

SiteMinder

정책 서버 구성 안내서

12.52 SP1



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

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

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

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

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

본 문서는 CA에서 제작되었습니다.

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

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

CA Technologies 제품 참조

이 문서에서 참조하는 CA Technologies 제품은 다음과 같습니다.

- CA DataMinder™ (이전의 CA DLP)
- CA Single Sign-On
- SiteMinder
- CA Enterprise Log Manager

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.

제 1 장: 설명서 변경 사항

SiteMinder 의 이전 릴리스에서 발견된 문제로 인해 다음과 같은 내용이 12.52 SP1 설명서에서 업데이트되었습니다.

- [SSL 을 통한 LDAP 사용자 디렉터리 연결 구성 방법](#) (페이지 202) - 인증 기관에서 서명된 서버 인증서도 인증서 데이터베이스로 가져온 루트 인증 기관 인증서가 필요함을 설명하는 정보가 3 단계에 추가되어 업데이트되었습니다. RTC 결함 118828 을 해결합니다.
- [DeviceDNA™를 사용한 고급 세션 보증을 위한 SiteMinder 환경 구성](#) (페이지 731) - 업그레이드 후에 정책 서버 구성 마법사를 실행하는 단계가 추가되었습니다. 이것은 STAR 이슈 # 21807419:01 을 해결합니다.
- [Kerberos 인증을 구성하는 방법](#) (페이지 335) - 부록의 이전 내용이 재작성되었습니다. 새로운 Kerberos 인증 체계 템플릿을 포함하도록 업데이트되었습니다.
- [리스크 기반 인증을 위해 SecurID HTML 양식 인증 지원을 구성하는 방법](#) (페이지 387) - 새 섹션에서 리스크 기반 인증(RBA)을 위한 SiteMinder SecurID HTML 양식 인증 지원을 구성하는 방법을 설명합니다.
- Active Directory 고려 사항 - IgnoreDefaultRedirectOnADnativeDisabled 레지스트리 설정과 관련한 잘못된 설명이 제거되었습니다. 이 업데이트는 CQ170141 및 STAR Issue # 21243447:03 을 해결합니다.
- [OAuth 인증 체계 구성 방법](#) (페이지 408) - "응용 프로그램을 OAuth 공급자에 등록" 절에서 필드 이름이 수정되었습니다. 이 필드 이름은 이제 "리디렉션 URI"로 표시됩니다. "OAuth 양식 자격 증명 수집기 수정" "OAuth 공급자 구성 파일 수정"과 일치하도록 예제 OAuth 공급자와 응용 프로그램 이름이 수정되었습니다.
- [개방 형식 쿠키를 생성하는 웹 에이전트 응답 생성](#) (페이지 603) - SM_USERIPADDRESS 및 SM_USERSESSIONIP 필드에 대한 설명이 명확하게 수정되었습니다.
- [OAuth 인증 체계 구성](#) (페이지 421) - 인쇄 오류가 수정되었습니다. 이 수정 사항은 CQ170232 를 해결합니다.
- 더 이상 지원되지 않는 SAML 가맹 에이전트에 대한 섹션이 제거되었습니다.
- Oracle 8 은 더 이상 지원되지 않기 때문에 "Solaris 의 Oracle 8 에 대해 비동기 호출 구성" 항목이 제거되었습니다. CQ 177973 을 해결합니다.
- [암호 정책 만들기](#) (페이지 709) - 사용자가 암호 정책에서 잘못된 것으로 간주하는 암호를 입력하는 경우 사용자가 리디렉션되는 FCC 의 특정 URL 이 추가되었습니다. CQ 172044 를 해결합니다.

- [호스트 구성 개체 복사](#) (페이지 112) - 호스트 구성 개체 이름은 하이픈("-") 문자로 시작할 수 없음을 알려 주는 참고가 추가되었습니다. CQ 177096 을 해결합니다.
- [사용자 컨텍스트 변수를 처리할 때 다중 값 사용자 특성 결과를 지원하도록 구성](#) (페이지 644) - 사용자 컨텍스트 변수를 처리할 때 다중 값 사용자 특성 결과를 지원하도록 정책 서버를 구성하는 방법을 설명하는 항목이 추가되었습니다. CQ 177120 및 STAR 이슈 21316166-1 을 해결합니다.
- [가장에 대한 보안 고려 사항](#) (페이지 691) - 이전에 r12.03 에 제공되었지만 그 후로는 포함되지 않은 가장 관련 항목이 추가되었습니다. CQ 176089 및 STAR 이슈 21533517-01 을 해결합니다.
- [리스크 기반 인증을 위해 SecurID HTML 양식 인증 지원을 구성하는 방법](#) (페이지 387) - 리스크 기반 인증을 위한 SecurID HTML 양식 인증 지원을 설명하는 섹션이 추가되었습니다. CQ 174046 을 해결합니다.
- [보안 HTML 양식 인증 템플릿 사용](#) (페이지 304) - en-US 로캘의 보안 양식 관련 내용과 이러한 보안 양식의 사용 방법을 설명하는 내용이 수정되었습니다. CQ 173591 을 해결합니다.
- [FIPS 전용 환경에서 테스트 도구를 사용하는 방법](#) (페이지 762) - FIPS 전용 환경에서 테스트 도구를 사용하는 방법을 설명하는 항목이 추가되었습니다. CQ 154567 및 STAR 이슈 20890864-1 을 해결합니다.
- [가장 체계 사전 요구 사항](#) (페이지 436) - smauthimpersonate.dll(Windows) 및 smauthimpersonate(UNIX) 파일이 웹 에이전트에 설치된다는 설명이 정책 서버에 설치된다는 올바른 설명으로 업데이트되었습니다. CQ 172378 및 STAR 이슈 21467135-1 을 해결합니다.
- [OpenID 인증 체계 구성](#) (페이지 434) - 후처리 체인 필드를 수정하는 경우 정책 서버를 다시 시작해야 한다는 참고가 추가되었습니다. 이 수정 사항은 CQ 178990 을 해결합니다.
- [CA Directory 암호 정책 제어](#) (페이지 718) - 정책 서버가 CA Directory 암호 정책을 따르는 방식을 설명하는 새로운 섹션입니다. 이 수정 사항은 CQ 174815 를 해결합니다.

이 안내서의 두 번째 에디션에는 다음과 같은 변경된 사항이 포함되어 있습니다.

설명서에서만 변경된 내용

- "SiteMinder 개요" 창이 삭제되었습니다. 구성 요소에 대한 자세한 내용은 *SiteMinder 구현 안내서*를 참조하십시오. 각 정책 개체에 대한 개요 설명은 이 안내서의 각 단원을 참조하십시오.
- "정책 기반 보안 구현" 장이 삭제되었습니다. 환경 구현에 대한 자세한 내용은 *SiteMinder 구현 안내서*를 참조하십시오.
- [DeviceDNA™ 끝점을 사용하여 고급 세션 보증 만들기](#) (페이지 732) - 1 단계에서 메뉴 순서가 수정되었습니다. 이 수정 사항은 CQ 181072 를 해결합니다.
- 도메인 정보에 대한 설명이므로 "사용자 디렉터리" 절에서 다음 항목이 제거되었습니다.
 - LDAP 에 대한 일반 정보
 - LDAP 디렉터리의 사용자 명확성
 - LDAP 검색 필터
 - 디렉터리 토폴로지 및 LDAP 조회
 - 향상된 LDAP 조회 처리
- [EVALUATE 함수](#) (페이지 915) - Evaluate 함수의 구문을 수정하기 위해 "식 평가" 단원이 업데이트되었습니다. 설명서는 12.52 SP1 에서 업데이트되었습니다. 이 변경 사항은 CQ 179704 를 해결합니다.
- [CA SiteMinder® for Secure Proxy Server 사용](#) (페이지 17) - CA SiteMinder® for Secure Proxy Server 를 사용하여 관리 UI 를 보호하는 절차를 설명합니다. 설명서는 12.52 SP1 에서 업데이트되었습니다. 이 변경 사항은 CQ 182613 을 해결합니다.

목차

제 2 장: 관리 UI 시작

정책 서버는 사용자의 관리 권한에 따라 관리 UI 를 통해 관리됩니다.

- 오른쪽의 태스크 창을 사용할 때는 항상 왼쪽의 메뉴 창을 열거나 닫기 전에 또는 다른 곳으로 이동하기 전에 변경 내용을 저장하십시오.
- 관리 UI 를 사용하는 동안에는 브라우저의 "새로 고침" 또는 "뒤로" 단추를 사용하지 마십시오. 이러한 단추를 사용하면 양식이 다시 제출되고 상태가 무효화됩니다.

다음 단계를 수행하십시오.

1. 웹 브라우저를 엽니다.

- 관리 UI 를 독립 실행형 옵션으로 설치하고 SSL 을 통해 등록한 경우 다음 위치로 이동합니다.

`https://host.domain:8443/iam/siteminder/adminui`

참고: SSL 을 통해 등록된 관리 UI 를 처음 실행하면 브라우저에서 보안 인증서가 신뢰하는 회사에서 발급되지 않았음을 경고하는 메시지가 표시됩니다. 이 경고는 SSL 등록 중에 생성된 자체 서명된 인증서와 관련이 있습니다. 인증서를 승인하고 계속하십시오.

- 관리 UI 를 독립 실행형 옵션으로 설치하고 SSL 을 통해 등록하지 않은 경우 다음 위치로 이동합니다.

`http://host.domain:8080/iam/siteminder/adminui`

- 기존 응용 프로그램 서버 인프라에 관리 UI 를 설치한 경우 다음 위치 중 하나로 이동합니다.

`http://host.domain:port/iam/siteminder/adminui`

`https://host.domain:port/iam/siteminder/adminui`

host

관리 UI 호스트 시스템의 이름을 지정합니다.

domain

관리 UI 호스트 시스템의 정규화된 도메인 이름을 지정합니다.

port

응용 프로그램 서버가 요청을 수신 대기하는 포트를 지정합니다.

2. 관리자의 자격 증명을 입력합니다.
3. "로그인"을 클릭합니다.

이 창の内容은 관리 UI에 로그인하는 데 사용한 관리자 계정의 권한에 따라 달라집니다.

정책 서버 개체 관리

관리 UI를 사용하여 정책 서버 개체를 관리할 수 있습니다. 각 태스크를 수행하는 구체적인 방법은 개체마다 다르지만 전반적인 방법은 유사합니다. 예를 들어 에이전트를 삭제하는 절차는 응답을 삭제하는 절차와 유사합니다.

정책 서버 개체 복사

정책 서버 개체를 만드는 가장 쉬운 방법은 기존 개체를 복사하여 속성을 수정하는 것입니다. 기존 개체의 속성을 템플릿으로 사용하고 새 개체와 다른 정보만 수정할 수 있습니다. 일부 개체에는 복사 옵션을 사용할 수 없습니다.

참고: 관리 권한에 따라 액세스 가능한 개체가 결정됩니다.

다음 단계를 수행하십시오.

1. 복제할 개체가 포함된 하위 구성 요소 유형으로 이동합니다.
예: "인프라", "에이전트"를 차례로 클릭합니다.
2. 복제할 개체의 유형을 선택합니다.
예: 에이전트
3. "만들기"를 클릭합니다.
4. "Create a copy of an object"(개체의 복사본 만들기)를 선택하고 검색 조건을 지정한 다음 "검색"을 클릭합니다.

-
5. 목록에서 개체를 선택하고 "확인"을 클릭합니다.
 6. 새 이름과 설명을 입력합니다.
 7. 기존 개체의 속성과 다르게 새 개체의 속성을 수정하고 "제출"을 클릭합니다.
- 개체가 생성됩니다.

정책 서버 개체 속성 보기

정책 서버 개체의 속성을 볼 수 있습니다.

참고: 관리 권한에 따라 액세스 가능한 개체가 결정됩니다.

다음 단계를 수행하십시오.

1. 보려는 개체의 하위 구성 요소를 선택합니다.
예: "정책", "도메인"을 차례로 선택합니다.
2. 개체의 유형을 클릭합니다.
예: 도메인
3. 검색 조건을 지정하고 "검색"을 클릭합니다.
4. 보고자 하는 개체의 이름을 클릭합니다.
보기 화면이 나타나고 선택한 개체에 대한 정보가 표시됩니다.

기존 정책 서버 개체 수정

관리 UI 를 사용하면 기존 정책 서버 개체의 속성을 수정할 수 있습니다.

참고: 관리 권한에 따라 액세스 가능한 개체가 결정됩니다.

다음 단계를 수행하십시오.

1. 수정할 개체의 하위 구성 요소로 이동합니다.
예: "정책", "도메인"을 차례로 클릭합니다.
2. 수정할 개체를 클릭합니다.
예: 영역
3. 검색 조건을 지정하고 "검색"을 클릭합니다.

-
- 수정할 개체의 이름을 클릭합니다.
 - 페이지 아래쪽으로 스크롤하여 "수정"을 클릭합니다.
 - 필요한 사항을 변경하고 "제출"을 클릭합니다.
개체가 수정되었습니다.

정책 서버 개체 삭제

더 이상 필요 없는 정책 서버 개체를 삭제할 수 있습니다.

참고: 관리 권한에 따라 액세스 가능한 개체가 결정됩니다.

다음 단계를 수행하십시오.

- 삭제할 개체의 하위 구성 요소를 선택합니다.
예: "인프라", "인증"을 차례로 클릭합니다.
- 개체의 유형을 클릭합니다.
예: 인증 체계
- 검색 조건을 지정하고 "검색"을 클릭합니다.
- 삭제할 개체를 선택합니다.
- "삭제"를 클릭합니다.
- 개체의 삭제를 승인합니다.
정책 서버 개체가 삭제됩니다.

런타임 성능을 개선하기 위해 태스크 지속성 데이터베이스 관리

모든 관리 UI 태스크는 관리자가 제거하지 않으면 태스크 지속성 데이터베이스에 무기한 저장됩니다. 정리 태스크를 예약하여 데이터베이스에서 태스크를 제거하고 디스크 공간을 비울 수 있습니다. 정리 태스크를 사용하면 태스크 지속성 데이터베이스의 크기를 유지 관리하고 런타임 성능을 개선할 수 있습니다.

태스크 지속성 데이터베이스의 모든 태스크는 다음 상태 중 하나입니다.

- 감사 상태

감사 상태의 태스크는 관리 UI 에서 시작되었지만 제출되지 않은 태스크입니다. 예를 들어 보기 태스크는 관리 UI 에서 시작되었지만 제출되지는 않습니다.

- 제출된 상태

제출된 태스크는 관리 UI 에서 처리를 위해 제출되었지만 아직 완료되지 않은 태스크입니다.

- 완료된 상태

완료된 태스크는 제출되고 처리가 완료된 태스크입니다. 완료된 태스크는 다음과 같은 태스크를 포함합니다.

- 처리를 성공적으로 완료한 태스크
- 처리를 성공적으로 완료하지 못했지만 그럼에도 불구하고 완료된 태스크

감사 상태와 완료된 상태의 태스크는 정리 태스크를 통해 태스크 지속성 데이터베이스에서 제거할 수 있습니다. 정리 태스크는 제출되었지만 아직 보류 중인 태스크는 제거할 수 없습니다.

다음 두 옵션을 통해 정리 태스크를 예약, 수정 및 삭제할 수 있습니다.

제출된 태스크 정리

새 정리 태스크를 예약하거나 기존 정리 태스크를 수정하려면 이 옵션을 사용합니다.

되풀이 작업 삭제

예약된 정리 태스크를 삭제하려면 이 옵션을 사용합니다.

제출된 태스크 정리

완료 상태 및 감사 상태의 태스크를 데이터베이스에서 제거하는 정리 태스크를 구성합니다. 정리 태스크 자체에 대한 제한을 구성할 수도 있습니다.

참고: 시스템 관리자로 로그인한 경우에만 제출된 태스크를 정리하기 위한 예약된 작업을 실행할 수 있습니다.. 시스템 관리자 계정은 "관리 인증 구성" 옵션을 사용하여 정의합니다. 이 계정은 관리 UI의 최초 등록 중에 사용되며, 외부 관리자 저장소의 계정일 수 있습니다. 제출된 태스크 정리 기능은 슈퍼 사용자 권한을 지닌 관리자를 포함한 기타 다른 관리자가 사용할 수 없습니다.

다음 단계를 수행하십시오.

1. "관리", "관리 UI", "제출된 태스크 정리"를 차례로 클릭합니다.
2. 다음 옵션 단추 중 하나를 선택합니다.
 - 지금 실행
예약 단계를 건너뛰고 "제출된 태스크 정리" 창으로 바로 가려면 이 옵션을 선택하고 "다음"을 클릭합니다.
 - 새 작업 예약
 - 기존 작업 수정
3. "작업 이름" 필드에서 정리 태스크 이름을 지정하고 "예약" 섹션에서 예약 유형 및 예약 상세 정보를 지정합니다. "다음"을 클릭합니다.
4. 다음 필드를 작성하십시오.

최소 사용 기간

제거되어야 하는 완료된 태스크의 최소 사용 기간(월, 주, 일, 시간 또는 분)을 지정합니다.

참고: 태스크 사용 기간은 태스크가 완료된 시점부터 측정됩니다.

감사 만료

(선택 사항) 태스크를 감사 상태로 태스크 지속성 데이터베이스에 유지할 최대 기간(일)을 지정합니다.

제한: 1 이상

기본값: 1

시간 제한

(선택 사항) 정리 태스크에 대한 시간 제한(분)을 지정합니다.

작업 제한

(선택 사항) 정리 태스크에 대한 태스크 제한을 지정합니다.

5. "마침"을 클릭합니다.

처리를 위해 정리 태스크가 제출됩니다.

되풀이 작업 삭제

예약된 정리 태스크가 더 이상 필요하지 않으면 삭제할 수 있습니다.

다음 단계를 수행하십시오.

1. "관리", "관리 UI", "되풀이 태스크 삭제"를 차례로 클릭합니다.
2. 삭제되어야 하는 하나 이상의 예약된 정리 태스크를 선택합니다.
3. 제출을 클릭합니다.

처리를 위해 삭제 태스크가 제출됩니다.

웹 에이전트 및 정책 서버에서 시간이 계산되는 방식

정책 서버나 웹 서버가 설치된 각 시스템에서 해당 시스템의 지리적 위치에 맞는 표준 시간대로 시스템 클럭을 설정해야 합니다. 정책 서버와 웹 에이전트는 표준 시간대를 사용하여 GMT(그리니치 표준시)를 기준으로 시간을 계산합니다.

다음 그림에서는 정책 서버가 시간에 따라 정책을 실행하는 방식을 보여 줍니다. 리소스는 메사추세츠의 웹 서버에 저장되어 있으며 캘리포니아의 정책 서버에서 보호됩니다. 이 정책은 오전 9:00~오후 5:00 사이에 리소스에 대한 액세스를 허용합니다. 하지만 정책이 정책 서버의 표준 시간대인 PST(태평양 표준시)를 기준으로 하며 PST는 웹 에이전트의 표준 시간대인 EST(동부 표준시)보다 3 시간 늦기 때문에 메사추세츠의 사용자는 오후 6:00 에도 리소스에 액세스할 수 있습니다.

오후 3시 PST

정책 서버

GMT -8

오후 6시 EST

웹 에이전트/웹 서버

GMT -5



정책 서버에 따르면 오후 6시는 메사추세츠에서 오후 3시이므로 메사추세츠 사용자가 리소스에 액세스할 수 있음

참고: Windows 시스템의 경우 "날짜/시간" 제어판에 설정된 시간과 표준 시간대가 일치해야 합니다. 예를 들어 미국에서 시스템을 동부 표준시에서 태평양 표준시로 재설정하려면 시스템 클럭을 3 시간 전으로 설정하고 표준 시간대를 태평양 표준시로 변경해야 합니다. 이 두 설정이 일치하지 않으면 여러 도메인 간의 싱글 사인온과 에이전트 키 관리가 올바르게 작동하지 않습니다.

SiteMinder 로 관리 UI 보호

SiteMinder 로 관리 UI 를 보호하려면 에이전트가 리버스 프록시 서버에서 작동하도록 구성하고 외부 관리자 저장소를 구성해야 합니다. 응용 프로그램 서버에서 직접 관리 UI 에 액세스하지 않고 리버스 프록시 서버를 통해 관리 UI 에 액세스합니다.

다음 사항을 고려하십시오.

- 보호할 관리 UI 가 둘 이상인 경우 리버스 프록시 서버와 함께 작동하는 별도의 에이전트로 각 인스턴스를 보호하는 것이 좋습니다.
- 관리 UI 가 WebSphere 에 설치된 경우 응용 프로그램 서버 호스트 시스템에 최소 500 MB 의 가용 메모리가 있어야 SiteMinder 인증을 사용할 수 있습니다.

CA SiteMinder® for Secure Proxy Server 사용

CA SiteMinder® for Secure Proxy Server 를 사용하여 관리 UI 를 보호할 수 있습니다. SiteMinder 에이전트를 사용하여 CA SiteMinder® for Secure Proxy Server 를 구성하면 관리 UI 를 보호하기 위한 프록시 서버로서 기능합니다.

CA SiteMinder® for Secure Proxy Server 를 사용하여 관리 UI 를 보호하기 위한 사전 요구 사항

다음 사전 요구 사항을 고려하십시오.

- 정책 서버 및 정책 저장소가 구성되었습니다.
- 정책 서버에서 관리 UI 가 성공적으로 구성되었습니다.
- 게이트웨이(CA SiteMinder® for Secure Proxy Server)가 설치되고 정책 서버에 대해 구성되었습니다.
- (선택 사항) SSL 에 대해 구성된 관리 UI 를 보호하려면 CA SiteMinder® for Secure Proxy Server 와 함께 설치된 호스트에서 SSL 을 구성하십시오.

참고:

- 관리 UI 와 CA SiteMinder® for Secure Proxy Server 의 버전은 동일해야 합니다.
- SSL 에 대해 구성된 관리 UI 에 액세스하려면 https 요청을 사용하십시오.

CA SiteMinder® for Secure Proxy Server 구성

관리 UI 에 대한 프록시 서버로서 기능하도록 CA SiteMinder® for Secure Proxy Server 를 구성하십시오.

다음 단계를 수행하십시오.

1. 다음 위치에 있는 Proxy Rules.xml 파일을 다음 프록시 프록시 규칙을 사용하여 업데이트합니다.

```
<CA SiteMinder® for Secure Proxy Server install location>\proxy-engine\conf
<!-- Proxy Rules-->
<nete:proxyrules xmlns:nete="http://<관리 UI hostname:port>/">
<nete:cond criteria="beginswith" type="uri">
<nete:case value="/iam/siteminder/">
  <nete:forward>http(s)://<관리 UI hostname:port>$0</nete:forward>
</nete:case>
<nete:case value="/castylesr5.1.1/">
  <nete:forward>http(s):// <관리 UI hostname:port>$0</nete:forward>
</nete:case>
<nete:default>
<nete:forward>http://www.example.com$0</nete:forward>
</nete:default>
</nete:cond>
</nete:proxyrules>
```

2. 다음 위치에 있는 server.conf 파일의 "Default Virtual Host" 섹션을 다음 매개 변수를 사용하여 업데이트합니다.

```
<CA SiteMinder® for Secure Proxy Server install location>\proxy-engine\conf
■ enabledirectrewrite
■ redirectrewritablehostnames
```

3. 관리 UI 가 SSL 포트에서 실행 중인 경우 관리 UI 를 호스트하는 서버의 자체 서명된 인증서를 다운로드합니다. 브라우저의 임시 파일을 삭제한 후에 관리 UI 에 액세스하십시오.
4. 관리 UI 의 자체 서명된 인증서를 다음 위치에 있는 CA SiteMinder® SPS 의 인증 기관 파일에 넣으십시오.

```
<CA SiteMinder® for Secure Proxy Server 설치 위치>/SSL/certs
```

5. CA SiteMinder® for Secure Proxy Server 를 다시 시작합니다.

관리 UI 인증 활성화

기본 인증을 활성화하기 위해 관리 인증을 구성하고 관리 UI 를 보호하기 위해 CA SiteMinder® for Secure Proxy Server 를 에이전트로 선택할 수 있습니다.

다음 단계를 수행하십시오.

1. 리버스 프록시를 사용하여 에이전트를 통해 관리 UI 에 액세스합니다.

예:

`http://hostname.example.com:port/iam/siteminder`

Hostname

CA SiteMinder® for Secure Proxy Server 와 함께 설치된 호스트의 이름을 지정합니다.

Port

CA SiteMinder® for Secure Proxy Server 가 실행 중인 포트를 지정합니다.

2. 관리 UI 의 기본 로그인 자격 증명을 제공합니다.
3. 관리 인증을 구성할 때 관리 UI 를 보호하기 위한 에이전트로서 CA SiteMinder® for Secure Proxy Server 를 선택하십시오.

참고: 자세한 내용은 "LDAP 관리자 저장소 연결 구성" 및 "RDB 관리자 저장소 연결 구성"을 참조하십시오.

CA SiteMinder® for Secure Proxy Server 를 에이전트로 선택하면 SiteMinderDomain 이란 이름의 도메인과 관련 영역 및 규칙이 생성됩니다. 새로 생성된 도메인은 기본 로그인 페이지 대신 기본 인증을 사용하여 관리 UI 를 보호합니다.

SiteMinder 인증을 시행하기 위해 응용 프로그램 서버가 자동으로 재시작됩니다.

4. 구성된 사용자 디렉터리에 있는 사용자의 사용자 이름과 암호를 제공합니다.

중요! 사용자 디렉터리 연결을 구성할 때 생성된 **superuser** 의 자격 증명을 사용하십시오.

관리 UI 홈 페이지가 성공적으로 표시됩니다.

참고: 주소 표시줄의 URL 이 변경되지 않고 프록시 서버의 URL 이 표시됩니다.

HTML 양식 인증 체계 사용

기본 인증은 사용자의 자격 증명을 지정하기 위해 팝업 창을 표시합니다. 사용자 자격 증명을 지정하기 위해 로그인 페이지가 필요한 경우 HTML 양식 인증 체계를 사용하십시오.

관리 UI에 대한 인증을 활성화한 후에 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. 관리 폴더를 복사합니다.

출처:

<관리 UI 설치 위치>/siteminder/webagent-resource

대상:

Webagent/samples

2. HTML 양식 인증 체계를 만듭니다.

참고: 자세한 내용은 "HTML 양식 인증을 구성하는 방법"을 참조하십시오.

3. "Scheme Setup" 섹션에서 1 단계에서 복사한 관리 폴더에 있는 .fcc 파일의 위치를 "Target"에 지정합니다.

예:

/siteminderagent/admin/login.fcc

4. 새로 만든 HTML 양식 인증 체계를 SiteMinderDomain 도메인에 추가합니다.

5. 캐시를 새로 고칩니다.

6. 다음과 같이 URL을 사용하여 관리 UI에 액세스합니다.

http://hostname.example.com:port/iam/siteminder/adminui

7. 허가된 사용자의 사용자 이름과 암호를 입력합니다.

관리 UI 홈 페이지가 나타납니다. 관리 UI에 액세스할 때 주소 표시줄에 프록시 서버의 URL이 표시됩니다.

리버스 프록시 서버로 Apache 사용

CA SiteMinder?for Secure Proxy Server에 추가하여, SiteMinder로 관리 UI를 보호하기 위해 Apache 웹 서버를 리버스 프록시 서버로 사용할 수도 있습니다.

Apache 를 사용하여 SiteMinder 로 관리 UI 보호

Apache 웹 서버를 리버스 프록시 서버로 사용하여 SiteMinder 로 관리 UI 를 보호할 수 있습니다.

다음 단계를 수행하십시오.

1. 에이전트가 리버스 프록시 서버에서 작동하도록 구성합니다.

SiteMinder 웹 에이전트를 지원하는 Apache 와 같은 특정 유형의 웹 서버도 리버스 프록시 서버로 작동할 수 있습니다. 지원되는 서버는 지원표를 참조하십시오.

참고: Apache 웹 서버가 리버스 프록시 서버로 작동하도록 하려면 Apache 웹 서버의 구성 파일을 업데이트하십시오. 리버스 프록시 서버 구성 및 구성 파일 업데이트에 대한 자세한 내용은 웹 에이전트 구성 설명서를 참조하십시오.

중요! 프록시 서버에 대해 설정된 규칙에서 사용되는 URL 은 처음에 관리 UI 를 등록할 때 사용한 URL 과 동일해야 합니다.

예:

관리 UI 가 처음에 다음 URL 로 등록된 경우 프록시 서버 규칙에 동일한 URL 을 지정하십시오.

`http://host_name:8080/iam/siteminder/adminui`

2. ACO(에이전트 구성 개체)에서 LogOffUri 매개 변수의 값을 다음 예와 같이 설정합니다.

`/iam/siteminder/logout.jsp`

3. 외부 관리자 저장소를 구성합니다.

참고: 외부 관리자 저장소를 구성하면 응용 프로그램 서버가 자동으로 다시 시작됩니다. 다시 시작되면 관리 UI 가 SiteMinder 로 보호됩니다.

제 1 장: 설명서 변경 사항

4

제 2 장: 관리 UI 시작

9

정책 서버 개체 관리	10
정책 서버 개체 복사	10
정책 서버 개체 속성 보기	11
기존 정책 서버 개체 수정	11
정책 서버 개체 삭제	12
런타임 성능을 개선하기 위해 태스크 지속성 데이터베이스 관리	12

제출된 태스크 정리	13
되풀이 작업 삭제	15
웹 에이전트 및 정책 서버에서 시간이 계산되는 방식	15
SiteMinder 로 관리 UI 보호	17
CA SiteMinder® for Secure Proxy Server 사용	17
리버스 프록시 서버로 Apache 사용	20
관리 UI 에 SiteMinder 인증 사용 안 함	45

제 3 장: SiteMinder 관리자 47

SiteMinder 관리자 개요	47
기본 슈퍼 사용자 관리자	47
관리자 계정	48
레거시 관리자 계정	49
관리자 저장소 옵션	49
외부 관리자 저장소를 구성하는 방법	50
외부 관리자 저장소 고려 사항	51
SSL 고려 사항	53
디렉터리 서버 정보 수집	53
데이터베이스 정보 수집	54
JDBC 데이터 원본 배포	54
LDAP 관리자 저장소 연결 구성	57
RDB 관리자 저장소 연결 구성	59
레거시 관리자 권한 마이그레이션	60
외부 관리자 저장소 자격 증명 업데이트	62
외부 관리자 저장소 연결 수정	66
관리자를 만드는 방법	66
관리자 고려 사항	67
관리자 계정 만들기	67
관리자에게 올바른 권한이 있는지 확인	68
범위 지정 관리자를 만드는 방법	68
범위 지정 관리자 지침	69
작업 영역 만들기	70
관리자 만들기 및 작업 영역 할당	72
관리자의 범위가 지정되었는지 확인	73
관리자 사용 사례	74
슈퍼 사용자가 Manager 관리자를 생성하는 경우	75
슈퍼 사용자가 작업 영역을 생성하고 할당하여 Manager 관리자의 범위를 지정하는 경우	76
Manager 관리자가 Junior 관리자를 생성하는 경우	76
Junior 관리자가 작업 영역을 생성하고 할당하여 Junior 관리자의 범위를 추가로 지정하는 경우	77

레거시 관리자를 만드는 방법	78
레거시 관리자 고려 사항	78
레거시 관리자 기록 만들기	78
관리 UI 권한 위임	81
관리자 비활성화	81
레거시 관리자 비활성화	82
관리자 액세스 권한 복원	83
관리 UI에 대한 접근성 모드를 구성하는 방법	83
정책 서버 개체 변경	85
관리자 유형 선택	85
관리자에 대한 접근성 모드 구성	87

제 4 장: 사용자 세션 91

사용자 세션 개요	91
비영구 및 영구 쿠키	91
비영구 및 영구 세션	91
세션 티켓	92
SiteMinder에서 사용자 세션이 관리되는 방식	93
사용자 세션이 시작되는 방식	95
영역 간에 세션이 유지되는 방식	96
여러 쿠키 도메인 간에 세션이 유지되는 방식	96
사용자 세션의 유효성이 검사되는 방식	97
세션 정보가 위임되는 방식	97
세션 시간 만료	98
에이전트 키 관리 및 세션 시간 만료가 조정되는 방식	99
사용자 세션이 종료되는 방식	100
Windows 사용자 보안 컨텍스트	100
사용자 보안 컨텍스트에 대한 영구 세션이 관리되는 방식	101
세션 유효성이 다시 검사되는 방식	102
Windows 사용자 보안 컨텍스트 요구 사항	102

제 5 장: 에이전트 및 에이전트 그룹 107

웹 에이전트의 트러스트된 호스트	107
정책 서버에 트러스트된 호스트 등록	107
트러스트된 호스트 구성 설정	108
트러스트된 호스트 개체 삭제	111
트러스트된 호스트의 호스트 구성 개체	112
호스트 구성 개체 복사	112

호스트 구성 개체에 여러 정책 서버 추가.....	113
호스트 구성 개체에 맞게 정책 서버 클러스터 구성	115
SiteMinder 에이전트 개요	118
웹 에이전트.....	118
RADIUS 에이전트	120
응용 프로그램 서버 에이전트	120
WSS(Web Services Security) 에이전트.....	121
웹 에이전트 구성 개요	121
웹 에이전트 중앙 구성의 장점	122
웹 에이전트 구성 요소	122
웹 에이전트 관련 정책 서버 개체	123
웹 에이전트 구성 방법	124
중앙에서 웹 에이전트 구성	125
호스트 구성 개체 만들기	125
로컬에서 웹 에이전트 구성	126
중앙 구성 및 로컬 구성 사용 예	127
웹 에이전트 아이덴티티를 설정하기 위해 에이전트 개체 만들기	128
4.x 웹 에이전트 아이덴티티를 사용하도록 에이전트 개체 구성	129
에이전트 구성 개체 개요	130
에이전트 구성 개체 복사	131
에이전트 구성 개체 만들기	132
필수 에이전트 구성 개체 매개 변수	133
에이전트 구성 매개 변수 수정	135
웹 에이전트 사용	136
RADIUS 에이전트 구성	137
에이전트 그룹	138
에이전트 그룹 구성	139
에이전트 그룹에 에이전트 추가	140
사용자 지정 에이전트	140
사용자 지정 에이전트 유형 구성	141
에이전트 아이덴티티에 대한 사용자 지정 에이전트 개체 만들기	141
에이전트 검색	142
에이전트 인스턴스 목록	143
정책 서버 하트비트 간격 구성	144
에이전트 검색 비활성화.....	145

제 6 장: 사용자 디렉터리 147

사용자 디렉터리 연결 개요	148
LDAP 개요	148

ODBC 데이터베이스 개요.....	148
Active Directory 개요.....	149
사용자 지정 디렉터리 개요.....	150
디렉터리 특성 개요.....	150
CA Directory 사용자 디렉터리 연결을 구성하는 방법	152
사용자 저장소 시스템 ping	152
CA Directory 사용자 디렉터리 연결 구성	152
사용자 저장소 DSA 매개 변수 사용.....	153
CA Directory 사용자 저장소에 대해 캐싱이 사용되도록 설정	153
CA Directory 캐시 구성 확인.....	154
CA LDAP Server for z/OS 사용자 디렉터리 연결 구성 방법	155
CA LDAP Server for z/OS 개요.....	155
CA LDAP Server for z/OS(TSS)에서 지원하지 않는 SiteMinder 기능	156
CA Top Secret r12(TSS) 백엔드 보안 옵션	157
CA LDAP Server r15 for z/OS(ACF2) 백엔드 보안 옵션	161
CA LDAP Server r15 for z/OS(RACF) 백엔드 보안 옵션.....	164
RACF 에 대한 정책 서버 레지스트리 항목 구성	165
정책 서버에서 CA LDAP Server for z/OS 로의 연결 구성	166
Oracle Directory Server Enterprise Edition 사용자 디렉터리 연결을 구성하는 방법	167
사용자 저장소 시스템 ping	167
Oracle Directory Server Enterprise Edition 사용자 디렉터리 연결 구성	167
IBM Directory Server 사용자 디렉터리 연결을 구성하는 방법	168
사용자 저장소 시스템 ping	168
IBM Directory Server 사용자 디렉터리 연결 구성.....	169
Domino 사용자 디렉터리를 사용자 저장소로 구성하는 방법	169
Domino 사용자 디렉터리가 정책 서버 요구 사항을 충족하는지 확인	170
사용자 저장소 시스템 ping	170
Domino Directory 연결 구성	170
Novell eDirectory LDAP 디렉터리 연결을 구성하는 방법	171
NetWare 구성	172
Novell eDirectory 에 익명 LDAP 액세스 구성.....	173
SiteMinder 관리를 위한 특수 액세스 권한	174
SiteMinder 관리에 사용할 Novell eDirectory 사용자 계정 만들기	175
사용자 저장소 시스템 ping	175
Novell eDirectory LDAP 디렉터리 연결 구성.....	176
Active Directory LDS 사용자 디렉터리 연결 구성 방법	176
사용자 저장소 시스템 ping	177
Active Directory LDS 사용자 저장소 디렉터리 연결 구성	177
Active Directory 사용자 저장소 연결을 구성하는 방법.....	178
사전 요구 사항.....	179

AD 네임스페이스 및 LDAP 네임스페이스 정보 검토	180
사용자 저장소 정보 수집	182
네이티브 설정으로 비활성화된 권한 없는 사용자에게 대해 암호 서비스 리디렉션이 사용되지 않도록 설정	183
개선된 Active Directory 통합 기능이 사용되도록 설정	184
사용자 저장소 연결 만들기	184
EnableADEnhancedReferrals 레지스트리 키 비활성화	186
SASL 바인드 레지스트리 키 활성화	187
사용자 저장소 연결 테스트	188
Active Directory 글로벌 카탈로그 사용자 디렉터리 연결을 구성하는 방법	188
사용자 저장소 시스템 ping	188
Active Directory 글로벌 카탈로그 디렉터리 연결 구성	189
Oracle Internet Directory 사용자 디렉터리 연결을 구성하는 방법	190
Oracle Internet Directory 사용자 디렉터리에 대한 LDAP 조회 제한	190
사용자 저장소 시스템 ping	190
OID 디렉터리에 대한 조직 단위 만들기	190
Oracle Internet Directory 연결 구성	191
OpenLDAP 서버 사용자 디렉터리 연결을 구성하는 방법	192
사용자 저장소 만들기	192
OpenLDAP Directory Server 사용자 디렉터리 연결 구성	192
Red Hat Directory Server 사용자 디렉터리 연결을 구성하는 방법	193
사용자 저장소 시스템 ping	193
Red Hat Directory Server 사용자 디렉터리 연결 구성	194
ODBC 사용자 디렉터리 연결을 구성하는 방법	194
사용자 저장소 시스템 ping	195
ODBC 디렉터리 연결 구성	195
SQL Server 사용자 저장소에서 대/소문자 비구분 및 불필요한 후행 공백이 있는 암호와 관련된 문제	196
사용자 지정 사용자 디렉터리 연결을 구성하는 방법	200
사용자 저장소 시스템 ping	201
사용자 지정 디렉터리 연결 구성	201
SSL 을 통한 LDAP 사용자 디렉터리 연결 구성 방법	202
SSL 을 통한 연결 구성 전 작업	202
인증서 데이터베이스 파일 만들기	203
인증서 데이터베이스에 루트 인증 기관 추가	204
인증서 데이터베이스에 서버 인증서 추가	206
인증서 데이터베이스의 인증서 목록 표시	208
사용자 디렉터리 연결에 대해 SSL 구성	209
정책 서버를 인증서 데이터베이스에 연결	209
SSL 연결 확인	210

SSL 을 통한 Oracle 사용자 디렉터리 연결 구성	210
정책 서버가 SSL 을 통해 Oracle 데이터베이스에 연결하는 방식	210
LDAP 부하 분산 및 장애 조치	213
포트 번호 고려 사항	214
장애 조치 구성	214
부하 분산 구성	215
부하 분산 및 장애 조치 구성	215
사용 사례 - 부하 분산 및 장애 조치	216
ODBC 데이터 원본 장애 조치 구성	217
SQL 쿼리 체계	218
SQL 쿼리 체계 구성	218
ODBC 사용자 디렉터리 연결에 SQL 쿼리 체계 추가	219
저장 프로시저를 사용한 인증을 위해 SQL 쿼리 체계 구성	220
장애 조치 및 연결 풀링 중 비동기 호출 지원	222
여러 정책 저장소에 동일한 사용자 디렉터리 연결 정의	224
사용자 디렉터리 콘텐츠 보기	225
사용자 디렉터리 검색	226
유니버설 ID	226
SiteMinder 에서 UID 가 사용되는 방식	227
명명된 식	227
명명된 식의 이점	229
명명된 식 정의	229
사용자 특성 매핑	244
사용자 특성 매핑 개요	245
특성 매핑의 작동 방식	246
특성 매핑 정의	248
고급 사용자 특성 매핑 예	264

제 7 장: 디렉터리 매핑 271

디렉터리 매핑 개요	271
권한 부여 및 유효성 검사 아이덴티티 매핑	273
아이덴티티 매핑 구성	273
아이덴티티 매핑에서 지원되는 디렉터리	274
아이덴티티 매핑 항목 유형	274
복잡한 사용자 검색 식 사용	275
권한 부여 아이덴티티 매핑을 구성하는 방법	276
유효성 검사 아이덴티티 매핑을 구성하는 방법	277
기본 전역 유효성 검사 디렉터리 매핑 구성	279
레거시 디렉터리 매핑 구성	280

인증 및 권한 부여 디렉터리 매핑을 구성하는 방법	280
AuthValidate 디렉터리 매핑을 구성하는 방법	282
영역에서 디렉터리 매핑 제거	283
디렉터리 매핑 예	283
Engineering 영역 리소스에 대한 직원 액세스	284
Quality Assurance 영역 리소스에 대한 임시 직원 액세스	284
유니버설 ID 기준 디렉터리 매핑	285
디렉터리 매핑 대/소문자 구분	285
복잡한 사용자 검색 조건을 사용한 아이덴티티 매핑	286
디렉터리 매핑 및 응답	286

제 8 장: 인증 체계 287

인증 체계 개요	287
지원되는 인증 체계 및 암호 정책	288
인증 중 정책 서버 검색을 단일 사용자 저장소로 제한	289
인증 체계 처리	290
인증 컨텍스트 데이터 유지	292
보호 수준	292
인증 체계 및 자격 증명 요구 사항	293
단일 인증 체계 구성의 여러 인스턴스	295
기본 인증 체계를 구성하는 방법	295
기본 체계 사전 요구 사항 검토	296
기본 인증 체계 구성	297
SSL 을 통한 기본 인증 체계를 구성하는 방법	297
SSL 을 통한 기본 인증 체계 사전 요구 사항 확인	298
SSL 을 통한 기본 인증 체계 구성	298
HTML 양식 인증을 구성하는 방법	300
에이전트 소유자에게 HTML 양식 인증이 필요하다고 알림	303
HTML 양식 인증 템플릿 파일 구성	303
HTML 양식 인증 체계 구성	314
FCC 국제화를 활성화하는 방법	317
Windows 인증 체계	331
Windows 인증 사전 요구 사항을 충족하는지 확인	332
Windows 인증 체계 구성	333
Kerberos 인증을 구성하는 방법	335
도메인 컨트롤러에서 Kerberos 인증 구성	335
정책 서버에서 Kerberos 인증 구성	342
웹 서버에서 Kerberos 인증 구성	345
Windows 워크스테이션에서 Kerberos 인증 구성	345

Kerberos 인증 체계 구성	346
Windows 호스트에서 Kerberos 외부 영역 구성.....	347
SiteMinder Kerberos 인증 문제 해결.....	348
정보 카드 인증 체계	351
아이덴티티 선택기 소개	352
SiteMinder ICAS(정보 카드 인증 체계).....	352
RADIUS CHAP/PAP 인증 체계	372
PAP 개요	372
CHAP 개요.....	372
RADIUS CHAP/PAP 체계 개요.....	373
RADIUS CHAP/PAP 체계 사전 요구 사항.....	373
RADIUS CHAP/PAP 인증 체계 구성	373
RADIUS 서버 인증 체계	374
RADIUS 서버 체계 사전 요구 사항	374
RADIUS 서버 인증 체계 구성	375
SafeWord 서버 인증 체계	375
SafeWord 서버 체계 사전 요구 사항	376
SafeWord 서버 인증 체계 구성	376
SafeWord 서버 및 HTML 양식 인증 체계	377
SafeWord 서버 및 HTML 양식 체계 사전 요구 사항	377
SafeWord 서버 및 HTML 양식 인증 체계 구성	378
SecurID 인증 체계.....	378
SecurID 기본 인증 체계를 구성하는 방법	382
SecurID HTML 양식 인증 체계를 구성하는 방법.....	384
SecurID 사용자의 재활성화 및 확인을 위한 SecurID HTML 양식 지원.....	385
새 사용자 계정의 활성화를 위한 SecurID HTML 양식 지원	386
리스크 기반 인증을 위해 SecurID HTML 양식 인증 지원을 구성하는 방법	387
X.509 클라이언트 인증서 인증 체계	389
인증서 인증을 위한 인증서 추출	390
SiteMinder 가 인증서 데이터를 사용하여 사용자를 식별하는 방식	391
X.509 클라이언트 인증 체계 사전 요구 사항	391
X.509 인증서 인증 체계 구성	392
X.509 클라이언트 인증서 및 기본 인증 체계.....	393
X.509 클라이언트 인증서 및 기본 체계 사전 요구 사항.....	393
X.509 인증서 및 기본 인증 체계 구성	394
X.509 인증서 또는 기본 인증 체계	395
X.509 클라이언트 인증서 또는 기본 체계 사전 요구 사항.....	396
X.509 인증서 또는 기본 인증 체계 구성	397
X.509 클라이언트 인증서 및 HTML 양식 인증 체계	398
X.509 클라이언트 인증서 및 HTML 양식 체계 사전 요구 사항	399

에이전트 API 지원	400
X.509 인증서 및 HTML 양식 인증 체계 구성	400
X.509 클라이언트 인증서 또는 HTML 양식 인증 체계	401
X.509 클라이언트 인증서 또는 HTML 양식 체계 사전 요구 사항	402
에이전트 API 지원	403
X.509 인증서 또는 HTML 양식 인증 체계 구성	403
익명 인증 체계	404
익명 체계 사전 요구 사항	405
익명 인증 체계 구성	405
사용자 지정 인증 체계	406
사용자 지정 체계 사전 요구 사항	407
사용자 지정 인증 체계 구성	407
OAuth 인증 체계를 구성하는 방법	408
OAuth 인증 프로세스	410
응용 프로그램을 OAuth 공급자에 등록합니다.....	411
OAuth 플러그인이 사용되도록 설정.....	413
OAuth 양식 자격 증명 수집기 수정.....	414
OAuth 공급자 구성 파일 수정.....	416
에이전트에서 FCCCompatMode 비활성화.....	421
OAuth 인증 체계 구성.....	421
OpenID 인증 체계.....	422
SiteMinder 에서 OpenID 인증이 작동하는 방식	423
OpenID 인증 체계를 구성하는 방법	424
레거시 페더레이션 인증 체계	435
가장 인증 체계	435
가장 체계 사전 요구 사항	436
가장 인증 체계 구성	436

제 9 장: X.509 인증서에 대한 인증서 매핑 및 유효성 검사 439

X.509 클라이언트 인증서 인증 체계에 대한 인증서 매핑	439
인증서 매핑 구성	439
인증서 매핑 테스트.....	441
사용자 지정 매핑 식.....	442
동일한 유형의 여러 특성에 대한 사용자 지정 인증서 매핑	446
X.509 클라이언트 인증서 인증을 위한 인증서 신뢰성 검사.....	447
유효성 검사를 구현하기 위한 사전 요구 사항.....	448
인증서 해지 목록 검사.....	448
OCSP(온라인 인증서 상태 프로토콜) 검사	456
OCSP 와 CRL 간의 장애 조치.....	469

인증서 유효성 검사 문제 해결	473

제 10 장: 강력한 인증 475

자격 증명 선택기 소개	475
자격 증명 선택기 사용 사례	476
암호 및/또는 인증서 인증을 사용한 액세스 요청	477
Windows 인증을 사용한 액세스 요청	478
SecurID 인증을 사용한 액세스 요청	478
SafeWord 인증을 사용한 액세스 요청	478
사용 사례에 대한 자격 증명 선택기 솔루션	479
프런트엔드 인증 체계 설정	479
FCC(양식 자격 증명 수집기) 사용	480
프런트엔드 인증을 위한 selectlogin.fcc 파일 구성	481
프런트엔드 인증 체계 구성	487
성공하지 못한 인증 시도 관리	489
백엔드 처리 설정	490
백엔드 처리를 위한 인증 체계 설정	490
백엔드 처리를 위한 정책 도메인 설정	490
백엔드 정책 도메인에 대한 영역 구성	491
백엔드 정책 도메인에 대한 규칙 만들기	492
백엔드 정책 도메인에 대한 AuthContext 응답 구성	493
백엔드 자격 증명 선택에 대한 정책 구성	495
샘플 응용 프로그램 보호	497
샘플 응용 프로그램의 영역 및 규칙	498
샘플 응용 프로그램을 보호하도록 정책 구성	501
샘플 응용 프로그램에 대한 응답 구성	502
자격 증명 선택기 솔루션 테스트	503

제 11 장: 응용 프로그램 개체에서 웹 응용 프로그램에 대한 보안 정책 정의 505

응용 프로그램 개체를 사용한 리소스 보안의 장점	505
응용 프로그램 개체에서 웹 응용 프로그램에 대한 보안 정책을 정의하는 방법	506
관리 권한 확인	508
응용 프로그램 개체 생성 및 보안 정책의 일반 속성 정의	508
응용 프로그램 리소스 지정	510
보호된 리소스에 액세스할 수 있는 사용자를 식별하는 역할 생성	511
(선택 사항) 웹 응용 프로그램을 사용자 지정하도록 응답 구성	511
(선택 사항) 웹 응용 프로그램을 사용자 지정하도록 응답 그룹 구성	512

리소스를 사용자 역할과 연결하도록 정책 구성.....	513
(선택 사항) 고급 응용 프로그램 옵션 구성	514
응용 프로그램 개체를 사용하여 응용 프로그램 보안 정책을 정의하기 위한 사용 사례.....	518
웹 포털 보호를 위한 응용 프로그램 보안 정책.....	518
역할 기반 응용 프로그램 보안 정책	523
사용자 매핑 및 명명된 식을 사용한 응용 프로그램 보안 정책	531
CA DataMinder 콘텐츠 분류 기반 응용 프로그램 보안 정책	541

제 12 장: 도메인 547

정책 도메인 개요.....	547
도메인 및 사용자 구성원	549
정책 도메인을 구성하는 방법	549
정책 도메인 구성	550
사용자 디렉터리 할당	550
영역 생성.....	551
도메인에 CA Identity Manager 환경 추가.....	553
도메인에 대한 전역 정책 처리가 사용되지 않도록 설정	554
도메인 수정	554
도메인 삭제	554

제 13 장: 영역 555

영역 개요.....	555
신뢰 수준 소개	556
에이전트, 영역 및 규칙별로 리소스 식별.....	557
보호되지 않은 영역, 규칙 및 정책	558
중첩된 영역	559
요청 처리에서의 영역	561
예	561
영역 구성	561
SiteMinder 웹 에이전트로 보호되는 영역 구성.....	562
RADIUS 에이전트로 보호되는 영역 구성	563
영역 수정	564
영역 삭제	564
중첩된 영역 구성	564
리소스 캐시에서 단일 영역 플러시	565

제 14 장: 규칙 567

규칙 개요.....	567

규칙이 정책의 일부로 작동하는 방식	568
정책 서버가 규칙을 처리하는 방식	569
규칙 및 중첩된 영역	570
규칙 작업	570
고급 규칙 옵션	574
웹 에이전트 작업을 위한 규칙 구성	575
인증 이벤트 작업을 위한 규칙 구성	576
권한 부여 이벤트 작업을 위한 규칙 구성	577
OnAccessReject 규칙에 대한 정책 고려 사항	578
가장 이벤트 작업을 위한 규칙 구성	579
리소스 일치 및 정규식	579
표준 리소스 일치	580
리소스 일치를 위한 정규식	580
규칙을 사용하거나 사용하지 않도록 설정	581
고급 규칙 옵션	582
규칙에 시간 제한 추가	582
활성 규칙 구성	583
규칙 삭제	584

제 15 장: 규칙 그룹 585

규칙 그룹 개요	585
규칙 그룹 만들기	586
규칙을 규칙 그룹에 추가	587
규칙 그룹 수정	587
규칙 그룹 삭제	588

제 16 장: 응답 및 응답 그룹 589

응답	589
응답 유형	590
응답 특성	590
응답 및 디렉터리 매핑	592
응답 구성	592
응답 특성 구성	592
응답의 변수 개체 사용	596
응답 특성 캐싱 구성	599
응답 편집	600
응답 삭제	600
개방 형식 쿠키를 생성하는 웹 에이전트 응답을 생성하는 방법	601

정책 서버 개체 변경	602
개방 형식 쿠키를 생성하는 웹 에이전트 응답 생성	603
규칙에 웹 에이전트 응답 추가	608
정책에 규칙 추가	609
샘플을 참조하여 응용 프로그램 사용자 지정	610
SiteMinder 생성 사용자 특성	610
SiteMinder 생성 응답 특성의 사용 여부	616
응답 그룹	617
응답 그룹 구성	618
응답 그룹에 응답 추가	619
응답 그룹 수정	619
응답 그룹 삭제	620

제 17 장: 정책 621

정책 개요	621
정책 바인딩	623
정책의 식	623
정책에서 신뢰 수준 구성	624
정책을 구성하는 방법	625
정책 생성	625
정책에 사용자 추가	627
정책에 규칙 추가	627

제 18 장: 변수 629

eTelligent 규칙	629
eTelligent 규칙에 대한 구성 요소 요구 사항	629
eTelligent 규칙의 이점	630
eTelligent 규칙을 구성하는 방법	630
eTelligent 규칙 속성 파일	631
변수 개요	634
변수 유형	634
정책에 변수 사용	636
응답에 변수 사용	636
웹 서비스 변수	637
웹 서비스 변수에 대한 구성 요소 요구 사항	639
웹 서비스 변수를 확인할 때의 보안 요구 사항	639
웹 서비스 변수 확인자 구성	640
샘플 WebServiceConfig.properties 구성 파일	640

인증 기관 및 웹 서비스 변수	641
변수 만들기	641
정적 변수 만들기	641
요청 컨텍스트 변수 만들기	642
사용자 컨텍스트 변수 만들기	643
사용자 컨텍스트 변수를 처리할 때 다중 값 사용자 특성 결과를 지원하도록 구성	644
양식 Post 변수 만들기	645
웹 서비스 변수 만들기	646

제 19 장: 키 및 인증서 관리 649

인증서 및 개인 키 사용	649
서명 및 확인 작업	651
암호화/암호 해독 작업	651
SSL 연결에 대한 인증서	652
아티팩트 백 채널에 보안을 적용하기 위한 인증서	652
인증서 데이터 저장소에서 지원하는 형식	654
트러스트된 인증서 및 키/인증서 쌍 가져오기	654
기존 파일에서 키/인증서 쌍 가져오기	655
키 및 인증서 쌍을 생성하는 방법	656
새 인증서 서명 요청 생성	658
인증서 데이터 저장소에서 인증서 업데이트	659
인증서 및 키 데이터 내보내기	660
인증 기관(CA) 인증서 사용	661
CA 인증서 가져오기	661
CRLs 를 사용하여 인증서 유효성 확인	662
인증서 관리를 위한 CRL 추가	663
CRL 업데이트	664
OCSP 를 사용하여 인증서 유효성 확인	664
OCSP 및 CRL 검사 간 장애 조치	665

제 20 장: 전역 정책, 규칙 및 응답 667

전역 정책	667
전역 정책 개체 특성	668
SiteMinder 전역 정책 개념	670
전역 정책 처리	671
전역 정책을 구성하는 방법	672
전역 규칙	672
전역 응답 개체	678

전역 응답에 대한 응답 특성	679
전역 정책 개체를 구성하는 방법	680
전역 정책을 사용하거나 사용하지 않도록 설정	682
전역 활성화 정책 구성	682
전역 정책에 사용할 수 있는 IP 주소	683
전역 정책에 대한 단일 IP 주소 지정	683
전역 정책에 대한 호스트 이름 추가	684
전역 정책에 대한 서브넷 마스크 추가	684
전역 정책에 대한 IP 주소 범위 추가	685
전역 정책 시간 제한 추가 및 제거	685

제 21 장: 가장 687

가장 세션이 시작되는 방법	688
가장에 대한 보안 고려 사항	691
인증 체계 보호 수준의 효과	691
세션 유효 시간 만료	692
가장 제한	692
가장 영역 및 이벤트	692
가장 구성	693
startimp.fcc 를 사용하도록 에이전트 구성	694
가장 인증 체계 구성	694
.fcc 파일을 통한 가장 활성화	695
가장 이벤트 구성	699
가장에 대한 정책 구성	699
다중 쿠키 도메인 지원	701
가장의 샘플 구현	701
샘플 가장 구현 평가	703
가장 프로세스를 시작하기 위한 양식	703

제 22 장: 암호 정책 707

암호 서비스 개요	707
암호 정책을 구성하는 방법	708
암호 정책 고려 사항	708
암호 정책 만들기	709
암호 만료 구성	710
암호 조합 구성	711
암호 정규식	712
암호 제한 구성	715

고급 암호 옵션 구성	716
암호 서비스를 위해 리디렉션 시 로그인 ID 제거	716
CA Directory 암호 정책 제어	718
사용자가 직접 암호 변경	718
암호 변경 링크 추가	719
암호 직접 변경	719
암호 변경 허용 오류 메시지	719
암호 정책 문제 해결	720
새 사용자 암호가 거부됨	720
사용자 계정이 잘못 비활성화됨	721
사용자 계정이 중간에 비활성화됨	721
암호 변경이 강제 적용됨	721
LDAP 사용자가 비활성화되지 않음	722
Active Directory 사용자가 암호를 변경할 수 없음	722
암호가 올바르지 않다는 메시지가 표시되지 않음	723

제 23 장: DeviceDNA™를 사용한 고급 세션 보증 725

DeviceDNA™를 사용한 고급 세션 보증 구성 방법	725
DeviceDNA™를 사용한 고급 세션 보증 제한 사항	728
DeviceDNA™를 사용한 고급 세션 보증을 위한 CA SiteMinder® for Secure Proxy Server 환경 구성	730
DeviceDNA™를 사용한 고급 세션 보증을 위한 SiteMinder 환경 구성	731
DeviceDNA™를 사용한 고급 세션 보증 끝점 만들기	732
영역에 끝점 추가	734
응용 프로그램 구성 요소에 끝점 추가	735
파트너 관계에서 DeviceDNA™를 사용한 고급 세션 보증 활성화	736
SM--Related 로그 파일	737
업그레이드 중 DeviceDNA™를 사용한 고급 세션 보증 구성 방법	737
DeviceDNA™를 사용한 고급 세션 보증 제한 사항	740
Windows 정책 서버 중지	742
UNIX 정책 서버 중지	743
감사 저장소 업그레이드 스크립트	743
Windows 정책 서버 시작	749
UNIX 정책 서버 시작	750
DeviceDNA™를 사용한 고급 세션 보증을 위한 CA SiteMinder® for Secure Proxy Server 환경 구성	751
DeviceDNA™를 사용한 고급 세션 보증을 위한 SiteMinder 환경 구성	752
DeviceDNA™를 사용한 고급 세션 보증 끝점 만들기	753
영역에 끝점 추가	755
응용 프로그램 구성 요소에 끝점 추가	756
파트너 관계에서 DeviceDNA™를 사용한 고급 세션 보증 활성화	757

SM--Related 로그 파일	758

제 24 장: SiteMinder 테스트 도구 759

테스트 도구 개요	759
테스트 환경 에이전트 구성	760
Windows 에서 테스트 도구 시작	761
UNIX 에서 테스트 도구 시작	762
FIPS 전용 환경에서 테스트 도구를 사용하는 방법	762
정책 서버 식별	766
테스트 모드 선택	768
리소스 정보 지정	768
사용자 자격 증명 지정	769
인코딩 사양 설정	769
테스트 도구 설정 파일에 테스트 구성 저장 및 로드	770
(선택 사항) 정책 서버에 대한 테스트 도구 연결 조정	771
기능 테스트 실행	772
(선택 사항) 재발 및 스트레스 테스트를 위해 명령 스크립트 파일에 테스트 기록	774
기능 테스트 결과	775
평균 경과 시간 계산	777
명령 스크립트 파일에 기록된 테스트를 재생하여 재발 테스트 수행	777
스트레스 테스트 실행	778
스레드 제어 파일 구성	778
"고급 재생" 모드에서 스레드 제어 파일을 실행하여 스트레스 테스트 수행	781
(선택 사항) 테스트에서 사용자 이름이 처리되는 방식 구성	782
(선택 사항) 안정적 로드를 시뮬레이트하기 위해 정책 서버 요청 간 대기 시간 구성	783
(선택 사항) 재생 테스트 결과를 CSV 형식의 파일에 기록하도록 테스트 도구 구성	783
보고서 보기	783
인증서 기반 인증 테스트	785
사용자 지정 매핑이 필요한 인증서 특성	785
테스트를 위한 사용자 지정 특성 매핑	786

제 25 장: 에이전트 구성 문제 해결 789

영어가 아닌 입력 문자에 정크 문자가 포함됨	789
고급 인증 서버의 오류 메시지	789
"토큰이 없습니다." 오류	790

부록 A: SSL 인증 체계 문제 해결 791

개요	791

SSL 연결 기능 확인.....	791
SSL 구성	792
Netscape 에서 웹 서버가 클라이언트 인증서를 트러스트하도록 설정	792
Windows 에서 웹 서버가 클라이언트 인증서를 트러스트하도록 설정	794
Apache 에서 웹 서버가 클라이언트 인증서를 트러스트하도록 설정	795
SSL 문제 해결.....	796
인증서에 대한 메시지가 표시되지 않음	796
이전 절차를 수행한 후에도 인증서 메시지가 표시되지 않음	796
인증서 메시지가 표시된 후 인증 실패 메시지가 표시됨	799
SiteMinder 정책이 액세스를 허용해야 하는데 SSL 인증 실패 메시지가 표시됨	800
구성 요소를 찾을 수 없다는 오류 메시지가 표시됨	800
인증서 또는 기본 인증을 실행 중인데 기본 자격 증명을 입력할 수 없음	801

부록 B: LanMan 사용자 디렉터리 803

LanMan 사용자 디렉터리 정보	803
LanMan 디렉터리 연결 사전 요구 사항	804
LanMan 디렉터리 연결 구성	804
LanMan 디렉터리 연결에 대한 레지스트리 키 구성	805
LanMan 사용자 디렉터리 연결 구성	806
Windows 사용자 디렉터리에 대한 장애 조치	806
LanMan 사용자 디렉터리 검색 조건	806

부록 C: CA SSO/WAC 통합 807

CA SSO/WAC 통합 개요	807
SiteMinder 및 CA SSO 통합 아키텍처 예	808
사용자가 CA SSO 로 보호된 리소스보다 SiteMinder 로 보호된 리소스에 먼저 액세스하는 경우	809
인증된 CA SSO 클라이언트 사용자가 SiteMinder 리소스에 액세스하는 경우	811
사용자가 SiteMinder 로 보호된 리소스보다 eTrust WAC 로 보호된 리소스에 먼저 액세스하는 경우	813
SiteMinder 및 CA SSO 통합 사전 요구 사항	814
SiteMinder 에서 CA SSO 로의 싱글 사인온 구성	815
CA SSO 클라이언트에서 SiteMinder 로의 싱글 사인온 구성	817
CA SSO 에서 SiteMinder 로의 싱글 사인온 구성	818
smetssockie 웹 에이전트 활성 응답 특성 구성	821
smauthetssso 사용자 지정 인증 체계 구성	822

부록 D: 정책 서버를 RADIUS 서버로 사용

정책 서버를 Radius 서버로 사용.....	827
RADIUS 클라이언트/서버 아키텍처	828
정책 서버에서 RADIUS 인증이 작동하는 방식	828
RADIUS 환경의 정책.....	830
RADIUS 및 비 RADIUS 리소스 비교.....	832
영역 힌트 사용.....	833
RADIUS 정책 도메인의 응답.....	835
응답 작동 방식.....	835
특성 유형.....	836
항상 RADIUS 특성을 반환하도록 SiteMinder 구성	839
에이전트 유형에 대한 특성 만들기	839
RADIUS 환경에서 SiteMinder 배포.....	844
RADIUS 장치를 보호하기 위한 지침	845
동종 RADIUS 환경에서 사용자를 인증하는 방법	845
사용자 디렉터리 설정	846
정책 도메인 설정	847
인증 체계 만들기.....	847
사용자 디렉터리가 한 개인 이중 RADIUS 환경에서 사용자 인증	848
단일 디렉터리를 사용하는 이중 환경에서 사용자가 인증되는 방식	848
시스템 및 정책 도메인 구성	850
단일 디렉터리를 사용하는 이중 환경에 대한 에이전트 정의	851
사용자 디렉터리 구성	851
정책 도메인 만들기	851
사용자 디렉터리가 두 개인 이중 RADIUS 환경에서 사용자를 인증하는 방법	852
시스템 및 정책 도메인을 구성하는 방법	854
두 개의 디렉터리를 사용하는 이중 환경에 대한 에이전트 정의	855
사용자 디렉터리 설정	855
두 개의 정책 도메인 만들기	856
RADIUS 에이전트 그룹 개요.....	856
RADIUS 에이전트 그룹 설정.....	857
RADIUS 응답 그룹화.....	858
RADIUS 문제 해결 및 테스트	859
계정 설정 및 디버깅을 위한 RADIUS 로그 생성	859
Smreadclog 를 사용하여 RADIUS 로그 파일 읽기	860
SiteMinder 테스트 도구를 사용하여 테스트하는 방법.....	861

부록 E: 특성 및 식 참조

863

데이터 형식	863
식 구문 개요	866
붙여넣기	868
연산자	870
같음 연산자	871
같지 않음 연산자	872
보다 작음 연산자	872
보다 큼 연산자	873
작거나 같음 연산자	874
크거나 같음 연산자	875
시작 문자 연산자	875
끝 문자 연산자	876
포함 연산자	876
집합 포함 연산자	877
패턴 일치 연산자	877
교집합 연산자	882
합집합 연산자	882
NOT 연산자	883
AND 연산자	883
OR 연산자	883
배타적 OR 연산자	884
문자열 연결 연산자	884
산술 더하기 연산자	885
산술 빼기 연산자	885
산술 곱하기 연산자	885
산술 나누기 연산자	886
조건부 연산자	886
인덱싱 연산자	887
식에서 사용할 수 있는 함수	887
ABOVE 함수 - 사용자가 지정된 LDAP DN 위에 있는지 여부	891
ABS 함수 - 절대값 찾기	892
AFTER 함수 - 문자열 찾기	892
ALL 함수 - 설정된 모든 비트	894
ANDBITS 함수 - bitwise AND 연산 수행	895
ANY 함수 - 설정된 임의 비트	895
AT 함수 - 사용자가 지정된 LDAP DN 에 있는지 여부	896
BEFORE 함수 - 문자열 찾기	897
BELOW 함수 - 사용자가 지정된 LDAP DN 아래에 있는지 여부	898

BOOLEAN 함수 - "TRUE" 또는 "FALSE"로 변환.....	899
CHAR 함수 - ASCII 값 변환.....	900
CENTER 함수 - 원본 문자열 채우기	901
COMMONDN 함수 - 공통 루트 찾기	903
COUNT 함수 - 집합의 요소 수 계산	904
DATE 함수 - 자정으로 설정(형식 1).....	905
DATE 함수 - 년, 월, 일, 시, 분 및 초 변환(형식 2).....	906
DATEFROMSTRING 함수 - 문자열을 숫자로 변환.....	907
DATETOSTRING 함수 - 숫자를 문자열로 변환.....	908
DAY 함수 - 월간 일자 반환	910
DOW 함수 - 요일 반환	911
DOY 함수 - 연간 일자 반환	912
ENUMERATE 함수 - 집합 요소 테스트	913
ERROR 함수 - 콘솔 로그에 오류 메시지 기록	914
EVALUATE 함수 - 식 평가.....	915
EXISTS 함수 - 파일 이름 조회	916
EXPLODEDN 함수 - LDAP DN 을 집합으로 변환.....	917
FILTER 함수 - 집합 요소 테스트.....	918
FIND 함수 - 문자열 내 위치 반환	919
GET 함수 - 사용자 디렉터리의 특성 찾기	921
HEX 함수 - 16 진수로 변환	922
HOURLY 함수 - 시간으로 변환	922
HOURLY24 함수 - 시간으로 변환	923
INFO 함수 - 콘솔 로그에 정보 메시지 기록	924
KEY 함수 - 키 조회	924
LCASE 함수 - 소문자로 변환	926
LEFT 함수 - 문자열의 일부 반환.....	926
LEN 함수 - 문자열 길이 반환	927
LOG 함수 - 파일에 문자열 기록	928
LOOP 함수 - 루프에서 가상 특성 호출	928
LPAD 함수 - 왼쪽에 원본 문자열 채우기	929
LTRIM 함수 - 문자열의 선행 공백 제거	931
MAX 함수 - 두 값 중 더 큰 값 확인.....	931
MAYBE 함수 - 미확정 결과 보고	932
MID 함수 - 문자열의 일부 반환	934
MIN 함수 - 두 숫자 중 더 작은 숫자 확인.....	935
MINUTE 함수 - 날짜의 분 구성 요소 반환	936
MOD 함수 - 나누기 나머지 반환.....	936
MONTH 함수 - 날짜의 월 구성 요소 반환	937
NOTBITS 함수 - bitwise NOT 수행	938

NOW 함수 - 현재 시간을 초 단위로 반환.....	938
NOWGMT 함수 - 현재 시간을 초 단위로 반환.....	939
NUMBER 함수 - 숫자 값으로 변환.....	940
ORBITS 함수 - bitwise OR 연산 수행.....	941
PARENTDN 함수 - LDAP 트리에서 부모 검색.....	941
PCASE 함수 - 문자열을 고유 명사 스타일 대/소문자로 변환.....	942
QS 함수 - 쿼리 문자열에서 항목 검색.....	943
RDN 함수 - LDAP DN 의 첫 번째 구성 요소 검색.....	945
RELATIONDN 함수 - 두 개의 고유 이름 비교.....	946
RIGHT 함수 - 문자열에서 문자 검색.....	947
RPAD 함수 - 오른쪽에 문자열 채우기.....	948
RPT 함수 - 문자열 반복.....	949
RTRIM 함수 - 문자열의 후행 공백 제거.....	950
SECOND 함수 - 날짜의 초 수 반환.....	951
SET 함수 - 특성 값 설정.....	951
SIGN 함수 - 숫자의 부호 반환.....	952
SORT 함수 - 집합 정렬.....	953
SPACE 함수 - 공백 문자열 반환.....	954
STRING 함수 - 문자열로 변환.....	955
THROW 함수 - 처리 중지 및 사용자 지정 오류 보고.....	955
WARNING 함수 - 콘솔 로그에 경고 메시지 기록.....	956
TRANSLATE 함수 - 문자열 값 바꾸기.....	957
UCASE 함수 - 대문자로 변환.....	958
URL 함수 - URL 문자열의 구성 요소 반환.....	958
URLDECODE 함수 - URL 문자열 디코딩.....	961
URLENCODE 함수 - 문자열 인코딩.....	962
VEXIST 함수 - 매개 변수 정의 여부 확인.....	963
WARNING 함수 - 콘솔 로그에 경고 메시지 기록.....	964
XORBITS 함수 - bitwise XOR 연산 수행.....	965
YEAR 함수 - 숫자 형식 날짜의 연도 구성 요소 반환.....	965
YEAR4 함수 - 날짜의 연도 구성 요소(4 자리) 반환.....	966

추가 정보:

[외부 관리자 저장소를 구성하는 방법](#) (페이지 50)

인증 체계 변경

관리 UI 를 보호하는 데 사용되는 기본 SiteMinder 인증 체계는 기본 사용자 이름 및 암호입니다. SAML 및 WS-Fed 인증을 제외하고 SiteMinder 에서 지원하는 모든 인증 체계로 기본 인증 체계를 변경할 수 있습니다.

다음 단계를 수행하십시오.

1. "정책", "도메인"을 차례로 클릭합니다.
2. "영역"을 클릭합니다.
3. 다음 영역을 검색하고 이름을 클릭하여 엽니다.

SiteMinder_ims_realm

참고: 이 영역은 SiteMinderDomain 이라는 도메인과 연결되어 있습니다.

4. "수정"을 클릭하여 설정이 사용되도록 설정합니다.
5. "인증 체계" 목록에서 원하는 인증 체계를 선택합니다.
6. 필요한 경우 추가 설정을 입력합니다.
7. "제출"을 클릭합니다.

선택한 인증 체계를 사용하여 관리 UI 가 보호됩니다.

추가 정보:

[인증 체계](#) (페이지 287)

관리 UI 에 SiteMinder 인증 사용 안 함

관리 UI 를 SiteMinder 로 보호하지 않으려면 SiteMinder 인증이 사용되지 않도록 설정할 수 있습니다. 관리 UI 에 대한 SiteMinder 보호를 제거한 후에도 리버스 프록시 서버를 통해서만 관리 UI 에 액세스할 수 있습니다.

응용 프로그램 서버에서 직접 관리 UI 에 액세스하려면 데이터 디렉터리를 삭제하고 정책 서버에 관리 UI 를 다시 등록하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "관리 인증" 마법사를 실행하여 더 이상 SiteMinder 인증으로 관리 UI 를 보호하지 않도록 지정합니다.

참고: 외부 관리자 저장소를 계속 사용하려면 기존 디렉터리 서버 또는 데이터베이스 연결 정보를 그대로 두십시오.

3. 관리 UI 호스트 시스템에 로그인합니다.
4. 관리 UI 데이터 디렉터리를 삭제합니다. 관리 UI 를 배포한 응용 프로그램 서버 유형에 따라 데이터 디렉터리의 위치가 결정됩니다.

- 독립 실행형 옵션을 사용하여 관리 UI 를 설치한 경우 데이터 디렉터리가 다음 위치에 있습니다.

`install_dir/adminui/server/default/data`

- 관리 UI 를 기존 응용 프로그램 서버에 설치한 경우 데이터 디렉터리의 기본 위치는 다음과 같습니다.

- (JBoss): `<JBoss Install>/server/default/data`

- (WebSphere):
`<WebSphere>\AppServer\profiles\<your_profile>\data`

- (WebLogic): `<weblogic install>\user_projects\domains\<user_domain>\data`

5. 정책 서버 호스트 시스템에 로그인하고 XPSRegClient 유틸리티를 사용하여 관리 UI 등록 창을 재설정합니다.
6. 정책 서버에 관리 UI 를 등록합니다.

제 3 장: SiteMinder 관리자

이 섹션은 다음 항목을 포함하고 있습니다.

- [SiteMinder 관리자 개요](#) (페이지 47)
- [외부 관리자 저장소를 구성하는 방법](#) (페이지 50)
- [관리자를 만드는 방법](#) (페이지 66)
- [범위 지정 관리자를 만드는 방법](#) (페이지 68)
- [관리자 사용 사례](#) (페이지 74)
- [레거시 관리자를 만드는 방법](#) (페이지 78)
- [관리자 비활성화](#) (페이지 81)
- [레거시 관리자 비활성화](#) (페이지 82)
- [관리자 액세스 권한 복원](#) (페이지 83)
- [관리 UI에 대한 접근성 모드를 구성하는 방법](#) (페이지 83)

SiteMinder 관리자 개요

관리자는 정책 서버 개체 및 도구에 액세스할 수 있는 사람입니다.

조직에서 서로 다른 관리자가 자신의 역할별로 다른 권한을 갖도록 여러 관리자 계정을 만들 수 있습니다.

이 모델을 사용하면 정책 서버 개체 및 도구의 관리를 다른 사람에게 위임할 수 있습니다.

관리자 아이덴티티의 기본 원본인 정책 저장소를 구성할 때 모든 시스템 권한이 있는 기본 SiteMinder 슈퍼 사용자 계정이 생성됩니다. 이 기본 구성을 사용하면 소프트웨어 설치 후 즉시 환경을 관리할 수 있습니다.

외부 관리자 사용자 저장소를 구성할 것을 권장합니다.

기본 슈퍼 사용자 관리자

정책 저장소를 구성할 때 기본 슈퍼 사용자 계정이 생성됩니다. 이 계정은 최대 시스템 권한을 가지며 다음 작업에 사용됩니다.

- 정책 서버에 관리 UI 등록
- 다른 관리자 계정을 포함하는 다른 유형의 정책 서버 개체 만들기

- 정책 서버 도구 사용
- 트러스트된 호스트 관리
- 정책 관리 API 관리

기본 슈퍼 사용자 계정의 자격 증명은 다음과 같습니다.

사용자 이름

siteminder

암호

정책 저장소를 구성할 때 지정한 암호

참고: 정책 저장소 구성에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오. 관리 UI 등록에 대한 자세한 내용은 "정책 서버 설치 안내서"를 참조하십시오.

관리자 계정

관리자 계정은 다음과 같은 SiteMinder 관리 태스크를 수행하는 데 사용할 수 있습니다.

- 관리 UI 를 사용하여 SiteMinder 개체 관리
- XPSImport 및 XPSExport 와 같은 정책 서버 도구 사용

관리자 계정을 생성하여 해당 관리자가 사용할 수 있는 관리 기능을 결정하는 세부적인 권한을 위임할 수 있습니다. 특히, 관리자 계정은 다음 속성을 정의합니다.

범위

관리자가 모든 SiteMinder 데이터에 액세스할 수 있는지 또는 할당된 관리 작업 영역에 정의된 개체에만 액세스할 수 있는지를 지정합니다.

액세스 방법

관리자가 SiteMinder 데이터를 액세스 및 관리하는 데 사용할 수 있는 방법을 지정합니다.

권한

관리자가 액세스할 수 있는 SiteMinder 개체의 범주 및 관리자가 해당 개체를 볼 수만 있는지 또는 보고 수정할 수 있는지를 지정합니다.

이러한 세분성 덕분에 관리자를 생성하고 조직에서의 관리 역할에 맞는 권한을 할당할 수 있습니다.

참고: 외부 관리자 저장소의 관리 사용자와 연결된 관리자 계정만 새로 생성할 수 있습니다. 그러나 정책 저장소에 저장된 레거시 관리자 기록에 대한 관리자 계정은 자동으로 생성되므로 관리자는 관리 UI에 액세스할 수 있습니다.

레거시 관리자 계정

레거시 관리자 계정은 다음과 같은 관리 태스크를 수행하는 데 사용할 수 있습니다.

- smobjimport 및 smobjexport 같은 정책 서버 도구 사용
- 트러스트된 호스트 관리자 역할 수행 트러스트된 호스트 관리자는 SiteMinder 에이전트 호스트 시스템에서 호스트 등록 프로세스를 실행할 권한이 있습니다. 등록 프로세스는 에이전트가 정책 서버와 통신할 수 있도록 해 줍니다.
- 정책 관리 API 사용

참고: 정책 관리 API를 사용하는 스크립트나 프로그램이 환경에 포함된 경우 레거시 관리자 계정이 필요합니다. 정책 관리 API를 통해 기능을 실행할 수 있는 인증 권한이 있는 레거시 관리자를 생성하십시오.

참고: 정책 저장소가 관리자 아이덴티티의 원본으로 구성된 경우(기본값) 레거시 관리자는 또한 관리 UI에 액세스할 수도 있습니다. 외부 관리자 저장소가 구성된 후에는 더 이상 레거시 관리자 계정이 관리 UI에 액세스할 수 없습니다.

추가 정보:

[관리자 저장소 옵션](#) (페이지 49)

관리자 저장소 옵션

기본적으로 관리 UI에서는 정책 저장소를 관리자 아이덴티티의 원본으로 사용합니다. 그러나 추가 관리자 계정에는 기업 디렉터리와 같은 외부 관리자 저장소를 사용하는 것이 좋습니다.

관리자 아이덴티티를 저장할 위치를 결정할 때는 다음 요소를 고려하십시오.

- 단일 정책 서버를 포함하는 관리 UI 를 구성하는 경우 정책 저장소를 사용하여 관리자 아이덴티티를 저장할 수 있습니다.
- 여러 정책 서버를 포함하는 관리 UI 를 구성하는 경우 외부 관리자 저장소를 사용해야 합니다.
- 정책 저장소에 관리자 아이덴티티를 저장하는 경우에는 레거시 관리자를 생성해야 정책 저장소에서 새 관리자 기록을 설정할 수 있습니다.
- 외부 저장소에 관리자 아이덴티티를 저장하는 경우에는 외부 저장소에서 관리자 기록을 찾을 수 있도록 관리자 계정을 생성합니다.

참고: 외부 관리자 저장소가 구성되면 새 레거시 관리자를 생성하거나 관리자 계정을 레거시 관리자 기록과 연결하여 관리 UI 액세스를 허용할 수 없습니다.

- 외부 관리자 저장소는 여러 관리 UI 인스턴스가 동일한 관리자 집합을 공유하도록 하는 데 사용할 수 있습니다. 기본적으로 관리 UI 는 등록된 정책 서버를 사용하여 구성된 정책 저장소를 사용합니다.

참고: 관리 UI 설치 및 추가 정책 서버 연결 구성에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.

외부 관리자 저장소를 구성하는 방법

외부 관리자 저장소에 대한 연결을 구성하려면 다음 단계를 완료하십시오.

1. (선택 사항) SiteMinder 로 관리 UI 를 보호하려면 에이전트가 리버스 프록시 서버에서 작동하도록 구성합니다.

참고: 리버스 프록시 서버를 구성하는 방법에 대한 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.

2. 외부 관리자 저장소 고려 사항을 검토합니다.
3. SSL 고려 사항을 고려합니다.
4. 저장소 유형에 따라 다음을 수행합니다.
 - (LDAP) 디렉터리 서버 연결 정보를 수집합니다.
 - (RDB) 데이터베이스 연결 정보를 수집합니다.

- (RDB) JDBC(Java Database Connectivity) 데이터 원본을 응용 프로그램 서버에 배포합니다.
 - 독립 실행형 옵션을 사용하여 관리 UI 를 설치한 경우 smjdbcsetup 유틸리티를 사용하여 데이터 원본을 구성하고 배포합니다.
 - 기존 응용 프로그램 서버 인프라에 관리 UI 를 설치한 경우 공급업체별 설명서에서 데이터 원본 구성 및 배포에 대한 정보를 확인하십시오.

참고: WebSphere 에 데이터 원본을 배포하려는 경우 데이터 원본 속성 아래에서 JNDI 이름 앞에 다음을 붙여야 합니다.

jdbc/

예: 데이터 원본 이름이 abc 인 경우 JNDI 이름은 jdbc/abc 입니다.

5. 외부 관리자 저장소에 대한 연결을 구성합니다.
6. (선택 사항) 레거시 관리자 관리 UI 권한을 마이그레이션합니다.

외부 관리자 저장소 고려 사항

외부 관리자 저장소 연결을 구성하기 전에 다음 사항을 고려하십시오.

- **중요!** 정책 저장소를 더 이상 관리자 아이덴티티의 원본으로 사용하지 않도록 설정할 경우 설정을 되돌릴 수 없습니다. 외부 관리자 저장소 구성은 외부 저장소를 사용하도록 구성된 관리 UI 에만 영향을 줍니다. 아직 외부 저장소를 사용하도록 구성되지 않은 다른 관리 UI 는 계속해서 정책 저장소를 사용하여 관리자를 식별합니다.
- 기본 SiteMinder 슈퍼 사용자 계정을 포함한 레거시 관리자는 다음 작업을 계속 수행할 수 있습니다.
 - 정책 관리 API 관리
 - 트러스트된 호스트 관리자 역할 수행
 - 정책 서버 도구 사용
- 기본 SiteMinder 슈퍼 사용자 계정을 포함한 레거시 관리자는 더 이상 관리 UI 에서 SiteMinder 개체를 관리할 수 없습니다.

