을 활성화하지 않은 경우에는 이 단계를 건너뛰십시오.

SSL 을 비활성화하려면

1. "SSL 구성" 대화 상자에서 시작합니다.
2. 활성 서비스를 모두 비활성화합니다. 이렇게 하려면 "포함된 웹 서버" 및/또는 "관리 UI" 섹션에서 "비활성화"를 클릭하십시오.

   SSL 을 비활성화할지 묻는 확인 메시지가 표시됩니다.
3. "예"를 클릭하여 비활성화를 완료합니다.

4. 운영 환경에 맞게 페더레이션 서비스를 다시 시작합니다.

   - **Windows**

     다음과 같이 중지 및 시작 바로 가기를 사용합니다. 로컬 관리자가 아닌 네트워크 사용자로 로그인한 경우에는 바로 가기를 마우스 오른쪽 단추로 클릭하고 "관리자 권한으로 실행"을 선택하십시오.

     a. "시작", "모든 프로그램", "CA", "Federation Standalone", "서비스 중지"

     b. "시작", "모든 프로그램", "CA", "Federation Standalone", "서비스 시작"

   - **UNIX**

     a. 명령 창을 엽니다.

     b. 다음 스크립트를 실행합니다.

     federation_install_dir/fedmanager.sh stop

     federation_install_dir/fedmanager.sh start

   참고: 서비스를 중지했다가 루트 사용자로 시작하지 마십시오.

이제 SSL 연결은 더 이상 활성 상태가 아니며 "SSL 구성 상태" 설정이 **서버 인증서가 CA 서명됨, SSL 준비됨**으로 바뀝니다. 인증서와 키 파일은 SSL 을 다시 사용할 수 있도록 보관됩니다.

기존 구성 백업

시스템 복구, 업그레이드 또는 마이그레이션의 일부로 기존 구성을 복원할 수 있습니다.

구성을 복원하려면 키 데이터베이스를 복사하고 구성 데이터를 내보냅니다. 제품에 포함되어 있는 XPSExport 도구를 사용하면 구성 데이터를 XML 파일로 내보낼 수 있습니다.

중요! 구성을 복원 중일 때는 페더레이션 트랜잭션이 실패합니다.

구성을 내보내려면

1. 키 데이터베이스를 복사하여 안전한 위치에 저장합니다. 키 데이터베이스는 다음 디렉터리에 있습니다.

   federation_mgr_home/siteminder/smkeydatabase

2. 명령 창에서 다음 명령을 입력하여 구성을 내보냅니다.

   XPSExport *export_file_name* -xa -passphrase *passphrase*

   export_file_name

   내보내기를 통해 생성되는 출력 파일의 이름을 지정합니다. XPSExport 의 출력은 XML 형식이므로 파일 이름 확장명은 **.xml** 이어야 합니다.

   passphrase

   중요한 데이터를 암호화하는 데 필요한 암호를 지정합니다. 암호는 8 자 이상이고 숫자, 대문자, 소문자를 각각 하나 이상 포함해야 합니다. 암호에 공백이 포함되어 있는 경우 암호를 따옴표로 묶어야 합니다.

   참고: 암호를 직접 입력하지 않으려면 명령에서 제외해도 됩니다. 그러면 XPSExport 도구가 화면에 표시되지 않게 암호와 암호 확인을 묻는 메시지를 표시합니다.

이제 암호화된 구성 데이터가 포함된 XML 파일이 생성되었습니다. 이 XML 파일을 사용하여 구성을 복원할 수 있습니다.

OPENSSL_FIPS 환경 변수 설정

OPENSSL_FIPS 환경 변수를 설정하여 FIPS 모드를 사용하도록 설정할 수 있습니다. 이 변수는 압축 모드에서 FIPS 전용 모드로 마이그레이션할 경우에만 한 번 설정하십시오.

다음 단계를 수행하십시오.

Windows

1. Windows 시스템 속성에 액세스합니다.
2. 환경 변수에 액세스합니다.
3. 다음과 같이 환경 변수를 추가합니다.

   변수 이름

   OPENSSL_FIPS

   변수 값

   1
4. 새 변수를 저장합니다.

UNIX

1. *federation_install_dir* 로 이동합니다.
2. 환경 스크립트 ca_federation_env.ksh 를 편집합니다.
3. 스크립트에 다음 항목을 추가합니다.

   ```
   OPENSSL_FIPS=1;export OPENSSL_FIPS=1
   ```

4. 환경 스크립트 ca_federation_env.ksh 를 실행하여 환경 변수를 설정합니다.
5. UNIX 시스템의 경우에만 *federation_install_dir*/bin/migratessltofips.sh 스크립트를 실행합니다.

   이 스크립트는 SSL 인증서와 연결된 개인 키가 적절하게 암호화되도록 합니다.

정책 엔진을 FIPS_MIGRATE 모드로 설정

FIPS_Only 모드로 마이그레이션하는 첫 번째 단계는 FIPS_MIGRATE 모드에서 정책 엔진을 구성하는 것입니다.

다음 단계를 수행하십시오.

1. CA SiteMinder® Federation Standalone 이 COMPAT 모드에 있는지 확인합니다. 이 모드에 있지 않은 경우에는 다시 설치한 후 COMPAT 모드에서 실행되도록 구성합니다.
2. 명령 프롬프트에서 다음과 같이 setFIPSmigration 명령을 실행합니다.

   Windows

   setFIPSmigration 을 입력합니다.

   UNIX

   a. *federation_install_dir*/siteminder/bin *으로 이동합니다.*
   b. setFIPSmigration.ksh 를 입력합니다.
   c. 환경 스크립트 ca_federation_env.ksh 를 실행하여 환경 변수를 설정합니다.

   마이그레이션 프로세스가 시작됩니다.

3. 다음 작업 중 하나를 수행하십시오.

   Windows

   CA SiteMinder® Federation Standalone 시스템을 재부팅합니다.

   UNIX

   명령 창에서 다음 스크립트를 실행하여 CA SiteMinder® Federation Standalone 서비스를 다시 시작합니다.

   a. *federation_install_dir*/fedmanager.sh stop

   b. *federation_install_dir*/fedmanager.sh start

   참고: 서비스를 중지했다가 루트 사용자로 시작하지 마십시오. 루트가 아닌 사용자여야 합니다.

4. smps.log 파일에서 정책 엔진이 이제 MIGRATE 모드에 있는지 확인합니다.

   로그 파일의 위치는 *federation_install_dir*/logs/server/smps.log 입니다.

이제 정책 엔진이 FIPS_MIGRATE 모드에서 작동합니다.

정책 저장소 암호화 키 다시 암호화

마이그레이션 프로세스의 다음 단계는 정책 저장소 암호화 키를 다시 암호화하는 것입니다.