- 관리 UI 를 계속 사용해야 하는 레거시 관리자가 있는 경우 공급업체 관련 도구를 사용하여 해당 사용자를 외부 저장소에 추가하십시오. 외부 저장소에 사용자 아이덴티티를 설정한 후 기존 사용자 경로를 정책 저장소에서 외부 저장소로 매핑하여 이러한 권한을 복원할 수 있습니다.

중요! 외부 관리자 인증에서는 단일 레거시 관리자 계정이 관리 UI, 정책 관리 API 및 트러스트된 호스트 권한에 대한 권한을 동시에 보유할 수 없습니다. 레거시 관리자가 이러한 역할을 계속 수행해야 할 경우에는 레거시 관리자를 변경하지 마십시오. 사용자가 외부 저장소에 있는지 확인하고 외부 사용자 아이덴티티를 사용하여 새 관리자를 별도로 구성하십시오.

- 외부 저장소에 대한 연결을 구성할 때 식별한 슈퍼 사용자가 기본 SiteMinder 슈퍼 사용자 계정을 대체합니다. 이 외부 사용자는 슈퍼 사용자가 되고 관리 UI 에서의 최대 권한과 모든 정책 서버 도구에 대한 액세스 권한을 갖게 됩니다.

외부 슈퍼 사용자를 사용하여 새 관리자에게 권한을 위임하십시오.

- 여러 관리 UI 인스턴스에서 동일한 관리자 인증 저장소를 사용하려는 경우 동일한 네트워크 식별자를 사용하여 각 연결을 구성해야 합니다. 동일한 외부 관리자 인증 저장소에 대한 여러 관리 UI 연결에 네트워크 식별자를 혼합해서 사용하는 것은 지원되지 않습니다.

예: 첫 번째 연결을 172.16.0.0 을 사용하여 구성한 경우 이후의 연결도 172.16.0.0 을 사용하여 생성합니다. 마찬가지로 첫 번째 연결을 comp001@example.com 을 사용하여 구성한 경우 이후의 연결도 comp001@example.com 을 사용하여 생성합니다.

SSL 고려 사항

SSL 을 통한 외부 관리자 저장소 연결을 구성할 경우 다음 사항을 고려하십시오.

- 디렉터리 서버가 SSL 을 통해 통신하도록 구성되어 있어야 합니다.
참고: 디렉터리 서버에 대해 SSL 을 구성하는 방법에 대한 자세한 내용은 해당 공급업체의 설명서를 참조하십시오.
- 독립 실행형 옵션으로 관리 UI 를 설치한 경우 관리 UI 는 포함된 인증서 데이터베이스와 함께 설치되어 있습니다.
- 기존 응용 프로그램 서버 인프라에 관리 UI 를 설치한 경우 사용 중인 응용 프로그램 서버 요구 사항에 맞게 인증서 데이터베이스를 구현하십시오.
참고: 인증서 데이터베이스 구현에 대한 자세한 내용은 해당 공급업체의 설명서를 참조하십시오.
- 디렉터리 연결 정보를 입력할 때 SSL 사용 포트를 입력해야 합니다. SSL 사용 포트를 입력하지 않으면 "관리 인증" 마법사가 응답하지 않습니다.

디렉터리 서버 정보 수집

디렉터리 서버에 대한 연결을 구성하려는 경우 다음 정보를 수집하십시오.

- **호스트 이름** - 디렉터리 서버 호스트 시스템의 IP 주소 또는 정규화된 도메인 이름을 식별합니다.
- **포트** - 디렉터리 서버가 수신 대기하는 포트를 식별합니다.
- **디렉터리 서버 사용자 자격 증명** - 디렉터리 서버에 대한 읽기/쓰기 권한이 있는 계정의 사용자 이름 및 암호를 식별합니다.
- **검색 루트** - 디렉터리 서버의 기본 DN 을 식별합니다.
- **SSL 인증서** - 디렉터리 서버가 SSL 연결을 통해 통신하도록 구성되어 있는 경우 SSL 인증서를 가져옵니다.

데이터베이스 정보 수집

데이터베이스에 대한 연결을 구성하려는 경우 다음 정보를 수집하십시오.

- **호스트 이름** - 데이터베이스 호스트 시스템의 이름을 식별합니다.
- **포트** - 데이터베이스가 수신 대기하는 포트를 식별합니다.
- **(Microsoft SQL Server) 데이터베이스 이름** - 데이터베이스 이름을 식별합니다.
- **(Oracle) 서비스 이름** - 데이터베이스의 서비스 이름을 식별합니다.
- **데이터베이스 사용자 자격 증명** - 데이터베이스에 대한 읽기/쓰기 권한이 있는 사용자 계정의 자격 증명을 식별합니다.

중요! Oracle 에 대한 연결을 구성하려는 경우 이 사용자에게 대한 기본 스키마를 설정해야 합니다. 기본 스키마는 관리 사용자가 포함된 테이블과 연결된 스키마여야 합니다. 이 사용자에게 대해 기본 스키마를 설정하지 않으면 "관리 인증" 마법사가 데이터베이스에서 사용자를 찾을 수 없습니다.

JDBC 데이터 원본 배포

관계형 데이터베이스에 대한 연결을 구성하려는 경우 관리 UI 가 관리자 저장소와 통신하려면 JDBC 데이터 원본이 필요합니다. 데이터 원본을 생성하려면 유틸리티가 필요합니다. 독립 실행형 옵션을 사용하여 관리 UI 를 설치한 경우 smjdbcsetup 유틸리티가 제공됩니다.

참고: 기존 응용 프로그램 서버에 관리 UI 를 설치한 경우 JDBC 데이터 원본 배포에 대한 자세한 내용은 해당 공급업체의 설명서를 참조하십시오. WebSphere 에 데이터 원본을 배포하려는 경우 데이터 원본 속성에서 JNDI 이름 앞에 다음 텍스트가 나오는지 확인하십시오.

jdbc/

예: 데이터 원본 이름이 abc 인 경우 JNDI 이름은 jdbc/abc 입니다.

다음 단계를 수행하십시오.

1. 관리 UI 호스트 시스템에 로그인합니다.
2. (UNIX) SiteMinder 관리 UI 서비스를 중지합니다.
참고: 서비스 중지에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.
3. `administrative_ui_home\CA\SiteMinder\adminui\bin` 으로 이동합니다.

administrative_ui_home

관리 UI 설치 경로를 지정합니다.

4. 다음 명령 중 하나를 실행합니다.

■ (Windows)

`smjdbcsetup.bat`

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

■ (UNIX)

`smjdbcsetup.sh`

고유 식별자를 묻는 메시지가 표시됩니다. 이 식별자는 데이터 원본에 추가됩니다.

5. 값을 입력하고 Enter 키를 누릅니다.
데이터베이스 드라이버 유형을 묻는 메시지가 표시됩니다. 드라이버 유형 앞에는 숫자가 나옵니다.
6. 숫자를 입력하여 드라이버 유형을 선택하고 Enter 키를 누릅니다.
데이터베이스 호스트 시스템의 이름을 묻는 메시지가 표시됩니다.
7. 데이터베이스 호스트 이름을 입력하고 Enter 키를 누릅니다.
데이터베이스가 수신 대기하는 포트를 묻는 메시지가 표시됩니다.
8. 데이터베이스 포트를 입력하고 Enter 키를 누릅니다.
 - Microsoft SQL Server 에 대한 연결을 구성하려는 경우 데이터베이스 이름을 묻는 메시지가 표시됩니다.
 - Oracle 에 대한 연결을 구성하려는 경우 서비스 이름을 묻는 메시지가 표시됩니다.

9. 데이터베이스 이름 또는 서비스 이름을 입력하고 **Enter** 키를 누릅니다.

데이터베이스 사용자 계정 이름을 묻는 메시지가 표시됩니다.

10. 데이터베이스 사용자 계정 이름을 입력하고 **Enter** 키를 누릅니다.

참고: 이 사용자 계정에는 데이터베이스에 대한 읽기/쓰기 권한이 있어야 합니다.

데이터베이스 사용자 암호를 묻는 메시지가 표시됩니다.

11. 암호를 입력하고 **Enter** 키를 누릅니다.

연결 상세 정보가 나타납니다.

12. 상세 정보를 검토하고 다음 단계 중 하나를 수행합니다.

- 데이터 원본을 구성 및 배포하려면 **y** 를 입력하고 **Enter** 키를 누릅니다.

`admin_ui_home\CA\SiteMinder\adminui\server\default\deploy` 에
데이터 원본이 배포되고, SiteMinder 관리 UI 서비스를 다시
시작하라는 메시지가 표시됩니다.

`admin_ui_home`

관리 UI 설치 경로를 지정합니다.

참고: 데이터 원본을 사용하여 연결을 생성하려면 SiteMinder 관리 UI
서비스를 다시 시작해야 합니다.

- 배포를 취소하려면 **n** 을 입력하고 **Enter** 키를 누릅니다.

13. 다음 단계 중 하나를 수행합니다.

- 서비스를 자동으로 시작하려면 다음 단계 중 하나를 수행합니다.
 - (Windows) **y** 를 입력하고 **Enter** 키를 누릅니다.
 - (UNIX) 서비스를 수동으로 시작해야 합니다. 서비스 시작에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.
- 서비스를 수동으로 시작하려면 **n** 을 입력하고 **Enter** 키를 누릅니다.
데이터 원본이 구성되고 유틸리티가 종료됩니다.

LDAP 관리자 저장소 연결 구성

연결을 구성하여 관리자 아이덴티티의 출처를 정책 저장소에서 외부 저장소로 변경하십시오.

다음 단계를 수행하십시오.

1. "관리", "관리 UI", "관리 인증 구성"을 클릭합니다.
 - 외부 관리자 저장소를 처음 구성하는 경우에는 "관리 인증 구성" 마법사가 나타납니다.
 - 관리 UI가 외부 관리자 저장소로 구성된 경우에는 연결 상세 정보가 표시됩니다. "확인"을 클릭하여 "관리 인증 구성" 마법사를 시작합니다.

2. (선택 사항) 제품을 사용하여 관리 UI를 보호하려면 드롭다운 목록에서 에이전트를 선택하고 "다음"을 클릭합니다.

CA SiteMinder® for Secure Proxy Server로 구성된 에이전트 또는 리버스 프록시 서버로 기능하도록 구성된 에이전트를 선택하십시오.

3. "디렉터리 유형" 목록에서 디렉터리 서버 공급업체를 선택하고 "다음"을 클릭합니다.

마법사에서 연결 상세 정보를 묻는 메시지가 표시됩니다.

4. 다음 태스크를 수행하십시오.

- a. 디렉터리 서버 호스트 시스템의 IP 주소 또는 정규화된 도메인 이름을 "호스트" 필드에 입력합니다.

중요! 여러 관리 UI 인스턴스가 동일한 관리자 인증 저장소를 사용해야 하는 경우 입력하는 네트워크 식별자를 기록해 두십시오. 동일한 외부 관리자 인증 저장소에 대한 여러 관리 UI 연결에 네트워크 식별자를 혼합해서 사용하는 것은 지원되지 않습니다.

예: 172.16.0.0 을 사용하여 첫 번째 연결을 구성하는 경우 이후 연결도 172.16.0.0 을 사용하여 생성합니다.

comp001@example.com 을 사용하여 첫 번째 연결을 구성하는 경우 이후 연결도 comp001@example.com 을 사용하여 생성합니다.

- b. 디렉터리 서버가 수신 대기하는 포트를 "포트" 필드에 입력합니다.

중요! SSL 을 통한 연결을 구성하는 경우에는 SSL 사용 포트를 입력하십시오. 그렇지 않으면 "관리 인증" 마법사가 응답하지 않습니다.

- c. (선택 사항) "SSL 사용"을 선택하고 CA(인증 기관) 인증서를 업로드하여 관리 UI 와 관리자 저장소 간에 SSL 통신을 사용할 수 있도록 합니다.

참고: 디렉터리 서버는 SSL 을 통해 통신해야 합니다. SSL 을 사용하도록 디렉터리 서버를 구성하는 방법에 대한 자세한 내용은 해당 공급업체의 설명서를 참조하십시오.

- d. 디렉터리 서버 사용자의 공용 이름과 암호를 각 필드에 입력합니다.

참고: 이 사용자에게는 디렉터리 서버에 대한 읽기/쓰기 권한이 있어야 합니다.

- e. "다음"을 클릭합니다.

5. 다음 태스크를 수행하십시오.

- a. "검색 루트" 필드에 디렉터리 서버 검색 루트를 입력합니다.
- b. 서틀 컨트롤을 사용하여 SiteMinder 관리자에 적용되는 개체 클래스를 추가하거나 제거합니다.
- c. "다음"을 클릭합니다.

6. 필요한 각 특성에 매핑되는 니모닉 특성 문자열을 선택하고 "다음"을 클릭합니다.

마법사에서 사용자를 검색하라는 메시지가 표시됩니다.

중요! LDAP 또는 기타 다른 응용 프로그램에 의해 사용되거나 작성된 특성을 가리키면 안 됩니다. 만일 이러한 특성을 가리키면 /logout.jsp 페이지로 리디렉션되고 관리 UI 에 로그인할 수 없게 됩니다.

- 7. "키워드" 필드에 사용자 이름의 전체 또는 일부를 입력합니다.
- 8. 한 사용자를 선택하고 "다음"을 클릭합니다.

참고: 한 명의 사용자만 선택할 수 있습니다. 연결이 구성되면 이 사용자가 슈퍼 사용자가 됩니다.

- 9. 연결 상세 정보를 확인하고 "마침"을 클릭합니다.

중요! 새로운 관리자 자격 증명으로 로그인하기 전에 응용 프로그램 서버를 수동으로 다시 시작하십시오.

RDB 관리자 저장소 연결 구성

연결을 구성하여 관리자 아이덴티티의 출처를 정책 저장소에서 외부 저장소로 변경하십시오.

다음 단계를 수행하십시오.

1. "관리", "관리 UI", "관리 인증 구성"을 클릭합니다.
 - 외부 관리자 저장소를 처음 구성하는 경우에는 "관리 인증 구성" 마법사가 나타납니다.
 - 관리 UI가 외부 관리자 저장소로 구성된 경우에는 연결 상세 정보가 표시됩니다. "확인"을 클릭하여 "관리 인증 구성" 마법사를 시작합니다.
2. (선택 사항) 제품을 사용하여 관리 UI를 보호하려면 드롭다운 목록에서 에이전트를 선택하고 "다음"을 클릭합니다.
리버스 프록시 서버와 작동하도록 구성된 에이전트를 선택하십시오.
3. "디렉터리 유형" 목록에서 다음 항목 중 *하나*를 선택합니다.
 - 사용자 스키마에 사용자의 전체 이름을 식별하는 열이 포함된 경우 "Relational Database (with full name column)"(관계형 데이터베이스(전체 이름 열 포함)) 템플릿을 선택합니다.
 - 사용자의 전체 이름을 계산해야 할 경우 "Relational Database (without full name column)"(관계형 데이터베이스(전체 이름 열 미포함)) 템플릿을 선택합니다.
4. "다음"을 클릭합니다.
참고: 데이터 원본이 나타나지 않을 경우 "취소"를 클릭하고 JDBC 데이터 원본을 응용 프로그램 서버에 배포하십시오. 데이터 원본이 배포되지 않은 경우에는 연결을 설정할 수 없습니다.
5. 데이터 원본을 선택하고 "다음"을 클릭합니다.
6. 사용자 테이블을 선택하고 "다음"을 클릭합니다.

7. 다음 태스크 중 *하나*를 수행합니다.

- "Relational Database (with full name column)"(관계형 데이터베이스(전체 이름 열 포함)) 템플릿을 선택한 경우 필요한 각 사용자 특성에 매핑되는 열 이름을 선택하십시오. "다음"을 클릭합니다.
- "관계형 데이터베이스"(전체 이름 미포함) 템플릿을 선택한 경우:
 - a. 필요한 각 사용자 특성에 매핑되는 열 이름을 선택합니다.
 - b. "Get Full Name Query"(전체 이름 가져오기 쿼리)를 작성합니다. `##FIRST_NAME`, `##LAST_NAME`, `##PRIMARY_KEY` 를 각 사용자 특성에 매핑되는 열 이름으로 바꾸십시오.

참고: 쿼리 끝의 물음표(?)는 그대로 둡니다.

예: `select SmUser.FirstName + ' ' + SmUser.LastName from SmUser where SmUser.UserID = ?`

- c. "다음"을 클릭합니다.

8. "사용자 키워드" 필드에 사용자 이름의 전체 또는 일부를 입력합니다.

9. 사용자를 선택하고 "다음"을 클릭합니다.

참고: 이 사용자는 슈퍼 사용자가 됩니다.

10. 연결 상세 정보를 확인하고 "마침"을 클릭합니다.

중요! 외부 관리자 저장소를 구성한 후에는 새로운 관리자 자격 증명으로 로그인하기 *전에* 응용 프로그램 서버를 수동으로 다시 시작하십시오.

레거시 관리자 권한 마이그레이션

외부 관리자 저장소에 대한 연결을 구성한 후에도 레거시 관리자가 계속 관리 UI 또는 정책 서버 도구를 사용해야 하는 경우에는 권한을 마이그레이션합니다.

중요! 외부 관리자 인증에서는 단일 레거시 관리자 계정이 관리 UI, 정책 서버 도구 및 정책 관리 API에 대한 권한과 트러스트된 호스트 권한을 동시에 보유할 수 없습니다. 레거시 관리자가 이러한 역할 중 하나 이상을 계속 사용해야 하는 경우에는 레거시 관리자를 변경하지 마십시오. 사용자가 외부 저장소에 있는지 확인하고 외부 사용자 아이덴티티를 사용하여 새 관리자를 별도로 구성하십시오.

다음 단계를 수행하십시오.

참고: 관리자가 외부 저장소에 있는지 확인하십시오. 외부 슈퍼 사용자를 사용하여 관리 UI에 로그인합니다.

1. "관리", "관리자"를 차례로 클릭합니다.

2. "관리자"를 클릭합니다.

"관리자" 페이지가 표시됩니다.

3. 사용자의 전체 이름을 사용하여 검색 조건을 지정하고 "검색"을 클릭합니다.

검색 조건과 일치하는 사용자가 표시됩니다.

4. 수정할 관리자의 이름을 클릭합니다.

"관리자 보기" 페이지가 표시됩니다. 사용자 경로가 정책 저장소를 가리킵니다.

5. "수정"을 클릭합니다.

설정과 컨트롤이 활성화됩니다.

6. "일반"에서 "조회"를 클릭합니다.

"사용자 선택" 페이지가 표시됩니다.

7. 검색 조건을 지정하고 "검색"을 클릭합니다.

지정된 기준과 일치하는 사용자가 표시됩니다.

8. 원하는 사용자를 선택하고 "선택"을 클릭합니다.

사용자 경로가 외부 저장소를 가리키도록 업데이트됩니다.

9. "제출"을 클릭합니다.

관리 UI에서 외부 저장소를 사용하여 관리자를 인증합니다. 관리자는 관리자 아이덴티티 저장에 정책 저장소가 사용될 때와 동일한 수준의 관리 UI 액세스 권한을 가집니다.

외부 관리자 저장소 자격 증명 업데이트

관리 UI 가 외부 관리자 저장소에 연결하는 데 사용하는 자격 증명이 변경된 경우 새 자격 증명을 관리 UI 에 제출하십시오. 그렇지 않으면 SiteMinder 관리자 인증이 실패합니다.

독립 실행형 옵션을 사용하여 관리 UI 를 설치한 경우 유틸리티가 두 개 제공됩니다.

- (LDAP) smjndisetaup 유틸리티를 사용하여 디렉터리 서버 사용자 계정 자격 증명을 업데이트합니다.

참고: 디렉터리 서버 호스트 시스템 이름 또는 포트 정보를 업데이트하려면 관리 UI 를 사용하여 외부 관리자 저장소에 대한 연결을 다시 생성하십시오. smjndisetaup 유틸리티는 호스트 또는 포트 정보를 업데이트할 수 있습니다.

- (RDB) smjdbcsetaup 유틸리티를 사용하여 데이터베이스 사용자 계정 자격 증명을 업데이트합니다.

참고: 데이터베이스 호스트 시스템 이름 또는 포트 정보를 업데이트하려면 smjdbcsetaup 유틸리티를 사용하여 JNDI 데이터 원본을 다시 배포하십시오.

기존 응용 프로그램 서버 인프라에 관리 UI 를 설치한 경우 다음 사항을 고려하십시오.

- (LDAP) 관리 UI 가 디렉터리 서버에 액세스하는 데 사용할 자격 증명을 업데이트하려면 "관리 인증" 마법사를 사용합니다.

중요! 마법사를 사용하여 자격 증명을 업데이트한 후 가능한 한 빨리 디렉터리 서버에서 자격 증명을 업데이트하십시오. 디렉터리 서버 자격 증명에 마법사를 사용하여 제공한 자격 증명과 일치하도록 업데이트되기 전까지는 관리자가 관리 UI 에 로그인할 수 없습니다.

- (RDB) 데이터베이스별 도구를 사용하여 데이터 원본을 업데이트합니다.

추가 정보:

[JDBC 데이터 원본 배포](#) (페이지 54)

디렉터리 서버 자격 증명 업데이트

smjndisetaup 유틸리티를 사용하여 디렉터리 관리자 자격 증명을 업데이트할 수 있습니다.

참고: smjndisetaup 유틸리티는 관리 UI 를 사용하여 구성된 연결 상세 정보를 업데이트만 할 수 있습니다. smjndisetaup 유틸리티로 연결 자격 증명을 생성할 수는 없습니다.

디렉터리 서버 자격 증명을 업데이트하려면

1. 관리 UI 호스트 시스템에 로그인합니다.
2. (UNIX) SiteMinder 관리 UI 서비스를 중지합니다.

참고: SiteMinder 관리 UI 서비스 중지에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.

3. `administrative_ui_home\CA\SiteMinder\adminui\bin` 으로 이동합니다.

administrative_ui_home

관리 UI 설치 경로를 지정합니다.

4. 다음 명령 중 하나를 실행합니다.

■ (Windows)

```
smjndisetaup.bat --reset-password
```

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

■ (UNIX)

```
smjndisetaup.sh --reset-password
```

사용자 이름을 묻는 메시지가 표시됩니다.

5. 다음 작업 중 하나를 수행하십시오.

- 새 디렉터리 사용자를 입력하고 Enter 키를 누릅니다.
- 기본 사용자 이름을 그대로 사용하려면 Enter 키를 누릅니다.
사용자 암호를 묻는 메시지가 표시됩니다.

6. 새 암호를 입력하고 Enter 키를 누릅니다.

자격 증명이 확인되고, 디렉터리 연결 자격 증명을 업데이트할지 묻는 메시지가 표시됩니다.

7. y 를 입력하고 Enter 키를 누릅니다.

- Windows 에서 유틸리티를 실행한 경우 SiteMinder 관리 UI 서비스가 다시 시작됩니다. 또한 새 디렉터리 연결 상세 정보가 업데이트됩니다.
- UNIX 에서 유틸리티를 실행한 경우 관리 UI 서비스를 시작하여 새 디렉터리 연결 상세 정보를 업데이트합니다.

참고: 관리 UI 서비스 시작에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.

데이터베이스 자격 증명 업데이트

smjdbcsetup 유틸리티를 사용하여 JNDI 데이터 원본의 데이터베이스 사용자 자격 증명을 업데이트할 수 있습니다.

데이터베이스 자격 증명을 업데이트하려면

1. 관리 UI 호스트 시스템에 로그인합니다.
2. (UNIX) SiteMinder 관리 UI 서비스를 중지합니다.
3. `administrative_ui_home\CA\SiteMinder\adminui\bin` 으로 이동합니다.

administrative_ui_home

관리 UI 설치 경로를 지정합니다.

4. 다음 명령 중 하나를 실행합니다.

- (Windows)

```
smjdbcsetup.bat --reset-password
```

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

- (UNIX)

```
smjdbcsetup.sh --reset-password
```

고유 식별자를 입력하라는 메시지가 표시됩니다.

5. 배포된 데이터 원본의 이름을 입력합니다.

참고: 데이터 원본 이름을 모르는 경우

`administrative_ui_home\SiteMinder\adminui\server\default\deploy` 에서 배포된 모든 데이터 원본을 찾을 수 있습니다.

`administrative_ui_home`

관리 UI 설치 경로를 지정합니다.

데이터베이스 사용자 이름을 묻는 메시지가 표시됩니다.

6. 사용자 이름을 입력하고 Enter 키를 누릅니다.

사용자 암호를 묻는 메시지가 표시됩니다.

7. 암호를 입력하고 Enter 키를 누릅니다.

새 데이터 원본 자격 증명을 확인하고 해당 자격 증명을 업데이트할 수 있는지 확인하라는 메시지가 표시됩니다.

8. y 를 입력하고 Enter 키를 눌러 새 데이터 원본 자격 증명을 확인합니다.
데이터 원본이 업데이트됩니다.

- (Windows) SiteMinder 관리 UI 서비스를 다시 시작하라는 메시지가 표시됩니다.
- (UNIX) SiteMinder 관리 UI 서비스를 수동으로 다시 시작해야 한다는 메시지가 표시됩니다.

9. 다음 태스크 중 하나를 수행합니다.

- (Windows) 유틸리티를 사용하여 SiteMinder 관리 UI 서비스를 다시 시작하고 업데이트된 데이터 원본을 배포하려면 y 를 입력하고 Enter 키를 누릅니다.
- (Windows) SiteMinder 관리 UI 서비스를 수동으로 시작하려면 n 을 입력하고 Enter 키를 누릅니다. 서비스가 시작되면 데이터 원본이 배포됩니다.
- (UNIX) 수동으로 SiteMinder 관리 UI 서비스를 시작하여 데이터 원본을 배포합니다.

참고: SiteMinder 관리 UI 서비스 시작에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.

외부 관리자 저장소 연결 수정

"관리 인증" 마법사를 다시 실행하여 관리자 인증을 위해 관리 UI 가 연결하는 외부 저장소를 변경할 수 있습니다.

추가 정보:

[외부 관리자 저장소를 구성하는 방법](#) (페이지 50)

관리자를 만드는 방법

SiteMinder 관리자 계정은 해당 관리자가 사용할 수 있는 관리 기능을 결정하는 세분화된 권한을 사용하여 구성할 수 있습니다.

SiteMinder 관리자에는 관리 UI 에서 가지는 관리 권한(예: 인증 체계 관리)을 정의하는 하나 이상의 보안 범주에 대한 권한이 할당됩니다. 기본적으로 관리자는 할당된 보안 범주와 관련된 모든 SiteMinder 개체에 액세스할 수 있습니다.



1. [관리자 고려 사항 검토](#) (페이지 67)
2. [관리자 계정 만들기](#) (페이지 67)
3. [새 관리자 계정의 권한 확인](#) (페이지 68)

관리자 고려 사항

관리자를 구성하기 전에 다음 지침을 검토하십시오.

- 관리 UI 에서 외부 저장소를 관리자 아이덴티티의 원본으로 사용하고 있는 경우에만 이 프로세스가 적용됩니다. 정책 저장소를 관리자 아이덴티티의 원본으로 사용하는 경우에는 레거시 관리자를 만드십시오.
- 관리자가 작업을 수행하기 위해 필요한 권한. 이러한 권한을 식별하면 관리자에게 적절한 보안 범주를 쉽게 위임할 수 있습니다.
- 관리자가 응용 프로그램 보안 정책을 담당하는지 여부

중요! 관리자는 동일하거나 낮은 권한으로만 다른 관리자를 생성할 수 있습니다. 예를 들어 GUI 및 보고서 권한이 있는 관리자는 로컬 API 권한이 아닌 GUI 및 보고서 권한이 있는 다른 관리자를 생성할 수 있습니다. 마찬가지로 관리자는 할당된 작업 영역에 정의된 것과 동일하거나 낮은 범위로만 관리자를 생성할 수 있습니다.

관리자 계정 만들기

관리자 계정을 생성하여 관리자를 생성합니다.

다음 단계를 수행하십시오.

1. 슈퍼 사용자나 적절한 권한이 있는 다른 관리자 계정을 사용하여 관리 UI 에 로그인합니다.
2. "관리", "관리자"를 차례로 클릭합니다.
3. "관리자"를 클릭합니다.
4. "관리자 만들기"를 클릭합니다.
5. "일반" 아래에서 "조회"를 클릭합니다.
6. 검색 조건을 지정하고 "검색"을 클릭합니다.
7. 원하는 관리자를 선택하고 "선택"을 클릭합니다.
8. 다음 태스크 중 하나를 수행합니다.
 - 모든 권한을 위임하려면 "슈퍼 사용자"를 선택하고 "제출"을 클릭합니다.
 - 세분화된 권한을 위임하려면 다음 단계로 이동합니다.

9. "액세스 방법" 섹션에서 관리자가 정책 서버와 상호 작용할 수 있는 방법을 지정합니다. 관리자가 자신의 역할에 대해 필요한 방법을 선택하십시오.

예: 관리자가 XPSImport 및 XPSExport 도구를 사용하려는 경우 "가져오기 허용됨" 및 "내보내기 허용됨"을 선택합니다.

10. "권한" 섹션에서 "추가"를 클릭합니다.
11. 관리자에게 부여할 보안 범주를 선택한 다음 "확인"을 클릭합니다.

참고: 보안 범주는 특정 SiteMinder 개체에 해당하는 하나 이상의 태스크로 구성됩니다.

12. 각 보안 범주에 대해 관리자에게 부여할 권한을 "권한" 테이블에서 지정합니다.

참고: 테이블의 보안 범주에 적용 가능한 권한만 사용할 수 있습니다.

13. 제출을 클릭합니다.
관리자가 생성됩니다.

관리자에게 올바른 권한이 있는지 확인

관리자 계정을 만든 후 올바른 권한을 가지는지 확인하십시오.

다음 단계를 수행하십시오.

1. 관리자 계정을 사용하여 관리 UI에 로그인합니다.
2. 관리 UI를 탐색하여 계정에 권한이 있는 보안 범주만 표시되는지 확인합니다.

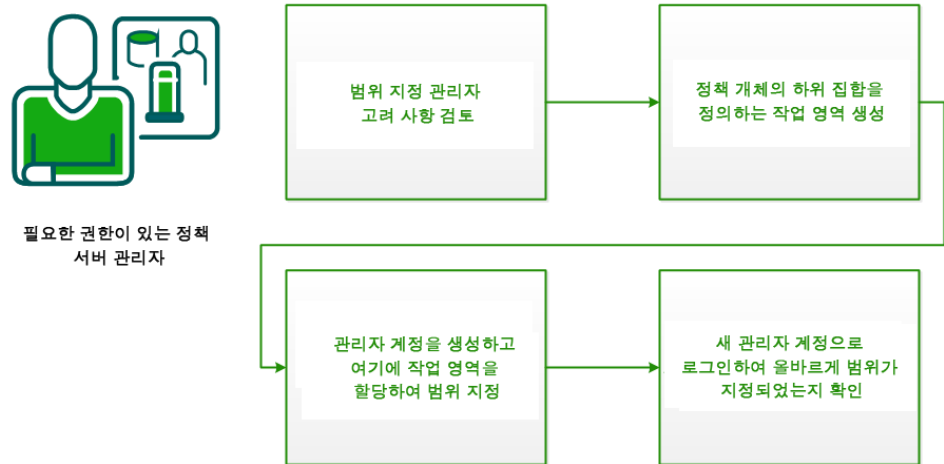
관리자 계정을 만드는 데 필요한 태스크를 완료했습니다.

범위 지정 관리자를 만드는 방법

SiteMinder 관리자 계정은 해당 관리자가 사용할 수 있는 관리 기능을 결정하는 세분화된 권한을 사용하여 구성할 수 있습니다.

SiteMinder 관리자 계정에는 관리 UI에서 가지는 관리 권한(예: 인증 체계 관리)을 정의하는 하나 이상의 보안 범주에 대한 권한이 할당됩니다. 기본적으로 관리자 계정은 할당된 보안 범주와 관련된 모든 SiteMinder 개체에 액세스할 수 있습니다.

작업 영역은 SiteMinder 개체의 하위 집합을 정의합니다. 하나 이상의 관리자 계정에 작업 영역을 할당하는 방법으로 해당 계정이 사용할 수 있는 개체를 필터링하여 각각의 관리 권한 범위를 추가적으로 제어할 수 있습니다. 할당된 작업 영역에 의해 관리 권한이 제한되는 관리자 계정을 **범위 지정 관리자**라고 합니다.



1. [범위 지정 관리자 고려 사항 검토](#) (페이지 69)
2. [SiteMinder 개체의 하위 집합을 정의하는 작업 영역 만들기](#) (페이지 70)
3. [관리자 계정 만들기 및 범위 지정](#) (페이지 72)
4. [새 관리자 계정의 범위 확인](#) (페이지 73)

범위 지정 관리자 지침

범위 지정 관리자는 정책 저장소에서 자신에게 **권한**이 있는 일부 개체를 관리할 수 없습니다. 관리 UI는 할당된 작업 영역에 정의된 개체만 포함하는 것으로 표시됩니다.

범위 지정 관리자가 최상위 개체를 새로 추가하는 경우 유사한 범위가 지정된 다른 모든 관리자가 해당 개체를 즉시 사용할 수 있게 됩니다.

새 관리자를 생성할 수 있는 권한이 있는 범위 지정 관리자는 작업 영역이 자신의 것과 동일하거나 더 제한적인 관리자만 생성할 수 있습니다. 범위 지정 관리자가 새 작업 영역을 생성하여 새 관리자의 범위를 추가로 지정하는 경우 이 새 작업 영역 개체가 자신의 현재 작업 영역에 추가됩니다. 그런 다음 관리자는 현재 작업 영역이나 새 작업 영역을 새 관리자에게 할당할 수 있습니다.

새 관리자가 개체를 추가하면 원래 관리자도 이 개체를 볼 수 있습니다. 원래 관리자가 볼 수 있는 유효 개체 집합에는 자신이 만든 작업 영역에 추가된 모든 새 개체가 포함됩니다.

범위 지정 관리자는 정책 저장소에서 자신에게 권한이 있는 일부 개체를 관리할 수 없습니다. 관리 UI 는 할당된 작업 영역의 개체만 포함하는 것으로 표시됩니다.

범위 지정 관리자가 최상위 개체를 새로 추가하는 경우 유사한 범위가 지정된 다른 모든 관리자가 해당 개체를 즉시 사용할 수 있게 됩니다.

중요! 관리자는 동일하거나 낮은 권한으로만 다른 관리자를 생성할 수 있습니다. 예를 들어 GUI 및 보고서 권한이 있는 관리자는 로컬 API 권한이 아닌 GUI 및 보고서 권한이 있는 다른 관리자를 생성할 수 있습니다. 마찬가지로 관리자는 할당된 작업 영역에 정의된 것과 동일하거나 낮은 범위로만 관리자를 생성할 수 있습니다.

새 관리자가 개체를 추가하면 원래 관리자도 이 개체를 볼 수 있습니다. 원래 관리자가 볼 수 있는 유효 개체 집합에는 자신이 만든 작업 영역에 추가된 모든 새 개체가 포함됩니다.

참고: 관리자 계정의 범위만 작업 영역을 사용하여 지정할 수 있습니다. 레거시 관리자의 범위는 지정할 수 없습니다. 그러나 정책 저장소의 임의의 레거시 관리자 기록과 연결된 관리자 계정의 범위는 지정할 수 있습니다.

범위 지정 관리자를 구성할 때는 해당 관리자의 다음 특성을 고려하십시오.

- 관리자의 범위. 관리자가 모든 정책 데이터를 관리할 수 있는지 또는 작업 영역에 정의된 정책 데이터의 하위 집합을 관리할 수 있는지를 나타냅니다.
- 관리자가 작업을 수행하기 위해 필요한 권한. 이러한 권한을 식별하면 관리자에게 적절한 보안 범주를 쉽게 위임할 수 있습니다.
- 관리자가 응용 프로그램 보안 정책을 담당하는지 여부

작업 영역 만들기

범위 지정 관리자가 관리 권한을 갖는 최상위 수준 정책 개체(예: 도메인 또는 인증 체계)의 하위 집합을 정의하기 위한 작업 영역을 만들 수 있습니다.

참고: 작업 영역의 실제 콘텐츠는 최상위 콘텐츠 및 자식 개체로 구성됩니다. 예에는 도메인 아래의 영역 및 임의의 필수 개체(자동으로 포함됨)가 있습니다.

작업 영역의 콘텐츠는 동적입니다.

- 작업 영역의 콘텐츠는 언제든지 수정할 수 있습니다. 작업 영역에 할당된 모든 관리자는 새 개체를 즉시 사용할 수 있습니다. 제거된 모든 개체는 작업 영역에 할당된 관리자가 더 이상 사용할 수 없습니다.
- 범위 지정 관리자가 개체 유형을 수정할 권한이 있는 경우 해당 관리자는 작업 영역에서 개체를 생성할 수 있습니다. 작업 영역에 할당된 모든 관리자는 이러한 새 개체를 즉시 사용할 수 있습니다.

다음 단계를 수행하십시오.

1. SiteMinder 슈퍼 사용자나 적절한 권한이 있는 다른 관리자 계정을 사용하여 관리 UI에 로그인합니다.
2. "관리", "관리자", "작업 영역", "작업 영역 만들기"를 차례로 클릭합니다. "작업 영역 만들기" 페이지가 표시됩니다.
3. "일반" 섹션의 필드에 작업 영역의 이름과 설명을 입력합니다.
4. "구성원" 섹션에서 작업 영역에 필요한 정책 데이터의 하위 집합을 정의하는 개체를 추가합니다.

참고: 일반적으로 사용되는 일부 개체가 작업 영역에 추가되어 "구성원" 목록에 기본적으로 표시됩니다. 필요한 경우 이 개체를 제거할 수 있습니다.

- a. "조회"를 클릭합니다. "작업 영역 콘텐츠 선택" 페이지가 표시됩니다.
- b. "다음 유형의 개체 검색:" 드롭다운 메뉴에서 작업 영역에 추가할 개체 유형을 선택합니다. 필요한 경우 이름이나 설명 또는 둘 모두를 기준으로 검색 범위를 특정 개체로 좁힙니다.
- c. "검색"을 클릭합니다.

일치하는 개체의 목록이 표시됩니다.

참고: 로그인하는 데 사용한 관리자 계정이 자체적으로 범위 지정된 경우 일치하는 개체 목록은 사용 가능한 해당 개체로 제한됩니다.

- d. 작업 영역에 추가할 개체를 선택하고 "선택"을 클릭합니다. "작업 영역 만들기" 페이지가 다시 열립니다.

5. (선택 사항) 해당하는 "읽기 전용" 확인란을 선택하여 작업 영역 구성원에 대한 관리자 권한을 읽기 전용으로 설정합니다.
6. 제출을 클릭합니다.

"작업 영역 만들기" 태스크가 처리를 위해 제출됩니다. SiteMinder 는 작업 영역이 일관된 상태인지, 즉 작업 영역의 개체와 관련되어 있는 필수 개체가 모두 작업 영역에 있는지 확인합니다. 일관된 상태가 아니면 누락된 개체가 추가되고 작업 영역을 일관성 있게 만들기 위해 일부 개체가 자동으로 추가되었다는 정보 대화 상자가 표시됩니다.

관리자 만들기 및 작업 영역 할당

관리자 계정을 생성하고 이 계정이 관리할 수 있는 개체의 범위를 정의하는 작업 영역을 할당하여 범위 지정 관리자를 생성합니다.

다음 단계를 수행하십시오.

1. 슈퍼 사용어나 적절한 권한이 있는 다른 관리자 계정을 사용하여 관리 UI 에 로그인합니다.
2. "관리", "관리자"를 차례로 클릭합니다.
3. "관리자"를 클릭합니다.
4. "관리자 만들기"를 클릭합니다.
5. "일반" 아래에서 "조회"를 클릭합니다.
6. 검색 조건을 지정하고 "검색"을 클릭합니다.
7. 원하는 관리자를 선택하고 "선택"을 클릭합니다.
8. 작업 영역 드롭다운 목록에서 관리자의 범위를 지정하는 개체의 하위 집합을 정의하는 작업 영역을 선택합니다.
9. 다음 태스크 중 하나를 수행합니다.
 - 모든 권한을 위임하려면 "슈퍼 사용자"를 선택하고 "제출"을 클릭합니다.
 - 세분화된 권한을 위임하려면 다음 단계로 이동합니다.

10. "액세스 방법" 섹션에서 관리자가 정책 서버와 상호 작용할 수 있는 방법을 지정합니다. 관리자가 자신의 역할에 대해 필요한 방법을 선택하십시오.

예: 관리자가 XPSImport 및 XPSExport 도구를 사용하려는 경우 "가져오기 허용됨" 및 "내보내기 허용됨"을 선택합니다.

11. "권한" 섹션에서 "추가"를 클릭합니다.
12. 관리자에 대한 보안 범주를 선택한 다음 "확인"을 클릭합니다.
참고: 보안 범주는 특정 개체에 해당하는 하나 이상의 태스크로 구성됩니다.
13. 권한(읽기, 권한, 수정 및 전파)을 선택하여 "권한" 섹션에서 추가한 보안 범주에 적용합니다.
14. 제출을 클릭합니다.

범위 지정 관리자가 생성됩니다.

관리자의 범위가 지정되었는지 확인

관리자 계정에 작업 영역을 할당한 후 이 계정이 범위 지정된 개체의 하위 집합에만 액세스할 수 있는지 확인하십시오.

다음 단계를 수행하십시오.

1. 범위 지정 관리자 계정을 사용하여 관리 UI에 로그인합니다.
2. 관리 UI를 탐색하여 작업 영역에서 범위 지정된 개체의 하위 집합만 표시되는지 확인합니다.

범위 지정 관리자 계정을 만드는 데 필요한 태스크를 완료했습니다.

관리자 사용 사례

이 관리자 사용 사례에서는 다음에 대해 설명합니다.

- 관리자를 만드는 방법
- 기존 관리자가 새 관리자를 생성하고 권한을 부여할 수 있는 방법

이 시나리오에는 세 가지 관리자가 포함됩니다.

- SiteMinder 기본 관리자(슈퍼 사용자)
- Manager 관리자
- Junior 관리자

세 가지 관리자를 사용하여 다음 시나리오에 대해 설명합니다.

- 슈퍼 사용자가 **Manager** 관리자를 생성하는 경우
- 슈퍼 사용자가 작업 영역을 생성하고 할당하여 **Manager** 관리자의 범위를 지정하는 경우
- **Manager** 관리자가 **Junior** 관리자를 생성하는 경우
- **Junior** 관리자가 작업 영역을 생성하고 할당하여 **Junior** 관리자의 범위를 추가로 지정하는 경우

사용 사례 전체에서 다음 용어가 사용됩니다.

액세스 방법

관리자가 정책 서버와 상호 작용하는 방법을 지정합니다.

보안 범주

관리자가 정책 서버 개체 또는 도구를 관리하는 태스크를 실행할 수 있는 기능 영역을 지정합니다.

범위

관리자 권한이 모든 정책 개체로 확대되는지 또는 할당된 작업 영역에 정의된 개체의 하위 집합으로 확대되는지를 나타냅니다.

권한

관리자가 보안 범주 관련 태스크를 읽거나 관리하거나 전파하거나 실행할 수 있는지를 결정합니다.

권한

관리자의 전체 권한 집합을 정의합니다. 역할은 보안 범주, 범위 및 권한을 기반으로 합니다.

슈퍼 사용자가 Manager 관리자를 생성하는 경우

슈퍼 사용자는 외부 관리자 저장소에 대한 연결을 구성할 때 시스템 권한이 위임된 관리자입니다. 슈퍼 사용자는 다른 모든 관리자에 모든 범주, 권한 및 범위를 할당할 수 있습니다.

관리 UI 에서 슈퍼 사용자는 **Manager** 관리자라는 관리자를 생성합니다. 슈퍼 사용자가 권한을 할당하지 않는 한 처음에 **Manager** 관리자는 아무 권한이 없습니다.

슈퍼 사용자는 **Manager** 관리자에 다음을 할당합니다.

액세스 방법

GUI 허용됨

권한

보안 범주	권한*
에이전트 관리	V, M
응용 프로그램 관리	V, M, P
정책 관리	V, M, P

* 권한: 보기(V), 관리(M), 전파(P), 실행(X)(보고서 실행 전용)

참고: 전파 권한은 한 관리자가 다른 관리자에 범주를 할당할 수 있도록 허용합니다.

이 단계에서 **Manager** 관리자가 관리 UI 에 로그인하는 경우 정책 저장소의 모든 에이전트, 응용 프로그램 및 도메인을 보고 수정할 수 있습니다.

Manager 관리자가 관리자 계정을 만드는 경우 해당 계정에 응용 프로그램 관리 및 정책 관리 보안 범주만 할당할 수 있습니다.

슈퍼 사용자가 작업 영역을 생성하고 할당하여 Manager 관리자의 범위를 지정하는 경우

슈퍼 사용자가 Manager 관리자의 범위를 제한하여 이 관리자가 정책 데이터의 하위 집합만 관리할 수 있게 하려고 합니다. 이렇게 하기 위해 슈퍼 사용자는 먼저 다음 구성원을 포함하는 Workspace1 이라는 작업 영역을 생성합니다.

유형	이름
에이전트	Agent1
응용 프로그램	Application1
응용 프로그램	Application2
도메인	DomainB

그런 다음 슈퍼 사용자는 Manager 관리자의 관리자 기록을 편집하여 Workspace1 을 할당합니다.

이 단계에서 Manager 관리자가 로그인하면 Agent1, Application1, Application2 및 DomainB 의 정책만 보고 수정할 수 있습니다. 정책 저장소의 다른 에이전트, 응용 프로그램 및 도메인은 관리 UI 에 표시되지 않습니다.

Manager 관리자가 Junior 관리자를 생성하는 경우

이 사용 사례의 두 번째 부분에서는 특정 권한 집합이 할당된 관리자가 다른 관리자를 생성하는 방법을 보여 줍니다.

Manager 관리자가 Junior 관리자라는 관리자를 생성합니다. Manager 관리자가 Junior 관리자에 대한 보안 범주를 추가할 때 Manager 관리자에 전파 권한이 있는 다음 두 범주만 사용할 수 있습니다.

- 응용 프로그램 관리
- 정책 관리

참고: 전파 권한은 한 관리자가 다른 관리자에 범주를 할당할 수 있도록 허용합니다.

Manager 관리자가 Junior 관리자에 액세스 방법 및 권한을 할당하는 작업을 다음과 같이 진행합니다.

액세스 방법

GUI 허용됨

권한

보안 범주	권한*
응용 프로그램 관리	V
정책 관리	V, M

* 권한: 보기(V), 관리(M), 전파(P), 실행(X)(보고서 실행 전용)

이 단계에서 Junior 관리자가 관리 UI 에 로그인하는 경우 Application1 및 Application2 를 볼 수 있습니다. DomainB(기본적으로 Manager 관리자 범위로 제한)를 보고 수정할 수 있습니다.

Junior 관리자가 작업 영역을 생성하고 할당하여 Junior 관리자의 범위를 추가로 지정하는 경우

Manager 관리자가 Junior 관리자의 범위를 더 제한하여 이 관리자가 더 작은 정책 데이터의 하위 집합만 관리할 수 있게 하려고 합니다. 이렇게 하기 위해 Manager 관리자는 먼저 다음 구성원을 포함하는 Workspace2 라는 작업 영역을 생성합니다.

유형	이름
응용 프로그램	Application2
도메인	DomainB

그런 다음 Manager 관리자는 Junior 관리자의 관리자 기록을 편집하여 Workspace2 를 할당합니다.

이 단계에서 Manager 관리자가 로그인하면 Application2 만 볼 수 있고 DomainB 의 정책을 보고 수정할 수 있습니다. 정책 저장소의 다른 응용 프로그램 및 도메인은 관리 UI 에 표시되지 않습니다.

레거시 관리자를 만드는 방법

레거시 관리자를 생성하려면 다음 단계를 완료하십시오.

1. [레거시 관리자 고려 사항을 검토합니다.](#) (페이지 78)
2. [레거시 관리자 기록을 생성합니다](#) (페이지 78).
3. [관리 UI 권한을 위임합니다](#) (페이지 81).

레거시 관리자 고려 사항

다음 조건 중 하나 이상을 충족하는 경우 이 프로세스가 적용됩니다.

- 정책 관리 API 를 사용하여 SiteMinder 개체를 관리하기 위해 레거시 관리자가 필요합니다.
- 트러스트된 호스트 관리자의 기능을 수행하기 위해 레거시 관리자가 필요합니다.

참고: 정책 저장소가 관리자 아이덴티티의 원본으로 구성된 경우(기본값) 레거시 관리자는 또한 관리 UI 에 액세스할 수도 있습니다. 외부 관리자 저장소가 구성된 후에는 더 이상 레거시 관리자 계정이 관리 UI 에 액세스할 수 없습니다.

레거시 관리자 기록 만들기

정책 저장소에 레거시 관리자 아이덴티티를 저장하려면 레거시 관리자 기록을 만드십시오.

다음 단계를 수행하십시오.

1. "관리", "관리자"를 차례로 클릭합니다.
2. "레거시 관리자"를 클릭합니다.
3. "레거시 관리자 만들기"를 클릭합니다.
4. "확인"을 클릭합니다.

5. "일반" 섹션에서 다음 태스크를 수행하십시오.

a. "이름" 필드에 고유 ID 를 입력합니다.

회사 표준을 따르는 고유 ID 를 입력하는 것이 좋습니다. 회사 표준을 따르면 다음의 이점이 있습니다.

- 관리자가 새로운 자격 증명 집합을 기억할 필요가 없어집니다.
- 레거시 관리자 ID 가 외부 저장소의 고유 ID 와 일치하기 때문에 외부 관리자 저장소로의 전환이 용이합니다.

b. "설명" 필드에 사용자의 전체 이름을 입력합니다.

값은 사용자가 관리 UI 에 로그인할 때 표시 이름으로 나타납니다. 표시 이름은 로그인한 사용자를 식별합니다.

예: Joe Smith 를 입력하면 관리 UI 표시 이름은 다음 형식으로 표시됩니다.

로그인한 사용자: Joe Smith

6. SiteMinder 데이터베이스 옵션 단추를 선택된 상태로 둡니다.

7. 해당 필드에 관리자 암호를 입력합니다.

8. 다음 항목 중 하나를 수행합니다.

■ 다음 태스크에 대한 권한만 포함하여 레거시 관리자를 만드는 경우에는 "제출"을 클릭합니다.

- 관리 UI 사용
- 정책 서버 도구 사용

관리자 기록이 생성됩니다.

■ 이전 태스크와 다음 항목 중 하나를 위한 권한을 포함하여 레거시 관리자를 만드는 경우에는 다음 단계로 이동합니다.

- 정책 관리 API 관리
- 트러스트된 호스트 관리자 역할 수행

9. "관리자 권한" 섹션에서 "시스템 또는 도메인" 옵션을 선택합니다.

참고: 레거시 관리자를 생성하고 나면 관리 UI 에 권한을 위임합니다.

시스템

관리자는 정책 관리 API 의 모든 정책 도메인에 대한 액세스 권한을 가집니다. "시스템"을 선택하면 "태스크" 섹션이 표시됩니다.

도메인

관리자는 정책 관리 API 에서 정책 도메인의 특정 하위 집합에 대한 액세스 권한을 가집니다. "도메인"을 선택하면 "태스크" 및 "범위" 섹션이 표시됩니다. "태스크" 섹션에는 수행할 수 있는 관리 태스크가 나열됩니다. "범위" 섹션에는 관리할 수 있는 사용 가능 도메인이 나열됩니다.

참고: "레거시 관리자 만들기" 화면의 "범위" 섹션은 작업 영역을 사용한 관리자 계정 범위 지정과 관련이 없습니다.

10. 관리자가 수행할 수 있는 태스크를 선택합니다.

- 시스템 관리자의 경우 다음 태스크 중 하나 이상을 선택합니다.
 - 시스템 및 도메인 개체 관리
 - 사용자 관리
 - 키 및 암호 정책 관리
 - 트러스트된 호스트 등록
- 도메인 관리자의 경우 다음 태스크를 수행합니다.
 - a. 다음 태스크 중 하나 이상을 선택합니다.
 - 도메인 개체 관리
 - 사용자 관리
 - 암호 정책 관리
 - b. "범위" 섹션에서 관리자가 관리해야 하는 도메인을 선택합니다.

11. 제출을 클릭합니다.

레거시 관리자를 생성했습니다.

참고: 정책 저장소의 레거시 관리자 기록과 연결된 관리자 계정은 관리 UI 액세스를 지원하는 용도로도 생성됩니다.

관리 UI 권한 위임

레거시 관리자가 생성된 경우 정책 저장소의 동일한 기록과 연결된 관리자 계정도 생성됩니다. 이 관리자 계정은 레거시 관리자에 대해 지정된 설정에 해당하는 관리 UI 액세스 권한으로 구성됩니다.

액세스 권한에 영향을 주는 레거시 관리자 설정을 변경하면 해당 변경 내용은 연결된 관리자 계정으로 자동 전파됩니다.

또한 연결된 관리자 설정을 직접 수정하여 관리자 계정에서 사용할 수 있는 세분화된 관리 UI 액세스 권한의 이점을 활용할 수 있습니다.

참고: 연결된 관리자 계정 설정에 대한 변경 내용은 다시 레거시 관리자로 전파되지 *않습니다*. 또한 연결된 관리자가 변경된 후에는 레거시 관리자에 대한 변경 내용이 더 이상 관리자 계정으로 전파되지 않습니다.

관리자 비활성화

계정을 삭제하지 않고 관리자를 일시적으로 비활성화할 수 있습니다. 계정을 비활성화하면 계정을 다시 생성할 필요 없이 권한을 복원할 수 있습니다.

관리자를 비활성화하려면

1. "관리", "관리자"를 차례로 클릭합니다.
2. "관리자"를 클릭합니다.
"관리자" 페이지가 표시됩니다.
3. 검색 조건을 지정하고 "검색"을 클릭합니다.
조건과 일치하는 사용자가 표시됩니다.
4. 비활성화할 사용자의 이름을 클릭합니다.
"관리자 보기" 페이지가 표시됩니다.
5. "수정"을 클릭합니다.
설정과 컨트롤이 활성화됩니다.

6. "사용 안 함"을 선택합니다.
7. "제출"을 클릭합니다.

관리자가 비활성화됩니다.

이 절차를 반복하여 "사용 안 함" 옵션을 선택 취소하고 변경 내용을 제출하면 언제든지 관리자를 활성화할 수 있습니다.

레거시 관리자 비활성화

계정을 삭제하지 않고 레거시 관리자를 일시적으로 비활성화할 수 있습니다. 계정을 비활성화하면 계정을 다시 생성할 필요 없이 권한을 복원할 수 있습니다.

다음 단계를 수행하십시오.

1. "관리", "관리자"를 차례로 클릭합니다.
2. "레거시 관리자"를 클릭합니다.
3. 검색 조건을 지정하고 "검색"을 클릭합니다.
4. 비활성화할 사용자의 이름을 클릭합니다.
5. "수정"을 클릭하여 설정을 활성화합니다.
6. 태스크의 선택을 취소하고 "제출"을 클릭합니다.

이제 레거시 관리자는 더 이상 정책 관리 API 또는 트러스트된 호스트 관리자 등의 기능에 액세스할 수 없습니다.

7. (선택 사항) 관리 UI 에서 레거시 관리자가 권한을 보유한 경우 다음 작업을 수행하십시오.
 - a. "관리", "관리자"를 차례로 클릭합니다.
 - b. "관리자"를 클릭합니다.
 - c. 검색 조건을 지정하고 "검색"을 클릭합니다.
 - d. 권한을 제거한 레거시 관리자의 이름을 클릭합니다.
 - e. "수정"을 클릭하여 설정을 활성화합니다.
 - f. "사용 안 함"을 선택하고 "제출"을 클릭합니다.레거시 관리자가 비활성화됩니다.

다음 작업을 수행하여 레거시 관리자를 활성화할 수 있습니다.

- 시스템 또는 도메인 특정 태스크가 포함되도록 레거시 관리자 계정 수정
- 해당되는 경우 각 관리자 기록에서 "사용 안 함" 확인란 선택 취소

관리자 액세스 권한 복원

정책 서버에 대한 모든 액세스 권한이 있는 관리자는 관리자 계정이 실수로 수정되거나 삭제된 경우 권한을 복원할 수 있습니다. 이러한 권한을 가진 두 관리자는 다음과 같습니다.

- 기본 SiteMinder 슈퍼 사용자 계정(siteminder). 정책 저장소에 관리자 아이덴티티를 저장하는 경우 siteminder 계정을 사용하여 권한을 복원하십시오.
- 외부 관리자 저장소 연결이 구성될 때 설정된 슈퍼 사용자 계정. 외부 저장소에 관리자 아이덴티티를 저장하는 경우 외부 슈퍼 사용자 계정을 사용하여 권한을 복원하십시오.

기본 관리자 계정에 액세스할 수 없는 경우 다음 작업을 수행하십시오.

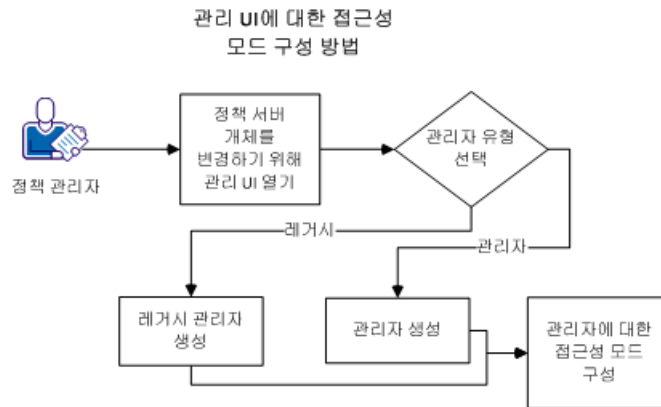
- smreg 유틸리티를 사용하여 기본 SiteMinder 슈퍼 사용자 계정의 암호를 변경하십시오.
- XPSSecurity 유틸리티를 사용하여 외부 관리자 저장소에 있는 임의 사용자를 슈퍼 사용자로 설정하십시오.

참고: 이러한 유틸리티의 사용에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

관리 UI에 대한 접근성 모드를 구성하는 방법

이 제품은 접근성을 개선하도록 구성할 수 있습니다.

다음 그림에서는 관리 UI에 대한 접근성 모드를 구성하는 방법을 보여줍니다.



다음 단계를 수행하십시오.

1. [관리 UI를 열어 정책 서버 개체를 변경합니다](#) (페이지 85).
2. 다음 목록에서 [관리자 유형을 선택합니다](#) (페이지 85).
 - [관리자를 생성합니다](#) (페이지 86).
 - [레거시 관리자를 생성합니다](#) (페이지 87).
3. [관리자에 대한 접근성 모드를 구성합니다](#) (페이지 87).

정책 서버 개체 변경

관리 UI를 열어 정책 서버의 개체를 변경합니다.

다음 단계를 수행하십시오.

1. 브라우저에서 다음 URL을 엽니다.

`https://host_name:8443/iam/siteminder/adminui`

host_name

정규화된 관리 UI 호스트 시스템 이름을 지정합니다.

2. "사용자 이름" 필드에 SiteMinder 슈퍼 사용자 이름을 입력합니다.
3. "암호" 필드에 SiteMinder 슈퍼 사용자 계정 암호를 입력합니다.

참고: 슈퍼 사용자 계정 암호에 달러-기호(\$) 문자가 있으면 달러 기호 문자의 각 인스턴스를 \$DOLLAR\$로 바꾸십시오. 예를 들어 SiteMinder 슈퍼 사용자 계정 암호가 \$password 이면 "암호" 필드에 \$DOLLAR\$password를 입력하십시오.

4. "서버" 드롭다운 목록에 올바른 서버 이름 또는 IP 주소가 나타나는지 확인합니다.
5. "로그인"을 선택합니다.

관리자 유형 선택

다음과 같은 유형의 관리자를 사용할 수 있습니다.

- 계정 및 자격 증명이 해당 제품 이외에 외부의 타사 데이터베이스에 저장되는 관리자
- 계정 및 자격 증명이 정책 저장소 내부에 저장되는 레거시 관리자

원하는 유형의 관리자를 선택하여 접근성 모드를 사용하도록 구성할 수 있습니다. 그러나 관리자를 생성하려면 [먼저 외부 데이터베이스를 구성해야 합니다](#) (페이지 50).

다음 중 접근성 모드를 구성할 관리자 유형 *하나*를 선택하십시오.

- [관리자](#) (페이지 86)
- [레거시 관리자](#) (페이지 87)

관리자 생성

관리 UI에서 레거시 관리자를 생성합니다. 이 레거시 관리자는 제품의 접근성 모드를 사용합니다.

다음 단계를 수행하십시오.

1. "관리", "관리자"를 차례로 선택합니다.
2. "관리자"를 선택합니다.
3. "관리자 만들기"를 선택합니다.
4. "일반"에서 "조회"를 선택합니다.
5. 검색 기준을 지정하고 "검색"을 선택합니다.
6. 원하는 관리자를 선택하고 "선택"을 선택합니다.
7. "제출"을 선택합니다.
8. [이 관리자에 대한 접근성 모드를 구성합니다](#) (페이지 87).

레거시 관리자 생성

관리 UI에서 레거시 관리자를 생성합니다. 이 레거시 관리자는 제품의 접근성 모드를 사용합니다.

다음 단계를 수행하십시오.

1. 관리 UI에서 "관리", "관리자", "레거시 관리자"를 차례로 선택합니다.
2. "레거시 관리자 만들기"를 선택합니다.
3. 다음 옵션 단추가 선택되어 있는지 확인합니다.

Create a new object of type Legacy Administrator(레거시 관리자 유형의 새 개체 만들기)

4. "OK"를 선택합니다.
5. "이름" 필드를 선택하고 레거시 관리자의 사용자 이름을 입력합니다.
6. 다음 옵션 단추가 선택되어 있는지 확인합니다.

SiteMinder 데이터베이스

7. "암호" 필드를 선택하고 레거시 관리자의 암호를 입력합니다.
8. "암호 확인"을 선택하고 7 단계에서 입력한 암호를 다시 입력합니다.
9. 다음 옵션 단추를 선택합니다.

시스템

10. "제출"을 선택합니다.
11. 이 관리자에 대한 접근성 모드를 구성합니다.

관리자에 대한 접근성 모드 구성

관리자를 생성한 후 해당 관리자에 대한 접근성 모드를 구성합니다.

다음 단계를 수행하십시오.

1. 관리 UI에서 "관리", "관리자", "관리자"를 차례로 선택합니다.
2. 접근성 모드를 구성할 레거시 관리자의 오른쪽에 있는 편집 아이콘을 선택합니다.
3. 다음 확인란을 선택합니다.

GUI 허용됨

4. "추가"를 선택합니다.

5. 다음 단계를 수행하여 접근성 모드를 구성합니다.
 - a. "권한 만들기" 화면에서 다음 표의 보안 범주 열에 표시된 항목에 해당하는 확인란을 선택합니다.
 - b. 보안 범주 열에 해당하는 확인란을 모두 선택한 후 "확인"을 선택합니다.
 - c. 다음 표에 나타난 대로 권한 열(V, M, X)에 대한 확인란을 선택합니다.
 6. "제출"을 선택합니다.
- 접근성 모드가 구성되고 확인 메시지가 나타납니다. 접근성 모드가 필요한 관리자는 이 관리자 계정을 사용하여 관리 UI에 액세스할 수 있습니다.

보안 범주	V	M	X	B	R	P
관리자 관리	X	X				
에이전트 관리	X	X				
에이전트 유형 관리	X	X				
응용 프로그램 관리	X	X				
응용 프로그램 역할 관리	X	X				
인증 관리	X	X				
디렉터리 관리	X	X				
도메인 관리	X	X				
식 관리	X	X				
전역 정책 관리	X	X				
호스트 관리	X	X				
레거시 도메인 관리	X	X				
매핑 관리	X	X				
암호 정책 관리	X	X				
정책 관리	X	X				
보고서: 사용자별 작업			X			
보고서: 관리 작업			X			

보안 범주	V	M	X	B	R	P
보고서: 응용 프로그램			X			
보고서: 사용자별 응용 프로그램			X			
보고서: 거부된 권한			X			
보고서: 거부된 리소스			X			
보고서: 역할별 정책			X			
보고서: 보호된 리소스			X			
보고서: 리소스 작업			X			
보고서: 사용자별 리소스			X			
보고서: 응용 프로그램별 역할			X			
보고서: 리소스별 역할			X			
보고서: 리소스별 사용자			X			
보고서: 역할별 사용자			X			
사용자 관리	X	X				
변수 관리	X	X				

제 4 장: 사용자 세션

사용자 세션 개요

이 제품은 다중 계층 응용 프로그램 전반에서 일관된 사용자 세션을 유지하고 관리합니다. 응용 프로그램과 온라인 비즈니스는 갈수록 위치의 제한을 받지 않고 환경과 응용 프로그램 기술 및 보안 요구 사항은 다양하기 때문에 사용자 세션 정보를 유지 관리하는 것은 매우 중요합니다.

비영구 및 영구 쿠키

표준 SiteMinder 세션 쿠키는 비영구 쿠키입니다. 비영구 쿠키는 웹 브라우저의 메모리 내에서만 유지 관리되는 쿠키입니다. 사용자가 브라우저를 닫으면 세션 쿠키가 삭제되고 사용자가 실제로 로그아웃됩니다.

쿠키를 웹 브라우저에서 유지 관리하는 것에 추가하여, 하드 디스크에 기록되는 쿠키를 사용하도록 SiteMinder 를 구성할 수 있습니다. SiteMinder 쿠키를 하드 디스크에서 유지 관리하는 것을 영구 쿠키라고 합니다. 영구 쿠키를 사용하면 사용자가 브라우저를 닫았다고 다시 열 경우 로그인된 상태가 유지됩니다.

비영구 및 영구 세션

SiteMinder에서는 영구 세션을 구성하여 Windows 보안 컨텍스트 기능과 페더레이션 웹 서비스에 대한 지원을 제공할 수도 있습니다. 영구 세션은 SiteMinder 쿠키가 SiteMinder 세션 저장소, 웹 브라우저의 메모리 및 하드 디스크(선택적)에서 유지 관리되는 세션입니다.

영구 세션을 구현하기 전에 다음 사항을 고려하십시오.

- 영구 세션은 영역별로 구성됩니다.
- 영구 세션은 필요한 경우에만 사용해야 합니다. 세션 서비스를 사용하여 세션을 유지 관리할 경우 시스템 성능에 영향을 주게 됩니다.

참고: 세션 서비스가 사용되도록 설정하고 구성하는 방법에 대한 자세한 내용은 "정책 서버 관리 안내서"를 참조하십시오.

세션 티켓

SiteMinder 는 세션 티켓을 사용하여 세션 관리를 구현합니다. 세션 티켓은 사용자에게 대한 기본 정보와 해당 사용자에게 대한 인증 정보를 포함합니다. 세션 티켓은 싱글 사인온 SiteMinder 환경의 모든 사이트에서 사용자 세션을 식별합니다. 세션 티켓은 암호화되며 정책 서버만 세션 티켓을 읽고 유효성을 검사할 수 있습니다. SiteMinder 에이전트는 세션 티켓을 사용하여 사용자를 식별하고 세션 정보를 정책 서버에 제공합니다.

세션 티켓이 처리되는 방식은 세션이 영구적인지, 비영구적인지에 따라 달라집니다.

참고: 비영구 및 영구 쿠키는 사용자의 SiteMinder 세션이 비영구적인지 또는 영구적인지와는 관련이 없습니다.

비영구 세션

웹 에이전트는 세션 티켓을 쿠키에 저장합니다. 쿠키는 사용자 세션 데이터를 포함하며 사용자 고유의 데이터는 쿠키 자체에 보관되지 않습니다. 에이전트는 쿠키 유효성을 검사하고 세션 시간 만료를 적용합니다.

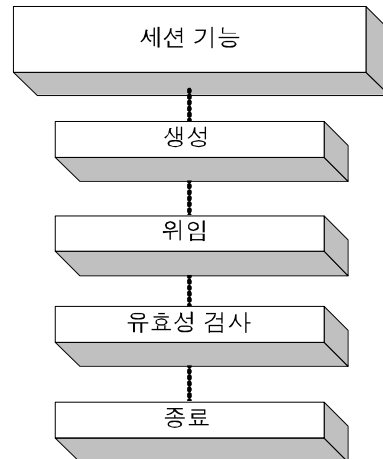
영구 세션

에이전트는 세션 티켓을 세션 저장소 데이터베이스에 저장하며 가능한 경우 클라이언트의 선택적 쿠키에도 저장합니다.

세션 티켓 데이터는 사용자 세션 데이터가 포함된 웹 에이전트 캐시에서 인덱스로 사용됩니다. 쿠키가 작성되어도 사용자 고유의 데이터는 쿠키 자체에 보관되지 않습니다. 에이전트는 세션 유효성을 검사하고 세션 시간 만료를 적용합니다.

SiteMinder 에서 사용자 세션이 관리되는 방식

SiteMinder 는 사용자 세션을 자동으로 관리하며 다음 그림에 표시된 것처럼 사용자 세션의 수명 주기 동안 많은 기능을 수행합니다.



세션 생성

사용자가 응용 프로그램에 성공적으로 로그인한 경우 세션을 설정합니다. 사용자가 인증에 실패하면 세션이 설정되지 않습니다.

세션 위임

응용 프로그램 환경 간에 세션 정보를 전달합니다. 응용 프로그램의 로직이 여러 응용 프로그램 계층에 걸쳐 있는 경우 세션 정보의 위임이 필요합니다.

세션 유효성 검사

세션 티켓을 확인하여 사용자 세션이 활성 상태인지, 즉, 만료되거나 종료되지 않았는지 확인합니다.

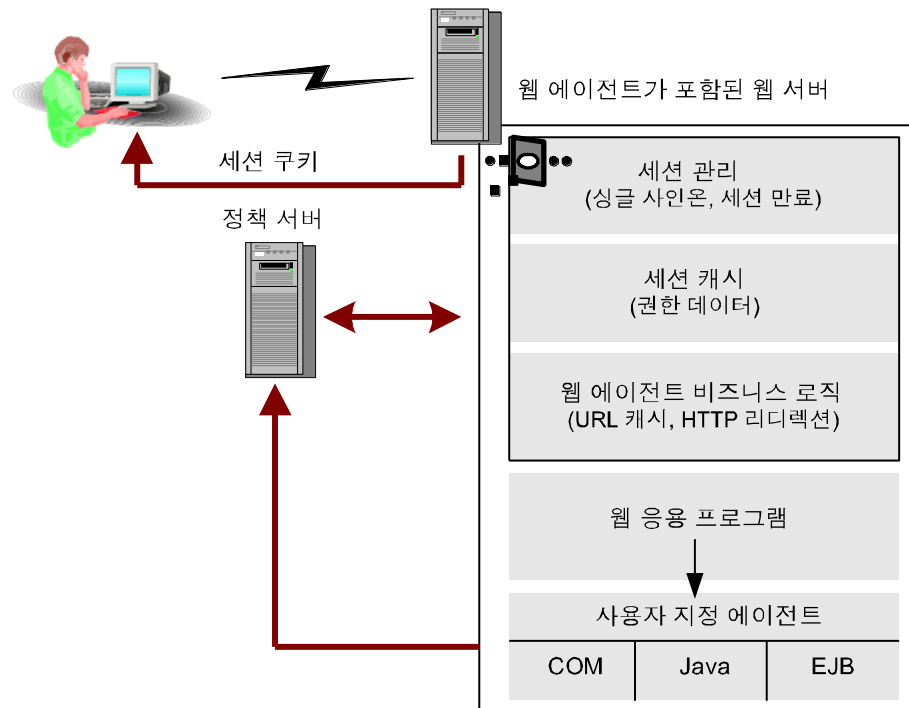
세션 종료

다음 이벤트 중 하나가 발생할 경우 사용자 세션을 종료합니다.

- 사용자가 로그아웃한 경우
- 구성된 세션이 만료된 경우
- SiteMinder 시스템 관리자가 사용자를 비활성화한 경우

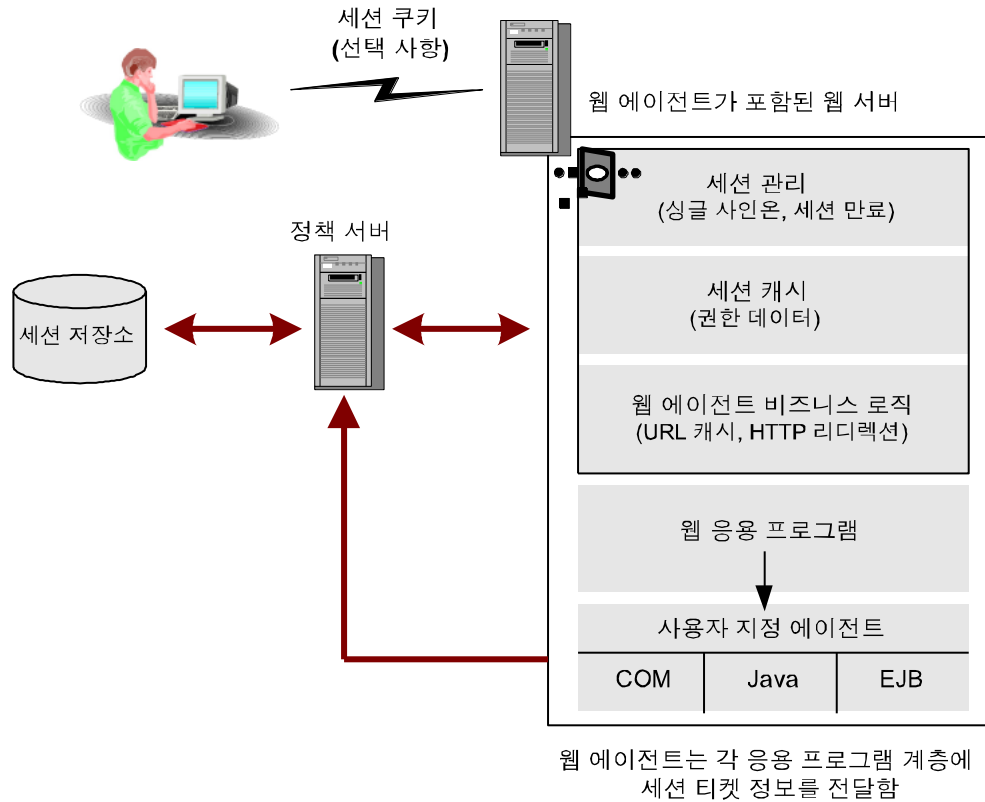
사용자가 로그아웃하거나 사용자 세션이 만료된 경우 새 세션을 생성하려면 다시 로그인해야 합니다. 수동으로 비활성화된 사용자는 세션을 다시 시작할 수 없습니다.

다음 그림은 SiteMinder가 비영구 세션을 관리하는 방식을 보여 줍니다.



웹 에이전트는 각 응용 프로그램 계층에 세션 티켓 정보를 전달함

다음 다이어그램에서는 SiteMinder가 영구 세션을 관리하는 방식을 보여줍니다.



사용자 세션이 시작되는 방식

사용자 세션은 사용자가 로그인하고 SiteMinder에 의해 인증될 때 시작됩니다. 정책 서버는 세션 티켓을 발행합니다. 이 세션 티켓은 해당 사용자 세션에 대한 이후의 모든 에이전트 요청에 필요합니다. 더 높은 보호 수준으로 인해 세션 중에 사용자가 다시 인증해야 할 경우에도 기존 세션이 유지됩니다.

세션은 사용자가 로그오프하거나 세션이 만료되거나 관리자가 사용자를 비활성화하여 세션이 종료될 때까지 활성 상태로 유지됩니다.

영역 간에 세션이 유지되는 방식

리소스에 대한 액세스를 요청하는 사용자는 리소스를 포함하는 영역의 컨텍스트 내에 생성된 세션을 갖습니다. 영역과 연결된 인증 체계는 사용자가 리소스에 액세스하려면 제공해야 하는 자격 증명의 유형을 결정합니다.

이 인증 컨텍스트는 다음과 같은 구성 요소를 정의하는 독점 HTTP 헤더를 사용하여 제품 환경의 모든 웹 서버에서 사용 가능하게 됩니다.

- 사용 중인 인증 체계
- 사용자가 인증하는 네임스페이스

생년월일 또는 전화 번호와 같은 사용자에 대한 추가 정보를 묻기 위해 정책에서 응답 특성을 구성할 수 있습니다.

제품에서 싱글 사인온이 구성된 경우 인증 체계는 또한 보호 수준을 가질 수 있습니다. 관리자는 이러한 보호 수준을 할당합니다. 수준 범위는 1 - 1000 사이입니다. 1은 보안 수준이 가장 낮고 1000은 가장 높습니다. 이러한 보호 수준을 통해 관리자는 더 안전하고 유연한 방식으로 싱글 사인온을 구현할 수 있습니다.

한 영역에서 인증된 사용자는 다른 영역의 세션에 대해 유효성 검사될 수 있습니다. 다른 영역의 보호 수준은 원래 영역보다 낮거나 같습니다. 보호 수준이 낮거나 같으면 해당 사용자는 다시 인증할 필요가 없습니다. 원래 사용자 세션은 유효한 상태로 유지됩니다. 더 높은 보호 수준을 갖는 인증 체계와 연결된 리소스에 대한 액세스를 요청하는 사용자는 본인의 자격 증명을 다시 입력해야 합니다. 원래 세션은 종료되고 새 세션이 생성됩니다.

싱글 사인온 환경에 대한 보호 수준을 구성하려면 [인증 체계](#) (페이지 287)를 참조하십시오.

여러 쿠키 도메인 간에 세션이 유지되는 방식

제품은 서로 다른 웹 서버 플랫폼이 공존하는 환경에서 여러 쿠키 도메인 간의 싱글 사인온을 지원합니다. 사용자가 `companyA.com` 을 방문한 다음 `companyB.com` 으로 이동하더라도 세션 정보는 그대로 유지됩니다. 여러 쿠키 도메인에서 세션 정보를 유지하려면 에이전트에서 싱글 사인온을 구성하십시오. 싱글 사인온이 구성되어 있으면 싱글 사인온 환경의 모든 에이전트와 서버에서 세션 정보가 포함된 쿠키를 사용할 수 있습니다.

이러한 쿠키 도메인은 사용자가 한 쿠키 도메인에서 인증된 후 정보를 다시 입력할 필요 없이 다른 쿠키 도메인으로 이동할 수 있도록 해 줍니다.

싱글 사인온은 쿠키 공급자를 사용하여 구현됩니다. 싱글 사인온 환경에서 쿠키 공급자는 웹 에이전트의 확장입니다.

서로 다른 쿠키 도메인에 있는 리소스에 대해 도메인 간 로그아웃이 가능하게 하려는 경우 개별 쿠키 도메인의 영역에 대해 영구 세션이 사용되도록 설정할 수 있습니다. 사용자가 한 도메인에서 로그아웃하면 정책 서버는 사용자 세션을 종료하는 로그아웃 이벤트를 전송합니다.

참고: 여러 쿠키 도메인 간의 싱글 사인온을 사용하기 위해 싱글 사인온 환경에서 동일한 사용자 디렉터리를 사용할 필요는 없습니다. 하지만 관리 UI에 구성된 사용자 디렉터리 연결은 각 쿠키 도메인에서 디렉터리 개체 이름을 공유해야 합니다.

사용자 세션의 유효성이 검사되는 방식

에이전트는 아직 활성화되어 있는지 여부를 검사하여 사용자 세션의 유효성을 검사합니다. 에이전트는 먼저 에이전트의 세션 캐시에서 세션 정보를 확인합니다. 에이전트가 캐시에 있는 쿠키 및 정보를 읽을 때 에이전트는 세션의 유효성을 검사합니다. 그렇지 않으면 에이전트는 정책 서버에 연결하여 사용자의 아이덴티티를 검사합니다. 에이전트는 또한 다른 세션 및 권한 부여 정보도 수집합니다.

사용된 것보다 더 높은 보호 수준을 갖는 리소스에 액세스하는 사용자는 또 다른 인증이 발생하더라도 본인의 세션 정보를 유지합니다.

세션 정보가 위임되는 방식

세션 티켓을 사용하여 SiteMinder 설치 환경의 응용 프로그램 계층 간에 사용자 세션을 위임할 수 있습니다. 세션 티켓은 응용 프로그램 계층 간에 사용자 아이덴티티가 전달되는 메커니즘입니다. 각 응용 프로그램은 세션 티켓을 받은 후 권한 부여를 위해 정책 서버를 호출할 수 있습니다.

SiteMinder 설치 환경에서 사용자 지정 에이전트를 사용하는 경우 사용자 지정 에이전트는 세션 티켓의 정보에 대한 액세스 권한이 있어야 세션 정보를 관리할 수 있습니다.

웹 에이전트는 위임에 세션 티켓을 사용할 뿐 아니라 세션 관리에 사용할 수 있는 기본 HTTP 헤더 집합을 생성합니다. 이러한 기본 헤더는 EJB(Enterprise Java Beans) 및 COM(구성 요소 개체 모델) 기반 계층과 같은 다양한 비즈니스 응용 프로그램 계층 간에 전달될 수 있습니다. 이러한 헤더에는 고유 세션 ID와 필요한 경우 유니버설 ID가 포함됩니다. 세션 ID는 활성 사용자 세션을 식별합니다.

유니버설 ID는 SiteMinder 환경의 응용 프로그램에 대해 사용자를 식별합니다. 이 ID는 일반적으로 사용자 로그인 ID와는 다르며 전화 번호 또는 고객 계정 번호 같은 다른 유형의 고유 식별자입니다. 유니버설 ID를 사용하면 이전 응용 프로그램과 새 응용 프로그램을 쉽게 식별할 수 있습니다. 유니버설 ID는 응용 프로그램에 관계없이 사용자 ID를 자동으로 전송하며 응용 프로그램에 기본 제공됩니다. 기본 제공 ID는 지속적으로 변경되는 사용자 디렉터리와는 별개의 사용자 식별 방법을 응용 프로그램에 제공합니다.

일관된 사용자 세션 관리를 위해 세션 ID와 유니버설 ID는 SiteMinder 환경의 모든 응용 프로그램 간에 공유됩니다.

세션 시간 만료

각 사용자 세션에는 세션 시간 만료 정보가 포함되어 있습니다. 시간 만료 값은 활성 세션의 길이와 세션이 무효화되기 전까지 비활성 상태로 유지될 수 있는 시간을 지정합니다. 세션 시간 만료는 영역별로 다음과 같은 시간 만료 옵션을 사용하여 구성하십시오.

이름	용도
최대 시간 만료 (모든 세션)	웹 에이전트가 사용자에게 재인증을 요청하기 전까지 사용자 세션이 활성 상태로 유지될 수 있는 최대 시간을 지정합니다. WebAgent-OnAuthAccept-Session-MaxTimeout 응답 특성을 사용하여 이 설정을 재정의할 수 있습니다.

이름	용도
휴식 시간 만료 (모든 세션)	웹 에이전트가 세션을 종료하기 전까지 사용자 세션이 휴식 상태로 유지될 수 있는 시간을 지정합니다. 세션이 만료되면 사용자가 다시 인증되어야 합니다. 참고: 영구 세션의 경우 이 값은 "세션 유효성 검사 기간"의 값보다 커야 합니다. WebAgent-OnAuthAccept Session-Idle-Timeout 응답 특성을 사용하여 이 설정을 재정의할 수 있습니다.
세션 유효성 검사 기간 (영구 세션)	에이전트가 세션 유효성을 검사하기 위해 정책 서버를 호출하는 최대 간격을 지정합니다(영구 세션에만 해당). 세션 유효성 검사 호출은 사용자가 계속 활성 상태임을 정책 서버에 알리고 또한 사용자 세션이 아직 유효한지 확인하는 두 가지 기능을 수행합니다.

에이전트 키 관리 및 세션 시간 만료가 조정되는 방식

에이전트는 키를 사용하여 제품이 보호하는 환경의 에이전트 간에 전달되는 쿠키를 암호화하고 해독합니다. 정책 서버와 통신하는 모든 에이전트에 대해 모든 키가 동일한 값으로 설정되어 있어야 합니다.