정책 저장소 키를 다시 암호화하려면

1. CA SiteMinder® Federation Standalone 웹 키트를 아직 다운로드하지 않은 경우에는 기술 지원 사이트로 이동하여 운영 환경에 맞는 키트를 다운로드합니다.
2. smreg 를 *federation_install_dir*/siteminder/bin 으로 복사합니다.
3. 명령 프롬프트 창을 엽니다.

4. 명령 프롬프트에 다음 명령을 입력합니다.

   smreg -cf MIGRATE -key *admin_password*

   admin_password

   설치할 때 제공한 CA SiteMinder® Federation Standalone 관리자 암호를 지정합니다.

5. *federation_install_dir*\siteminder\bin 디렉터리의 EncryptionKey.txt 파일을 엽니다.

   여기에 새 암호화 키가 있으며 AES 와 같은 FIPS 호환 알고리즘의 접두사가 붙어 있습니다.

다시 암호화가 완료되었습니다.

데이터베이스 관리자 암호 다시 암호화

마이그레이션 프로세스에서는 데이터베이스 관리자 암호를 다시 암호화해야 합니다.

암호를 다시 암호화하려면

1. 명령 프롬프트에서 다음과 같이 fedconfig 유틸리티를 실행합니다.

   Windows

   federation_install_dir/bin 으로 이동하고 fedconfig.bat 을 입력합니다.

   UNIX

   a. *federation_install_dir* 로 이동합니다.

   b. 환경 스크립트 ca_federation_env.ksh 를 실행하여 환경 변수를 설정합니다.

   c. /bin 디렉터리로 이동합니다.

   d. fedconfig.sh 를 입력합니다.

   fedconfig 유틸리티가 유틸리티 옵션 목록을 표시합니다.

2. 5 를 입력하여 데이터베이스 관리자 암호를 변경합니다.

3. C 를 입력하고 CA SiteMinder® Federation Standalone 구성 마법사를 실행할 때 입력한 암호를 입력합니다.

4. 암호 항목을 확인합니다.
5. 0 을 입력하여 암호를 저장하고 종료합니다.

암호를 변경했습니다.

슈퍼 사용자 암호 다시 암호화

FIPS_Only 모드로 마이그레이션하려면 CA SiteMinder?Federation Standalone 슈퍼 사용자 암호를 다시 암호화하십시오.

슈퍼 사용자 암호를 다시 암호화하려면

1. CA SiteMinder® Federation Standalone 웹 키트를 아직 다운로드하지 않은 경우에는 기술 지원 사이트로 이동하여 운영 환경에 맞는 키트를 다운로드합니다.
2. smreg 를 *federation_install_dir*/siteminder/bin 으로 복사합니다.
3. 다음 명령을 입력합니다.

   smreg -cf MIGRATE -su *admin_password*

   admin_password

   설치할 때 제공한 CA SiteMinder® Federation Standalone 관리자 암호를 지정합니다.
4. siteminder\bin 에서 smreg 를 삭제합니다.

   참고: smreg 를 삭제하면 이전 암호를 모르는 다른 사람은 암호를 변경할 수 없게 됩니다.

슈퍼 사용자 암호가 설정되었습니다.

프록시 엔진 에이전트 공유 암호 다시 암호화

마이그레이션하려면 프록시 엔진 웹 에이전트에 대한 공유 암호를 다시 암호화하십시오.

공유 암호를 다시 암호화하려면

1. 명령 프롬프트 창을 엽니다.
2. *federation-mgr_home*\secure-proxy\proxy-engine\conf\defaultagent\SmHost.conf 에 있는 SmHost.conf 파일로 이동합니다.

3. 일부 설정의 경우 SmHost.conf 파일에 있는 값을 사용하여 다음 명령을 입력합니다.

   smreghost -i *policy_server_ip_address,port,port,port* -u *admin_user_name* -p *admini_password* -hn *host_name* -hc *host_config_object* -f *host_config_file_path* -o -cf MIGRATE

   policy_server_ip_address, port, port, port

   정책 엔진의 IP 주소와 포트 번호를 지정합니다. SmHost.conf 파일에서 주소를 찾습니다. 기본 포트는 44441, 44442, 44443 입니다.

   기본이 아닌 포트를 사용할 경우에만 포트 번호를 지정하면 됩니다. 기본이 아닌 포트의 경우 세 포트 모두에 동일한 번호를 사용하거나 서로 다른 번호를 사용할 수 있습니다.

   admin_user_name

   관리자 이름을 지정합니다. smreghost 유틸리티를 사용할 때는 이 값에 **siteminder** 를 입력합니다.

   admin_password

   설치할 때 지정한 CA SiteMinder® Federation Standalone 관리자의 암호를 지정합니다.

   hostname

   정책 엔진이 호스트 등록에 사용하는 신뢰할 수 있는 호스트의 이름을 지정합니다. 이 매개 변수에 대한 고유한 값을 입력합니다. SmHost.conf 파일의 호스트 이름은 정책 저장소에 이미 있으므로 사용하지 마십시오.

   host_config_object

   정책 엔진이 사용하는 호스트 구성 개체의 이름을 나타냅니다. SmHost.conf 파일에서 호스트 이름의 값을 찾습니다.

   host_config_file_path

   SmHost.conf 파일의 위치를 지정합니다.

   예

   ```
   smreghost -i localhost -u siteminder -p mypassword
   -hn lfed-localhost20090511024942 -hc fed-localhost20090511024942
   -f "C:\Program Files\CA\FederationManager\secure-proxy\proxy-engine
   \conf\defaultagent\SmHost.conf" -o –cf  MIGRATE
   ```

   이 명령을 실행하면 공유 암호의 다시 암호화가 완료됩니다.

4. 다음 디렉터리에 있는 SmHost.conf 파일로 이동합니다.

   federation-mgr_home\secure-proxy\proxy-engine\conf\defaultagent\SmHost.conf

5. SmHost.conf 파일을 열고 공유 암호가 있으며 {AES}와 같이 FIPS 승인 알고리즘 접두사가 있는지 확인합니다.

공유 암호의 다시 암호화가 완료되었습니다.

정책 저장소 및 키 저장소 데이터 다시 암호화

FIPS 호환 암호화 알고리즘을 사용하도록 정책 및 키 저장소 데이터를 다시 암호화합니다.

정책 및 키 저장소 데이터를 다시 암호화하려면

1. 명령 프롬프트 창을 엽니다.
2. 다음 명령을 입력하여 키 데이터를 내보냅니다.

   smkeyexport -d*admin_name* -w*admin_password* -o*export_file* -l -v -t -cf

   admin_name

   관리자 이름을 지정합니다. smkeyexport 유틸리티를 사용할 때는 이 값에 대해 siteminder 를 입력해야 합니다.

   admin_password

   CA SiteMinder® Federation Standalone 관리자 암호를 지정합니다.

   export_file

   내보내기를 통해 생성된 파일의 이름을 지정합니다. 이 파일의 확장명은 .smdif 여야 합니다.

3. 다음 명령을 입력하여 정책 저장소 데이터를 내보냅니다.

   XPSExport *export_file* -xa –xs –xc -passphrase *passphrase* -v -e *file_name* -l *log_file*

   export_file

   내보내기를 통해 생성되는 출력 파일의 이름을 지정합니다. XPSExport 의 출력은 XML 형식이므로 파일 이름은 **.xml** 확장명으로 끝나야 합니다.

passphrase

중요한 데이터를 암호화하는 데 필요한 암호를 지정합니다. 암호는 8 자 이상이고 숫자, 대문자, 소문자를 각각 하나 이상 포함해야 합니다. 암호에 공백이 포함되어 있는 경우 암호를 따옴표로 묶어야 합니다.

참고: 암호를 직접 입력하지 않으려면 명령에서 지정하지 마십시오. 그러면 XPSExport 도구가 화면에 표시되지 않게 암호와 암호 확인을 묻는 메시지를 표시합니다.

file_name

CA SiteMinder® Federation Standalone 이 오류 메시지를 기록하는 오류 파일의 이름을 지정합니다.

log_file

CA SiteMinder® Federation Standalone 이 내보내기의 결과를 기록하는 로그 파일의 이름을 지정합니다. 이 파일의 이름에는 제한이 없지만 확장명은 .log 를 사용하는 것이 좋습니다.

파일의 전체 경로를 입력하거나 파일 이름만 입력할 수 있습니다. 파일 이름만 입력하면 CA SiteMinder® Federation Standalone 은 XPSExport 명령이 실행된 위치에 파일을 만듭니다. 이 매개 변수에 대해 입력하는 이름은 정책 저장소 데이터를 가져올 때 입력한 log_path 값과 달라야 합니다.

4. 다음 명령을 입력하여 키 데이터를 새 키 저장소 또는 기존 키 저장소로 가져옵니다.

   참고: 정책 저장소를 키 저장소로 사용할 수 있습니다.

   smkeyimport -i*export_file* -da*dmin_name* -w*admin_password* -l -v -t -cf

   export_file

   원본 저장소의 내보내기를 통해 생성된 XML 파일의 이름을 지정합니다.

   admin_name

   관리자 이름을 지정합니다. smkeyimport 유틸리티를 사용할 때는 이 값에 대해 siteminder 를 입력해야 합니다.

   admin_password

   CA SiteMinder® Federation Standalone 관리자 암호를 지정합니다.

5. 다음 명령을 입력하여 정책 저장소 데이터를 새 정책 저장소 또는 기존 정책 저장소로 가져옵니다.

   XPSImport –fo *export_file* -passphrase *passphrase* -vT -vI -vW -vE -vF -l *log_path*

   export_file

   원래 구성을 내보낼 때 생성된 XML 파일의 이름을 지정합니다.

   passphrase

   중요한 데이터의 암호를 해독하는 데 필요한 암호를 지정합니다. 암호는 이전 단계에서 XPSExport 명령을 실행할 때 지정한 암호와 동일해야 합니다.

   log_path

   CA SiteMinder® Federation Standalone 이 가져오기의 결과를 기록하는 로그 파일의 위치와 이름을 지정합니다. 이 파일의 이름에는 제한이 없지만 확장명은 .log 를 사용하는 것이 좋습니다.

CA SiteMinder® Federation Standalone UI 를 FIPS_Only 모드로 설정

FIPS 호환 알고리즘을 사용하도록 모든 필요한 데이터를 다시 암호화한 후에는 모든 파트너 관계 및 SSL 구성이 FIPS 와 호환되는지 확인하십시오.

다음 단계를 수행하십시오.

1. 운영 환경에 맞게 페더레이션 서비스를 다시 시작합니다.

   - **Windows**

     다음과 같이 중지 및 시작 바로 가기를 사용합니다. 로컬 관리자가 아닌 네트워크 사용자로 로그인한 경우에는 바로 가기를 마우스 오른쪽 단추로 클릭하고 "관리자 권한으로 실행"을 선택하십시오.

     a. "시작", "모든 프로그램", "CA", "Federation Standalone", "서비스 중지"

     b. "시작", "모든 프로그램", "CA", "Federation Standalone", "서비스 시작"

- **UNIX**

  a. 명령 창을 엽니다.

  b. 다음 스크립트를 실행합니다.

  federation_install_dir/fedmanager.sh stop

  federation_install_dir/fedmanager.sh start

  참고: 서비스를 중지했다가 루트 사용자로 시작하지 마십시오.

2. Administrative UI 에 로그인합니다.
3. "인프라", "배포 설정"으로 이동합니다.

   "배포 설정 구성" 대화 상자가 열립니다.
4. "배포 설정" 섹션의 "확인" 단추가 활성화되어 있으며 "Ready to Migrate to Only mode"(전용 모드로 마이그레이션 준비) 메시지가 "예"로 설정되어 있는지 확인합니다.

   이 두 조건이 충족되지 않으면 하나 이상의 파트너 관계 또는 SSL 구성이 FIPS 를 사용하도록 설정되지 않은 것입니다. 파트너 관계가 FIPS 를 사용하도록 설정되지 않은 이유는 다음과 같습니다.

   - "응용 프로그램 통합" 대화 상자에서 PBE 알고리즘이 적용되는 열린 파일 에어전트를 사용한 "리디렉션 모드" 설정

     PBE 암호화 알고리즘이 적용되는 열린 파일 에어전트를 사용하도록 "리디렉션 모드" 설정을 구성하면 모드는 FIPS 와 호환되지 않습니다.

   - 프로비저닝의 전송 유형이 PBE 알고리즘이 적용되는 개방 형식 쿠키로 설정되었습니다.

     PBE 암호화 알고리즘이 적용되는 열린 파일 에어전트를 사용하도록 "Provisioning Delivery Type"(프로비저닝 전송 유형)을 구성한 경우 이 전송 메커니즘은 FIPS 와 호환되지 않습니다.

   - 위임된 인증에 대한 전역 개방 형식 쿠키 설정이 PBE 알고리즘을 사용한 설정으로 설정되었습니다.

     "배포 설정" 대화 상자에서 PBE 암호화 알고리즘을 사용하도록 개방 형식 쿠키를 지정한 경우 쿠키는 FIPS 와 호환되지 않습니다.

이 문제를 해결하려면 다음 작업을 수행하십시오.

- 비 FIPS 파트너 관계가 있는 경우에는 이 파트너 관계를 비활성화하거나 이러한 모든 파트너 관계가 FIPS 승인 인증서 및 암호화 알고리즘을 사용하는지 확인하십시오.
- SSL 구성이 FIPS 승인을 받지 않은 경우 SSL 을 비활성화한 다음 FIPS 승인 인증서를 사용하여 다시 구성합니다.

5. "확인"을 클릭하여 UI 를 FIPS_ONLY 모드로 마이그레이션합니다.