정기적으로 변경되는 동적 에이전트 키를 사용하도록 제품 설치를 환경을 구성할 수 있습니다. 동적 키 롤오버를 사용하면 동적 키를 정기적으로 업데이트하여 암호화된 쿠키의 보안을 강화할 수 있습니다. 관리 UI의 "롤오버 빈도 설정" 대화 상자에서 키 롤오버가 수행되는 시간을 지정하십시오. 제품 설치 환경 전체에서 키 업데이트를 수행하는 데는 최대 3분이 소요될 수 있습니다.

세션 시간 만료를 고려하여 키 업데이트를 조율하십시오. 그렇지 않으면 세션 정보가 수록된 쿠키가 무효화될 수 있습니다. 조직에서 정책을 설계하는 사람과 동적 키 롤오버를 구성하는 사람이 다를 수 있기 때문에 이 조정은 중요합니다.

세션 만료 시간은 구성된 에이전트 키 롤오버 간격의 두 배 이하여야 합니다. 세션 만료 전에 에이전트 키 롤오버가 2 회 발생하면 첫 번째 키 롤오버 전에 작성된 모든 쿠키는 무효화됩니다. 세션 만료 시간이 지정된 롤오버 간격보다 큰 경우 사용자 세션이 종료되기 전에 해당 사용자에게 ID 인증이 요청될 수 있습니다.

예를 들어, 매 3 시간마다 키 롤오버가 발생하도록 구성하는 경우 최대 세션 시간 만료를 6 시간으로 설정하십시오. 이렇게 설정하면 여러 키 롤오버가 세션 쿠키를 무효화하지 않도록 방지할 수 있습니다.

사용자 세션이 종료되는 방식

사용자 세션은 다음과 같은 경우 종료됩니다.

- 사용자가 로그아웃합니다.
- 세션 만료 시간이 만료됩니다.
- 시스템 관리자가 사용자를 비활성화합니다.

Windows 사용자 보안 컨텍스트

Windows 네트워크에서 보안 컨텍스트란 사용자 아이덴티티와 인증 정보로 정의됩니다. 응용 프로그램(예: Microsoft Exchange Server 또는 SQL Server)이 Microsoft 액세스 제어 목록(ACL) 또는 기타 도구를 사용하여 보안을 제공하려면 사용자 보안 컨텍스트가 필요합니다.

참고: Windows 보안 컨텍스트에서 사용자 저장소는 Active Directory(AD)여야 합니다.

에이전트는 IIS 웹 서버(Windows 2000 플랫폼)의 웹 리소스에 액세스할 수 있도록 Windows 사용자 보안 컨텍스트를 제공할 수 있습니다. 사용자 보안 컨텍스트를 설정하면 서버는 이 아이덴티티를 사용하여 액세스 제어 메커니즘을 적용할 수 있습니다.

Windows 사용자 보안 컨텍스트를 제공함으로써 제품은 다음과 같은 이점이 있습니다.

- 두 수준의 보안

제품의 모든 기능을 사용하여 웹 리소스를 보호하면서 동시에 Microsoft의 보안 도구를 사용하여 응용 프로그램을 보호하는 추가적인 이점을 얻을 수 있습니다.

- 에이전트는 다양한 웹 브라우저와 통신할 수 있을 뿐 아니라 Windows 보안 컨텍스트도 제공합니다.

제품은 HTTP 1.x 요청, HTTP 쿠키 및 SSL/TLS(해당하는 경우)를 지원하는 모든 브라우저에서 작동할 수 있습니다.

- 에이전트는 SSL 연결을 통해 사용자 자격 증명을 수집한 후 비 SSL 연결을 통해 후속 요청을 허용할 수 있습니다. 제품은 리소스에 대한 액세스를 허용할 때 이 자격 증명 수집 메커니즘과 Windows 보안 컨텍스트를 함께 사용합니다.

- 제품은 양식 기반 인증을 사용한 싱글 사인온을 구현할 수 있으며 사용자 아이덴티티를 백오피스 응용 프로그램으로 전달할 수 있습니다.

Microsoft는 일반 용도의 양식 자격 증명 수집을 제공하지 않습니다.

사용자 보안 컨텍스트에 대한 영구 세션이 관리되는 방식

에이전트가 특정 리소스에 대한 보안 컨텍스트를 제공할 수 있도록 하려면 해당 리소스가 포함된 모든 영역에 대해 영구 세션이 사용되도록 설정하십시오. 영구 세션은 세션 저장소가 관리합니다.

세션 저장소는 사용자의 암호화된 자격 증명을 저장하고 사용자와 세션 ID를 연결합니다. 클라이언트와 에이전트 간에 세션이 설정되면 Windows 사용자 계정이 설정되고 세션에 연결됩니다. 웹 에이전트의 사용자 세션 캐시가 삭제되면 에이전트는 세션 저장소에서 사용자의 자격 증명을 가져옵니다. 자격 증명을 가져오면 에이전트가 세션을 다시 구성할 수 있습니다. 세션 저장소는 또한 싱글 사인온 환경 전체에서 전파를 위한 보안 컨텍스트를 저장합니다.

세션 유효성이 다시 검사되는 방식

정책 서버를 통해 세션 저장소에 연결하여 세션 유효성을 다시 검사하도록 웹 에이전트를 명시적으로 구성할 수 있습니다. 사용자 브라우저에 저장된 세션 쿠키는 세션 ID 를 포함합니다. 쿠키는 세션 ID 를 사용하여 세션 저장소에서 사용자 자격 증명을 다시 가져옵니다.

참고: 세션 쿠키가 만료되면 이 ID 에 연결된 자격 증명은 무효화됩니다. 이 경우 사용자는 다시 인증해야 합니다.

유효성 검사 기간은 에이전트가 세션을 다시 유효성 검사하는 빈도를 결정합니다. 유효성 검사 기간은 에이전트가 캐시에 있는 정보를 사용하여 세션의 활성화를 유지하는 기간을 정의합니다. 유효성 검사 기간이 만료되면 에이전트가 세션 저장소에 연결합니다.

유효성 검사 기간이 너무 작으면 에이전트가 자주 세션 저장소로 다시 연결되므로 제품이 요청을 처리하는 속도에 영향을 줍니다. 유효성 검사 값은 높은 숫자로 설정하십시오. 활성 세션 수가 에이전트의 최대 사용자 세션 캐시 값보다 낮을 경우 에이전트는 캐시된 정보를 사용합니다.

참고: 세션 저장소가 작동하지 않을 경우 유효성 검사 기간이 무한대가 되어 에이전트가 세션 저장소에 연결하지 않습니다.

Windows 사용자 보안 컨텍스트 요구 사항

IIS 웹 서버 환경에서 Windows 보안 컨텍스트 기능을 사용하려면 다음 요구 사항을 충족해야 합니다.

- 사용자가 인증하고 있는 도메인에서 모든 IIS 서버가 트러스트되어야 합니다. 서버 간에 트러스트 관계를 설정하여 사용자 그룹에 대해 분산 서비스를 제공할 수 있습니다.
- 사용자에게 웹 서버에 로컬로 로그인할 수 있는 권한이 있어야 합니다. 서버가 여러 개인 경우에는 모든 서버에 로컬로 로그인할 수 있는 권한이 있어야 합니다.
- World Wide Web Publishing 서비스를 시작하는 계정에 대해 다음 사항을 고려하십시오.
 - 시스템 계정은 추가 구성이 필요 없습니다.
 - 도메인 계정은 운영 체제의 일부로 기능하려면 연결된 사용자의 권한이 필요합니다.

구성 개요

단계	제품 구성 요소
관계형 데이터베이스를 세션 저장소로 지정	정책 서버 관리 콘솔의 "데이터" 탭
Windows 사용자가 포함된 사용자 디렉터리에서 보안 컨텍스트를 실행할 수 있도록 설정	"사용자 디렉터리" 창의 "디렉터리 설정" 그룹 상자에 있는 "인증된 사용자의 보안 컨텍스트 사용" 확인란
지원되는 인증 체계 (페이지 104) 중 하나를 각 영역과 연결	"영역" 창의 "리소스" 그룹 상자
각 영역에 대해 영구 세션이 사용되도록 설정하고 "Validation Enabled Period"(유효성 검사 사용 기간) 값을 높게 설정	"영역" 창의 "세션" 그룹 상자
IIS 웹 서버가 물리적으로 안전한 위치에 있지 않은 경우 insecureserver 를 YES 로 설정	에이전트 구성 개체 또는 WebAgent.conf

지원되는 인증 체계

다음 인증 체계가 지원됩니다.

- 기본 인증 체계
- SSL 을 통한 기본 인증 체계
- HTML 양식 인증 체계
- X.509 클라이언트 인증서 및 기본 인증 체계
- X.509 클라이언트 인증서 및 HTML 양식 인증 체계

사용자의 자격 증명이 제공되지 않았으므로 에이전트는 인증서만 단독으로 사용할 수 없습니다. 인증서 인증과 기본 또는 양식 인증을 결합하여 사용자 자격 증명을 수집해야 합니다.

NTLM 인증 체계는 이 제품에 대한 Windows 사용자 보안 컨텍스트와 호환되지 않습니다. 웹 서버의 일부 리소스에 대해 NTLM 을 사용하고 동일한 웹 서버의 다른 리소스에 대해 Windows 사용자 보안 컨텍스트를 사용하십시오. NTLM 을 사용하여 액세스하는 리소스는 Windows 사용자 보안 컨텍스트 메커니즘을 통해 액세스하는 리소스와 다른 영역에 있어야 합니다.

추가 정보:

[인증 체계](#) (페이지 287)

Active Directory 및 NetBIOS 이름

Active Directory 도메인은 DNS 명명 표준에 따라 이름이 지정되지만 NetBIOS 이름은 Active Directory 도메인을 생성할 때 정의되어야 합니다.

제품이 Microsoft 보안 컨텍스트를 원활하게 지원하려면 Microsoft 의 권장에 따라 NetBIOS 이름이 DNS 도메인 이름과 일치해야 합니다.

Active Directory 도메인의 DNS 이름이 NetBIOS 이름과 다르면 사용자 도메인은 구성할 수 없습니다. 제품이 LDAP 사용자 디렉터리를 사용하도록 구성된 경우 웹 서버는 보안 컨텍스트를 제공할 수 없습니다.

보안 컨텍스트의 싱글 사인온

제품은 지원되는 모든 웹 서버 간의 싱글 사인온을 제공하는 동시에 원활한 Microsoft 보안 컨텍스트에 필요한 보안 컨텍스트를 유지합니다.

하지만 모든 영역이 존속해야 합니다. 그렇지 않으면 제품이 보안 컨텍스트를 유지하려고 시도할 때 사용자가 다시 자격 증명을 제공해야 합니다.

제 5 장: 에이전트 및 에이전트 그룹

이 섹션은 다음 항목을 포함하고 있습니다.

[웹 에이전트의 트러스트된 호스트](#) (페이지 107)

[트러스트된 호스트의 호스트 구성 개체](#) (페이지 112)

[SiteMinder 에이전트 개요](#) (페이지 118)

[웹 에이전트 구성 개요](#) (페이지 121)

[웹 에이전트 구성 방법](#) (페이지 124)

[에이전트 구성 개체 개요](#) (페이지 130)

[웹 에이전트 사용](#) (페이지 136)

[RADIUS 에이전트 구성](#) (페이지 137)

[에이전트 그룹](#) (페이지 138)

[사용자 지정 에이전트](#) (페이지 140)

[에이전트 검색](#) (페이지 142)

웹 에이전트의 트러스트된 호스트

트러스트된 호스트는 웹 에이전트를 하나 이상 설치할 수 있는 임의의 클라이언트 시스템입니다.

정책 서버에 트러스트된 호스트 등록

에이전트를 설치하는 시스템에서 트러스트된 호스트를 등록하십시오. 호스트 설치의 에이전트 구성 프로세스의 일부입니다. 등록 도구는 SmHost.conf 파일을 생성합니다. 이 파일이 성공적으로 생성되면 클라이언트 컴퓨터가 트러스트된 호스트가 됩니다. 트러스트된 호스트는 등록되어야만 정책 서버와 통신할 수 있습니다.

중요! 호스트 등록은 웹 에이전트를 설치하거나 구성할 때마다 수행하는 것이 아니라 한 번만 수행합니다.

에이전트는 초기화될 때 호스트 구성 파일(SmHost.conf)에 있는 트러스트된 호스트의 구성 설정을 사용합니다. 에이전트는 호스트 구성 파일에 나열된 첫 번째 정책 서버로 연결하려고 시도합니다. 첫 번째 시도가 실패하면 트러스트된 호스트가 나열된 다음 정책 서버에 연결하려고 시도합니다.

참고: 관리 UI 를 사용하여 트러스트된 호스트를 생성할 수 없습니다. 관리 UI 에서는 등록된 트러스트된 호스트를 보거나 삭제할 수만 있습니다.

웹 에이전트가 해당 부트스트랩 정책 서버에 연결하면 트러스트된 호스트는 Smhost.conf 파일에서 호스트 구성 개체를 찾습니다. 트러스트된 호스트는 이 호스트 구성 개체에서 구성 정보를 가져옵니다.

트러스트된 호스트 구성 설정

트러스트된 호스트 구성 설정의 대부분은 호스트 구성 개체에서 설정됩니다. PolicyServer 및 RequestTimeout 매개 변수만 예외적으로 호스트 구성 파일(SmHost.conf)에서 설정됩니다.

요청 시간 만료

RequestTimeout 매개 변수는 정책 서버를 사용할 수 없는 것으로 결정하기 전까지 트러스트된 호스트가 대기하는 시간(초)을 지정합니다. 웹 서버의 응답 시간을 최적화하려면 이 설정을 사용하십시오.

참고: 트래픽이 많거나 네트워크 연결 속도가 느려 정책 서버의 사용량이 많을 경우에는 RequestTimeout 값을 늘리십시오.

작동 모드

작동 모드는 트러스트된 호스트가 여러 정책 서버와 작동하는 방식을 결정합니다. 다음과 같은 작업 모드를 사용할 수 있습니다.

장애 조치 모드

장애 조치는 중복 모드입니다. 기본 정책 서버에서 장애가 발생할 경우 백업 정책 서버가 이 서버의 정책 작업을 승계할 수 있습니다. 장애 조치가 기본 작동 모드입니다. 트러스트된 호스트는 초기화될 때 장애 조치 모드에서 작동합니다.

이 모드에서는 모든 트러스트된 호스트 요청이 목록의 첫 번째 정책 서버로 전송됩니다. 정책 서버가 응답하지 않으면 트러스트된 호스트는 이 서버를 *사용 불가*로 표시합니다. 트러스트된 호스트는 목록에 있는 다음 정책 서버로 요청을 보냅니다. 이전에 장애가 발생했던 정책 서버는 복구 시 목록의 원래 위치로 돌아갑니다.

라운드 로빈 모드

라운드 로빈 모드는 동적 부하 분산 모드입니다. 에이전트는 호스트 구성 개체에 나열된 모든 정책 서버 사이에서 요청을 균형 있게 분산시킵니다.

라운드 로빈 모드에서는 트러스트된 호스트가 요청을 목록의 첫 번째 정책 서버로 전송합니다. 다음 요청은 목록의 두 번째 정책 서버로, 그리고 그 다음 서버로 계속 전달됩니다. 이 프로세스는 트러스트된 호스트가 요청을 사용 가능한 모든 정책 서버로 전달할 때까지 계속됩니다. 다음 요청은 목록의 첫 번째 정책 서버로 되돌아오고 이 주기가 다시 시작됩니다.

한 정책 서버에서 장애가 발생하면 목록의 다음 서버로 요청이 리디렉션됩니다. 트러스트된 호스트는 장애가 발생한 서버를 *사용할 수 없음*으로 표시하고 모든 요청을 다른 서버로 리디렉션합니다. 장애가 발생한 서버는 복구 시 자동으로 목록의 원래 위치로 돌아갑니다.

여러 정책 서버를 사용할 경우 동적 부하 분산을 이용하면 처리량이 개선되고 결과적으로 사용자 인증 및 권한 부여가 보다 효율적으로 이루어지므로 이 설정을 사용하는 것이 좋습니다. 동적 부하 분산을 사용할 경우 단일 정책 서버가 요청으로 과부하되는 것도 방지됩니다. 부하 분산 정책 서버 중 하나를 사용할 수 없어도 장애 조치는 계속 수행됩니다.

작동 모드 구현

작동 모드는 트러스트된 호스트가 여러 정책 서버와 작동하는 방식을 결정합니다. 작동 모드에는 장애 조치와 라운드 로빈의 두 가지 모드가 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버를 여러 개 구성합니다.
2. 모든 정책 서버를 공통 정책 저장소로 설정합니다.
3. EnableFailover 매개 변수를 설정합니다.
 - 장애 조치 모드를 사용하려면 EnableFailover 매개 변수를 YES 로 설정합니다.
 - 라운드 로빈 동적 부하 분산을 사용하려면 EnableFailover 매개 변수를 NO 로 설정합니다.

EnableFailover 매개 변수의 값은 호스트 구성 개체에 지정된 모든 정책 서버에 적용됩니다.

TCP/IP 연결

트러스트된 호스트와 정책 서버는 TCP/IP 연결을 통해 통신합니다. 정책 서버의 권한 부여, 인증, 계정 포트에 대한 사용 가능한 소켓 수에 따라 사용 가능한 TCP/IP 연결 수가 결정됩니다.

포트당 소켓 수는 웹 서버에서 정책 서버에 액세스하는 동시 스레드 수를 제어합니다. 각 사용자 액세스에서 요구되는 웹 서버 스레드 핸들을 분리하십시오. 각 스레드는 자체 소켓이 필요합니다. 웹 서버는 요청에 사용할 스레드 풀을 유지 관리하며, 사용 가능한 스레드가 더 이상 없는 경우에만 스레드를 생성합니다. 트래픽이 증가하면 포트당 소켓 수도 늘어나야 합니다.

일부 설정이 트러스트된 호스트와 정책 서버 간의 TCP/IP 연결 수에 영향을 줍니다.

포트당 최대 소켓

트러스트된 호스트가 정책 서버와의 통신에 사용하는 최대 TCP/IP 연결 수를 정의합니다. 기본적으로 이 값은 20 으로 설정되며, 웹 사이트의 트래픽이 적거나 보통인 경우 이 정도면 충분합니다. 다음과 같은 상황에서는 이 숫자를 늘리십시오.

- 트래픽이 높은 웹 사이트를 관리하고 있습니다.
- 가상 서버에 대해 에이전트 아이덴티티를 정의했습니다.

포트당 최소 소켓

정책 서버가 시작될 때 서버에 대해 열리는 TCP/IP 연결 수를 결정합니다. 기본값은 2 입니다. 트래픽이 많은 웹 사이트를 관리하는 경우에는 이 값을 늘리십시오.

새 소켓 단계

새 연결이 필요한 경우 에이전트가 여는 TCP/IP 연결 수를 지정합니다. 기본값은 2 입니다. 소켓이 더 필요한 경우 각 수준에 추가할 소켓 수를 늘리십시오.

트러스트된 호스트 개체 삭제

트러스트된 호스트는 다시 등록할 때 삭제합니다. 호스트를 다시 등록할 때는 smregghost 등록 도구를 사용합니다. 이 도구는 웹 에이전트와 함께 설치됩니다.

참고: 웹 에이전트 구성 마법사를 실행하여 트러스트된 호스트를 다시 등록할 수 있지만 SmHost.conf 파일 또는 마법사를 삭제하거나 이름을 바꿀 때 트러스트된 호스트를 등록하라는 메시지가 나타나지 않습니다. smregghost 도구를 사용하는 것이 좋습니다. 트러스트된 호스트의 등록 및 재등록에 대한 자세한 내용은 *웹 에이전트 설치 안내서*를 참조하십시오.

트러스트된 호스트를 삭제하려면

1. "인프라", "호스트"를 차례로 클릭합니다.
 2. "트러스트된 호스트"를 클릭합니다.
- "트러스트된 호스트" 페이지가 표시됩니다.

3. 검색 조건을 지정하고 "검색"을 클릭합니다.
검색 조건과 일치하는 트러스트된 호스트의 목록이 열립니다.
4. 목록에서 트러스트된 호스트를 선택합니다.
참고: 한 번에 여러 개의 트러스트된 호스트를 선택할 수 있습니다.
5. "트러스트된 호스트 삭제"를 클릭합니다.
호스트 삭제를 확인하는 메시지가 표시됩니다.
6. "예"를 클릭합니다.
트러스트된 호스트가 삭제됩니다.

트러스트된 호스트의 호스트 구성 개체

호스트 구성 개체에는 트러스트된 호스트에 대한 구성 설정이 보관됩니다. 트러스트된 호스트는 정책 서버에 연결한 후 호스트 구성 개체의 설정을 사용합니다.

SmHost.conf 파일의 hostconfigobject 매개 변수는 에이전트가 사용하는 호스트 구성 개체를 식별합니다. 에이전트는 각 웹 서버 자식 프로세스를 초기화하는 동안 SmHost.conf 파일의 설정을 사용합니다. SmHost.conf 파일은 시작할 때 사용되는 것은 물론, 새 자식 프로세스를 시작하는 웹 서버에 의해 런타임에서도 사용됩니다. 이 초기화 후에는 호스트 구성 개체의 설정이 사용됩니다.

트러스트된 호스트 개체를 생성하려면 먼저 호스트 구성 개체를 생성하십시오.

호스트 구성 개체 복사

호스트 구성 개체를 생성하려면 기존 호스트 구성 개체를 복사하여 해당 속성을 수정하는 것이 좋습니다. DefaultHostSettings 개체를 복사한 후 해당 속성을 새 개체의 템플릿으로 사용할 수 있습니다.

중요! 호스트 구성 개체의 이름은 고유해야 합니다. 기존 에이전트 개체와 동일한 이름을 사용하지 마십시오. 다른 웹 에이전트에 할당된 이름을 사용하면 트러스트된 호스트가 있다는 메시지가 표시됩니다.

다음 단계를 수행하십시오.

1. "인프라", "호스트"를 차례로 클릭합니다.
2. "호스트 구성 개체"를 클릭합니다.
"호스트 구성 개체" 페이지가 표시됩니다.
3. "호스트 구성 만들기"를 클릭합니다.
"호스트 구성 검색" 페이지가 표시됩니다.
4. "Create a copy of an object of type Host Configuration"(호스트 구성 유형 개체의 복사본 만들기)를 선택하고 "확인"을 클릭합니다.

참고: 기본적으로 "DefaultHostSettings" 호스트 구성 개체가 선택됩니다.
"호스트 구성 만들기" 페이지가 표시됩니다.

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

5. 이름과 설명을 입력합니다.

참고: 하이픈("-") 문자로 호스트 구성 개체 이름을 시작하지 마십시오.

6. "구성 값" 및 "클러스터"에서 기존 개체와 다른 새 개체의 속성을 수정합니다.
7. 제출을 클릭합니다.
호스트 구성 개체가 생성됩니다.

호스트 구성 개체에 여러 정책 서버 추가

트러스트된 호스트는 여러 정책 서버에 액세스할 수 있습니다. 트러스트된 호스트 연결과 장애 조치 또는 라운드 로빈 작업을 설정하려면 호스트 구성 개체에 정책 서버를 추가하십시오.

참고: 정책 서버를 여러 가상 IP 주소(VIP)로서 노출하는 하드웨어 부하 분산 장치의 경우 이러한 VIP 를 장애 조치 모드로 구성하는 것이 좋습니다. 하드웨어 부하 분산 장치가 동일한 기능을 더욱 효율적으로 수행하기 때문에 라운드 로빈 모드는 필요하지 않습니다.

다음 단계를 수행하십시오.

1. "인프라", "호스트"를 차례로 클릭합니다.

2. "호스트 구성 개체"를 클릭합니다.

"호스트 구성 개체" 페이지가 표시됩니다.

3. "호스트 구성 만들기"를 클릭하고 "확인"을 클릭합니다.

"호스트 구성 만들기" 페이지가 표시됩니다.

참고: 기본적으로 "호스트 구성 유형의 새 개체 만들기" 옵션이 선택됩니다.

4. 호스트 구성 개체의 이름과 설명을 입력합니다.

5. 호스트 구성 설정을 지정합니다.

6. "클러스터" 그룹 상자에서 "추가"를 클릭합니다.

"클러스터 추가" 페이지가 표시됩니다.

7. 클러스터에 추가할 정책 서버의 IP 주소와 포트 번호를 입력합니다.

참고: 다른 정책 서버를 클러스터에 추가하려면 "클러스터에 추가"를 클릭하십시오. 정책 서버를 클러스터에서 삭제하려면 "포트" 옆의 빼기 기호를 클릭하십시오. 클러스터에서 정책 서버의 순서를 변경하려면 위쪽 및 아래쪽 화살표를 클릭하십시오.

8. "확인"을 클릭합니다.

클러스터가 추가됩니다.

참고: 클러스터를 수정하려면 왼쪽에 있는 오른쪽 방향 화살표를 클릭하십시오. 클러스터를 삭제하려면 오른쪽의 빼기 기호를 클릭하십시오. 다른 클러스터를 추가하려면 "클러스터" 아래의 "추가"를 클릭하고 6 단계와 7 단계를 반복하십시오.

9. 장애 조치 임계값의 백분율을 입력합니다.

참고: 활성 서버의 비율이 지정된 비율보다 작거나 같으면 클러스터가 목록에 있는 다음 클러스터로 장애 조치됩니다.

10. 제출을 클릭합니다.

호스트 구성 개체가 정책 서버 상세 정보로 업데이트됩니다.

호스트 구성 개체에 맞게 정책 서버 클러스터 구성

장애 조치 작업을 위해 클러스터에 여러 개의 정책 서버를 구성할 수 있습니다. 서버 클러스터링을 통해 한 서버 그룹에서 다른 서버 그룹으로 장애 조치를 사용할 수 있습니다.

참고: 하드웨어 부하 분산 장치를 사용하여 정책 서버를 다중 VIP(가상 IP 주소)로 노출하는 경우 장애 조치 구성에서 해당 VIP 를 구성하는 것이 좋습니다. 하드웨어 부하 분산 장치가 동일한 기능을 더 효율적으로 수행하기 때문에 클러스터링은 중복되는 기능입니다.

정책 서버 클러스터는 호스트 구성 개체의 일부로 정의됩니다. 웹 에이전트가 초기화될 때 호스트 구성 개체의 설정을 사용하여 정책 서버와의 통신이 설정됩니다.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다.

다음 단계를 수행하십시오.

1. "인프라", "호스트"를 차례로 클릭합니다.
2. "호스트 구성 개체"를 클릭합니다.
"호스트 구성 개체" 페이지가 표시됩니다.
3. "호스트 구성 만들기"를 클릭하고 "확인"을 클릭합니다.
"호스트 구성 만들기" 페이지가 표시됩니다.

참고: 기본적으로 "호스트 구성 유형의 새 개체 만들기" 옵션이 선택됩니다.

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

4. 호스트 구성 개체의 이름과 설명을 입력합니다.
5. 호스트 구성 설정을 지정합니다.
6. "클러스터" 섹션에서 "추가"를 클릭합니다.
"클러스터 추가" 페이지가 표시됩니다.

7. 클러스터에 추가할 정책 서버의 IP 주소와 포트 번호를 입력합니다.

참고: 다른 정책 서버를 클러스터에 추가하려면 "클러스터에 추가"를 클릭하십시오. 정책 서버를 클러스터에서 삭제하려면 "포트" 옆의 빼기 기호를 클릭하십시오. 클러스터에서 정책 서버의 순서를 변경하려면 위쪽 및 아래쪽 화살표를 클릭하십시오.

8. "확인"을 클릭합니다.

클러스터가 추가됩니다.

참고: 클러스터를 수정하려면 첫 번째 열의 오른쪽 방향 화살표를 클릭하십시오. 클러스터를 삭제하려면 마지막 열의 빼기 기호를 클릭하십시오. 다른 클러스터를 추가하려면 "추가"를 클릭하고 7 단계와 8 단계를 반복하십시오.

9. "장애 조치 임계값"의 백분율을 입력합니다.

SM에서는 클러스터에 구성된 정책 서버의 수와 사용자가 지정하는 "장애 조치 임계값 백분율" 모두를 기반으로 하는 "장애 조치 임계값"을 자동으로 계산합니다. "장애 조치 임계값"(각 클러스터에서 서버 목록 오른쪽의 열에 표시됨)은 구성에 따라 사용 가능한 클러스터로 간주되기 위해 클러스터에서 활성화되어야 하는 총 정책 서버 수입니다. 클러스터의 활성 서버 수가 표시된 "장애 조치 임계값"보다 낮아지면 클러스터는 목록 중 다음으로 사용 가능한 클러스터로 장애 조치됩니다. 구성에 기반한 "장애 조치 임계값"의 계산 결과가 정수가 아닌 값이 되면 정책 서버는 이 값을 가장 가까운 정수로 반올림합니다.

5 개의 정책 서버가 구성된 클러스터를 예로 들겠습니다.

"장애 조치 임계값"이

[0% - 19%]의 범위에 있으면 필요한 활성 서버의 값(장애 조치 임계값)은 1 로 반올림됩니다.

20%이면 "장애 조치 임계값"의 계산된 값은 1 입니다.

[21% - 39%]의 범위에 있으면 "장애 조치 임계값"의 값은 2 로 반올림됩니다.

40%이면 "장애 조치 임계값"의 계산된 값은 2 입니다.

[41% - 59%]의 범위에 있으면 "장애 조치 임계값"의 값은 3 으로 반올림됩니다.

60%이면, "장애 조치 임계값"의 계산된 값은 3 입니다.

[61% - 79%]의 범위에 있으면 "장애 조치 임계값"의 값은 4 로 반올림됩니다.

80%이면, "장애 조치 임계값"의 계산된 값은 4 입니다.

[81% - 99%]의 범위에 있으면 "장애 조치 임계값"의 값은 5 로 반올림됩니다.

100%이면 "장애 조치 임계값"의 계산된 값은 5 입니다.

"장애 조치 임계값 백분율"을 설정하면 이 값은 호스트 구성 개체를 사용하는 모든 클러스터에 적용됩니다.

참고: 클러스터에서 활성 서버의 백분율이 지정된 백분율 이하가 되면 클러스터는 클러스터 목록 중 다음으로 사용 가능한 클러스터로 장애 조치됩니다.

10. 제출을 클릭합니다.

호스트 구성 개체가 정책 서버에서 구성됩니다.

중요! "구성 값"은 지정된 클러스터가 없을 때만 사용되는 단일 정책 서버 및 단순 장애 조치 작업을 지정합니다. 단순 장애 조치 작업을 사용하기 위해 모든 클러스터를 삭제하기로 결정한 경우에는 모든 정책 서버 정보를 삭제해야 합니다.

추가 정보:

[정책 서버 개체 복사](#) (페이지 10)

SiteMinder 에이전트 개요

에이전트는 네트워크 액세스 제어 또는 웹 액세스 제어를 시행하는 필터로서 기능하는 네트워크 엔터티입니다. 에이전트는 PEP(정책 적용 지점)로 간주됩니다. 에이전트 모니터는 리소스를 요구합니다. 사용자는 보호된 리소스를 요구합니다. 에이전트는 사용자에게 인증 체계에 기초한 자격 증명을 묻습니다. 에이전트는 정책 서버로 자격 증명을 보냅니다.

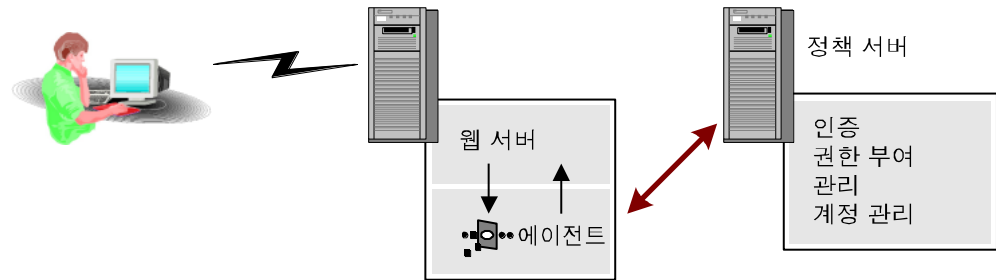
정책 서버는 자격 증명을 기반으로 사용자가 인증될 수 있는지 여부와 요청된 리소스에 대한 권한을 부여받을 수 있는지 여부를 결정합니다. 그런 다음 정책 서버는 에이전트에 이를 전달하고 에이전트는 요청된 리소스에 대한 액세스를 허용하거나 거부합니다.

기본적으로 사용할 수 있는 에이전트는 웹 에이전트, 가맹 에이전트, EJB 에이전트, 서블릿 에이전트 및 RADIUS 에이전트입니다. 다른 모든 에이전트는 에이전트 API 를 사용하여 생성해야 하는 사용자 지정 에이전트로 간주됩니다. 생성된 사용자 지정 에이전트는 관리 UI 에서 구성할 수 있습니다.

웹 에이전트

에이전트는 웹 서버와 함께 동작합니다. 사용자가 웹 서버로부터 페이지를 요청하면 웹 에이전트는 정책 서버와 통신합니다. 에이전트는 사용자가 리소스에 액세스할 수 있기 전에 인증 및 권한 부여 요청을 처리합니다. 정책 서버는 또한 사용자에게 개인화된 정보를 제공하기 위해 에이전트에 대한 정보를 제공할 수도 있습니다.

다음 그림은 에이전트 및 정책 서버가 처리하는 가장 기본적인 세 가지 트랜잭션을 설명합니다. 이러한 트랜잭션은 사용자 지정된 콘텐츠를 사용하고 제품의 다른 기능을 지원하기 위해 추가적인 세부 정보를 포함할 수 있습니다. 이 프로세스는 사용자가 에이전트에 의해 관리되는 웹 서버를 통해 리소스에 액세스하려고 시도할 때마다 유사합니다.



1. 리소스가 보호되어 있습니까? 그렇다면 사용자의 자격 증명을 요청합니다.
2. 사용자가 인증되었습니까? 그렇다면 권한 부여 정책을 확인합니다.
3. 사용자에게 권한이 부여되었습니까? 그렇다면 보호된 리소스에 대한 액세스를 허용합니다.

위의 그림에서는 사용자가 권한을 갖고 있는 보호된 리소스를 요청한다고 가정합니다. 에이전트는 정책 서버를 확인하여 해당 리소스가 보호되는지 확인합니다. 보호된 리소스의 경우 에이전트는 사용자로부터 자격 증명을 수집하여 정책 서버로 전달합니다.

정책 서버는 사용자를 인증하고 사용자가 올바르게 식별되었음을 웹 에이전트에 알려 줍니다. 마지막으로, 웹 에이전트는 정책 서버를 확인하여 사용자가 해당 리소스에 대해 권한이 있는지 여부를 파악합니다. 정책 서버가 권한 부여를 확인하면 에이전트가 통보를 받습니다. 에이전트는 웹 서버가 보호된 리소스를 사용자에게 표시하도록 허용합니다.

동일한 리소스를 제어하며 유형이 동일한 에이전트(모든 웹 에이전트 또는 모든 RADIUS 에이전트)를 그룹화할 수 있습니다.

추가 정보:

[에이전트 그룹](#) (페이지 138)

RADIUS 에이전트

RADIUS(Remote Authentication Dial-In User Service) 프로토콜은 NAS(Network Access Servers)와 RADIUS 인증 서버 사이에서 세션 인증 및 구성 정보를 교환합니다. 프록시 서비스, 방화벽 또는 전화 접속 보안 장치는 종종 RADIUS 프로토콜을 사용합니다.

RADIUS 에이전트는 RADIUS 프로토콜을 사용하여 통신하는 전체 응용 프로그램을 보호합니다.

정책 서버는 RADIUS 인증 서버로 사용될 수 있습니다. RADIUS 에이전트는 정책 서버가 NAS 클라이언트 장치와 통신할 수 있도록 합니다.

추가 정보:

[정책 서버를 Radius 서버로 사용](#) (페이지 827)

응용 프로그램 서버 에이전트

응용 프로그램 서버 에이전트는 WebLogic 및 WebSphere 응용 프로그램 서버 리소스를 보호하기 위해 모든 기능의 에이전트를 제공하는 Java 구성 요소 모음입니다. 응용 프로그램 서버 에이전트는 제품을 J2EE 플랫폼과 통합합니다.

응용 프로그램 서버 에이전트는 다음과 같은 구성 요소를 보호할 수 있습니다.

- 웹 응용 프로그램(서블릿, HTML 페이지, JSP, 이미지 파일 포함)
- JNDI 조회
- EJB 구성 요소
- JMS 연결 팩터리, 항목, 큐
- JDBC 연결 풀

응용 프로그램 서버 에이전트는 단일 에이전트입니다. 정책 서버의 관점에서는 응용 프로그램 서버 리소스를 보호하는 다른 에이전트 유형이 있습니다. 에이전트 유형은 다음과 같은 방식으로 서블릿 및 EJB 구성 요소를 보호하는 융통성을 제공합니다.

- 서블릿 또는 EJB 에이전트 사용
- 에이전트 사용

WSS(Web Services Security) 에이전트

WSS 에이전트(이전 명칭 SOA)는 웹 및 응용 프로그램 서버와 통합되어 이러한 서버에서 호스트되는 SOAP/XML 기반 웹 서비스 리소스에 대한 액세스 요청을 인증하고 권한을 부여합니다.

웹 에이전트 구성 개요

에이전트를 구성하는 옵션은 다음과 같습니다.

중앙 구성

에이전트가 정책 서버에서 구성됨을 나타냅니다. 정책 저장소에는 에이전트 그룹이 공유하는 구성 매개 변수 집합이 보관됩니다. 매개 변수 설정은 관리 UI 를 사용하여 구성됩니다.

에이전트 구성은 에이전트 구성 개체에서 지정됩니다.

참고: 중앙 구성은 RADIUS, EJB, 서블릿 또는 사용자 지정 에이전트에는 적용되지 않습니다. 이러한 에이전트는 로컬 구성만 가능합니다.

로컬 구성

웹 에이전트가 설치된 각 웹 서버에 있는 로컬 구성 파일을 사용하여 웹 에이전트가 구성됨을 나타냅니다.

일부 매개 변수는 중앙에 저장하고 나머지는 로컬에 저장할 수 있습니다.

참고: 에이전트를 사용하거나 사용하지 않도록 설정하는 작업은 정책 서버가 아니라 웹 서버의 파일에서만 수행할 수 있습니다.

웹 에이전트 중앙 구성의 장점

에이전트를 중앙에서 구성할 경우 설정이 웹 서버의 로컬 구성 파일이 아니라 정책 저장소에 저장됩니다.

중앙 구성을 로컬 구성과 비교할 경우 장점은 다음과 같습니다.

중앙 에이전트 구성을 사용할 경우 사용성 개선

- 여러 웹 에이전트의 구성 설정을 쉽고 빠르게 업데이트할 수 있습니다. 한 곳에서 설정을 변경한 후 변경 내용을 여러 에이전트로 전파할 수 있습니다.
- 웹 에이전트 설치 시 관리자가 공유 암호를 지정할 필요가 없습니다. 정책 서버가 공유 암호를 생성합니다.

중앙 에이전트 구성을 수행할 경우 보안 강화

- 웹 에이전트 구성에 대한 액세스 제어가 더 쉽습니다. 예를 들어 웹 서버 관리자가 구성 설정을 변경할 수 없도록 방지할 수 있습니다.
- 구성 설정을 웹 서버 대신 내부 방화벽 뒤에 저장할 수 있습니다.
- 하드웨어에 바인딩된 키는 공유 암호를 생성할 수 있습니다. 클라이언트 쪽에서는 이 암호를 사용하여 정책 서버에 대한 보안 연결을 구성합니다. 트러스트된 호스트는 정책 서버에 대한 연결을 처리합니다.

웹 에이전트 구성 요소

네트워크의 에이전트 쪽의 몇몇 주요 에이전트 작업은 다음과 같습니다.

에이전트

웹 서버에 대한 가상 인터페이스로, 규칙을 트리거하고 정책을 적용합니다.

트러스트된 호스트

에이전트가 하나 이상 설치된 클라이언트 컴퓨터로, 이 호스트는 정책 서버에 대한 연결을 처리합니다. 서버 하나에 트러스트된 호스트를 여러 개 구성할 수 있지만 각각은 고유한 이름이 필요합니다.

트러스트된 호스트는 정책 서버에 등록되어 있기 때문에 "트러스트"됩니다. 해당 호스트에 설치된 웹 에이전트가 정책 서버와 통신할 수 있도록 트러스트된 호스트를 등록하십시오.

다음 데이터는 트러스트된 호스트를 식별합니다.

- 호스트 이름
- 호스트 IP 주소
- 호스트 설명
- 공유 암호
- 호스트 OID(개체 식별자)

웹 에이전트 구성 파일(WebAgent.conf 또는 LocalConfig.conf)

에이전트가 있는 웹 서버에 저장된 이 파일은 로컬 구성에 사용됩니다. LocalConfig.conf 파일은 각 웹 에이전트에 대한 에이전트 구성 매개 변수를 수록하고 있습니다. WebAgent.conf 파일은 에이전트를 활성화 또는 비활성화하며, 모든 관련 플러그인을 로드합니다.

호스트 구성 파일(SmHost.conf)

웹 에이전트가 있는 웹 서버에 저장된 이 파일에는 트러스트된 호스트의 초기화 매개 변수가 보관됩니다. 트러스트된 호스트는 정책 서버에 연결한 후 호스트 구성 개체의 설정을 사용합니다. 호스트 구성 개체는 이 파일의 hostconfigobject 매개 변수에 지정됩니다.

추가 정보:

[웹 에이전트 구성 개요](#) (페이지 121)

웹 에이전트 관련 정책 서버 개체

정책 서버 쪽에서 다음과 같은 개체가 에이전트 구성과 관련됩니다.

에이전트 개체

특정 웹 서버에 매핑될 수 있는 에이전트 아이덴티티를 설정하여 에이전트 이름을 지정합니다.

에이전트 구성 개체

웹 에이전트 구성 매개 변수를 포함합니다. 중앙에서 에이전트 그룹을 관리하려면 에이전트 구성 개체를 사용하십시오. 이 개체는 주로 중앙 에이전트 구성에 사용되지만, 정책 서버에 로컬 구성을 사용하도록 지시하는 매개 변수도 포함합니다.

호스트 구성 개체

트러스트된 호스트의 구성 매개 변수를 포함합니다. 초기화 매개 변수를 제외한 트러스트된 호스트 매개 변수는 항상 호스트 구성 개체에서 유지 관리됩니다.

구성 개체는 정책 저장소에 저장됩니다. 이러한 개체는 관리 UI 를 사용하여 생성 또는 수정하십시오.

추가 정보:

[웹 에이전트 구성 개요](#) (페이지 121)

웹 에이전트 구성 방법

에이전트를 구성하려면 몇몇 태스크를 완료해야 합니다. 이러한 태스크는 에이전트의 로컬 및 중앙 구성에 적용됩니다.

참고: 에이전트를 설치하고 트러스트된 호스트를 등록하기 전에 정책 서버에서 에이전트 통신을 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버를 설치합니다.
2. 호스트 구성 개체를 생성합니다.
3. 정책 서버 관리자에게 "트러스트된 호스트 등록" 권한을 부여합니다. 관리자는 이 권한이 있어야 트러스트된 호스트를 등록할 수 있습니다.

참고: "트러스트된 호스트 등록" 권한 만 있는 관리자를 생성할 경우 해당 관리자는 관리 UI 를 사용할 수 없습니다.

4. 에이전트 개체를 만듭니다. 이 개체는 에이전트의 이름을 정의합니다. 에이전트 개체와 에이전트 구성 개체를 혼동하지 마십시오.
5. 에이전트 구성 개체를 생성합니다.

에이전트를 로컬에서 구성하려는 경우에도 이 개체가 있어야 로컬 구성 매개 변수 `AllowLocalConfig` 를 설정할 수 있습니다.

6. 클라이언트 사이트에 에이전트를 설치합니다.

7. 트러스트된 호스트를 등록합니다. 이 과정 중에 정책 서버에 이미 생성한 호스트 구성 개체의 이름을 제공합니다.
8. 에이전트 관련 정책 개체가 구성되었으면 해당 에이전트가 사용되도록 설정합니다. 이 설정은 로컬 에이전트 구성 파일에 있습니다.

중앙에서 웹 에이전트 구성

중앙에서 웹 에이전트를 구성하려면 "웹 에이전트 구성"에 간략하게 설명된 단계를 수행하십시오. 이러한 태스크는 웹 에이전트의 로컬 및 중앙 구성에 적용됩니다.

구성 매개 변수를 로컬에서 지정할 경우, 두 구성 원본의 입력 내용이 병합되어 로컬 에이전트 구성 파일에 있는 매개 변수 값이 해당하는 에이전트 구성 개체의 값을 재정의합니다.

에이전트 구성 개체와 에이전트 구성 파일의 입력 내용을 조합하지 않고 로컬 구성만 사용하려면 **AllowLocalConfig** 매개 변수만 포함하고 이 매개 변수 값을 **yes** 로 설정하여 에이전트 구성 개체를 구성하십시오. 이렇게 하면 로컬 구성 파일의 구성 데이터만 웹 에이전트에 적용됩니다.

중앙 구성과 로컬 구성의 상호 작동 방식을 보다 잘 이해하려면 "중앙 구성과 로컬 구성 조합"을 참조하십시오.

호스트 구성 개체 만들기

호스트 구성 개체를 생성(또는 복제)할 수 있습니다.

다음 단계를 수행하십시오.

1. "인프라", "호스트"를 차례로 클릭합니다.
2. "호스트 구성 개체"를 클릭합니다.
3. "호스트 구성 만들기"를 클릭합니다.

4. 다음 태스크 중 하나를 수행합니다.
 - (권장) 기존 호스트 구성 개체의 복사본을 생성하고 해당 속성을 수정합니다. **DefaultHostSettings** 개체를 복사한 후 해당 설정을 새 개체의 템플릿으로 사용하십시오. 정책 서버 설치 프로그램이 **DefaultHostSettings** 개체를 생성합니다.
중요! **DefaultHostSettings** 개체를 직접 수정하여 사용하지 마십시오. 항상 이 개체를 복사한 후 복사본을 수정하십시오.
 - 개체를 만듭니다.
5. "확인"을 클릭합니다.
6. 이름과 설명을 입력합니다.
7. "구성 값"에서 호스트 구성 설정을 지정합니다.
8. 제출을 클릭합니다.

로컬에서 웹 에이전트 구성

에이전트는 에이전트 구성 개체와 로컬 에이전트 구성 파일 모두를 읽습니다. 로컬 에이전트 구성 파일의 값은 에이전트 구성 개체의 이러한 값보다 우선합니다. 에이전트는 이러한 설정 모두를 함께 사용합니다. 에이전트 매개 변수 중 일부만 로컬에서 수정하고 구성 설정의 나머지 부분은 중앙 에이전트 구성 개체를 사용할 수 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버 관리자에게 요청하여 로컬 구성을 수행할 수 있는 권한을 받습니다.
2. 웹 에이전트를 구성합니다.
3. 에이전트 구성 개체에서 **AllowLocalConfig** 매개 변수를 **yes** 로 설정합니다.
4. 웹 에이전트 구성 파일(**LocalConfig.conf**)을 편집합니다.

웹 에이전트 구성 파일의 복사본을 수정하고 백업 복사본을 보관해 두어야 합니다.

모든 에이전트는 **<web_agent_home>\config** 디렉터리에 샘플 **WebAgent.conf.sample** 파일이 있습니다. 이 파일을 수정한 다음 **WebAgent.conf** 라는 이름으로 해당하는 웹 서버 위치에 저장하십시오.

중앙 구성 및 로컬 구성 사용 예

시나리오:

각 에이전트를 개별적으로 구성할 필요 없이 네트워크에서 여러 쿠키 도메인 간 싱글 사인온을 구성하려고 합니다.

에이전트 구성 개체의 **CookieDomain** 매개 변수는 **example.com** 으로 설정되어 있습니다. 네트워크에 있는 한 에이전트에 대해 **CookieDomain** 매개 변수를 **example.org** 로 설정하십시오. 에이전트 구성 개체에 설정된 모든 다른 매개 변수 값 설정을 사용하십시오.

해결책:

다음 단계를 수행하십시오.

1. 사용 환경에 해당하는 모든 매개 변수를 사용하여 에이전트 구성 개체를 구성합니다.
2. 에이전트 구성 개체에서 **AllowLocalConfig** 매개 변수를 **yes** 로 설정합니다.
3. 에이전트 하나에 대해 **CookieDomain** 매개 변수만 **example.org** 으로 변경합니다. 다른 매개 변수는 수정하지 *마십시오*.

에이전트 구성 파일의 **CookieDomain** 매개 변수 값은 에이전트 구성 개체의 값보다 우선합니다. 에이전트 구성 개체는 다른 모든 매개 변수의 설정을 결정합니다.

웹 에이전트 아이덴티티를 설정하기 위해 에이전트 개체 만들기

웹 에이전트 아이덴티티를 생성하려면 관리 UI 에서 에이전트 개체를 생성합니다. 개체 이름은 에이전트 구성 파일 또는 에이전트 개체의 **AgentName** 또는 **DefaultAgentName** 매개 변수의 값과 일치해야 합니다. 정책 서버는 웹 에이전트를 호스팅하는 웹 서버의 IP 주소로 에이전트 이름을 매핑합니다. 이 매핑은 정책과 에이전트를 연결합니다. 에이전트 개체 및 아이덴티티를 만들면 에이전트를 영역과 연결할 수 있습니다.

다음 단계를 수행하십시오.

1. "인프라", "에이전트"를 차례로 클릭합니다.
2. "에이전트"를 클릭합니다.
3. "에이전트 만들기"를 클릭합니다.
4. "확인"을 클릭합니다.
5. 에이전트의 이름과 설명을 입력합니다.

참고: 웹 에이전트 이름에는 다음과 같은 제한이 있습니다.

- 에이전트 이름에는 하나 이상의 인쇄 가능한 문자를 비롯하여 32-127 범위의 7 비트 ASCII 문자가 포함되어야 합니다.
 - 에이전트 이름에는 앰퍼샌드(&)와 별표(*) 문자를 사용할 수 없습니다.
 - 에이전트 이름은 대/소문자를 구분하지 않습니다. 예를 들어 **MyAgent** 라는 이름의 에이전트가 있을 때는 **myagent** 라는 에이전트를 생성할 수 없습니다.
6. "에이전트 스타일"로 **SiteMinder** 를 선택하고 "에이전트 유형"으로 "웹 에이전트"를 선택합니다.
 7. 제출을 클릭합니다.

4.x 웹 에이전트 아이덴티티를 사용하도록 에이전트 개체 구성

4.x 웹 에이전트 아이덴티티를 생성하려면 관리 UI 에서 에이전트 개체를 생성합니다. 개체 이름은 로컬 웹 에이전트 구성 파일의 에이전트 이름과 일치해야 합니다. 웹 에이전트 개체 및 아이덴티티를 만들면 웹 에이전트를 영역과 연결할 수 있습니다.

다음 단계를 수행하십시오.

1. "인프라", "에이전트"를 차례로 클릭합니다.
2. "에이전트"를 클릭합니다.
3. "에이전트 만들기"를 클릭합니다.

"Create a new object of type Agent"(에이전트 유형의 새 개체 만들기) 옵션이 선택되어 있는지 확인합니다.

4. "확인"을 클릭합니다.
5. 에이전트의 이름과 설명을 입력합니다.

참고: 웹 에이전트 이름에는 다음과 같은 제한이 있습니다.

- 에이전트 이름에는 하나 이상의 인쇄 가능한 문자를 비롯하여 32-127 범위의 7 비트 ASCII 문자가 포함되어야 합니다.
- 에이전트 이름에는 앰퍼샌드(&)와 별표(*) 문자를 사용할 수 없습니다.
- 에이전트 이름은 대/소문자를 구분하지 않습니다. 예를 들어 MyAgent 라는 이름의 에이전트가 있을 때는 myagent 라는 에이전트를 생성할 수 없습니다.

6. 다음 설정을 확인합니다.
 - SiteMinder 옵션이 선택되어 있습니다.
 - "에이전트 유형" 드롭다운 목록에 "웹 에이전트"가 표시됩니다.
7. "4.x 에이전트 지원" 옵션을 선택합니다.
"트러스트 설정" 페이지가 표시됩니다.
8. 에이전트가 있는 서버의 IP 주소를 입력합니다.

참고: 단일 서버와 마찬가지로 가상 서버에도 이름과 IP 주소가 정의되어 있습니다. 가상 서버의 각 에이전트마다 고유한 에이전트 이름이 있어야 합니다.

9. 공유 암호를 입력하고 확인합니다.

제한:

- 제공하는 암호는 웹 서버에 웹 에이전트를 설치할 때 할당한 암호와 일치해야 합니다.
- 암호에는 최소 하나의 문자가 포함되어야 하며 255 자를 넘지 않아야 합니다.
- 암호에는 영숫자만 사용할 수 있습니다.
- 암호에는 포함된 공백을 사용할 수 없습니다.

참고: 같은 웹 서버에 있는 모든 가상 서버는 동일한 암호를 사용해야 합니다. 4.x 에이전트가 정책 서버에 연결하려고 할 때 에이전트와 정책 서버는 상호 인증을 위해 공유 암호를 사용합니다.

10. 제출을 클릭합니다.

4.x 웹 에이전트 개체가 생성됩니다.

에이전트 구성 개체 개요

에이전트 구성 개체에는 에이전트 구성을 정의하는 매개 변수가 보관됩니다. 구성 개체는 `LocalConfig.conf` 에이전트 구성 파일에 해당하는 정책 서버 측 요소입니다.

에이전트를 구성할 때 에이전트 구성 개체의 이름을 지정하라는 메시지가 표시됩니다. 구성 개체는 구성 중인 에이전트와 연결됩니다.

추가 정보:

[필수 에이전트 구성 개체 매개 변수](#) (페이지 133)

에이전트 구성 개체 복사

기존 에이전트 구성 개체를 복사하여 새 에이전트 구성 개체를 생성할 수 있습니다. 지원되는 웹 에이전트를 위한 샘플 에이전트 구성 개체가 제공됩니다. 새 에이전트 구성 개체를 만든 후에는 해당 매개 변수 목록과 값을 수정해야 합니다.

참고: 매개 변수 및 기본 설정에 대한 자세한 내용은 [웹 에이전트 구성 안내서](#)를 참조하십시오.

에이전트 구성 개체를 복사하려면

1. "인프라", "에이전트"를 차례로 클릭합니다.
2. "에이전트 구성 개체"를 클릭합니다.
"에이전트 구성 개체" 페이지가 표시됩니다.
3. "에이전트 구성 만들기"를 클릭합니다.
"에이전트 구성 만들기" 페이지가 표시됩니다.
4. "Create a copy of an object of type Agent Configuration"(에이전트 구성 유형 개체의 복사본 만들기) 옵션을 선택하고 다음 작업 중 하나를 수행하십시오.
 - 목록에서 기본 에이전트 구성 개체 중 하나를 선택합니다.
 - "검색"을 클릭하고 표시된 "에이전트 구성 개체" 목록에서 하나를 선택합니다.
5. "확인"을 클릭합니다.
"에이전트 구성 만들기:" 페이지가 표시됩니다.
6. 새 이름과 설명을 입력하고 "제출"을 클릭합니다.
매개 변수를 지정하거나, 계속해서 설명을 입력하라는 메시지가 표시됩니다.
7. 설명을 입력하고 "예"를 클릭합니다.
기본 에이전트 구성 개체를 기반으로 한 에이전트 구성 개체가 생성됩니다.

에이전트 구성 개체 만들기

정책 서버 설치 관리자는 기본 설정이 포함된 여러 지원되는 웹 서버에 대한 에이전트 구성 개체를 여러 개 생성합니다. 이러한 샘플 개체의 이름으로는 **IISDefaultSettings** 또는 **iPlanetDefaultSettings** 등이 있습니다. 이러한 기본 개체를 복제한 다음 이를 에이전트 구성의 템플릿으로 사용할 수 있습니다.

참고: 기존 개체를 복사하고 해당 매개 변수 목록과 값을 수정하여 새 에이전트 구성 개체를 만드는 것이 좋습니다. 기존 구성 개체를 복사하지 않고 새 에이전트 구성 개체를 만드는 경우에는 모든 매개 변수와 해당 값을 직접 입력해야 합니다.

다음 단계를 수행하십시오.

1. "인프라", "에이전트"를 차례로 클릭합니다.
2. "에이전트 구성 개체"를 클릭합니다.
"에이전트 구성 개체" 페이지가 표시됩니다.
3. "에이전트 구성 만들기"를 클릭합니다.
"Create a new object of type Agent Configuration"(에이전트 구성 유형의 새 개체 만들기) 옵션이 선택되어 있는지 확인합니다.
4. "확인"을 클릭합니다.
"에이전트 구성 만들기" 페이지가 표시됩니다.
참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.
5. 에이전트의 이름과 설명을 입력합니다.
6. "추가"를 클릭합니다.
"매개 변수 만들기" 페이지가 표시됩니다.
7. 매개 변수의 이름과 설명을 입력합니다.

8. (선택 사항) 다음 작업 중 *하나*를 수행하십시오.
 - 매개 변수의 값을 암호화하려면 "암호화" 옵션을 선택합니다.
 - 매개 변수 값을 여러 개 추가하려면 다음 작업을 수행하십시오.
 - a. "복수 값" 옵션을 선택합니다.
 - b. 매개 변수의 값을 입력합니다.
 - c. "추가"를 클릭합니다.
 - d. b 단계와 c 단계를 반복하여 원하는 값을 모두 추가합니다.
 - e. (선택 사항) 여러 값의 순서를 변경하려면 위쪽 및 아래쪽 화살표를 클릭하십시오. 여러 개의 값은 "매개 변수" 페이지에 표시될 때 대괄호(`[]`)로 구분됩니다. 값을 삭제하려면 빼기 기호를 클릭하십시오.

참고: 암호화된 매개 변수의 값은 여러 개를 입력할 수 없습니다. 하나의 암호화된 값이 기호의 문자열로 표시됩니다.
9. "확인"을 클릭합니다.

목록에 매개 변수가 추가됩니다.

참고: 매개 변수는 이름을 기준(사전순)으로 나열됩니다. 목록의 매개 변수를 편집하려면 오른쪽 화살표를 클릭하십시오. 목록에서 매개 변수를 삭제하려면 빼기 기호를 클릭하십시오. 에이전트 구성 개체에 매개 변수를 더 추가하려면 4~7 단계를 반복하십시오.
10. 제출을 클릭합니다.

에이전트 구성 개체가 생성됩니다.

필수 에이전트 구성 개체 매개 변수

에이전트 구성 개체는 다음과 같은 매개 변수에 대한 설정이 필요합니다.

- 모든 에이전트 - DefaultAgentName
- IIS 에이전트 - DefaultUserName 및 DefaultPassword
- (Domino 에이전트만 해당) DominoDefaultUser
- (Domino 에이전트만 해당) DominoSuperUser

참고: 이러한 매개 변수에 대한 자세한 내용은 "웹 에이전트 설치 안내서"를 참조하십시오.

IIS 프록시 사용자 지정

IIS 웹 에이전트는 에이전트 구성 개체에 다음과 같은 설정이 필요합니다.

DefaultUserName

IIS 프록시 사용자의 사용자 이름을 지정합니다.

DefaultPassword

IIS 프록시 사용자의 암호를 지정합니다.

참고: NTLM 인증 체계를 사용하거나 Windows 사용자 보안 컨텍스트 기능을 사용하는 경우 이러한 매개 변수를 비워두십시오.

이러한 매개 변수는 제품이 보호하는 IIS 웹 서버의 리소스에 액세스할 수 있는 권한이 있는 기존 NT 사용자 계정을 식별합니다. 액세스를 요청하는 사용자에게 필요한 서버 액세스 권한이 없을 수 있습니다. 에이전트는 이 NT 사용자 계정을 요구합니다. 관리자는 제품에 대한 프록시 사용자 계정으로 기능하는 이 NT 계정을 할당합니다.

Domino 사용자 지정

Domino 서버에 에이전트를 구성하려면 다음 설정을 시스템과 일치하도록 편집해야 합니다.

DominoDefaultUser

Domino 웹 에이전트가 Domino 서버에 대해 해당 사용자를 식별하는 데 사용하는 이름을 지정합니다. 이 상황은 사용자가 Domino Directory에 있지 않고 사용자가 또 다른 사용자 디렉터리에 대해 제품에 의해 인증된 경우 발생합니다. 이 값은 암호화될 수 있습니다.

DominoSuperUser

제품에 성공적으로 로그인한 모든 사용자가 Domino SuperUser 로서 Domino에 로그인 로그인되도록 합니다. 이 값은 암호화될 수 있습니다.

에이전트 이름 지정

모든 에이전트에 대해 DefaultAgentName 값을 지정해야 합니다.

DefaultAgentName

할당된 에이전트 아이덴티티가 없는 IP 주소에 대해 웹 에이전트가 사용하는 에이전트 아이덴티티를 식별합니다.

기본값: 기본 에이전트 이름은 설치된 웹 에이전트의 이름입니다.

에이전트 구성 매개 변수 수정

에이전트 구성 개체에서 매개 변수의 이름과 값을 편집할 수 있습니다. 매개 변수 이름은 고유해야 합니다. 매개 변수 값은 일반 값, 암호화된 값 또는 다중값일 수 있습니다. 비활성 매개 변수를 활성화하려면 파운드 기호(#)를 제거하십시오.

다음 단계를 수행하십시오.

1. "인프라", "에이전트"를 차례로 클릭합니다.
2. "에이전트 구성 개체"를 클릭합니다.
3. 검색 조건을 지정하고 "검색"을 클릭합니다.
4. 수정할 에이전트 구성 개체의 이름을 클릭합니다.
5. "수정"을 클릭합니다.
6. 매개 변수 이름 왼쪽에 있는 오른쪽 화살표를 클릭합니다.
7. 매개 변수의 값을 편집합니다.

참고: 값을 삭제하려면 빼기 기호를 클릭하십시오. 여러 값의 순서를 변경하려면 위쪽 및 아래쪽 화살표를 클릭하십시오. 하나의 매개 변수에 여러 개의 값을 지정하려면 "추가"를 클릭하십시오. 꺾쇠 기호(□)는 여러 매개 변수에서 각각을 구분합니다.

8. (선택 사항) "암호화" 옵션을 선택합니다.

참고: "암호화"를 선택하면 하나의 매개 변수에 여러 개의 값을 지정하는 옵션이 비활성화됩니다. 하나의 암호화된 값은 "매개 변수" 페이지에서 하나의 기호 문자열로 표시됩니다.

9. "확인"을 클릭합니다.

참고: 매개 변수는 이름을 기준(사전순)으로 나열됩니다. 목록의 매개 변수를 편집하려면 오른쪽 화살표를 클릭하십시오. 목록에서 매개 변수를 삭제하려면 빼기 기호를 클릭하십시오. 에이전트 구성 개체에 대한 여러 매개 변수를 편집하려면 5~8 단계를 반복하십시오.

10. 제출을 클릭합니다.

웹 에이전트 사용

WebAgent.conf 파일에서만 에이전트를 활성화 및 비활성화할 수 있습니다.

EnableWebAgent 매개 변수 값에 따라 에이전트의 사용 여부가 결정됩니다. 에이전트를 사용하려면 이 매개 변수를 **yes** 로 설정하십시오.

에이전트를 활성화하려면 다음 사전 요구 사항을 충족시키십시오.

- 정책 서버 및 에이전트 통신을 위해 필요한 모든 개체를 설정하십시오.
- 에이전트를 설치 및 구성하십시오.

RADIUS 에이전트 구성

RADIUS 에이전트 아이덴티티를 생성하려면 관리 UI 에서 에이전트 개체를 생성합니다. 개체 이름은 에이전트가 설치될 때 지정된 에이전트 이름과 일치해야 합니다. 웹 에이전트 관리 콘솔 또는 **WebAgent.conf** 파일에서 에이전트 이름을 변경한 경우에는 개체 이름도 변경해야 합니다. 정책 서버는 RADIUS 에이전트 아이덴티티를 사용하여 **NAS** 클라이언트 장치와 통신합니다. RADIUS 에이전트 개체 및 아이덴티티를 만들면 RADIUS 에이전트를 영역과 연결할 수 있습니다.

RADIUS 에이전트 아이덴티티를 만든 후에는 RADIUS 클라이언트 또는 응용 프로그램 서버에 에이전트를 설치하고 구성할 수 있습니다. RADIUS 에이전트만 로컬에서 구성할 수 있습니다.

다음 단계를 수행하십시오.

1. "인프라", "에이전트"를 차례로 클릭합니다.
2. "에이전트"를 클릭합니다.
3. "에이전트 만들기"를 클릭합니다.
4. "확인"을 클릭합니다.
5. 에이전트의 이름과 설명을 입력합니다.

제한:

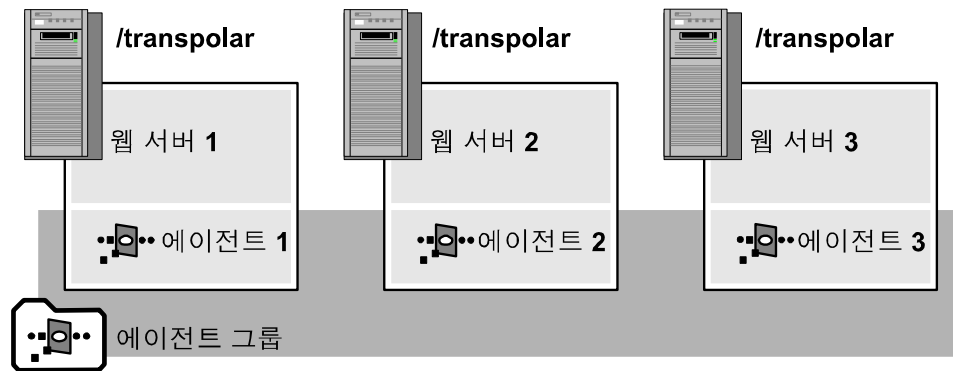
- 에이전트 이름에는 하나 이상의 인쇄 가능한 문자를 비롯하여 32-127 범위의 7 비트 ASCII 문자가 포함되어야 합니다.
 - 에이전트 이름에는 앰퍼샌드(&)와 별표(*) 문자를 사용할 수 없습니다.
 - 에이전트 이름은 대/소문자를 구분하지 않습니다. **MyAgent** 라는 이름의 에이전트가 있을 때는 **myagent** 라는 에이전트를 생성할 수 없습니다.
6. Radius 옵션을 선택한 다음 RADIUS 공급업체를 선택합니다.
참고: "에이전트 유형"으로 일반 RADIUS 를 선택하여 모든 유형의 RADIUS 장치를 보호할 수 있습니다. 일반 RADIUS 에이전트 유형은 공급업체 특정 응답 특성에 대한 액세스를 지원하지 않습니다.
 7. 다음의 트러스트 설정을 지정합니다.
 - RADIUS 클라이언트(NAS 장치)의 IP 주소를 입력합니다.
 - 영숫자 공유 암호를 입력하고 확인합니다.

8. RADIUS 영역 힌트의 번호를 입력합니다.
9. 제출을 클릭합니다.

에이전트 그룹

에이전트 그룹은 유형이 같은 에이전트의 집합입니다. 이러한 에이전트 그룹을 사용하면 많은 웹 서버에서 리소스가 중복된 경우 더 큰 사용자 집합에게 동일한 리소스에 대한 액세스를 허가할 수 있습니다. 그룹은 또한 모든 웹 에이전트에 대해 정책을 하나만 정의하면 되므로 시간도 절약됩니다. 에이전트 그룹은 동일한 리소스에 대한 액세스를 제공하기 위해 라운드 로빈 처리를 사용하는 웹 서버 그룹을 보호할 수 있습니다.

다음 그림은 하나의 정책 집합을 사용하여 웹 팜을 보호하는 방법을 설명합니다. 하나의 에이전트 그룹이 이 정책 집합에 바인딩되었습니다.



에이전트를 만들기 전에 에이전트 그룹을 만들 수 있습니다. 에이전트 그룹을 편집하고 새 에이전트를 그룹에 추가하십시오.

참고: 에이전트 그룹의 구성 설정을 에이전트 구성 개체와 공유하십시오.

추가 정보:

[정책](#) (페이지 621)

에이전트 그룹 구성

에이전트 그룹을 사용하여 공용 리소스를 보호하는 에이전트를 보다 효율적으로 관리하십시오. 그룹 내의 에이전트는 모두 유형이 동일해야 합니다.

다음 단계를 수행하십시오.

1. "인프라", "에이전트"를 차례로 클릭합니다.
2. "에이전트 그룹"을 클릭합니다.
3. "에이전트 그룹 만들기"를 클릭합니다.
4. "확인"을 클릭합니다.
5. 에이전트 그룹의 이름과 설명을 입력합니다.
6. "에이전트 스타일" 및 "에이전트 유형"을 선택합니다.

참고: 에이전트 그룹에는 모든 웹 에이전트, 모든 가맹 에이전트 또는 모든 RADIUS 에이전트와 같은 한 가지 유형의 에이전트만 포함될 수 있습니다.

7. "추가/제거"를 클릭합니다.

참고: 지정된 에이전트 유형의 에이전트만 "사용 가능한 구성원" 아래에 나열됩니다. 예를 들어 지정된 에이전트 스타일이 Radius 이고 지정된 에이전트 유형이 3-Com 인 경우에는 3-Com 에이전트만 나열됩니다. 지정된 에이전트 유형이 "일반 Radius"인 경우에는 모든 RADIUS 에이전트가 나열됩니다.

8. "사용 가능한 구성원" 목록에서 하나 이상의 에이전트를 선택하고 오른쪽 방향 화살표를 클릭합니다.
9. "확인"을 클릭합니다.
10. 제출을 클릭합니다.

에이전트 그룹에 에이전트 추가

기존 에이전트를 에이전트 그룹에 추가할 수 있습니다.

다음 단계를 수행하십시오.

1. "인프라", "에이전트"를 차례로 클릭합니다.
2. "에이전트 그룹"을 클릭합니다.
3. 검색 조건을 지정하고 "검색"을 클릭합니다.
4. 수정할 에이전트 그룹의 이름을 클릭합니다.
5. "수정"을 클릭합니다.
6. "추가/제거"를 클릭합니다.

참고: 지정된 에이전트 유형의 에이전트만 "사용 가능한 구성원" 아래에 나열됩니다. 예를 들어 지정된 에이전트 스타일이 **Radius** 이고 지정된 에이전트 유형이 **3-Com** 인 경우에는 **3-Com** 에이전트만 나열됩니다. 지정된 에이전트 유형이 "일반 **Radius**"인 경우에는 모든 **RADIUS** 에이전트가 나열됩니다.

7. "사용 가능한 구성원" 목록에서 하나 이상의 에이전트를 선택하고 오른쪽 방향 화살표를 클릭합니다.
8. "확인"을 클릭합니다.
9. 제출을 클릭합니다.

사용자 지정 에이전트

사용자 지정 에이전트를 생성하려면 **C** 또는 **Java** 버전의 에이전트 **API** 를 사용하십시오. 에이전트 **API** 및 관련 설명서는 별도로 제공되는 소프트웨어 개발 키트에 포함되어 있습니다.

사용자 지정 에이전트를 개발한 후에는 새 에이전트 유형을 구성하십시오. 에이전트 유형은 에이전트의 동작을 정의하며 사용자 지정 에이전트를 사용하여 리소스를 보호할 수 있게 해 줍니다. 예를 들어 사용자 지정 **FTP** 에이전트를 개발한 후에는 **FTP** 에이전트 유형을 정의해야 합니다.

사용자 지정 에이전트 유형 구성

사용자 지정 에이전트 유형을 구성하여 사용자 지정 에이전트의 동작을 정의하고 에이전트 개체를 생성할 때 이 사용자 지정 에이전트를 식별하십시오. 제품에 포함된 API 를 사용하여 에이전트 유형을 만드십시오.

에이전트 아이덴티티에 대한 사용자 지정 에이전트 개체 만들기

사용자 지정 에이전트 아이덴티티를 생성하려면 관리 UI 에서 에이전트 개체를 생성합니다. 에이전트 개체 및 아이덴티티를 만들면 에이전트를 영역과 연결할 수 있습니다.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다.

다음 단계를 수행하십시오.

1. "인프라", "에이전트"를 차례로 클릭합니다.
2. "에이전트"를 클릭합니다.

"에이전트" 페이지가 표시됩니다.

3. "에이전트 만들기"를 클릭합니다.

"Create a new object of type Agent"(에이전트 유형의 새 개체 만들기) 옵션이 선택되어 있는지 확인합니다.

4. "확인"을 클릭합니다.

"에이전트 만들기" 페이지가 표시됩니다.

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

5. 에이전트의 이름과 설명을 입력합니다.

제한:

- 에이전트 이름에는 하나 이상의 인쇄 가능한 문자를 비롯하여 32-127 범위의 7 비트 ASCII 문자가 포함되어야 합니다.
- 에이전트 이름에는 앰퍼샌드(&)와 별표(*) 문자를 사용할 수 없습니다.
- 에이전트 이름은 대/소문자를 구분하지 않습니다. 즉, MyAgent 라는 이름의 에이전트가 있을 때는 myagent 라는 다른 에이전트를 생성할 수 없습니다.

6. "에이전트 스타일"로 **SiteMinder** 를 선택하고 "에이전트 유형"으로 "웹 에이전트"를 선택하고, "4.x 에이전트 지원" 옵션을 선택합니다.

"트러스트 설정" 필드가 표시됩니다.

7. 에이전트가 있는 서버의 IP 주소를 입력합니다.
8. 공유 암호를 입력하고 확인합니다.

제한:

- 제공하는 암호는 웹 서버에 에이전트를 설치할 때 할당된 암호와 일치해야 합니다.
- 암호에는 최소 하나의 문자가 포함되어야 하며 255 자를 넘지 않아야 합니다.
- 암호에는 영숫자만 사용할 수 있습니다.
- 암호에는 포함된 공백을 사용할 수 없습니다.

9. 제출을 클릭합니다.

에이전트 개체가 생성됩니다.

에이전트 검색

에이전트 검색을 사용하면 다른 에이전트 유형 및 버전의 인스턴스를 검색할 수 있습니다. 에이전트가 검색되면 버전, 상태 등 각 에이전트의 상세 정보를 볼 수 있습니다. 또한 엔터프라이즈의 다양한 호스트에 배포된 에이전트 목록을 확인하고 원하지 않는 에이전트 인스턴스 항목을 목록에서 삭제할 수도 있습니다.

참고: 에이전트 검색은 기존 에이전트를 지원하지 않습니다.

하트비트 메시지는 **r12.5** 에이전트를 식별하는 데 도움이 됩니다. 에이전트에서 정책 서버에 하트비트 메시지를 보내는 빈도를 하트비트 간격이라고 합니다. 하트비트 간격을 나타내는

MinTimeBetweenAgentStatusUpdates 매개 변수는 정책 서버가 저장소에서 에이전트 인스턴스 개체를 업데이트하기 전에 대기해야 하는 최소 시간을 제어합니다. 최소 대기 시간이 경과하기 전에 정책 서버가 수신하는 하트비트 메시지는 모두 무시됩니다. 이 매개 변수의 기본값은 24 시간이고 최소값은 1 시간입니다. 에이전트는 **MinTimeBetweenAgentStatusUpdates** 매개 변수에 설정된 시간이 경과했는지 여부에 관계없이 시작할 때 식별합니다.

에이전트 검색은 에이전트 버전에 관계없이 정기적으로 정책 서버와 통신하는 모든 에이전트를 식별합니다. 에이전트 검색은 r12.5 이전 버전의 에이전트를 식별하기 위해 에이전트의 트러스트된 호스트와 IP 주소를 조합하여 사용합니다. 에이전트의 이 조합이 변경되면 같은 에이전트에 대해 여러 항목이 나타나게 됩니다.

에이전트 검색은 r12.5 보다 오래된 ASA 에이전트를 인식하지 않습니다. 이러한 오래된 에이전트는 정책 서버에 어떠한 정보도 보내지 않습니다. ASA 에이전트의 특성은 "에이전트 인스턴스" 목록에 알 수 없는 특성으로 표시됩니다. ASA 에이전트 호스트에 r12.5 이전 버전의 다른 에이전트가 있는 경우 이 에이전트가 동일한 호스트 및 트러스트된 호스트 조합을 사용하면 목록에서 ASA 항목이 숨겨집니다.

관리 UI 의 "인프라"에 있는 "에이전트 인스턴스"를 사용하면 엔터프라이즈에 배포된 에이전트 인스턴스 목록을 볼 수 있습니다.

참고: r12.5 이전 버전의 에이전트인 경우 IP 주소가 호스트 이름으로 표시됩니다.

에이전트 인스턴스 목록

에이전트 인스턴스 목록을 표시하여 엔터프라이즈 전체에 배포된 에이전트의 수를 확인할 수 있습니다. 또한 검색 조건을 지정하여 에이전트 인스턴스 목록을 볼 수도 있습니다. 검색 조건은 에이전트 인스턴스의 특성이 될 수 있습니다.

이 목록에서 에이전트 인스턴스와 관련된 모든 정보를 확인하고 하나 이상의 에이전트 인스턴스 항목을 삭제할 수 있습니다. r12.5 이전 버전의 에이전트를 삭제하면 트러스트된 호스트를 제외한 모든 에이전트 특성이 목록에 표시되지 않습니다. 삭제된 에이전트를 다시 시작하면 해당 에이전트의 모든 특성이 다시 목록에 나타납니다.

참고: 에이전트 인스턴스 항목을 삭제한 후에도 해당 에이전트 인스턴스는 정책 서버와 정기적으로 통신하는 동안 활성 상태를 유지합니다.

에이전트 인스턴스의 특성을 정렬하면 선택한 특성을 사용하는 에이전트 인스턴스의 목록을 확인할 수 있습니다.

다음 단계를 수행하십시오.

1. "인프라", "에이전트"를 차례로 클릭합니다.
2. "에이전트 인스턴스"를 클릭합니다.
3. "상세 정보 표시" 아래의 아이콘을 클릭합니다.

참고: r12.5 보다 오래된 에이전트의 경우 구성 모드는 "FIPS 전용" 또는 "Compact"(압축)입니다. 관리 UI에는 서버와 에이전트 간 통신에 사용되는 실제 모드에 따라 상세 정보가 표시됩니다.

4. (선택 사항) "검색" 필드에 검색 조건을 지정합니다.
검색 조건에 따라 에이전트 인스턴스 목록이 필터링됩니다.
5. (선택 사항) 특성 제목 표에서 화살표를 클릭하여 선택한 특성을 기준으로 에이전트 인스턴스 목록을 정렬합니다.

정책 서버 하트비트 간격 구성

하트비트 간격은 에이전트 검색이 에이전트 상태를 판별하는 데 도움이 됩니다. 24 시간이 지날 때까지 에이전트가 하트비트 메시지를 보내지 않으면 에이전트 인스턴스가 비활성 상태로 변경됩니다. 기본값인 24 시간을 변경하도록 하트비트 간격을 구성할 수 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버를 호스트하는 컴퓨터에서 명령 프롬프트를 엽니다.
2. 다음 명령을 입력합니다.
`XPSConfig`
3. SM 를 입력합니다.
4. MinTimeBetweenAgentStatusUpdates 옵션에 대한 값을 입력합니다.
5. C 를 입력합니다.
6. 새 값을 입력합니다.
기본값: 24 시간
최소값: 1 시간
7. Q 를 세 번 입력합니다.

에이전트 검색 비활성화

일부 환경에서는 에이전트 검색으로 인해 데이터베이스 다중 마스터 복제 흐름이 발생할 수 있습니다. 필요한 경우 에이전트 검색을 비활성화할 수 있습니다. 에이전트 검색을 비활성화하려면 **XPSConfig** 도구를 사용하여 전역 구성 매개 변수 **AgentDiscoveryEnabled** 에 값을 할당하십시오. 이 매개 변수는 다음과 같은 값을 지원합니다.

0=비활성화된

1=자동 검색

2=활성화된

기본값은 자동 검색인 1 입니다. 이 경우 정책 저장소에서 모든 에이전트 인스턴스 개체를 검색할 수 있습니다. 개체를 찾지 못하면 이 값은 0 으로 업데이트되며, 에이전트 인스턴스 개체를 찾은 경우 이 값은 2 로 업데이트됩니다. 에이전트 검색이 비활성화되면 정책 서버 추적 로그에 추적 메시지가 표시됩니다. 이 매개 변수의 값을 변경하는 경우에는 변경 내용이 반영되도록 정책 서버를 다시 시작하십시오.

제 6 장: 사용자 디렉터리

이 섹션은 다음 항목을 포함하고 있습니다.

[사용자 디렉터리 연결 개요](#) (페이지 148)

[CA Directory 사용자 디렉터리 연결을 구성하는 방법](#) (페이지 152)

[CA LDAP Server for z/OS 사용자 디렉터리 연결 구성 방법](#) (페이지 155)

[Oracle Directory Server Enterprise Edition 사용자 디렉터리 연결을 구성하는 방법](#) (페이지 167)

[IBM Directory Server 사용자 디렉터리 연결을 구성하는 방법](#) (페이지 168)

[Domino 사용자 디렉터리를 사용자 저장소로 구성하는 방법](#) (페이지 169)

[Novell eDirectory LDAP 디렉터리 연결을 구성하는 방법](#) (페이지 171)

[Active Directory LDS 사용자 디렉터리 연결 구성 방법](#) (페이지 176)

[Active Directory 사용자 저장소 연결을 구성하는 방법](#) (페이지 178)

[Active Directory 글로벌 카탈로그 사용자 디렉터리 연결을 구성하는 방법](#) (페이지 188)

[Oracle Internet Directory 사용자 디렉터리 연결을 구성하는 방법](#) (페이지 190)

[OpenLDAP 서버 사용자 디렉터리 연결을 구성하는 방법](#) (페이지 192)

[Red Hat Directory Server 사용자 디렉터리 연결을 구성하는 방법](#) (페이지 193)

[ODBC 사용자 디렉터리 연결을 구성하는 방법](#) (페이지 194)

[사용자 지정 사용자 디렉터리 연결을 구성하는 방법](#) (페이지 200)

[SSL 을 통한 LDAP 사용자 디렉터리 연결 구성 방법](#) (페이지 202)

[SSL 을 통한 Oracle 사용자 디렉터리 연결 구성](#) (페이지 210)

[LDAP 부하 분산 및 장애 조치](#) (페이지 213)

[ODBC 데이터 원본 장애 조치 구성](#) (페이지 217)

[SQL 쿼리 체계](#) (페이지 218)

[여러 정책 저장소에 동일한 사용자 디렉터리 연결 정의](#) (페이지 224)

[사용자 디렉터리 콘텐츠 보기](#) (페이지 225)

[사용자 디렉터리 검색](#) (페이지 226)

[유니버설 ID](#) (페이지 226)

[명명된 식](#) (페이지 227)

[사용자 특성 매핑](#) (페이지 244)

사용자 디렉터리 연결 개요

사용자 아이덴티티를 확인하기 위해 정책 저장소는 사용자 디렉터리를 사용하여 저장소 조직 정보, 사용자 특성, 사용자 자격 증명을 저장합니다. 관리 UI 를 통해 기존 사용자 디렉터리 및 데이터베이스에 대한 연결을 구성합니다. 이러한 디렉터리 연결은 정책 서버가 사용자 아이덴티티에 대한 컨텍스트를 구성하는 방법을 결정합니다.

정책 서버는 다음과 같은 유형의 사용자 디렉터리를 지원합니다.

- LDAP
- ODBC
- Oracle
- 사용자 지정

LDAP 개요

정책 서버는 LDAP(Lightweight Data Access Protocol)을 사용하는 사용자 디렉터리와 통신할 수 있습니다. 정책 서버는 LDAP 사용자 저장소에 연결할 때 세 개의 연결을 엽니다.

- 첫 번째 연결은 사용자 저장소가 시작되어 실행 중인지 확인합니다. 기본적으로 정책 서버는 이 연결에서 30 초마다 사용자 저장소에 연결합니다.
- 두 번째 연결은 검색 및 업데이트에 사용됩니다. 예를 들어 정책 서버는 바인딩 실패 시 사용자를 조회하고 특성을 설정하는 데 이 연결을 사용합니다.
- 세 번째 연결은 자격 증명을 테스트하는 데 사용됩니다. 정책 서버는 제공된 자격 증명을 사용하여 사용자 저장소에 바인딩하려고 합니다. 바인딩 시도의 결과는 자격 증명의 허용 여부를 결정합니다.