이제 Administrative UI 가 FIPS_ONLY 모드에서 작동합니다.

보안 프록시 엔진을 FIPS_Only 모드로 설정

마이그레이션 프로세스의 일부로 보안 프록시 엔진을 FIPS_Only 모드로 설정할 수 있습니다.

보안 프록시 엔진을 FIPS_Only 모드로 설정하려면

1. 명령 창을 엽니다.
2. *federation-manager_home*\secure-proxy\proxy-engine\conf\defaultagent\SmHost.conf 로 이동합니다.
3. 텍스트 편집기에서 SmHost.conf 파일을 엽니다.
4. fipsmode 설정을 MIGRATE 에서 ONLY 로 변경합니다.

   예: fipsmode="ONLY"

이제 프록시 엔진이 FIPS_Only 모드에서 작동합니다.

정책 엔진을 FIPS_Only 모드로 설정

마이그레이션 프로세스의 마지막 단계는 정책 엔진을 FIPS_Only 모드로 설정하는 것입니다.

다음 단계를 수행하십시오.

1. (Solaris 에만 해당) CA SiteMinder® Federation Standalone 환경 스크립트 ca_federation_env.ksh 의 경로를 수정하여 적절한 환경 변수를 설정합니다.
2. 명령 프롬프트에서 다음과 같이 setFIPSmigration 명령을 실행합니다.

   Windows

   setFIPSonly 를 입력합니다.

   UNIX

   a. *federation_install_dir*\secure-proxy 로 이동합니다.

   b. setFIPSonly.ksh 를 입력합니다.

   c. 환경 스크립트 ca_federation_env.ksh 를 실행하여 환경 변수를 설정합니다.

   명령에 성공하면 명령 프롬프트에 FIPS_ONLY 라는 단어가 나타납니다.
3. 다음 작업 중 하나를 수행하십시오.

   Windows

   페더레이션 시스템을 재부팅합니다.

   UNIX

   명령 창에서 다음 스크립트를 실행하여 페더레이션 서비스를 다시 시작합니다.

   a. *federation_install_dir*/fedmanager.sh stop

   b. *federation_install_dir*/fedmanager.sh start
4. 정책 엔진이 FIPS_ONLY 모드에서 작동하는지 확인합니다. *federation_install_dir*\logs\server 디렉터리에서 smps 로그를 확인합니다.

FIPS 호환 SSL 인증서 가져오기(선택 사항)

페더레이션 시스템을 FIPS_Only 모드로 마이그레이션하고 나면 CA SiteMinder?Federation Standalone 이 SSL 구성을 위해 사용하는 서버 인증서가 FIPS 와 호환되어야 합니다. 시스템이 SSL 에 사용하는 서버 인증서가 MD5 형식인 경우에는 FIPS 와 호환되는 SHA1 알고리즘을 사용하는 새 인증서를 받으십시오.

SSL 인증서를 업데이트해야 하는지 여부를 확인하려면

1. 현재 SSL 인증서의 FIPS 상태를 확인합니다.

   이러한 인증서는 포함된 웹 서버 및 Administrative UI 에 사용되는 인증서입니다.

2. FIPS 상태가 False 이면 새 인증서를 요청합니다.
3. 새 FIPS 호환 서버 인증서를 업로드합니다.

구체적인 절차는 이어지는 단원에서 설명합니다.

SSL 인증서의 FIPS 상태 확인

포함된 웹 서버 및 관리 UI 에 대한 SSL 인증서의 FIPS 상태를 확인합니다. 새 FIPS 승인 인증서가 필요한지 확인합니다.

SSL 인증서의 상태를 확인하려면

1. Administrative UI 에 로그인합니다.
2. "인프라", "SSL 구성"으로 이동합니다.

   "SSL 구성" 대화 상자가 표시됩니다.

3. "FIPS 승인됨" 필드에서 포함 웹 서버 및 관리 UI 를 찾습니다. 다음 작업 중 하나를 수행하십시오.
   - "FIPS 승인됨" 상태가 True 인 경우 추가 작업을 수행하지 않습니다.
   - 상태가 False 인 경우 다음 절차의 설명에 따라 FIPS 승인 인증서를 받습니다.

FIPS 호환 서버 인증서 요청

포함된 웹 서버 또는 관리 UI 에 대한 "FIPS 승인됨" 설정이 False 인 경우에는 새 FIPS 호환 인증서를 요청합니다. 두 구성 요소 모두에 새 인증서가 필요한 경우 각 구성 요소마다 별도의 요청을 생성하고 전체 요청 프로세스를 완료합니다.

FIPS 호환 서버 인증서를 요청하려면

1. Administrative UI 에 로그인합니다.
2. "인프라", "SSL 구성"으로 이동합니다.

   "SSL 구성" 대화 상자가 표시됩니다.
3. 새 인증서가 필요한 구성 요소에 해당하는 섹션에서 "요청"을 클릭합니다.

   "인증서 요청" 대화 상자가 표시됩니다.
4. "인증서 요청" 대화 상자의 필드를 완성합니다.

   인증서가 FIPS 승인을 받도록 SHA-1 서명 알고리즘이 적용된 인증서를 요청해야 합니다. 일부 CA 는 다른 알고리즘의 사용을 요청하는 경우를 제외하고 기본적으로 MD5 를 사용합니다.
5. "저장"을 클릭합니다.

   PKCS#10 형식의 파일이 저장됩니다.
6. 파일을 인증 기관에 제출하고 새 인증서를 받습니다. 요청을 제출하기에 적절한 절차에 대해서는 인증 기관에 문의하십시오.

   CA 는 서명된 인증서가 포함된 응답을 보냅니다.
7. 다음 절차의 설명에 따라 새 인증서를 키 저장소에 업로드합니다.
8. 필요한 경우 다른 요청에 대해 이 절차를 반복합니다.

FIPS 호환 인증서 업로드

새 인증서를 받은 후에 키 저장소에 업로드합니다. 둘 이상의 인증서를 요청한 경우에는 하나씩 따로 업로드합니다.

새 인증서를 업로드하려면

1. "인프라", "SSL 구성"으로 이동합니다.

   "SSL 구성" 대화 상자가 표시됩니다.

2. "서명된 인증서 응답" 필드 옆의 "찾아보기"를 클릭하여 새로 서명된 응답 파일을 찾습니다.

   참고: SSL 은 둘 이상의 쌍을 지원하지 않기 때문에 SSL 기능에는 하나의 키와 인증서 쌍만 필요합니다.

3. "CA 인증서" 필드의 풀다운 메뉴에서 SSL 인증서에 서명한 CA 를 선택합니다.

   CA 인증서가 키 저장소에 없으면 SSL 인증서 요청에 서명하는 데 사용된 CA 인증서의 복사본을 가져옵니다.

4. "가져오기"를 클릭하여 인증서를 가져오고 가져오기 단계를 완료합니다.