ODBC 데이터베이스 개요

SiteMinder 는 ODBC 호환 데이터베이스의 전용 스키마를 인증 및 권한 부여용 사용자 디렉터리로 사용할 수 있습니다. 정책 서버는 다음 유형의 ODBC 호환 데이터베이스에 대한 연결을 지원합니다.

- Microsoft SQL Server - Windows 정책 서버만 해당
- Oracle RDBMS

정책 서버가 데이터베이스를 사용자 디렉터리로 사용하도록 구성하려면:

- "SQL 쿼리 체계" 창의 필드에 SQL 쿼리 정보를 입력합니다. 이 창은 "사용자 디렉터리" 창에서 액세스할 수 있습니다. 이 창의 필드는 정책 서버와 ODBC 호환 데이터베이스 사이에서 정보를 매핑합니다.
참고: 각 쿼리 체계에 사용할 고유한 데이터 원본을 생성하십시오.
- 사용자 정보가 포함된 데이터베이스를 가리키는 ODBC 데이터 원본을 정의합니다. ODBC 데이터 원본을 시스템 DSN 으로 구성하십시오. 데이터 원본은 Microsoft SQL Server 데이터베이스나 Oracle 데이터베이스를 가리킵니다.

Active Directory 개요

SiteMinder 는 Microsoft Active Directory 플랫폼에서 사용자 디렉터리를 지원합니다. Active Directory(AD) 및 LDAP 네임스페이스에 대한 구성은 일부 기능 차이를 제외하고는 유사합니다.

Active Directory 사용자 저장소를 구성할 때 AD 네임스페이스를 사용하면 다음과 같은 장점이 있습니다.

- 네이티브 Windows 인증서 데이터베이스를 사용하는 SSL 연결이 사용됩니다.
참고: 정책 서버와 Active Directory 사용자 저장소를 호스트하는 시스템 모두에 트러스트가 설정되어 있어야 합니다.
- 보안 LDAP 바인딩 작업을 허용하는 네이티브 Windows SASL 이 지원됩니다.

Active Directory 사용자 저장소를 구성할 때 AD 네임스페이스를 사용하면 다음과 같은 장점이 있습니다.

- 향상된 LDAP 조회가 지원되지 않습니다.
- LDAP 페이징 및 정렬 작업이 지원되지 않습니다.

참고: 정책 서버가 UNIX 운영 체제에 설치되어 있으면 AD 사용자 저장소에 연결하는 데 AD 네임스페이스를 사용할 수 없습니다.

사용자 지정 디렉터리 개요

관리 UI 는 SiteMinder 디렉터리 API 를 사용하여 공유 라이브러리를 생성함으로써 사용자 지정 사용자 디렉터리 연결을 가능하게 합니다. 이 C 언어 API 는 소프트웨어 개발 키트에 별도로 제공됩니다. 정책 서버는 사용자 지정 연결을 통해 레거시 디렉터리와 상호 작용할 수 있습니다. "사용자 디렉터리" 창에서 사용자 지정 네임스페이스를 구성합니다.

디렉터리 특성 개요

일부 기능을 사용하려면 7 개의 SiteMinder 특성에 대한 읽기 또는 쓰기 액세스 권한이 필요합니다. 이 특성 값은 정책 서버에 연결된 사용자 디렉터리에 있습니다. 디렉터리 사용자 특성을 "사용자 특성" 섹션의 SiteMinder 특성과 매핑합니다. 또한 특성 매핑을 사용하여 자체 일반 이름을 정의할 수도 있습니다. 각 이름을 여러 사용자 디렉터리의 사용자 특성 이름과 매핑할 수 있습니다.

다음 표에 설명된 것처럼 각 SiteMinder 특성은 데이터 형식 하나와 디렉터리 유형 하나 이상에 연결됩니다. (R)은 특성에 대한 읽기 권한이 필요함을 나타내고 (RW)는 특성에 대한 읽기/쓰기 권한이 필요함을 나타냅니다.

특성 이름	데이터 형식	디렉터리 유형	설명
유니버설 ID(R)	문자열	LDAP 데이터베이스 WinNT	SiteMinder 가 사용자 아이덴티티를 관리하기 위해 보호된 응용 프로그램에 전달하는 유니버설 ID 또는 사용자 식별자를 지정합니다. 이 기능은 대개 특성을 사용하여 사용자를 식별하는 레거시 응용 프로그램과 SiteMinder 간의 브리지 역할을 합니다. 유니버설 ID 는 디렉터리 매핑을 구성하는 데도 사용됩니다.
비활성화된 플래그(RW)	문자열	LDAP 데이터베이스	사용자 계정의 상태를 지정합니다. 자세한 내용은 <i>정책 서버 관리 안내서</i> 를 참조하십시오.

특성 이름	데이터 형식	디렉터리 유형	설명
암호 특성(RW)	바이너리	LDAP 데이터베이스	사용자 암호를 지정합니다.
암호 데이터(RW)	바이너리	LDAP 데이터베이스	암호 정책 정보를 추적하는 데 사용됩니다.
익명 ID(RW)	문자열	LDAP 데이터베이스	익명 인증 체계를 사용하여 인증된 사용자의 DN 을 저장합니다.
전자 메일(R)	문자열	LDAP 데이터베이스	이 특성은 현재 SiteMinder 기능에 사용되지 않습니다.
챌린지/응답(RW)	문자열	LDAP	암호 서비스와 DMS 에서 암호를 잊은 경우에 사용되는 질문과 대답 쌍을 지정합니다. 챌린지 문자열은 사용자에게 전달되는 암호 힌트입니다.

참고: 정책 서버가 디렉터리에 액세스하는 데 사용하는 관리자 자격 증명을 지정할 수 있습니다. 이러한 자격 증명은 표에 나오는 해당 사용자 특성과 동일한 읽기 및 쓰기 권한을 가지고 있습니다.

추가 정보:

[사용자 특성 매핑](#) (페이지 244)

CA Directory 사용자 디렉터리 연결을 구성하는 방법

다음 프로세스에는 정책 서버에 대한 CA Directory 사용자 저장소 연결을 생성하는 단계가 나와 있습니다.

1. CA Directory 사용자 디렉터리 연결을 구성합니다.
2. 사용자 저장소 DSA 매개 변수를 활성화합니다.
3. (선택 사항) CA Directory 사용자 저장소에 대한 캐싱을 활성화합니다.
4. (선택 사항) CA Directory 캐시 구성을 확인합니다.

사용자 저장소 시스템 ping

정책 서버와 사용자 디렉터리 또는 데이터베이스 사이에 네트워크 연결이 있는지 확인하기 위해 구성하기 전에 사용자 저장소 시스템을 ping 하십시오.

참고: 일부 사용자 저장소 시스템의 경우 정책 서버가 자격 증명을 제공해야 합니다.

CA Directory 사용자 디렉터리 연결 구성

정책 서버가 CA Directory 사용자 저장소와 통신할 수 있도록 사용자 디렉터리 연결을 구성할 수 있습니다.

다음 단계를 수행하십시오.

1. "인프라", "디렉터리"를 차례로 클릭합니다.
2. "사용자 디렉터리"를 선택합니다.
3. "사용자 디렉터리 만들기"를 클릭합니다.
4. "일반" 및 디렉터리 설정 영역에서 필요한 연결 정보를 지정합니다.
5. "LDAP 설정" 영역에서 "LDAP 검색" 및 "LDAP 사용자 DN 조회" 설정을 구성합니다.
6. "관리자 자격 증명" 영역에서 "자격 증명 필요"를 선택합니다.
7. 관리자 계정의 자격 증명을 입력합니다.
8. (선택 사항) "사용자 특성" 영역에서 예약된 사용자 디렉터리 프로필 특성을 지정합니다.

9. (선택 사항) "특성 매핑 목록" 영역에서 "만들기"를 클릭하여 사용자 특성 매핑을 구성합니다.
10. 제출을 클릭합니다.
사용자 디렉터리 연결이 생성됩니다.

사용자 저장소 DSA 매개 변수 사용

정책 서버는 각 인증 요청에 대한 바인드 요청을 수행하여 CA Directory에 연결합니다. 이러한 요청을 처리하도록 CA Directory를 구성하십시오. 그렇지 않으면 연결 수가 부족해 인증이 실패합니다.

다음 단계를 수행하십시오.

1. 사용자 저장소 DSA의 .dxi 파일을 엽니다.
2. 파일 맨 아래에 다음 항목을 정의합니다.

```
#SiteMinder
set mimic-netscape-for-siteminder = true;
set concurrent-bind-user = DN;
set hold-ldap-connections = true;
```

3. .dxi 파일을 저장한 후 닫습니다.

사용자 저장소 DSA 매개 변수가 활성화됩니다.

참고: DN은 x500 형식입니다.

예: <o acme><cn smadmin>

CA Directory 사용자 저장소에 대해 캐싱이 사용되도록 설정

CA Directory DXcache 기능이 사용되도록 설정하여 대규모 사용자 저장소에 대한 인증 및 권한 부여 성능을 개선할 수 있습니다. 사용자 저장소 크기가 5 MB 이면 대규모로 간주됩니다.

다음 단계를 수행하십시오.

1. dsa 사용자가 DXI 파일(예:
<dxserver_install>\config\servers\eTrustDsa.dxi)의 끝에 다음 줄을
추가합니다.

■ **r12**

```
# cache configuration
set max-cache-size = 100;
set cache-index = commonName, surname, objectClass;
set cache-attrs = all-attributes;
set cache-load-all = true;
set lookup-cache = true;
```

참고: max-cache-size 항목은 총 캐시 크기(MB)입니다. CA Directory Server의 사용 가능한 총 메모리와 사용자 저장소의 전체 크기에 따라 이 값을 조정하십시오. 또한 cache-index 필드를 사용자 저장소에서 사용자 검색을 수행하기 위해 사용된 필드로 설정하십시오. 예를 들어 사용자가 사용자의 일반 이름(cn=*)을 기반으로 인증되고 권한이 부여되는 경우 cache-index에 commonName을 설정해야 합니다.

■ **r12 SP1 이상**

```
# cache configuration
set ignore-name-bindings = true;
```

2. dsa 사용자 권한으로 사용자 DSA를 중지했다가 다시 시작하여 DXcache 구성 변경 내용을 적용합니다.

```
dxserver stop eTrustDsa
dxserver start eTrustDsa
```

CA Directory 캐시 구성 확인

사용자 저장소에 대해 CA DXcache 기능을 구성한 후에는 DXmanager 사용자 인터페이스를 사용하여 캐시가 사용되도록 설정되었는지 확인할 수 있습니다.

다음 단계를 수행하십시오.

1. 웹 브라우저에서 CA DXmanager 웹 인터페이스에 연결합니다.

예를 들면 다음과 같습니다.

`http://<CA_host>:8080/dxmanager/ManagerServlet?hostgroup=All`

2. DSA 구성 페이지로 이동하여 정책 저장소 DSA에 대해 "DXcache 상태" 필드가 "사용"으로 설정되었는지 확인합니다.

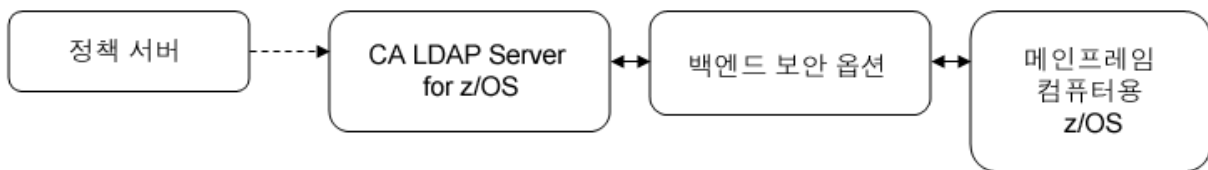
CA LDAP Server for z/OS 사용자 디렉터리 연결 구성 방법

다음 프로세스에는 정책 서버에 대한 CA LDAP Server for z/OS 사용자 저장소 연결을 구성하는 단계가 나와 있습니다.

1. 다음 정보를 검토합니다.
 - CA LDAP Server for z/OS 개요
 - CA LDAP Server for z/OS 에서 지원하지 않는 SiteMinder 기능
 - CA Top Secret r12(TSS) 백엔드 보안 옵션과 해당 개체 클래스 계층
 - CA LDAP Server for z/OS r15(ACF2) 백엔드 보안 옵션과 해당 개체 클래스 계층
 - CA LDAP Server for z/OS r15(RACF) 백엔드 보안 옵션과 해당 네임스페이스 계층
2. TSS, ACF2 또는 RACF 에 대한 정책 서버 레지스트리 항목을 구성합니다.
3. 사용자 디렉터리 연결을 구성합니다.

CA LDAP Server for z/OS 개요

정책 서버에서 CA LDAP Server for z/OS 로의 연결을 구성하여 LDAP Server 를 사용자 저장소로 구성할 수 있습니다. 정책 서버에서 LDAP Server 로의 연결을 구성하는 방법은 LDAP Server 보안에 사용하는 백엔드 옵션에 따라 달라집니다.



CA 에서는 CA LDAP Server 에 다음과 같은 백엔드 보안 옵션을 지원합니다.

- CA Top Secret r12(TSS)
- CA LDAP Server r15 for z/OS(RACF)
- CA LDAP Server r15 for z/OS(ACF2)

정책 서버에서 LDAP Server 로의 연결을 구성하기 전에 이러한 백엔드 보안 옵션의 개체 클래스 계층에 대해 잘 알아 두십시오. 또한 LDAP 네임스페이스의 정책 서버 레지스트리에 백엔드 관련 개체 클래스를 추가하십시오.

참고: z/OS 는 메인프레임 컴퓨터용 IBM 운영 체제입니다.

CA LDAP Server for z/OS(TSS)에서 지원하지 않는 SiteMinder 기능

CA LDAP Server for z/OS 는 다음 기능을 지원하지 않습니다.

암호 서비스

암호 서비스가 지원되지 않습니다.

익명 바인딩

CA LDAP Server r15 for z/OS 를 사용자 저장소로 구성하는 경우 "사용자 디렉터리 만들기" 페이지에서 "관리자 자격 증명" 값을 제공하십시오.

사용자 이름에 지원되지 않는 문자

사용자 이름에 지원되지 않는 문자는 다음과 같습니다.

- 공백
- 작은따옴표
- 여는 괄호
- 닫는 괄호
- 쉼표
- 백슬래시

사용자 그룹 및 정책

사용자 그룹을 정책에 추가하고 해당 그룹의 사용자에게 권한을 부여하려고 하면 실패합니다.

부하 분산 및 장애 조치(TSS)

부하 분산 및 장애 조치가 지원되지 않습니다.

LDAP 장애 조치 및 복제(RACF 및 ACF2)

LDAP 장애 조치 및 복제가 지원되지 않습니다.

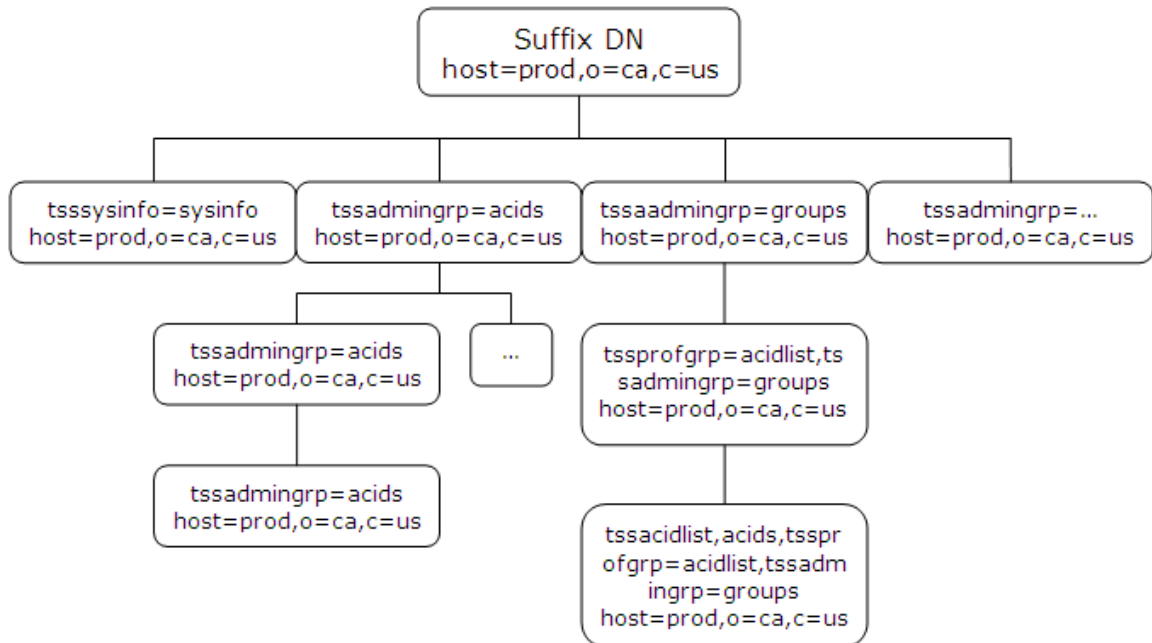
CA Top Secret r12(TSS) 백엔드 보안 옵션

CA LDAP Server for z/OS 의 보안에 TSS 를 사용하는 경우 정책 서버에서 CA LDAP Server 로의 연결을 구성하기 전에 다음 단계를 완료하십시오.

1. TSS 개체 클래스 계층에 대해 잘 알아 둡니다.
2. LDAP 네임스페이스의 정책 서버 레지스트리에 TSS 개체 클래스를 추가합니다.

TSS 개체 클래스 계층

다음 다이어그램에서는 CA Top Secret DIT(디렉터리 정보 트리)에 있는 개체 클래스 항목의 계층을 보여 줍니다. 다이어그램 아래에는 각 개체 클래스에 대한 설명이 나옵니다.



host 개체 클래스

CA Top Secret 데이터베이스의 개체 클래스 계층에 대한 액세스를 시작하는 데 사용되는 개체 클래스입니다.

tsssysinfo 개체 클래스

개체 클래스 계층에서 호스트 아래에 분기를 생성하는 데 사용되는 개체 클래스입니다.

tssadmingrp 개체 클래스

개체 클래스 계층에서 호스트 아래에 분기를 생성하는 데 사용되는 개체 클래스입니다.

값:

- acids
- profiles
- 그룹
- departments
- divisions
- zones

tssacid 개체 클래스

모든 사용자 유형의 ACID 레코드 필드에 액세스하는 데 사용되는 개체 클래스입니다.

tssacidgrp 개체 클래스

개체 클래스 계층에서 acid 아래에 분기를 생성하는 데 사용되는 개체 클래스입니다.

TSS 에 대한 정책 서버 레지스트리 항목 구성

CA LDAP Server for z/OS 에는 다른 LDAP 서버와는 구별되는 개체 클래스가 있습니다. 정책 서버에서 CA LDAP Server 로의 연결을 구성하기 전에 LDAP 네임스페이스의 특정 정책 서버 레지스트리 항목에 TSS 개체 클래스를 추가해야 합니다. 다음 정책 서버 레지스트리 항목의 기본값을 대체 값으로 바꿉니다.

registry_entry_home

다음 레지스트리 항목 위치를 지정합니다.

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Ds.

default_value

레지스트리 항목의 기본값을 지정합니다.

replacement_value

레지스트리 항목에 대해 TSS 개체 클래스를 포함하는 새 값을 지정합니다.

- registry_entry_home\ClassFilters
class_filters_default_value:
organization,organizationalUnit,groupOfNames,groupOfUniqueNames,group
class_filters_replacement_value:
class_filters_default_value,eTTSSAcidName,tssacidgrp,tssadmingrp
- registry_entry_home\GroupClassFilters
group_class_filters_default_value:
groupOfNames,groupOfUniqueNames,group
group_class_filters_replacement_value:
group_class_filters_default_value,eTTSSAcidName,tssacidgrp,tssadmingrp
- registry_entry_home\PolicyClassFilters
policy_class_filters_default_value:
organizationalPerson,inetOrgPerson,organization,organizationalUnit,
groupOfNames,groupOfUniqueNames,group
policy_class_filters_replacement_value:
policy_class_filters_default_value,eTTSSAcidName,tssacidgrp,tssadmingrp
- registry_entry_home\PolicyResolution

다음 TSS 개체 클래스를 이 레지스트리 항목에 추가합니다.

TSS 개체 클래스	레지스트리 키 종류	Data
eTTSSAcidName	REG_DWORD	0x00000001(1)
tssacid	REG_DWORD	0x00000001(1)
tssacidgrp	REG_DWORD	0x00000002(2)
tssadmingrp	REG_DWORD	0x00000003(3)

참고: 정책 서버가 실행하는 일부 LDAP 쿼리(예: 전체 사용자 목록)는 완료되는 데 최대 60 초가 소요될 수 있습니다. 이러한 경우 정책 서버 측에서 실행한 대부분의 쿼리는 시간 만료됩니다. 연결 성능을 개선하려면 이 레지스트리 키 항목을 다음과 같이 수정하면 됩니다.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Debug]
```

```
LDAPpingTimeout = 300;          REG_DWORD
```

CA LDAP Server for z/OS 사용자 디렉터리 연결 구성

정책 서버가 사용자 저장소와 통신할 수 있도록 사용자 디렉터리 연결을 구성합니다.

참고: 이 LDAP 서버에서는 부하 분산 및 장애 조치가 지원되지 않습니다.

다음 단계를 수행하십시오.

1. "인프라", "디렉터리"를 차례로 클릭합니다.
2. "사용자 디렉터리"를 선택합니다.
3. "사용자 디렉터리 만들기"를 클릭합니다.
4. "일반" 및 디렉터리 설정 영역에서 필요한 연결 정보를 지정합니다.
5. "LDAP 설정" 영역에서 "LDAP 검색" 및 "LDAP 사용자 DN 조회" 설정을 구성합니다.

참고: "최대 시간"에는 100 을 입력해야 합니다. 정책 서버가 현재 LDAP 서버에서 데이터를 검색하려면 이 정도의 시간이 필요합니다.

6. "관리자 자격 증명" 영역에서 다음 작업을 수행하십시오.
 - a. "자격 증명 필요" 옵션을 선택합니다.
 - b. "사용자 이름"에 관리자의 전체 DN 을 입력합니다.
 - c. "암호"에 관리자 암호를 입력합니다.

참고: TSS 에서는 사용자 저장소에 대한 익명 바인딩을 허용하지 않습니다.

7. (선택 사항) "사용자 특성" 영역에서 SiteMinder 용으로 예약된 사용자 디렉터리 프로필 특성을 지정합니다.

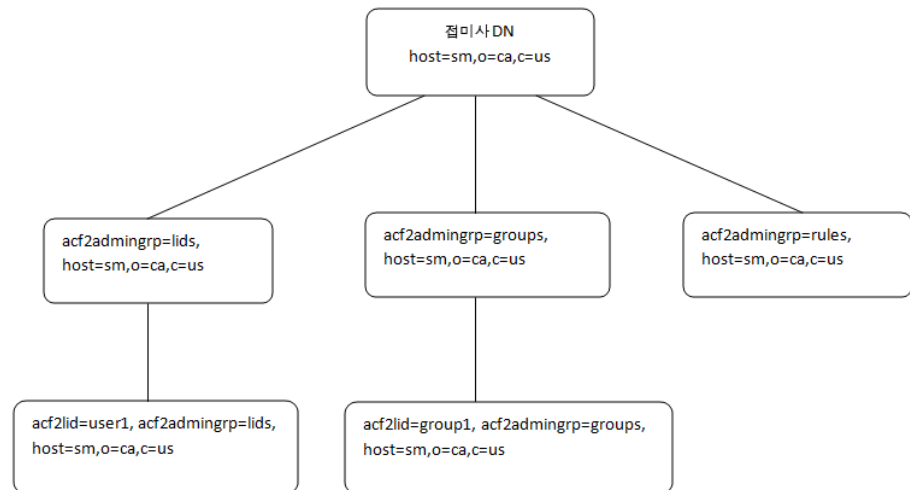
8. (선택 사항) "특성 매핑 목록" 영역에서 "만들기"를 클릭하여 사용자 특성 매핑을 구성합니다.
9. 제출을 클릭합니다.
사용자 디렉터리 연결이 생성됩니다.

CA LDAP Server r15 for z/OS(ACF2) 백엔드 보안 옵션

이 단원에서는 정책 서버에서 CA LDAP Server r15 for z/OS(ACF2)를 사용자 저장소로 구성하는 데 필요한 설정에 대해 설명합니다.

ACF2 개체 클래스 계층

다음 그림에서는 CA ACF2 DIT(디렉터리 정보 트리)에 있는 개체 클래스 항목의 계층을 보여 줍니다. 그림에는 각 개체 클래스에 대한 설명이 나와 있습니다.



host 개체 클래스

CA ACF2 데이터베이스의 개체 클래스 계층에 대한 액세스를 시작하는데 사용되는 개체 클래스입니다.

acf2admingrp 개체 클래스

개체 클래스 계층에서 호스트 아래에 분기를 생성하는 데 사용되는 개체 클래스입니다.

값:

- lids
- groups
- rules

acf2lid 개체 클래스

LID 레코드 필드(사용자 레코드)에 액세스하는 데 사용되는 개체 클래스입니다. acf2lid 는 추가, 수정 및 삭제가 가능한 유일한 개체 클래스입니다. 다른 모든 개체 클래스 개체는 읽기 전용입니다.

acf2lidgrp 개체 클래스

CA ACF2 에서 그룹을 에플레이트하는 데 사용되는 개체 클래스입니다.

acf2ruletype 개체 클래스

유사한 규칙 유형을 그룹화하는 데 사용되는 개체 클래스입니다. acf2ruletype 개체 클래스는 읽기 전용이며 수정, 추가 또는 삭제할 수 없습니다.

ACF2 에 대한 정책 서버 레지스트리 항목 구성

CA LDAP Server r15 for z/OS(ACF2)에는 다른 LDAP 서버와 구별되는 개체 클래스 집합이 있습니다. 정책 서버에서 CA LDAP Server 로의 사용자 디렉터리 연결을 구성하기 전에 LDAP 네임스페이스의 특정 정책 서버 레지스트리 항목에 ACF2 개체 클래스를 추가해야 합니다. 다음 정책 서버 레지스트리 항목의 기본값을 대체 값으로 바꿉니다.

registry_entry_home

다음 레지스트리 항목 위치를 지정합니다.

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Ds.

default_value

레지스트리 항목의 기본값을 지정합니다.

replacement_value

레지스트리 항목에 대해 ACF2 개체 클래스를 포함하는 새 값을 지정합니다.

- registry_entry_home\ClassFilters
class_filters_default_value:
organization,organizationalUnit,groupOfNames,groupOfUniqueNames,group
class_filters_replacement_value:
class_filters_default_value,*
- registry_entry_home\GroupClassFilters
group_class_filters_default_value:
groupOfNames,groupOfUniqueNames,group
group_class_filters_replacement_value:
group_class_filters_default_value,*
- registry_entry_home\PolicyClassFilters
policy_class_filters_default_value:
organizationalPerson,inetOrgPerson,organization,organizationalUnit,group
OfNames,groupOfUniqueNames,group
policy_class_filters_replacement_value:
policy_class_filters_default_value,*
- registry_entry_home\PolicyResolution
다음 ACF2 개체 클래스를 이 레지스트리 항목에 추가합니다.

ACF2 개체 클래스	레지스트리 키 종류	Data
acf2lid	REG_DWORD	0x00000001(1)
acf2admingrp	REG_DWORD	0x00000002(2)
eTACFLidName	REG_DWORD	0x00000001(1)

- registry_entry_home\Debug
UNIX 의 경우 다음 ACF2 개체 클래스를 이 레지스트리 항목에 추가합니다.

ACF2 개체 클래스	레지스트리 키 종류	Data
LDAPPingTimeout=	REG_DWORD	300;

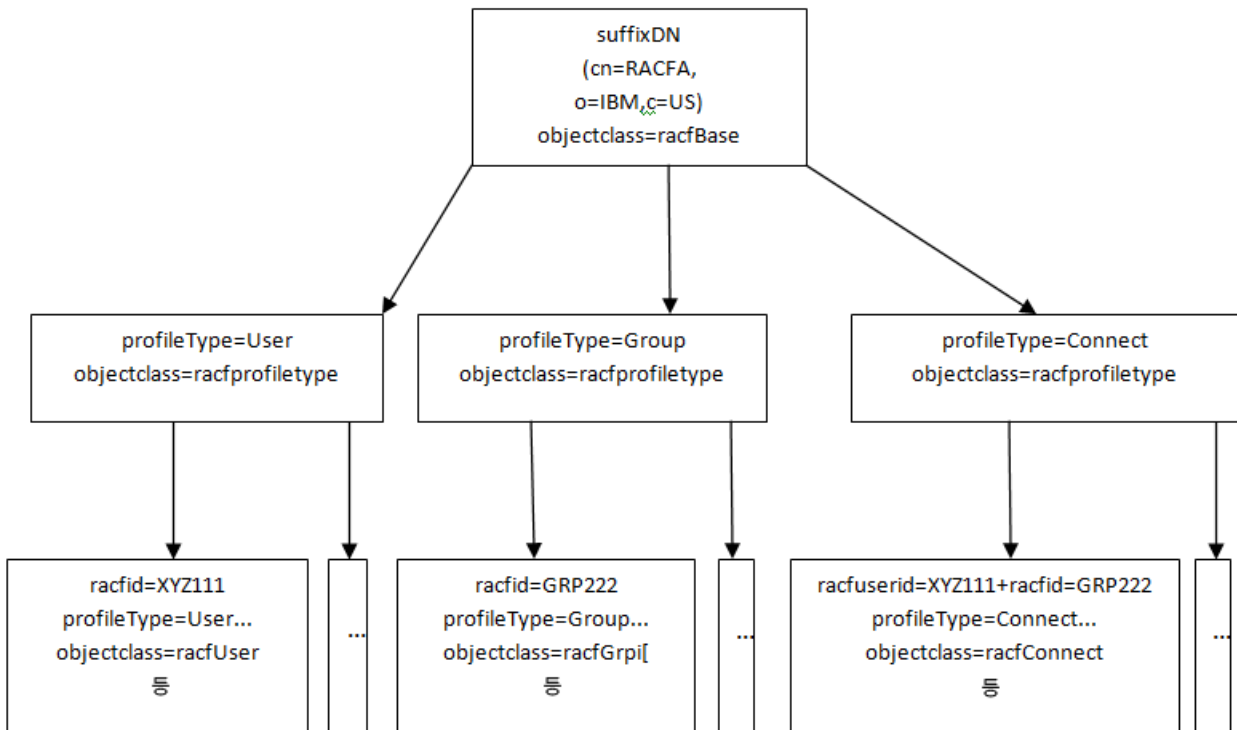
참고: CA LDAP Server r15 for z/OS(ACF2)의 응답 시간에 따라 이 레지스트리 키 값을 변경할 수 있습니다.

CA LDAP Server r15 for z/OS(RACF) 백엔드 보안 옵션

이 단원에서는 정책 서버에서 CA LDAP Server r15 for z/OS(RACF)를 사용자 저장소로 구성하는 데 필요한 설정에 대해 설명합니다.

RACF 네임스페이스 계층

다음 그림에서는 RACF DIT(디렉터리 정보 트리)에 있는 네임스페이스 항목의 계층을 보여 줍니다. 그림에는 각 네임스페이스에 대한 설명이 나와 있습니다. RACF 네임스페이스 계층은 ACF2 개체 클래스 계층과 비슷합니다.



ACF2 서버와 마찬가지로 계층에서 맨 위 4 개 항목은 서버에서 생성한 예약된 읽기 전용 항목입니다. 이러한 예약된 항목은 RACF 사용자, 그룹 및 연결을 계층적으로 나타내는 데 사용됩니다.

RACF 에 대한 정책 서버 레지스트리 항목 구성

CA LDAP Server r15 for z/OS(RACF)에는 다른 LDAP 서버와 구별되는 개체 클래스 집합이 있습니다. 정책 서버에서 CA LDAP Server 로의 사용자 디렉터리 연결을 구성하기 전에 LDAP 네임스페이스의 특정 정책 서버 레지스트리 항목에 RACF 개체 클래스를 추가해야 합니다. 다음 정책 서버 레지스트리 항목의 기본값을 대체 값으로 바꿉니다.

registry_entry_home

다음 레지스트리 항목 위치를 지정합니다.

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Ds.

default_value

레지스트리 항목의 기본값을 지정합니다.

replacement_value

레지스트리 항목에 대해 RACF 개체 클래스를 포함하는 새 값을 지정합니다.

■ registry_entry_home\ClassFilters

class_filters_default_value:

organization,organizationalUnit,groupOfNames,groupOfUniqueNames,group

class_filters_replacement_value:

class_filters_default_value,*

■ registry_entry_home\GroupClassFilters

group_class_filters_default_value:

groupOfNames,groupOfUniqueNames,group

group_class_filters_replacement_value:

group_class_filters_default_value,*

■ registry_entry_home\PolicyClassFilters

policy_class_filters_default_value:

organizationalPerson,inetOrgPerson,organization,organizationalUnit,groupOfNames,groupOfUniqueNames,group

policy_class_filters_replacement_value:

policy_class_filters_default_value,*

■ registry_entry_home\PolicyResolution

다음 RACF 개체 클래스를 이 레지스트리 항목에 추가합니다.

RACF 개체 클래스	레지스트리 키 종류	Data
eTRACUserid	REG_DWORD	0x00000001(1)
eTRACAdminGrp	REG_DWORD	0x00000002(2)

■ registry_entry_home\Debug

UNIX 의 경우 다음 RACF 개체 클래스를 이 레지스트리 항목에 추가합니다.

RACF 개체 클래스	레지스트리 키 종류	Data
LDAPPingTimeout=	REG_DWORD	300;

참고: CA LDAP Server r15 for z/OS(RACF)의 응답 시간에 따라 이 레지스트리 키 값을 변경할 수 있습니다.

정책 서버에서 CA LDAP Server for z/OS 로의 연결 구성

정책 서버에서 CA LDAP Server for z/OS(RACF) 또는 CA LDAP Server for z/OS(ACF2)로의 연결을 구성하려면 관리 UI 에서 기존 사용자 디렉터리 개체를 여십시오.

다음 단계를 수행하십시오.

1. "사용자 디렉터리" 대화 상자를 엽니다.
2. "디렉터리 설정"에서 네임스페이스로 "LDAP"을 선택합니다.
3. LDAP 디렉터리에 대한 연결 정보를 입력합니다.

참고: 이 LDAP Server 에는 장애 조치가 지원되지 않습니다.

4. "LDAP 검색" 섹션의 "최대 시간" 필드에서 300 초를 지정합니다.

참고: 정책 서버가 이 LDAP Server 에서 데이터를 가져오는 데는 많은 시간이 소요되므로 시간 만료 값을 높게 지정해야 합니다.

5. "자격 증명 및 연결"에서 정책 서버가 이 LDAP Server 에 연결할 때 사용할 관리자 자격 증명을 지정합니다.

중요! CA LDAP Server r15 for z/OS(RACF) 및 CA LDAP Server r15 for z/OS(ACF2)에서는 사용자 저장소에 대한 익명 바인딩이 허용되지 않으므로 관리자 자격 증명을 반드시 지정해야 합니다.

Oracle Directory Server Enterprise Edition 사용자 디렉터리 연결을 구성하는 방법

다음 프로세스에는 Oracle Directory Server Enterprise Edition 사용자 저장소 연결을 생성하는 단계가 나와 있습니다.

1. 사용자 저장소 시스템을 ping 합니다.
2. Oracle Directory Server Enterprise Edition 사용자 디렉터리 연결을 구성합니다.

사용자 저장소 시스템 ping

정책 서버와 사용자 디렉터리 또는 데이터베이스 사이에 네트워크 연결이 있는지 확인하기 위해 구성하기 전에 사용자 저장소 시스템을 ping 하십시오.

참고: 일부 사용자 저장소 시스템의 경우 정책 서버가 자격 증명을 제공해야 합니다.

Oracle Directory Server Enterprise Edition 사용자 디렉터리 연결 구성

정책 서버가 Oracle Directory 사용자 저장소와 통신할 수 있도록 연결을 구성합니다.

다음 단계를 수행하십시오.

1. "인프라", "디렉터리"를 차례로 클릭합니다.
2. "사용자 디렉터리"를 선택합니다.
3. "사용자 디렉터리 만들기"를 클릭합니다.
4. "일반" 및 디렉터리 설정 영역에서 필요한 연결 정보를 지정합니다.

5. "LDAP 설정" 영역에서 "LDAP 검색" 및 "LDAP 사용자 DN 조회" 설정을 구성합니다.
6. (선택 사항) "관리자 자격 증명" 영역에서 다음 작업을 수행하십시오.
 - a. "자격 증명 필요"를 선택합니다.
 - b. 관리자 계정의 자격 증명을 입력합니다.

참고: Oracle에서는 cn=Directory Manager 이외의 관리자 계정을 사용할 것을 권장합니다. cn=Directory Manager를 사용하면 이 계정에 적용된 보안 정책 때문에 성능 문제가 발생할 수 있습니다. 디렉터리를 관리할 수 있는 권한이 있는 사용자를 생성하고 이 사용자를 "사용자 이름"에 지정합니다.

7. (선택 사항) "사용자 특성" 영역에서 SiteMinder 용으로 예약된 사용자 디렉터리 프로필 특성을 지정합니다.
 8. (선택 사항) "특성 매핑 목록" 영역에서 "만들기"를 클릭하여 사용자 특성 매핑을 구성합니다.
 9. 제출을 클릭합니다.
- 사용자 디렉터리 연결이 생성됩니다.

IBM Directory Server 사용자 디렉터리 연결을 구성하는 방법

다음 프로세스에는 정책 서버에 대한 IBM Directory Server 사용자 저장소 연결을 생성하는 단계가 나와 있습니다.

1. 사용자 저장소 시스템 ping
2. IBM Directory Serve 사용자 디렉터리 연결 구성

사용자 저장소 시스템 ping

정책 서버와 사용자 디렉터리 또는 데이터베이스 사이에 네트워크 연결이 있는지 확인하기 위해 구성하기 전에 사용자 저장소 시스템을 ping 하십시오.

참고: 일부 사용자 저장소 시스템의 경우 정책 서버가 자격 증명을 제공해야 합니다.

IBM Directory Server 사용자 디렉터리 연결 구성

정책 서버가 IBM Directory Server 사용자 저장소와 통신할 수 있도록 연결을 구성합니다.

다음 단계를 수행하십시오.

1. "인프라", "디렉터리"를 차례로 클릭합니다.
2. "사용자 디렉터리"를 선택합니다.
3. "사용자 디렉터리 만들기"를 클릭합니다.
4. "일반" 및 디렉터리 설정 영역에서 필요한 연결 정보를 지정합니다.
5. "LDAP 설정" 영역에서 "LDAP 검색" 및 "LDAP 사용자 DN 조회" 설정을 구성합니다.
6. (선택 사항) "관리자 자격 증명" 영역에서 다음 작업을 수행하십시오.
 - a. "자격 증명 필요" 옵션을 선택합니다.
 - b. 관리자 계정의 자격 증명을 입력합니다.
7. (선택 사항) "사용자 특성" 영역에서 SiteMinder 용으로 예약된 사용자 디렉터리 프로필 특성을 지정합니다.
8. (선택 사항) "특성 매핑 목록" 영역에서 "만들기"를 클릭하여 사용자 특성 매핑을 구성합니다.
9. 제출을 클릭합니다.

사용자 디렉터리 연결이 생성됩니다.

참고: IBM Directory Server 조회는 SiteMinder 와 호환되지 않습니다.

Domino 사용자 디렉터리를 사용자 저장소로 구성하는 방법

Domino 사용자 디렉터리를 사용자 저장소로 구성하는 과정은 다음 두 단계로 이루어집니다.

1. Domino 사용자 디렉터리가 정책 서버 요구 사항을 충족하는지 확인
2. 정책 서버에서 Domino 사용자 저장소로의 연결 구성

Domino 사용자 디렉터리가 정책 서버 요구 사항을 충족하는지 확인

Domino 사용자 디렉터리는 LDAP 디렉터리입니다. Domino 사용자 디렉터리를 사용자 저장소로 구성하기 전에 다음 사전 요구 사항을 충족하는지 확인하십시오.

- Domino 사용자 그룹은 정책 서버에서 Domino 사용자 저장소로의 연결을 구성할 때 지정한 루트 DN 을 공유합니다.

예: Lotus Notes 의 주소록(names.nsf)에 *marketing/myorg.org* 그룹을 추가할 때 "사용자 디렉터리" 화면의 "루트" 필드에 *o=myorg.org* 를 입력합니다.

- Domino 사용자 디렉터리에 새로 추가하는 각 사용자마다 사용자 이름 항목과 인터넷 암호 항목이 있습니다.

참고: Domino 사용자 디렉터리에 사용자를 추가할 때 등록도 함께 하는 것이 좋습니다. 이 추가 단계를 수행하면 Domino 사용자 디렉터리에 사용자 이름 항목이 여러 개 추가되는 것을 방지할 수 있습니다. 디렉터리에 항목이 여러 개 있는 경우 정책 서버는 첫 번째 이름을 사용합니다. 다른 사용자 이름으로 로그인하려고 하면 실패합니다.

사용자 저장소 시스템 ping

정책 서버와 사용자 디렉터리 또는 데이터베이스 사이에 네트워크 연결이 있는지 확인하기 위해 구성하기 전에 사용자 저장소 시스템을 ping 하십시오.

참고: 일부 사용자 저장소 시스템의 경우 정책 서버가 자격 증명을 제공해야 합니다.

Domino Directory 연결 구성

정책 서버가 Domino 사용자 저장소와 통신할 수 있도록 연결을 구성합니다.

다음 단계를 수행하십시오.

1. "인프라", "디렉터리"를 차례로 클릭합니다.
2. "사용자 디렉터리"를 선택합니다.
3. "사용자 디렉터리 만들기"를 클릭합니다.
4. "일반" 및 디렉터리 설정 영역에서 필요한 연결 정보를 지정합니다.

5. "LDAP 설정" 영역에서 "LDAP 검색" 및 "LDAP 사용자 DN 조회" 설정을 구성합니다.

참고: "루트"에 지정하는 값은 Lotus Notes 에서 할당한 조직 이름과 일치합니다.

예: 미국에 위치한 "myorg"라는 조직이 있는 경우 검색 루트는 o=myorg,c=us 로 지정됩니다.

참고: "사용자 DN 조회 시작" 및 "사용자 DN 조회 끝" 필드에 지정하는 검색 문자열은 Lotus Notes 단축 표기법이 아니라 적절한 LDAP 표기법을 따릅니다.

6. (선택 사항) "구성"을 클릭하여 부하 분산 및 장애 조치를 구성합니다.
7. (선택 사항) "관리자 자격 증명" 영역에서 다음 작업을 수행하십시오.
 - a. "자격 증명 필요" 옵션을 선택합니다.
 - b. 관리자 계정의 자격 증명을 입력합니다.
8. (선택 사항) "사용자 특성" 영역에서 SiteMinder 용으로 예약된 사용자 디렉터리 프로필 특성을 지정합니다.
9. (선택 사항) "특성 매핑 목록" 영역에서 "만들기"를 클릭하여 사용자 특성 매핑을 구성합니다.
10. 제출을 클릭합니다.

사용자 디렉터리 연결이 생성됩니다.

Novell eDirectory LDAP 디렉터리 연결을 구성하는 방법

Novell eDirectory LDAP 사용자 디렉터를 사용자 저장소로 사용할 수 있습니다. 다음 프로세스에는 정책 서버에 대한 사용자 저장소 연결을 생성하는 단계가 나와 있습니다.

1. NetWare 구성
2. Novell eDirectory 에 익명 LDAP 액세스 구성

또는

특정 SiteMinder 관리자를 위한 액세스 권한 만들기:

- SiteMinder 관리자를 위한 특수 액세스 권한
- SiteMinder 관리에 사용할 Novell eDirectory 사용자 계정 만들기

3. Novell eDirectory LDAP 디렉터리 연결 구성

NetWare 구성

이 구성은 정책 서버가 Novell eDirectory 에 로그인하고, 디렉터리의 내용을 보고, 디렉터리 특성을 가져오도록 해 줍니다. 일부 고급 기능을 사용하려면 정책 서버 쓰기 액세스를 허용하도록 Novell eDirectory 를 구성해야 할 수도 있습니다.

LDAP 가 Novell eDirectory 설치의 일부인 경우, Novell eDirectory 에서 서버의 이름을 "LDAP Server"로 지정하고 LDAP 그룹을 "LDAP Group"으로 지정하십시오. LDAP 서버는 LDAP 그룹의 구성원입니다.

다음 단계를 수행하십시오.

1. Novell eDirectory 에 LDAP 서버를 생성합니다. 이 예에서는 이 LDAP 서버를 LDAP Server 라고 합니다.
2. Novell eDirectory 에 LDAP 그룹을 생성합니다. 이 예에서는 이 LDAP 그룹을 LDAP Group 이라고 합니다.
3. LDAP Server 에 LDAP Group 을 할당합니다.

- a. NW Admin 도구에서 "LDAP Server"(LDAP 서버)를 마우스 오른쪽 단추로 클릭합니다.

참고: NW Admin 도구 대신 Netware ConsoleOne 도구를 사용하여 Novell eDirectory 를 수정할 경우 ConsoleOne 에서 제공하는 도구를 사용하여 동일한 태스크를 완료해야 합니다. 두 도구의 인터페이스는 유사합니다. 자세한 내용은 Novell 설명서를 참조하십시오.

- b. 팝업 메뉴에서 "Details"(상세 정보)를 선택합니다.
- c. "LDAP Group"(LDAP 그룹) 필드에 LDAP Group 을 입력합니다.
- d. "OK"(확인)를 클릭합니다.

추가 정보:

[디렉터리 특성 개요](#) (페이지 150)

Novell eDirectory 에 익명 LDAP 액세스 구성

정책 서버가 Novell eDirectory 와 상호 작용하려면 디렉터리에 대한 액세스를 허용할 수 있는 관리 권한이 있는 계정을 생성하십시오. 가장 간편한 구성은 LDAP 서버에 익명 사용자를 생성하고 이 사용자를 프록시로 설정하는 것입니다. 사용자는 모든 기능을 수행하는 데 충분한 권한이 할당됩니다.

아래 절차에서는 익명 사용자에게 관리자 권한을 할당하지만, 이보다 제한된 권한으로 사용자를 구성할 수도 있습니다. LDAP 디렉터리에 대한 모든 익명 액세스는 SiteMinder 에 제공하는 것과 동일한 권한을 얻습니다.

<fsp>

1. 사용자 namedLDAP_Anonymous 를 만듭니다.

다음 절차는 예제입니다.

- a. NW Admin 도구의 메뉴 표시줄에서 "Object"(개체), "Create"(만들기), "User"(사용자)를 차례로 선택합니다.
- b. LDAP_Anonymous 라는 이름을 추가합니다.
- c. 암호는 할당하지 마십시오.
- d. 오른쪽 프레임에서 "Security Equal To"(보안 수준이 다음과 같음)를 선택하고 관리 사용자(예: Admin.transpolar)를 추가합니다.
- e. "확인"을 클릭합니다.

2. 프록시 계정을 설정합니다.

다음 절차는 예제입니다.

- a. NW Admin 도구에서 "LDAP Group"(LDAP 그룹)을 선택합니다.
- b. 팝업 메뉴에서 "Details"(상세 정보)를 선택합니다.
- c. 계속을 클릭합니다.
- d. "Proxy Username"(프록시 사용자 이름) 필드에 LDAP_Anonymous 를 입력합니다.
- e. 오른쪽 프레임에서 "Access Control"(액세스 제어)을 선택하고 "Add"(추가)를 클릭합니다.
- f. "LDAP ACL Name"(LDAP ACL 이름) 필드에 LDAP_Anonymous 를 입력합니다.

- g. "LDAP Distinguished Name"(LDAP 고유 이름) 확인란을 선택하고 cn=LDAP_Anonymous 를 입력합니다.
- h. "All Attributes and Object Rights"(모든 특성 및 개체 권한) 확인란을 선택합니다.
- i. "확인"을 클릭합니다.
- j. 오른쪽 프레임에서 "Access Control"(액세스 제어)을 선택하고 "Add"(추가)를 클릭합니다.
- k. "LDAP ACL Name"(LDAP ACL 이름) 상자에 Everyone 을 입력합니다.
- l. "Everything"(모두) 확인란을 선택합니다.
- m. "All Attributes and Object Rights"(모든 특성 및 개체 권한) 확인란을 선택합니다.
- n. "확인"을 클릭합니다.
- o. "확인"을 클릭합니다.

Novell eDirectory 를 정책 서버에서 사용할 수 있도록 구성하는 작업을 계속하려면 관리 UI 에서 [Novell eDirectory LDAP 연결 구성](#) (페이지 176)을 참조하십시오.

SiteMinder 관리자를 위한 특수 액세스 권한

아래 대체 지침은 오직 정책 서버에 대한 특수 액세스만 허용합니다. 이 지침은 일부 환경에서 보다 적절할 수 있습니다.

1. SiteMinder 관리자를 나타내는 Novell eDirectory 사용자를 만듭니다. 예: siteminder_admin.
2. SiteMinder 관리자가 생성한 암호를 이 사용자에게 제공합니다. 이 암호는 관리 UI 에서 입력합니다.

SiteMinder 관리에 사용할 Novell eDirectory 사용자 계정 만들기

NW Admin 도구를 사용하여 정책 관리자에 대한 사용자 계정을 만들 수 있습니다.

다음 단계를 수행하십시오.

1. NW Admin 도구에서 "LDAP Group"(LDAP 그룹)을 마우스 오른쪽 단추로 클릭합니다.
2. 팝업 메뉴에서 "Details"(상세 정보)를 선택합니다.
3. 오른쪽 패널에서 "Access Control"(액세스 제어)을 클릭합니다.
4. ACL 을 추가합니다.
5. ACL 의 이름을 입력합니다.
6. "Access By List"(액세스 가능 사용자 목록) 화면에서 "Add"(추가)를 클릭합니다.
7. "Access By List"(액세스 가능 사용자 목록) 패널에서 "LDAP Distinguished Name"(LDAP 고유 이름)을 클릭합니다.
8. 다음을 입력합니다: cn=siteminder_admin

기본적으로 액세스 수준은 "Read"(읽기)로 설정하십시오. 이 수준이면 기본 기능에 액세스하는 데 충분합니다. 활성 API 나 고급 기능(예: 암호 서비스, 사용자 비활성화, 등록 서비스)을 사용하는 고객의 경우 쓰기 권한이 필요할 수도 있습니다.

사용자 저장소 시스템 ping

정책 서버와 사용자 디렉터리 또는 데이터베이스 사이에 네트워크 연결이 있는지 확인하기 위해 구성하기 전에 사용자 저장소 시스템을 ping 하십시오.

참고: 일부 사용자 저장소 시스템의 경우 정책 서버가 자격 증명을 제공해야 합니다.

Novell eDirectory LDAP 디렉터리 연결 구성

정책 서버가 Novell eDirectory 사용자 저장소와 통신할 수 있도록 사용자 디렉터리 연결을 구성할 수 있습니다.

다음 단계를 수행하십시오.

1. "인프라", "디렉터리"를 차례로 클릭합니다.
2. "사용자 디렉터리"를 선택합니다.
3. "사용자 디렉터리 만들기"를 클릭합니다.
4. "일반" 및 디렉터리 설정 영역에서 필요한 연결 정보를 지정합니다.
5. "LDAP 설정" 영역에서 "LDAP 검색" 및 "LDAP 사용자 DN 조회" 설정을 구성합니다.

참고: 사용자 디렉터리에 여러 조직이 포함된 경우 "루트" 필드를 비워둘 수 있습니다. 이렇게 하면 정책 서버가 여러 조직에서 사용자를 검색할 수 있습니다.

6. (선택 사항) "관리자 자격 증명" 영역에서 다음 작업을 수행하십시오.
 - a. "자격 증명 필요" 옵션을 선택합니다.
 - b. 관리자 계정의 자격 증명을 입력합니다.
7. (선택 사항) "사용자 특성" 영역에서 SiteMinder 용으로 예약된 사용자 디렉터리 프로필 특성을 지정합니다.
8. (선택 사항) "특성 매핑 목록" 영역에서 "만들기"를 클릭하여 사용자 특성 매핑을 구성합니다.
9. 제출을 클릭합니다.

사용자 디렉터리 연결이 생성됩니다.

Active Directory LDS 사용자 디렉터리 연결 구성 방법

Active Directory LDS 를 사용자 저장소로 사용할 수 있습니다. 다음 절차를 완료하십시오.

1. 사용자 저장소 시스템을 ping 합니다.
2. 사용자 디렉터리 연결을 구성합니다.

사용자 저장소 시스템 ping

정책 서버와 사용자 디렉터리 또는 데이터베이스 사이에 네트워크 연결이 있는지 확인하기 위해 구성하기 전에 사용자 저장소 시스템을 ping 하십시오.

참고: 일부 사용자 저장소 시스템의 경우 정책 서버가 자격 증명을 제공해야 합니다.

Active Directory LDS 사용자 저장소 디렉터리 연결 구성

정책 서버가 Active Directory LDS 사용자 저장소와 통신할 수 있도록 사용자 디렉터리 연결을 구성할 수 있습니다.

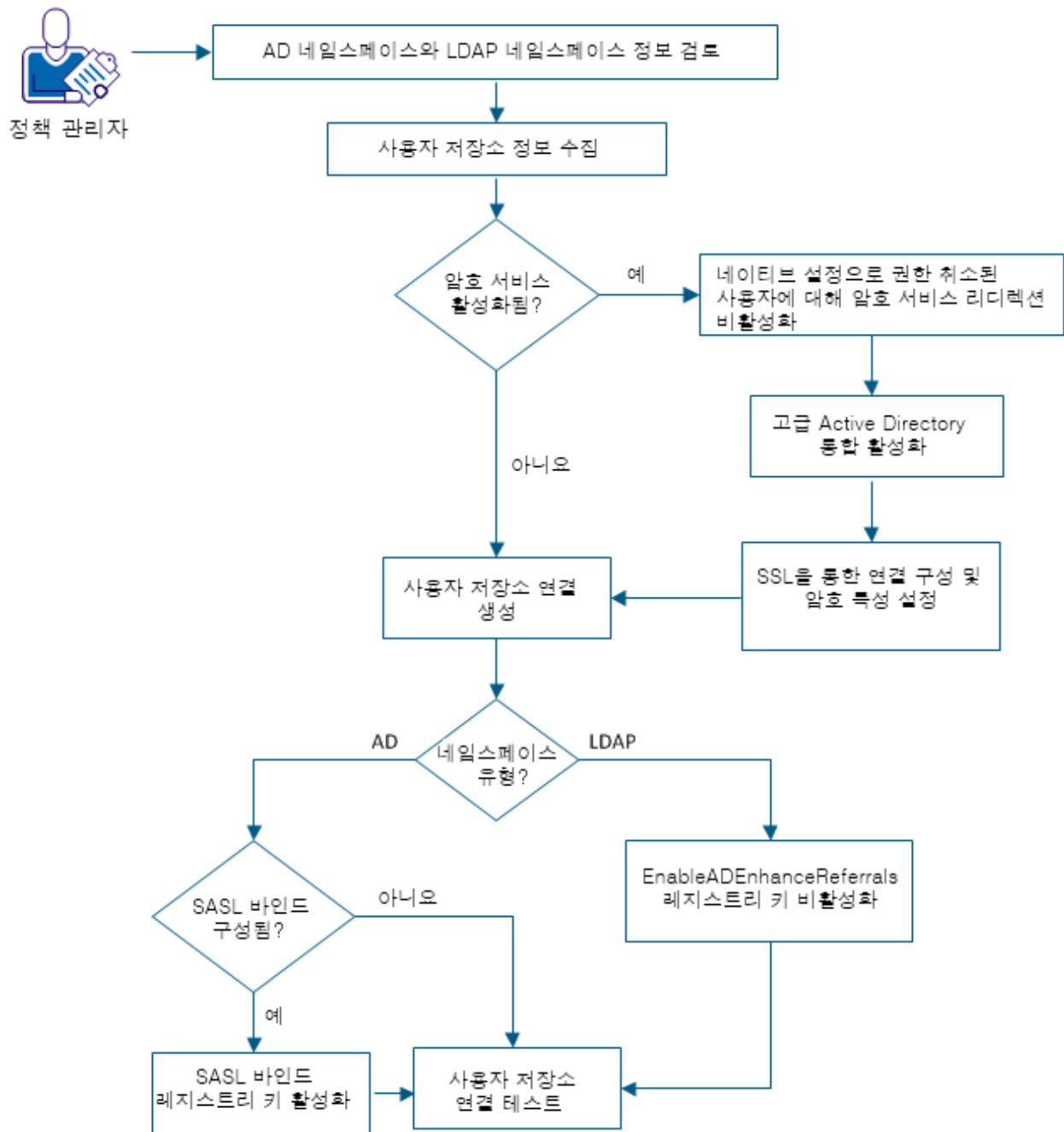
다음 단계를 수행하십시오.

1. "인프라", "디렉터리"를 차례로 클릭합니다.
 2. "사용자 디렉터리"를 선택합니다.
 3. "사용자 디렉터리 만들기"를 클릭합니다.
 4. "일반" 및 디렉터리 설정 영역에서 필요한 연결 정보를 지정합니다.
 5. "LDAP 설정" 영역에서 "LDAP 검색" 및 "LDAP 사용자 DN 조회" 설정을 구성합니다.
 6. (선택 사항) "관리자 자격 증명" 영역에서 다음 작업을 수행하십시오.
 - a. "자격 증명 필요" 옵션을 선택합니다.
 - b. 관리자 계정의 자격 증명을 입력합니다.
 7. (선택 사항) "사용자 특성" 영역에서 SiteMinder 용으로 예약된 사용자 디렉터리 프로필 특성을 지정합니다.
 8. (선택 사항) "특성 매핑 목록" 영역에서 "만들기"를 클릭하여 사용자 특성 매핑을 구성합니다.
 9. 제출을 클릭합니다.
- 사용자 디렉터리 연결이 생성됩니다.

Active Directory 사용자 저장소 연결을 구성하는 방법

다음 그림은 Active Directory 사용자 저장소 연결을 구성하기 위해 필요한 단계를 표시합니다.

Active Directory 사용자 저장소 연결을 구성하는 방법



AD 사용자 저장소 연결을 구성하려면 다음 절차를 완료하십시오.

1. AD 네임스페이스와 LDAP 네임스페이스 정보를 검토합니다.
2. [사용자 저장소 정보를 수집합니다](#) (페이지 182).
3. [네이티브 설정으로 비활성화된 권한 없는 사용자에게 대해 암호 서비스 리디렉션을 비활성화합니다](#) (페이지 183).
4. [개선된 Active Directory 통합 기능을 활성화합니다](#) (페이지 184).
5. [사용자 저장소 연결을 만듭니다](#) (페이지 184).
6. [EnableADEnhancedReferrals 레지스트리 키를 비활성화합니다](#) (페이지 186).
7. [SASL 바인드 레지스트리 키를 활성화합니다](#) (페이지 187).
8. [사용자 저장소 연결을 테스트합니다](#) (페이지 188).

사전 요구 사항

AD 사용자 저장소 연결을 구성하기 전에 다음 사항을 확인하십시오.

- 관리 UI가 설치되었고 정책 서버에 등록되었습니다.
- 사용자 저장소 연결을 만들기 위해 필요한 권한이 있는 관리자 계정이 있습니다.

AD 네임스페이스 및 LDAP 네임스페이스 정보 검토

AD 또는 LDAP 네임스페이스로서 사용자 저장소 연결을 구성할 수 있습니다. 선택하는 네임스페이스의 유형은 지원되는 기능 및 SiteMinder 기능의 다른 영역에 영향을 줍니다.

다음 표는 AD 및 LDAP 네임스페이스의 장점 및 단점을 설명합니다.

네임스페이스 유형	장점	단점
AD	■ 네이티브 Windows 인증서 데이터베이스를 사용하는 SSL 연결이 사용됩니다. 참고: 정책 서버와 Active Directory 사용자 저장소를 호스트하는 시스템 모두에 트러스트가 설정되어 있어야 합니다. ■ 보안 LDAP 바인딩 작업을 허용하는 네이티브 Windows SASL 이 지원됩니다.	■ 향상된 LDAP 조회가 지원되지 않습니다. ■ LDAP 페이징 및 정렬 작업이 지원되지 않습니다. 참고: 사용 중인 코드 페이지에 관계없이 SiteMinder 는 문자를 유니코드 정의에 따라 처리합니다. 특수 문자가 사용 중인 코드 페이지에 싱글바이트로 나오더라도 유니코드에 멀티바이트 문자로 정의되어 있으면 SiteMinder 는 이를 멀티바이트 문자로 처리합니다.

네임스페이스 유형	단점
LDAP ■ 향상된 LDAP 조회가 지원됩니다. ■ LDAP 페이징 및 정렬이 지원됩니다.	■ 네이티브 Windows SASL 이 지원되지 않습니다. ■ 개체 클래스 특성이 인덱싱되지 않습니다. SiteMinder 를 Active Directory 사용자 디렉터리와 함께 효율적으로 실행하려면 Active Directory 에서 개체 클래스 특성을 인덱싱하십시오. 참고: 자세한 내용은 공급업체별 설명서를 참조하십시오. ■ Windows 사용자 보안 컨텍스트를 사용합니다. 에이전트는 IIS 웹 서버의 웹 리소스를 액세스하기 위해 Windows 사용자 보안 컨텍스트에서 실행될 수 있습니다. SiteMinder 가 Windows 사용자 보안 컨텍스트를 제공하려면 먼저 영역별로 세션 저장소를 구성하고 영구 세션을 활성화하십시오. 이 기능을 활성화하려면 관리 UI 를 사용하여 사용자 디렉터리를 만들 때 "디렉터리 설정" 아래에서 다음 옵션을 선택하십시오. 인증된 사용자의 보안 컨텍스트 사용

사용자 저장소 정보 수집

사용자 저장소 연결을 만들기 전에 **LDAP** 설정 및 사용자 특성에 대해 필요한 정보를 수집하십시오.

이 정보를 수집하려면 디렉터리 서버 관리자에게 문의하십시오.

서버

Active Directory 호스트 시스템의 IP 주소와 포트를 지정합니다.

LDAP 검색 루트

정책 서버가 디렉터리 연결의 시작점으로 사용하는 LDAP 트리 위치를 지정합니다. 정책 서버는 사용자를 찾을 때 루트에서 검색을 시작합니다.

예: dc=domainname,dc=com

사용자 DN 조회

LDAP 사용자 저장소에서 사용자를 찾기 위해 LDAP 검색 식의 텍스트 문자열 또는 사용자 DN 을 지정합니다. 완전한 조회를 위해서는 "시작" 및 "끝" 문자열이 필요합니다. "시작" 문자열, 사용자 이름 및 "끝" 문자열의 조합을 사용하여 LDAP 사용자 저장소를 검색합니다.

예 (시작): (sAMAccountName=

예 (End):)

유니버설 ID

SiteMinder 가 유니버설 ID 로 사용하는 특성의 이름을 지정합니다.

예: sAMAccountName

비활성화된 플래그

사용자의 비활성화된 상태를 유지하는 사용자 디렉터리 특성의 이름을 지정합니다.

예: carLicense(또는 임의의 정수 특성)

암호

SiteMinder 가 사용자의 암호를 인증하기 위해 사용하는 사용자 디렉터리 특성의 이름을 지정합니다.

예: unicodePwd

암호 데이터

SiteMinder 가 암호 서비스 데이터에 사용할 수 있는 사용자 디렉터리 특성의 이름을 지정합니다.

예: audio

"암호 데이터"의 값은 큰 바이너리 특성일 수 있습니다. 이 값은 기본 암호 서비스를 사용하는 경우에만 필요합니다.

네이티브 설정으로 비활성화된 권한 없는 사용자에 대해 암호 서비스 리디렉션이 사용되지 않도록 설정

기본적으로, SiteMinder 는 사용자가 디렉터리 서버에서 네이티브 설정으로 비활성화된 경우 사용자에게 자격 증명을 다시 요구합니다. SiteMinder 는 이러한 사용자를 암호 서비스로 리디렉션하며, 이는 리소스를 보호하는 인증 체계에 암호 서비스가 사용되지 않는 경우에도 해당됩니다.

이러한 동작이 수행되지 않도록 하려면 다음 레지스트리 키가 필요합니다.

`IgnoreDefaultRedirectOnADnativeDisabled`

정책 서버 관리자에게 문의하여 해당 키를 생성하고 활성화하도록 요청하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 레지스트리 편집기를 열고 다음 위치로 이동합니다.

`HKEY_LOCAL_MACHINE\Software\Netegrity\SiteMinder\CurrentVersion\Ds\LDAPProvider`

3. 레지스트리 유형이 REG_DWORD 인 `IgnoreDefaultRedirectOnADnativeDisabled` 레지스트리 키를 만듭니다.

값: 0(사용 안 함) 또는 1(사용)

기본값: 0

4. 값을 1로 설정합니다.
5. 레지스트리 편집기를 종료합니다.
6. 정책 서버를 다시 시작합니다.

중요! 암호 서비스로 리디렉션하도록 지정된 암호 정책이 적용될 경우 이 레지스트리 키의 설정에 관계없이 SiteMinder 는 네이티브 설정으로 비활성화된 사용자를 암호 서비스로 리디렉션합니다.

개선된 Active Directory 통합 기능이 사용되도록 설정

Active Directory 2008에는 Windows NOS(네트워크 운영 체제)에 사용되는 여러 사용자 및 도메인 특성이 있습니다. LDAP 표준에는 이러한 사용자 및 도메인 특성이 필요 없습니다. "암호 서비스"가 활성화된 경우 관리 UI를 사용하여 "개선된 Active Directory 통합 기능"을 활성화하십시오. 이 옵션을 사용하면 AD 사용자 특성을 SiteMinder의 매핑된 사용자 특성과 동기화하여 정책 서버의 사용자 관리 기능 및 암호 서비스와 AD 간의 통합이 개선됩니다.

다음 단계를 수행하십시오.

1. 관리 UI에 로그인합니다.
2. "관리", "정책 서버", "전역 도구"를 차례로 클릭합니다.
3. "개선된 Active Directory 통합 기능"을 선택합니다.
4. 제출을 클릭합니다.

개선된 Active Directory 통합 기능이 활성화됩니다.

사용자 저장소 연결 만들기

사용자 저장소 연결을 구성하면 정책 서버가 Active Directory와 통신할 수 있습니다. 환경에서 암호 서비스를 사용하는 경우 SSL 연결과 암호 특성(예: unicodePWD)이 필요합니다.

참고: SSL을 통해 통신하도록 Active Directory를 구성하는 방법에 대한 자세한 내용은 사용하는 제품 설명서를 참조하십시오.

다음 단계를 수행하십시오.

1. 관리 UI에 로그인합니다.
2. "인프라", "디렉터리", "사용자 디렉터리"를 차례로 클릭합니다.
3. "사용자 디렉터리 만들기"를 클릭합니다.
4. Microsoft Active Directory는 LDAP 호환 사용자 디렉터리입니다. AD 네임스페이스 또는 LDAP 네임스페이스를 사용하여 연결을 구성할 수 있습니다. 다음 작업 중 하나를 수행하십시오.
 - 기본 LDAP 설정을 그대로 둡니다.
 - "네임스페이스" 목록에서 AD를 선택합니다.

5. "일반" 및 디렉터리 설정 영역에서 나머지 필요한 연결 정보를 지정합니다.

참고: 정책 서버 및 Active Directory 네임스페이스가 SSL 을 통해 통신하는 경우 "디렉터리 설정" 아래의 "서버"에 IP 주소와 포트를 지정하십시오. IP 주소를 지정하지 않으면 사용자 디렉터리에 연결할 수 없다는 오류가 로깅됩니다. 인증서가 서버 이름과 일치하지 않는다는 Windows 이벤트도 로깅됩니다.

참고: 다음과 같은 조건인 경우 정책 서버와 디렉터리 저장소가 사용하는 인증서는 FIPS 호환 인증서여야 합니다.

- 정책 서버가 FIPS 모드에서 작동하고 있는 경우
- 정책 서버와 통신할 때 디렉터리 연결이 보안 SSL 연결을 사용하는 경우

6. (선택 사항) "디렉터리 설정"에서 "구성"을 클릭하여 부하 분산 및 장애 조치를 구성합니다.

7. "관리자 자격 증명"에서 다음을 수행합니다.

- a. "자격 증명 필요"를 선택합니다.
- b. 관리자 계정의 자격 증명을 입력합니다.

참고: Active Directory(AD) 네임스페이스의 사용자 디렉터리를 구성하는 경우 "사용자 이름" 필드에 관리자의 FQDN(정규화된 도메인 이름)을 지정합니다. 그렇지 않으면 사용자 인증이 실패할 수 있습니다.

8. "LDAP 설정" 영역에서 "LDAP 검색" 및 "LDAP 사용자 DN 조회" 설정을 구성합니다.

9. "사용자 특성" 영역에서 SiteMinder 용으로 예약된 사용자 디렉터리 프로필 특성을 지정합니다.

10. (선택 사항) "특성 매핑 목록" 영역에서 "만들기"를 클릭하여 사용자 특성 매핑을 구성합니다.

11. 제출을 클릭합니다.

사용자 디렉터리 연결이 생성됩니다.

EnableADEnhancedReferrals 레지스트리 키 비활성화

사용자 저장소 연결이 LDAP 네임스페이스를 사용하여 구성된 경우 EnableADEnhancedReferrals 레지스트리 키를 비활성화하십시오. 이 레지스트리 키를 비활성화하면 LDAP 연결 오류가 발생하지 않습니다.

정책 서버 관리자에게 문의하여 해당 키를 비활성화하도록 요청하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 레지스트리 편집기를 열고 다음 위치로 이동합니다.

```
HKEY_LOCAL_MACHINE\Software\Netegrity\SiteMinder\CurrentVersion\Ds\LDAPProvider
```

3. EnableADEnhancedReferrals 키에 대해 이 값을 0 으로 설정합니다.

값: 0(사용 안 함) 또는 1(사용)

기본값: 1

4. 레지스트리 편집기를 종료합니다.

SASL 바인드 레지스트리 키 활성화

Windows 기반 정책 서버는 SASL 을 사용하여 Active Directory 의 사용자를 인증할 수 있습니다. SASL 바인드를 사용하도록 활성화하려면 EnableSASLBind 레지스트리 키를 만들어 활성화하십시오.

참고: 이 설정을 사용할 경우 사용자 디렉터리 구성의 관리자 이름을 정규화된 고유 이름 대신 AD 로그인 이름으로 설정하십시오.

중요! 정책 서버와 사용자 저장소 사이에서 SSL 연결을 구성하는 경우 이 레지스트리 키를 활성화하지 마십시오.

정책 서버 관리자에게 문의하여 해당 키를 생성하고 활성화하도록 요청하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 레지스트리 편집기를 열고 다음 위치로 이동합니다.

HKEY_LOCAL_MACHINE\Software\Netegrity\SiteMinder\CurrentVersion\Ds\LDAPProvider

3. 레지스트리 유형이 REG_DWORD 인 EnableSASLBind 레지스트리 키를 만듭니다.
4. 값을 1 로 설정합니다.
5. 레지스트리 편집기를 종료합니다.
6. 정책 서버를 다시 시작합니다.

사용자 저장소 연결 테스트

사용자를 쿼리하여 연결을 테스트하십시오.

다음 단계를 수행하십시오.

1. 관리 UI에 로그인합니다.
2. "인프라", "디렉터리", "사용자 디렉터리"를 차례로 클릭합니다.
3. 만든 사용자 저장소의 이름을 클릭합니다.
4. "디렉터리 설정" 아래에서 "콘텐츠 보기"를 클릭합니다.
5. 검색 유형이 "특성-값"으로 선택되어 있는지 확인합니다.
6. "특성"에 "유니버설 ID"를 입력합니다.

예: sAMAccountName

7. "값"에 *를 입력합니다.
8. "실행"을 클릭합니다.

계정 상세 정보가 나타납니다. 사용자 저장소에 성공적으로 연결되었습니다.

Active Directory 글로벌 카탈로그 사용자 디렉터리 연결을 구성하는 방법

Active Directory 글로벌 카탈로그를 사용자 저장소로 사용할 수 있습니다. 다음 프로세스에는 정책 서버에 대한 사용자 저장소 연결을 생성하는 단계가 나와 있습니다.

1. 사용자 저장소 시스템 ping
2. Active Directory 글로벌 카탈로그 연결 구성

사용자 저장소 시스템 ping

정책 서버와 사용자 디렉터리 또는 데이터베이스 사이에 네트워크 연결이 있는지 확인하기 위해 구성하기 전에 사용자 저장소 시스템을 ping 하십시오.

참고: 일부 사용자 저장소 시스템의 경우 정책 서버가 자격 증명을 제공해야 합니다.

Active Directory 글로벌 카탈로그 디렉터리 연결 구성

정책 서버가 Active Directory 글로벌 카탈로그 사용자 저장소와 통신할 수 있도록 사용자 디렉터리 연결을 구성할 수 있습니다.

정책 서버 사용자 저장소는 Active Directory 의 글로벌 카탈로그 지원 기능을 지원합니다. 하지만 글로벌 카탈로그는 Active Directory 에 대한 쓰기를 지원하지 않기 때문에 암호 서비스와 같이 Active Directory 쓰기가 필요한 기능은 지원되지 않습니다.

다음 단계를 수행하십시오.

1. "인프라", "디렉터리"를 차례로 클릭합니다.
2. "사용자 디렉터리"를 선택합니다.
3. "사용자 디렉터리 만들기"를 클릭합니다.
4. "일반" 및 디렉터리 설정 영역에서 필요한 연결 정보를 지정합니다.
5. "LDAP 설정" 영역에서 "LDAP 검색" 및 "LDAP 사용자 DN 조회" 설정을 구성합니다.
6. (선택 사항) "구성"을 클릭하여 부하 분산 및 장애 조치를 구성합니다.
참고: 부하 분산 및 장애 조치에 대한 자세한 내용은 "LDAP 부하 분산 및 장애 조치" 단원을 참조하십시오.
7. (선택 사항) "관리자 자격 증명" 영역에서 다음 작업을 수행하십시오.
 - a. "자격 증명 필요" 옵션을 선택합니다.
 - b. 관리자 계정의 자격 증명을 입력합니다.
8. (선택 사항) "사용자 특성" 영역에서 SiteMinder 용으로 예약된 사용자 디렉터리 프로필 특성을 지정합니다.
9. (선택 사항) "특성 매핑 목록" 영역에서 "만들기"를 클릭하여 사용자 특성 매핑을 구성합니다.
10. 제출을 클릭합니다.

사용자 디렉터리 연결이 생성됩니다.

Oracle Internet Directory 사용자 디렉터리 연결을 구성하는 방법

Oracle Internet Directory(OID) 사용자 디렉터를 사용자 저장소로 사용할 수 있습니다. 다음 프로세스에는 정책 서버에 대한 사용자 저장소 연결을 생성하는 단계가 나와 있습니다.

1. 사용자 저장소 시스템 ping
2. Oracle Internet Directory 에 조직 단위 만들기
3. Oracle Internet Directory 연결 구성

Oracle Internet Directory 사용자 디렉터리에 대한 LDAP 조회 제한

Oracle Internet Directory Server 10g(9.0.4)가 사용자 저장소로 구성되어 있고 향상된 조회가 사용되는 경우에는 LDAP 조회가 작동하지 않습니다. 이는 OID 의 제한 때문입니다.

사용자 저장소 시스템 ping

정책 서버와 사용자 디렉터리 또는 데이터베이스 사이에 네트워크 연결이 있는지 확인하기 위해 구성하기 전에 사용자 저장소 시스템을 ping 하십시오.

참고: 일부 사용자 저장소 시스템의 경우 정책 서버가 자격 증명을 제공해야 합니다.

OID 디렉터리에 대한 조직 단위 만들기

OID 디렉터리에 사용자를 추가할 때 사용할 조직 단위를 생성할 수 있습니다.

OID 디렉터리에 대한 조직 단위를 생성하려면

1. ADD 를 사용하여 도메인에 조직 단위를 생성합니다.
예: OracleSchemaVersion
2. 조직 단위를 선택하고 고유 이름을 입력합니다.
예: ou=people,cn=OracleSchemaVersion

3. "Entry Management"(항목 관리)를 마우스 오른쪽 단추로 클릭하고 "Create"(만들기)를 선택합니다.
4. "Distinguished Name"(고유 이름) 대화 상자에서 "Add"(추가)를 클릭하고 "inetOrgPerson"을 선택합니다.
5. "Mandatory Properties"(필수 속성) 탭에서 다음 값을 입력합니다.
 - cn=user1
 - sn=user1
 - uid=user1
 - userpassword=user1
6. dn 을 cn=user1,ou=people,cn=OracleSchemaVersion 으로 지정합니다.

Oracle Internet Directory 연결 구성

정책 서버가 OID 사용자 저장소와 통신할 수 있도록 사용자 디렉터리 연결을 구성할 수 있습니다.

다음 단계를 수행하십시오.

1. "인프라", "디렉터리"를 차례로 클릭합니다.
2. "사용자 디렉터리", "사용자 디렉터리 만들기"를 차례로 클릭합니다.
참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.
3. "네임스페이스" 목록에서 LDAP 을 선택합니다.
 LDAP 설정이 열립니다.
4. "일반" 및 디렉터리 설정 그룹 상자에서 필요한 나머지 연결 정보를 지정합니다.
참고: 정책 서버가 FIPS 모드에서 작동 중이며 정책 서버와 통신할 때 디렉터리 연결이 보안 SSL 연결을 사용할 경우 정책 서버와 디렉터리 저장소가 사용하는 인증서는 FIPS 를 준수해야 합니다.
5. "LDAP 설정" 그룹 상자의 필드에서 "LDAP 검색" 및 "LDAP 사용자 DN 조회" 설정을 입력합니다.
6. (선택 사항) "관리자 자격 증명" 영역에서 다음 작업을 수행하십시오.
 - a. "자격 증명 필요" 옵션을 선택합니다.
 - b. 관리자 계정의 자격 증명을 입력합니다.

7. (선택 사항) "사용자 특성" 영역에서 SiteMinder 용으로 예약된 사용자 디렉터리 프로필 특성을 지정합니다.
8. (선택 사항) "특성 매핑 목록" 영역에서 "만들기"를 클릭하여 사용자 특성 매핑을 구성합니다.
9. 제출을 클릭합니다.
사용자 디렉터리 연결이 생성됩니다.

OpenLDAP 서버 사용자 디렉터리 연결을 구성하는 방법

OpenLDAP 서버를 사용자 저장소로 사용할 수 있습니다. 사용자 디렉터리 연결을 생성하려면 다음 단계를 완료하십시오.

1. 사용자 저장소를 생성합니다.
2. OpenLDAP 서버 사용자 디렉터리 연결을 구성합니다.

사용자 저장소 만들기

OpenLDAP Directory Server 를 사용자 저장소로 사용할 수 있습니다.

사용자 저장소를 생성하려면

1. LDIF 파일을 사용하여 루트 DN 아래에 ou=People 을 생성합니다.
2. 조직 단위 아래에 사용자를 생성합니다.

OpenLDAP Directory Server 사용자 디렉터리 연결 구성

정책 서버가 OpenLDAP 서버 사용자 저장소와 통신할 수 있도록 사용자 디렉터리 연결을 구성할 수 있습니다.

다음 단계를 수행하십시오.

1. "인프라", "디렉터리"를 차례로 클릭합니다.
2. "사용자 디렉터리"를 선택합니다.
3. "사용자 디렉터리 만들기"를 클릭합니다.
4. "일반" 및 디렉터리 설정 영역에서 필요한 연결 정보를 지정합니다.

5. "LDAP 설정" 영역에서 "LDAP 검색" 및 "LDAP 사용자 DN 조회" 설정을 구성합니다.
6. "관리자 자격 증명" 영역에서 다음 단계를 수행하십시오.
 - a. "자격 증명 필요" 옵션을 선택합니다.
 - b. 관리자 계정의 자격 증명을 입력합니다.
7. (선택 사항) "사용자 특성" 영역에서 SiteMinder 용으로 예약된 사용자 디렉터리 프로필 특성을 지정합니다.
8. (선택 사항) "특성 매핑 목록" 영역에서 "만들기"를 클릭하여 사용자 특성 매핑을 구성합니다.
9. 제출을 클릭합니다.
사용자 디렉터리 연결이 생성됩니다.

Red Hat Directory Server 사용자 디렉터리 연결을 구성하는 방법

Red Hat Directory Server 를 사용자 저장소로 사용할 수 있습니다. 사용자 디렉터리 연결을 생성하려면 다음 단계를 완료하십시오.

1. 사용자 저장소 시스템을 ping 합니다.
2. 사용자 디렉터리 연결을 구성합니다.

사용자 저장소 시스템 ping

정책 서버와 사용자 디렉터리 또는 데이터베이스 사이에 네트워크 연결이 있는지 확인하기 위해 구성하기 전에 사용자 저장소 시스템을 ping 하십시오.

참고: 일부 사용자 저장소 시스템의 경우 정책 서버가 자격 증명을 제공해야 합니다.

Red Hat Directory Server 사용자 디렉터리 연결 구성

정책 서버가 Red Hat Directory Server 사용자 저장소와 통신할 수 있도록 사용자 디렉터리 연결을 구성할 수 있습니다.

다음 단계를 수행하십시오.

1. "인프라", "디렉터리"를 차례로 클릭합니다.
2. "사용자 디렉터리"를 선택합니다.
3. "사용자 디렉터리 만들기"를 클릭합니다.
4. "일반" 및 디렉터리 설정 영역에서 필요한 연결 정보를 지정합니다.
5. "LDAP 설정" 영역에서 "LDAP 검색" 및 "LDAP 사용자 DN 조회" 설정을 구성합니다.
6. "관리자 자격 증명" 영역에서 다음 작업을 수행하십시오.
 - a. "자격 증명 필요" 옵션을 선택합니다.
 - b. 관리자 계정의 자격 증명을 입력합니다.
7. (선택 사항) "사용자 특성" 영역에서 SiteMinder 용으로 예약된 사용자 디렉터리 프로필 특성을 지정합니다.
8. (선택 사항) "특성 매핑 목록" 영역에서 "만들기"를 클릭하여 사용자 특성 매핑을 구성합니다.
9. 제출을 클릭합니다.

사용자 디렉터리 연결이 생성됩니다.

ODBC 사용자 디렉터리 연결을 구성하는 방법

ODBC 사용자 디렉터리를 사용자 저장소로 사용할 수 있습니다. 다음 프로세스에는 정책 서버에 대한 사용자 저장소 연결을 생성하는 단계가 나와 있습니다.

1. 사용자 저장소 시스템 ping
2. ODBC 디렉터리 연결 구성

사용자 저장소 시스템 ping

정책 서버와 사용자 디렉터리 또는 데이터베이스 사이에 네트워크 연결이 있는지 확인하기 위해 구성하기 전에 사용자 저장소 시스템을 ping 하십시오.

참고: 일부 사용자 저장소 시스템의 경우 정책 서버가 자격 증명을 제공해야 합니다.

ODBC 디렉터리 연결 구성

정책 서버가 ODBC 사용자 저장소와 통신할 수 있도록 사용자 디렉터리 연결을 구성할 수 있습니다.

감사 로그에 Microsoft SQL Server 데이터베이스를 사용 중이며 캐싱이 작동 중인 경우 부하가 높으면 정책 서버가 로깅을 위해 메시지를 큐에 넣기 때문에 성능이 느려질 수 있습니다. 문제를 완화하려면 많은 사용자가 액세스하는 리소스와 연관된 영역에 대해 비동기 감사를 설정하십시오.

다음 단계를 수행하십시오.

1. "인프라", "디렉터리"를 차례로 클릭합니다.
사용자 디렉터리와 관련된 개체가 왼쪽에 표시됩니다.
2. "사용자 디렉터리"를 클릭합니다.
"사용자 디렉터리" 화면이 표시됩니다.
3. "사용자 디렉터리 만들기"를 클릭합니다.
"사용자 디렉터리 만들기" 화면이 나타나고 LDAP 연결을 구성하는 데 필요한 설정이 표시됩니다.
4. "네임스페이스" 목록에서 ODBC 을 선택합니다.
ODBC 설정이 표시됩니다.
5. "일반" 및 디렉터리 설정 영역에서 나머지 필요한 연결 정보를 지정합니다.
참고: 정책 서버가 FIPS 모드에서 작동 중이며 정책 서버와 통신할 때 디렉터리 연결이 보안 SSL 연결을 사용할 경우 정책 서버와 디렉터리 저장소가 사용하는 인증서는 FIPS 를 준수해야 합니다.
6. SQL 쿼리 체계를 선택합니다.

7. (선택 사항) "관리자 자격 증명" 영역에서 다음 작업을 수행하십시오.

- a. "자격 증명 필요"를 선택합니다.
- b. 관리자 계정의 자격 증명을 입력합니다.

참고: 사용자 이름은 사용자 디렉터리 데이터가 포함된 테이블을 소유한 사용자와 일치해야 합니다. 예를 들어 SmSampleUsers 스키마를 사용하는 경우 이 사용자는 SmUser, SmUserGroup 및 SmGroup 테이블의 소유자여야 합니다. 관리자 계정에는 사용자 디렉터리에 대해 읽기 또는 읽기/쓰기 권한이 있어야 합니다.

8. (선택 사항) "사용자 특성" 영역에서 SiteMinder 용으로 예약된 사용자 디렉터리 프로필 특성을 지정합니다.

9. (선택 사항) "특성 매핑 목록" 영역에서 "만들기"를 클릭하여 사용자 특성 매핑을 구성합니다.

10. 제출을 클릭합니다.

사용자 디렉터리 연결이 생성됩니다.

SQL Server 사용자 저장소에서 대/소문자 비구분 및 불필요한 후행 공백이 있는 암호와 관련된 문제

SQL Server 사용자 저장소에서는 대/소문자가 구분되지 않고 사용자 암호의 불필요한 후행 공백이 무시될 수 있습니다. 이 경우 사용자가 암호를 입력할 때 대/소문자를 구분하지 않거나 불필요한 후행 공백을 포함하더라도 보호된 리소스에 액세스할 수 있기 때문에 문제가 될 수 있습니다. 예를 들어 암호 정책이 "ABCD"와 같이 대/소문자를 구분하는 암호를 사용하도록 구성되어 있는 경우 사용자가 "ABcd"를 입력하더라도 SQL Server 에서 이 입력이 허용됩니다. 또 다른 예로, 암호 정책 구성에 따라 사용자 암호가 "A B C"여야 하는데 사용자가 "A B C"를 입력하더라도 SQL Server에서는 암호에 포함된 불필요한 후행 공백이 무시되고 이 입력이 허용됩니다.

다음은 이러한 문제에 대한 두 가지 해결책입니다.

첫 번째 문제: SQL Server 사용자 저장소에서 대/소문자가 구분되지 않음

SQL Server 데이터베이스가 데이터 정렬을 올바르게 수행하지 않고 암호의 대/소문자를 구분하지 않습니다.

해결책 1

SQL Server 사용자 저장소에서 대/소문자가 구분되도록 하려면 데이터베이스 설치 시 테이블을 생성하는 동안 올바른 데이터 정렬을 선택하십시오.

데이터 정렬에 대한 자세한 내용은 다음 항목을 참조하십시오.

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/instsql/in_collation_30a6.asp

해결책 2

기본 데이터 정렬을 사용하여 SQL Server 를 설치한 경우 데이터베이스에서 암호의 대/소문자 구분 여부를 인식하지 못하면 사용자 저장소에 대한 테이블을 생성할 때 올바른 데이터 정렬을 생성하십시오.

데이터 정렬을 지정하려면 다음 스크립트 중 하나를 수정한 후 가져오십시오.

siteminder_install\db\SQL\smsampleusers_sqlserver.sql

siteminder_install\db\SQL\smsampleusers_sqlserver_upgrade.sql

참고: 이 두 스크립트 파일은 기본 지역화(미국 영어)를 사용합니다.

smsampleusers_sqlserver.sql 스크립트 파일

smsampleusers_sqlserver.sql 스크립트 파일에서 굵게 강조 표시된 다음 행을 변경하십시오.

```
CREATE TABLE SmGroup (  
    GroupID          int NOT NULL,  
    Name nvarchar(255) COLLATE Latin1_General_CS_AS NOT NULL ,  
    PRIMARY KEY (GroupID)  
)  
DROP TABLE SmUser  
go  
CREATE TABLE SmUser (  
    UserID          int NOT NULL,  
    Name  nvarchar(255) COLLATE Latin1_General_CS_AS NOT NULL,  
    Password nvarchar(255) COLLATE Latin1_General_CS_AS NOT NULL,  
    LastName nvarchar(255) COLLATE Latin1_General_CS_AS NOT NULL,  
    FirstName nvarchar(255) COLLATE Latin1_General_CS_AS NOT NULL,  
    EmailAddress nvarchar(255) COLLATE Latin1_General_CS_AS NOT NULL,  
    TelephoneNumber nvarchar(255) COLLATE Latin1_General_CS_AS NOT NULL ,  
    Disabled nvarchar(255) COLLATE Latin1_General_CS_AS NOT NULL ,  
    PIN      nvarchar(255) COLLATE Latin1_General_CS_AS NOT NULL ,  
    Mileage int NOT NULL,  
    PasswordData varchar(2000) NOT NULL,  
    PRIMARY KEY (UserID)  
)  
go
```

이 스크립트를 수정한 후 SQL Server 데이터베이스로 가져와야 합니다.

중요! 이 스크립트를 실행하면 기존 데이터가 제거되고 새 테이블이 생성되므로 기존 데이터를 백업해 두십시오.

smsampleusers_sqlserver_upgrade.sql 스크립트 파일

smsampleusers_sqlserver_upgrade.sql 스크립트 파일에서 굵게 강조 표시된 다음 행을 변경해야 합니다.

```
/* Upgrade table SmGroup*/
ALTER TABLE SmGroup ALTER COLUMN Name nvarchar(255) COLLATE Latin1_General_CS_AS NOT
NULL
go
/* Upgrade table SmUser*/
ALTER TABLE SmUser ALTER COLUMN Name nvarchar(255) COLLATE Latin1_General_CS_AS NOT
NULL
go
ALTER TABLE SmUser ALTER COLUMN Password nvarchar(255) COLLATE Latin1_General_CS_AS
NOT NULL
go
ALTER TABLE SmUser ALTER COLUMN LastName nvarchar(255) COLLATE Latin1_General_CS_AS
NOT NULL
go
ALTER TABLE SmUser ALTER COLUMN FirstName nvarchar(255) COLLATE Latin1_General_CS_AS
NOT NULL
go
ALTER TABLE SmUser ALTER COLUMN EmailAddress nvarchar(255) COLLATE
Latin1_General_CS_AS NOT NULL
go
ALTER TABLE SmUser ALTER COLUMN TelephoneNumber nvarchar(255) COLLATE
Latin1_General_CS_AS NOT NULL
go
ALTER TABLE SmUser ALTER COLUMN Disabled nvarchar(255) COLLATE Latin1_General_CS_AS
NOT NULL
go
ALTER TABLE SmUser ALTER COLUMN PIN nvarchar(255) COLLATE Latin1_General_CS_AS NOT
NULL
go
```

이 스크립트를 수정한 후 SQL Server 데이터베이스로 가져와야 합니다.

중요! 이 스크립트를 실행하면 기존 데이터가 제거되고 새 테이블이 생성되므로 기존 데이터를 백업해 두십시오.

두 번째 문제: SQL Server 에서 암호의 후행 공백이 무시됨

SQL Server 가 비교되는 두 문자열에 채우기를 적용하여 둘의 길이를 같게 만듭니다.

해결책

SQL Server 에서 데이터베이스에 저장된 암호의 후행 공백을 인식하도록 하려면 관리 UI 를 사용하여 ODBC 쿼리 체계 개체의 사용자 인증 쿼리를 수정하십시오. SQL Server 가 문자열을 채우기 또는 자르기 없이 비교하도록 하려면 = 연산자 대신 LIKE 조건자를 포함하십시오. LIKE 조건자 식의 오른쪽에 후행 공백을 포함한 값을 사용하면 SQL Server 는 비교를 수행하기 전에 두 값을 같은 길이가 되도록 채우지 않습니다. 인증 쿼리의 예는 다음과 같습니다.

```
select Name from SmUser where Name = '%s' and Password LIKE '%s'
```

중요! 암호 일치 쿼리에 LIKE 조건자 식을 사용할 경우 보안 허점이 발생할 수 있습니다. 사용자가 암호에 '%'를 입력할 경우 SQL Server 는 이를 LIKE 조건자에 대한 와일드카드 문자로 처리하므로 사용자가 여러 암호를 사용하여 인증할 수 있습니다.

다음에 주의하십시오.

- SDK 를 사용하여 ODBC 쿼리 체계 개체를 생성할 경우 Sm_PolicyApi_ODBCQueryScheme_t 개체의 pszQueryAuthenticateUser 특성을 사용하여 인증 쿼리를 지정할 수 있습니다.
- Perl 스크립팅 인터페이스를 사용하여 ODBC 쿼리 체계 개체를 생성할 경우 CreateODBCQueryScheme() API 를 호출하는 동안 인증 쿼리를 지정할 수 있습니다.

사용자 지정 사용자 디렉터리 연결을 구성하는 방법

사용자 지정 디렉터를 사용자 저장소로 사용할 수 있습니다. 다음 프로세스에는 정책 서버에 대한 사용자 저장소 연결을 생성하는 단계가 나와 있습니다.

1. 사용자 저장소 시스템 ping
2. 사용자 지정 디렉터리 연결 구성

사용자 저장소 시스템 ping

정책 서버와 사용자 디렉터리 또는 데이터베이스 사이에 네트워크 연결이 있는지 확인하기 위해 구성하기 전에 사용자 저장소 시스템을 ping 하십시오.

참고: 일부 사용자 저장소 시스템의 경우 정책 서버가 자격 증명을 제공해야 합니다.

사용자 지정 디렉터리 연결 구성

정책 서버가 사용자 지정 사용자 저장소와 통신할 수 있도록 사용자 디렉터리 연결을 구성할 수 있습니다.

다음 단계를 수행하십시오.

1. "인프라", "디렉터리"를 차례로 클릭합니다.
2. "사용자 디렉터리"를 클릭합니다.
3. "사용자 디렉터리 만들기"를 클릭합니다.

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

4. "네임스페이스" 목록에서 "사용자 지정"을 선택합니다.
5. "일반" 및 디렉터리 설정 영역에서 필요한 연결 정보를 지정합니다.
6. (선택 사항) "관리자 자격 증명" 영역에서 다음 단계를 완료합니다.
 - a. "자격 증명 필요" 옵션을 선택합니다.
 - b. 관리자 계정의 자격 증명을 입력합니다.
7. (선택 사항) "특성 매핑 목록" 영역에서 "만들기"를 클릭하여 사용자 특성 매핑을 구성합니다.

참고: 정책 서버는 공유 라이브러리를 사용하여 사용자 지정 디렉터리에 사용 가능한 사용자 특성을 결정합니다. 사용자 특성을 입력하기 전에 사용자 디렉터리 연결을 생성하십시오.

8. 제출을 클릭합니다.

사용자 디렉터리 연결이 생성됩니다.

SSL 을 통한 LDAP 사용자 디렉터리 연결 구성 방법

SSL 을 통한 LDAP 사용자 디렉터리 연결을 사용하려면 인증서 데이터베이스 파일을 구성해야 합니다.

다음 단계를 수행하십시오.

1. 인증서 데이터베이스 파일을 생성합니다.
2. 인증서 데이터베이스에 루트 CA(인증 기관)를 추가합니다.
3. 인증서 데이터베이스에 서버 인증서를 추가합니다. 서버 인증서가 인증 기관에서 발급된 경우 각 인증 기관의 루트 인증서를 인증서 데이터베이스에도 추가하십시오.
4. 인증서 데이터베이스의 인증서를 나열합니다.
5. 사용자 디렉터리 연결에 대해 SSL 을 구성합니다.
6. 정책 서버가 인증서 데이터베이스를 가리키도록 설정합니다.
7. SSL 연결을 확인합니다.

SSL 을 통한 연결 구성 전 작업

SSL 을 통한 LDAP 사용자 디렉터리 연결을 구성하기 전에 다음 사항을 검토하십시오.

- 디렉터리 서버가 SSL 이 사용되도록 설정되었는지 확인합니다.
- 데이터베이스 파일이 Netscape 데이터베이스 버전 파일 형식(cert8.db)인지 확인하십시오. 정책 서버는 Mozilla LDAP SDK 를 사용하여 LDAP 디렉터리와 통신합니다.

중요! cert8.db 데이터베이스 파일에 인증서를 설치할 때 Microsoft Internet Explorer 를 사용하지 마십시오.

- (Active Directory) 다음 사항을 고려합니다.
 - AD 네임스페이스를 사용하여 사용자 디렉터리 연결이 구성된 경우에는 이후 항목에 설명되어 있는 SSL 프로세스가 적용되지 않습니다. AD 네임스페이스는 SSL 연결 설정 시 네이티브 Windows 인증서 리포지토리를 사용합니다. SSL 을 통해 통신하도록 AD 네임스페이스를 구성할 경우 다음과 같이 하십시오.
 - 사용자 디렉터리 연결에 대해 보안 연결이 구성되었는지 확인합니다.
 - Active Directory 인스턴스를 호스트하는 컴퓨터에서 루트 CA 인증서와 서버 인증서가 서비스 인증서 저장소에 추가되었는지 확인합니다.

인증서 데이터베이스 파일 만들기

인증서 데이터베이스 파일을 만들려면 정책 서버에 포함된 Mozilla Network Security Services(NSS) certutil 응용 프로그램을 사용하십시오.

참고: 다음 절차에서는 태스크를 완료하는 데 필요한 옵션 및 인수에 대해 자세히 설명합니다. NSS 유틸리티 옵션 및 인수의 전체 목록은 [NSS project page](#) (NSS 프로젝트 페이지)에서 Mozilla 설명서를 참조하십시오.

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

다음 단계를 수행하십시오.

1. 명령 프롬프트에서 설치 bin 디렉터리로 이동합니다.

예: C:\Program Files\CA\SiteMinder\bin

참고: Windows 에는 네이티브 certutil 유틸리티가 있습니다. 정책 서버의 bin 디렉터리에서 작업 중인지 확인하십시오. 그렇지 않을 경우 실수로 Windows certutil 유틸리티를 실행할 수 있습니다.

2. 다음 명령을 입력합니다.

```
certutil -N -d certificate_database_directory
```

-N

cert8.db, key3.db 및 secmod.db 인증서 데이터베이스 파일을 생성합니다.

-d certificate_database_directory

certutil 도구가 인증서 데이터베이스 파일을 생성할 디렉터리를 지정합니다.

참고: 파일 경로에 공백이 있으면 경로를 따옴표로 묶으십시오.

데이터베이스 키 암호화에 사용할 암호를 묻는 메시지가 표시됩니다.

3. 암호를 입력하고 확인합니다.

필요한 다음 인증서 데이터베이스 파일이 생성됩니다.

- cert8.db
- key3.db
- secmod.db

예: 인증서 데이터베이스 파일 만들기

```
certutil -N -d C:\certdatabase
```

인증서 데이터베이스에 루트 인증 기관 추가

루트 인증 기관(CA)을 추가하려면 정책 서버에 있는 Mozilla Network Security Services(NSS) certutil 응용 프로그램을 사용하십시오.

참고: 다음 절차에서는 태스크를 완료하는 데 필요한 옵션 및 인수에 대해 자세히 설명합니다. NSS 유틸리티 옵션 및 인수의 전체 목록은 [NSS project page](#) (NSS 프로젝트 페이지)에서 Mozilla 설명서를 참조하십시오.

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

다음 단계를 수행하십시오.

1. 명령 프롬프트에서 정책 서버 설치 bin 디렉터리로 이동합니다.

예: C:\Program Files\CA\SiteMinder\bin

참고: Windows 에는 네이티브 certutil 유틸리티가 있습니다. NSS 유틸리티의 bin 디렉터리에서 작업 중인지 확인하십시오. 그렇지 않을 경우 실수로 Windows certutil 유틸리티를 실행할 수 있습니다.

2. 다음 명령을 실행합니다.

```
certutil -A -n alias -t trust_arguments -i root_CA_path -d
certificate_database_directory
```

-A

인증서 데이터베이스에 인증서를 추가합니다.

-n alias

인증서의 별칭을 지정합니다.

참고: 별칭에 공백이 있는 경우 별칭을 따옴표로 묶으십시오.

-t trust_arguments

인증서에 적용할 트러스트 특성을 지정합니다. 세 개의 사용 가능한 트러스트 범주는 다음 순서로 표시됩니다: "SSL, 전자 메일, 개체 서명". 각 범주 위치에서 다음 특성 인수를 0 개 이상 사용할 수 있습니다.

p

유효한 피어입니다.

P

트러스트된 피어입니다. 이 인수는 p 를 내포합니다.

c

유효한 CA 입니다.

T

클라이언트 인증서를 발급하도록 트러스트된 CA 입니다. 이 인수는 c 를 내포합니다.

C

서버 인증서를 발급하도록 트러스트된 CA 입니다(SSL 만 해당). 이 인수는 c 를 내포합니다.

중요! 이 인수는 SSL 트러스트 범주에 필요합니다.

u

인증 또는 서명에 인증서를 사용할 수 있습니다.

-i root_CA_path

루트 CA 파일의 경로를 지정합니다. 이 경로는 인증서 이름을 포함합니다. 인증서의 유효한 확장명에는 cert, .cer, .pem 이 포함됩니다.

참고: 파일 경로에 공백이 있으면 경로를 따옴표로 묶으십시오.

-d certificate_database_directory

인증서 데이터베이스가 포함된 디렉터리의 경로를 지정합니다.

참고: 파일 경로에 공백이 있으면 경로를 따옴표로 묶으십시오.

예: 인증서 데이터베이스에 루트 CA 추가

```
certutil -A -n "My Root CA" -t "C,," -i C:\certificates\cacert.cer -d C:\certdatabase
```

인증서 데이터베이스에 서버 인증서 추가

SSL 을 통한 통신을 사용하려면 인증서에 서버 인증서를 추가하십시오. 정책 서버에 있는 Mozilla Network Security Services(NSS) certutil 응용 프로그램을 사용하십시오.

참고: 다음 절차에서는 태스크를 완료하는 데 필요한 옵션 및 인수에 대해 자세히 설명합니다. NSS 유틸리티 옵션 및 인수의 전체 목록은 [NSS project page](#) (NSS 프로젝트 페이지)에서 Mozilla 설명서를 참조하십시오.

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

다음 단계를 수행하십시오.

1. 명령 프롬프트에서 정책 서버 설치 bin 디렉터리로 이동합니다.

예: C:\Program Files\CA\SiteMinder\bin

참고: Windows 에는 네이티브 certutil 유틸리티가 있습니다. NSS 유틸리티의 bin 디렉터리에서 작업 중인지 확인하십시오. 그렇지 않을 경우 실수로 Windows certutil 유틸리티를 실행할 수 있습니다.

2. 다음 명령을 실행합니다.

```
certutil -A -n alias -t trust_arguments -i server_certificate_path -d  
certificate_database_directory
```

-A

인증서 데이터베이스에 인증서를 추가합니다.

-n alias

인증서의 별칭을 지정합니다.

참고: 별칭에 공백이 있는 경우 별칭을 따옴표로 묶으십시오.

-t trust_arguments

트러스트 인수를 지정합니다. 각 인증서에 대한 세 개의 사용 가능한 트러스트 범주는 다음 순서로 표시됩니다: "SSL, 전자 메일, 개체 서명". 각 범주 위치에서 다음 특성 인수를 0 개 이상 사용할 수 있습니다.

p

유효한 피어입니다.

P

트러스트된 피어입니다. 이 인수는 p 를 내포합니다.

중요! 이 인수는 SSL 트러스트 범주에 필요합니다.

-i server_certificate_path

서버 인증서의 경로를 지정합니다. 이 경로는 인증서 이름을 포함합니다. 인증서의 유효한 확장명에는 cert, .cer, .pem 이 포함됩니다.

참고: 파일 경로에 공백이 있으면 경로를 따옴표로 묶으십시오.

-d certificate_database_directory

인증서 데이터베이스가 포함된 디렉터리의 경로를 지정합니다.

참고: 파일 경로에 공백이 있으면 경로를 따옴표로 묶으십시오.

NSS 에서 인증서 데이터베이스에 서버 인증서를 추가합니다.

예: 인증서 데이터베이스에 서버 인증서 추가

```
certutil -A -n "My Server Certificate" -t "P,," -i C:\certificates\servercert.cer -d C:\certdatabase
```

인증서 데이터베이스의 인증서 목록 표시

인증서가 인증서 데이터베이스에 있는지 확인하려면 **Mozilla Network Security Services(NSS) certutil** 응용 프로그램을 사용하십시오. 정책 서버에는 이 도구가 포함되어 있습니다.

참고: 다음 절차에서는 태스크를 완료하는 데 필요한 옵션 및 인수에 대해 자세히 설명합니다. NSS 유틸리티 옵션 및 인수의 전체 목록은 [NSS project page](#) (NSS 프로젝트 페이지)에서 **Mozilla** 설명서를 참조하십시오.

중요! **Windows Server 2008** 에서 **SiteMinder** 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

다음 단계를 수행하십시오.

1. 명령 프롬프트에서 정책 서버 설치 bin 디렉터리로 이동합니다.

예: C:\Program Files\CA\SiteMinder\bin

참고: Windows 에는 네이티브 certutil 유틸리티가 있습니다. NSS 유틸리티의 bin 디렉터리에서 작업 중인지 확인하십시오. 그렇지 않을 경우 실수로 Windows certutil 유틸리티를 실행할 수 있습니다.

2. 다음 명령을 실행합니다.

```
certutil -L -d certificate_database_directory
```

-L

인증서 데이터베이스에 있는 모든 인증서의 목록을 표시합니다.

-d certificate_database_directory

인증서 데이터베이스가 포함된 디렉터리의 경로를 지정합니다.

참고: 파일 경로에 공백이 있으면 경로를 따옴표로 묶으십시오.

이 명령은 루트 CA 별칭, 서버 인증서 별칭, 그리고 인증서를 인증서 데이터베이스에 추가할 때 지정한 트러스트 특성을 표시합니다.

예: 인증서 데이터베이스의 인증서 목록 표시

```
certutil -L -d C:\certdatabase
```

사용자 디렉터리 연결에 대해 SSL 구성

정책 서버와 사용자 저장소가 적절히 통신할 수 있도록 사용자 저장소에 대한 SSL 연결을 구성합니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "인프라", "디렉터리"를 차례로 클릭합니다.
3. "사용자 디렉터리"를 클릭합니다.
4. 원하는 사용자 디렉터리 연결의 이름을 클릭합니다.
5. 아래로 스크롤하고 "수정"을 클릭합니다.
6. 디렉터리 설정 영역에서 "보안 연결" 옵션을 선택하고 "제출"을 클릭합니다.

사용자 디렉터리 연결은 SSL 을 통해 통신할 수 있습니다.

정책 서버를 인증서 데이터베이스에 연결

SSL 을 통해 사용자 디렉터리와 통신하려면 정책 서버에서 인증서 데이터베이스를 지정해야 합니다.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 시작합니다.

중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자 권한으로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "데이터" 탭을 클릭합니다.
3. "Netscape 인증서 데이터베이스 파일" 필드에 인증서 데이터베이스 파일의 경로를 입력합니다.

예: C:\certdatabase\cert8.db

참고: key3.db 파일은 cert8.db 파일과 동일한 디렉터리에 있어야 합니다.

4. 정책 서버를 다시 시작합니다.

정책 서버가 SSL 을 통하여 사용자 디렉터리와 통신할 수 있습니다.

SSL 연결 확인

사용자 디렉터리와 정책 서버가 올바르게 통신하는지 확인하려면 SSL 연결을 확인하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "인프라", "디렉터리"를 차례로 클릭합니다.
3. "사용자 디렉터리"를 클릭합니다.
4. 원하는 사용자 디렉터리 연결의 이름을 클릭합니다.
5. "콘텐츠 보기"를 클릭합니다.

SSL이 적절하게 구성된 경우 "디렉터리 콘텐츠" 화면이 나타나고 사용자 디렉터리의 콘텐츠가 나열됩니다.

SSL 을 통한 Oracle 사용자 디렉터리 연결 구성

SSL 을 통해 통신하도록 정책 서버와 Oracle 데이터베이스 사이의 연결을 구성할 수 있습니다. 연결을 구성하기 전에 Oracle 데이터베이스에서 SSL 이 활성화되어 있는지 확인하십시오.

정책 서버가 SSL 을 통해 Oracle 데이터베이스에 연결하는 방식

SSL 을 통해 정책 서버와 Oracle 데이터베이스 간의 연결이 설정되는 과정은 다음과 같습니다.

1. 정책 서버가 연결을 요청하면 Oracle 데이터베이스 서버는 서버의 공용 인증서를 제공합니다. Oracle 데이터베이스 서버가 제공하는 인증서의 신뢰성을 검사하도록 정책 서버를 구성할 수 있습니다.

필요한 경우 인증서 유효성을 검사하도록 정책 서버를 구성하지 않고도 SSL 을 통해 Oracle 데이터베이스와 통신하도록 정책 서버를 구성할 수 있습니다.

참고: 정책 서버는 트러스트 저장소를 사용하여 인증서의 신뢰성을 검사합니다. 트러스트 저장소는 인증 기관(CA)의 단일 공용 인증서입니다. 또한 트러스트 인증서는 트러스트된 CA 의 여러 공용 인증서를 포함하는 PKCS12 트러스트 저장소입니다. 공용 인증서는 암호로 보호되지 않는 반면 PKCS12 트러스트 저장소는 암호화되고 암호로 보호됩니다.

2. Oracle 인증서가 트러스트 저장소의 인증서와 일치하면 정책 서버와 Oracle 데이터베이스 간에 암호화된 연결이 설정됩니다. 인증서가 트러스트 저장소의 인증서와 일치하지 않으면 연결이 실패하고 정책 서버에서 오류가 생성됩니다.

Windows 에서 SSL 구성

"ODBC 데이터 원본 관리자" 콘솔을 사용하여 정책 서버가 SSL 을 통해 Oracle 과 통신하도록 구성할 수 있습니다.

다음 단계를 수행하십시오.

1. "ODBC 데이터 원본 관리자" 콘솔을 엽니다.
2. "시스템 DSN" 탭에서 SiteMinder Oracle 데이터베이스의 DSN 을 선택합니다.
3. "구성"을 클릭합니다.

"ODBC Oracle Wire Protocol Driver 설정" 대화 상자가 표시됩니다.

4. "보안" 탭을 클릭합니다.
5. 다음 암호화 매개 변수를 지정합니다.

Encryption Method(암호화 방법)

정책 서버와 Oracle 데이터베이스 서버 간에 전송되는 데이터를 암호화하기 위해 정책 서버에서 사용할 암호화 방법을 지정합니다.

기본값: 0 - No Encryption(암호화 안 함)

필요한 값: 1 - "SSL Auto"(SSL 자동)

Validate Server Certificate(서버 인증서 유효성 검사)

(선택 사항) 정책 서버에서 Oracle 데이터베이스가 제공하는 인증서의 신뢰성을 검사하도록 지정합니다.

기본값: 선택됨

정책 서버에서 Oracle 데이터베이스가 제공하는 인증서의 신뢰성을 검사할 필요가 없도록 SSL 을 구성하려면 이 항목의 선택을 취소합니다.

Trust Store(트러스트 저장소)

트러스트 저장소 파일의 경로 이름을 정의합니다. Oracle 데이터베이스가 제공하는 인증서의 신뢰성을 확인하려면 정책 저장소를 요청할 때 이 값을 지정하십시오.

필요한 값: 트러스트 저장소는 CA 의 공용 인증서이거나 하나 이상의 인증서가 포함된 PKCS12 트러스트 저장소일 수 있습니다. 공용 인증서는 암호로 보호되지 않는 단일 인증서입니다. PKCS12 트러스트 저장소는 암호로 보호됩니다.

Trust Store Password(트러스트 저장소 암호)

트러스트 저장소에 액세스하는 데 필요한 암호를 정의합니다.

Host Name In Certificate(인증서의 호스트 이름)

인증서의 호스트 이름을 정의합니다. 인증서의 호스트 이름은 Oracle 데이터베이스 서버에 연결하는 데 사용되는 호스트 이름과 일치해야 합니다. 호스트 이름이 일치하지 않으면 연결이 실패합니다.

참고: 이 연결에는 "키 저장소", "키 저장소 암호" 및 "키 암호" 매개 변수를 적용할 수 없습니다.

6. "확인"을 클릭합니다.

UNIX 에서 SSL 구성

정책 서버가 SSL 을 통해 Oracle 과 통신할 수 있도록 하려면 UNIX 에서 정책 서버에 대해 SSL 을 구성하십시오.

다음 단계를 수행하십시오.

1. 편집기를 사용하여 system_odbc.ini 파일을 편집합니다. system_odbc.ini 파일은 /nete_ps_root/db 디렉터리에 있습니다.

2. SSL 을 통해 연결할 Oracle DSN 에 다음 매개 변수를 추가합니다.

`ValidateServerCertificate=0` 또는 `1`

서버 인증서의 유효성을 검사하려면 `1` 을 지정하십시오. 서버 인증서의 유효성을 검사하지 않으려면 `0` 을 지정하십시오.

`TrustStore=CA` 인증서 또는 `PKCS12` 트러스트 저장소의 경로

`TrustStorePassword=트러스트 저장소 암호`

`HostNameInCertificate=호스트 이름.도메인.com`

예:

`ValidateServerCertificate=1`

`TrustStore=\nete_ps_root\db\MyCAcert.cer` or

`\nete_ps_root\db\MyCertTrustStore.p12`

`TrustStorePassword=abcd`

`HostNameInCertificate=mydbhost.abc.com`

3. `system_odbc.ini` 파일을 저장한 후 닫습니다.

LDAP 부하 분산 및 장애 조치

장애 조치 및 부하 분산 기능을 사용하기 위해 정책 서버는 LDAP 쿼리를 여러 LDAP 서버로 분산시킬 수 있습니다. 정책 서버는 LDAP 서버 하나에서 더 이상 응답이 없을 때까지 해당 LDAP 서버에서 모든 요청을 처리합니다. 기본 서버가 응답하지 않을 경우 정책 서버는 장애 조치용으로 지정된 다음 서버로 요청을 라우팅합니다. 이 프로세스는 여러 서버에서 반복될 수 있습니다. 기본 서버가 요청을 다시 처리할 수 있게 되면 정책 서버는 원래 서버로 요청을 라우팅합니다.

부하 분산이 구성되어 있는 경우 정책 서버는 지정된 LDAP 서버로 요청을 분산합니다. 부하 분산 기능을 사용하면 LDAP 사용자 디렉터리 정보에 대한 액세스 효율성이 높아지고 서버 장애에 대비한 중복성이라는 추가적인 이점까지 얻을 수 있습니다.

포트 번호 고려 사항

개별 LDAP 서버와 장애 조치 그룹에 직접 포트 번호를 할당하거나, 정책 서버가 LDAP 서버에 기본 포트 번호를 사용하도록 할 수 있습니다.

다음 지침은 포트 번호를 직접 지정할 때 적용됩니다.

조건	결과
장애 조치 그룹의 마지막 서버를 제외한 모든 서버에 포트 번호가 지정됨	정책 서버는 그룹에서 특정 포트가 지정되지 않은 서버에는 기본 포트가 사용된다고 가정합니다. SSL의 기본값은 636입니다. 비 SSL의 기본값은 389입니다. 예를 들어 장애 조치 서버 그룹에 다음이 포함되어 있다고 가정합니다. 123.123.12.12:350 123.123.34.34 이 장애 조치 그룹의 첫 번째 서버는 포트 350을 포함합니다. 해당 서버와의 통신은 포트 350에서 수행됩니다. 장애 조치 그룹의 두 번째 서버에는 포트가 지정되지 않았기 때문에 첫 번째 서버가 실패할 경우 정책 서버는 기본 포트 389를 사용하여 두 번째 서버와 통신합니다.

장애 조치 구성

중복성을 제공하기 위해 장애 조치를 구성합니다. 두 디렉터리가 동일한 포트 번호를 공유하므로 장애 조치 디렉터리는 기본 디렉터리로서 동일한 유형을 통신(SSL 또는 비 SSL)을 사용합니다.

다음 단계를 수행하십시오.

1. "사용자 디렉터리" 창의 "디렉터리 설정" 그룹 상자에서 "구성"을 클릭합니다.
2. "장애 조치 추가"를 클릭합니다.
3. 정책 서버가 장애 조치되어야 하는 서버의 호스트 이름 및 포트를 입력합니다.

참고: 포트 번호를 지정하지 않을 경우 기본 포트가 사용됩니다. SSL의 기본 포트는 636입니다. 비 SSL의 기본 포트는 389입니다.

4. 2~3 단계를 반복하여 추가 장애 조치 서버를 정의합니다.

참고: 마지막 서버에 대해 포트를 지정하고 그룹의 다른 서버에 대해서는 포트를 지정하지 않을 경우 지정된 포트가 그룹의 모든 서버에 사용됩니다.

5. "확인"을 클릭합니다.

부하 분산 구성

부하 분산을 구성하여 정책 서버가 모든 LDAP 서버에 요청을 고르게 분산하도록 할 수 있습니다.

다음 단계를 수행하십시오.

1. "디렉터리 설정" 그룹 상자에서 "구성"을 클릭합니다.
2. "부하 분산 추가"를 클릭합니다.
3. 정책 서버가 부하를 분산해야 하는 서버의 호스트 이름 및 포트를 입력합니다.
4. 2~3 단계를 반복하여 추가 부하 분산 서버를 정의합니다.
5. "확인"을 클릭합니다.

"사용자 디렉터리" 창이 열립니다. "서버" 필드에 부하 분산용으로 지정된 서버가 나열됩니다. 부하 분산용으로 지정된 각 서버는 쉼표(,)로 구분됩니다.

부하 분산 및 장애 조치 구성

여러 서버로 요청을 분산시켜 중복성을 제공하기 위해 부하 분산 기능 및 장애 조치를 구성합니다.

다음 단계를 수행하십시오.

1. "디렉터리 설정" 그룹 상자에서 "구성"을 클릭합니다.
2. 장애 조치를 위해 할당된 정책 서버의 호스트 이름과 포트를 입력합니다.

포트 번호를 지정하지 않을 경우 기본 포트가 사용됩니다. SSL의 기본 포트는 636입니다. 비 SSL의 기본 포트는 389입니다.

3. 2~3 단계를 반복하여 다른 장애 조치 서버를 정의합니다.

마지막 서버에 대한 포트를 지정할 때는 다른 포트를 지정하지 마십시오.
정책 서버는 다른 서버에 대해 지정된 포트를 사용합니다.

4. "부하 분산 추가"를 클릭합니다.

새 장애 조치 그룹이 열립니다.

5. 부하 분산을 위해 할당된 정책 서버의 호스트 이름과 포트를 입력합니다.

참고: 동일한 서버를 부하 분산용으로 여러 번 추가하여 특정 시스템에서 더 많은 요청을 처리하도록 할 수 있습니다. 예를 들어 그룹에 서버 1 과 서버 2 라는 두 개의 서버가 있다고 가정합니다. 서버 1 은 고성능 서버이고 서버 2 는 그보다 성능이 낮습니다. 이 경우 서버 1 을 부하 분산 목록에 두 번 추가하면 서버 2 가 요청을 하나 처리할 때마다 서버 1 은 요청을 두 개 처리하게 됩니다.

6. 5~6 단계를 반복하여 다른 부하 분산 서버를 정의합니다.

7. "확인"을 클릭합니다.

"사용자 디렉터리" 창이 열립니다. "서버" 필드에 장애 조치 및 부하 분산용으로 지정된 서버가 나열됩니다. 장애 조치용으로 지정된 각 서버는 공백으로 구분됩니다. 부하 분산용으로 지정된 각 서버는 쉼표(,)로 구분됩니다.

사용 사례 - 부하 분산 및 장애 조치

이 예에서는 SiteMinder 환경에 A 와 B 라는 두 개의 사용자 디렉터리가 있고 두 디렉터리가 다음 요구 사항을 충족해야 한다고 가정합니다.

- 사용자 디렉터리 A 는 사용자 디렉터리 B 로 장애 조치되고 B 와 부하를 분산해야 합니다.
- 사용자 디렉터리 B 는 사용자 디렉터리 A 로 장애 조치되고 A 와 부하를 분산해야 합니다.

공백은 장애 조치를 나타내고 쉼표는 부하 분산을 나타낼 경우 이 요구 사항을 다음과 같이 표현할 수 있습니다.

A B, B A

해결책:

이 구성에는 장애 조치 그룹이 두 개 필요합니다.

1. 사용자 디렉터리 B를 첫 번째 장애 조치 그룹에 추가합니다.

현재 구성은 A B입니다.

2. 부하 분산 그룹을 추가합니다.

참고: 부하 분산 그룹은 새 장애 조치 그룹으로 열립니다.

3. 사용자 디렉터리 B를 부하 분산 그룹의 첫 번째 서버로 나열합니다.

현재 구성은 A B, B입니다.

4. 사용자 디렉터리 A를 부하 분산 그룹의 두 번째 서버로 나열합니다.

결과적으로 서로 부하를 분산하는 "A B"와 "B A"라는 두 개의 장애 조치 그룹이 생성됩니다. 두 디렉터리를 모두 사용할 수 있는 경우 각 장애 조치 그룹의 첫 번째 디렉터리인 A와 B 간에 부하가 분산됩니다. 사용자 디렉터리 A를 사용할 수 없게 되면 사용자 디렉터리 B로 장애 조치되어, 사용자 디렉터리 A를 사용할 수 있게 될 때까지 사용자 디렉터리 B에서 모든 요청이 처리됩니다.

ODBC 데이터 원본 장애 조치 구성

기본 ODBC 데이터 원본과 이후 ODBC 데이터 원본을 사용할 수 없게 될 경우 중복성을 제공하기 위해 장애 조치를 구성합니다.

다음 단계를 수행하십시오.

1. "디렉터리 설정" 섹션에서 "구성"을 클릭합니다.
2. "추가"를 클릭합니다.
3. 장애 조치를 위해 지정된 데이터 원본을 입력합니다.
4. 2~3 단계를 반복하여 다른 데이터 원본을 추가합니다.
5. "확인"을 클릭합니다.

"사용자 디렉터리" 창이 열립니다. "서버" 필드에 장애 조치용으로 지정된 데이터 원본이 나열됩니다.

SQL 쿼리 체계

정책 서버는 SQL 쿼리 체계를 사용하여 관계형 데이터베이스에서 사용자 데이터를 찾는 쿼리를 작성합니다. SQL 쿼리 체계를 생성하고 편집하려면 "SQL 쿼리 체계" 대화 상자를 사용하십시오.

참고: 열 이름의 "SM_"은 특수 이름에 사용하도록 예약된 접두사입니다. 사용자 디렉터리의 열 이름은 "SM_" 접두사로 시작하지 마십시오.

SQL 쿼리 체계 구성

사용자 저장소 관계형 데이터베이스에서 사용자 데이터를 찾는 SQL 쿼리 체계를 구성할 수 있습니다.

다음 단계를 수행하십시오.

1. "인프라", "디렉터리"를 차례로 클릭합니다.
2. "SQL 쿼리 체계"를 클릭합니다.
3. "SQL 쿼리 체계 만들기"를 클릭합니다.
4. "새 개체 만들기" 옵션이 선택되어 있는지 확인하고 "확인"을 클릭합니다.
5. "일반" 영역의 필드에 이름과 설명을 입력합니다.
6. 데이터베이스 스키마에 맞게 쿼리 필드 내용을 업데이트합니다.

관계형 데이터베이스에서 작동하도록 각 쿼리를 구성합니다. 다음 데이터베이스 테이블 및 열 이름을 관계형 데이터베이스의 테이블 및 열 이름으로 바꿉니다.

- Name
사용자에 대한 Name 매개 변수는 고유합니다.
- SmUser - 테이블
- SmGroup - 테이블
- Password
- SmUserGroup - 테이블
- ID
- UserID

- FirstName
 - LastName
 - TelephoneNumber
 - EmailAddress
 - Mileage
 - PIN
 - GroupID
 - Disabled
7. 쿼리 유형을 선택하고 "제출"을 클릭합니다.
쿼리가 저장됩니다. 쿼리 체계를 사용자 디렉터리 연결과 연관시킬 수 있습니다.
 8. 정책 서버를 다시 시작합니다.

ODBC 사용자 디렉터리 연결에 SQL 쿼리 체계 추가

"사용자 디렉터리" 대화 상자를 사용하여 SQL 쿼리 체계를 선택할 수 있습니다.

다음 단계를 수행하십시오.

1. 기존 사용자 디렉터리 연결 개체에 대한 "사용자 디렉터리" 창을 엽니다.
2. "SQL 쿼리 체계" 목록에서 SQL 쿼리 체계를 선택하고 "제출"을 클릭합니다.
3. 정책 서버 관리 콘솔을 사용하여 정책 서버를 다시 시작합니다.

참고: 쿼리가 아포스트로피 문자(예: O'Neil)를 포함하는 이름을 반환하는 경우 쿼리 문자열의 모든 '%' 인스턴스를 "%s"로 바꾸십시오. 이 문제를 방지하려면 아포스트로피가 포함되지 않은 사용자 ID 로 쿼리를 작성하거나 '%'가 포함된 쿼리 문자열을 수정하십시오.

저장 프로시저를 사용한 인증을 위해 SQL 쿼리 체계 구성

ODBC 사용자 디렉터리에 대한 인증에 저장 프로시저가 필요한 경우 다음과 같이 저장 프로시저를 호출하도록 SQL 쿼리 체계를 구성하십시오.

SQLServer

구문: `Call Procedure_Name %s , %s`

예: `Call EncryptPW %s , %s`

SQLServer 의 저장 프로시저는 다음 요구 사항을 충족해야 합니다.

- 첫 번째 매개 변수는 사용자 이름이어야 하고 두 번째 매개 변수는 암호여야 합니다.
- 모든 매개 변수는 **OUT** 키워드를 사용하여 정의되어야 합니다.
- 저장 프로시저가 정수 값을 반환해야 합니다.

다음 예에서는 SQLServer 사용자 디렉터리에 사용할 저장 프로시저를 생성하는 방법을 보여 줍니다.

```
CREATE PROCEDURE EncryptPW
@UserName varchar(20) OUT ,
@PW varchar(20) OUT
AS
SELECT Smuser.name from Smuser where Smuser.name= @UserName and password = @PW
SELECT Smuser.password from Smuser where name= @UserName and password = @PW
return 0
```

MySQL

구문: `Call Procedure_Name %s, %s`

예: `Call EncryptPW %s, %s`

MySQL 의 저장 프로시저는 다음 요구 사항을 충족해야 합니다.

- 첫 번째 매개 변수는 사용자 이름이어야 하고 두 번째 매개 변수는 암호여야 합니다.
- 저장 프로시저가 값을 반환하지 않아야 합니다.

다음 예에서는 MySQL 사용자 디렉터리에 사용할 저장 프로시저를 생성하는 방법을 보여 줍니다.

```
CREATE PROCEDURE EncryptPW(INOUT p_UserName varchar(20), INOUT p_PW varchar(20))
BEGIN
SELECT SmUser.Name into p_UserName from test.SmUser where SmUser.Name =
p_UserName and SmUser.Password = p_PW;
SELECT SmUser.Password into p_PW from test.SmUser where SmUser.Name =
p_UserName and SmUser.Password = p_PW;
END;
```

Oracle 함수

Oracle 사용자 디렉터리의 경우 아래의 템플릿을 사용하여 다음 함수를 생성할 수 있습니다.

- EncryptPW
- ChangePW

Oracle 함수의 저장 프로시저는 다음 요구 사항을 충족해야 합니다.

- 첫 번째 매개 변수는 사용자 이름이어야 하고 두 번째 매개 변수는 암호여야 합니다.

EncryptPW 함수

EncryptPW 함수는 다음과 같이 정수 값을 반환해야 합니다.

- 값 0 은 성공을 나타냅니다.
- 값 1 은 실패를 나타냅니다.

다음 템플릿을 사용하여 EncryptPW 함수를 생성할 수 있습니다.

```
CREATE OR REPLACE FUNCTION EncryptPW(p_UserName IN OUT SmUser.Name%type, p_PW IN OUT
SmUser.Password%type)
RETURN INTEGER IS
nRet INTEGER :=1;
nCount NUMBER := 0;
BEGIN
select count(*) into nCount
from SmUser
where SmUser.Name = p_UserName and SmUser.Password = p_PW;
IF (nCount = 1) THEN
SELECT SmUser.Name into p_UserName
from SmUser
where SmUser.Name = p_UserName and SmUser.Password = p_PW;
```

```
SELECT SmUser.Password into p_PW
from SmUser
where SmUser.Name = p_UserName and SmUser.Password = p_PW;
RETURN 0;
END IF;
RETURN nRet;
END EncryptPW;
```

ChangePW 함수

ChangePW 함수는 다음과 같이 정수 값을 반환해야 합니다.

- 값 1 은 성공을 나타냅니다.
- 값 0 은 실패를 나타냅니다.

다음 템플릿을 사용하여 ChangePW 함수를 생성할 수 있습니다.

```
CREATE OR REPLACE FUNCTION ChangePW(p_PW IN SmUser.Password%type, p_UserName IN
SmUser.Name%type)
RETURN INTEGER IS
nRet INTEGER :=1;
nCount NUMBER := 0;
BEGIN
select count(*) into nCount
from SmUser
where SmUser.Name = p_UserName;
IF (nCount = 1) THEN
UPDATE SmUser
SET SmUser.Password = p_PW
where SmUser.Name = p_UserName;
COMMIT;
RETURN 0;
END IF;
```

장애 조치 및 연결 풀링 중 비동기 호출 지원

동기 호출은 요청이 완료된 경우에만 반환됩니다. 비동기 호출은 즉시 반환됩니다. 네트워크 오류와 관련된 지연을 방지하기 위해 호출자는 비동기 호출을 중지할 수 있습니다.

다음과 같은 데이터베이스로 비동기 호출을 보낼 수 있습니다.

- SQLServer
- Windows NT 및 Solaris 의 Oracle 8 - Oracle 11g

비동기 호출 지원 구성

다음 레지스트리 옵션은 레지스트리 하위 키
Netegrity\SiteMinder\CurrentVersion\Database 아래에 저장됩니다.

AsynchronousCalls

데이터베이스 호출이 비동기적으로 수행되는지 여부를 결정합니다.

값: 0(아니요), 1(예)

기본값: 0

AsynchronousSleepTime

각 호출 사이에서 미해결 SQL 호출의 상태를 확인하기 전까지 대기하는 시간을 지정합니다.

값: 0~n 밀리초

기본값: 15 밀리초

LoginTimeout

한 연결에서 데이터베이스에 로그인할 때까지 허용되는 시간입니다.

값: 최소 1 초

기본값: 15 초

QueryTimeout

쿼리가 취소되기 전까지 쿼리를 완료하는 데 허용되는 시간입니다.

값: 최소 1 초

기본값: 15 초

참고: Windows NT 에서 SQL Server 를 실행하는 경우 비동기 호출 지원으로 인해 약간의 메모리 누수가 발생할 수 있습니다. 네트워크 상태가 안정적이지 않은 경우 설정을 조정하여 만료 시간을 늘리고 장애 조치 횟수를 줄일 수 있습니다.

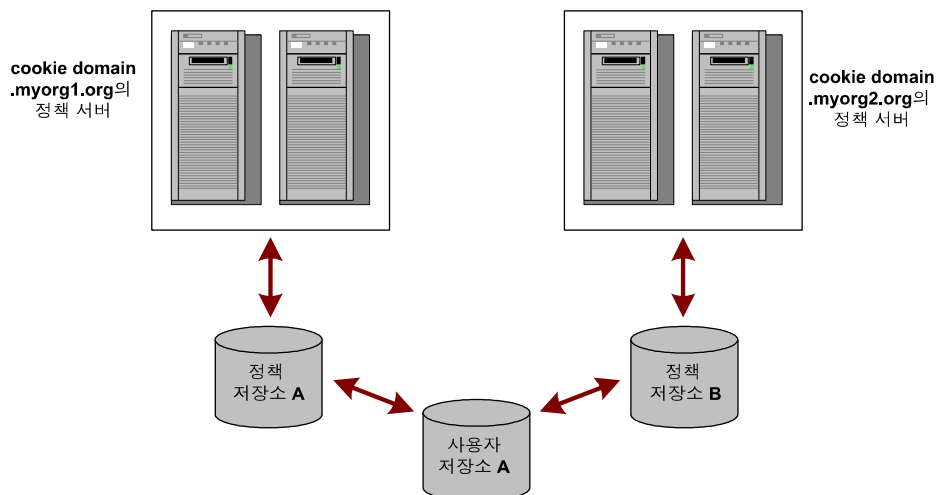
ODBC 연결 풀링

ODBC 연결 풀링에는 다음 조건이 적용됩니다.

- ODBC 데이터 원본이 연결을 풀링합니다. 여러 디렉터리가 데이터 원본을 사용하는 경우, 사용 가능한 연결 수는 디렉터리 및 저장소의 전체 수에 도달할 수 있습니다. 정책 저장소는 데이터 원본을 사용해야 하고, 정책 저장소의 또 다른 저장소는 데이터 원본을 사용해야 합니다.
- SQL Server 의 연결 공유 방식은 Oracle 의 경우보다 제한적입니다. 두 호출자는 열려 있는 결과 집합을 공유할 수 없습니다. 동시 작업은 제한되며, 특히 다중 프로세서 컴퓨터에서 제한됩니다. 연결 수를 늘리면 일반적으로 동시성이 개선됩니다.
- Oracle 에서는 여러 호출자가 하나의 연결을 공유하는 것이 허용되지만 내부적으로 호출이 직렬화될 수 있습니다.
- 연결을 공유되면 많은 활성 요청이 여러 개이면 풀에 있는 연결 간에 요청이 분산됩니다.
- 정책 서버가 중단되면 열려 있는 연결이 종료됩니다.

여러 정책 저장소에 동일한 사용자 디렉터리 연결 정의

모든 정책 서버는 정책 저장소에 연결합니다. 여러 정책 서버가 단일 정책 저장소를 가리키도록 구성할 수 있습니다. 추가 및 수정하는 개체는 정책 서버와 관련된 정책 저장소에 저장됩니다. 다음 그림과 같이 환경에는 정책 서버 데이터를 관리하기 위한 독립 정책 저장소가 여러 개 있을 수 있습니다.



myorg1의 정책 서버는 정책 저장소 A에 연결되어 있고 myorg2의 정책 서버는 정책 저장소 B에 연결되어 있습니다. 하지만 두 조직에는 모두 사용자 저장소 A의 데이터가 필요합니다.

다음 단계를 수행하십시오.

1. 배포 환경에 포함된 정책 저장소 중 하나와 연결된 관리 UI를 엽니다.
2. 사용자 디렉터리 연결을 구성합니다.
사용자 디렉터리 연결을 정의할 때 "이름" 필드에 제공한 값을 적어 두십시오.
3. 배포 환경에 포함된 다른 정책 저장소와 연결된 관리 UI를 엽니다.
4. 동일한 사용자 디렉터리 연결을 구성합니다.
사용자 디렉터리 연결을 정의할 때 2 단계에서 사용한 것과 동일한 이름을 사용하십시오.
5. 동일한 사용자 저장소에 액세스할 배포 환경의 모든 독립 정책 저장소에 대해 이 과정을 반복합니다.

각 독립 정책 저장소에 사용자 저장소에 대한 연결을 정의할 때 동일한 사용자 디렉터리 이름을 사용할 수 있습니다. 다양한 정책 저장소의 정책으로 보호된 리소스에 액세스하는 사용자에 대해 싱글 사인온을 사용할 수 있습니다.

추가 정보:

[CA Directory 사용자 디렉터리 연결을 구성하는 방법](#) (페이지 152)

사용자 디렉터리 콘텐츠 보기

관리 UI에서 사용자 디렉터리의 콘텐츠를 볼 수 있습니다.

다음 단계를 수행하십시오.

1. 기존 사용자 디렉터리 연결에 대한 "사용자 디렉터리" 대화 상자를 엽니다.

참고: 디렉터리 연결을 저장하기 전까지는 디렉터리의 콘텐츠를 볼 수 없습니다.

2. "콘텐츠 보기"를 클릭합니다.

참고: 기본 보기에는 그룹 목록이 표시됩니다. 개별 디렉터를 보려면 검색 기능을 사용하십시오.

사용자 디렉터리 검색

관리 UI에는 사용자 디렉터리 검색 기능이 있습니다. 사용자 디렉터리 검색 기능을 사용하면 검색 식이나 디렉터리 특성을 기준으로 사용자나 사용자 그룹을 볼 수 있습니다. 사용자 디렉터리 검색 기능은 사용자 디렉터리 유형에 따라 달라집니다.

참고: "정책 사용자/그룹" 창에서 사용자 디렉터리 검색 기능에 액세스할 수도 있습니다. 이 창은 정책에 사용자 및 그룹을 추가하거나 제거할 때 사용합니다. "정책 사용자/그룹" 창에는 아래에 설명된 대로 사용자 검색 기능에 액세스할 때 사용하는 것과 동일한 검색 아이콘이 있습니다.

다음 단계를 수행하십시오.

1. 검색할 디렉터리에 대한 "사용자 디렉터리" 창을 엽니다.
2. "콘텐츠 보기"를 클릭합니다.

"디렉터리 콘텐츠" 창이 열립니다. 이 창에 표시되는 콘텐츠는 보려고 하는 디렉터리의 유형에 따라 달라집니다.

3. 검색 조건을 입력하고 "실행"을 클릭합니다.

조건과 일치하는 결과가 열립니다.

유니버설 ID

UID(유니버설 ID)는 SiteMinder가 제어하는 모든 응용 프로그램에서 고객 식별자입니다. UID는 대개 사용자 로그인 이름과는 다릅니다.

UID 는 새 응용 프로그램과 레거시 응용 프로그램 사이의 빈 틈을 메우며, 하부 사용자 리포지토리의 변경을 방지할 수 있습니다. UDI 의 용도는 응용 프로그램의 수나 유형에 관계없이 이 ID 를 응용 프로그램에 전달하는 프로세스를 자동화하는 데 있습니다. 예를 들어 회사에 직원 ID 번호를 기준으로 사용자 정보를 조회하는 레거시 응용 프로그램이 있다고 가정합니다. 관리 UI 에서 사용자 디렉터리 연결을 구성할 경우 "사용자 디렉터리" 창의 "사용자 특성" 섹션에 UID 를 지정할 수 있습니다.

추가 정보:

[CA Directory 사용자 디렉터리 연결을 구성하는 방법](#) (페이지 152)

SiteMinder 에서 UID 가 사용되는 방식

UID 를 사용하여 사용자 디렉터리 연결을 구성한 경우 사용자가 SiteMinder 에 로그인하면 정책 서버는 사용자 디렉터리의 프로필에 있는 지정된 특성에서 UID 를 가져옵니다.

이 값은 세션 티켓(SESSIONSPEC)에 저장되었다가 요청하는 에이전트에 반환됩니다. 웹 에이전트는 이 값을 헤더 변수(HTTP_SM_UNIVERSALID)에 포함하여 웹 기반 응용 프로그램에 제공합니다. 이 값은 에이전트 API 를 사용하여 세션 티켓의 유효성을 검사하거나 권한 부여를 요청하도록 설계된 응용 프로그램 또는 개체로 전달될 수 있습니다. 어느 경우든 성공할 경우 UID 가 반환됩니다.

명명된 식

사용자 디렉터리에는 조직 정보, 사용자 및 그룹 특성, 개별 자격 증명 등의 사용자 특성이 저장됩니다. 일부 사용자 특성 값은 사용자 디렉터리에서 바로 읽을 수 있지만 다른 값은 필요할 때마다 계산되어야 합니다. 이러한 계산은 명명되거나 명명되지 않은 식으로 저장됩니다.

명명된 식은 이름으로 참조하는 정책 저장소 개체입니다. 이 식은 응용 프로그램 개체에 정의된 보안 정책에서 재사용할 수 있습니다. 명명되지 않은 식은 응답과 마찬가지로 도메인 개체에 저장됩니다. 이 식은 기존 보안 정책에서 사용하기 위한 규칙입니다.

참고: 명명된 식은 응용 프로그램 개체에서만 사용할 수 있습니다. 명명된 식은 응답 및 규칙과 같은 도메인 개체를 사용하여 정의된 기존 보안 정책에는 사용할 수 없습니다.

명명된 식과 명명되지 않은 식 모두는 계산된 사용자 특성의 값을 결정하는데 사용됩니다.

명명된 식을 생성하려면 관리자에게 적절한 권한이 있어야 합니다.

참고: 활성 식과 명명된 식은 동일하지 않습니다. 두 유형의 식은 모두 런타임에 평가되지만 다음과 같은 차이점이 있습니다.

- 활성 식은 부울 식인 반면, 명명된 식은 문자열, 숫자 또는 부울 값을 반환할 수 있습니다.
- 활성 식은 있는 그대로 참조되고 사용할 때마다 다시 입력해야 하는 반면, 명명된 식은 이름으로 참조되며 어느 위치에서나 참조되고 재사용될 수 있습니다.

명명된 식의 이점

명명된 식은 다음과 같은 이점이 있습니다.

- 명명된 식은 이름으로 참조되고 재사용될 수 있는 정책 저장소에 개체로 저장됩니다.
- 시스템 관리자는 명명된 식을 각각 한 번씩만 생성하면 됩니다. 도메인 관리자는 기본 식이 아니라 식 이름을 참조하여 사용자 정보를 가져옵니다. 따라서 관리자는 사용자 정보가 필요할 때마다 전체 식을 다시 입력할 필요가 없습니다.
- 시스템 관리자는 명명된 식을 한 곳에서 생성하고 관리합니다. 식을 변경해야 할 경우 관리자가 한 번만 변경하면 됩니다.
- 비즈니스 논리에 따라 식을 변경해야 할 경우 시스템 관리자가 식을 한 번만 변경하면 됩니다. 도메인 관리자는 기본 식의 변경 여부에 관계없이 계속해서 식 이름을 참조할 수 있습니다.
- 적절한 권한이 있는 관리자만 명명된 식을 생성할 수 있습니다. 명명된 식에서는 권한 있는 기본 제공 함수뿐 아니라 개인 식으로 표시된 식을 포함한 모든 명명된 식을 호출할 수 있습니다. 예를 들어 명명된 식에서는 현재 사용자를 그룹에 추가하는 개인 식을 호출할 수 있지만 명명되지 않은 식에서는 그럴 수 없습니다. 이 제한으로 인해 도메인 관리자는 현재 사용자를 관리 그룹에 추가하는 등의 방법으로 보안을 바이패스할 수 없습니다.

명명된 식 정의

명명된 식은 응용 프로그램 개체에 정의된 보안 정책에서 이름으로 참조되고 재사용될 수 있는 정책 저장소 개체입니다.

참고: 명명된 식은 응용 프로그램 개체에서만 사용할 수 있습니다. 명명된 식은 응답 및 규칙과 같은 도메인 개체를 사용하여 정의된 기존 보안 정책에는 사용할 수 없습니다.

SiteMinder는 명명된 식을 평가하여 계산된 사용자 특성의 값을 결정합니다.

명명된 식에는 다음 두 가지 유형이 있습니다.

- [가상 사용자 특성](#) (페이지 230)
- [사용자 클래스](#) (페이지 232)

가상 사용자 특성

가상 사용자 특성을 사용하면 재사용 가능한 식을 정의하여 사용자 정보를 계산할 수 있습니다. 이 유형의 식은 사용자 특성이 사용자 디렉터리에서 고유하게 참조되지 않는 경우에 사용됩니다. 이 경우 사용자 특성은 특성과 비즈니스 논리에 의해 설정된 다른 기준을 사용하여 계산되어야 합니다.

가상 사용자 특성은 다음 데이터 형식의 값을 반환하는 식을 명명합니다.

- 문자열
- 숫자
- 부울

가상 사용자 특성은 "파운드" 기호(#)로 시작합니다. "파운드" 기호는 이름이 사용자 특성 이름 및 매핑과 충돌하지 않도록 하며 해당 사용자 특성 값이 계산된다는 것을 시각적으로 알려 줍니다.

가상 사용자 특성 식에는 다음 항목이 포함될 수 있습니다.

- 사용자 특성(디렉터리별 특성 또는 매핑된 특성)
- 다른 명명된 식에 대한 참조
- 기본 제공 함수 및 식 구문

참고: 명명된 식은 응용 프로그램 개체에서만 사용할 수 있습니다. 명명된 식은 응답 및 규칙과 같은 도메인 개체를 사용하여 정의된 기존 보안 정책에는 사용할 수 없습니다.

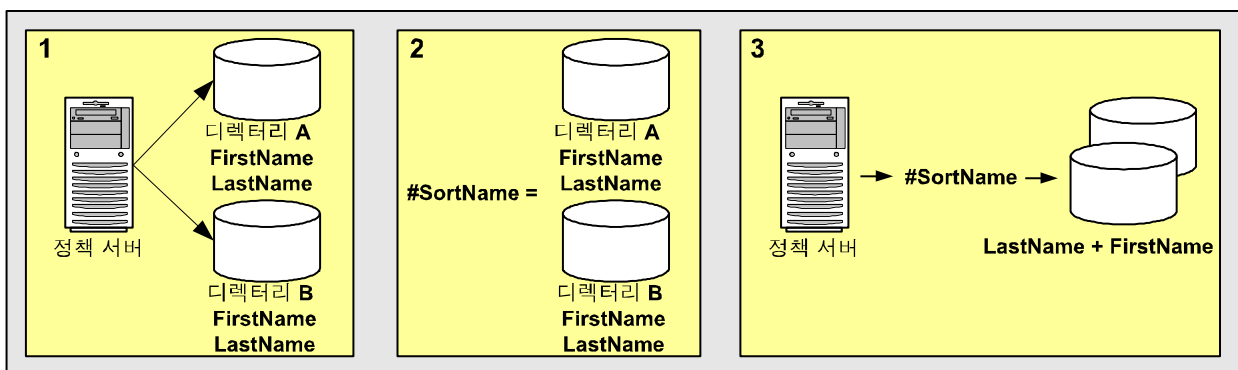
추가 정보:

[식 구문 개요](#) (페이지 866)

가상 사용자 특성 사용 사례

이 사용 사례에서는 두 개의 LDAP 사용자 디렉터리가 서로 다른 기본 스키마를 사용하여 사용자의 이름과 성을 식별하는 기본 시나리오를 보여줍니다.

다음 그림에서는 사용자 특성 매핑을 통해 서로 다른 사용자 디렉터리에 있는 사용자에 대해 가상 사용자 특성 **#SortName(LastName,FirstName)**이 계산되는 방식을 보여줍니다. 사용자 특성 매핑을 사용하면 하나의 일반 이름을 서로 다른 사용자 디렉터리에 있는 다양한 사용자 특성 이름에 매핑할 수 있습니다.



- 두 사용자 디렉터리에서는 사용자의 이름과 성이 서로 다르게 식별됩니다. 사용자 특성 매핑을 생성하여 이러한 정보의 공통 보기를 생성할 수 있습니다.
 - **FirstName** 은 디렉터리 A 와 디렉터리 B 에 있는 사용자의 이름을 식별하는 기본 디렉터리 스키마에 매핑됩니다.
 - **LastName** 은 디렉터리 A 와 디렉터리 B 에 있는 사용자의 성을 식별하는 기본 디렉터리 스키마에 매핑됩니다.
- #SortName** 은 다음 식을 사용하여 두 디렉터리 모두에 있는 사용자의 정렬 이름을 계산할 수 있는 가상 사용자 특성입니다.
(LastName + "," + FirstName)
- (LastName + "," + FirstName) 식을 반복해서 입력하는 대신 **#SortName** 이라는 가상 사용자 특성을 생성하고 이를 (FirstName + "," + LastName)으로 정의할 수 있습니다. 그런 다음 이 식이 필요할 때마다 **#SortName** 을 입력하면 됩니다.

가상 사용자 특성 정의

가상 사용자 특성을 정의하여 하나 이상의 사용자 디렉터리에서 고유하게 참조하지 않는 사용자 정보를 계산할 수 있습니다.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다.

다음 단계를 수행하십시오.

1. "정책", "식"을 차례로 클릭합니다.
2. "명명된 식"을 클릭합니다.
3. "명명된 식 만들기"를 클릭합니다.
4. 새 개체 만들기 옵션이 선택되어 있는지 확인하고 "확인"을 클릭합니다.

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

5. "가상 사용자 특성" 옵션을 선택하고 "일반" 영역에 식의 이름을 입력합니다.
6. "명명된 식 추가" 영역의 "식" 필드에 식을 입력합니다.
7. (선택 사항) "명명된 식 추가" 영역에서 "사용 안 함" 옵션을 선택하여 식을 비활성화합니다. 비활성화된 식은 식 편집기에 나열되지 않으며 다른 명명된 식이나 명명되지 않은 식이 이 식을 호출할 수 없습니다.
8. (선택 사항) "명명된 식 추가" 영역에서 "개인" 옵션을 선택합니다. 다른 명명된 식만 개인 식을 호출할 수 있습니다. 명명되지 않은 식은 개인 식을 호출할 수 없습니다.
9. (선택 사항) "명명된 식 추가" 영역에서 "편집"을 클릭하여 식 편집기를 엽니다.
10. 제출을 클릭합니다.

명명된 식이 생성됩니다.

사용자 클래스

사용자 클래스를 사용하면 재사용 가능한 식을 정의하여 사용자 정보를 계산할 수 있습니다. 이 유형의 식은 사용자 특성이 사용자 디렉터리에서 고유하게 참조되지 않는 경우에 사용됩니다. 이 경우 사용자 특성은 특성과 비즈니스 논리에 의해 설정된 다른 기준을 사용하여 계산되어야 합니다.

사용자 클래스는 사용자가 지정된 클래스의 구성원일 경우 **TRUE** 값을 반환하고 그렇지 않을 경우 **FALSE** 값을 반환하는 식을 명명합니다.

사용자 클래스는 "at" 기호(@)로 시작합니다. @ 기호는 이름이 사용자 특성 이름 및 매핑과 충돌하지 않도록 하며 해당 사용자 특성 값이 계산된다는 것을 시각적으로 알려 줍니다.

사용자 클래스 식에는 다음 항목이 포함될 수 있습니다.

- 사용자 특성(디렉터리별 특성 또는 매핑된 특성)
- 다른 명명된 식에 대한 참조
- SiteMinder 기본 제공 함수 및 식 구문

참고: 명명된 식은 응용 프로그램 개체에서만 사용할 수 있습니다. 명명된 식은 응답 및 규칙과 같은 도메인 개체를 사용하여 정의된 기존 보안 정책에는 사용할 수 없습니다.

사용자 클래스는 역할이 아닙니다. 역할은 EPM(Enterprise Policy Management)의 기능입니다. 역할에 사용자 클래스를 사용할 수는 있지만 역할에는 추가 정보가 연결됩니다. 역할에 대한 자세한 내용은 "EPM(Enterprise Policy Management)"을 참조하십시오.

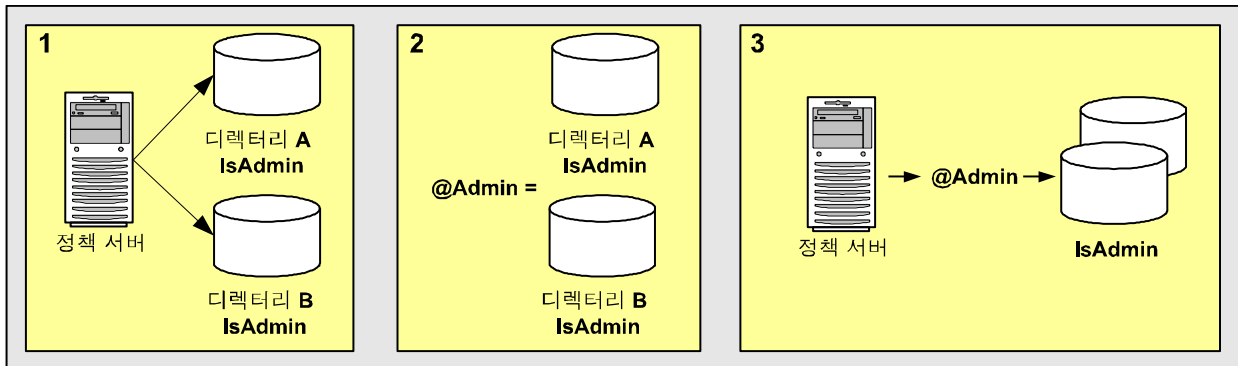
추가 정보:

[식 구문 개요](#) (페이지 866)

사용자 클래스 사용 사례

이 사용 사례에서는 두 개의 LDAP 사용자 디렉터리가 서로 다른 기본 스키마를 사용하여 관리자 그룹의 구성원을 식별하는 기본 시나리오를 보여 줍니다.

다음 그림에서는 사용자 특성 매핑을 통해 서로 다른 사용자 디렉터리에 있는 사용자에 대해 사용자 클래스 **@Admin** 이 계산되는 방식을 보여 줍니다. 사용자 특성 매핑을 사용하면 하나의 일반 이름을 서로 다른 사용자 디렉터리에 있는 다양한 사용자 특성 이름에 매핑할 수 있습니다.



- 두 사용자 디렉터리는 관리자 그룹의 구성원을 서로 다르게 식별합니다. 사용자 특성 매핑을 생성하여 이러한 정보의 공통 보기를 생성할 수 있습니다.
 - **IsAdmin** 은 디렉터리 A 의 관리자 그룹에 있는 구성원을 식별하는 기본 디렉터리 스키마에 매핑됩니다.
 - **IsAdmin** 은 디렉터리 B 의 관리자 그룹에 있는 구성원을 식별하는 기본 디렉터리 스키마에 매핑됩니다.
- @Admin** 은 SiteMinder 가 두 사용자 디렉터리의 사용자가 관리자인지 확인하기 위해 평가하는 사용자 클래스 유형의 명명된 식입니다.
(IsAdmin)
- (IsAdmin) 식을 반복해서 입력하는 대신 **@Admin** 이라는 사용자 클래스를 생성하고 이를 (IsAdmin)으로 정의할 수 있습니다. 그런 다음 이 식이 필요할 때마다 **@Admin** 을 입력하면 됩니다.

사용자 클래스 정의

사용자 클래스 특성을 정의하여 하나 이상의 사용자 디렉터리에서 고유하게 참조하지 않는 사용자 정보를 계산할 수 있습니다. 가능한 계산 결과는 TRUE 또는 FALSE 입니다. 결과는 사용자에게 적용되거나 적용되지 않습니다.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다.

다음 단계를 수행하십시오.

1. "정책", "식"을 차례로 클릭합니다.
2. "명명된 식"을 클릭합니다.
3. "명명된 식 만들기"를 클릭합니다.
4. "새 개체 만들기" 옵션이 선택되어 있는지 확인하고 "확인"을 클릭합니다.
5. "사용자 클래스" 옵션을 선택하고 "일반" 영역에서 식의 이름을 입력합니다.
6. "명명된 식 추가" 영역의 "식" 필드에 식을 입력합니다.

참고: 식은 부울 식이어야 합니다.

7. (선택 사항) "명명된 식 추가" 영역에서 "사용 안 함" 옵션을 선택하여 식을 비활성화합니다. 비활성화된 식은 식 편집기에 나열되지 않으며 다른 명명된 식이나 명명되지 않은 식이 이 식을 호출할 수 없습니다.
8. (선택 사항) "명명된 식 추가" 영역에서 "개인" 옵션을 선택합니다. 다른 명명된 식만 개인 식을 호출할 수 있습니다. 명명되지 않은 식은 개인 식을 호출할 수 없습니다.
9. (선택 사항) "명명된 식 추가" 영역에서 "편집"을 클릭하여 식 편집기를 엽니다.
10. 제출을 클릭합니다.
명명된 식이 생성됩니다.

식 편집기 사용 방법

식 편집기를 사용하여 다음과 같은 작업을 수행할 수 있습니다.

- 함수, 연산자 및 사용자 정의 명명된 식 조회
- 부울 식 작성

참고: 식을 직접 입력하려는 경우 "취소"를 클릭하고 "Create Expression: Name(식 만들기: 이름) 창으로 돌아가 "명명된 식 추가" 그룹 상자의 "식" 필드에 식을 입력할 수 있습니다.

식 편집기에서 부울 식을 작성하는 과정은 2 단계로 이루어집니다. 단계를 순서에 관계없이 반복할 수도 있습니다.

1. 조건 만들기
2. 식 편집

부울 식 작성 과정의 1 단계에서는 조건을 생성하여 "중위 표기법" 그룹 상자에 추가합니다. 조건은 함수 또는 연산 하나로 구성된 간단한 부울 식입니다. 편집기에서는 다음과 같은 형식으로 함수에 최대 세 개의 매개 변수를 사용할 수 있습니다.

```
FUNCTION_NAME(parameter_1[, parameter_2][, parameter_3])
```

연산에는 피연산자 두 개가 필요하며 형식은 다음과 같습니다.

```
left_operand operator right_operand
```

조건은 부울 식이므로 부울 값을 반환합니다. 조건에 문자열을 반환하는 함수나 연산이 포함된 경우에는 결과가 부울 값으로 변환됩니다. 다시 말해, "TRUE", "true", "YES" 및 "yes"는 TRUE 로 변환됩니다. 다른 모든 문자열 값은 FALSE 로 변환됩니다.

마찬가지로, 조건에 숫자를 반환하는 함수나 연산이 포함된 경우에도 결과가 부울 값으로 변환됩니다. 0 이 아닌 모든 숫자는 TRUE 로 변환되고 0 은 FALSE 로 변환됩니다.

각 조건은 다음과 같이 "중위 표기법" 그룹 상자의 필드에 한 줄에 하나씩 표시되고 부울 연산자 한 개 또는 두 개를 사용하여 위의 줄에 있는 조건에 연결됩니다.

```
condition_1  
AND | OR | XOR [NOT] condition_2
```


부울 식 작성 과정의 2 단계에서는 "중위 표기법" 그룹 상자의 필드에서 조건을 수정 및 삭제하고, 조건을 그룹화하는 괄호를 변경하고, 조건을 연결하는 부울 연산자를 변경하여 식을 편집할 수 있습니다. 예를 들어 다음과 같이 조건이 그룹화되는 방식을 변경할 수 있습니다.

```
(condition_1
AND condition_2)
OR NOT condition_3
```

위 조건을 다음과 같이 변경할 수 있습니다.