5. "적용"을 클릭하여 서버 인증서를 CA SiteMinder® Federation Standalone 에 업로드합니다.

   확인 메시지가 표시되고, 인증서 업데이트를 나타내도록 SSL 구성이 변경됩니다.

6. "활성화"를 클릭하고 SSL 구성을 다시 시작합니다.

   "FIPS 승인됨" 상태는 인증서가 FIPS 와 호환됨을 나타내는 True 여야 합니다.

7. 운영 환경에 맞게 페더레이션 서비스를 다시 시작합니다.

   - **Windows**

     다음과 같이 중지 및 시작 바로 가기를 사용합니다. 로컬 관리자가 아닌 네트워크 사용자로 로그인한 경우에는 바로 가기를 마우스 오른쪽 단추로 클릭하고 "관리자 권한으로 실행"을 선택하십시오.

     a. "시작", "모든 프로그램", "CA", "Federation Standalone", "서비스 중지"

     b. "시작", "모든 프로그램", "CA", "Federation Standalone", "서비스 시작"

- **UNIX**

  a. 명령 창을 엽니다.

  b. 다음 스크립트를 실행합니다.

  federation_home/fedmanager.sh stop

  federation_home/fedmanager.sh start

  참고: 서비스를 중지했다가 루트 사용자로 시작하지 마십시오.

이제 SSL 구성에 대한 서버 인증서가 FIPS 와 호환됩니다.

제 6 장: CA SiteMinder® Federation Standalone 문제 해결

이 섹션은 다음 항목을 포함하고 있습니다.

설치 문제 해결 (페이지 121)
키 데이터베이스 마이그레이션 문제 해결 (페이지 123)
XML 서명 래핑 공격 방지 (페이지 128)
기존 시스템의 JDK 업그레이드 (페이지 128)

설치 문제 해결

다음은 설치 및 구성 문제를 해결하는 데 도움이 될 수 있는 정보입니다.

CA SiteMinder® Federation Standalone 라이선스를 받거나 소프트웨어를 다운로드할 때 문제 발생

증상

CA SiteMinder® Federation Standalone 라이선스를 받거나 CA SiteMinder® Federation Standalone 소프트웨어를 다운로드할 때 문제가 발생합니다.

해결 방법

고객 영업 관리자에게 지원을 요청하십시오.

CA SiteMinder® Federation Standalone UI 또는 구성 요소 서비스가 시작되지 않음

증상

CA SiteMinder® Federation Standalone UI 가 시작되지 않습니다.

해결 방법

1. URL 의 포트 및 호스트 이름이 올바른지 확인합니다.
2. 운영 환경에 맞게 페더레이션 서비스를 다시 시작합니다.
   - **Windows**

     다음과 같이 중지 및 시작 바로 가기를 사용합니다. 로컬 관리자가 아닌 네트워크 사용자로 로그인한 경우에는 바로 가기를 마우스 오른쪽 단추로 클릭하고 "관리자 권한으로 실행"을 선택하십시오.

     a. "시작", "모든 프로그램", "CA", "Federation Standalone", "서비스 중지"

     b. "시작", "모든 프로그램", "CA", "Federation Standalone", "서비스 시작"

   - **UNIX**

     a. 명령 창을 엽니다.

     b. 다음 스크립트를 실행합니다.

     federation_install_dir/fedmanager.sh stop

     federation_install_dir/fedmanager.sh start

참고: 서비스를 중지했다가 루트 사용자로 시작하지 마십시오.

구성 관리자를 실행할 때 설치가 실패함

증상

구성 관리자를 실행할 때 CA SiteMinder® Federation Standalone 설치가 중지되거나 실패합니다.

해결 방법

데이터베이스 서버 정보를 묻는 메시지가 나타나면 정규화된 호스트 이름이 아니라 데이터베이스 서버의 IP 주소를 입력하십시오. IP 주소를 사용하면 설치 및 구성이 성공적으로 완료됩니다.

키 데이터베이스 마이그레이션 문제 해결

다음 단원에서는 키 데이터베이스를 인증서 데이터 저장소로 마이그레이션할 때 발생하는 문제를 해결하는 방법을 자세히 설명합니다.

SiteMinder 키 데이터베이스 마이그레이션의 상태를 알 수 없음

증상

CA SiteMinder® Federation Standalone 이 업그레이드되었습니다. 하지만 인증서 데이터 저장소로의 smkeydatabase 마이그레이션이 성공했는지 여부가 불확실합니다.

해결 방법

마이그레이션이 성공했는지 확인하려면 smkeydatabase 마이그레이션 유틸리티(smmigratecds)를 사용하십시오.

참고: 이 유틸리티의 기본 위치는 *federation_install_dir*\siteminder\bin 입니다.

federation_install_dir

CA SiteMinder® Federation Standalone 설치 경로를 지정합니다.

다음 단계를 수행하십시오.

1. smkeydatabase 가 함께 배치된 호스트 시스템에 로그인합니다.
2. 다음 단계 중 하나를 수행합니다.
   - (Windows) 명령 프롬프트를 열고 다음 명령을 입력합니다.

     ```
     smmigratecds.bat –isComplete
     ```

     -isComplete

     이전 마이그레이션이 성공했는지 확인합니다.
   - (UNIX) 셸을 열고 다음 명령을 실행합니다.

     ```
     smmigratecds.sh –isComplete
     ```

마이그레이션에 성공한 경우 시스템이 이미 마이그레이션되었다는 메시지가 표시됩니다. 마이그레이션에 실패한 경우에는 시스템을 마이그레이션해야 한다는 메시지가 표시됩니다.

마이그레이션 실패 오류 발생

증상

smkeydatabase 마이그레이션이 실패했다는 메시지가 표시됩니다.

해결 방법

마이그레이션 유틸리티(smmigratecds)는 smkeydatabase 의 콘텐츠를 인증서 데이터 저장소와 비교하여 하나 이상의 데이터 불일치를 찾아냅니다. 데이터 불일치의 예는 서로 다른 인증서에 동일한 별칭이 매핑된 경우입니다.

이러한 불일치가 있으면 마이그레이션이 실패합니다.

다음 단계를 수행하십시오.

1. smkeydatabase 마이그레이션 로그(smkeydatabaseMigration.log)를 사용하여 문제를 찾습니다.

   smmigratecds 유틸리티를 실행하면 로그 파일을 지정할 수 있습니다.

   로그 파일의 기본 위치는 *federation_install_dir*/siteminder/log 입니다.

   CA SiteMinder® Federation Standalone 의 설치 디렉터리는 *federation_install_dir* 입니다.

2. 액세스 레거시 키 저장소 플래그(–accessLegacyKS)로 smkeytool 유틸리티를 사용하여 smkeydatabase 에 액세스합니다.
3. 실패의 원인이 된 데이터 불일치를 해결합니다.