```
condition_1
AND (condition_2
OR NOT condition_3)
```

함수를 포함하는 조건 만들기

식 편집기에서 기본 제공 SiteMinder 함수를 포함하는 조건을 생성하여 식에 추가할 수 있습니다.

기본 제공 SiteMinder 함수를 포함하는 조건을 생성하려면

1. "식 편집기" 창의 "조건" 그룹 상자에 있는 함수 드롭다운 목록에서 이름을 선택하거나 "함수" 필드에 이름을 입력합니다.
2. "명명된 식"을 클릭하거나 "조건" 그룹 상자의 "첫 번째 매개 변수" 필드에 직접 입력하는 방법으로 첫 번째 매개 변수를 지정합니다.
참고: "명명된 식"을 클릭하면 "변수 조회" 그룹 상자가 열립니다.
3. (선택 사항) "명명된 식"을 클릭하거나 "조건" 그룹 상자의 "두 번째 매개 변수" 필드에 직접 입력하는 방법으로 두 번째 매개 변수를 지정합니다.
참고: "명명된 식"을 클릭하면 "변수 조회" 그룹 상자가 열립니다.
4. (선택 사항) 드롭다운 목록에서 "TRUE" 또는 "FALSE"를 선택하거나 "조건" 그룹 상자의 "마지막 매개 변수" 필드에 직접 입력하는 방법으로 마지막 매개 변수를 지정합니다.
5. "추가"를 클릭합니다.

지정한 함수가 "중위 표기법" 및 "결과 표기법" 그룹 상자에 추가됩니다.

연산을 포함하는 조건 만들기

식 편집기에서 기본 제공 SiteMinder 연산을 포함하는 조건을 생성하여 식에 추가할 수 있습니다.

다음 단계를 수행하십시오.

1. "식 편집기" 창의 "조건" 그룹 상자에 있는 드롭다운 목록에서 연산자 유형과 연산자를 선택합니다.
2. "명명된 식"을 클릭하거나 "조건" 그룹 상자의 "Left Operand"(왼쪽 피연산자) 필드에 직접 입력하는 방법으로 왼쪽 피연산자를 지정합니다.
3. "명명된 식"을 클릭하거나 "조건" 그룹 상자의 "Right Operand"(오른쪽 피연산자) 필드에 직접 입력하는 방법으로 오른쪽 피연산자를 지정합니다.
4. "추가"를 클릭합니다.

지정한 연산이 "중위 표기법" 및 "결과 표기법" 그룹 상자에 추가됩니다.

식을 편집하는 방법

식 편집기에서 생성하는 각 조건은 "중위 표기법" 그룹 상자의 필드에 한 줄에 하나씩 표시됩니다. 식을 작성할 때 "중위 표기법" 그룹 상자의 단추를 사용하여 조건을 그룹화하는 괄호와 조건을 연결하는 부울 연산자를 변경할 수 있습니다.

식을 편집하는 과정은 3 단계로 이루어집니다. 첫 번째 단계에는 네 개의 옵션이 포함되며 이러한 옵션을 순서에 관계없이 반복할 수 있습니다.

1. 옵션을 선택합니다.
 - [식에 포함된 조건 수정](#) (페이지 239)
 - [식에서 조건 삭제](#) (페이지 239)
 - [식에 포함된 조건 그룹화](#) (페이지 239)
 - [식에 포함된 부울 연산자 변경](#) (페이지 241)
2. (선택 사항) 1 단계를 반복합니다.
3. "확인"을 클릭하여 식 편집기를 닫습니다.

식에 포함된 조건 수정

식 편집기에서 "중위 표기법" 그룹 상자의 "수정" 단추를 클릭하여 식에 포함된 조건을 수정할 수 있습니다.

식에 포함된 조건을 수정하려면

1. 조건을 클릭하여 선택합니다.
2. "수정"을 클릭합니다.

"편집" 그룹 상자가 열리고 그룹 상자에 조건이 표시됩니다.

식에서 조건 삭제

식 편집기에서 "중위 표기법" 그룹 상자의 "제거" 단추를 클릭하여 식에서 조건을 하나 이상 삭제할 수 있습니다.

식에서 조건을 삭제하려면

1. 조건을 클릭하여 선택합니다.

참고: 인접한 조건을 여러 개 선택하려면 Shift 키를 누른 채 조건을 클릭하십시오.

2. "제거"를 클릭합니다.

선택한 조건이 식에서 제거됩니다.

참고: 조건을 여러 개 선택한 경우 "제거"를 클릭하면 조건이 한 번에 하나씩 삭제됩니다.

식에 포함된 조건 그룹화

식 편집기의 "중위 표기법" 그룹 상자에서 괄호를 추가하고 제거하는 단추를 클릭하여 식에 포함된 조건 그룹을 변경할 수 있습니다.

식에 포함된 조건 그룹을 변경하려면

1. 인접한 조건을 둘 이상 클릭하여 선택합니다.

참고: 인접한 조건을 여러 개 선택하려면 Shift 키를 누른 채 조건을 클릭하십시오.

2. 다음 두 단추 중 하나를 클릭합니다.

()

선택한 조건의 외부에 괄호를 추가합니다.

예:

condition_1

AND condition_2

위 조건이 다음과 같이 변경됩니다.

(condition_1

AND condition_2)

() 제거

선택한 조건의 외부에서 괄호를 삭제합니다.

예:

(condition_1

OR condition_2

OR condition_3)

위 조건이 다음과 같이 변경됩니다.

condition_1

OR condition_2

OR condition_3

편집한 식이 식 편집기의 "결과 표기법" 및 "중위 표기법" 그룹 상자에 있는 필드에 표시됩니다.

식에 포함된 부울 연산자 변경

식 편집기의 "중위 표기법" 그룹 상자에서 다음 단추 중 하나를 클릭하여 식에 포함된 부울 연산자를 변경할 수 있습니다.

- And/Or
- Not
- XOR
- 조건부?예:아니요

다음 단계를 수행하십시오.

1. 조건 또는 조건 그룹을 하나 클릭하여 선택합니다.

참고: 인접한 조건을 여러 개 선택하려면 **Shift** 키를 누른 채 조건을 클릭하십시오.

2. 다음 단추 중 하나를 클릭합니다.

And/Or

부울 연산자 AND 와 OR 사이에서 전환합니다.

예:

AND condition_1

위 조건이 다음과 같이 변경됩니다.

OR condition_1

참고: AND/OR 단추를 사용할 경우 XOR 는 AND 로 전환됩니다.

Not

부울 연산자 NOT 의 추가 동작과 제거 동작 사이에서 전환합니다.

예:

AND condition_1

위 조건이 다음과 같이 변경됩니다.

AND NOT condition_1

XOR

부울 연산자 AND 와 OR 를 XOR 로 전환합니다.

예:

AND condition_1

위 조건이 다음과 같이 변경됩니다.

XOR condition_1

참고: 배타적 OR(XOR) 연산자는 부울 피연산자를 두 개 사용하며, 두 피연산자 중 하나만 TRUE 일 경우에 TRUE 를 반환합니다.

조건부?예:아니요

조건부 결정 연산자를 추가합니다.

예:

condition_1

위 조건이 다음과 같이 변경됩니다.

condition_1 ? "YES" : "NO"

편집한 식이 식 편집기의 "결과 표기법" 및 "중위 표기법" 그룹 상자에 있는 필드에 표시됩니다.

명명된 식 적용

이 사용 사례의 시나리오에서는 한 소매 의류업체가 신용 한도에 도달하거나 이를 초과한 고객에 대해 웹에서 신용 구매를 할 수 없도록 하는 역할을 정의하려고 한다고 가정합니다. 회사 정책에 고객의 신용 한도는 1,000 달러로, 직원의 신용 한도는 2,000 달러로 명시되어 있습니다.

이 사용 사례의 환경에는 사용자 디렉터리가 두 개 있습니다.

- 디렉터리 A 에는 직원이 저장됩니다. 직원은 고객이 될 수도 있습니다. 따라서 디렉터리 A 는 직원이면서 동시에 `cn=Customers,ou=Groups,o=acme.com` 의 구성원인 고객을 식별합니다.
- 디렉터리 B 에는 고객만 저장됩니다. 모든 사용자가 고객이 되므로 디렉터리 B 에는 고객을 식별하는 사용자 특성이 없습니다.

다음 절차에서는 특성 매핑, 가상 사용자 특성 및 사용자 클래스를 사용하여 회사의 신용 정책을 충족하는 방법을 자세히 설명합니다.

1. 각 사용자 디렉터리에 대해 사용자 특성 매핑을 생성하고 고객을 식별하는 유니버설 스키마 또는 일반 이름을 생성합니다.
 - a. 디렉터리 A(직원)에 대해 *그룹 이름* 특성 매핑을 생성합니다.
 - 매핑의 이름을 **IsCustomer** 로 지정합니다.
 - IsCustomer 를 **cn=Customers,ou=Groups,o=acme.com** 으로 정의합니다.
 - b. 디렉터리 B(고객)에 대해 *상수* 특성 매핑을 생성합니다.
 - 매핑의 이름을 **IsCustomer** 로 지정합니다.
 - IsCustomer 를 **TRUE** 로 정의합니다.

참고: IsCustomer 는 디렉터리 A 와 B 의 동일한 사용자 정보에 매핑되는 일반 이름입니다. 이 정보에 액세스하려면 식에 IsCustomer 를 사용하면 됩니다.
2. 각 사용자 디렉터리에 대해 *상수* 특성 매핑을 생성하고 회사의 신용 한도를 식별하는 유니버설 스키마 또는 일반 이름을 생성합니다.
 - a. 디렉터리 A(직원)에 대해 *상수* 특성 매핑을 생성합니다.
 - 매핑의 이름을 **CreditLimit** 로 지정합니다.
 - CreditLimit 를 **2000** 으로 정의합니다.
 - b. 디렉터리 B(고객)에 대해 *상수* 특성 매핑을 생성합니다.
 - 매핑의 이름을 **CreditLimit** 로 지정합니다.
 - CreditLimit 를 **1000** 으로 정의합니다.

참고: CreditLimit 는 디렉터리 A 와 B 의 동일한 사용자 정보에 매핑되는 일반 이름입니다. 이 정보에 액세스하려면 식에 CreditLimit 를 사용하면 됩니다.
3. **#CreditBalance** 는 계정 데이터베이스에서 사용자의 신용 잔액을 가져오는 가상 사용자 특성이라고 가정합니다.
4. 고객의 신용 잔액이 신용 한도 미만인 경우 **TRUE** 값을 반환하는 사용자 클래스를 생성합니다.
 - 사용자 클래스의 이름을 **@IsUnderCreditLimit** 로 지정합니다.
 - @IsUnderCreditLimit 를 다음과 같이 정의합니다.
(IsCustomer AND (#CreditBalance < CreditLimit))

참고: 이 식은 SiteMinder 식 구문 규칙을 따릅니다.

5. 고객의 신용 잔액이 신용 한도 미만인 경우 웹 기반 구매를 할 수 있도록 하는 EPM 역할을 생성합니다.
 - 역할의 이름을 **PurchaseWithCredit** 로 지정합니다.
 - 역할을 **@IsUnderCreditLimit** 로 정의합니다.

사용자 특성 매핑

정책 서버에서 사용자 디렉터리로의 연결을 구성할 때 다음과 같은 7 개의 기본 제공 특성을 디렉터리별 사용자 특성 이름에 매핑할 수 있습니다.

- 유니버설 ID
- 비활성화된 플래그
- 암호 특성
- 암호 데이터
- 익명 ID
- 전자 메일
- 챌린지/응답

사용자 특성 매핑을 사용하면 **SiteMinder** 에 일반 이름을 정의하고 각 이름을 사용자 특성 이름에 매핑할 수 있습니다. 특성 이름은 다른 기본 스키마를 사용하는 여러 사용자 디렉터리에 있을 수 있습니다.

사용자 특성 매핑 개요

사용자 특성 매핑의 5 개 유형은 다음과 같습니다.

- 별칭
- 그룹 이름
- 마스크
- 상수
- 식

명명된 식의 유형은 다음과 같습니다.

- 가상 사용자 특성
- 사용자 클래스

사용자 특성 매핑은 명명된 식과 유사하지만 다음과 같은 차이점이 있습니다.

- 액세스
 - 사용자 특성 매핑의 일부 유형은 읽기 전용(R)이며 사용자 특성 값에 매핑됩니다. 이러한 특성은 변경되지 않습니다. 사용자 특성 매핑의 다른 유형은 읽기/쓰기(RW)이며 사용자 특성 값에 매핑됩니다. 이러한 특성은 수정할 수 있습니다.
 - 명명된 식은 모두 읽기 전용(R)입니다.
- 데이터 형식
 - 사용자 특성 매핑은 지정된 데이터 형식의 사용자 특성에 매핑됩니다.
 - 명명된 식은 실행 시 지정된 데이터 형식으로 값을 반환합니다.
- 가시성
 - 사용자 특성 매핑은 전역 설정이 아니므로 매핑을 적용할 각 사용자 디렉터리에 대해 정의해야 합니다.
 - 명명된 식은 전역 설정이므로 모든 사용자 디렉터리의 모든 사용자에게 적용될 수 있습니다.

- 접두사
 - 사용자 특성 매핑은 사용자 특성 이름과 동일한 구문 규칙을 따릅니다.
 - 명명된 식은 사용자 특성 이름과 동일한 구문 규칙을 따르되 접두사를 사용합니다.
 - 가상 사용자 특성은 "파운드" 기호(#)로 시작해야 합니다.
 - 사용자 클래스는 "at" 기호(@)로 시작해야 합니다.

다음 표에는 이러한 차이점이 요약되어 있습니다.

사용자 특성 매핑 유형	데이터 형식	가시성	접두사
별칭(RW)	문자열, 숫자, 부울	디렉터리별	없음
그룹 이름(RW)	부울	디렉터리별	없음
마스크(RW)	부울	디렉터리별	없음
상수(R)	문자열, 숫자, 부울	디렉터리별	없음
식(R)	문자열, 숫자, 부울	디렉터리별	없음

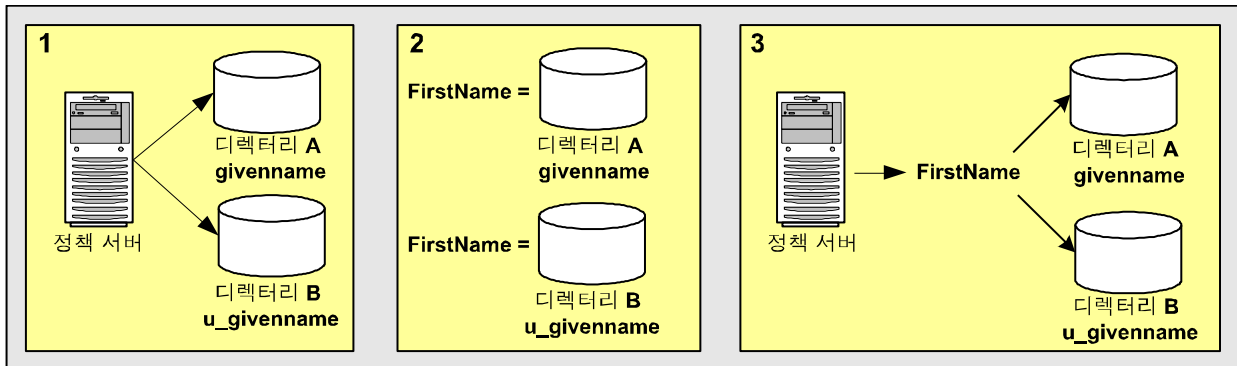
명명된 식 유형	데이터 형식	가시성	접두사
가상 사용자 특성(R)	문자열, 숫자, 부울	전역	#
사용자 클래스(R)	부울	전역	@

특성 매핑의 작동 방식

사용자 특성 매핑의 목적은 유니버설 스키마를 정의하여 동일한 사용자 정보의 공통 보기를 생성하는 데 있습니다. 이 유니버설 스키마는 여러 사용자 디렉터리에서 사용자 정보를 확인합니다. 사용자 특성을 식별하는 기본 디렉터리 스키마에 *일반 이름*을 매핑하여 사용자 특성 매핑을 정의할 수 있습니다. 사용 환경에 포함된 각 사용자 디렉터리의 기본 스키마에 동일한 일반 이름을 매핑하면 사용자 특성에 대한 유니버설 스키마가 생성됩니다.

이러한 보기를 만들면 디렉터리 유형에 관계없이 사용자 특성을 참조합니다. 여러 사용자 디렉터리를 고려하여 구성되어야 하는 정책 또는 다른 개체의 수를 크게 줄일 수 있습니다. 각 사용자 특성 매핑은 해당 사용자 특성 매핑이 정의된 사용자 디렉터리에 대해 적용됩니다.

다음 그림은 사용자 특성 매핑의 기본 개념을 보여 줍니다.



1. 두 사용자 디렉터리에서 사용자의 이름은 서로 다르게 식별됩니다.
 - 디렉터리 A 는 **givenname** 을 사용하여 사용자의 이름을 식별합니다.
 - 디렉터리 B 는 **u_givenname** 을 사용하여 사용자의 이름을 식별합니다.

이 구성을 사용하면 동일한 사용자 정보가 서로 다른 방식으로 표현되고 표시됩니다.
2. **FirstName** 은 기본 디렉터리 스키마에 매핑된 일반 이름입니다.
 - 디렉터리 A 에서는 **FirstName** 이 **givenname** 에 매핑됩니다.
 - 디렉터리 B 에서는 **FirstName** 이 **u_givenname** 에 매핑됩니다.
3. **FirstName** 를 사용하면 동일한 사용자 정보의 공통 보기가 생성됩니다. 디렉터리별 스키마에 관계없이 사용자의 이름을 사용해야 하는 정책, 식 또는 기타 개체를 정의할 때 **FirstName** 을 참조할 수 있습니다. 디렉터리는 기능적으로 동일합니다.

특성 매핑 정의

다음과 같은 특성 매핑 유형 중 하나 이상을 사용할 수 있습니다.

- [별칭](#) (페이지 248)
- [그룹 이름](#) (페이지 250)
- [마스크](#) (페이지 253)
- [상수](#) (페이지 258)
- [식](#) (페이지 261)

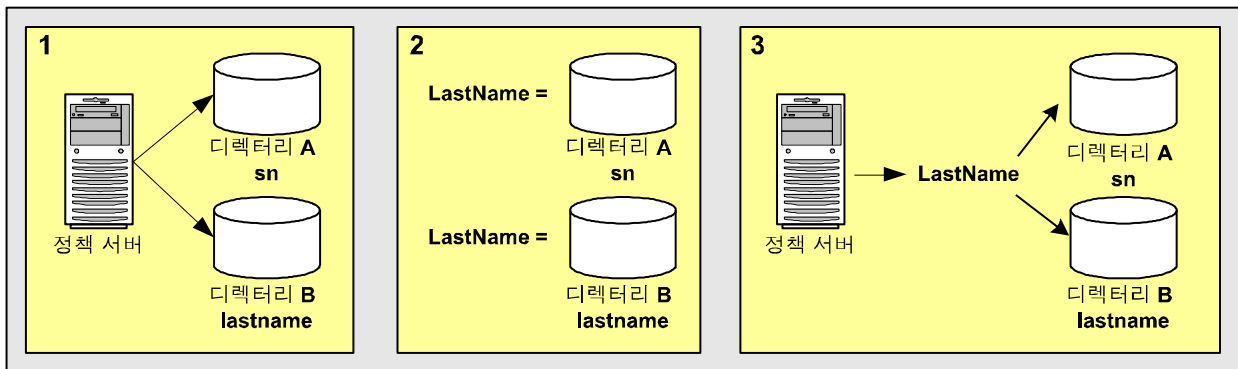
별칭

별칭 특성 매핑은 읽거나 변경할 수 있는 사용자 특성 값에 일반 이름을 매핑합니다. 이러한 유형의 액세스를 읽기/쓰기(RW)라고 합니다. **별칭** 특성 매핑은 다음과 같은 데이터 형식의 사용자 특성에 매핑할 수 있습니다.

- 문자열
- 숫자
- 부울

별칭 특성 사용 사례

이 사용 사례에서는 사용자의 성을 식별하지만 각각 기본 스키마가 서로 다른 두 LDAP 사용자 디렉터리를 보여 줍니다. 다음 그림에서는 별칭 특성 매핑을 두 개 사용하여 동일한 사용자 정보의 공통 보기를 생성하는 방법을 보여 줍니다.



1. 두 사용자 디렉터리에서 사용자의 성은 서로 다르게 식별됩니다.
 - 디렉터리 A 는 sn 을 사용하여 사용자의 성을 식별합니다.
 - 디렉터리 B 는 lastname 을 사용하여 사용자의 성을 식별합니다.
 이 구성을 사용하면 동일한 사용자 정보가 서로 다른 방식으로 표시됩니다.
2. LastName 은 기본 디렉터리 스키마에 매핑된 일반 이름 또는 별칭입니다.
 - 디렉터리 A 에서는 LastName 이 sn 에 매핑됩니다.
 - 디렉터리 B 에서는 LastName 이 lastname 에 매핑됩니다.

LastName 를 사용하면 동일한 사용자 정보의 공통 보기가 생성됩니다. LastName 은 성을 사용해야 하는 정책, 식 또는 기타 개체를 정의할 때 사용합니다.

별칭 특성 매핑 만들기

사용자 디렉터리의 기본 스키마에 지정된 사용자 특성 이름에 일반 이름 또는 별칭을 매핑할 수 있습니다. 사용자 특성 매핑은 디렉터리별로 적용됩니다.

다음 단계를 수행하십시오.

1. "사용자 디렉터리: *이름*" 창으로 이동합니다.
2. "특성 매핑 목록" 그룹 상자에서 "만들기"를 클릭합니다.
"특성 매핑 만들기" 창이 열립니다.
3. "Create a new object"(새 개체 만들기)가 선택되어 있는지 확인하고 "확인"을 클릭합니다.
"특성 매핑 만들기: *이름*" 창이 열립니다.
4. "일반" 그룹 상자의 필드에 특성 매핑의 일반 이름과 설명을 입력합니다.
참고: 일반 이름은 사용자 특성 이름과 동일한 규칙을 따라야 합니다.
5. "속성" 그룹 상자에서 "별칭"을 선택합니다.

6. "속성" 그룹 상자의 "정의" 상자에 정의를 입력합니다.

예:

이름: `FirstName`

정의: `givenname`

설명: 일반 이름 `FirstName` 은 사용자 특성 이름 `givenname` 에 매핑됩니다.

7. (선택 사항) "사용 안 함"을 선택하여 이 특성 매핑이 사용되지 않도록 설정합니다.
8. "확인"을 클릭합니다.
처리를 위해 "특성 매핑 만들기" 태스크가 제출되고 "특성 매핑 목록" 그룹 상자의 목록에 새 특성 매핑이 추가됩니다.

그룹 이름

그룹 이름 특성을 사용하여 사용자가 특정 그룹에 속해 있는지 여부를 식별하는 기본 디렉터리 스키마에 일반 이름을 매핑할 수 있습니다. 그룹 이름 특성 매핑은 읽거나 변경할 수 있는 사용자 특성에 일반 이름을 매핑합니다.

그룹 이름 특성 매핑의 결과는 부울 값입니다. 사용자가 지정된 그룹의 구성원인 경우 매핑 결과는 `TRUE` 값입니다. 그렇지 않은 경우 매핑 결과는 `FALSE` 입니다.

그룹 이름 특성 매핑과 명명된 식의 한 유형인 사용자 클래스는 다음과 같은 유사점이 있습니다.

- 둘 모두 그룹 구성원 자격을 확인하는 데 사용됩니다.
- 둘 모두 부울 값을 반환합니다.

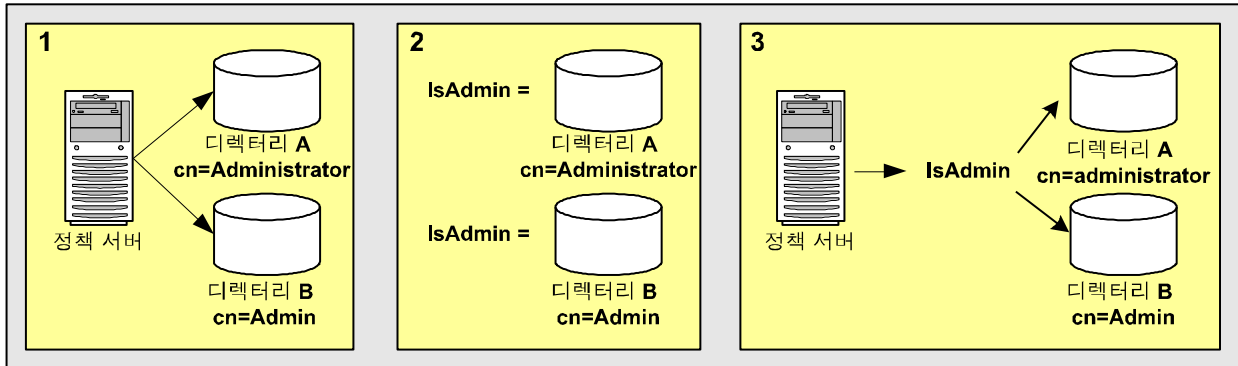
그룹 이름 특성 매핑과 사용자 클래스에는 다음과 같은 차이점이 있습니다.

- 그룹 이름 특성 매핑은 특정 사용자 디렉터리에 대해 정의됩니다. 사용자 클래스는 전역 설정이므로 모든 사용자 디렉터리의 모든 사용자에게 적용될 수 있습니다.
- 그룹 이름 특성 매핑은 사용자 디렉터리에 있는 그룹의 구성원 자격을 변경할 수 있습니다. 사용자 클래스는 부울 식으로, 변경할 수 없습니다.
- 사용자 클래스는 "at" 기호(@)로 시작해야 합니다. 그룹 이름 매핑은 "at" 기호로 시작되지 않습니다.

그룹 이름 사용 사례

이 사용 사례에서는 관리자 그룹에 속한 사용자를 식별하는 데 서로 다른 기본 스키마를 사용하는 두 개의 LDAP 사용자 디렉터리를 보여 줍니다.

다음 그림에서는 그룹 이름 특성 매핑을 두 개 사용하여 동일한 사용자 정보의 공통 보기를 생성하는 방법을 보여 줍니다.



1. 두 사용자 디렉터리는 관리자 그룹의 구성원을 서로 다르게 식별합니다.

- 디렉터리 A 는 관리자 그룹의 구성원을
cn=Administrators,ou=groups,o=acme.com 으로 식별합니다.
- 디렉터리 B 는 관리자 그룹의 구성원을
cn=Admin,ou=groups,o=acme.com 으로 식별합니다.

이 구성을 사용하면 동일한 사용자 정보가 서로 다른 방식으로 표시됩니다.

2. IsAdmin 은 기본 디렉터리 스키마에 매핑된 일반 이름입니다.

- 디렉터리 A 에서는 IsAdmin 이
cn=Administrators,ou=groups,o=acme.com 에 매핑됩니다.
- 디렉터리 B 에서는 IsAdmin 이 cn=Admin,ou=groups,o=acme.com 에 매핑됩니다.

따라서 IsAdmin 을 사용하면 관리자 그룹의 공통 보기가 생성됩니다. 관리자 그룹에 적용되는 정책, 식 또는 기타 개체를 정의할 때 IsAdmin 을 참조할 수 있습니다.

그룹 이름 특성 매핑 만들기

그룹 이름 특성을 정의하여 사용자가 특정 그룹에 속해 있는지 여부를 식별하는 기본 디렉터리 스키마에 일반 이름을 매핑할 수 있습니다. 그룹 이름 특성 매핑의 결과는 부울 값입니다. 그룹 이름 특성 매핑을 사용하여 사용자 디렉터리의 사용자 그룹 이름을 읽거나 변경할 수 있습니다. 사용자 특성 매핑은 디렉터리별로 적용됩니다.

다음 단계를 수행하십시오.

1. "사용자 디렉터리: *이름*" 창으로 이동합니다.
2. "특성 매핑 목록" 그룹 상자에서 "만들기"를 클릭합니다.
"특성 매핑 만들기" 창이 열립니다.
3. "Create a new object"(새 개체 만들기)가 선택되어 있는지 확인하고 "확인"을 클릭합니다.
"특성 매핑 만들기: *이름*" 창이 열립니다.
4. "일반" 그룹 상자의 필드에 특성 매핑의 일반 이름과 설명을 입력합니다.

참고: 일반 이름은 사용자 특성 이름과 동일한 규칙을 따라야 합니다.

5. "속성" 그룹 상자에서 "그룹"을 선택합니다.
6. "속성" 그룹 상자의 "정의" 상자에 정의를 입력합니다.

예:

이름: IsAdmin

정의: cn=administrators,ou=groups,o=acme.com

설명: 일반 이름 IsAdmin 은 그룹 이름

cn=administrators,ou=groups,o=acme.com 에 매핑됩니다. 사용자가

cn=administrators,ou=groups,o=acme.com 의 구성원인 경우

IsAdmin 은 TRUE 입니다.

7. (선택 사항) "사용 안 함"을 선택하여 이 특성 매핑이 사용되지 않도록 설정합니다.
8. "확인"을 클릭합니다.

"특성 매핑 만들기" 태스크가 처리를 위해 제출됩니다. 새 특성 매핑은 "특성 매핑 목록" 그룹 상자의 목록에 나타납니다.

마스크

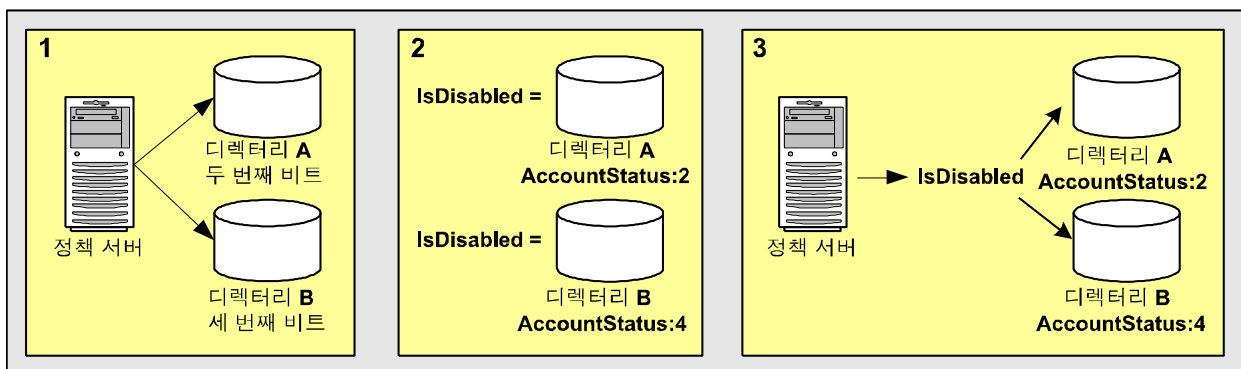
마스크 특성 매핑을 사용하면 비트 패턴을 저장하는 사용자 특성을 식별하는 데 사용되는 이름에 일반 이름을 매핑할 수 있습니다. 마스크 특성은 읽거나 변경할 수 있는 사용자 특성에 일반 이름을 매핑합니다. 마스크 특성 매핑의 결과는 부울 값입니다. 사용자 디렉터리의 비트 패턴이 지정된 마스크와 일치할 경우 매핑 결과는 TRUE 값입니다. 그렇지 않은 경우 매핑 결과는 FALSE 입니다.

마스크 사용 사례

일부 디렉터리 구현에서는 특성의 개별 비트를 사용하여 계정 상태와 같은 특성 관련 정보를 제공합니다. 특성에 비트 마스크를 적용할 수 있습니다.

이 사용 사례에서는 비활성화된 사용자 계정을 식별하는 두 개의 Active Directory 사용자 저장소를 보여 줍니다. 각 계정에는 서로 다른 기본 스키마가 있습니다.

다음 그림에서는 마스크 특성 매핑을 두 개 사용하여 동일한 사용자 정보의 공통 보기를 생성하는 방법을 보여 줍니다.



1. 두 사용자 디렉터리에는 **AccountStatus** 라는 사용자 특성이 포함되어 있습니다. **AccountStatus** 는 사용자 정보를 각 비트가 플래그인 비트 패턴으로 저장합니다.

- 디렉터리 A에서는 두 번째 비트가 비활성화된 계정에 플래그를 설정합니다. 두 번째 비트가 1 인 경우 해당 계정은 비활성화된 것입니다.
- 디렉터리 B에서는 세 번째 비트가 비활성화된 계정에 플래그를 설정합니다. 세 번째 비트가 1 인 경우 해당 계정은 비활성화된 것입니다.

이 구성을 사용하면 동일한 사용자 정보가 서로 다른 방식으로 표시됩니다.

2. **IsDisabled** 는 기본 디렉터리 스키마에 매핑된 일반 이름입니다. 두 디렉터리 모두에서 **IsDisabled** 는 **AccountStatus** 에 매핑됩니다.

- 디렉터리 A에서는 비트 마스크 2(10 진수)가 **AccountStatus** 의 두 번째 비트가 설정되어 있고 계정이 비활성화되었는지 여부를 확인합니다.
- 디렉터리 B에서는 비트 마스크 4(10 진수)가 **AccountStatus** 의 세 번째 비트가 설정되어 있고 계정이 비활성화되었는지 여부를 확인합니다.

IsDisabled 를 사용하면 비활성화된 사용자 계정의 공통 보기가 생성됩니다. 사용자의 계정 상태가 필요한 정책, 식 또는 기타 개체를 정의할 때 **IsDisabled** 를 참조할 수 있습니다.

마스크 특성 매핑 만들기

사용자 디렉터리의 기본 스키마에 지정된 사용자 특성 이름에 해당하는 비트 패턴에 일반 이름을 매핑할 수 있습니다. 마스크 특성 매핑의 결과는 부울 값입니다. 마스크 매핑을 사용하여 사용자 디렉터리의 사용자 특성 값을 읽거나 변경할 수 있습니다. 사용자 특성 매핑은 디렉터리별로 적용됩니다.

마스크 유형의 사용자 특성 매핑을 생성하려면

1. "사용자 디렉터리: 이름" 창으로 이동합니다.
2. "특성 매핑 목록" 그룹 상자에서 "만들기"를 클릭합니다.
"특성 매핑 만들기" 창이 열립니다.

3. "Create a new object"(새 개체 만들기)가 선택되어 있는지 확인하고 "확인"을 클릭합니다.

"특성 매핑 만들기: *이름*" 창이 열립니다.

4. "일반" 그룹 상자의 필드에 특성 매핑의 일반 이름과 설명을 입력합니다.

참고: 일반 이름은 사용자 특성 이름과 동일한 규칙을 따라야 합니다.

5. "속성" 그룹 상자에서 "마스크"를 선택합니다.
6. "속성" 그룹 상자의 "정의" 상자에 정의를 입력합니다.

예:

이름: IsDisabled

정의: AccountStatus:4

설명:

일반 이름 IsDisabled 는 사용자 특성 이름 AccountStatus 에 매핑됩니다. AccountStatus 는 하나 이상의 상태를 비트 패턴으로 저장합니다. 예를 들어 AccountStatus 는 계정 상태를 세 번째 비트에 저장합니다. 계정이 비활성화된 경우 세 번째 비트는 1 로 설정됩니다. 반대로 계정이 활성화된 경우에는 세 번째 비트가 0 으로 설정됩니다.

SiteMinder 는 AccountStatus 와 지정된 상태 또는 마스크(이 예의 경우 4)에 대해 bitwise AND 연산을 수행하여 계정이 비활성화되어 있는지 여부를 확인합니다. 계정이 비활성화된 경우 IsDisabled 는 TRUE 입니다.

7. (선택 사항) "사용 안 함"을 선택하여 이 특성 매핑이 사용되지 않도록 설정합니다.
8. "확인"을 클릭합니다.

처리를 위해 "특성 매핑 만들기" 태스크가 제출되고 "특성 매핑 목록" 그룹 상자의 목록에 새 특성 매핑이 추가됩니다.

마스크 특성 매핑의 비트 마스크

비트 마스크 특성 매핑은 사용자 특성의 다른 비트 값을 마스크하여 하나 이상의 비트 값을 테스트합니다.

마스크 특성 매핑은 다음과 같이 정의됩니다.

```
user_attribute_name:bit_mask
```

예를 들어 사용자 특성 이름이 **AccountStatus** 라고 가정합니다. **AccountStatus** 특성은 다음 세 플래그의 상태를 비트 패턴으로 저장합니다.

비트 패턴	플래그
00?	계정 비활성화 여부
0?0	암호 만료 여부
?00	골드 구성원 여부

비트가 1 인 경우 플래그는 **TRUE** 입니다. 다음 표에서는 결과를 보여 줍니다.

비트 패턴	계정 상태
000 (0)	어떤 플래그도 TRUE 가 아님
001 (1)	계정 비활성화됨
010 (2)	암호 만료됨
100 (4)	골드 구성원
011 (3)	암호 만료됨, 계정 비활성화됨
101 (5)	골드 구성원, 계정 비활성화됨
110 (6)	골드 구성원, 암호 만료됨
111 (7)	골드 구성원, 암호 만료됨, 계정 비활성화됨

참고: 해당하는 10 진수 값은 괄호 안에 표시되어 있습니다.

사용자가 골드 구성원인지 여부만 테스트하려 한다고 가정합니다. 이 비트를 테스트하려면 비트 마스크로 골드 구성원에 해당하는 비트 패턴, 즉 100(이진수)을 선택하고 해당 값을 4(10 진수)로 지정하십시오. 결과 마스크 특성 매핑은 다음과 같이 정의됩니다.

AccountStatus:4

그러면 AccountStatus 에 대한 bitwise AND 연산이 비트 마스크에 대해 수행되고 결과가 비트 마스크와 같은지 여부가 테스트됩니다. 결과가 같으면 테스트된 비트의 값이 1 이고 플래그가 TRUE 임을 의미합니다. 다음 표에서는 결과를 보여 줍니다.

계정 상태	비트 마스크	bitwise AND 결과	골드 구성원 여부
000 (0)	100 (4)	000 (0)	FALSE
001 (1)	100 (4)	000 (0)	FALSE
010 (2)	100 (4)	000 (0)	FALSE
011 (3)	100 (4)	000 (0)	FALSE
100 (4)	100 (4)	100 (4)	TRUE
101 (5)	100 (4)	100 (4)	TRUE
110 (6)	100 (4)	100 (4)	TRUE
111 (7)	100 (4)	100 (4)	TRUE

참고: 해당하는 10 진수 값은 괄호 안에 표시되어 있습니다.

비트 마스크를 사용하여 비트 집합 또는 여러 비트의 값을 한 번에 테스트할 수도 있습니다. 계정이 비활성화되어 있고 암호가 만료되었는지를 확인하려 한다고 가정합니다. 이러한 비트를 테스트하려면 비트 마스크를 011(이진수) 또는 3(10 진수)으로 지정하십시오. 결과 마스크 특성 매핑은 다음과 같이 정의됩니다.

AccountStatus:3

그러면 AccountStatus 에 대한 bitwise AND 연산이 비트 마스크에 대해 수행되고 결과가 비트 마스크와 같은지 여부가 테스트됩니다. 결과가 같으면 테스트된 두 비트의 값이 모두 1 이고 두 플래그가 모두 TRUE 임을 의미합니다. 다음 표에서는 결과를 보여 줍니다.

계정 상태	비트 마스크	bitwise AND 결과	두 플래그가 모두 설정되었는지 여부
000 (0)	011 (3)	000 (0)	FALSE
001 (1)	011 (3)	001 (1)	FALSE
010 (2)	011 (3)	010 (2)	FALSE
011 (3)	011 (3)	011 (3)	TRUE
100 (4)	011 (3)	000 (0)	FALSE
101 (5)	011 (3)	001 (1)	FALSE
110 (6)	011 (3)	010 (2)	FALSE
111 (7)	011 (3)	011 (3)	TRUE

참고: 해당하는 10 진수 값은 괄호 안에 표시되어 있습니다.

상수

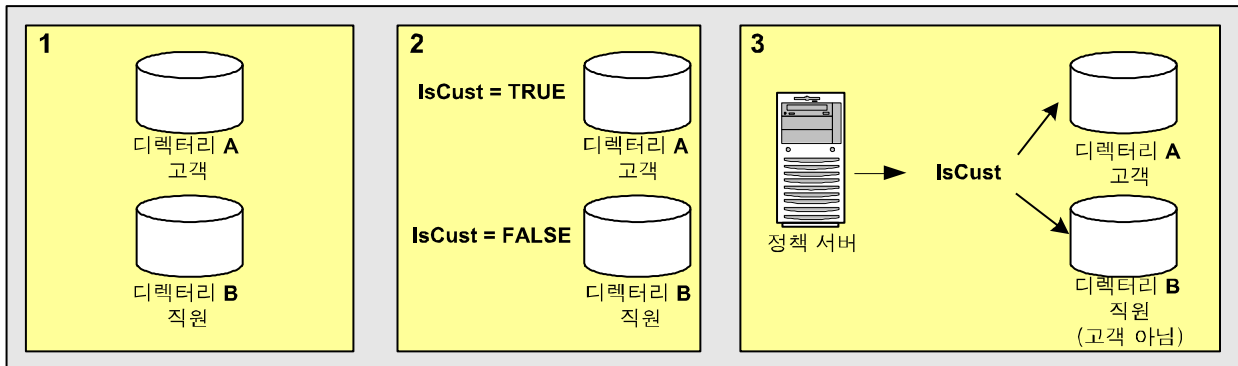
상수특성 매핑을 사용하면 디렉터리의 모든 사용자에게 대해 동일하거나 상수인 값에 일반 이름을 매핑할 수 있습니다. 상수특성 매핑은 읽기 전용(R)인 상수에 일반 이름을 매핑하므로 시스템 관리자를 제외하고는 이를 변경할 수 없습니다.

상수특성 매핑은 다음과 같은 데이터 형식의 상수에 매핑할 수 있습니다.

- 문자열
- 숫자
- 부울

상수 사용 사례

이 사용 사례는 하나의 사용자 디렉터리가 고객만 저장하고 다른 사용자 디렉터리가 직원만 저장하는 시나리오를 나타냅니다. 다음 그림은 두 개의 상수 특성 매핑이 다른 사용자 디렉터리에 대해 다른 값을 나타낼 수 있는 방법을 설명합니다.



1. 디렉터리 A 에는 고객만 저장됩니다. 디렉터리 B 에는 직원만 저장됩니다.
2. IsCust 는 서로 다른 디렉터리의 각기 다른 값에 매핑된 일반 이름입니다.
 - 디렉터리 A 에서는 IsCust 가 TRUE 에 매핑됩니다.
 - 디렉터리 B 에서는 IsCust 가 FALSE 에 매핑됩니다.
3. 정책, 식 또는 기타 개체를 정의할 때 IsCust 를 참조합니다. 일반 이름을 사용하면 시스템이 사용자가 저장된 특정 디렉터리에 관계없이 사용자가 고객인지 여부를 확인할 수 있습니다. 이 매핑은 디렉터리 A 의 모든 사용자가 고객인 반면 디렉터리 B 의 모든 사용자는 고객이 아님을 나타냅니다.

상수 특성 매핑 만들기

디렉터리의 모든 사용자에게 정보를 전달하는 상수 값에 일반 이름을 매핑할 수 있습니다. 상수의 데이터 형식은 문자열, 숫자 또는 부울일 수 있습니다. 상수 특성 매핑을 사용하여 사용자 디렉터리의 모든 사용자에게 적용되는 사용자 특성 값을 읽을 수 있습니다. 사용자 특성 매핑은 디렉터리별로 적용됩니다.

다음 단계를 수행하십시오.

1. "사용자 디렉터리: *이름*" 창으로 이동합니다.
2. "특성 매핑 목록" 그룹 상자에서 "만들기"를 클릭합니다.
"특성 매핑 만들기" 창이 열립니다.
3. "Create a new object"(새 개체 만들기)가 선택되어 있는지 확인하고 "확인"을 클릭합니다.
"특성 매핑 만들기: *이름*" 창이 열립니다.
4. "일반" 그룹 상자의 필드에 특성 매핑의 일반 이름과 설명을 입력합니다.

참고: 일반 이름은 사용자 특성 이름과 동일한 규칙을 따라야 합니다.

5. "속성" 그룹 상자에서 "상수"를 선택합니다.
6. "속성" 그룹 상자의 "정의" 상자에 정의를 입력합니다.

예:

이름: IsCustomer

정의: TRUE

설명: 일반 이름 IsCustomer 는 상수 값 TRUE 에 매핑됩니다. 이 사용자 디렉터리에는 고객만 저장되므로 사용자는 항상 고객이고 IsCustomer 는 항상 TRUE 에 매핑됩니다.

7. (선택 사항) "사용 안 함"을 선택하여 이 특성 매핑이 사용되지 않도록 설정합니다.
8. "확인"을 클릭합니다.
"특성 매핑 만들기" 태스크가 처리를 위해 제출됩니다. 새 특성 매핑은 "특성 매핑 목록" 그룹 상자에 나타납니다.

식

식 특성 매핑을 사용하면 식에 일반 이름을 매핑할 수 있습니다. 이 식은 기본 스키마에 의해 지정되는 하나 이상의 사용자 특성 이름을 포함할 수 있습니다. 이 식은 SiteMinder 식 구문 규칙을 따라야 합니다.

식 특성 매핑은 읽을 수만 있고 변경할 수는 없는 식에 일반 이름을 매핑합니다. 이러한 유형의 액세스를 읽기 전용(R)이라고 합니다. 이 식은 실행 시 문자열, 숫자 또는 부울 값을 반환합니다.

식 특성 매핑과 명명된 식의 한 유형인 가상 사용자 특성은 다음과 같은 유사점이 있습니다.

- 둘 모두 SiteMinder 식입니다.
- 둘 모두 읽기 전용(R)입니다.
- 둘 모두 다음 데이터 형식 중 하나를 반환합니다.
 - 문자열
 - 숫자
 - 부울

식 특성 매핑과 가상 사용자 특성은 다음과 같은 차이점이 있습니다.

- 식 특성 매핑은 특정 사용자 디렉터리에 대해 정의됩니다. 가상 사용자 특성은 전역 설정이므로 모든 사용자 디렉터리의 모든 사용자에게 적용될 수 있습니다.
- 가상 사용자 특성은 파운드 기호(#)로 시작해야 합니다. 식 매핑은 그렇지 않습니다.

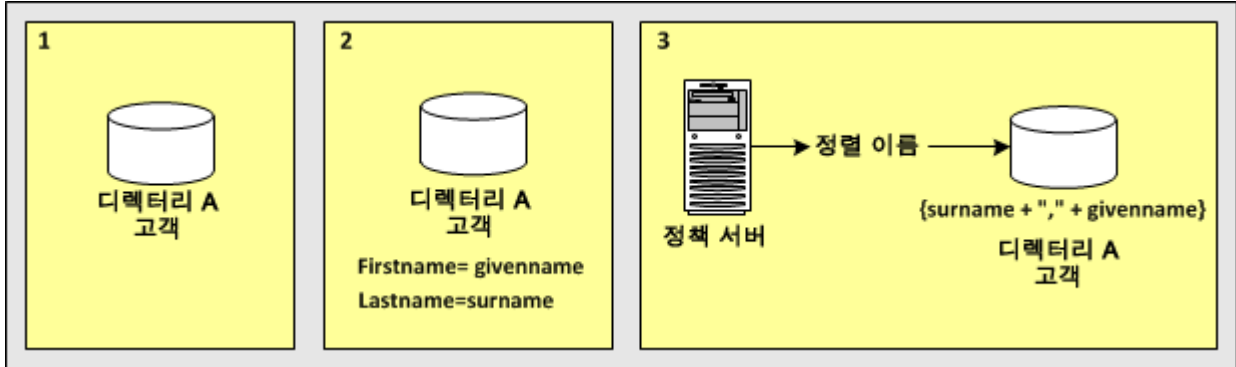
추가 정보:

[명명된 식](#) (페이지 227)

식 사용 사례

이 사용 사례에서는 식 특성 매핑을 사용하여 한 디렉터리의 여러 사용자 특성에 대한 참조를 단순화하는 방법을 보여 줍니다. 보호된 리소스에는 각 사용자의 *정렬 이름*(성, 이름)이 필요합니다. 사용자 디렉터리는 이 특성을 고유하게 참조하지 않습니다. 대신 이 디렉터리에는 각 사용자의 성이 `surname` 으로, 각 사용자의 이름이 `givenname` 으로 저장됩니다.

다음 그림에서는 식 특성 매핑을 사용하여 동일한 사용자 정보의 공통 보기를 생성하는 방법을 자세히 설명합니다.



단일 사용자 디렉터리에서는 일반 이름이 디렉터리의 사용자 특성 이름을 사용하여 정렬 이름을 생성하는 식에 매핑됩니다.

- 디렉터리 A에는 모든 사용자 레코드가 포함되어 있습니다.
- 매핑의 이름은 **SortName**입니다.
- SortName을 정의하는 식은 다음과 같습니다.

{surname + "," + givenname}

참고: 이 식은 SiteMinder 식 구문 규칙을 따라야 합니다.

- SortName은 surname 및 givenname 특성을 포함하는 식에 매핑된 일반 이름입니다.

디렉터리별 스키마에 관계없이 사용자의 정렬 이름을 사용해야 하는 정책, 식 또는 기타 개체를 정의할 때 **SortName**을 참조합니다.

식 특성 매핑 만들기

기본 스키마에 의해 지정된 사용자 특성 이름을 하나 이상 참조하는 식에 일반 이름을 매핑할 수 있습니다. 식 특성 매핑 데이터 형식은 문자열, 숫자 또는 부울입니다. 식 특성 매핑을 사용하여 식의 결과를 읽을 수 있지만 사용자 디렉터리에 값을 쓸 수는 없습니다.

참고: 사용자 특성 매핑은 디렉터리별로 적용됩니다. 식으로 정의된 전역 개체를 생성하려면 명명된 식을 생성하십시오.

다음 단계를 수행하십시오.

1. "사용자 디렉터리: *이름*" 창으로 이동합니다.
2. "특성 매핑 목록" 그룹 상자에서 "만들기"를 클릭합니다.
"특성 매핑 만들기" 창이 열립니다.
3. "Create a new object"(새 개체 만들기)가 선택되어 있는지 확인하고
"확인"을 클릭합니다.
"특성 매핑 만들기: *이름*" 창이 열립니다.
4. "일반" 그룹 상자의 필드에 특성 매핑의 일반 이름과 설명을
입력합니다.
참고: 일반 이름은 사용자 특성 이름과 동일한 규칙을 따라야 합니다.
5. "속성" 그룹 상자에서 "식"을 선택합니다.
참고: "식"을 선택하면 "편집" 단추가 활성화됩니다. "편집"을 클릭하면
식 편집기가 열립니다. 식은 SiteMinder 식 구문 규칙을 따라야 합니다.
6. "속성" 그룹 상자의 "정의" 상자에 정의를 입력합니다.
예:
이름: SortName
정의: (surname + ',' + givenname)
설명: 일반 이름 SortName 은 사용자 특성 이름 surname 및
givenname 을 참조하는 식에 매핑됩니다.
7. (선택 사항) "사용 안 함"을 선택하여 이 특성 매핑이 사용되지 않도록
설정합니다.
8. "확인"을 클릭합니다.
"특성 매핑 만들기" 태스크가 처리를 위해 제출됩니다. 새 특성 매핑은
"특성 매핑 목록" 그룹 상자에 나타납니다.

고급 사용자 특성 매핑 예

다음 예에서는 보다 복잡한 사용자 특성 매핑 구성을 보여 줍니다.

이 예의 배포 대상은 서로 다른 유형의 사용자 디렉터리 두 개를 사용하는 소매 의류업체입니다.

디렉터리 A

직원 전용의 내부 LDAP 사용자 디렉터리입니다.

디렉터리 B

고객 전용의 ODBC 사용자 디렉터리입니다.

각 사용자 특성 매핑은 해당 사용자 특성 매핑이 정의된 사용자 디렉터리에 대해 적용됩니다.

다음 표에서는 디렉터리 A 와 디렉터리 B 에서 동일한 사용자 정보가 식별되는 방식을 자세히 설명합니다. 함께 제공되는 사용 사례에서는 서로 다른 특성 매핑을 사용하여 동일한 사용자 정보의 공통 보기를 정의하는 방법에 대해 설명합니다. 공통 보기는 디렉터리의 작동 방식이 동일하게 만드는 유니버설 스키마의 역할을 합니다.

특성 설명	디렉터리 A 특성(LDAP)	디렉터리 B 특성(ODBC)
각 사용자의 이름	givenname	u_first_name
각 사용자의 성	surname	u_last_name
각 사용자의 정렬 이름(성, 이름)	사용자 디렉터리에는 사용자 특성이 고유하게 저장되지 않습니다.	sort_name
고객인 사용자	group:cn=customer,ou=groups,o=acme.com	사용자가 항상 고객입니다.
사용자 계정의 상태	AccountStatus 특성(플래그 집합). 두 번째 비트는 비활성화된 계정입니다.	u_disabled

별칭 매핑 유형을 사용하여 이름 특성 매핑

별칭 특성 매핑을 두 개 사용하여 디렉터리 A 와 디렉터리 B 의 이름 사용자 특성을 나타낼 수 있습니다.

배포

디렉터리 A 는 `givenname` 을 사용하여 사용자의 이름을 식별합니다.

디렉터리 B 는 `u_first_name` 을 사용하여 사용자의 이름을 식별합니다.

해결책

1. 디렉터리 A 에 대한 별칭 특성 매핑을 생성합니다.

이름

`FirstName`

매핑 유형

별칭

정의

`givenname`

2. 디렉터리 B 에 대한 별칭 특성 매핑을 생성합니다.

이름

`FirstName`

매핑 유형

별칭

정의

`u_first_name`

디렉터리 A 의 사용자를 참조할 때는 `FirstName` 이 `givenname` 에 매핑됩니다.

디렉터리 B 의 사용자를 참조할 때는 `FirstName` 이 `u_first_name` 에 매핑됩니다.

별칭 매핑 유형을 사용하여 성 특성 매핑

별칭 특성 매핑을 두 개 사용하여 디렉터리 A 와 디렉터리 B 의 성 사용자 특성을 나타낼 수 있습니다.

배포

사용자 디렉터리 A 는 `surname` 을 사용하여 사용자의 성을 식별합니다.
디렉터리 B 는 `u_last_name` 을 사용하여 사용자의 성을 식별합니다.

해결책

1. 디렉터리 A 에 대한 별칭 특성 매핑을 생성합니다.

이름

`LastName`

매핑 유형

별칭

정의

`surname`

2. 디렉터리 B 에 대한 별칭 특성 매핑을 생성합니다.

이름

`LastName`

매핑 유형

별칭

정의

`u_last_name`

디렉터리 A 의 사용자를 참조할 때는 공통 보기에서 사용자의 성이 `surname` 으로 식별되는지 확인합니다. 디렉터리 B 의 사용자를 참조할 때는 공통 보기에서 사용자의 성이 `u_last_name` 으로 식별되는지 확인합니다.

식 및 별칭 매핑 유형을 사용하여 정렬 이름 특성 매핑

디렉터리 A 와 디렉터리 B 에서 사용자의 정렬 이름을 나타내려면 식 특성 매핑과 별칭 특성 매핑을 사용하십시오.

배포

- 디렉터리 A 는 각 사용자의 정렬 이름을 고유하게 식별하지 않습니다. 디렉터리 A 에는 각 사용자에게 대해 이름이 `givenname` 으로, 성이 `surname` 으로 저장됩니다.
- 디렉터리 B 는 `sort_name` 을 사용하여 정렬 이름을 식별합니다.

해결책

1. 디렉터리 A 에 대한 식 특성 매핑을 생성합니다.

이름

SortName

매핑 유형

식

정의

(surname + "," + givenname)

참고: 식은 식 구문 규칙을 따라야 합니다.

2. 디렉터리 B 에 대한 별칭 특성 매핑을 생성합니다.

이름

SortName

매핑 유형

별칭

정의

sort_name

디렉터리 A 의 사용자를 참조할 때는 정렬 이름이 지정된 식을 기반으로 계산됩니다. 디렉터리 B 의 사용자를 참조할 때는 정렬 이름이 `sort_name` 특성으로 표시됩니다.

그룹 및 상수 매핑 유형을 사용하여 고객 매핑

디렉터리 A 와 디렉터리 B 의 고객을 식별하려면 그룹 및 상수 특성 매핑을 사용하십시오.

배포

- 디렉터리 A 에는 직원이 저장됩니다. 회사의 직원은 고객일 수도 있으므로 디렉터리 A 는 고객을 다음 그룹에 속해 있는 직원으로 식별합니다.
`cn=Customers,ou=Groups,o=acme.com`
- 디렉터리 B 에는 고객만 저장됩니다. 디렉터리 B 에는 고객을 식별하는 사용자 특성이 없습니다. 디렉터리 B 에 사용자를 저장한다는 것은 사용자가 곧 고객임을 의미합니다.

해결책

1. 디렉터리 A 에 대한 그룹 특성 매핑을 생성합니다.

이름

`IsCustomer`

매핑 유형

`Group`

정의

`cn=Customers,ou=Groups,o=acme.com`

2. 디렉터리 B 에 대한 상수 특성 매핑을 생성합니다.

이름

`IsCustomer`

매핑 유형

`상수`

정의

`TRUE`

디렉터리 A 를 참조할 때는 `cn=Customers,ou=Groups,o=acme.com` 에 속한 사용자가 고객으로 간주됩니다. 디렉터리 B 를 참조할 때는 모든 사용자가 고객입니다.

마스크 및 식 매핑 유형을 사용하여 계정 상태 매핑

디렉터리 A 와 디렉터리 B 에서 비활성화된 사용자 계정을 식별하려면 마스크 특성 매핑과 식 특성 매핑을 사용하십시오.

배경

- 디렉터리 A 는 플래그 집합인 **AccountStatus** 라는 사용자 특성을 사용하여 비활성화된 계정을 식별합니다. 두 번째 비트는 비활성화된 계정을 나타냅니다.
- 디렉터리 B 는 **u_disabled** 라는 사용자 특성을 사용하여 비활성화된 계정을 식별합니다. **u_disabled** 가 "y"이면 계정이 비활성화된 것입니다. **u_disabled** 가 "n"이면 계정이 활성 상태입니다.

해결책

1. 디렉터리 A 에 대한 마스크 특성 매핑을 생성합니다.

이름

IsDisabled

매핑 유형

마스크

정의

AccountStatus:2

이 정의는 **AccountStatus** 에 비트 패턴이 저장되며 비트 마스크가 2(10 진수)임을 나타냅니다.

2. 디렉터리 B 에 대한 식 특성 매핑을 생성합니다.

이름

IsDisabled

매핑 유형

식

정의

(u_disabled = "y")

u_disabled 는 부울 식입니다.

디렉터리 A 를 참조할 때는 비트 패턴이 사용자 비활성화 여부를 확인합니다. 디렉터리 B 를 참조할 때는 식이 사용자 비활성화 여부를 확인합니다.

제 7 장: 디렉터리 매핑

이 섹션은 다음 항목을 포함하고 있습니다.

[디렉터리 매핑 개요](#) (페이지 271)

[아이덴티티 매핑 구성](#) (페이지 273)

[레거시 디렉터리 매핑 구성](#) (페이지 280)

[영역에서 디렉터리 매핑 제거](#) (페이지 283)

[디렉터리 매핑 예](#) (페이지 283)

[디렉터리 매핑 및 응답](#) (페이지 286)

디렉터리 매핑 개요

정책 서버는 사용자가 동일한 사용자 디렉터리에서 인증되고 권한이 부여된다고 가정합니다. 하지만 사용자는 하나의 디렉터리에 대해 인증되고 별도 디렉터리에 대해 권한 부여될 수 있습니다. 이 기능을 디렉터리 매핑이라고 합니다.

권한 부여 정보를 저장하는 별도의 분산된 사용자 디렉터리를 사용하여 인증 정보를 저장하는 중앙 디렉터리를 매핑할 수 있습니다. 권한 부여 디렉터리는 특정 네트워크 응용 프로그램과 연결되어 있습니다. 이 매핑은 별도 권한 부여 디렉터리에서 관련 사용자를 찾습니다.

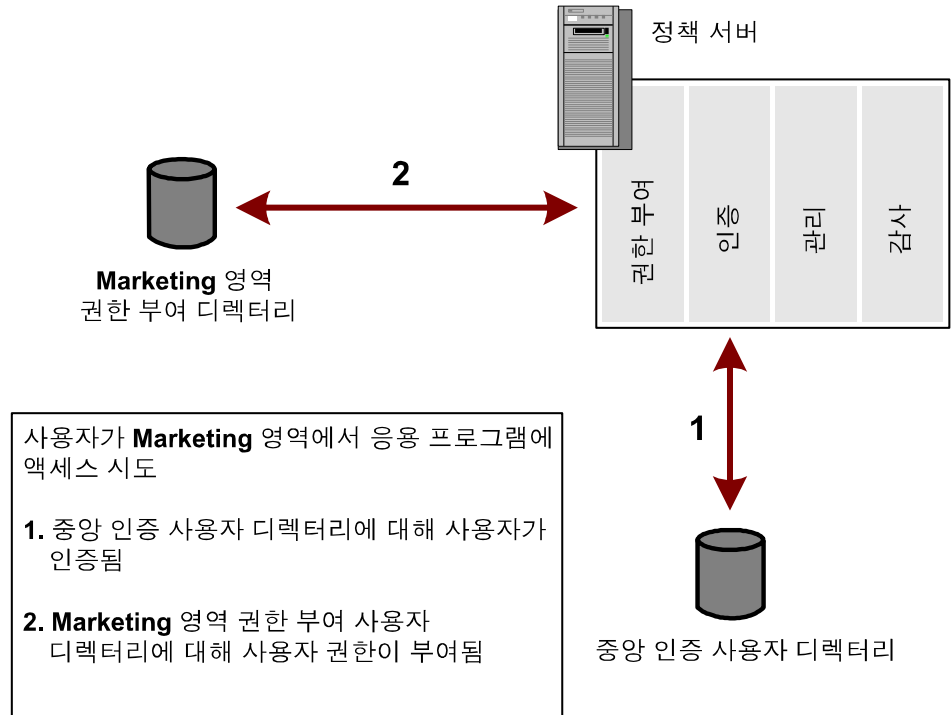
참고: 디렉터리 매핑은 가장을 지원하지 않습니다. 가장되는 사용자는 도메인과 연결된 인증 디렉터리에 고유하게 존재해야 합니다. 그렇지 않으면 가장이 실패합니다.

인증 디렉터리에서 권한 부여 디렉터리로의 매핑은 세 단계 프로세스로 수행됩니다.

1. 사용자 디렉터리 연결을 설정합니다.
2. 디렉터리 매핑을 구성합니다.
3. 영역에 디렉터리 매핑을 할당합니다. 사용자는 특정 네트워크 응용 프로그램과 관련하여 이 디렉터리에 대해 권한 부여됩니다.

예를 들어, 회사의 모든 사용자는 하나의 중앙 사용자 디렉터리에 대해 인증됩니다. 마케팅 조직은 별도의 사용자 디렉터리에 대해 권한 부여됩니다. 인증과 마케팅 권한 부여 사용자 디렉터리 사이에 디렉터리 매핑을 구성한 다음 마케팅 응용 프로그램을 위한 영역을 만들 수 있습니다. 이 영역은 매핑에 정의된 권한 부여 디렉터리를 사용합니다. 사용자가 마케팅 응용 프로그램에 액세스하려고 시도하면 이 사용자는 중앙 사용자 디렉터리에 대해 인증되고 마케팅 사용자 디렉터리에 대해 권한 부여됩니다.

이 예제는 다음 다이어그램에 표시되어 있습니다.



권한 부여 및 유효성 검사 아이덴티티 매핑

아이덴티티 매핑을 통해 여러 개의 대상 사용자 디렉터리를 구성하고 사용자 지정 검색 조건을 사용할 수 있습니다. 이 구성은 환경을 설정하는데 융통성을 줍니다.

아이덴티티 매핑에는 두 가지 유형이 있습니다.

권한 부여 아이덴티티 매핑

하나의 디렉터리에 대해 사용자를 인증하고 다른 디렉터리에 대해 사용자에게 권한을 부여하는 디렉터리 매핑입니다.

유효성 검사 아이덴티티 매핑

하나의 디렉터리에 대해 사용자를 인증하고 다른 디렉터리에 대해 사용자의 유효성을 검사하는 디렉터리 매핑입니다. 정책 서버에 연결된 인증 사용자 디렉터리는 다른 정책 서버에 연결된 유효성 검사 사용자 디렉터리에 매핑됩니다.

아이덴티티 매핑은 기존 사용자 디렉터리 연결이 필요 없습니다.

레거시(Auth/Az 및 AuthValidate) 디렉터리 매핑이라고 불리는 디렉터리 매핑을 위한 레거시 방법이 있습니다. 이 레거시 방법은 이 릴리스에서 여전히 사용되며 모든 기존 레거시 매핑도 동일한 방식으로 계속 사용할 수 있습니다.

레거시 디렉터리 매핑을 사용하려면 정책 서버와 사용자 디렉터리의 연결이 인증 디렉터리 및 권한 부여 또는 유효성 검사 디렉터리에 존재해야 합니다.

아이덴티티 매핑 구성

아이덴티티 매핑은 사용자 지정 검색 조건을 사용하여 원본 디렉터리에서 대상 디렉터리로 사용자를 매핑하는 향상된 방법을 제공합니다. 사용자 권한 부여 및 사용자 유효성 검사에서 아이덴티티 매핑을 사용할 수 있습니다.

아이덴티티 매핑은 다음 두 가지 매핑 방법을 제공합니다.

- 권한 부여 매핑(기본값)
- 유효성 검사 매핑

아이덴티티 매핑을 통해 사용자 지정 검색을 사용하고 서로 다른 아이덴티티 매핑 항목 개체를 통해 매핑 규칙 순서를 제어할 수 있습니다. 정책 서버는 먼저 아이덴티티 매핑에 정의된 매핑 메커니즘을 사용하여 사용자를 찾으려고 시도합니다. 이 매핑이 실패하면 사용자를 찾기 위해 세션 사용자 디렉터리가 사용됩니다. 이 세션 디렉터리는 정책 서버가 기본적으로 검색할 수 있도록 정책 저장소에 있어야 합니다.

참고: 유효성 검사 매핑의 경우 인증 디렉터리는 로컬 저장소에 있지 않아도 됩니다.

아이덴티티 매핑에서 지원되는 디렉터리

다음 표에는 지원되는 유형의 디렉터리 매핑과 인증 디렉터리를 권한 부여 또는 유효성 검사 디렉터리에 매핑하는 데 사용할 수 있는 방법이 나열되어 있습니다.

권한 부여 디렉터리/유효성 검사 디렉터리		
인증 디렉터리	LDAP	관계형 데이터베이스
LDAP	동일한 DN	유니버설 ID
	유니버설 ID	사용자 지정 검색
	사용자 지정 검색	
AD	동일한 DN	유니버설 ID
	유니버설 ID	사용자 지정 검색
	사용자 지정 검색	
관계형 데이터베이스	유니버설 ID	동일한 DN
	사용자 지정 검색	유니버설 ID
		사용자 지정 검색

아이덴티티 매핑 항목 유형

아이덴티티 매핑에는 하나 이상의 항목이 포함될 수 있습니다. 아이덴티티 매핑 항목은 대상 디렉터리에서 사용자를 찾는 방법을 지정하는 규칙을 정의합니다. 대상 디렉터리에서 사용자를 찾기 위해 정책 서버는 세션 티켓 정보에 기초한 검색 기준을 사용합니다.

아이덴티티 매핑에는 대상 사용자 디렉터리가 여러 개 포함될 수 있습니다. 서로 다른 대상 사용자 디렉터리에 대한 항목을 동일한 아이덴티티 매핑 개체에 추가할 수 있습니다. 아이덴티티 매핑 항목은 순서가 지정된 매핑 목록으로 처리됩니다.

다음은 두 가지 유형의 아이덴티티 매핑 항목입니다.

권한 부여 아이덴티티 매핑 항목

원본 디렉터리와 대상 디렉터리에 대한 링크를 지정합니다. 이 링크를 사용할 수 없으면 권한 부여에 인증 디렉터리가 사용됩니다. 동일한 DN, 유니버설 ID 를 선택할 수도 있고 사용자 지정 검색 조건을 지정할 수도 있습니다.

유효성 검사 아이덴티티 매핑 항목

텍스트 문자열 형식의 원본 디렉터리 이름과 대상 디렉터리에 대한 링크를 지정합니다. 원본 디렉터리의 이름을 제공하거나 기본값인 **SMSESSION** 사용자 디렉터리를 선택할 수 있습니다. 기본값은 유효성 검사에 세션 티켓 내의 사용자 디렉터리가 사용됨을 나타냅니다. 대상 디렉터리에 대한 링크가 없으면 유효성 검사에 인증 디렉터리가 사용됩니다. 동일한 DN, 유니버설 ID 를 선택할 수도 있고 사용자 지정 검색 특성을 지정할 수도 있습니다.

복잡한 사용자 검색 식 사용

복잡한 사용자 검색 조건을 사용하여 인증 디렉터리를 권한 부여 디렉터리 또는 유효성 검사 디렉터리에 매핑할 수 있습니다. 사용자 검색 조건은 특성의 조합입니다. 특성은 원본 디렉터리 또는 대상 디렉터리에 있을 수 있습니다.

일반적으로 사용자 검색 조건은 사용자 디렉터리마다 다릅니다. 예를 들어 ODBC 기반 사용자 검색 조건은 LDAP 기반 사용자 검색 조건과 다를 수 있습니다.

다양한 네임스페이스의 사용자 디렉터리를 지원하려면 각각의 사용자 디렉터리에 대해 검색 조건을 정의하십시오. 또한 대상 사용자 디렉터리에 대해 사용자 디렉터리 특성 매핑을 정의할 수도 있습니다. 그러면 각 사용자 디렉터리에서 특성 매핑에 대한 자체의 고유한 검색 조건을 정의해야 합니다. 사용자 디렉터리 특성 매핑을 통해 사용자 디렉터리별 검색 조건을 정의할 수 있습니다.

권한 부여 아이덴티티 매핑을 구성하는 방법

인증-권한 부여 아이덴티티 매핑 구성은 두 단계 프로세스로 수행됩니다.

1. 권한 부여 아이덴티티 매핑 구성
2. 권한 부여 아이덴티티 매핑을 영역에 할당

권한 부여 아이덴티티 매핑 구성

한 디렉터리에 대해 사용자를 인증하고 다른 디렉터리에 대해 사용자에게 권한을 부여하려면 아이덴티티 매핑을 구성하십시오.

다음 단계를 수행하십시오.

1. "인프라", "디렉터리"를 차례로 클릭합니다.
2. "아이덴티티 매핑"을 클릭합니다.
3. "아이덴티티 매핑 만들기"를 클릭합니다.
4. 매핑의 이름과 설명을 지정합니다.
5. 매핑 유형으로 "인증-권한 부여"를 선택합니다.
6. "항목 만들기"를 클릭합니다.
7. 아이덴티티 매핑 항목의 이름을 지정합니다.
8. 각 목록에서 원본 디렉터리와 대상 디렉터를 선택합니다.
9. 사용자 검색 기준으로서 다음 옵션 중 하나를 선택합니다.

동일한 DN

인증 디렉터리에서 유효성 검사 디렉터리로 사용자의 DN(고유 이름)을 매핑합니다.

유니버설 ID

인증 디렉터리의 유니버설 ID 특성 값을 유효성 검사 디렉터리의 유니버설 ID 값과 매칭합니다.

사용자 지정 검색

대상 디렉터리와 원본 디렉터리의 특성을 지정합니다. 원본 디렉터리 특성은 사용자가 지정한 특성이거나 SiteMinder 세션 특성일 수 있습니다.

10. "확인"을 클릭합니다.

아이덴티티 매핑 항목이 권한 부여 아이덴티티 매핑 개체에 추가됩니다.

11. 제출을 클릭합니다.

권한 부여 아이덴티티 매핑 개체가 구성됩니다.

권한 부여 아이덴티티 매핑을 영역에 할당

권한 부여 아이덴티티 매핑을 영역에 할당하십시오. 정책 서버는 영역에 지정된 권한 부여 매핑을 사용하여 사용자에게 권한을 부여합니다.

다음 단계를 수행하십시오.

1. "정책", "도메인", "영역"을 클릭합니다.

"영역" 페이지가 표시됩니다.

2. 수정할 영역을 선택합니다.

3. "수정"을 클릭합니다.

4. "권한 부여 매핑" 목록에서 권한 부여 디렉터리로 사용할 아이덴티티 매핑을 선택합니다.

5. 제출을 클릭합니다.

권한 부여 아이덴티티 매핑이 선택한 영역에 할당됩니다.

추가 정보:

[응용 프로그램에 대한 고급 정책 구성 요소 구성](#) (페이지 517)

유효성 검사 아이덴티티 매핑을 구성하는 방법

인증 및 유효성 검사 아이덴티티 매핑 구성은 두 단계 프로세스로 수행됩니다.

1. 유효성 검사 아이덴티티 매핑을 구성합니다.

2. 유효성 검사 아이덴티티 매핑을 영역에 할당합니다.

참고: 동일한 저장소에 있는 여러 디렉터리에 대해 유효성 검사 매핑을 생성할 수 있습니다. 원본 디렉터리는 로컬 저장소에 있지 않아도 됩니다.

유효성 검사 아이덴티티 매핑 구성

한 디렉터리에서 사용자를 인증하고 다른 디렉터리에서 사용자의 유효성을 검사하도록 아이덴티티 매핑을 구성하십시오.

다음 단계를 수행하십시오.

1. "인프라", "디렉터리"를 차례로 클릭합니다.
2. "아이덴티티 매핑"을 클릭합니다.
3. "아이덴티티 매핑 만들기"를 클릭합니다.
4. 이름과 설명을 입력합니다.
5. 매핑 유형으로 "인증-유효성 검사"를 선택합니다.
6. "항목 만들기"를 클릭합니다.
7. 이름을 입력합니다.
8. 원본 디렉터리가 해당 세션 내에 있지 않을 경우 원본 디렉터를 지정합니다.
9. 대상 디렉터를 선택합니다.
10. 사용자 검색 조건을 선택합니다.

사용자 지정 검색을 선택하는 경우 대상 디렉터리와 원본 디렉터리에서 특성을 지정합니다.

원본 디렉터리 특성은 사용자가 지정한 특성이거나 SiteMinder 세션 특성일 수 있습니다.

11. "확인"을 클릭합니다.

아이덴티티 매핑 항목이 유효성 검사 아이덴티티 매핑 개체에 추가됩니다.

12. 제출을 클릭합니다.

유효성 검사 아이덴티티 매핑 개체가 구성됩니다.

유효성 검사 아이덴티티 매핑을 영역에 할당

유효성 검사 아이덴티티 매핑을 영역에 할당합니다. 정책 서버는 영역에 지정된 유효성 검사 디렉터리 매핑을 사용하여 사용자에게 권한을 부여합니다.

다음 단계를 수행하십시오.

1. "정책", "도메인", "영역"을 클릭합니다.
2. 수정할 영역을 선택합니다.
3. "수정"을 클릭합니다.
4. "유효성 검사 매핑" 목록에서 권한 부여 디렉터리로 사용할 아이덴티티 매핑을 선택합니다.
5. 제출을 클릭합니다.

유효성 검사 아이덴티티 매핑이 선택한 영역에 할당됩니다.

추가 정보:

[응용 프로그램에 대한 고급 정책 구성 요소 구성](#) (페이지 517)

기본 전역 유효성 검사 디렉터리 매핑 구성

하나의 유효성 검사 아이덴티티 매핑은 유효성 검사 매핑을 위한 전역 기본값으로 사용될 수 있습니다. 전역 유효성 검사 아이덴티티 매핑을 설정하면 모든 영역에 대해 매핑을 설정할 필요가 없으므로 시간이 절약됩니다. 하지만 전역 유효성 검사 아이덴티티 매핑을 로컬 매핑으로 재정의할 수 있습니다.

다음 단계를 수행하십시오.

1. "정책", "전역"을 차례로 클릭합니다.
2. "전역 유효성 검사 디렉터리 매핑 선택"을 클릭합니다.
"전역 유효성 검사 디렉터리 매핑 선택" 페이지가 표시됩니다.
3. 해당 목록에서 유효성 검사 아이덴티티 매핑 개체를 선택합니다.
4. 제출을 클릭합니다.

선택한 유효성 검사 아이덴티티 매핑 개체가 유효성 검사 매핑의 전역 기본값으로 설정됩니다.

레거시 디렉터리 매핑 구성

레거시 디렉터리 매핑은 동일한 **DN** 또는 유니버설 **ID** 를 사용하여 인증 디렉터리를 권한 부여 또는 유효성 검사 디렉터리에 매핑합니다.

다음은 레거시 디렉터리 매핑 방법의 두 가지 유형입니다.

- **Auth/Az**(권한 부여 매핑)
- **AuthValidate**(유효성 검사 매핑)

Auth/Az 또는 **AuthValidate** 매핑이 구성된 경우 정책 서버는 먼저 세션 사용자 디렉터를 사용하여 사용자를 찾은 다음 세션 사용자 디렉터리에서 사용자를 찾을 수 없는 경우에만 지정된 매핑 메커니즘을 사용합니다.

인증 및 권한 부여 디렉터리 매핑을 구성하는 방법

Auth/Az 디렉터리 매핑 구성은 두 단계 프로세스로 수행됩니다.

1. 디렉터리 매핑을 구성합니다.
2. 영역에 권한 부여 디렉터를 할당합니다.

디렉터리 매핑 구성

한 디렉터리에 대해 사용자를 인증하고 다른 디렉터리에 대해 사용자에게 권한을 부여하려면 디렉터리 매핑을 구성하십시오.

다음 단계를 수행하십시오.

1. "인프라", "디렉터리"를 차례로 클릭합니다.
2. "Auth/Az 매핑"을 클릭합니다.
3. "디렉터리 매핑 만들기"를 클릭합니다.
4. 해당 목록에서 인증 및 권한 부여 디렉터를 선택합니다.
5. "동일한 DN" 또는 "유니버설 ID"를 선택합니다.

중요! 디렉터리 매핑은 유니버설 ID가 권한 부여 디렉터리의 단일 항목을 가리킬 때만 성공합니다.

6. 제출을 클릭합니다.

"디렉터리 매핑 만들기" 태스크가 처리를 위해 제출됩니다.

추가 정보:

[유니버설 ID](#) (페이지 226)

영역에 권한 부여 디렉터리 할당

영역에 디렉터리 매핑을 할당합니다. 정책 서버는 영역에 지정된 권한 부여 디렉터를 사용하여 사용자에게 권한을 부여합니다.

다음 단계를 수행하십시오.

1. 디렉터리 매핑을 할당할 영역을 엽니다.
2. "디렉터리 매핑" 목록에서 영역이 인증된 사용자를 권한 부여하는 데 사용할 수 있는 사용자 디렉터를 선택합니다.

기본값은 디렉터리 매핑이 없음을 나타냅니다. 인증 디렉터리는 사용자가 영역에 있는 리소스에 액세스를 시도할 때 권한 부여 디렉터리로 사용됩니다. 이 목록에는 기존 디렉터리 매핑에서 권한 부여 디렉터리로 구성된 사용자 디렉터리만 포함됩니다.

중요! 각 영역에 권한 부여 디렉터를 하나씩만 매핑할 수 있습니다.

3. 제출을 클릭합니다.

디렉터리 매핑이 저장됩니다. 이제 이 영역에 액세스하는 사용자는 정상적으로 인증되고 영역에 지정된 디렉터리에 대해 권한이 부여됩니다.

추가 정보:

[영역 구성](#) (페이지 561)

AuthValidate 디렉터리 매핑을 구성하는 방법

AuthValidate 디렉터리 매핑은 인증 및 권한 부여 디렉터리 매핑이 확장된 것입니다. 두 유형의 디렉터리 매핑을 모두 사용하면 사용자가 한 사용자 디렉터리에 대해 인증되고 다른 사용자 디렉터리에 대해서는 권한이 부여될 수 있습니다. 두 경우 모두 디렉터리 매핑 유형을 보다 세부적으로 "동일한 DN" 또는 "유니버설 ID"로 지정할 수 있습니다.

AuthValidate 디렉터리 매핑은 인증 및 권한 부여 디렉터리 매핑을 다음과 같은 세 가지 방식으로 확장합니다.

- AuthValidate 디렉터리 매핑을 사용하면 한 정책 서버에 연결된 인증 사용자 디렉터리를 다른 정책 서버에 연결된 유효성 검사 사용자 디렉터리에 매핑할 수 있습니다. 사용자 디렉터리는 OID 및 디렉터리 이름으로 찾습니다.
- AuthValidate 디렉터리 매핑을 사용하면 사용자 디렉터리의 유형이 다양해질 수 있습니다.
- AuthValidate 디렉터리 매핑을 사용하면 DN 기준 사용자 조회가 실패할 경우 유니버설 ID 기준 사용자 조회가 시도됩니다.

AuthValidate 디렉터리 매핑 구성

한 디렉터리에 대해 사용자를 인증하고 다른 디렉터리에 대해 사용자의 유효성을 검사하려면 AuthValidate 디렉터리 매핑을 구성하십시오.

참고: AuthValidate 매핑은 전역 설정입니다.

다음 단계를 수행하십시오.

1. "인프라", "디렉터리"를 차례로 클릭합니다.
2. "AuthValidate 디렉터리 매핑"을 클릭합니다.
3. "AuthValidate 디렉터리 매핑 만들기"를 클릭합니다.
4. "인증 디렉터리" 필드에 사용자를 인증하는 데 사용할 디렉터리의 이름을 입력합니다.
5. "유효성 검사 디렉터리" 목록에서 사용자의 유효성을 검사하는 데 사용할 디렉터를 선택합니다.
6. 사용 가능한 옵션에서 매핑된 DN 을 선택합니다.
7. 제출을 클릭합니다.

"AuthValidate 디렉터리 매핑" 태스크가 생성됩니다.

영역에서 디렉터리 매핑 제거

권한 부여 또는 유효성 검사 유형의 디렉터리 매핑을 업데이트 또는 삭제하려면 기존 영역에서 해당 디렉터리 매핑을 삭제하십시오.

다음 단계를 수행하십시오.

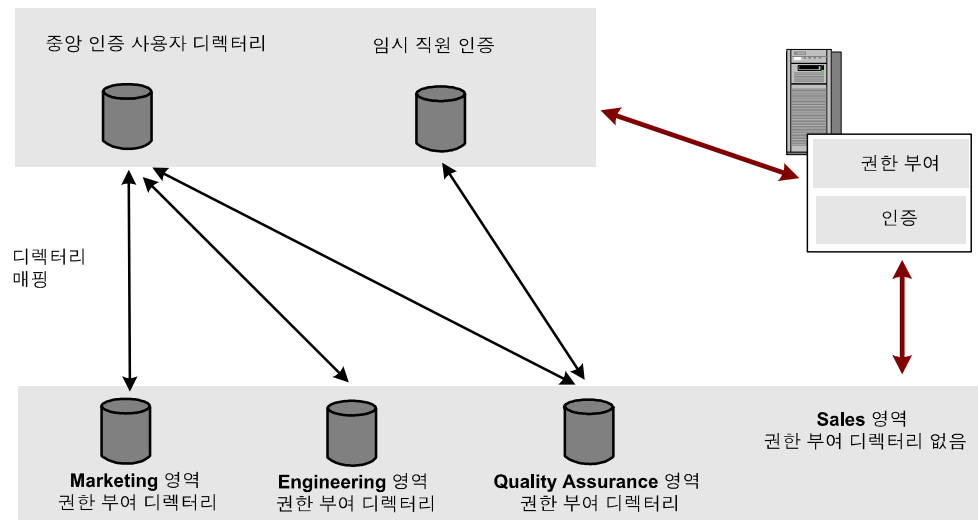
1. "정책", "도메인", "영역"을 클릭합니다.
2. 수정할 영역을 선택합니다.
3. "수정"을 클릭합니다.
4. 해당 목록에서 분리할 디렉터리 매핑을 선택합니다.
5. 제출을 클릭합니다.

디렉터리 매핑이 선택한 영역에서 제거됩니다.

동일한 절차를 수행하여 권한 부여 및 유효성 검사 유형의 아이덴티티 매핑을 영역에서 분리할 수 있습니다.

디렉터리 매핑 예

네트워크 리소스에 액세스할 수 있는 사용자를 인증하고 권한을 부여하기 위해서는 여러 디렉터리 매핑이 필요합니다. 다음 그림에서는 여러 디렉터리 매핑이 필요한 간단한 샘플 예를 보여 줍니다.



이 예에는 별개의 권한 부여 사용자 디렉터리가 있는 영역 세 개와 자체의 고유한 권한 부여 사용자 디렉터리가 없는 영역 하나가 있습니다. 사용자 인증 정보는 별개의 두 인증 디렉터리에서 유지됩니다. 요청한 리소스가 마케팅, 엔지니어링 또는 품질 보증 영역에 있을 경우 정책 서버는 인증 디렉터리 중 하나를 사용합니다. 이 결정은 세션 티켓 정보의 디렉터리에 기반합니다.

복잡한 사용자 검색 조건을 사용하여 디렉터리를 매핑하려면 아이덴티티 매핑을 사용할 수 있습니다.

추가 정보:

[영역](#) (페이지 555)

Engineering 영역 리소스에 대한 직원 액세스

여러 사용자 디렉터리가 표시된 앞의 그림에서 정규 직원에 대한 인증 데이터는 중앙 인증 사용자 디렉터리에 있습니다. 직원이 **Engineering** 영역의 리소스에 액세스를 시도하면 이 직원은 인증됩니다.

정책 서버는 **Engineering** 영역이 자체 권한 부여 디렉터를 사용하는 것을 인식합니다. 정책 서버는 중앙 인증 사용자 디렉터리와 **Engineering** 영역 권한 부여 사용자 디렉터리 간의 디렉터리 매핑을 찾습니다. 그런 다음 서버는 사용자 아이덴티티를 인증 디렉터리에 매핑합니다. 정책 서버는 이제 직원이 요청한 영역에 액세스할 수 있는지 여부를 확인할 수 있습니다.

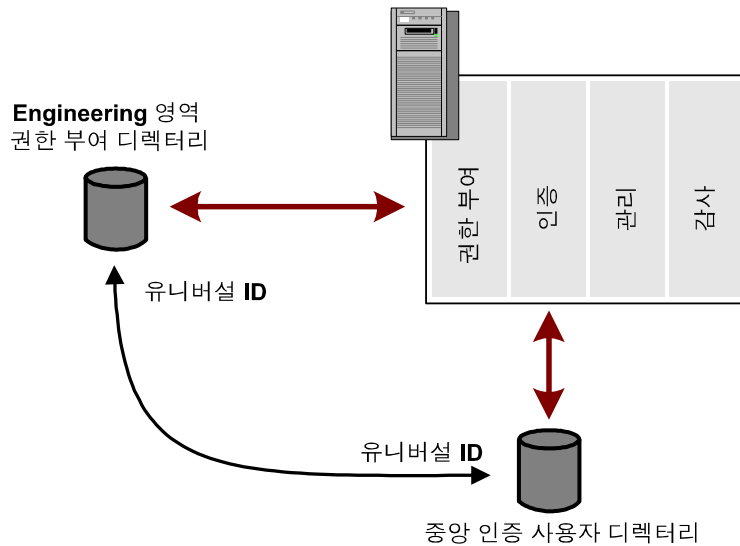
Quality Assurance 영역 리소스에 대한 임시 직원 액세스

여러 사용자 디렉터리가 표시된 앞의 그림에서 임시 직원에 대한 인증 데이터는 임시 직원 인증 사용자 디렉터리에 있습니다. 직원이 **Sales** 영역의 리소스에 액세스하려고 시도합니다. **Sales** 영역에는 고유한 권한 부여 디렉터리가 연결되어 있지 않습니다.

정책 서버는 인증 디렉터리의 직원을 인증한 다음 디렉터리 매핑이 설정되어 있는지 여부를 확인합니다. **Sales** 영역에는 고유한 권한 부여 디렉터리가 없으므로 정책 서버는 직원이 인증된 동일한 디렉터를 통해 직원에게 권한을 부여하려고 시도합니다.

유니버설 ID 기준 디렉터리 매핑

여러 사용자 디렉터리가 표시된 앞의 그림에서 직원에 대한 인증 데이터는 중앙 인증 사용자 디렉터리에 있습니다. 직원이 **Engineering** 영역의 리소스에 액세스하려고 시도합니다. 직원이 인증되면 정책 서버는 디렉터리 매핑을 사용하여 **Engineering** 인증 디렉터리에서 해당 직원을 찾습니다. 사용자는 직원 유니버설 ID로 식별됩니다. 다음 그림을 참조하십시오.



앞의 그림에서는 디렉터리 매핑에 유니버설 ID가 사용된다고 가정합니다. 권한 부여 디렉터리에서 일치하는 유니버설 ID를 찾기 위해 정책 서버는 인증 디렉터리에 정의된 유니버설 ID 특성을 사용합니다. 권한 부여 디렉터리에서 유니버설 ID를 찾은 후에는 정책 처리가 끝나고 사용자가 보호된 리소스에 액세스할 수 있는지 여부가 결정될 수 있습니다.

디렉터리 매핑 대/소문자 구분

Oracle 데이터베이스와 같은 대/소문자 구분 디렉터리에서는 값 "ROBIN"과 "robin"이 서로 다른 두 개의 사용자 이름으로 처리됩니다. LDAP 디렉터리 등의 다른 디렉터리에서는 대/소문자가 구분되지 않으므로 값 "Robin", "ROBIN", "robin" 및 "RobIn"이 모두 동일한 사용자 이름으로 처리됩니다. 인증 디렉터리가 대/소문자를 구분하지 않는데 권한 부여 디렉터리가 대/소문자를 구분하면 충돌이 발생할 수 있습니다.

인증 디렉터리가 대/소문자를 구분하기 때문에 인증이 실패할 수 있습니다. 하지만 사용자가 디렉터리가 요구하는 형식으로 사용자 이름을 다시 입력하면 인증이 성공합니다. 예를 들어 디렉터리에서 "Name"과 같은 형식의 사용자 이름을 사용해야 하는 경우 이름을 "Robin"으로 올바르게 다시 입력하면 됩니다. 대/소문자 구분 때문에 권한 부여가 실패하는 경우 정책 서버는 이를 해결할 방법이 없습니다.

권한 부여 디렉터리가 대/소문자를 구분하는 경우 인증된 사용자 이름의 형식을 권한 부여 디렉터리 형식과 일치하도록 변경하십시오. 인증된 사용자 이름이 "RoBiN"이지만 권한 부여 디렉터리에는 "Name" 형식이 필요한 경우 먼저 "RoBiN"을 "Robin"으로 변경한 다음 사용자에게 권한을 부여하십시오.

복잡한 사용자 검색 조건을 사용한 아이덴티티 매핑

아이덴티티 매핑은 세션 티켓 정보와 아이덴티티 매핑 항목의 구성을 기반으로 사용자를 찾습니다.

XPS 함수 `IDENTITY_MAP` 은 이름을 기준으로 아이덴티티 매핑 개체를 찾습니다. 해당 항목을 확인하여 대상 사용자 디렉터리에서 사용자를 찾으면 두 번째 매개 변수에 지정된 특성의 값이 반환됩니다.

예:

"target"이라는 이름의 아이덴티티 매핑에 정의된 대상 사용자 디렉터리에서 사용자의 성을 찾으려면 다음을 제공하십시오.

```
IDENTITY_MAP ("target", last_name);
```

디렉터리 매핑 및 응답

사용자 디렉터리 특성을 통합할 수 있는 응답을 구성할 수 있습니다. 디렉터리 매핑을 사용하는 경우에는 매핑이 응답에 미치는 영향을 고려하십시오. 예를 들어, `OnAuth` 이벤트의 경우 디렉터리 매핑은 인증 디렉터리에서 값을 가져옵니다. `OnAccess` 이벤트의 경우 디렉터리 매핑은 권한 부여 디렉터리에서 값을 가져옵니다. 응답과 관련된 이벤트에 대한 설명은 [응답 및 응답 그룹](#) (페이지 589)을 참조하십시오.

제 8 장: 인증 체계

이 섹션은 다음 항목을 포함하고 있습니다.

- [인증 체계 개요](#) (페이지 287)
- [기본 인증 체계를 구성하는 방법](#) (페이지 295)
- [SSL 을 통한 기본 인증 체계를 구성하는 방법](#) (페이지 297)
- [HTML 양식 인증을 구성하는 방법](#) (페이지 300)
- [Windows 인증 체계](#) (페이지 331)
- [Kerberos 인증을 구성하는 방법](#) (페이지 335)
- [정보 카드 인증 체계](#) (페이지 351)
- [RADIUS CHAP/PAP 인증 체계](#) (페이지 372)
- [RADIUS 서버 인증 체계](#) (페이지 374)
- [SafeWord 서버 인증 체계](#) (페이지 375)
- [SafeWord 서버 및 HTML 양식 인증 체계](#) (페이지 377)
- [SecurID 인증 체계](#) (페이지 378)
- [X.509 클라이언트 인증서 인증 체계](#) (페이지 389)
- [X.509 클라이언트 인증서 및 기본 인증 체계](#) (페이지 393)
- [X.509 인증서 또는 기본 인증 체계](#) (페이지 395)
- [X.509 클라이언트 인증서 및 HTML 양식 인증 체계](#) (페이지 398)
- [X.509 클라이언트 인증서 또는 HTML 양식 인증 체계](#) (페이지 401)
- [익명 인증 체계](#) (페이지 404)
- [사용자 지정 인증 체계](#) (페이지 406)
- [OAuth 인증 체계를 구성하는 방법](#) (페이지 408)
- [OpenID 인증 체계](#) (페이지 422)
- [레거시 페더레이션 인증 체계](#) (페이지 435)
- [가장 인증 체계](#) (페이지 435)

인증 체계 개요

일반적으로 네트워크 리소스의 소유자는 이러한 리소스를 액세스하려고 시도하는 사용자의 아이덴티티가 정상인지 확인하길 원합니다. 사용자를 식별하면 사용자가 액세스할 수 있는 리소스가 결정되고 해당 사용자의 콘텐츠를 개인화하는 방법이 결정됩니다. 익명 사용자를 고유하게 추적하면 이 사용자가 네트워크에 다시 액세스할 때 해당 사용자 기록을 사용하여 높은 품질의 서비스를 제공할 수 있으므로 유용합니다. 사용자를 식별하기 위해 인증 체계가 사용됩니다.

인증 체계를 사용하면 자격 증명을 수집하고 사용자의 아이덴티티를 확인할 수 있습니다. 인증 중 웹 에이전트는 정책 서버와 통신하여 자격 증명이 올바른지 확인합니다. 이 자격 증명은 리소스를 요청하는 사용자에게서 가져와야 합니다.

정책 서버는 여러 인증 체계를 지원합니다. 리스크가 낮은 네트워크 리소스에는 간단한 체계를 사용하고 중요 네트워크 리소스에는 보안이 강력한 복잡한 체계를 사용하십시오.

정책 서버는 정책 서버에게 체계를 처리하는 데 필요한 정보를 제공하는 인증 체계 템플릿을 사용합니다. 관리 UI 를 사용하여 인증 체계 템플릿을 구성하십시오.

지원되는 인증 체계 및 암호 정책

일부 인증 체계 유형은 암호 정책을 지원합니다. 관리 UI 에서 "인증 체계 속성" 대화 상자를 열어 특정 인증 체계 유형이 암호 정책을 지원하는지 여부를 확인할 수 있습니다. 특정 인증 체계 유형을 보려면 "체계 일반 설정" 그룹 상자의 드롭다운 목록에서 유형을 선택하십시오. "이 인증 체계에 대해 암호 정책 사용" 확인란을 봅니다. 인증 체계에서 암호 정책을 지원하지 않는 경우 확인란 설명이 흐리게 표시되고 확인란을 사용할 수 없습니다.

다음 표에는 지원되는 인증 체계 유형 및 암호 정책 지원 유무가 나열되어 있습니다.

인증 체계 유형	암호 정책 지원 여부
익명	아니요
기본	예
SSL 을 통한 기본 인증	예
사용자 지정	예
HTML 양식	예
가장	아니요
OAuth	아니요
OpenID	아니요
RADIUS CHAP/PAP	예

인증 체계 유형	암호 정책 지원 여부
RADIUS 서버	예
SafeWord	아니요
SafeWord 및 HTML 양식	아니요
SecurID	아니요
SecurID 및 HTML 양식	아니요
X.509 클라이언트 인증서	아니요
X.509 클라이언트 인증서 및 기본	예
X.509 클라이언트 인증서 또는 기본	예
X.509 클라이언트 인증서 및 HTML 양식	예
X.509 클라이언트 인증서 또는 HTML 양식	예
Windows 인증	예

인증 중 정책 서버 검색을 단일 사용자 저장소로 제한

단일 사용자가 정책 도메인과 연결된 여러 사용자 디렉터리 또는 데이터베이스에 저장될 수 있습니다. 이 사용자의 암호는 각 사용자 저장소에서 동일합니다. 인증 프로세스 중에 정책 서버는 사용자가 한 사용자 저장소에서 비활성화되어 있음을 발견할 수 있습니다. 하지만 기본적으로 해당 정책 도메인과 관련된 모든 저장소의 사용자에게 대한 검색이 계속됩니다. 연결된 모든 사용자 저장소에서 해당 사용자가 비활성화된 경우에만 사용자 인증이 실패합니다. 연결된 사용자 저장소 중 어느 하나에서든 해당 사용자가 활성화되어 있는 경우에는 사용자가 인증됩니다.

이 기본 동작은 구성할 수 있습니다. 사용자 저장소에서 비활성화된 사용자를 찾으려면 정책 서버가 디렉터리 검색을 중지하도록 하십시오.

다음 단계를 수행하십시오.

1. 레지스트리 키 ReturnOnDisabledUser 를 추가합니다.

Windows

다음 위치에 레지스트리 키 ReturnOnDisabledUser 를 추가합니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion  
PolicyServer
```

Solaris

sm.registry 파일에 다음 행을 추가합니다.

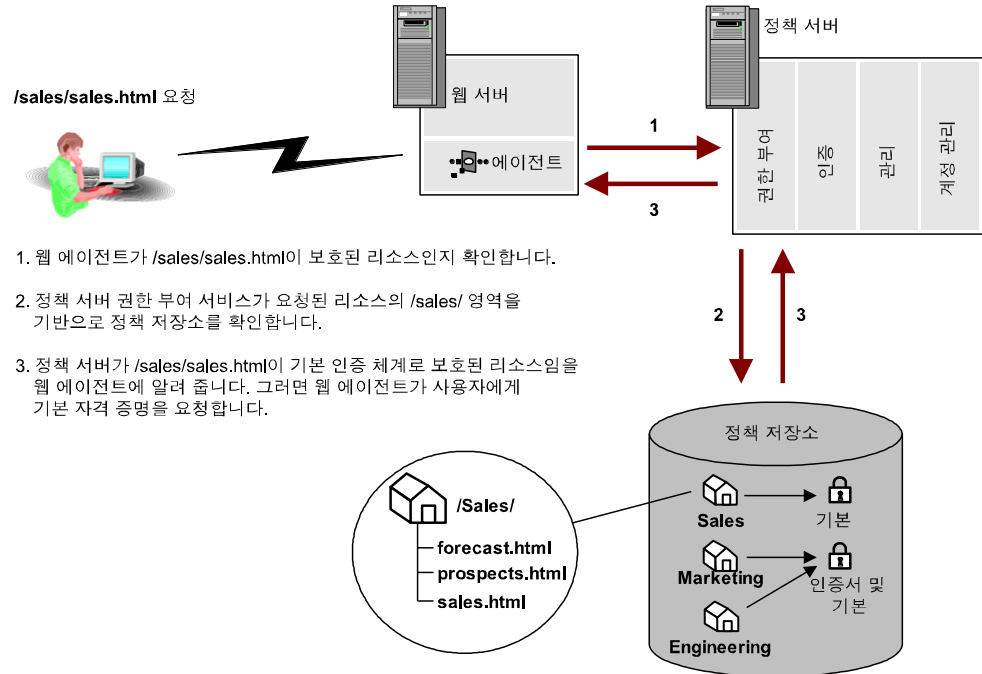
```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion  
PolicyServer  
ReturnOnDisabledUser=0x1; REG_DWORD
```

2. ReturnOnDisabledUser 에 값 1 을 할당합니다.

인증 체계 처리

사용자의 아이덴티티를 파악하기 위해 정책 서버는 해당 리소스가 있는 영역에 대한 인증 체계를 사용합니다. 인증 체계는 사용자가 인증을 위해 제공해야 하는 자격 증명과 정책 서버가 사용자 아이덴티티의 유효성을 검사하는 데 사용하는 방법을 지정합니다.

인증 체계를 구성하려면 관리 UI 를 사용하여 영역에 체계를 할당하십시오. 다음 다이어그램에서는 사용자가 보호된 리소스에 액세스하려고 할 때 인증 체계가 호출되는 방식을 보여 줍니다.



위의 예에서 사용자는 /Sales/ 영역의 보호된 리소스인 sales.html 을 요청합니다. 이 영역에는 기본 인증이 필요합니다. 정책 서버는 웹 에이전트에게 리소스가 보호되어 있음을 알리고 웹 에이전트를 통해 사용자에게 기본 자격 증명을 요구합니다. 에이전트는 사용자에게 사용자 이름과 암호를 묻습니다.

추가 정보:

[영역 구성](#) (페이지 561)

인증 컨텍스트 데이터 유지

정책 서버는 인증 컨텍스트 데이터를 세션 저장소에 유지할 수 있습니다. 데이터를 세션 저장소에 저장하는 것은 일부 인증 체계의 선택적 기능입니다. 세션 저장소는 사용자 데이터를 저장하기 위해 세션 티켓 외에 추가적으로 사용할 수 있는 또 다른 리포지토리입니다.

정책 서버는 세션 변수를 생성하고 이를 세션 변수에 따라 명명된 세션 티켓 필드로 처리합니다. 정책 서버는 세션 저장소의 세션 변수에 액세스하고 인증 결정에 영향을 줄 수 있습니다.

유지된 인증 데이터에서 세션 컨텍스트 특성을 조작, 저장 또는 다시 전송할 수 있도록 응답 및 정책을 구성할 수 있습니다. 정보는 세션 저장소에서 검색되고 웹 에이전트로 전송됩니다. 웹 에이전트는 데이터를 다시 저장하거나, 평가를 위해 권한 부여 엔진에 데이터를 제공할 수 있습니다. 또한 고유한 세션 변수를 구성하여 권한 부여에 사용할 수 있습니다.

인증 컨텍스트 정보를 저장하려면 인증 체계 구성의 "체계 설정" 섹션에서 "인증 세션 변수 유지" 확인란을 선택하십시오. 이 옵션은 다음 체계에 사용할 수 있습니다.

- 사용자 지정 체계
- SAML 인증 체계
- OpenID 인증 체계
- OAuth 인증 체계
- X.509 인증서 체계

중요! 세션 저장소에 인증 데이터를 유지하면 인증 시 성능 저하가 발생합니다. 나중에 인증 결정을 위해 변수를 사용하려는 경우에만 이 옵션을 선택하십시오. 그렇지 않으면 아무런 이점 없이 성능에 상당한 영향을 미칠 수 있습니다.

보호 수준

인증 체계에는 보호 수준이 필요합니다. 이 수준의 범위는 0에서 1000 사이입니다. 숫자가 높을수록 체계에서 더 높은 보호 수준을 제공합니다. 사용자가 체계에 대해 성공적으로 인증되면 보호 수준이 현재 인증 체계와 같거나 낮은 모든 리소스에 액세스할 수 있습니다. 이 경우에도 사용자가 리소스에 액세스하려면 권한이 부여되어야 합니다.

참고: 익명 인증 체계에서는 보호 수준이 항상 0입니다. 사용자 지정 체계의 보호 수준은 0에서 1000 사이입니다. 다른 모든 인증 체계의 보호 수준은 1에서 1000 사이입니다.

예를 들어 모든 네트워크 사용자가 사용할 수 있는 리소스 집합의 경우 기본(사용자 이름 및 암호) 인증 체계를 할당할 수 있습니다. 회사 경영진만 사용할 수 있는 수익 정보의 경우 보호 수준이 더 높은 X.509 클라이언트 인증서 체계를 할당할 수 있습니다. 사용자 이름 및 암호를 사용하여 인증된 사용자는 두 번째에 디지털 인증서로 인증되어 수익 정보에 액세스할 수 있습니다.

경우에 따라 인증 체계의 미리 정의된 보호 수준만으로는 불충분할 수 있습니다. 예를 들어 페더레이션 시나리오에서 어설션 당사자는 신뢰 당사자를 수용하기 위해 다른 보호 수준이 필요할 수 있습니다. 이 경우 관리자는 인증 체계 라이브러리의 보호 값이 UI에 지정된 보호 수준을 재정의하도록 지정할 수 있습니다. 라이브러리의 값은 사용자 세션 티켓에 기록됩니다. 사용자 지정 및 SAML 인증 체계의 경우 "인증 체계 만들기" 대화 상자의 "체계 일반 설정" 섹션에서 "보호 무시 허용" 확인란을 선택하십시오.

인증 체계 및 자격 증명 요구 사항

다음 표에는 지원되는 모든 인증 체계와 해당 자격 증명 요구 사항이 나와 있습니다.

자격 증명 요구 사항					
인증 체계	디렉터리 사용자 이름	디렉터리 암호	토큰의 코드	X.509 인증서	사용자 프로필 특성
익명					
기본	예	예			
SSL을 통한 기본 인증	예	예			
사용자 지정	선택 사항	선택 사항	선택 사항	선택 사항	선택 사항
HTML 양식(필요한 경우 SSL 사용)	사용자 지정 자격 증명	사용자 지정 자격 증명			선택 사항
가장	예				선택 사항
NTLM 또는 Windows	예*	예*			

자격 증명 요구 사항					
인증 체계	디렉터리 사용자 이름	디렉터리 암호	토큰의 코드	X.509 인증서	사용자 프로필 특성
RADIUS CHAP/PAP	예	예			
RADIUS 서버	예	예			
SafeWord 서버	예	예			
SafeWord 및 양식	예	예			선택 사항
SecurID	예		예		
SecurID 및 양식	예		예		선택 사항
TeleID	예		예		
X.509 클라이언트 인증서				예	
X.509 클라이언트 인증서 및 기본(SSL 사용)	예	예		예	
X.509 클라이언트 인증서 또는 기본(필요한 경우 SSL 사용)	예(기본의 경우)	예(기본의 경우)		예(인증서의 경우)	
X.509 클라이언트 인증서 및 HTML 양식	사용자 지정 자격 증명	사용자 지정 자격 증명		예	선택 사항
X.509 클라이언트 인증서 또는 HTML 양식	HTML 양식용 사용자 지정 자격 증명	HTML 양식용 사용자 지정 자격 증명		예(인증서의 경우)	선택 사항(HTML 양식의 경우)

*NTLM 또는 Windows 를 사용하여 리소스에 액세스하는 경우 정책 서버는 사용자에게 사용자 이름과 암호를 입력하도록 요청하지 않습니다. 이 체계를 사용하려면 IIS 웹 서버가 사용자의 자격 증명을 받아 확인할 수 있도록 올바르게 구성되어 있어야 합니다. 정책 서버는 권한 부여를 결정할 때 IIS 서버가 어설션한 사용자의 아이덴티티를 기반으로 합니다.

단일 인증 체계 구성의 여러 인스턴스

관리 UI 에서 대부분의 인증 체계에 대한 여러 인스턴스를 구성할 수 있습니다. 예를 들어 로그인, 잊어버린 암호 요청, 로그아웃을 처리하기 위해 여러 HTML 양식 기반 체계를 만들 수 있습니다. 체계 유형의 여러 인스턴스를 만드는 경우 보안 요건에 맞게 보호 수준을 설정하십시오.

기본 인증 체계를 구성하는 방법

정책 서버 설치 중에는 기본 인증 체계가 자동으로 구성됩니다. 이 체계는 인증을 위해 사용자 디렉터리 서비스에 전달된 사용자 이름 및 암호에 따라 사용자 아이덴티티를 확인합니다. 기본 인증 체계에서는 ASCII 문자만 지원합니다.

사용자가 기본 인증으로 보호된 리소스에 액세스하려고 하면 웹 에이전트는 사용자에게 사용자 이름과 암호를 입력하라는 메시지를 표시합니다. 사용자가 이름과 암호를 입력하면 에이전트는 암호화된 연결을 통해 정책 서버에 이 자격 증명을 전달합니다. 정책 서버는 자격 증명을 처리하여 성공하는 경우 웹 에이전트가 액세스를 허가하도록 지시합니다. 인증에 실패할 경우 사용자는 자격 증명을 다시 입력해야 합니다.

참고: 기본적으로 이 체계에서는 브라우저에서 웹 에이전트로 전달되는 자격 증명을 암호화하지 않습니다. 데이터를 전달하기 위해 표준 HTTP 기본 프로토콜이 사용됩니다. 그러나 웹 에이전트와 정책 서버 간의 통신은 항상 암호화된 연결을 통해 이루어집니다. 간단한 사용자 이름 및 암호를 기반으로 하는 암호화된 인증 체계에 대한 자세한 내용은 SSL 을 통한 기본 인증 체계를 참조하십시오.

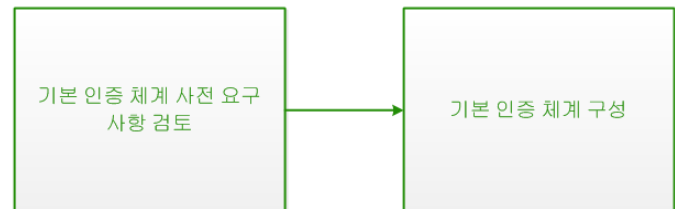
기본적으로 관리 UI 에서 생성하는 응용 프로그램과 영역에는 기본 인증 체계가 사용됩니다. 이 인증 체계를 변경할 수 있습니다.

영어가 아닌 영역 이름을 표시하고 기본 인증 창에서 로그인 자격 증명으로 영어가 아닌 문자를 입력할 수 있도록 하려면 다음 조건이 충족되는지 확인하십시오.

- Windows 웹 서버에서 IIS 및 Apache 에 대한 웹 브라우저로 Internet Explorer 만 사용하십시오.
- 웹 서버 컴퓨터의 로캘은 웹 브라우저의 로캘과 일치해야 합니다.



정책 관리자



기본 인증 체계를 구성하려면

1. [기본 인증 체계 사전 요구 사항을 검토](#) (페이지 296)합니다.
2. [기본 인증 체계를 구성](#) (페이지 297)합니다.

기본 체계 사전 요구 사항 검토

기본 인증 체계를 구성하기 전에 다음 사전 요구 사항을 충족하는지 확인하십시오.

- 클라이언트 사용자 이름 및 암호 정보가 사용자 디렉터리에 있어야 합니다.
- 정책 서버와 사용자 디렉터리 간에 디렉터리 연결이 있어야 합니다.

추가 정보:

[사용자 디렉터리](#) (페이지 147)

기본 인증 체계 구성

관리 UI에서 기본 인증 체계를 구성하여 사용자 디렉터리에 있는 사용자 이름과 암호를 기준으로 사용자 아이덴티티를 확인할 수 있습니다.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다.

다음 단계를 수행하십시오.

1. "인프라", "인증"을 차례로 클릭합니다.
2. "인증 체계"를 클릭합니다.
3. "인증 체계 만들기"를 클릭합니다.
"인증 체계 유형의 새 개체 만들기"가 선택되어 있는지 확인합니다.
"확인"을 클릭합니다.
4. 이름 및 보호 수준을 입력합니다.
5. "인증 체계 유형" 목록에서 "기본 템플릿"을 선택합니다.
6. "제출"을 클릭합니다.
인증 체계가 저장되고 이제 영역에 할당할 수 있습니다.

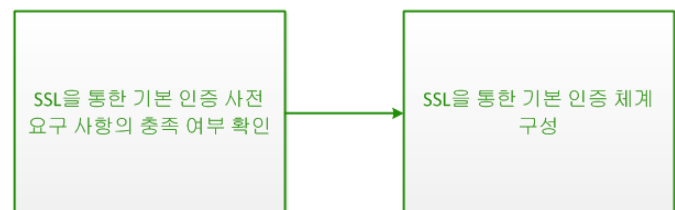
SSL을 통한 기본 인증 체계를 구성하는 방법

SSL을 통한 기본 인증 체계에서는 사용자 이름 및 암호 자격 증명을 사용자 디렉터리에 전달하여 사용자 아이덴티티를 확인합니다. 이 프로세스는 기본 인증과 유사하지만 자격 증명 전달은 항상 암호화된 SSL(Secure Sockets Layer) 연결을 통해 수행됩니다. SSL 연결은 보호된 URL이 SSL을 요청하도록 설정되지 않은 경우에도 사용됩니다.

참고: SSL을 통한 기본 인증 체계에서는 ASCII 문자만 지원합니다.



정책 관리자



1. [SSL 을 통한 기본 인증 체계의 사전 요구 사항을 충족하는지 확인](#) (페이지 298)
2. [SSL 을 통한 기본 인증 체계 구성](#) (페이지 298)

SSL 을 통한 기본 인증 체계 사전 요구 사항 확인

SSL 을 통한 기본 인증 체계를 구성하기 전에 다음 사전 요구 사항이 충족되는지 확인하십시오.

- 클라이언트 사용자 이름 및 암호가 사용자 디렉터리에 있어야 합니다.
- 정책 서버와 사용자 디렉터리 간에 디렉터리 연결이 있어야 합니다.
- SSL 웹 서버에 X.509 서버 인증서가 설치되어 있고 SSL 이 구성되어 있어야 합니다.
- 네트워크가 HTTPS 프로토콜을 사용하는 클라이언트 브라우저에 대한 SSL 연결을 지원해야 합니다.
- 요청이 SSL 을 위해 리디렉션되는 웹 서버에 웹 에이전트가 설치되어 있어야 합니다. 웹 에이전트는 서버가 인증 체계가 요구하는 .scc MIME 유형을 처리할 수 있도록 해 줍니다.

추가 정보:

[사용자 디렉터리](#) (페이지 147)

SSL 을 통한 기본 인증 체계 구성

사용자 디렉터리에 있는 사용자 이름과 암호를 기준으로 사용자 아이덴티티를 확인하려면 SSL 을 통한 기본 인증 체계를 사용하십시오. 자격 증명은 암호화된 SSL(Secure Sockets Layer) 연결을 통해 전송됩니다.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다.

다음 단계를 수행하십시오.

1. "인프라", "인증"을 차례로 클릭합니다.
2. "인증 체계"를 클릭합니다.

3. "인증 체계 만들기"를 클릭합니다.
"인증 체계 유형의 새 개체 만들기"가 선택되어 있는지 확인합니다.
"확인"을 클릭합니다.
4. 이름과 설명(선택 사항)을 입력합니다.
5. 보호 수준을 선택합니다.
6. "인증 체계 유형" 목록에서 "SSL을 통한 기본 인증 템플릿"을 선택합니다.
7. 다음 체계 관련 필드를 채웁니다.

서버 이름

SSL 연결 설정을 수행하는 웹 서버의 정규화된 도메인 이름을 지정합니다. 이 서버는 웹 에이전트가 설치된 서버와 동일할 수도 있지만 일반적으로는 동일하지 않습니다.

참고: IP 주소는 지원되지 않습니다.

이 서버는 정책 서버가 SSL 연결을 통해 사용자 자격 증명을 리디렉션하는 데 사용하는 URL의 시작 부분이 됩니다.

도메인 이름에는 마침표가 두 개 이상 있어야 합니다. 서버를 다음 형식으로 입력합니다.

servername.domainname.com

예: server1.example.com

Port

SSL 서버가 수신 대기하는 포트를 지정합니다. 이 값은 기본이 아닌 포트를 통해 통신하는 경우에만 필요합니다.

대상

SSL 자격 증명 수집기(SCC)의 경로 및 이름을 지정합니다.

대상 값은 SCC 를 호출하는 데 사용할 항목을 에이전트에 알려 줍니다. 대상은 정책 서버가 SSL 연결을 통해 사용자 자격 증명을 리디렉션하는 데 사용하는 URL 의 끝 부분이 됩니다. SSL 을 통한 기본 인증을 지원하기 위해 프록시 서버에 특정 URL 이 필요한 경우 대상을 사용자 지정할 수 있습니다.

"대상" 필드의 기본값은 다음과 같습니다.

`/siteminder/nocert/smgetcred.scc`

8. 제출을 클릭합니다.

인증 체계가 저장됩니다. 이제 응용 프로그램이나 영역에 이 체계를 할당할 수 있습니다.

HTML 양식 인증을 구성하는 방법

HTML 양식 인증 체계는 사용자 지정 HTML 양식에서 수집된 자격 증명을 사용하여 사용자를 인증합니다. 이 유연한 자격 증명 수집 방법을 사용하면 다음과 같은 이점이 있습니다.

- 회사 로고 등을 포함한 "브랜드된" 화면 표시를 제공할 수 있습니다.
- 사용자 이름 및 암호 수집에 사용자 지정 레이블을 대신 사용할 수 있습니다. 예를 들어 사용자가 이름 및 암호보다는 계정 번호 및 PIN 과 관련된 것으로 인식하는 경우 이 기능을 사용할 수 있습니다.
- 사용자 디렉터리 특성을 사용하여 사용자 이름과 암호가 아닌 다른 자격 증명을 기반으로 하는 인증을 제공할 수 있습니다. 정책 서버 시스템의 인증 체계 라이브러리가 사용자 데이터를 DN 에 매핑합니다. 사용자를 DN 에 매핑하면 정책 서버가 특성 목록을 사용자 디렉터리의 해당 값과 일치시킬 수 있습니다. 이 프로세스를 백엔드 매핑이라고 합니다.

- 사용자 이름과 암호 외에 다른 사용자 특성도 포함된 자격 증명을 기반으로 하는 인증을 제공할 수 있습니다. 특성 확인에는 사용자 지정 인증 체계 라이브러리가 필요하지 않습니다. 예를 들어 암호를 잊어버린 사용자를 위해 사용자 지정 양식을 사용하여 이름과 암호 구를 수집할 수 있습니다.
- 로그인, 로그아웃, 잊어버린 암호를 위한 여러 HTML 양식을 제공할 수 있습니다.

참고: HTML 양식 인증 체계에는 멀티바이트 문자를 사용할 수 있습니다.

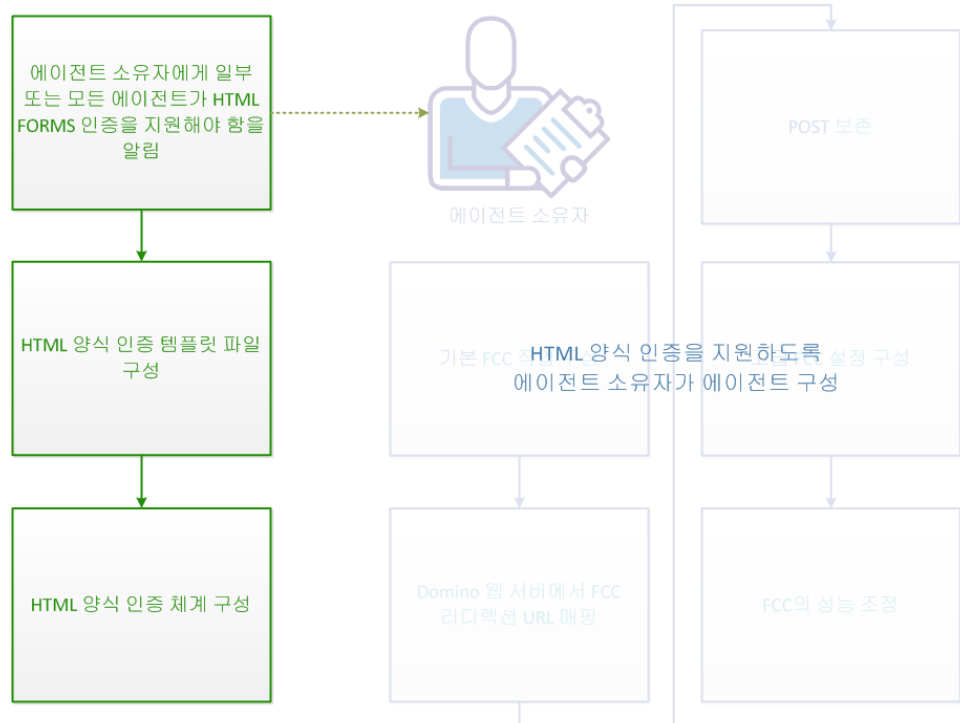
HTML 양식 인증이 SSL(Secure Sockets Layer) 연결을 통해 실행되도록 구성할 수 있지만 이것은 선택 사항입니다.

정책 서버가 HTML 양식 인증을 사용하여 사용자 아이덴티티의 유효성을 검사하도록 구성하려면 정책 관리자와 에이전트 소유자가 모두 구성 프로세스를 수행해야 합니다. 이 시나리오에서는 정책 관리자가 HTML 양식 인증을 구성하기 위해 따라야 하는 프로세스를 보여 줍니다.

참고: 웹 에이전트에서 HTML 양식 인증을 지원하도록 구성하는 방법에 대한 자세한 내용은 관련 시나리오 *웹 에이전트에서 HTML 양식 인증을 지원하도록 구성*을 참조하십시오.



정책 관리자



1. [에이전트 소유자에게 일부 또는 모든 에이전트가 HTML 양식 인증을 지원해야 한다고 알림](#) (페이지 303)
2. [HTML 양식 인증 템플릿 파일 구성](#) (페이지 303)
3. [HTML 양식 인증 체계 구성](#) (페이지 314)

에이전트 소유자에게 HTML 양식 인증이 필요하다고 알림

이 시나리오에 간략하게 설명된 단계 외에도 에이전트 소유자는 에이전트에서 HTML 양식 인증 체계를 사용하여 아이덴티티의 유효성을 검사하도록 구성해야 합니다.

에이전트에서 HTML 양식 인증 체계를 사용하도록 구성해야 함을 에이전트 소유자 또는 담당자에게 알리십시오.

HTML 양식 인증 템플릿 파일 구성

웹 에이전트에는 HTML 양식 인증을 처리하는 *FCC(양식 자격 증명 수집기)* 구성 요소가 있습니다. 사용자가 HTML 양식 체계로 보호되는 리소스를 요청하면 에이전트는 사용자를 양식 인증 템플릿 파일로 리디렉션합니다.

양식 인증 템플릿 파일은 FCC 를 호출합니다. 그런 다음 FCC 는 양식 인증 템플릿 파일의 내용을 기반으로 하는 브라우저 페이지를 생성합니다. 템플릿 파일은 웹 서버의 네임스페이스에 있으며 다른 HTML 파일과 동일한 방식으로 액세스됩니다.

양식 인증 템플릿 파일은 HTML 과 일부 사용자 지정 표기법을 포함하는 간단한 마크업 언어로 작성됩니다.

템플릿 FCC 파일은 다음 디렉터리에 있습니다.

- Windows: webagent\samples\forms
- UNIX: webagent/samples/forms

이러한 샘플 양식 인증 템플릿 파일을 사용하려면 [HTML 양식 인증 체계를 구성](#) (페이지 315)할 때 적절한 대상 디렉터리를 지정하십시오.

또한 여러 기타 언어로 로컬라이즈된 샘플 양식 인증 템플릿 파일이 제공됩니다. 기본적으로 SiteMinder 에는 영어 양식 인증 템플릿 파일이 사용됩니다. 로컬라이즈된 양식 인증 템플릿을 구성하는 방법에 대한 자세한 내용은 [FCC 국제화를 활성화하는 방법](#) (페이지 317)을 참조하십시오.

추가 정보:

[양식 기반 인증 및 기본 암호 서비스 파일 로컬라이즈](#) (페이지 325)

보안 HTML 양식 인증 템플릿 사용

보안 버전의 HTML 양식 인증 템플릿을 사용할 수도 있습니다. 보안 HTML 양식 인증 템플릿과 표준 버전에는 다음과 같은 차이점이 있습니다.

- 보안 버전은 반환되는 메시지에 사용자 이름을 표시하지 않습니다.
- 보안 버전의 경우 양식 템플릿의 오른쪽 위에는 사용자를 로그아웃시키고 사용자 지정 로그오프 페이지로 리디렉션하는 "로그아웃" 하이퍼링크가 있습니다.
- 보안 버전의 모든 텍스트 필드에는 자동 완성 기능이 해제되어 있습니다.

사용자 지정할 수 있는 기본 보안 템플릿 파일은 다음 디렉터리에 위치합니다.

- Windows: `webagent\secureforms`
- UNIX: `webagent/secureforms`

보안 버전의 HTML 양식 인증 템플릿을 사용하려면 `secureforms` 디렉터리의 파일을 다음 위치에 복사하여 표준 버전을 대체하십시오.

- Windows: `webagent\samples\forms`
- UNIX: `webagent/samples/forms`

또한 미국 영어(en-US) 로캘의 보안 양식 집합은 다음 디렉터리에서 사용할 수 있습니다.

- Windows: `webagent\secureforms_en-US`
- UNIX: `webagent/secureforms_en-US`

보안 버전의 미국 영어 로캘 양식을 사용하려면 `secureforms_en-US` 디렉터리의 파일을 다음 위치에 복사하여 표준 버전을 대체하십시오.

- Windows: `webagent\samples\forms_en-US`
- UNIX: `webagent/samples/forms_en-US`

추가 정보:

[양식 기반 인증 및 기본 암호 서비스 파일 로컬라이즈](#) (페이지 325)

양식 인증 템플릿 파일에 다른 파일 확장명 사용

양식 인증 템플릿 파일의 기본 확장명은 .fcc 입니다. 따라서 양식 인증 템플릿 파일을 .fcc 파일이라고도 합니다. 그러나 다음과 같이 다른 확장명을 사용할 수도 있습니다.

다음 단계를 수행하십시오.

- Apache 웹 서버의 경우 원하는 확장명을 사용하도록 웹 서버를 구성합니다.

참고: 자세한 내용은 *웹 에이전트 설치 안내서*를 참조하십시오.

- Domino 또는 IIS 웹 서버의 경우 웹 에이전트 구성 파일이나 웹 에이전트 구성 개체의 FCCExtensions 매개 변수에 원하는 확장명을 지정합니다.

참고: 웹 에이전트 구성 매개 변수에 대한 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.

양식 인증 템플릿 사용자 지정

양식 인증 템플릿 파일(.fcc)은 표준 HTML 태그와 약간의 전용 표기법을 사용하여 작성됩니다. 이러한 표기법은 특성을 확인하고 사용자 지정 기능을 사용하는 데 필요합니다.

중요! Windows 시스템에서 .fcc 파일을 생성하거나 편집하고 해당 파일을 UNIX 시스템으로 이동할 경우 파일에 UNIX 시스템과 호환되지 않는 줄 바꿈 문자가 추가될 수 있습니다. UNIX 시스템에서 비 UNIX 줄 바꿈 문자가 사용되면 인증 중에 .fcc 파일에서 오류가 발생합니다. 따라서 Windows 텍스트 편집기에서 생성한 파일을 UNIX 시스템으로 이동한 경우에는 파일을 검사하여 추가된 문자를 제거하십시오. 이 문제를 방지하려면 UNIX 환경에서 사용할 .fcc 파일은 UNIX 시스템에서 생성하고 편집하십시오.

FCC의 첫 번째 부분에는 .fcc 파일에서 POST 작업을 실행하는 동안 사용되는 지시문이 포함됩니다. 이 지시문은 클라이언트에 전달되지 않습니다. 이 지시문은 파일의 시작 부분에 @name=value 형식으로 있어야 합니다.

여기서 name은 변수의 이름입니다. value는 변수의 값입니다. value에는 %name1% 형식의 문자열이 포함될 수 있습니다. FCC는 이 문자열을 name1과 연결된 변수의 값으로 대체합니다.

.fcc 파일의 두 번째 부분에는 .fcc 파일에서 GET 작업을 수행할 때 반환되는 HTML 코드가 포함됩니다. 이 부분에는 FCC가 name과 연결된 값으로 대체하는 "\$\$name\$\$" 형식의 텍스트(큰따옴표(") 포함)가 포함될 수 있습니다. name은 대/소문자를 구분하지 않습니다.

다음 표에서 숨겨진 입력에는 자격 증명 수집기의 상태가 포함됩니다. 각 값과 함께 큰따옴표(")를 포함하십시오.

이름	동적 값	유지되는 데이터
target	"\$\$target\$\$"	사용자가 액세스하려고 하는 리소스
smauthreason	"\$\$smauthreason\$\$"	로그인 실패 원인
postpreservationdata	"\$\$postpreservationdata\$\$"	사용자가 Post 요청을 통해 제출하는 데이터
smagentname	"\$\$smagentname\$\$"	사용자 로그인에 사용되는 에이전트 이름

.fcc 파일에는 최소한 다음 항목이 수집되어야 합니다.

- 사용자 이름
- 암호
- 대상

중요! 사용자가 다음 목록의 인증 체계로 보호되는 리소스에 대해 POST 요청을 제출할 경우 **postpreservationdata** 입력을 사용해야 합니다. 그렇지 않으면 요청된 리소스에 대해 사용자가 포스트하려고 하는 데이터가 손실됩니다.

체계

SSL을 통한 기본 인증 체계

HTML 양식 인증 체계

X.509 클라이언트 인증서 인증 체계

X.509 클라이언트 인증서 및 기본 인증 체계

X.509 인증서 또는 기본 인증 체계

체계

X.509 클라이언트 인증서 및 HTML 양식 인증 체계

X.509 클라이언트 인증서 또는 HTML 양식 인증 체계

다음은 간단하지만 유효한 .fcc 파일의 예입니다.

양식 데이터를 기반으로
사용자 이름 생성

사용자 암호 수집

사용자 조직 수집

```
@username=uid=%USER%,ou=%GROUP%,o=%ORG%
@smretries=3
<html>
<head><title>Sample Login Form</title></head>
<body>
<h3> Please enter your login credentials</h3>
<form method=post><table>
<tr>
<td>User Name:</td>
<td><input type=text name=USER></td>
</tr>
<tr>
<td>Password:</td>
<td><input type=password name=PASSWORD></td>
</tr>
<tr>
<td>Group: </td><td><input type=text name=GROUP></td>
</tr>
<BR>
<tr>
<td>Organization: </td>
<td><Select Name=ORG SIZE=1>
<OPTION>Company A
<OPTION>Company B
<OPTION>Company C
<OPTION>Company D
</SELECT></td>
<input type=hidden name=target value="$$target$$">
<input type=hidden name=smauthreason value="$$smauthreason$$">
<tr><td><input type=submit value=LOGIN></td></tr>
</table></form></body>
</html>
```

위의 파일은 기본 옵션으로 설치된 에이전트에 포함된 usermap.fcc 샘플 파일입니다. 이 .fcc 파일은 사용자가 HTML 양식의 "User Name" 필드와 "Organization" 목록에 입력한 정보를 기반으로 사용자의 DN(고유 이름)을 생성합니다. 이 DN은 사용자 이름 인증 자격 증명입니다. 사용자 암호는 HTML 양식의 "Password" 필드에서 수집됩니다. 인증이 완료되면 사용자를 해당 리소스에 연결할 수 있도록 숨겨진 영역 및 대상 입력 값도 수집됩니다.

특수 이름/값 쌍

FCC 는 비표준 처리를 호출하는 다양한 특수 이름/값 쌍(@ 지시문)을 해석할 수 있습니다. 특수 @ 지시문과 해당 의미는 다음과 같습니다.

username

로그인 사용자 이름으로 사용할 이름입니다.

password

로그인을 수행하기 위한 암호입니다.

target

로그인 후 액세스할 리소스입니다.

smheaders

네임스페이스에 포함할 응답 이름을 포함하는 콜론으로 구분된 목록입니다. 이 콜론으로 구분된 목록에는 트랜잭션에 포함할 각 헤더에 대한 항목이 하나씩 포함되어야 합니다. 예를 들어 트랜잭션의 일부로 header1 및 header2 의 값을 전달하려면 FCC 에 다음 행을 포함하십시오.

@smheaders=header1:header2

smerrorpage

사용자 지정 양식에 대한 POST 작업 시 오류가 발생할 경우 사용자 브라우저가 리디렉션되는 페이지입니다. .fcc 파일에 이 특수 값이 지정되어 있지 않으면 시스템에서는 .fcc 파일과 연결된 .unauth 파일을 오류 페이지로 사용합니다.

smretries

허용되는 최대 로그인 시도 횟수를 지정합니다. 이 지시문을 0 으로 설정하면 재시도 횟수에 제한이 없습니다. 1 이상으로 숫자로 설정할 경우에는 해당 숫자가 허용되는 재시도 횟수입니다.

참고: 사용자가 .fcc 양식에 대한 POST 를 사용하여 로그인할 경우 해당 사용자에게 smretries 지시문 값을 초과하는 추가 로그인 시도 횟수가 제공될 수도 있습니다. 그러나 smretries 에 지정된 시도 횟수 이내에 유효한 자격 증명을 입력할 경우에만 사용자 액세스가 허용됩니다.

smpasswordfcc

데이터가 암호 서비스 FCC 파일에서 포스트되는지 다른 FCC 파일에서 포스트되는지를 결정합니다.

기본값: 1

중요! 기본값을 사용하십시오. SafeWord 인증 체계는 기본값을 사용할 경우 올바르게 동작합니다.

smusrmsg

사용자가 인증 요청을 받거나 로그인에 실패한 이유를 설명하는 텍스트입니다.

smauthreason

로그인 실패와 연결된 사유 코드입니다.

smsavecreds

사용자 자격 증명을 사용자 브라우저의 영구 쿠키에 저장하려면 Yes 로 설정하십시오.

smsave

영구 쿠키로 저장할 콜론으로 구분된 이름 목록입니다.

save

smsave 의 다른 이름입니다.

smtransient

임시 쿠키로 저장할 콜론으로 구분된 이름 목록입니다.

smagentname

사용자가 자격 증명을 입력하고 인증을 위한 양식을 제출할 때 정책 서버에 제공되는 에이전트 이름을 지정합니다. 에이전트 매개 변수 FCCCompatMode 가 NO 인 경우 이 지시문을 사용하여 값을 지정하십시오.

smlogout

LogoffUri 매개 변수와 마찬가지로 사용자를 시스템에서 로그아웃시킵니다. .fcc 템플릿에 @smlogout=true 를 배치하면 FCC 는 사용자를 로그아웃시키고 대상으로 리디렉션합니다. 따라서 @smlogout 지시문은 일반적으로 @target 지시문(@target=<yoururlhere>)과 함께 사용됩니다.

urlencode(*name*)

명명된 변수의 URL 인코딩 값으로 대체됩니다.

참고: 추가 특성 또는 암호에 특수 문자(" . & = + ? ; / : @ = , \$ %)를 포함해야 할 경우 .fcc 템플릿 파일에서 각각의 추가 특성 값을 URL 로 인코딩하십시오. 이 템플릿에는 US-ASCII 인코딩이 사용됩니다.

urldecode(*name*)

명명된 변수의 URL 디코딩 값으로 대체됩니다.

참고: 이름/값 쌍의 "sm" 접두사는 시스템에 필요한 추가 특수 이름을 위해 예약된 접두사입니다. 로그인 페이지의 이름을 생성할 때 "sm" 접두사를 사용하지 마십시오.

FCC 파일에서 이름/값 쌍이 생성되는 방식

login.fcc 템플릿은 `$$name$$` 확장과 특수 이름 값 쌍에 사용할 네임스페이스를 생성합니다. 이름을 여러 번 입력할 경우 마지막 값이 우선합니다. 이름/값 쌍은 이 네임스페이스에 다음과 같은 순서로 추가됩니다.

1. 쿼리 문자열의 이름/값(Get 에서만 해당)
2. 대상 값을 복사하여 생성된 이름 smtarget(Get 에서만 해당)
3. Post 데이터의 이름/값
4. 쿠키의 이름/값
5. @ 지시문의 이름/값(POST 에서만 해당)
6. "smheaders" 이름/값 쌍에 명명된 응답(POST 에서만 해당)

지역화 이름/값 쌍

.fcc 템플릿 파일에는 다음 두 개의 지역화 매개 변수가 포함되어 있습니다.

smlocale

사용자 정보를 수집하거나 상태 메시지를 표시하는 HTML 양식에 사용되는 언어를 결정하는 데 사용됩니다.

smlocale 과 쌍으로 연결되는 값은 지역화 속성 파일의 이름 일부에 해당합니다. 지역화 속성 파일에는 지정된 언어의 텍스트 문자열에 매핑되는 ID 가 포함되어 있습니다.

smlocale 값의 형식은 다음과 같습니다.

COUNTRY-LANGUAGE

예를 들어 미국 영어의 **smlocale** 값은 다음과 같습니다.

SMLOCALE=US-EN

smenc

사용할 언어 인코딩을 브라우저에 알리는 정보가 포함됩니다. 이 변수의 기본값을 변경하면 다음 **META** 태그에 설정된 인코딩이 무시됩니다.

```
<meta http-equiv="Content-Type"
content="text/html; charset=ISO-8859-1">
```

추가 특성 수집

사용자 이름과 암호 외에도 전자 메일 주소 또는 직책 등의 추가 특성을 사용자로부터 수집할 수 있습니다.

다음 단계를 수행하십시오.

1. HTML 양식 인증 체계와 관련 .fcc 템플릿 파일을 구성하여 특성을 하나 이상 지정합니다.
2. "체계 설정" 대화 상자의 "추가 특성 목록" 필드에서 새 특성을 지정하여 HTML 양식 인증 체계를 구성합니다.

참고: 추가 특성 또는 암호에 특수 문자(" . & = + ? ; / : @ = , \$ %)를 포함해야 할 경우 .fcc 템플릿 파일에서 각각의 추가 특성 값을 URL 로 인코딩하십시오. 이 템플릿에는 US-ASCII 인코딩이 사용됩니다.

3. 추가 특성을 수집하도록 .fcc 템플릿 파일을 수정합니다.

파일의 시작 부분에 다음 행을 추가합니다.

```
@password=PASSWORD=%PASSWORD%&newattr1=%newattr1%&newattr2=%newattr2%
```

추가 특성에 특수 문자가 있는 경우에는 이 행을 다음 샘플과 같이 추가합니다.

```
@password=PASSWORD=%urlencode(PASSWORD)%&newattr1=%urlencode(newattr1)%&newattr2=%urlencode(newattr2)%
```

newattr1=%newattr1%

첫 번째 추가 특성을 나타냅니다.

newattr2=%newattr2%

두 번째 추가 특성을 나타냅니다.

같은 기호 앞의 값은 특성 이름이며 백분율 기호(%) 사이의 값은 특성 값입니다.

FCC 는 특성 값에서 새 특성의 이름을 구문 분석합니다.

참고: @password 지시문에 추가 특성을 추가할 때는 앰퍼샌드(&) 문자를 사용하십시오.

템플릿 파일에 특성을 추가할 때는 다음 사항을 고려하십시오.

- **%attribute_name%** 형식으로 식별되는 특성 이름은 파일에도 추가하는 입력 이름 항목과 일치해야 합니다. 예를 들어 다음과 같은 새 특성 주소를 추가한다고 가정합니다.

```
@password=PASSWORD=%PASSWORD%&mail=%address%
```

또는

```
@password=PASSWORD=%urlencode(PASSWORD)%&mail=%urlencode(address)%
```

.fcc 파일에 다음과 같은 문자열을 추가합니다.

```
<input name="address" type="text">
```

- 추가 특성의 이름은 사용자 디렉터리의 특성 이름과 일치해야 합니다. 예를 들어 LDAP 디렉터리에서 전자 메일 주소를 수집하려면 다음 문자열 중 하나를 지정하십시오.

```
@password=PASSWORD=%PASSWORD%&mail=%address%
```

또는

```
@password=PASSWORD=%urlencode(PASSWORD)%&mail=%urlencode(address)%
```

여기서 mail 은 전자 메일 주소를 저장하는 LDAP 특성의 이름입니다.

- `@password` 지시문에 지정한 값 뒤에 공백을 추가하지 마십시오. 추가 공백이 의미 있는 문자로 해석되어 사용자가 인증되지 않을 수도 있습니다.
- HTML 양식 인증 체계의 특성 이름은 `.fcc` 파일의 추가 특성 이름과 일치해야 합니다.
예를 들어 앞의 예에서 인증 체계에 `mail` 특성을 추가하려면 "추가 특성 목록" 필드에 다음 문자열을 입력하십시오.

`AL=PASSWORD,mail`

참고: 추가 특성 이름은 대/소문자를 구분합니다.

사용자에게 로그인 실패 이유 알리기

양식 기반 인증의 기본 동작은 인증되지 않았거나 권한이 부여되지 않은 사용자를 다시 원래 로그인 양식으로 리디렉션하는 것입니다. 사용자의 추가 로그인 시도를 방지하려면 `smretries` 지시문(`@smretries`)을 구성하십시오. 기본적으로 사용자에게 로그인이 실패한 이유를 알리는 메시지가 표시되지 않음에 유의하십시오.

웹 에이전트는 `DynamicRetry.fcc` 및 `DynamicRetry.unauth` 파일과 함께 제공됩니다. 이 `.fcc` 파일 쌍은 리디렉션 동작을 변경합니다. 로그인 페이지(`DynamicRetry.fcc`)는 로그인 시도가 한 번 실패한 후 사용자를 권한 없는 페이지(`DynamicRetry.unauth`)로 보내도록 구성되어 있습니다. 권한 없는 페이지는 로그인 파일과는 다른 템플릿 파일입니다. 따라서 권한 없는 페이지에는 로그인 실패 이유를 알리는 메시지가 포함될 수 있습니다. 기본적으로 사용자가 액세스를 시도하는 리소스에 대해 잘못된 자격 증명을 입력했다는 메시지가 권한 없는 페이지에 표시됩니다.

참고: `DynamicRetry.unauth` 를 열고 `h3` 태그 사이의 텍스트를 업데이트하여 이 메시지를 변경할 수 있습니다.

사용자에게 로그인 실패 이유를 알리려면 인증 체계를 구성할 때 `DynamicRetry.fcc` 파일의 대상 경로를 지정하십시오. `DynamicRetry.fcc` 파일의 기본 경로는 `agent_home\samples\forms\DynamicRetry.fcc` 입니다.

`agent_home`

웹 에이전트 설치 경로를 지정합니다.

.fcc 파일의 `DynamicRetry` 쌍을 사용할 때는 다음 제한 사항을 고려하십시오.

- `SMTRYNO` 쿠키를 기반으로 사용자 로그인 시도 횟수를 계산할 수 없습니다.
- 로그인 시도 횟수는 제한할 수 없습니다.

참고: 이 방법을 암호 서비스와 함께 사용하면 로그인 시도가 지정된 횟수만큼 실패한 후 암호 정책으로 사용자를 비활성화할 수 있습니다. 암호 정책에 대한 자세한 내용은 "암호 정책"을 참조하십시오.

HTML 양식 인증 체계 구성

HTML 양식 인증 체계는 사용자 지정 HTML 양식에서 수집된 자격 증명을 기반으로 하는 인증 방법을 제공합니다.

동일한 정책 저장소에 여러 양식 기반 인증 체계를 구성할 수 있습니다.

다음 단계는 양식 인증 체계를 설정하는 데 필요합니다.

1. [HTML 양식 체계 사전 요구 사항 검토](#) (페이지 314)
2. [HTML 양식 인증 체계 구성](#) (페이지 315)

HTML 양식 체계 사전 요구 사항 검토

HTML 양식 인증 체계를 구성하기 전에 다음 사전 요구 사항을 충족하는지 확인하십시오.

- HTML 양식 인증을 구현할 쿠키 도메인의 웹 에이전트 서버에 사용자 지정된 .fcc 파일이 있어야 합니다. CA 는 웹 에이전트가 설치된 `Samples/Forms` 하위 디렉터리에 샘플 .fcc 파일을 제공합니다.

- 사용자 지정된 .unauth 파일이 웹 에이전트 서버에 있어야 합니다.

참고: .fcc 파일에 `smerrorpage` 지시문이 사용된 경우에는 이 파일이 필요하지 않습니다.

- 정책 서버와 사용자 디렉터리 간에 디렉터리 연결이 있어야 합니다.

- 기본 HTML 양식 라이브러리가 설치되어 있어야 합니다. 이 라이브러리는 HTML 양식 인증 프로세스를 처리합니다.
 - SmAuthHTML.dll(Windows 의 경우)
 - smauthhtml.so(Solaris 의 경우)
 이러한 파일은 웹 에이전트를 구성할 때 자동으로 설치됩니다.
- (Sun Java Systems) Sun Java Systems 웹 서버를 사용하는 경우 magnus.conf 파일의 StackSize 매개 변수 값을 131072 보다 큰 값으로 늘려야 합니다. 값을 변경하지 못하면 양식을 사용한 인증 요청이 있을 때마다 웹 서버가 코어를 덤프하고 재시작됩니다.

사용자 지정 인증 체계 라이브러리 작성 및 설치

FCC가 수집하는 사용자 이름과 암호는 정책 서버에 전달되고, 정책 서버는 이를 인증 체계 라이브러리에 전달합니다.

백엔드 매핑이 필요하지 않는 한 SmAuthHTML 인증 체계 라이브러리를 사용할 수 있습니다. SmAuthHTML 은 정책 서버와 함께 배포되므로 이미 정책 서버 시스템에 설치되어 있습니다.

참고: 백엔드 매핑에는 사용자 지정 인증 체계 라이브러리가 필요합니다. 소프트웨어 개발 키트를 설치한 경우 "API Reference Guide for C"(C 용 API 참조 안내서)"를 참조하십시오.

사용자 지정 인증 체계를 작성하고 사용자 이름 및 암호 이상의 추가 데이터를 수집하려는 경우 FCC 는 이러한 데이터를 사용자 이름 및 암호 필드에 배치해야 합니다. 이러한 필드는 511 자보다 작아야 합니다. 그러면 사용자 지정 인증 체계 라이브러리가 데이터의 압축을 풀고 이를 사용자 이름 및 암호에 매핑할 수 있습니다.

FCC 는 정책 서버와 동일한 시스템에 설치할 수 있습니다.

HTML 양식 인증 체계 구성

HTML 양식 인증 체계를 사용하여 사용자 지정 HTML 양식으로 사용자를 인증할 수 있습니다.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다. 자세한 내용은 "정책 서버 개체 복제"를 참조하십시오.

다음 단계를 수행하십시오.

1. "인프라", "인증"을 차례로 클릭합니다.
2. "인증 체계"를 클릭합니다.
3. "인증 체계 만들기"를 클릭합니다.
"인증 체계 유형의 새 개체 만들기"가 선택되어 있는지 확인합니다.
"확인"을 클릭합니다.
4. 이름 및 보호 수준을 입력합니다.
5. "인증 체계 유형" 목록에서 "HTML 양식 템플릿"을 선택합니다.
6. "웹 서버 이름", "대상" 및 "추가 특성 목록" 정보를 입력합니다.
참고: "대상" 필드에 지정하는 .fcc 파일이 이 필드에 대한 지침을 준수하는지 확인하십시오.
7. 제출을 클릭합니다.

인증 체계가 저장되고 이를 영역에 할당할 수 있습니다.

비 브라우저 클라이언트 지원 사용

비 브라우저 HTML 클라이언트를 사용하여 기본 자격 증명(사용자 이름 및 암호)을 수집하는 HTTP 양식 체계를 구성할 수 있습니다. 이러한 클라이언트는 HTTP 프로토콜을 사용하여 통신하는 Perl 스크립트, C++ 및 Java 프로그램으로 개발할 수 있습니다.

사용자 지정 클라이언트는 HTTP 권한 부여 헤더를 통해 초기 요청과 함께 기본 자격 증명을 보내야 하며, 그렇지 않으면 정책 서버가 사용자를 인증하지 않습니다. HTTP 권한 부여 헤더를 통해 자격 증명을 보내지 않는 경우 정책 서버는 비 브라우저 클라이언트를 지원하지 않는 HTML 양식 체계로 리디렉션됩니다.

다음 단계를 수행하십시오.

1. HTML 양식 인증 체계를 엽니다.
2. "비 브라우저 클라이언트 지원" 확인란을 선택합니다.
3. 제출을 클릭합니다.
비 브라우저 클라이언트 지원이 활성화됩니다.

FCC 국제화를 활성화하는 방법

SiteMinder 는 FCC 국제화를 위한 다음과 같은 기능을 지원합니다.

- 인증 체계에 대한 FCC
- 기본 암호 서비스
- 오류 응답 페이지

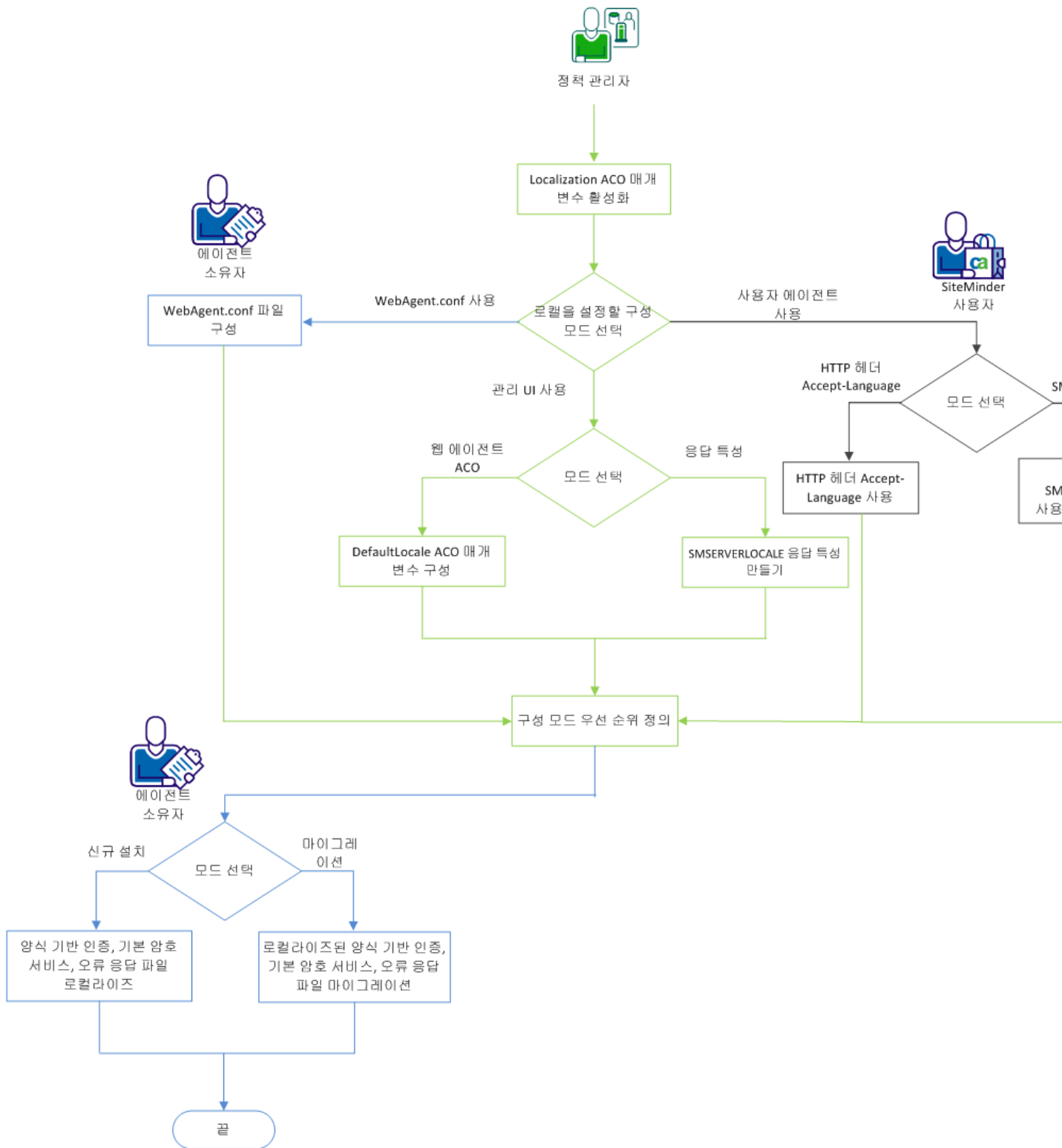
SiteMinder 가 로그인, 기본 암호 서비스, 오류 응답을 위한 HTML 페이지에 표시할 때 사용할 로캘을 설정할 수 있습니다. 조직에서 이 시나리오를 구현하려면 다음과 같은 사용자 역할이 필요합니다.

- 정책 관리자
- 에이전트 소유자
- SiteMinder 사용자

다음 다이어그램은 FCC 국제화를 위해 각 사용자가 반드시 수행해야 하는 단계를 설명합니다.

참고: 다음 다이어그램에서 파란색은 정책 관리자의 태스크를, 노란색은 에이전트 소유자의 태스크를, 검은색은 SiteMinder 사용자의 태스크를 각각 나타냅니다.

FCC 국제화 활성화 방법



FCC 국제화를 활성화하려면 다음 단계를 수행해야 합니다.

1. [관리 UI 를 사용하여 Localization ACO 매개 변수를 활성화합니다](#) (페이지 321). 이 태스크는 정책 관리자가 수행해야 합니다.
2. [선호하는 로캘을 선택하기 위해 구성 모드를 선택합니다](#) (페이지 321). 이 태스크는 다음 방법으로 수행할 수 있습니다.
 - 사용자 에이전트 사용. SiteMinder 사용자는 다음 방법으로 사용자 에이전트를 사용하여 선호하는 로캘을 설정할 수 있습니다.
 - HTTP 헤더 SMCLIENTLOCALE 사용
 - HTTP [헤더 Accept-Language 사용](#) (페이지 322)
 - [관리 UI 사용](#) (페이지 322). 정책 관리자는 다음 방법으로 관리 UI 를 사용하여 선호하는 로캘을 설정할 수 있습니다.
 - [SMSERVERLOCALE 응답 특성 사용](#) (페이지 322)
 - [DefaultLocale ACO 매개 변수 사용](#) (페이지 323)
 - [WebAgent.conf 파일 사용](#) (페이지 323). 에이전트 소유자는 WebAgent.conf 파일에서 Locale 매개 변수를 구성하여 선호하는 로캘을 설정할 수 있습니다.
3. [구성 모드의 우선 순위를 정의합니다](#) (페이지 324). 정책 관리자는 관리 UI 를 사용하여 이 태스크를 수행해야 합니다.
4. 다음 단계 중 *하나*를 수행합니다.
 - HTML 페이지를 처음 로컬라이즈하는 경우 에이전트 소유자가 다음 단계를 수행해야 합니다.
 - a. [양식 기반 인증 파일 및 기본 암호 서비스 파일을 로컬라이즈합니다](#) (페이지 325).
 - b. [오류 응답 파일을 로컬라이즈합니다](#) (페이지 326).
 - 로컬라이즈된 파일을 마이그레이션하려면 에이전트 소유자가 다음 단계를 수행해야 합니다.
 - a. [양식 기반 인증 파일 및 기본 암호 서비스 파일을 마이그레이션합니다](#) (페이지 329).
 - b. [로컬라이즈된 오류 응답 파일을 마이그레이션합니다](#) (페이지 331).

SiteMinder 가 FCC 국제화를 활성화하도록 구성되었습니다.

로컬라이제이션 매개 변수 활성화

지원되는 기능을 로컬라이즈하려면 정책 관리자가 **Localization ACO** 매개 변수를 **true** 로 설정해야 합니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "인프라", "에이전트"를 차례로 클릭합니다.
3. "에이전트 구성 개체"를 클릭합니다.
4. 웹 에이전트의 에이전트 구성 개체로 이동합니다.
5. 에이전트 구성 개체의 이름을 클릭합니다.
6. "수정"을 클릭합니다.
7. **Localization** 매개 변수로 이동한 다음 매개 변수 옆의 오른쪽 화살표를 클릭합니다.
"매개 변수 편집" 페이지가 열립니다.
8. 매개 변수의 값을 **yes** 로 설정합니다.
9. 변경 내용을 저장합니다.

선호하는 로캘 설정

Accept-Language HTTP 헤더 형식으로 여러 선호하는 로캘을 정의할 수 있습니다.

예: `es-ES,en-US;q=0.8,as-IN;q=0.6,fr-FR;q=0.4,en-IN;q=0.2`

로캘은 런타임 중에 동적으로 결정되지만 로캘은 요청 처리 중에 변경될 수 있습니다. 예를 들어, 성공적인 인증 후에 로캘이 변경될 수 있습니다.

다음 구성 모드에서 선호하는 로캘을 정의하십시오.

- 사용자 에이전트 사용
- 관리 관리 UI 사용
- **WebAgent.conf** 파일 사용

사용자 에이전트를 통해 선호하는 로캘 설정

사용자는 선호하는 로캘로 브라우저 설정을 구성할 수 있습니다. 정책 서버는 선호하는 로캘을 사용하여 지원되는 기능과 관련된 요청을 보냅니다.

사용자는 다음 방법을 사용하여 로캘을 설정할 수 있습니다.

- HTTP 헤더 **SMCLIENTLOCALE** 사용
- HTTP 헤더 **Accept-Language** 사용

HTTP 헤더 **SMCLIENTLOCALE** 사용

웹 요청에 대한 HTTP 헤더 **SMCLIENTLOCALE** 을 사용하여 선호하는 로캘을 설정하십시오. 웹 응용 프로그램이 선호하는 로캘을 설정하는 옵션을 제공하는 경우 사용자는 로캘을 선택할 수 있습니다. 정책 서버는 웹 요청의 **SMCLIENTLOCALE** 헤더를 사용하여 로캘을 받습니다. 로캘이 있는 경우 지원되는 기능이 나열된 페이지가 요청된 로캘로 표시됩니다.

HTTP 헤더 **Accept-Language** 사용

사용자는 로컬 웹 브라우저 설정을 사용하여 선호하는 로캘을 설정할 수 있습니다. 웹 요청의 HTTP 헤더 **Accept-Language** 는 로캘을 지정합니다.

관리 UI 를 통해 선호하는 로캘 설정

정책 관리자는 관리 UI 를 사용하여 선호하는 로캘을 설정할 수 있습니다. 정책 서버는 이 로캘을 사용하여 지원되는 기능과 관련된 요청을 보냅니다.

SMSEVERLOCALE 응답 헤더 변수 설정

선호하는 로캘을 응답으로 설정하려면 **SMSEVERLOCALE** 응답 특성을 사용하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "정책", "도메인"을 차례로 클릭합니다.
3. "응답"을 클릭합니다.
4. 수정할 응답을 편집합니다.
5. "응답 정의" 탭을 클릭합니다.
6. 수정할 응답 특성을 편집합니다.

7. "특성 유형"을 "WebAgent-HTTP-Header 변수"로 선택합니다.
8. "변수 이름"에 SMSERVERLOCALE 을 입력합니다.
9. "변수 값"에 선호하는 로캘을 입력합니다.
10. 변경 내용을 저장합니다.

DefaultLocale ACO 속성 설정

DefaultLocale ACO 매개 변수에 선호하는 로캘 정보를 설정하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "인프라", "에이전트"를 차례로 클릭합니다.
3. "에이전트 구성 개체"를 클릭합니다.
4. 웹 에이전트의 에이전트 구성 개체로 이동합니다.
5. 에이전트 구성 개체의 이름을 클릭합니다.
6. "수정"을 클릭합니다.

설정과 컨트롤이 활성화됩니다.

7. DefaultLocale 매개 변수로 이동한 다음 매개 변수 옆의 오른쪽 화살표를 클릭합니다.

"매개 변수 편집" 페이지가 열립니다.

8. 선호하는 로캘로 속성을 업데이트합니다.
9. 변경 내용을 저장합니다.

WebAgent.conf 파일을 사용하여 선호하는 로캘 설정

Locale 속성을 에이전트 소유자로서 설정하려면 WebAgent.conf 파일을 구성하십시오. 이 파일은 설치 중 지정되는 로캘 정보가 수록되어 있습니다.

다음 단계를 수행하십시오.

1. 웹 에이전트 컴퓨터에 로그인합니다.
2. 텍스트 편집기에서 WebAgent.conf 파일을 엽니다.
3. Locale 속성으로 이동하여 선호하는 로캘로 값을 설정합니다.
4. 변경 내용을 저장합니다.

구성 모드 우선 순위 정의

5 개 구성 모드의 우선 순위를 결정하려면 관리자는 `ClientLocalePreferred` ACO 매개 변수를 설정해야 합니다. `ClientLocalePreferred` 매개 변수가 `true` 로 설정되면 시스템은 구성 모드를 검사하여 다음 순서로 로캘을 결정합니다.

1. HTTP 헤더 `SMCLIENTLOCALE`
2. HTTP 헤더 `Accept-Language`
3. 응답 헤더 변수 `SMSERVERLOCALE`
4. `DefaultLocale` ACO 매개 변수
5. `WebAgent.conf` 파일의 `Locale` 속성

`ClientLocalePreferred` 가 `false` 로 설정되면 시스템은 구성 모드를 검사하여 다음 순서로 로캘을 결정합니다.

1. 응답 헤더 변수 `SMSERVERLOCALE`
2. HTTP 헤더 `SMCLIENTLOCALE`
3. HTTP 헤더 `Accept-Language`
4. `DefaultLocale` ACO 매개 변수
5. `WebAgent.conf` 파일의 `Locale` 속성

정책 서버는 정의된 모드를 사용하여 선호하는 로캘을 처리하고 선호하는 로캘의 목록을 만듭니다. 이 목록은 각 선호하는 로캘의 `q` 요소를 기준으로 정렬됩니다. 웹 요청이 전달되면 이 목록은 지원되는 기능의 HTML 페이지가 표시되는 로캘을 나타냅니다.

`ClientLocalePreferred` 매개 변수를 로캘의 원하는 순서로 설정하십시오.

다음 단계를 수행하십시오.

1. "인프라", "에이전트"를 차례로 클릭합니다.
2. "에이전트 구성 개체"를 클릭합니다.
3. 웹 에이전트의 에이전트 구성 개체로 이동합니다.
4. 에이전트 구성 개체의 이름을 클릭합니다.
5. "수정"을 클릭합니다.
6. 설정과 컨트롤이 활성화됩니다.

7. ClientLocalePreferred 매개 변수로 이동합니다.
"매개 변수 편집" 페이지가 열립니다.
8. 매개 변수 값을 수정합니다.
9. 변경 내용을 저장합니다.

양식 기반 인증 및 기본 암호 서비스 파일 로컬라이즈

에이전트 소유자는 양식 기반 인증 및 기본 암호 서비스 파일을 로컬라이즈할 수 있습니다. 기본적으로, 여러 로캘로 된 샘플 양식이 제공됩니다. 이러한 샘플은 `webagent_home/samples` 디렉터리에 있습니다.

각 로캘에는 로캘 관련 파일을 위한 폴더가 있습니다. 각 폴더 및 파일에는 다음과 같은 형식의 RFC 3066 표준 명명 규칙을 따르는 로캘 언어 코드가 붙습니다.

`forms_<locale language code>`

`forms_<locale language code>/filename_<locale language code>.fcc`

예를 들면 다음과 같습니다.

영어의 경우 폴더 이름은 `samples/forms_en-US`, `login.fcc` 파일 이름은 `login_en-US.fcc`, `WebAgent.properties` 파일 이름은 `WebAGent_en-US.properties` 입니다.

샘플 양식 폴더와 별도로 기본 양식 폴더가 제공됩니다. 이 폴더에는 로캘 언어 코드가 없는 파일이 수록되어 있습니다. 웹 에이전트가 로캘에 대한 요청을 받으면 정책 서버는 선호하는 로캘의 목록에 요청된 로캘이 있는지 여부를 확인합니다. 그런 다음 시스템은 다음 태스크 중 *하나*를 수행합니다.

- 요청된 로캘이 목록에 있는 로캘과 일치하면 요청이 요청된 로캘로 처리됩니다.
- 요청된 로캘이 목록의 로캘과 일치하지 않으면 요청이 기본 양식 폴더의 로캘을 사용하여 처리됩니다.

새 로캘을 지원하도록 폴더 사용자 지정

기본 양식 폴더는 **en-US** 로 되어 있습니다. **en-US** 가 아닌 새 로캘을 지원하려면 에이전트 소유자가 기본 폴더 및 파일을 사용자 지정해야 합니다.

다음 단계를 수행하십시오.

1. 웹 에이전트 컴퓨터에 로그인합니다.
2. 다음 위치로 이동합니다.
`webagent_home/samples`
3. 다음 형식으로 새 로캘에 대한 폴더를 만듭니다.
`forms_<locale language code>`
4. .fcc 파일을 사용자 지정합니다.
 - a. 관련 FCC 파일을 기본 양식 폴더에서 새 폴더로 복사합니다.
 - b. 다음 형식으로 각 FCC 파일에 로캘의 언어 코드를 붙입니다.
`filename_<locale language code>.fcc`
5. 속성 파일을 사용자 지정합니다.
 - a. 관련 .properties 파일을 기본 양식 폴더에서 새 로캘 폴더로 복사합니다.
 - b. 다음과 같이 각 파일에 새 로캘에 대한 언어 코드를 붙입니다.
`filename_<locale language code>.properties`
6. 영어 메시지를 새 로캘의 언어로 변경하는 등, 로캘에 맞게 파일을 수정합니다.
7. 변경 내용을 저장합니다.

오류 응답 파일 로컬라이즈

에이전트 소유자는 오류 응답 파일을 로컬라이즈할 수 있습니다. 여러 로캘로 된 샘플 오류 응답 파일이 다음 디렉터리에서 제공됩니다.

`webagent_home/samples/error-responses`

각 로캘에는 로캘 관련 파일을 위한 폴더가 있습니다. 각 폴더 및 파일에는 다음과 같은 형식의 RFC 3066 표준 명명 규칙을 따르는 로캘 언어 코드가 붙습니다.

`responses_<locale language code>`

`filename_<locale language code>.err`

샘플 오류 응답 폴더 이외에, 로캘 언어 코드가 없는 기본 오류 응답 폴더 및 파일도 있습니다. 웹 에이전트가 특정 로캘의 요청을 받으면 정책 서버가 다음 태스크 중 하나를 수행합니다.

- 해당 로캘이 있고 오류가 발생하는 경우 해당 로캘 폴더의 오류 응답 파일을 사용하여 오류 응답이 표시됩니다.
- 해당 로캘이 없고 오류가 발생하는 경우 기본 오류 응답 폴더의 파일을 사용하여 오류 응답이 표시됩니다.

새 로캘을 지원하도록 SiteMinder 사용자 지정

기본적으로 제공되지 않는 새 로캘을 지원하려면 기본 폴더 및 파일을 사용자 지정하십시오.

선호하는 로캘에 맞게 다음과 같은 오류 응답 파일을 사용자 지정할 수 있습니다.

- CSS 파일에 대해 생성된 `csserror.err`
- 서버 오류에 대해 생성된 `servererror.err`
- 쿠키 오류에 대해 생성된 `cookieerror.err`
- 인증 및 인증 오류에 대해 생성된 `custom401error.err`

오류가 발생하면 다음 위치에서 오류 페이지를 가져옵니다.

`ErrorResponseLocation_home/responses_<locale language code>`

예:

영어 로캘의 경우 오류 응답 파일은

`ErrorResponseLocation_home/responses_en-US` 폴더에 저장됩니다. 쿠키 오류가 발생하면 `cookieerror_en-US.err` 오류 응답 파일을 이 폴더에서 가져옵니다.

오류 응답을 사용자 지정하려면 다음 단계를 수행하십시오.

1. 웹 에이전트를 구성합니다.
2. 웹 에이전트 ACO 를 구성합니다.

웹 에이전트 구성

오류 응답 파일을 로컬라이즈하려면 에이전트 소유자가 웹 에이전트를 구성해야 합니다.

다음 단계를 수행하십시오.

1. 웹 에이전트 컴퓨터에 로그인합니다.
2. 다음 위치로 이동합니다.
`webagent_home/samples/error-responses`
3. 다음 형식으로 새 로캘에 대한 폴더를 만듭니다.
`responses_<locale language code>`
4. 응답 파일을 기본 응답 폴더에서 새 폴더로 복사합니다.
5. 다음과 같이 각 오류 응답 파일에 새 로캘에 대한 언어 코드를 붙입니다.
`filename_<locale language code>`
6. 새 로캘에 맞게 파일을 수정합니다. 예를 들어, 영어 메시지를 새 로캘에 대한 언어로 변경하십시오.

웹 에이전트 ACO 구성

오류 응답 파일을 로컬라이즈하려면 정책 관리자가 에이전트 ACO 매개 변수를 구성해야 합니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "인프라", "에이전트"를 차례로 클릭합니다.
3. "에이전트 구성 개체"를 클릭합니다.
4. 웹 에이전트의 에이전트 구성 개체로 이동합니다.
5. 에이전트 구성 개체의 이름을 클릭합니다.

6. "수정"을 클릭합니다.
7. 다음 매개 변수의 값이 'no'로 설정되었는지 확인합니다.
 - servererrorfile
 - csserrorfile
 - reqcookieerrorfile
 - custom401errorfile

참고: 이러한 속성은 `ErrorResponseLocation` 매개 변수보다 우선 순위가 더 높습니다. 오류 응답 파일을 로컬라이즈하려면 이러한 속성을 비활성화하십시오.
8. `ErrorResponseLocation` 매개 변수로 이동한 다음 매개 변수 옆의 오른쪽 화살표를 클릭합니다.

"매개 변수 편집" 페이지가 표시됩니다.
9. 오류 응답 파일의 새 경로를 입력합니다.

참고: `ErrorResponseLocation` 속성의 값은 URL 이 아니어야 합니다.
10. 변경 내용을 저장합니다.

로컬라이즈된 파일 마이그레이션

12.51 이전 릴리스에 로컬라이즈된 FCC 파일, 기본 암호 서비스, 오류 응답 파일이 있는 경우, 에이전트 소유자는 이러한 파일을 재사용하기 위해 파일을 12.51 이상으로 마이그레이션할 수 있습니다.

양식 기반 인증 파일 및 기본 암호 서비스 파일 마이그레이션

에이전트 소유자는 양식 기반 인증 파일 및 기본 암호 서비스 파일을 마이그레이션할 수 있습니다.

다음 단계를 수행하십시오.

1. 웹 에이전트 컴퓨터에 로그인합니다.
2. 로컬라이즈된 파일이 있는 위치로 이동합니다.

기본 경로: `webagent_home/samples`

3. 폴더를 만들거나 다음 단계로 건너뛰고 기존 로캘 폴더의 이름을 변경합니다. 다음 단계 중 *하나*만 수행하십시오.

- a. 다음 형식으로 폴더를 만듭니다.

`forms_<locale language code>`

- b. 기존 로컬라이즈된 FCC 파일을 새 폴더로 복사합니다.

- c. 다음 형식으로 각 파일에 로캘의 언어 코드를 붙입니다.

`filename_<locale language code>.fcc`

- d. 관련 `.properties` 파일을 기존 폴더에서 새 로캘의 양식 폴더로 복사합니다.

- e. 다음 형식으로 각 파일에 로캘의 언어 코드를 붙입니다.

`filename_<locale language code>.properties`

4. (선택 사항) 기존 폴더의 이름을 변경합니다(이 단계는 폴더 생성 방법에 대한 대안).

- a. 다음 형식으로 기존 폴더의 이름을 변경합니다.

`forms_<locale language code>`

- b. 다음 형식으로 로캘의 언어 코드를 사용하여 각 파일 이름을 수정합니다.

`filename_<locale language code>.fcc`

- c. 다음 형식으로 로캘의 언어 코드를 사용하여 각 파일 이름을 수정합니다.

`filename_<locale language code>.properties`

5. FCC 파일에서 다음 단계를 수행합니다.

- a. 하드 코드된 인코딩 매개 변수를 `$$SMENC$$` 태그로 바꿉니다.

예:

- `<meta http-equiv="Content-Type" content="text/html; charset=$$SMENC$$">`
- `<INPUT TYPE=HIDDEN NAME="SMENC" VALUE=$$SMENC$$">`

- b. 각 파일의 첫 번째 줄은 양식을 인코딩하는 데 사용한 문자 집합의 이름을 포함해야 합니다. 예: `<!-- SiteMinder Encoding=UTF-8; -->`. 여기서 **UTF-8** 은 양식을 인코딩하는 데 사용됩니다.

6. 변경 내용을 저장합니다.

오류 응답 파일 마이그레이션

에이전트 소유자는 로컬라이즈된 오류 응답 파일을 마이그레이션할 수 있습니다.

다음 단계를 수행하십시오.

1. 웹 에이전트 컴퓨터에 로그인합니다.
2. 로컬라이즈된 파일이 있는 위치로 이동합니다.

기본 경로: `webagent_home/samples/error-responses`

3. 폴더를 만들려면 다음 단계를 수행하십시오. 또는, 다음 단계로 건너뛰어 기존 폴더의 이름을 변경하십시오.

- a. 다음 형식으로 폴더를 만듭니다.

`responses_<locale language code>`

- b. 기존 로컬라이즈된 오류 응답 파일을 새 폴더로 복사합니다.

- c. 다음 형식으로 각 파일에 로캘의 언어 코드를 붙입니다.

`filename_<locale language code>`

4. (선택 사항) 기존 폴더의 이름을 변경하려면:

- a. 다음 형식으로 기존 파일의 이름을 변경합니다.

`responses_<locale language code>`

- b. 다음 형식으로 로캘의 언어 코드를 사용하여 각 파일 이름을 수정합니다.

`filename_<locale language code>`

FCC 국제화가 이제 완료되었습니다.

Windows 인증 체계

IWA(Windows 통합 인증)는 Microsoft 가 순수한 Windows 환경에서 사용자의 유효성을 검사하기 위해 개발한 전용 메커니즘입니다. 정책 서버에서 사용할 수 있는 Windows 인증 체계는 Microsoft Windows 통합 인증 인프라가 획득하는 사용자 자격 증명을 처리하여 리소스를 보호합니다.

제품의 이전 버전에서는 NTLM 인증 체계를 통해 Windows 인증을 지원했습니다. 그러나 이러한 지원은 NT 도메인을 사용하는 환경이나 Active Directory 서비스가 혼합 모드에서 레거시 NT 도메인을 지원하도록 구성된 환경으로 제한되었습니다.

Windows 인증 체계는 네이티브 모드에서 실행되는 Active Directory 를 사용한 배포에서 액세스 제어를 제공합니다. 이 체계는 또한 NTLM 인증을 지원하도록 구성된 Active Directory 도 지원합니다. Windows 인증 체계는 제품의 NTLM 인증 체계를 대체합니다. 기존 NTLM 인증 체계도 계속 지원되며 새 Windows 인증 체계를 사용하여 구성할 수 있습니다.

참고: 일부 경우에는 Windows 인증 체계를 사용하는 대신 Windows 사용자 보안 컨텍스트 기능과 다른 인증 체계를 함께 사용하는 것이 좋습니다.

Windows 인증 체계는 IIS 웹 서버의 웹 에이전트가 보호하는 리소스에 사용됩니다. 이 경우 사용자는 Internet Explorer 웹 브라우저를 사용하여 리소스에 액세스합니다. 이 체계를 사용하려면 IIS 웹 서버가 사용자 자격 증명을 받아 확인할 수 있도록 올바르게 구성되어 있어야 합니다. 정책 서버는 IIS 서버에 의해 어설션될 때 사용자 아이덴티티를 기초로 권한 부여를 결정합니다.

추가 정보:

[Windows 사용자 보안 컨텍스트 요구 사항](#) (페이지 102)

Windows 인증 사전 요구 사항을 충족하는지 확인

Windows 인증 체계를 구성하기 전에 다음 사전 요구 사항을 충족하는지 확인하십시오.

- 혼합 모드의 레거시 WinNT 디렉터리 또는 Active Directory 가 다음 조건을 충족하는지 확인합니다.
 - 관리 UI 에서 생성한 사용자 디렉터리 연결에 WinNT 네임스페이스가 지정되어 있습니다.
 - 요청된 리소스는 어떤 유형의 웹 서버에 있든 관계없습니다. 하지만 이러한 리소스를 보호하는 인증 서버와 웹 에이전트는 Microsoft IIS 웹 서버에 있어야 합니다.

- 네이티브 모드에서 실행되는 Active Directory 가 다음 조건을 충족하는지 확인합니다.
 - 사용자 데이터가 Active Directory 에 있습니다.
 - 사용자 디렉터리 연결에 LDAP 또는 AD 네임스페이스가 지정되어 있어야 합니다.
 - 요청된 리소스는 어떤 유형의 웹 서버에 있든 관계없습니다. 하지만 이러한 리소스를 보호하는 인증 서버와 웹 에이전트는 Microsoft IIS 웹 서버에 있어야 합니다.
 - 클라이언트 및 서버 계정을 위임할 수 있습니다.
- 사용자는 Windows 자격 증명 전달을 지원하며 이러한 자격 증명을 자동으로 전달하도록 올바르게 구성된 브라우저를 사용해야 합니다.
- Windows 의 IIS 에서 작업하려는 경우 "와일드카드 응용 프로그램 매핑"의 "파일이 있는지 확인" 옵션이 설정되어 있지 않아야 합니다.
- 또한 Windows 인증 체계에서는 creds.ntc 파일이 포함된 IIS 웹 서버의 모든 가상 디렉터리를 보호되지 않은 상태로 두어야 합니다.
- 사용자의 현재 사용자 이름 및 암호를 사용하여 자동으로 로그인하도록 Internet Explorer 브라우저 옵션이 구성되어 있습니다.