   참고: 자세한 내용은 smkeytool 사용 방법을 검토하십시오.
4. 키 데이터베이스를 수동으로 마이그레이션합니다.

인증서 데이터 저장소 오류 발생

증상

인증서 데이터 저장소가 구성되지 않았다는 메시지가 표시됩니다.

해결 방법

다음 단계를 수행하십시오.

1. CA SiteMinder® Federation Standalone 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행합니다.

   ```
   XPSDDInstall CDSObjects.xdd
   ```

   정책 저장소 스키마가 인증서 데이터 저장소를 지원하도록 확장됩니다.
3. 다음 단계 중 하나를 수행합니다.
   - (Windows) 명령 프롬프트를 열고 다음 명령을 입력합니다.

     ```
     smmigratecds.bat –validateInstall
     ```

     validateInstall

     인증서 데이터 저장소가 올바르게 설치되었는지 확인합니다.
   - (UNIX) 셸을 열고 다음 명령을 실행합니다.

     ```
     smmigratecds.sh -validateInstall
     ```

     인증서 저장소가 올바르게 구성된 경우 설치가 유효하다는 메시지가 표시됩니다. 인증서 데이터 저장소 설치가 실패한 경우에는 설치가 유효하지 않다는 메시지가 표시됩니다.
4. 키 데이터베이스를 수동으로 마이그레이션합니다.

SiteMinder 키 데이터베이스 수동 마이그레이션

증상

smkeydatabase 인증서 데이터를 인증서 데이터 저장소로 수동으로 마이그레이션하고자 합니다.

해결 방법

smkeydatabase 마이그레이션 유틸리티(smmigratecds)를 사용하십시오.

다음 단계를 수행하십시오.

1. 모든 smkeydatabase 인스턴스가 동기화되었는지 확인합니다.
2. smkeydatabase 가 함께 배치된 페더레이션 호스트 시스템에 로그인합니다.
3. 다음 단계 중 하나를 수행하여 인증서 데이터 저장소가 올바르게 구성되었는지 확인합니다.
   - (Windows) 명령 프롬프트를 열고 다음 명령을 입력합니다.

     ```
     smmigratecds.bat –validateInstall
     ```

     -validateInstall

     인증서 데이터 저장소가 올바르게 설치되었는지 확인합니다.
   - (UNIX) 셸을 열고 다음 명령을 실행합니다.

     ```
     smmigratecds.sh -validateInstall
     ```
4. smkeydatabase 의 콘텐츠를 인증서 데이터 저장소와 비교합니다. 콘텐츠를 비교하면 마이그레이션 실패의 원인이 될 수 있는 데이터 불일치를 확인할 수 있습니다.

   운영 플랫폼에 맞는 단계를 수행합니다.
   - (Windows) 다음 명령을 실행합니다.

     ```
     smmigratecds.bat –validate -log log_file
     ```

     -validate

     smkeydatabase의 내용을 인증서 데이터 저장소와 비교합니다.

     -log

     확인 결과를 로그로 보냅니다.

     log_file

     유틸리티가 로그를 보낼 로그 파일의 이름과 위치를 지정합니다.

     예: -log "C:\FederationStandalone\logs"
   - (UNIX) 다음 명령을 실행합니다.

     ```
     smmigratecds.sh -validate -log log_file
     ```
5. (선택 사항) 데이터 불일치가 존재하는 경우 로그 파일을 사용하여 문제를 찾습니다.

6. 다음 단계 중 하나를 수행하여 마이그레이션을 시작합니다.

   - (Windows) 다음 명령을 실행합니다.

     ```
     smmigratecds.bat -migrate -log log_file -p
     unencrypted_password
     ```

   - (UNIX) 다음 명령을 실행합니다.

     ```
     smmigratecds.sh -migrate -log log_file -p unencrypted_password
     ```

   명령 인수는 다음 작업을 나타냅니다.

   -migrate

   smkeydatabase를 인증서 데이터 저장소로 마이그레이션합니다.

   -log

   마이그레이션 결과를 로그로 보냅니다.

   log_file

   유틸리티가 로그를 보낼 로그 파일의 이름과 위치를 지정합니다.

   예:

   -log "C:\Progam Files\Sample\Logs"

   -log export/fed/Sample/Logs"

   -p

   (선택 사항) smkeydatabase 암호의 암호화되지 않은 값을 지정합니다. 시스템이 smkeydatabase.properties 파일에 저장된 암호를 암호 해독할 수 없는 경우와 관련된 문제를 방지하기 위해 이 인수를 사용합니다.

   unencrypted_password

   smkeydatabase에 대해 암호화되지 않은 암호를 지정합니다.

7. (선택 사항) 마이그레이션에 실패한 경우 로그 파일을 사용하여 원인을 파악합니다.

XML 서명 래핑 공격 방지

악의적인 사용자가 서명을 무효화하지 않고 문서 서명의 내용을 변경하여 XML 서명 래핑 공격을 실행할 수 있습니다.

페더레이션 트랜잭션이 실패하는 경우 smtracedefault.log 파일과 fwstrace.log 파일을 검사하십시오. 이러한 로그 파일에 서명 확인 오류가 포함되어 있을 수 있습니다. 다음과 같은 이유로 서명 확인 오류가 발생할 수 있습니다.

- XML 문서에 중복 ID 요소가 있으며 중복 ID 특성이 허용되지 않는 경우
- 서명이 해당 중복 ID 를 참조하는 경우
- 서명이 필요한 부모 요소를 참조하지 않는 등의 서명 래핑 취약점이 로깅되는 경우

서명 취약점으로부터 보호하려면

1. 다음 위치 중 하나에 있는 xsw.properties 파일로 이동합니다.
   - smtracedefualt.log 파일에 오류 메시지가 있는 경우 *federation_install_dir*/siteminder/config/properties 로 이동합니다.
   - fwstrace.log 에 오류 메시지가 있는 경우 *federation_install_dir*/secure-proxy/tomcat/webapps/affwebservices/web-INF/classes 로 이동합니다.
2. xsw.properties 파일에 다음 설정을 추가하고 각각을 true 로 설정합니다.

   DisableXSWCheck=true

   DisableUniqueIDCheck=true
3. 파일을 저장합니다.

기존 시스템의 JDK 업그레이드

기존 CA SiteMinder?Federation Standalone 시스템에서 JDK 를 업그레이드하는 경우 CA SiteMinder?Federation Standalone 설치 프로그램을 다시 실행하고 업그레이드된 JDK 버전을 가리키십시오.

제 7 장: 키 도구 참조

키 도구 유틸리티(smkeytool)는 CDS 마이그레이션 문제를 해결하기 위한 용도로만 사용됩니다. 다른 모든 인증서 관리에는 CA SiteMinder?Federation Standalone Administrative UI 를 사용합니다.

키 도구 유틸리티(smkeytool)는 다음과 같은 기능을 지원합니다.

- r12.52 SP1 로 업그레이드/마이그레이션하는 동안 레거시 smkeydatabase 에 대한 액세스를 지원합니다. 레거시 키 저장소 액세스 플래그(-accessLegacyKS)를 사용하여 인증서 데이터 저장소로의 마이그레이션 실패를 초래할 수 있는 모든 데이터 충돌을 해결할 수 있습니다.
- 다음 위치에 설치됩니다.

  *federation_install_dir/siteminder/*bin

  federation_install_dir

  제품의 설치 경로를 지정합니다.

다음 단계를 수행하십시오.

1. 명령줄 또는 셸을 엽니다.
2. 다음 명령 중 하나를 실행합니다.
   - (Windows) smkeytool.bat -*option* [-*arguments*]
   - (UNIX) smkeytool.sh -*option* [-*arguments*]

이 섹션은 다음 항목을 포함하고 있습니다.

개인 키 및 인증서 쌍 추가 (페이지 130)
인증서 추가 (페이지 132)
해지 정보 추가 (페이지 133)
해지 정보 삭제 (페이지 134)
인증서 데이터 제거 (페이지 134)
인증서 삭제 (페이지 135)
인증서 또는 개인 키 내보내기 (페이지 135)
별칭 찾기 (페이지 136)
기본 CA 인증서 가져오기 (페이지 137)
모든 인증서의 메타데이터 나열 (페이지 137)
해지 정보 나열 (페이지 138)
인증서 메타데이터 표시 (페이지 139)
별칭 이름 변경 (페이지 139)
인증서 유효성 검사 (페이지 140)

개인 키 및 인증서 쌍 추가

개인 키/인증서 쌍만 인증서 데이터 저장소로 가져오려면 addPrivKey 옵션을 사용하십시오. 다음 사항을 고려하십시오.

- 저장소에 여러 개의 개인 키/인증서 쌍이 있을 수 있지만 SiteMinder 는 저장소의 RSA 키만 지원합니다.
- 개인 키/인증서 쌍만 암호화된 형식으로 저장됩니다.
- 생산 기관의 정책 서버는 다음을 수행합니다.
  - 단일 개인 키/인증서 쌍을 사용하여 SAML 어설션에 서명합니다.
  - 인증서를 사용하여 소비 기관에서 받은 암호화된 SAML 어설션을 암호 해독합니다.

  일반적으로 키는 인증서 데이터 저장소에서 발견된 첫 번째 개인 키/인증서 쌍입니다.

- 인증서 파일을 가져오기 전에 인증서 파일에서 인증서 메타데이터를 삭제하십시오. --BEGIN CERTIFICATE-- 표시로 시작하고 --END CERTIFICATE-- 표시로 끝나는 데이터만 가져오십시오. 표시를 포함하십시오.

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 r12.52 SP1 인증서 데이터 저장소에 적용됩니다.

-alias *alias*

필수입니다. 데이터베이스의 개인 키/인증서 쌍에 별칭을 할당합니다. 별칭은 고유한 문자열이어야 하며 영숫자 문자만 포함할 수 있습니다.

-certfile *cert_file*

개인 키/인증서 쌍과 연결된 인증서 위치의 전체 경로를 지정합니다. PKCS1, PKCS5 및 PKCS8 형식의 키에 필요합니다.

-keyfile *private_key_file*

개인 키 파일 위치의 전체 경로를 지정합니다. PKCS1, PKCS5 및 PKCS8 형식의 키에 필요합니다.

-keycertfile *key_cert_file*

개인 키/인증서 쌍 데이터가 포함된 PKCS12 파일 위치의 전체 경로를 지정합니다. PKCS12 형식의 키에 필요합니다.

-password *password*

(선택 사항) 쌍이 생성될 때 개인 키/인증서 쌍을 암호화하는 데 사용된 암호를 지정합니다. 인증서 데이터 저장소에 쓰기 전에 개인 키/인증서 쌍을 암호 해독하려면 이 암호를 제공하십시오.

참고: 이 암호는 인증서 데이터 저장소에 저장되지 않습니다.

키/인증서 쌍이 암호 해독되어 인증서 데이터 저장소에 저장된 후에는 SiteMinder 에서 자체 암호를 사용하여 쌍을 다시 암호화합니다.

인증서 추가

공개 인증서 또는 트러스트된 CA 인증서를 인증서 데이터 저장소에 추가하려면 addCert 옵션을 사용하십시오.

다음 사항을 고려하십시오.

- 인증서는 개인 키/인증서 쌍과 연결된 인증서일 수 있습니다. 하지만 인증서만 인증서 데이터 저장소에 추가됩니다.
- 인증서를 인증 기관으로 신뢰하는 경우 이 인증서는 항상 CA 인증서로 취급됩니다.
- X.509 인증서 형식의 경우 SiteMinder 는 V1, V2 및 V3 버전을 지원합니다. 인코딩 형식의 경우 SiteMinder 는 DER 및 PEM 형식을 지원합니다.
- 인증 기관 인증서를 추가할 때 웹 에이전트를 다시 시작하십시오.
- 인증서 파일을 가져오기 전에 인증서 파일에서 인증서 메타데이터를 삭제하십시오. --BEGIN CERTIFICATE-- 표시로 시작하고 --END CERTIFICATE-- 표시로 끝나는 데이터만 가져오십시오. 표시를 포함하십시오.

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 r12.52 SP1 인증서 데이터 저장소에 적용됩니다.

-alias *alias*

필수입니다. 인증서 데이터 저장소의 개인 키와 연결된 인증서에 별칭을 지정합니다.

제한: 영숫자 문자만 포함하는 고유한 문자열이어야 합니다.

-infile *cert_file*

필수입니다. 새로 추가된 인증서 위치의 전체 경로를 지정합니다.

-trustcacert

선택 사항입니다. 인증서를 추가할 사용자 공급자 인증서가 CA 인증서인지 확인합니다. 유틸리티가 인증서에 디지털 서명 확장이 있고 인증서에 동일한 IssuerDN 및 SubjectDN 값이 있는지를 확인합니다.

-noprompt

(선택 사항) 사용자에게 인증서 추가를 확인하라는 메시지가 표시되지 않습니다.

해지 정보 추가

CRL 의 위치를 지정하려면 addRevocationInfo 옵션을 사용하십시오. 인증서 데이터 저장소는 CRL 의 위치를 참조합니다.

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 r12.52 SP1 인증서 데이터 저장소에 적용됩니다.

-issueralias *issuer_alias*

필수입니다. CRL 을 발급하는 인증 기관의 별칭을 지정합니다.

예: -issueralias verisignCA

-type (*ldapcrl* | *filecrl*)

필수입니다. CRL 이 LDAP 기반인지 아니면 파일 기반인지를 지정합니다.

-location *location*

필수입니다. CRL 의 위치를 지정합니다.

- (파일 기반) 파일의 전체 경로입니다.

  예: -location c:\crls\siteminder_root_ca.crl

- (LDAP 디렉터리 서비스) LDAP 서버 노드의 전체 경로입니다.

  예: -location "http://localhost:880/sn=siteminderroot, dc=crls,dc=com"

해지 정보 삭제

인증서 데이터 저장소에서 CRL 을 삭제하려면 deleteRevocationInfo 옵션을 사용하십시오.

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 r12.52 SP1 인증서 데이터 저장소에 적용됩니다.

-issueralias *issuer_alias*

(필수) CRL 을 발급하는 인증 기관의 이름을 지정합니다.

-noprompt

(선택 사항) 사용자에게 CRL 이 삭제될 수 있음을 확인하라는 메시지가 표시되지 않습니다.

인증서 데이터 제거

인증서 데이터 저장소에서 모든 인증서 데이터를 제거하려면 removeAllCertificateData 옵션을 사용하십시오.

이 옵션의 인수는 다음과 같습니다.

-noprompt

(선택 사항) 사용자에게 인증서 데이터가 제거될 수 있음을 확인하라는 메시지가 표시되지 않습니다.

인증서 삭제

인증서를 인증서 데이터 저장소에서 제거하려면 delete 옵션을 사용하십시오. 인증서에 개인 키가 연결되어 있는 경우에는 개인 키도 삭제됩니다.

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 r12.52 SP1 인증서 데이터 저장소에 적용됩니다.

-alias *<alias>*

(필수) 옵션으로 제거할 인증서의 별칭을 지정합니다.

-noprompt

(선택 사항) 사용자에게 인증서가 제거될 수 있음을 확인하라는 메시지가 표시되지 않습니다.

인증서 또는 개인 키 내보내기

인증서 또는 개인 키를 파일로 내보내려면 export 옵션을 사용하십시오.

다음 사항을 고려하십시오.

- 인증서 데이터는 PEM 인코딩을 사용하여 내보냅니다.
- 개인 키 데이터는 DER 인코딩 PKCS8 형식을 사용하여 내보냅니다.

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 r12.52 SP1 인증서 데이터 저장소에 적용됩니다.

-alias *alias*

(필수) 내보낼 인증서 또는 키를 식별합니다.

-outfile *out_file*

(필수) 데이터를 내보낼 파일의 전체 경로를 지정합니다.

-type (key|cert)

(선택 사항) 인증서 또는 키 중에서 어느 것을 내보낼지 지정합니다.

기본값: certificate.

-password *password*

개인 키를 내보낼 때만 필요합니다. 내보낼 때 개인 키를 암호화하는 데 사용할 암호를 지정합니다. 공개 키가 있는 인증서를 내보낼 때는 인증서를 일반 텍스트로 내보내므로 암호가 필요하지 않습니다.

이 개인 키를 다시 인증서 데이터 저장소에 추가하려면 이 암호와 함께 addPrivKey 옵션을 함께 사용하십시오.

별칭 찾기

인증서 데이터 저장소의 인증서와 연결된 별칭을 찾으려면 findAlias 옵션을 사용하십시오.

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 r12.52 SP1 인증서 데이터 저장소에 적용됩니다.

-infile *cert_file*

(필수) 원하는 별칭과 연결된 인증서 파일의 전체 경로를 지정합니다.

-password *password*

password–protected P12 파일이 인증서 파일로 지정된 경우에만 필요합니다.

기본 CA 인증서 가져오기

SiteMinder 에 포함된 모든 기본 트러스트된 인증 기관 인증서를 인증서 데이터 저장소로 가져오려면 importDefaultCACerts 옵션을 사용하십시오.

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 r12.52 SP1 인증서 데이터 저장소에 적용됩니다.

모든 인증서의 메타데이터 나열

인증서 데이터 저장소에 저장된 모든 인증서의 일부 메타데이터를 나열하려면 listCerts 옵션을 사용하십시오.

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 r12.52 SP1 인증서 데이터 저장소에 적용됩니다.

-alias *alias*

(선택 사항) 지정된 별칭과 연결된 인증서 및 키의 메타데이터 상세 정보를 나열합니다.

이 옵션은 별표(*)를 와일드카드 문자로 지원합니다. 와일드카드는 다음 위치에 사용할 수 있습니다.

- 별칭 값의 시작 또는 끝
- 별칭 값의 시작 및 끝

명령 셸이 와일드카드 문자를 해석하지 않도록 하려면 와일드카드를 따옴표로 묶으십시오.

해지 정보 나열

인증서 데이터 저장소에 있는 인증서 해지 목록의 목록을 표시하려면 listRevocationInfo 옵션을 사용하십시오. 다음 항목이 나열됩니다.

- CRL 이름
- CRL 이 파일 기반인지 LDAP 기반인지 여부
- CRL 위치

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 r12.52 SP1 인증서 데이터 저장소에 적용됩니다.

-issueralias *issuer_alias*

(선택 사항) CRL 을 발급하는 인증 기관의 이름입니다.

이 옵션은 별표(*)를 와일드카드 문자로 지원합니다. 와일드카드는 다음 위치에 사용할 수 있습니다.

- 별칭 값의 시작 또는 끝
- 별칭 값의 시작 및 끝

명령 셸이 와일드카드 문자를 해석하지 않도록 하려면 와일드카드를 따옴표로 묶으십시오.

인증서 메타데이터 표시

지정된 인증서에 대한 일부 메타데이터를 표시하려면 printCert 옵션을 사용하십시오. 이 명령은 인증서 속성을 보기 어려운 시스템에서 유용합니다.

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 r12.52 SP1 인증서 데이터 저장소에 적용됩니다.

-infile *cert_file*

필수입니다. 인증서 파일의 위치입니다.

-password *password*

암호는 암호로 보호된 P12 파일이 인증서 파일로 지정된 경우에만 필요합니다.

별칭 이름 변경

인증서와 연결된 별칭의 이름을 바꾸려면 renameAlias 옵션을 사용하십시오.

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 r12.52 SP1 인증서 데이터 저장소에 적용됩니다.

-alias *current_alias*

(필수) 인증서와 연결된 별칭을 지정합니다.

-newalias *new_alias*

(필수) 새 별칭 이름을 지정합니다.

제한: 영숫자 문자만 포함하는 고유한 문자열이어야 합니다.

인증서 유효성 검사

인증서가 해지되었는지 확인하려면 validateCert 옵션을 사용하십시오.

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 r12.52 SP1 인증서 데이터 저장소에 적용됩니다.

-alias *alias*

(필수) 인증서 데이터 저장소의 개인 키와 연결된 인증서에 별칭을 지정합니다.

제한: 영숫자 문자만 포함하는 고유한 문자열이어야 합니다.

-infile *crl_file*

(선택 사항) 유틸리티에서 유효성을 확인하기 위해 인증서를 찾을 CRL 을 지정합니다.