Windows 인증 체계 구성

Windows 환경에서 사용자를 인증하려면 Windows 인증 체계를 사용하십시오.

참고: 정책 서버가 아닌 IIS 웹 서버는 Internet Explorer 웹 브라우저에서 받은 자격 증명을 기반으로 인증을 수행합니다. 따라서 OnAuthAttempt 인증 이벤트를 사용하여 사용자 저장소에 없는 사용자를 리디렉션할 수 없습니다.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다. 자세한 내용은 "정책 서버 개체 복제"를 참조하십시오.

다음 단계를 수행하십시오.

1. "인프라", "인증"을 차례로 클릭합니다.
2. "인증 체계"를 클릭합니다.

3. "인증 체계 만들기"를 클릭합니다.
"인증 체계 유형의 새 개체 만들기"가 선택되어 있는지 확인합니다.
"확인"을 클릭합니다.
4. 이름 및 보호 수준을 입력합니다.
5. "인증 체계 유형" 목록에서 "Windows 인증 템플릿"을 선택합니다.
6. "서버 이름", "대상" 및 "사용자 DN" 정보를 입력합니다. 사용자 환경에 NT 챌린지/응답 인증이 필요한 경우 에이전트 소유자에게서 다음의 값을 가져옵니다.

서버 이름

다음과 같은 IIS 웹 서버의 정규화된 도메인 이름입니다.

server1.myorg.com

대상

/siteminderagent/ntlm/smntlm.ntc

참고: 디렉터리는 설치 환경에서 이미 구성된 가상 디렉터리와 일치해야 합니다. 대상 파일인 smntlm.ntc 는 없어도 되며 .ntc 로 끝나는 모든 이름이나 기본값 대신 사용하는 사용자 지정 MIME 유형일 수 있습니다.

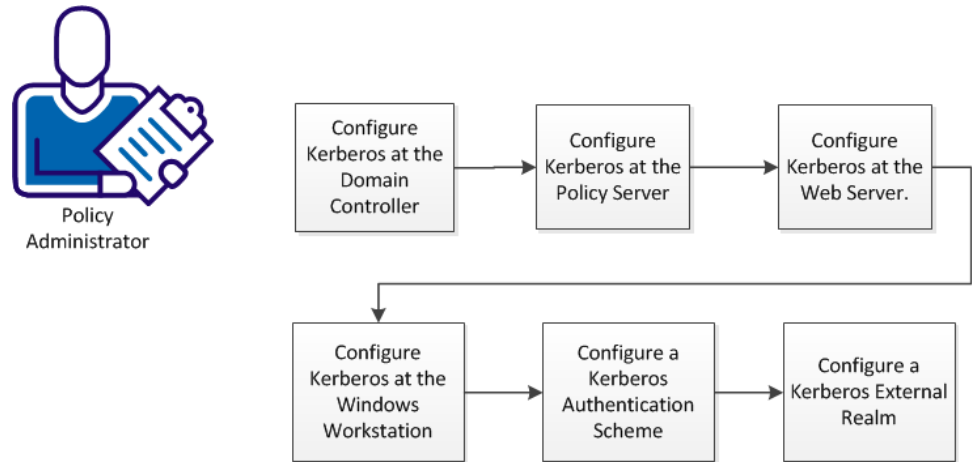
라이브러리

smauthntlm

7. 제출을 클릭합니다.
인증 체계가 저장되고 이를 영역에 할당할 수 있습니다.

Kerberos 인증을 구성하는 방법

Kerberos 인증은 클라이언트 및 서버의 호스트 환경에 따라 다양한 구성 시나리오를 지원합니다. 각 시나리오마다 약간 다르긴 하지만 SiteMinder 환경에서 Kerberos 인증을 구현하기 위해서는 정책 관리자가 다음 다이어그램에 표시된 태스크를 수행해야 합니다.



Kerberos 인증을 구성하려면 다음 절차를 완료하십시오.

1. [도메인 컨트롤러에서 Kerberos 를 구성합니다](#) (페이지 335).
2. [정책 서버에서 Kerberos 를 구성합니다](#) (페이지 342).
3. [웹 서버에서 Kerberos 를 구성합니다](#) (페이지 345).
4. [Windows 워크스테이션에서 Kerberos 를 구성합니다](#) (페이지 345)
5. [Kerberos 인증 체계 구성](#) (페이지 346)
6. [Kerberos 외부 영역을 구성합니다](#) (페이지 347).

도메인 컨트롤러에서 Kerberos 인증 구성

순수한 Windows 환경에서는 Kerberos 영역이 Windows 도메인에 해당합니다. 도메인 컨트롤러 호스트는 사용자, 서비스 계정, 자격 증명, Kerberos 티켓 서비스 및 Windows 도메인 서비스에 대한 저장소를 제공합니다.

Kerberos 인증에는 사용자에게 암호를 요구하지 않고 KDC 로 사용자를 인증할 수 있게 해 주는 **keytab** 파일이 필요합니다. **keytab** 파일은 **ktpass** 유틸리티를 사용하여 생성합니다. **ktpass** 명령 도구 유틸리티는 Windows 지원 도구입니다. UNIX에서는 **ktadd** 유틸리티가 이에 해당합니다.

도메인 컨트롤러 호스트(Windows 또는 UNIX)에서 정책 서버에 KDC 를 구성하는 일반적인 순서는 다음과 같습니다.

1. 사용자 계정을 생성합니다. 이 계정은 워크스테이션에 로그인하는 데 사용됩니다.
2. 웹 서버 호스트에 로그인하는 데 사용할 웹 서버의 서비스 계정을 생성합니다.
3. 정책 서버 호스트에 로그인하는 데 사용할 정책 서버의 서비스 계정을 생성합니다.
4. 웹 서버 계정을 웹 서버 프린서플 이름과 연결합니다.
5. 웹 서버 호스트로 전송되는 **keytab** 파일을 생성합니다.
6. 정책 서버 계정을 정책 서버 프린서플 이름과 연결합니다.
7. 정책 서버 호스트로 전송되는 다른 **keytab** 파일을 생성합니다.
8. 웹 서버 및 정책 서버 계정이 위임에 대해 트러스트되도록 지정합니다.

중요! Kerberos 프로토콜을 사용하는 서비스의 경우 **SPN**(서비스 프린서플 이름)을 표준 형식, 즉 **service/fqdn_host@REALM_NAME** 으로 생성해야 합니다.

추가 정보:

[Windows 에서 KDC 구성 예](#) (페이지 337)

[UNIX 에서 KDC 구성 예](#) (페이지 340)

Windows 에서 KDC 구성 예

다음에 절차는 Kerberos 인증을 지원하도록 Windows 도메인 컨트롤러/KDC 를 구성하는 방법을 보여 줍니다. 이 예는 다음과 같은 서버 및 계정 이름을 사용합니다.

- 서버
도메인 컨트롤러: kdc.example.com
정책 서버: smps.example.com
웹 서버: www.example.com
Active Directory 도메인: EXAMPLE
Kerberos 영역: EXAMPLE.COM
- 계정
사용자 계정: testkrb
웹 에이전트 서비스 계정: krbsvc-smwa
정책 서버 서비스 계정: krbsvc-smps

다음 단계를 수행하십시오.

1. Windows 서버에 Active Directory 도메인 서비스 역할을 추가합니다.
이 작업은 Windows 서버를 도메인 컨트롤러로 만듭니다. Windows 도메인 컨트롤러는 Kerberos 키 배포 센터(KDC)로서 동작하고 Kerberos V5 프로토콜을 구현하며 Kerberos 관련 인증 기능을 수행합니다.
2. 명령창에서 Windows dcpromo 유틸리티를 실행하거나 서비스 관리자에 있는 링크(dcpromo 유틸리티를 시작)를 클릭합니다.
3. 도메인 기능 수준을 확인합니다.
 - a. "관리 도구"에서 "Active Directory 사용자 및 컴퓨터" 대화 상자를 엽니다.
 - b. 대화 상자 왼쪽의 example.com 드롭다운을 마우스 오른쪽 단추로 클릭합니다.
 - c. "도메인 기능 수준 올리기"를 클릭합니다.
 - d. Active Directory 의 도메인 기능 수준이 최소한 Windows Server 2003 과 같은지 확인합니다. 그렇지 않은 경우 도메인 기능 수준을 높이십시오.

중요! 도메인 기능 수준을 높이는 작업은 되돌릴 수 없습니다.

4. 사용자 계정(예: `testkrb`)을 생성합니다. 이 계정에 대한 암호를 제공합니다. 옵션의 선택을 취소하면 사용자가 다음에 로그인할 때 암호를 변경해야 합니다. Windows 워크스테이션은 이 계정을 사용하여 `example.com`에 로그인합니다.
5. 웹 서버의 서비스 계정(예: `krbsvc-smwa`)을 생성합니다. 이 계정에 대한 암호를 생성합니다. 옵션의 선택을 취소하면 사용자가 다음에 로그인할 때 암호를 변경해야 합니다.
6. 정책 서버의 서비스 계정(예: `krbsvc-smpps`)을 생성합니다. 이 계정에 대한 암호를 제공합니다. 옵션의 선택을 취소하면 사용자가 다음에 로그인할 때 암호를 변경해야 합니다.
7. 웹 서버 서비스 계정(`krbsvc-smwa`)을 Kerberos 서비스 프린서플 이름(`HTTP/www.example.com@EXAMPLE.COM`)과 연결하고 `Ktpass` 유틸리티를 사용하여 `keytab` 파일을 생성합니다. 항상 지원 도구의 버전을 확인하십시오. 기본 암호화 유형은 `RC4-HMAC`입니다. 암호화 유형은 명령 프롬프트에서 `kpass /?`를 사용하여 확인할 수 있습니다.

```
ktpass -out c:\krbsvc-smwa.keytab -princ HTTP/www.example.com@EXAMPLE.COM  
dc.example.com -ptype KRB5_NT_PRINCIPAL -mapuser EXAMPLE\krbsvc-smwa -pass "*"
대상 도메인 컨트롤러: dc.example.com
Using legacy password setting method
Successfully mapped HTTP/www.example.com to krbsvc-smwa..
Key created.
Output keytab to c:\krbsvc-smwa.keytab:
Keytab version: 0x502
keysize 82 dc.example.com ptype 1 (KRB5_NT_PRIN  
CIPAL) vno 3 etype 0x17 (RC4-HMAC) keylength 16 (0xf3d3d2a17c7ea172ff22044806443  
9a9)
```

암호는 웹 서버의 서비스 계정을 생성하는 데 사용한 암호와 동일합니다.

8. 정책 서버 서비스 계정(krb5vc-smpps)을 Kerberos 서비스 프린서펄 이름(smpps/smpps.example.com@EXAMPLE.COM)과 연결하고 정책 서버 호스트에 대한 또 다른 keytab 파일을 생성합니다.

```
Ktpass -out c:\krb5vc-smpps.keytab -princ smpps/smpps.example.com@EXAMPLE.COM
-ptype KRB5_NT_PRINCIPAL -mapuser EXAMPLE\krb5vc-smpps -pass *
```

대상 도메인 컨트롤러: dc.example.com.com

Using legacy password setting method

Successfully mapped smpps/smpps.example.com to krb5vc-smpps.

Key created.

Output keytab to c:\krb5vc-smpps.keytab:

Keytab version: 0x502

keysize 72 smpps/smpps.example.com@EXAMPLE.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 2

etype 0x17 (RC4-HMAC) keylength 16 (0xfd77a26f1f5d61d1fafd67a2d88784c7)

암호는 정책 서버의 서비스 계정을 생성하는 데 사용한 암호와 동일합니다.

9. 다음과 같이 서버 서비스 계정을 "위임용으로 트러스트"로 지정합니다.
 1. 서비스 계정(krb5vc-smwa) 속성을 마우스 오른쪽 단추로 클릭합니다.
 2. "위임" 탭을 선택합니다.
 3. 두 번째 옵션인 "모든 서비스에 대한 위임용으로 이 사용자 트러스트(Kerberos 만)"를 선택합니다.

이제 이 도메인 컨트롤러를 Kerberos 인증에 사용할 수 있습니다.

UNIX 에서 KDC 구성 예

다음 절차는 Kerberos 인증을 지원하도록 UNIX 호스트의 KDC Kerberos 영역을 구성하는 방법을 보여 줍니다. 이 예는 다음과 같은 서버 및 계정 이름을 사용합니다.

- 서버
도메인 컨트롤러: dc.example.com
정책 서버: smps.example.com
웹 서버: www.example.com
Active Directory 도메인: EXAMPLE
Kerberos 영역: EXAMPLE.COM
- 계정
사용자 계정: testkrb
웹 에이전트 서비스 계정: krbsvc-smwa
정책 서버 서비스 계정: krbsvc-smps

다음 단계를 수행하십시오.

1. 필요한 경우 MIT Kerberos 를 설치합니다.
2. kdb5_util 명령을 사용하여 Kerberos 데이터베이스와 선택적 stash 파일을 생성합니다. stash 파일은 호스트 자동 부팅 시퀀스의 일부로 kadmind 및 krb5kdc 데몬을 시작하기 전에 KDC 를 자동으로 자체 인증하는 데 사용됩니다.

stash 파일과 keytab 파일은 모두 침입에 악용될 수 있는 진입점입니다. stash 파일을 설치할 경우 이 파일은 루트에서만 읽을 수 있고 백업되지 않아야 하며 KDC 로컬 디스크에만 있어야 합니다. stash 파일이 필요하지 않으면 -s 옵션 없이 kdb5_util 을 실행하십시오.

이 예에서는 `kdc.conf` 파일에 지정된 디렉터리에 다음과 같은 다섯 개의 데이터베이스 파일을 생성합니다.

- Kerberos 데이터베이스 파일 두 개: `principal.db` 및 `principal.ok`
- Kerberos 관리 데이터베이스 파일 한 개: `principal.kadm5`
- 관리 데이터베이스 잠금 파일 한 개: `principal.kadm5.lock`
- stash 파일 한 개: `.k5stash`

```
[root@rhasmit init.d]# kdb5_util create -r EXAMPLE.COM -s
Initializing database '/var/kerberos/krb5kdc/principal' for realm
'EXAMPLE.COM',
master key name 'K/M@EXAMPLE.COM'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key:
Re-enter KDC database master key to verify:
```

3. 프린서필(`testkrb`)을 생성합니다.
4. 웹 서버 호스트에 대한 사용자 프린서필(예: `testwakrb`), 호스트 프린서필(`HTTP/www.example.com@EXAMPLE.COM`), 서비스 프린서필(`krbsvc-smwa`)을 생성합니다. 호스트 계정을 생성하는 데 사용된 암호는 웹 서버 호스트에서 `ksetup` 유틸리티를 사용할 때 지정한 암호와 동일해야 합니다.
5. 정책 서버 호스트에 대한 사용자 프린서필(`testpskrb`), 호스트 프린서필(`smpls/smpl.example.com`), 서비스 프린서필(`krbsvc-smpls`)을 생성합니다. 호스트 계정을 생성하는 데 사용된 암호는 정책 서버 호스트에서 `ksetup` 유틸리티를 사용할 때 지정한 암호와 동일해야 합니다.
6. 다음과 같이 웹 서버 서비스 프린서필에 대한 `keytab` 파일을 생성합니다.

```
ktadd -k /tmp/krbsvc-smwa.keytab HTTP/www.example.com
```

7. 다음과 같이 정책 서버 서비스 프린서필에 대한 `keytab` 을 생성합니다.

```
ktadd -k /tmp/krbsvc-smpls.keytab smpls/smpl.example.com
```

UNIX 호스트에서 Kerberos 영역이 구성됩니다.

정책 서버에서 Kerberos 인증 구성

Kerberos 인증 체계를 사용하려면 다음과 같이 에이전트 구성 개체(ACO)를 수정해야 합니다.

1. 관리 UI에 로그인합니다.
2. "인프라", "에이전트 구성", "에이전트 구성 수정"을 차례로 클릭합니다.
3. 에이전트의 "에이전트 구성" 개체에 대한 편집 단추를 클릭합니다.
4. 에이전트 구성 개체에 다음 세 개의 매개 변수를 추가합니다.

매개 변수	값
KCCExt	.kcc
HttpServicePrincipal	웹 서버 프린서플 이름을 지정합니다. 예: HTTP/www.example.com@EXAMPLE.COM
SmpsServicePrincipal	정책 서버 프린서플 이름을 지정합니다. 예: smps.example.com@EXAMPLE.COM

정책 서버에서 다음 추가 단계를 완료하십시오.

- 정책 서버 프린서플을 포함하는 KDC의 keytab 파일을 정책 서버의 보안 위치로 배포합니다.
- Kerberos 구성 파일(krb5.ini)을 구성하여 Windows의 시스템 루트 경로 또는 UNIX의 KRB5_CONFIG에 넣습니다.

중요! 정책 서버는 Windows에 설치되어 있고 KDC는 UNIX에 배포된 경우 [Ksetup 유틸리티](#) (페이지 347)를 사용하여 정책 서버 호스트에서 추가 구성 작업을 수행하십시오.

추가 정보:

[정책 서버에서 Kerberos 구성 예제](#) (페이지 343)

정책 서버에서 Kerberos 구성 예제

다음 절차에서는 Kerberos 인증 체계를 지원하도록 Windows의 정책 서버를 구성하는 방법을 예로 보여 줍니다. Windows 및 UNIX에서의 구성은 다음 차이점을 제외하고 유사합니다.

- Windows에서 Kerberos 구성 파일은 C:\windows\krb5.ini에 있습니다. UNIX에서 이 파일은 KRB5_CONFIG 환경 변수가 정규화된 경로로 설정되어 있는 한 어느 위치에든 저장할 수 있습니다.
- keytab의 위치는 시스템에 따라 다릅니다. 예: C:\windows\krbsvc-smps.keytab (Windows) 또는 /opt/CA/siteminder/krbsvc-smps.keytab (UNIX). Kerberos 구성 파일의 default_keytab_name 구성 옵션은 파일에 대한 정규화된 경로를 지정합니다.
- UNIX keytab은 서비스 계정 keytab과 호스트 keytab을 하나의 keytab 파일로 병합합니다.

참고: 정책 서버는 Windows에 설치되어 있고 KDC는 UNIX에 배포된 경우 [Ksetup 유틸리티](#) (페이지 347)를 사용하여 정책 서버 호스트에서 필요한 추가 구성 작업을 수행하십시오.

다음 단계를 수행하십시오.

1. 정책 서버를 설치하고 구성합니다.
2. 정책 저장소 디렉터리 서비스를 설치하고 구성합니다.
3. 정책 서버를 참조하는 호스트 구성 개체를 추가합니다.

4. 에이전트 구성 개체를 생성하고 다음 세 개의 새 매개 변수를 추가합니다.

KCCExt

값: .kcc

HttpServicePrincipal

웹 서버 프린서플 이름을 지정합니다.

예: HTTP/www.example.com@EXAMPLE.COM

SmppsServicePrincipal

정책 서버 프린서플 이름을 지정합니다.

예: smpps@smpps.example.com

5. 사용자 디렉터리를 생성합니다.
6. 사용자 디렉터리에 사용자(예: testkrb)를 생성합니다.
7. 관리 UI 를 사용하여 새 인증 체계를 구성합니다. [Kerberos 인증 체계 구성](#) (페이지 346)을 참조하십시오.
8. 정책 도메인을 구성합니다.
9. 인증 체계를 사용하여 리소스를 보호할 영역을 추가합니다.
10. 사용자 testkrb 에 대해 액세스를 허용하는 규칙 및 정책을 추가합니다.
11. Kerberos 구성 파일(krb5.ini)을 구성하고 krb5.ini 를 Windows 시스템 루트 경로에 넣습니다. 정책 서버 프린서플 자격 증명이 포함된 Windows 2008 KDC keytab 파일을 사용하도록 krb5.ini 를 구성합니다. 다음의 샘플 krb5.ini 를 참조하십시오.

```
[libdefaults]
default_realm = EXAMPLE.COM
default_keytab_name = C:\WINDOWS\krbsvc-smpps.keytab
default_tkt_enctypes = rc4-hmac
default_tgs_enctypes = rc4-hmac
[realms]
EXAMPLE.COM = {
kdc = dc.example.com:88
default_domain = example.com
}
[domain_realm]
.example.com = EXAMPLE.COM
```

12. 정책 서버의 보안 위치에 대한 정책 서버 프린서펄 자격 증명이 포함된 Windows KDC keytab 파일을 배포합니다.

Windows 호스트의 정책 서버에 대해 Kerberos 인증이 구성되었습니다.

웹 서버에서 Kerberos 인증 구성

Windows 또는 UNIX 웹 서버가 Kerberos 인증을 지원하도록 구성하는 일반적인 단계는 다음과 같습니다.

1. Kerberos 인증 체계를 지원하는 웹 에이전트를 설치합니다.
2. 트러스트된 호스트를 정책 서버에 등록하고 웹 에이전트를 구성합니다.
3. 웹 서버 자격 증명이 포함된 keytab 파일(KDC에 생성됨)을 웹 서버의 안전한 위치에 배포합니다.
4. Kerberos 구성 파일(krb5.ini)을 구성합니다.
 - Kerberos 영역(도메인)에 대한 KDC를 구성합니다.
 - 웹 서버 프린서펄의 자격 증명이 포함된 keytab 파일을 사용하도록 krb5.ini를 구성합니다.
 - krb5.ini를 시스템 루트 경로(Windows의 경우) 또는 KRB5_CONFIG(UNIX의 경우)에 저장합니다.

중요! 웹 서버는 Windows에 설치되어 있고 KDC는 UNIX에 배포된 경우 [Ksetup 유틸리티](#) (페이지 347)를 사용하여 웹 서버에서 추가 구성 작업을 수행하십시오.

Windows 워크스테이션에서 Kerberos 인증 구성

Kerberos 인증을 지원하려면 몇 가지 Internet Explorer 설정이 필요하며 워크스테이션 호스트는 KDC 도메인에 추가됩니다.

중요! KDC가 UNIX에 배포된 경우 [Ksetup 유틸리티](#) (페이지 347)를 사용하여 워크스테이션에서 필요한 추가 구성 작업을 수행하십시오.

다음 단계를 수행하십시오.

1. KDC 도메인에 Windows 워크스테이션에 대한 호스트를 추가합니다.
2. KDC 에 생성된 사용자 계정을 사용하여 호스트에 로그인합니다.
3. 자격 증명을 자동으로 전달하도록 브라우저를 구성합니다.

Kerberos 인증 체계 구성

Kerberos 는 인증 및 싱글 사인온을 위한 플랫폼 독립적 아키텍처를 제공합니다. 이 인증 체계를 사용할 때는 작동 중인 Kerberos 설정이 있다고 가정합니다.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다. 자세한 내용은 "정책 서버 개체 복제"를 참조하십시오.

다음 단계를 수행하십시오.

1. "인프라", "인증"을 차례로 클릭합니다.
2. "인증 체계"를 클릭합니다.
3. "인증 체계 만들기"를 클릭합니다.
"인증 체계 유형의 새 개체 만들기"가 선택되어 있는지 확인합니다.
"확인"을 클릭합니다.
4. 이름을 입력합니다.
5. 보호 수준을 입력합니다. 기본값은 5 입니다.
6. (선택 사항) 이 인증 체계에 대해 활성화된 암호 정책을 선택합니다.
7. "인증 체계 유형" 목록에서 Kerberos 인증 템플릿"을 선택합니다.
8. "서버 이름", "대상", "프린서필 이름" 및 "사용자 DN" 정보를 입력합니다.
이러한 필드에 대한 설명은 "도움말"을 참조하십시오.

9. Kerberos 영역과 Windows 도메인 간의 매핑을 지정합니다. Kerberos 영역 하나를 여러 Windows 도메인에 매핑할 수 있습니다.

참고: "사용자 DN 조회" 필드에 DOMAIN 변수를 지정할 경우 영역과 도메인의 이름이 동일하더라도 이 매핑이 필요합니다.

10. 제출을 클릭합니다.

Kerberos 인증 체계가 저장되었습니다. 체계를 영역에 바인딩하십시오.

Windows 호스트에서 Kerberos 외부 영역 구성

Windows 워크스테이션이 UNIX 에 배포된 Kerberos KDC 를 사용하도록 하려면 Kerberos KDC 서버와 워크스테이션을 모두 구성해야 합니다.

Kerberos 영역에서 Windows 호스트의 호스트 프린서펄을 생성합니다. 다음 명령을 사용합니다.

```
kadmin.local: addprinc host/machine-name.dns-domain_name.
```

예를 들어 Windows 워크스테이션 이름이 W2KW 이고 Kerberos 영역 이름이 EXAMPLE.COM 인 경우 프린서펄 이름은 host/w2kw.example.com 입니다.

Kerberos 영역은 Windows 도메인이 아니므로 KDC 운영 환경이 작업 그룹의 구성원으로 구성되어야 합니다. 이 작업은 다음 절차를 따를 때 자동으로 수행됩니다.

1. Windows 도메인에서 호스트를 제거합니다.
2. 로컬 사용자 데이터베이스에 테스트 사용자(예: testkrb)를 추가합니다.
3. Kerberos 영역을 추가합니다.

```
ksetup /SetRealm EXAMPLE.COM
```

4. 호스트를 다시 시작합니다.

5. KDC 를 추가합니다.

```
ksetup /addkdc EXAMPLE.COM rhasmit
```

6. 새 암호를 설정합니다.

```
ksetup /setmachpassword password
```

참고: 여기에 사용되는 암호는 MIT KDC 에서 호스트 프린서펄 계정을 생성하는 동안 사용된 암호와 동일합니다.

7. 호스트를 다시 시작합니다.

참고: 외부 KDC 및 영역 구성을 변경할 때마다 호스트를 다시 시작해야 합니다.

8. 영역 플래그를 설정합니다.

```
ksetup /SetRealmFlags EXAMPLE.COM delegate
```

9. AddKpasswd 를 실행합니다.

```
ksetup /AddKpasswd EXAMPLE.COM rhasmit
```

10. Ksetup 을 통해 Kerberos 프린서플에 대한 Windows 호스트 계정 간의 계정 매핑을 정의하여 로컬 워크스테이션 계정의 싱글 사인온을 구성합니다. 예를 들면 다음과 같습니다.

```
ksetup /mapuser testkrb@EXAMPLE.COM testkrb  
ksetup /mapuser * *
```

두 번째 명령은 클라이언트를 동일한 이름의 로컬 계정에 매핑합니다. 인수 없이 Ksetup 을 사용하여 현재 설정을 확인합니다.

SiteMinder Kerberos 인증 문제 해결

Kerberos 인증을 사용할 경우 다음 문제에 주의하십시오.

- 정책 서버 시스템 클록은 KDC 시스템 클록과 동기화(2 분 이내)되어야 합니다. 그렇지 않으면 클록 차이 오류로 인해 Kerberos 인증이 실패합니다.
- 모든 호스트의 /etc/hosts 파일에는 IP 주소, FQDN(정규화된 도메인 이름) 및 호스트 이름에 대한 적절한 항목이 있어야 합니다. 일부 경우에는 이러한 항목의 순서가 중요할 수 있습니다. 또한 이러한 항목 사이에는 다음과 같이 공백이 하나 이상 포함되어야 합니다.

```
IP Address FQDN hostname
```


- 자격 증명 캐시에 있는 티켓의 목록을 표시하려면 `klist`(UNIX KDC 클라이언트)를 사용하십시오. `-f` 플래그를 사용하면 티켓 플래그에 대한 정보가 제공됩니다. 이러한 티켓은 Kerberos 인증 프로세스를 완료하기 위해 전달됩니다.

예를 들어 다음에 나오는 샘플 `klist` 출력을 참조하십시오.

```
bash-2.05$ klist
Ticket cache: /tmp/krb5cc_1002
Default principal: HTTP/sol8sunone.test.com@TEST.COM

Valid starting          Expires                Service principal
Wed Dec 26 15:00:03 2007 Wed Dec 26 21:40:03 2007 krbtgt/TEST.COM@TEST.COM
```

- 항상 MIT KDC 호스트와 UNIX KDC 클라이언트의 사용자 및 서비스 프린서펄에 대해 `kinit` 프로그램을 사용하십시오.

사용자 프린서펄에 대한 `kinit` 구문은 다음과 같습니다.

```
kinit principalname
```

이 명령은 사용자 프린서펄을 생성하는 동안 사용된 암호를 요구합니다.

서비스 프린서펄에 대한 `kinit` 구문은 다음과 같습니다(호스트에 따라 다를 수 있음).

```
kinit -k [-t keytab location containing service principal] principalname
```

`kinit` 명령은 `keytab` 파일을 사용하여 서비스 프린서펄을 인증하므로 암호를 요구하지 않습니다.

- 브라우저와 웹 서버 간에 교환되는 Kerberos 토큰을 확인하려면 워크스테이션에 네트워크 패킷 추적 유틸리티를 설치하십시오. TIR로 시작하는 토큰은 NTLM 토큰을 나타내고, YII로 시작하는 토큰은 Kerberos 토큰을 나타냅니다.
- KDC에서 암호화 유형을 변경한 후에는 워크스테이션에서 로그오프하십시오. 또한 Kerberos 구성이나 `keytab` 파일을 변경한 후에는 정책 서버 및 웹 서버 서비스를 다시 시작하십시오.
- KDC는 날짜가 지난 티켓을 지원하지 않습니다.
- MIT 상호 운용성을 위해 DES-CBC-MD5 및 DES-CBC-CRC 암호화 유형만 사용할 수 있습니다.
- 정책 서버 및 웹 에이전트 로그를 항상 사용하도록 설정하여 인증 오류 메시지를 기록하십시오.
- 호스트에 대한 `keytab` 파일의 이름 및 위치가 `krb5.conf` 파일의 이름 및 위치와 일치하는지 확인하십시오.

- SPN 은 항상 대/소문자를 구분합니다. 정책 서버 및 웹 서버 호스트에 대한 `krb5.keytab` 파일에는 호스트 및 서비스 프린서플이 포함되어 있어야 합니다.
- `ktpass` 유틸리티의 버전을 확인하십시오. `ktpass` 명령 도구 유틸리티는 Windows 지원 도구에 포함되어 있으며 MSDN 에서 다운로드하여 설치할 수 있습니다.
- `keytab` 파일을 생성하는 동안 사용된 암호화 유형을 항상 확인하십시오. Windows 는 기본적으로 RC4-HMAC 암호화를 지원합니다.
- `kvno`(Kerberos 버전 번호)를 확인하십시오. 서비스 프린서플의 `kvno` 는 `keytab` 파일의 `kvno` 와 일치해야 합니다. `keytab` 의 `kvno` 번호는 `keytab` 이 생성될 때 표시됩니다.

Windows Active Directory 에 대한 서비스 계정의 `kvno` 를 파악하려면 다음과 같이 ADSI Edit 을 사용하십시오.

1. 명령 프롬프트에서 `adsiedit.msc` 를 실행합니다.
2. 왼쪽의 "Domain [fqdn_ADhost]" 드롭다운에서 `CN=Users, DC=domain, DC=com` 아래의 서비스 계정으로 이동합니다.
3. 서비스 계정을 마우스 오른쪽 단추로 클릭하고 "속성"을 클릭합니다.
4. `msDs-KeyVersionNumber` 특성의 값이 서비스 계정에 대한 `keytab` 파일을 생성할 때 표시된 값과 일치하는지 확인합니다.

사용자 계정에 대한 `kvno` 는 암호가 변경될 때마다 변경됩니다. 버전 번호가 일치하지 않으면 계정과 `keytab` 을 생성하거나, `kvno` 가 `keytab` 의 `kvno` 와 일치하도록 암호를 변경하십시오.

UNIX MIT KDC 에 대한 서비스 계정의 `kvno` 를 파악하려면 `kvno` 유틸리티를 사용하십시오. 이 명령의 구문은 다음과 같습니다.

`Kvno principalname`

- `keytab` 파일 유효성 확인

Windows: 정책 서버 및 웹 에이전트에 Windows 지원 도구를 설치하여 `keytab` 파일이 유효한지 여부를 확인하십시오. 다음 명령을 실행합니다.

`Kinit -k -t <keytab file location> <respective spn>`

예를 들면 다음과 같습니다.

`kinit -k -t C:\Windows\webserver.keytab HTTP/websvriis6.test.com@KRISH.COM`

`keytab` 파일이 유효하면 이 명령은 오류를 반환하지 않습니다.

Solaris: 다음 명령을 실행하여 두 **keytab** 파일의 유효성을 모두 확인하십시오.

```
Kinit -k -t <keytab file> <SPN>
```

예를 들면 다음과 같습니다.

```
kinit -k -t host.keytab host/<fqdn>@DOMAIN.COM
```

```
kinit -k -t smps.keytab smps/<fqdn>@DOMAIN.COM
```

- 오류가 발생하지 않으면 **keytab** 파일이 정상이고 **krb.conf** 파일의 값이 유효한 것입니다.
- 오류가 발생하면 다음 명령을 사용하여 **SPN** 이 KDC 에서 유효한지 확인하십시오.

```
Kinit host/<fqdn>@DOMAIN.COM
```

이 명령은 일반적으로 암호를 요구합니다. 유효한 암호를 제공하면 오류 메시지가 표시되지 않습니다. 이 명령이 암호를 요구하지 않으면 **SPN** 이 식별되지 않은 것입니다. 해당 개체의 속성을 확인하십시오. **SPN** 항목은 "계정" 탭에 있습니다(예: *host/fqdn*). 다른 개체에 **SPN** 과 동일한 항목 집합이 있으면 안 됩니다.

정보 카드 인증 체계

ICAS(정보 카드 인증 체계) 기능을 사용하면 여러 정보 카드 인증 체계를 생성할 수 있습니다. 각 정보 카드 인증 체계는 사용자 지정 인증 체계로 구성됩니다.

정보 카드는 지갑에 넣고 다니는 실제 카드와 비슷합니다. 각 정보 카드는 아이덴티티 정보 집합을 나타냅니다. 예를 들어 운전 면허증을 나타내는 정보 카드에는 사진, 생년월일, 성 및 이름, 운전 면허 번호 등의 중요한 아이덴티티 정보가 포함될 수 있습니다. 정보 카드를 사용하면 사용자가 자신의 아이덴티티 정보를 관리할 수 있습니다. 사용자는 자신의 정보 카드와 관련 아이덴티티 정보를 볼 수 있습니다. 또한 특정 정보 교환을 위해 사용 가능한 카드 중 하나를 선택하고 선택한 카드와 연결된 아이덴티티 정보의 공개 권한을 부여할 수 있습니다.

아이덴티티 선택기는 정보 카드를 노출하는 응용 프로그램입니다.

아이덴티티 선택기 소개

아이덴티티 선택기는 사용자가 자신의 아이덴티티 정보뿐 아니라 신뢰 당사자 및 아이덴티티 공급자와의 온라인 관계도 관리할 수 있게 해 주는 응용 프로그램입니다. RP(신뢰 당사자)는 사용자를 인증하기 위해 아이덴티티 정보를 필요로 하는 웹 사이트, 응용 프로그램 또는 서비스입니다. IdP(아이덴티티 공급자)는 아이덴티티 정보를 인증하고 사용자가 신뢰 당사자와 공유할 수 있는 보안 토큰을 생성하는 제 3 자입니다.

아이덴티티 선택기를 사용하면 사용자가 다수의 사용자 이름 및 암호를 관리하지 않고도 웹 기반 리소스에 액세스할 수 있습니다. 또한, 기업은 더 이상 부정확하거나 악용될 가능성이 있는 사용자 아이덴티티 정보의 데이터베이스를 유지 관리할 필요가 없습니다. 사용자 및 데이터베이스의 유지 관리가 사라지면 리스크와 법적 책임이 줄고 민첩성이 개선됩니다.

또한 사용자는 아이덴티티 선택기를 사용하여 각 신뢰 당사자에게 공개되는 아이덴티티 정보를 제어할 수 있습니다. 마지막으로, 아이덴티티 선택기는 사용자에게 일관된 사용자 인터페이스와 뛰어난 사용자 환경을 제공합니다.

Windows CardSpace

Windows CardSpace 는 Microsoft 가 구현한 아이덴티티 선택기입니다. CardSpace 는 사용자가 신뢰 당사자 또는 아이덴티티 공급자와 상호 작용하는 데 사용할 수 있는 일관된 사용자 인터페이스를 제공합니다. 정책 서버는 ICAS(정보 카드 인증 체계)라는 사용자 지정 인증 체계를 통해 Windows CardSpace 를 지원합니다.

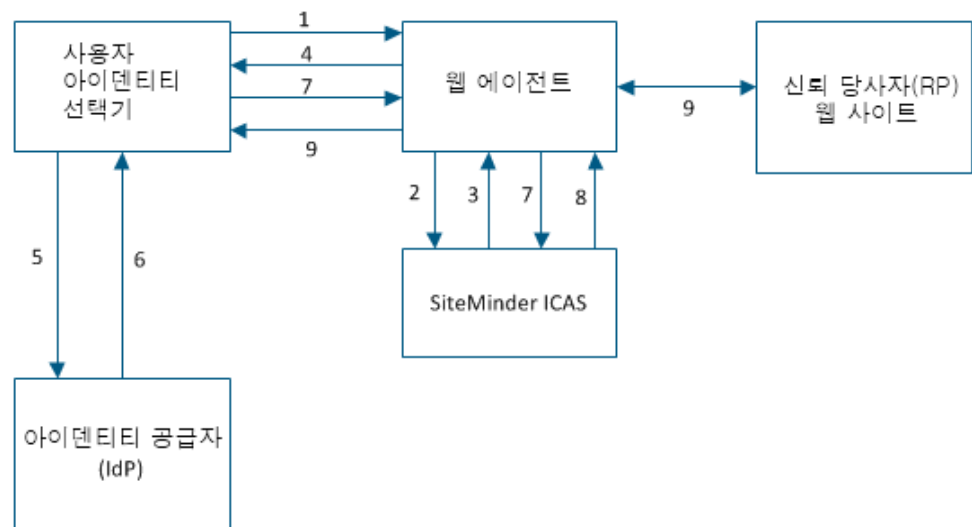
SiteMinder ICAS(정보 카드 인증 체계)

정책 서버에서 제공되는 ICAS(정보 카드 인증 체계)는 Windows CardSpace 를 지원합니다. 각 ICAS 인스턴스는 관리 UI 에서 사용자 지정 인증 체계로 구성되며 다른 사용자 지정 인증 체계와 마찬가지로 방식으로 구현됩니다.

ICAS 개요

ICAS 를 사용한 사용자 인증은 다음과 같은 구성 요소 및 단계가 필요합니다.

- 사용자
- 아이덴티티 선택기
- 웹 에이전트
- RP(신뢰 당사자)
- IdP(아이덴티티 공급자)



1. 사용자가 보호된 웹 사이트나 RP(신뢰 당사자)에 방문하려고 합니다.
2. 웹 에이전트가 사용자의 요청을 가로채고 ICAS 를 호출합니다.
3. ICAS 가 RP 정책 요구 사항을 웹 에이전트로 보냅니다.
4. 웹 에이전트가 사용자 컴퓨터에서 아이덴티티 선택기를 시작하도록 브라우저에 지시하고 RP 의 정책 요구 사항을 보냅니다.
5. 아이덴티티 선택기가 정책 요구 사항을 읽고 사용자를 위해 요구 사항을 충족하는 정보 카드를 강조 표시합니다. 사용자는 강조 표시된 카드 중 하나를 선택합니다. 아이덴티티 선택기는 사용자의 자격 증명을 수집한 후 인증을 위해 IdP(아이덴티티 공급자)로 보냅니다. 또한 아이덴티티 선택기는 RP 정책 요구 사항을 IdP 로 보내고 토큰을 요청합니다.

참고: 사용자는 RP 에 필요하지 않은 선택적 클레임이 포함된 카드를 선택할 수 있습니다.

6. IdP 가 사용자를 인증하고 정책 요구 사항을 처리합니다. IdP 는 필요한 클레임이 포함된 토큰을 생성한 후 다시 아이덴티티 선택기로 보냅니다.

7. 아이덴티티 선택기가 클레임을 표시하면 사용자는 해당 클레임을 RP 에 공개하는 것을 승인합니다.
8. ICAS 가 토큰의 암호를 해독하고 토큰의 신뢰성 및 무결성을 확인한 다음 사용자의 클레임을 사용자 데이터베이스에 있는 사용자 아이덴티티에 연결합니다. 그러면 정책 서버는 표준 정책 기반 권한 부여를 수행하고 권한이 부여된 경우 사용자에게 액세스 권한을 부여합니다.
9. 사용자가 웹 사이트에 액세스합니다.

ICAS 용어

다음 용어는 ICAS 를 이해하는 데 유용합니다.

아이덴티티 메타 시스템

사용자, 신뢰 당사자 및 아이덴티티 공급자가 아이덴티티 정보를 공유하는 방식을 지정하는 아키텍처입니다.

사용자

공유되는 아이덴티티 정보의 소유자입니다. 이 사용자를 주체라고도 합니다.

RP(신뢰 당사자)

아이덴티티 정보를 요청하고 소비하는 웹 사이트입니다.

IdP(아이덴티티 공급자)

아이덴티티 정보를 인증하고, 공유 토큰을 생성하여 이 정보를 신뢰 당사자와 공유하는 제 3 자입니다. 아이덴티티 공급자의 예로는 신용 카드 회사, 은행, 정부 기관, 고용주 및 보험 회사가 있습니다.

STS(보안 토큰 서비스)

아이덴티티 공급자가 보안 토큰을 생성하는 데 사용하는 기술입니다. 보안 토큰 서비스는 다음 작업을 수행합니다.

- 사용자를 인증합니다.
 - 다음과 같은 보안 토큰을 생성합니다.
 - 신뢰 당사자의 요구 사항과 사용자의 제한 사항에 따라 각기 다른 아이덴티티 정보 하위 집합을 포함하는 보안 토큰
 - 다양한 유형의 보안 토큰
- 참고:** SAML 1.0 및 1.1 사양이 지원됩니다.
- 보안을 위해 암호화되고 신뢰성 및 무결성을 위해 서명된 보안 토큰

보안 토큰

암호화 방식으로 서명되고 암호화된 클레임 집합입니다.

클레임

사실에 대한 어설션입니다. 각 토큰에는 사용자의 아이덴티티에 대한 클레임이 하나 이상 포함됩니다. 클레임의 예로는 이름, 성, 전자 메일 주소, 생년월일 등이 있습니다. 사용자 또는 타사 아이덴티티 공급자가 클레임을 생성할 수 있습니다.

정보 카드

아이덴티티 정보 집합입니다. 정보 카드는 지갑에 넣고 다니는 실제 카드와 비교할 수 있습니다. 예를 들어 운전 면허증에 해당하는 정보 카드에는 사진, 생년월일, 성 및 이름, 운전 면허 번호, 시/도, 신장, 성별 등의 중요한 아이덴티티 정보가 포함될 수 있습니다.

개인 카드

사용자가 자신에 대해 어설션하지만 제 3 자가 확인하지는 않는 클레임이 포함된 정보 카드입니다. 개인 카드에는 카드가 생성될 때 함께 생성된 PPID(Private Personal Identifier)가 포함되어 있습니다. 개인 카드는 전자 메일 주소와 같이 중요도가 낮은 아이덴티티 정보에 적합합니다.

참고: 개인 카드를 자체 발급 카드라고도 합니다.

관리되는 카드

사용자가 자신에 대해 어설션하며 제 3 자가 확인하는 클레임이 포함된 정보 카드입니다. 관리되는 카드에는 카드가 생성될 때 함께 생성된 PPID(Private Personal Identifier)와 아이덴티티 공급자의 STS 에 대한 포인터가 포함되어 있습니다. 관리되는 카드는 신용 카드 번호와 같이 중요한 아이덴티티 정보에 적합합니다.

아이덴티티 선택기

사용자가 신뢰 당사자 및 아이덴티티 공급자와의 관계를 관리하고 자신의 아이덴티티 정보가 공유 및 사용되는 방식을 제어할 수 있게 해주는 응용 프로그램입니다. 아이덴티티 선택기는 다음과 같은 기능을 합니다.

- 여러 통신 프로토콜 및 보안 기술을 사용하는 당사자 간에 정보를 공유할 수 있도록 합니다.
- 정보 카드를 사용하는 여러 아이덴티티 공급자 및 신뢰 당사자 간에 일관된 사용자 인터페이스를 제공합니다.

- 각 아이덴티티 정보 교환에 사용할 수 있는 정보 카드를 강조 표시합니다.
- 사용자가 아이덴티티 정보를 확인하고 이를 공유하는 데 동의할 수 있도록 합니다.

Windows CardSpace

Microsoft 의 Windows 운영 체제용 아이덴티티 선택기입니다.

ICAS(정보 카드 인증 체계)

Microsoft 의 아이덴티티 선택기인 Windows Cardspace 를 지원하며 SiteMinder 에서 사용자 지정 인증 체계로 구현됩니다.

PPID(Private Personal Identifier)

정보 카드가 생성될 때 아이덴티티 선택기에 의해 생성되는 식별자입니다.

ICAS 파일

ICAS 의 각 인스턴스를 구성하려면 fcc 파일과 속성 파일이 필요합니다.

filename.fcc

ICAS 의 각 인스턴스에 대해 사용자 지정할 수 있는 인증 설정을 지정합니다.

InfoCard.fcc

웹 에이전트 키트와 함께 제공되는 샘플 fcc 파일입니다.

filename.properties

ICAS 인스턴스의 동작을 지정합니다.

InfoCard.properties

샘플 속성 파일입니다.

참고: 관리 UI 에서 ICAS 인스턴스를 구성할 때 관리자는 속성 파일의 경로를 지정합니다.

ICAS 사전 요구 사항

ICAS 를 구축하려면 먼저 다음 조건이 충족되어야 합니다.

웹 브라우저 구성

다음 웹 브라우저 중 하나를 사용하십시오.

- Internet Explorer 7.0
- CardSpace 플러그인이 설치된 Firefox 2.x

웹 서버 구성

웹 서버가 SSL 을 통해 통신하도록 구성되어야 합니다. 이 구성은 fcc 파일을 보호합니다.

참고: 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.

웹 에이전트 구성

웹 에이전트 키트와 함께 제공되는 InfoCard.fcc 는 ICAS 의 각 인스턴스에 맞게 사용자 지정되어야 합니다.

참고: 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.

JRE(Java Runtime Environment) 구성

JRE(Java Runtime Environment)는 강력한 암호화 알고리즘으로 암호화된 보안 토큰을 암호 해독하도록 구성되어야 합니다.

정책 서버 구성

정책 서버 구성에는 다음 태스크가 포함됩니다.

- ICAS 속성 파일 구성
- 인증서 데이터 저장소 구성
- ICAS 에 맞게 사용자 디렉터리 구성
- ICAS 의 인스턴스 생성
- 클레임 값을 검색하는 활성 응답 구성

ICAS 에 맞게 JRE(Java Runtime Environment) 구성

JCE(Java Cryptography Extension) Unlimited Strength Jurisdiction Policy Files 를 설치하여 JRE(Java Runtime Environment)를 구성하십시오. 이러한 파일은 강력한 암호화 알고리즘으로 암호화된 보안 토큰의 암호를 해독하는 데 필요합니다.

중요! 새 정책 파일을 설치하기 전에 JRE 와 함께 제공되는 기본 정책 파일을 백업하십시오.

다음 단계를 수행하십시오.

1. <http://www.oracle.com/technetwork/java/index.html> 에서 JCE(Java Cryptography Extension) Unlimited Strength Jurisdiction Policy Files 를 다운로드합니다.
2. 이 파일을 \$NETE_JRE_ROOT\lib\security 디렉터리에 설치합니다.
3. \$NETE_JRE_ROOT\lib\security\java.security 파일에 다음 행을 추가합니다.
`security.provider.7=com.rsa.jsafe.provider.JsafeJCE`

ICAS 용 정책 서버를 구성하는 방법

ICAS 용 정책 서버 구성 단계에는 다음이 포함됩니다.

1. ICAS 속성 파일을 구성합니다.
2. 나중에 활성 응답에서 사용할 수 있도록 요청을 저장합니다.
3. ICAS 를 위한 인증서 데이터 저장소를 구성합니다.
4. ICAS 에 맞게 사용자 디렉터리를 구성합니다.
5. ICAS 인스턴스를 생성합니다.
6. 요청 값을 검색하는 활성 응답을 구성합니다.
7. ICAM 허용 목록에 대한 지원을 구성합니다.

ICAS 속성 파일을 구성합니다.

ICAS 속성 파일은 ICAS 인스턴스가 작동하는 방식을 지정합니다. 관리 UI 에서 ICAS 인스턴스를 구성할 때 관리자는 관련 속성 파일의 경로를 지정합니다. 새 속성 파일을 구성하려면 텍스트 편집기에서 샘플 속성 파일을 열고 내용을 편집합니다. 항상 새 속성 파일을 저장하고 이름을 바꾸십시오.

참고: 여러 ICAS 인스턴스가 동일한 속성 파일을 사용할 수 있습니다.

예: InfoCard.properties 라는 속성 파일에는 다음과 같은 속성 및 샘플 값이 있습니다.

fcc

정보 카드 fcc 파일의 위치를 지정합니다.

예: fcc=https://web_server_home/siteminderagent/forms/InfoCard.fcc

참고: 아이덴티티 선택기를 활성화하려면 "https"를 지정하십시오.

vppid_attribute

VPPID 특성 값을 지정합니다. 명령 UpdateUserStoreWithVPPID 는 사용자 특성을 업데이트하기 위해 이 특성이 필요합니다.

예: vppid_attribute=mail

vppid_claim

사용자 명확성 처리에 필요한 클레임을 지정합니다.

예:

vppid_claim=http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname

vppid_claim=http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname

vppid_claim=http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

alias

신뢰 당사자의 SSL 인증서를 검색하는 데 사용되는 인증서 데이터 저장소의 키를 지정합니다.

예: alias=rpssl

guestuser

ICAS 가 익명 모드로 구성된 경우 이 설정은 게스트 사용자 로그인을 지정합니다.

예: guestuser=guest

tokenPrim

tokenPrim 인터페이스의 공급자를 지정합니다.

예: tokenPrim=com.ca.sm.authscheme.infocard.higgins.TokenAdapter

storeclaims_attribute

StoreClaimsToUserStore 명령을 실행할 때 클레임이 저장되는 사용자 특성을 지정합니다.

예: storeclaims_attribute=description

preprocessingchain

사용자 명확성 처리 과정에서 실행할 명령 체인을 정의합니다.

예: preprocessingchain=+vppidchain

참고: 자세한 내용은 [ICAS 명령 체인 구성](#) (페이지 361)을 참조하십시오.

postprocessingchain

사용자 인증 시 실행할 명령 체인을 정의합니다.

예:

postprocessingchain=+vppidchain;com.ca.sm.icas.command.StoreClaimsToContext

참고: 자세한 내용은 [ICAS 명령 체인 구성](#) (페이지 361)을 참조하십시오.

errorprocessingchain

오류 처리 동안 실행할 명령 체인을 정의합니다.

참고: 자세한 내용은 [ICAS 명령 체인 구성](#) (페이지 361)을 참조하십시오.

whiteListLocation

(선택 사항) 연방 ICAM(Identity, Credentialing, and Access Management)에서 지정한 허용 목록을 포함하는 XML 파일의 위치를 정의합니다.

예: whiteListLocation=C:\\Program Files\\ca\\siteminder\\config\\WhiteList.xml

참고: ICAM 허용 목록에 대한 자세한 내용은 [ICAM 허용 목록에 대한 지원 구성](#) (페이지 370)을 참조하십시오.

ICAS 명령 체인 구성

명령 체인은 ICAS 속성 파일에서 정의합니다. 체인이란 순서대로 실행되는 명령의 집합입니다.

명명된 명령 체인은 다음과 같습니다.

- preprocessing
- postprocessing
- errorprocessing

이러한 명명된 체인은 기본적으로 표시됩니다.

다음 정보를 고려하십시오.

- ICAS 속성 파일에 특정 명명된 체인이 있는 경우 ICAS 는 이러한 명명된 체인을 사용합니다.
- 고유한 체인을 정의한 다음 ICAS 속성 파일에 넣고 명명된 체인에서 참조할 수 있습니다.
- 사용자 지정된 체인이 이러한 명명된 명령 체인 중 어디에서도 참조되지 않는 경우 해당 체인의 실행은 무시됩니다.

요구 사항에 따라 다음 클래스 파일을 구성하십시오.

- [ICAS 를 구성하기 위한 키 클래스 파일](#) (페이지 362)
- [요청 값을 확인하기 위한 클래스 파일](#) (페이지 363)
- [디버그하기 위한 클래스 파일](#) (페이지 364)

ICAS 를 구성하기 위한 키 클래스 파일

ICAS 를 구성하는 데 사용되는 키 클래스 파일은 다음과 같습니다.

com.ca.sm.icas.StoreClaimsToSessionStore

추출된 클레임을 정책 서버의 세션 저장소에 저장합니다.

com.ca.sm.icas.command.ExecuteClaimChain

클레임을 통해 명령 집합을 실행합니다. 네임스페이스의 마지막 부분을 구성하는 각 클레임 이름에 대해 ICAS 는 속성 파일에서 chainID.claimID 로 정의된 체인을 찾습니다. 체인 정의를 찾으면 ICAS 는 이를 실행하고 특정 클레임과 함께 컨텍스트를 전달합니다.

예:

executeClaimCommand1=com.ca.sm.icas.command.ExecuteClaimChain 의 경우 전자 메일 클레임을 다음과 같이 정의합니다.

executeClaimCommand1.emailaddress=com.ca.sm.icas.command.DumpClaimsCommand;

emailaddress 클레임이 있는 토큰을 찾은 경우
DumpClaimsCommand 를 처리합니다.

com.ca.sm.icas.command.HashVPPID

VPPID 클레임 특성의 해시를 생성합니다.

com.ca.sm.icas.command.SetVPPIDAsAnonymous

VPPID 클레임 특성 값을 익명으로 설정합니다. 이 클래스 파일은 사용자 계정에 연결되지 않은 정보 카드로 로그인하기 위해 사용됩니다(익명 액세스).

com.ca.sm.icas.command.SetVPPIDFromToken

정보 카드 토큰의 VPPID 클레임 특성 값을 컨텍스트 개체로 설정합니다.

com.ca.sm.icas.command.StopChain

true 값을 반환하며 현재 실행 중인 체인의 실행이 중지됩니다.

com.ca.sm.icas.command.StoreClaimsToContext

정보 카드 토큰에서 클레임을 읽어 응용 프로그램 관련 컨텍스트에 저장합니다.

com.ca.sm.icas.command.StoreClaimsToUserStore

정보 카드 토큰에서 읽은 클레임을 사용자 디렉터리의 ICAS 속성 파일에 있는 지정된 사용자 특성에 저장합니다.

com.ca.sm.icas.command.TransformScriptInClaim

클레임에서 HTML 엔터티를 사용하여 스크립트 태그(<, >)를 이스케이프합니다. 예를 들어 <td>는 <td;> 가 됩니다.

com.ca.sm.icas.command.TransformSqlInClaim

클레임 값의 문자를 이스케이프하여 SQL 쿼리로 전달될 수 있게 합니다.

com.ca.sm.icas.command.TranslateErrorCode

컨텍스트 내에서 찾은 예외 문자열을 변환합니다. 이 변환된 문자열은 FCC 에서 사용할 수 있는 context.userText 에 다시 저장됩니다.

com.ca.sm.icas.command.TranslateErrorCodeFromParms

ICAS 속성 파일 내에서 찾은 예외 문자열을 변환합니다. 이 변환된 문자열은 FCC 에서 사용할 수 있는 context.userText 에 다시 저장됩니다.

com.ca.sm.icas.command.UpdateUserStoreWithVPPID

정보 카드 토큰에서 읽은 클레임을 사용자 디렉터리의 ICAS 속성 파일에 있는 지정된 사용자 특성에 저장합니다.

요청 값을 확인하기 위한 클래스 파일

요청 값을 확인하는 데 사용되는 클래스 파일은 다음과 같습니다.

com.ca.sm.icas.StoreClaimsToSessionStore

추출된 클레임을 정책 서버의 세션 저장소에 저장합니다.

com.ca.sm.icas.command.ErrorIfEmptyClaim

요청이 비어 있는 경우 예외를 생성합니다.

com.ca.sm.icas.command.ErrorIfMultiValueClaim

지정된 요청에 여러 값이 있는 경우 예외를 생성합니다.

com.ca.sm.icas.command.ErrorIfNotEmptyClaim

지정된 요청이 비어 있지 않은 경우 예외를 생성합니다.

com.ca.sm.icas.command.ErrorIfNotMultiValueClaim

지정된 요청이 다중 값이 아닌 경우 예외를 생성합니다.

com.ca.sm.icas.command.ErrorIfNotNullClaim

지정된 요청이 null 이 아닌 경우 예외를 생성합니다.

com.ca.sm.icas.command.ErrorIfNotSingleValueClaim

지정된 요청이 단일 값이 아닌 경우 예외를 생성합니다.

com.ca.sm.icas.command.ErrorIfNullClaim

지정된 요청이 null 인 경우 예외를 생성합니다.

com.ca.sm.icas.command.ErrorIfSingleValueClaim

지정된 요청이 단일 값인 경우 예외를 생성합니다.

디버그하기 위한 클래스 파일

디버깅 용도로 사용되는 클래스 파일은 다음과 같습니다.

com.ca.sm.icas.command.debug.DumpChainID

체인 ID 를 콘솔에 표시합니다.

참고: 출력을 보려면 정책 서버를 콘솔 모드로 시작하십시오.

com.ca.sm.icas.command.debug.DumpClaim

콘솔에 VPPID 클레임 상세 정보(이름과 값)를 표시합니다.

참고: 출력을 보려면 정책 서버를 콘솔 모드로 시작하십시오.

com.ca.sm.icas.command.debug.DumpClaims

토큰에 있는 모든 클레임에 대한 상세 정보를 콘솔에 표시합니다.

참고: 출력을 보려면 정책 서버를 콘솔 모드로 시작하십시오.

com.ca.sm.icas.command.debug.DumpContext

컨텍스트 개체에 대한 상세 정보를 콘솔에 표시합니다.

참고: 출력을 보려면 정책 서버를 콘솔 모드로 시작하십시오.

com.ca.sm.icas.command.debug.DumpParameters

ICAS 속성 파일에 지정된 매개 변수에 대한 상세 정보를 콘솔에 표시합니다.

참고: 출력을 보려면 정책 서버를 콘솔 모드로 시작하십시오.

com.ca.sm.icas.command.debug.DumpSystemVars

시스템 환경에 대한 상세 정보를 콘솔에 표시합니다.

참고: 출력을 보려면 정책 서버를 콘솔 모드로 시작하십시오.

com.ca.sm.icas.command.debug.DumpThreadStack

실행 중인 스레드에 대한 스택 추적을 콘솔에 표시합니다.

참고: 출력을 보려면 정책 서버를 콘솔 모드로 시작하십시오.

com.ca.sm.icas.command.debug.GenerateClaim_claims_AsHTML

알려진 클레임을 나타내는 HTML 테이블을 포함하는 새 클레임 "_claims_"를 생성합니다. 활성 응답에서 이 클레임을 사용하여 검색된 클레임을 사용자에게 표시하는 쿠키나 헤더를 생성할 수 있습니다.

com.ca.sm.icas.command.debug.GenerateClaim_parameters_AsHTML

ICAS 속성 파일에 지정된 매개 변수를 나타내는 HTML 테이블을 생성합니다. 활성 응답에서 이 HTML 테이블을 사용하여 검색된 클레임을 사용자에게 표시하는 쿠키나 헤더를 생성할 수 있습니다.

com.ca.sm.icas.command.debug.LogClaim

체인 컨텍스트의 클레임 상세 정보(이름과 값)를 정책 서버 추적 로그에 기록합니다.

com.ca.sm.icas.command.debug.LogClaims

토큰의 모든 클레임에 대한 상세 정보를 정책 서버 추적 로그에 기록합니다.

com.ca.sm.icas.command.debug.LogDecryptedClaims

암호 해독된 XML 토큰을 정책 서버 추적 로그에 기록합니다.

com.ca.sm.icas.command.debug.LogEncryptedClaims

IDP 에서 가져온 암호화된 토큰을 정책 서버 추적 로그에 기록합니다.

com.ca.sm.icas.command.debug.START

START 메시지를 콘솔에 표시합니다.

참고: 출력을 보려면 정책 서버를 콘솔 모드로 시작하십시오.

com.ca.sm.icas.command.debug.STOP

STOP 메시지를 콘솔에 표시합니다.

참고: 출력을 보려면 정책 서버를 콘솔 모드로 시작하십시오.

com.ca.sm.icas.command.debug.ThrowException

클레임 값을 메시지의 일부로 포함하는 예외 개체를 생성합니다.

나중에 활성 응답에서 사용할 수 있도록 클레임 저장

나중에 활성 응답에서 사용할 수 있도록 클레임을 저장할 수 있습니다. 나중에 사용할 수 있도록 클레임을 저장하려면 속성 파일에 다음 속성을 추가하십시오.

postprocessingchain

사용자 인증 시 실행할 명령 체인을 정의합니다. 이 단계에는 클레임 변환 및 저장 명령이 포함됩니다.

예:

```
postprocessingchain=com.ca.sm.authscheme.infocard.command.StoreClaimsToContext
```

ICAS 에 대해 인증서 데이터 저장소 구성

다음 정보를 고려하십시오.

- 신뢰 당사자는 SSL 을 사용하여 fcc 파일을 보호해야 합니다.
- 신뢰 당사자는 웹 사이트와 연결된 SSL 인증서를 pfx 파일로 내보내야 합니다.
- 정책 저장소 관리자는 신뢰 당사자 웹 사이트에서 SSL 인증서를 가져와서 인증서 데이터 저장소를 ICAS 에 대해 구성합니다.
- 가져온 인증서는 fcc 파일에 저장되는 별칭과 연결됩니다. 인증서의 개인 키를 사용하여 암호 토큰을 암호 해독하고 디지털 서명을 확인합니다.

다음 단계를 수행하십시오.

1. 웹 서버 인증서 마법사를 사용하여 SSL 인증서를 IIS 웹 서버에서 pfx 파일로 내보냅니다.

참고: 자세한 내용은 Microsoft 설명서를 참조하십시오. pfx 파일에서 SSL 인증서를 가져오기 위해 정책 서버는 SSL 인증서를 pfx 파일에 내보낼 때 제공하는 암호를 사용합니다.

2. 관리 UI 를 사용하여 SSL 인증서를 인증서 데이터 저장소로 가져옵니다.

ICAS 에 맞게 사용자 디렉터리 구성

사용자를 인증하기 위해서는 ICAS 에 제공된 클레임 중 하나와 사용자 데이터베이스의 사용자 특성 간에 일치 항목을 찾아야 합니다. 토큰 디스어셈블리 중에는 지정된 클레임 값이 사용자 디렉터리에서 조회 값으로 사용됩니다. 따라서 LDAP 조회 문자열이나 SQL 쿼리 체계가 지정된 클레임에 해당하는 사용자 특성을 지정하도록 사용자 디렉터리를 구성하십시오.

다음 예에서는 전자 메일 주소에 대한 LDAP 조회 문자열 및 SQL 쿼리 체계를 구성하는 방법을 보여 줍니다.

LDAP 예제

LDAP 사용자 DN 조회

시작

(mail=

끝

)

SQL 예제

SQL 쿼리

사용자/그룹 정보 가져오기

```
SELECT EmailAddress, 'User' FROM SmUser WHERE EmailAddress = '%s'
UNION SELECT Name, 'Group' FROM SmGroup WHERE Name = '%s'
```

사용자 인증

```
SELECT EmailAddress FROM SmUser WHERE EmailAddress = '%s' AND
Password = '%s'
```

ICAS 의 인스턴스 만들기

관리 UI 에서 사용자 지정 인증 체계를 지정하여 ICAS 의 인스턴스를 생성할 수 있습니다.

제한: 각 정책 저장소는 최대 10 개의 ICAS 인스턴스를 지원할 수 있습니다.

다음 단계를 수행하십시오.

1. "인프라", "인증"을 차례로 클릭합니다.
2. "인증 체계"를 클릭합니다.
3. "인증 체계 만들기"를 클릭합니다.
4. "Create a new object of type Authentication Scheme"(인증 체계 유형의 새 개체 만들기)를 선택하고 "확인"을 클릭합니다.
5. 인증 체계의 이름과 설명을 입력합니다.
6. "인증 체계 유형" 목록에서 "사용자 지정 템플릿"을 선택합니다.
"체계 설정" 그룹 필드가 표시됩니다.
7. "보호 수준" 필드에 값을 입력합니다.
8. 이 인증 체계 유형에 대해 활성화된 "암호 정책"의 선택을 취소합니다.
참고: ICAS 는 암호 정책을 지원하지 않습니다.
9. "체계 설정"에 다음 필드에 대한 값을 입력합니다.

라이브러리

smjavaapi

참고: 사용자 지정 인증 체계는 Java 인증 API 를 사용합니다.

암호 및 암호 확인

이 필드는 비워 둡니다.

참고: 사용자 지정 인증 체계는 공유 암호를 사용하지 않습니다.

매개 변수

"매개 변수" 필드에 다음 두 개의 매개 변수를 공백으로 구분하여 입력합니다.

com.ca.sm.icas.SmAuthInfoCard

SmAuthScheme 인터페이스를 구현하는 클래스의 정규화된 이름입니다.

policy_server_home\config\icas\InfoCard.properties

속성 파일의 위치입니다.

예:

```
com.ca.sm.icas.SmAuthInfoCard
policy_server_home\config\icas\InfoCard.properties
```

10. (선택 사항) "체계 설정"에서 "Store Auth Scheme Context to Session Store"(인증 체계 컨텍스트를 세션 저장소에 저장) 옵션을 선택합니다. 이 옵션은 인증 컨텍스트 데이터가 유지되도록 지정합니다.

11. 제출을 클릭합니다.

"인증 체계 만들기" 태스크가 처리를 위해 제출됩니다.

요청 값을 검색하는 활성 응답 구성

인증이 완료된 후 클레임 값을 가져오는 활성 응답을 구성하려면 사용자 지정 클래스 com.ca.sm.icas.GetClaimValue 를 사용하십시오.

참고: 요청 값을 저장하고 검색하려면 세션 저장소가 필요합니다. 세션 저장소에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

다음 단계를 수행하십시오.

1. "정책", "도메인"을 차례로 클릭합니다.
2. "응답"을 클릭합니다.
3. "응답 만들기"를 클릭합니다.
4. 도메인을 선택하고 "다음"을 클릭합니다.
5. 응답의 이름과 설명을 입력합니다.
6. "에이전트 유형"으로 웹 에이전트를 지정합니다.
7. "특성 목록"에서 "응답 특성 만들기"를 클릭합니다.

8. "특성 유형"의 특성 목록에서 "WebAgent-HTTP-Header-Variable" 또는 "WebAgent-HTTP-Cookie-Variable"을 선택합니다.
9. "특성 설정"에서 "특성 종류"로 "활성 응답"을 선택합니다.
10. "특성" 필드에 다음 값을 입력합니다.

쿠키 또는 변수 이름

요청의 이름을 지정합니다.

예: emailaddress

라이브러리 이름

라이브러리의 이름을 지정합니다.

값: smjavaapi

함수 이름

함수의 이름을 지정합니다.

값: JavaActiveExpression

매개 변수

정보 카드 모델에 따라 표준 요청 유형을 정의하는 claims.xsd 파일의 위치와 사용자 지정 ICAS 명령을 지정합니다.

예: com.ca.sm.authscheme.infocard.GetClaimValue

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

11. "확인"을 클릭합니다.

요청 값을 검색하는 응답이 생성됩니다.

ICAM 허용 목록에 대한 지원 구성

ICAS 구현에서는 LOA 권한 부여 및 발급자의 허용 목록을 기반으로 하는 연방 Identity, Credentialing, and Access Management Identity Metasystem Interoperability 1.0 Profile(ICAM IMI 1.0 Profile) 사양을 지원합니다.

참고: 허용 목록 및 LOA 지원에 대한 자세한 내용은 *ICAM IMI 1.0 Profile Release Candidate*(ICAM IMI 1.0 Profile 릴리스 후보)를 참조하십시오.

허용 목록 처리가 사용되도록 설정하려면 *Infocard.properties* 파일에서 다음 매개 변수를 업데이트하십시오.

postprocessingchain

사용자 인증 시 실행할 명령 체인을 정의합니다.

예: `postprocessingchain=com.ca.sm.icas.whiteListChecker.whiteListChecker`

whitelistlocation

ICAM 에서 지정한 허용 목록을 포함하는 XML 파일의 위치를 정의합니다.

예: `whitelistlocation=C:\\Program
Files\\ca\\siteminder\\config\\WhiteList.xml`

ICAS 구현에서는 다음 3 가지 LOA(보증 수준)를 확인할 수 있습니다.

- LOA1
- LOA2
- LOA3

LOA1, LOA2 및 LOA3 을 확인하려면 허용 목록 처리가 필요합니다. LOA 처리를 지원하려면 `postprocessingchain` 매개 변수에 다음 정보를 추가하십시오.

- LOA1 처리의 경우

```
postprocessingchain=com.ca.sm.icas.whiteListChecker.whiteListChecker;  
com.ca.sm.icas.whiteListChecker.ErrorIfLOA1ClaimMissing
```

- LOA2 처리의 경우

```
postprocessingchain=com.ca.sm.icas.whiteListChecker.whiteListChecker;  
com.ca.sm.icas.whiteListChecker.ErrorIfLOA2ClaimMissing
```

- LOA3 처리의 경우

```
postprocessingchain=com.ca.sm.icas.whiteListChecker.whiteListChecker;  
com.ca.sm.icas.whiteListChecker.ErrorIfLOA3ClaimMissing
```

RADIUS CHAP/PAP 인증 체계

다이제스트 인증 체계는 디렉터리에 저장된 암호화된 사용자 특성 문자열을 읽습니다. 그런 다음 이 체계는 사용자로부터 가져오는 암호화된 문자열과 이 문자열을 비교합니다. 암호화된 문자열이 일치하는 경우 정책 서버는 사용자를 인증합니다. 암호화된 문자열의 비교는 암호화된 전송 없이 수행됩니다.

다음과 같은 다이제스트 인증 체계를 사용할 수 있습니다.

- RADIUS CHAP
- RADIUS PAP

PAP 개요

PAP(암호 인증 프로토콜)은 사용자가 양방향 핸드셰이크를 사용하여 인증할 수 있는 간단한 방법을 제공합니다. PAP는 인증 서버에 대한 초기 연결 중에만 이 프로세스를 실행합니다. 사용자의 컴퓨터는 인증이 승인되거나 연결이 종료될 때까지 인증 서버로 ID/암호 쌍을 지속적으로 보냅니다.

원격 호스트에서 로그인을 시뮬레이트하기 위해 일반 텍스트 암호를 사용할 수 있어야 하는 경우에 이 인증 방법을 사용하는 것이 가장 적절합니다. 이러한 경우에 이 방법을 사용하면 원격 호스트에서 일반적인 사용자 로그인과 유사한 보안 수준이 제공됩니다.

CHAP 개요

CHAP(Challenge-Handshake 인증 프로토콜)은 PAP보다 안전한 인증 체계입니다. CHAP 체계에서는 사용자의 아이덴티티를 설정하기 위해 다음과 같은 프로세스가 수행됩니다.

1. 사용자 컴퓨터와 인증 서버 간의 링크가 만들어진 후 서버는 챌린지 메시지를 연결 요청자에게 보냅니다. 요청자는 단방향 해시 함수를 사용하여 가져온 값으로 응답합니다.
2. 서버는 이 값을 서버에서 계산한 예상 해시 값과 비교하여 응답을 확인합니다.
3. 값이 일치하면 인증이 승인되고, 그렇지 않으면 연결이 종료됩니다.

언제든지 서버는 연결된 당사자에 요청하여 새 챌린지 메시지를 보낼 수 있습니다. CHAP 식별자는 자주 변경되고 언제든지 서버가 인증을 요청할 수 있으므로 CHAP는 PAP보다 강화된 보안을 제공합니다.

RADIUS CHAP/PAP 체계 개요

RADIUS CHAP/PAP 체계는 사용자 암호의 다이제스트를 계산하여 사용자를 인증합니다. 그런 다음 정책 서버는 이 다이제스트를 RADIUS 패킷에 있는 CHAP 암호화 비교합니다. 다이제스트는 해시된 암호로 구성되며, 디렉터리 특성을 사용하여 계산됩니다. 이 특성은 RADIUS CHAP/PAP 인증 체계의 구성 중에 지정됩니다.

RADIUS CHAP/PAP 체계 사전 요구 사항

RADIUS CHAP/PAP 인증 체계를 구성하기 전에 다음과 같은 사전 요구 사항을 충족시키십시오.

- 일반 텍스트 암호용으로 지정된 사용자 디렉터리의 필드에는 값이 포함되어 있어야 합니다.
- 정책 서버가 FIPS 전용 모드에서 작동하고 있지 않아야 합니다. 정책 서버가 FIPS 전용 모드에서 작동 중이면 RADIUS CHAP/PAP 인증 체계가 지원되지 않습니다.

RADIUS CHAP/PAP 인증 체계 구성

RADIUS 프로토콜을 사용하는 경우 RADIUS CHAP/PAP 인증 체계를 사용하십시오.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다. 자세한 내용은 "정책 서버 개체 복제"를 참조하십시오.

다음 단계를 수행하십시오.

1. "인프라", "인증"을 차례로 클릭합니다.
2. "인증 체계"를 클릭합니다.

3. "인증 체계 만들기"를 클릭합니다.
"인증 체계 유형의 새 개체 만들기"가 선택되어 있는지 확인합니다.
"확인"을 클릭합니다.
4. 이름 및 보호 수준을 입력합니다.
5. "인증 체계 유형" 목록에서 "RADIUS CHAP/PAP 템플릿"을 선택합니다.
6. "체계 설정" 섹션에서 일반 텍스트 암호를 지정합니다.
7. 제출을 클릭합니다.
인증 체계가 저장되고 영역에 할당할 수 있습니다.

RADIUS 서버 인증 체계

RADIUS 프로토콜을 지원하려면 정책 서버가 RADIUS 서버로 동작하도록 해야 합니다. NAS 클라이언트는 RADIUS 클라이언트로서 동작합니다. RADIUS 에이전트는 정책 서버가 NAS 클라이언트 장치와 통신할 수 있도록 합니다. RADIUS 서버 인증 체계에서 정책 서버는 보호되는 네트워크에 연결됩니다.

이 체계는 자격 증명으로 사용자 이름과 암호를 받아들입니다. 이 체계의 여러 인스턴스를 정의할 수 있습니다. 이 체계는 RADIUS 서버가 인증 응답에서 반환할 수 있는 RADIUS 특성을 해석하지 않습니다.

RADIUS 서버 인증에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

RADIUS 서버 체계 사전 요구 사항

RADIUS 서버 인증 체계를 구성하기 전에 다음 사전 요구 사항을 완료하십시오.

- RADIUS 서버가 정책 서버에서 액세스할 수 있는 네트워크에 있어야 합니다.
- 정책 서버가 FIPS 전용 모드에서 작동하고 있지 않아야 합니다. 정책 서버가 FIPS 전용 모드에서 작동 중이면 RADIUS 서버 인증 체계가 지원되지 않습니다.

RADIUS 서버 인증 체계 구성

정책 서버를 RADIUS 서버로 사용하고 NAS 클라이언트를 RADIUS 클라이언트로 사용하는 경우 RADIUS 서버 인증 체계를 사용하십시오.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다. 자세한 내용은 "정책 서버 개체 복제"를 참조하십시오.

다음 단계를 수행하십시오.

1. "인프라", "인증"을 차례로 클릭합니다.
2. "인증 체계"를 클릭합니다.
3. "인증 체계 만들기"를 클릭합니다.
"인증 체계 유형의 새 개체 만들기"가 선택되어 있는지 확인합니다.
"확인"을 클릭합니다.
4. 이름 및 보호 수준을 입력합니다.
5. "인증 체계 유형" 목록에서 "RADIUS 서버 템플릿"을 선택합니다.
6. "체계 설정"에서 RADIUS 서버 IP 주소, 포트 번호 및 공유 암호를 입력합니다.
7. 제출을 클릭합니다.

인증 체계가 저장됩니다. 이 인증 체계를 영역에 할당할 수 있습니다.

SafeWord 서버 인증 체계

SafeWord 인증 체계는 SafeWord 서버를 사용하여 사용자를 인증합니다. 여기에는 SafeWord 하드웨어 토큰을 통해 로그인하는 사용자도 포함됩니다. 이 체계의 여러 인스턴스를 정의할 수 있습니다. SafeWord 서버의 정확한 구성 매개 변수는 SafeWord 구성 파일에 지정되어 있습니다.

참고: SafeWord 인증 체계인 smauthenigma 및 smauthenigmahtml 은 6.0 SP3 CR03 버전 이후부터 Windows 및 Solaris 플랫폼에서만 지원됩니다.

SafeWord 서버 체계 사전 요구 사항

SafeWord 인증 체계를 구성하기 전에 다음 사전 요구 사항을 완료하십시오.

- SafeWord 서버가 정책 서버에서 액세스할 수 있는 네트워크에 설치되어 있어야 합니다.
- SafeWord 구성 파일에 SafeWord 서버의 정확한 위치가 지정되어 있어야 합니다.

SafeWord 서버 인증 체계 구성

SafeWord 하드웨어 토큰을 통해 로그인하는 사용자를 포함하여 SafeWord 서버에 대해 사용자를 인증해야 할 경우에는 SafeWord 서버 인증 체계를 사용하십시오.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다. 자세한 내용은 "정책 서버 개체 복제"를 참조하십시오.

다음 단계를 수행하십시오.

1. "인프라", "인증"을 차례로 클릭합니다.
2. "인증 체계"를 클릭합니다.
3. "인증 체계 만들기"를 클릭합니다.
"인증 체계 유형의 새 개체 만들기"가 선택되어 있는지 확인합니다.
"확인"을 클릭합니다.
4. 이름 및 보호 수준을 입력합니다.
5. "인증 체계 유형" 목록에서 "SafeWord 템플릿"을 선택합니다.
6. SafeWord 서버 구성 파일의 위치를 입력합니다.
7. 제출을 클릭합니다.

인증 체계가 저장됩니다. 이제 이 인증 체계를 영역에 할당할 수 있습니다.

SafeWord 서버 및 HTML 양식 인증 체계

SafeWord 서버 및 HTML 양식 인증 체계는 사용자 지정 HTML 양식과 함께 SafeWord 서버를 사용하여 사용자를 인증합니다. 이 체계는 또한 SafeWord 하드웨어 토큰을 사용하여 로그인하는 사용자도 처리합니다. 이 체계의 여러 인스턴스를 정의할 수 있습니다. SafeWord 서버의 정확한 구성 매개 변수는 SafeWord 구성 파일에 정의되어 있습니다.

SafeWord 서버 및 HTML 양식 체계 사전 요구 사항

SafeWord 서버 및 HTML 양식 인증 체계를 구성하기 전에 다음 사전 요구 사항을 완료하십시오.

- SafeWord 서버가 정책 서버에서 액세스할 수 있는 네트워크에 설치되어 있어야 합니다.
- SafeWord 구성 파일에 SafeWord 서버의 정확한 위치가 지정되어 있어야 합니다.
- HTML 양식 인증을 구현할 쿠키 도메인의 웹 에이전트 서버에 사용자 지정된 .fcc 파일이 있어야 합니다. CA 는 웹 에이전트가 설치된 Samples/Forms 하위 디렉터리에 샘플 .fcc 파일을 제공합니다.
- 사용자 지정된 .unauth 파일이 웹 에이전트 서버에 있어야 합니다.
참고: .fcc 파일에 smerrorpage 지시문이 사용된 경우에는 .unauth 파일이 필요하지 않습니다.
- 정책 서버와 사용자 디렉터리 간에 디렉터리 연결이 있어야 합니다.
- 기본 HTML 양식 라이브러리가 설치되어 있어야 합니다. HTML 양식 라이브러리는 HTML 양식 인증 프로세스를 처리합니다.
 - SmAuthHTML.dll(Windows 의 경우)
 - smauthhtml.so(Solaris 의 경우)
 이러한 파일은 웹 에이전트를 구성할 때 자동으로 설치됩니다.
- (Sun Java Systems) Sun Java Systems 웹 서버를 사용하는 경우 magnus.conf 파일의 StackSize 매개 변수 값을 131072 보다 큰 값으로 늘려야 합니다. 값을 변경하지 못하면 양식을 사용하여 인증을 요청할 때마다 웹 서버가 코어를 덤프하고 재시작됩니다.

SafeWord 서버 및 HTML 양식 인증 체계 구성

SafeWord 서버 및 사용자 지정 HTML 양식에 대해 사용자를 인증하려면 SafeWord 서버 및 HTML 양식 인증 체계를 사용하십시오. 이 체계는 또한 SafeWord 하드웨어 토큰을 통해 로그인하는 사용자도 처리합니다.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다. 자세한 내용은 "정책 서버 개체 복제"를 참조하십시오.

다음 단계를 수행하십시오.

1. "인프라", "인증"을 차례로 클릭합니다.
2. "인증 체계"를 클릭합니다.
3. "인증 체계 만들기"를 클릭합니다.
"인증 체계 유형의 새 개체 만들기"가 선택되어 있는지 확인합니다.
"확인"을 클릭합니다.
4. 이름 및 보호 수준을 입력합니다.
5. "인증 체계 유형" 목록에서 "SafeWord HTML 양식 템플릿"을 선택합니다.
6. 서버 이름, SafeWord 구성 파일의 위치 및 서버와 대상 정보를 입력합니다.
7. 제출을 클릭합니다.
인증 체계가 저장되고 이를 영역에 할당할 수 있습니다.

SecurID 인증 체계

RSA Ace/SecureID 인증 체계는 사용자 이름, PIN 및 토큰 코드가 포함된 ACE 자격 증명을 사용하여 로그인하는 사용자를 인증합니다. ACE 사용자 이름 및 암호는 ACE/서버 사용자 저장소에 있으며, ACE/서버 관리자는 이 자격 증명을 변경할 수 있습니다. SecureID 토큰은 단일 사용 TOKENCODE 를 생성합니다.

다음과 같은 SecurID 인증 체계를 사용할 수 있습니다.

SecurID 인증

이 체계는 RSA SecureID 하드웨어 토큰을 통해 로그인하는 사용자를 인증합니다. 이 체계는 사용자 이름과 암호를 받아들입니다. 암호는 사용자의 토큰 PIN 과 그 다음에 나오는 동적 코드로 구성됩니다.

참고: Ace 서버에 사용자의 `userid` 를 매핑하려면 LDAP 디렉터리 특성 '`uid`'를 사용하십시오. 그렇지 않으면 SecurID 템플릿 인증 체계가 사용자를 인증하지 못합니다. `uid` 이외의 LDAP 디렉터리 특성을 Ace 서버의 `userid` 에 매핑할 때는 SecurID HTML 양식 템플릿을 사용하십시오.

HTML 양식 지원을 사용한 SecurID 인증

이 체계는 HTML 양식 지원을 포함합니다. 사용자가 PIN 또는 토큰 정보를 잘못 입력하여 비활성화된 경우 해당 사용자는 HTML 양식을 사용하여 자신을 식별하고 계정을 다시 활성화할 수 있습니다.

RSA ACE/SecurID 체계는 자신의 ACE PIN 을 변경하도록 허용되지 않는 사용자 또는 *NextTokenCode* 모드에 있지 않은 사용자를 인증합니다. 하지만 자신의 PIN 을 변경하는 사용자 및 *NextTokenCode* 모드에 있는 사용자는 HTML 양식을 사용한 RSA ACE/SecurID 체계를 통해 인증됩니다. 두 체계 모두 ACE/서버 - Ace/에이전트 모델을 기반으로 하며 RSA/SecurID(토큰) 및 RSA/ACE(서버 소프트웨어) 제품이 필요합니다.

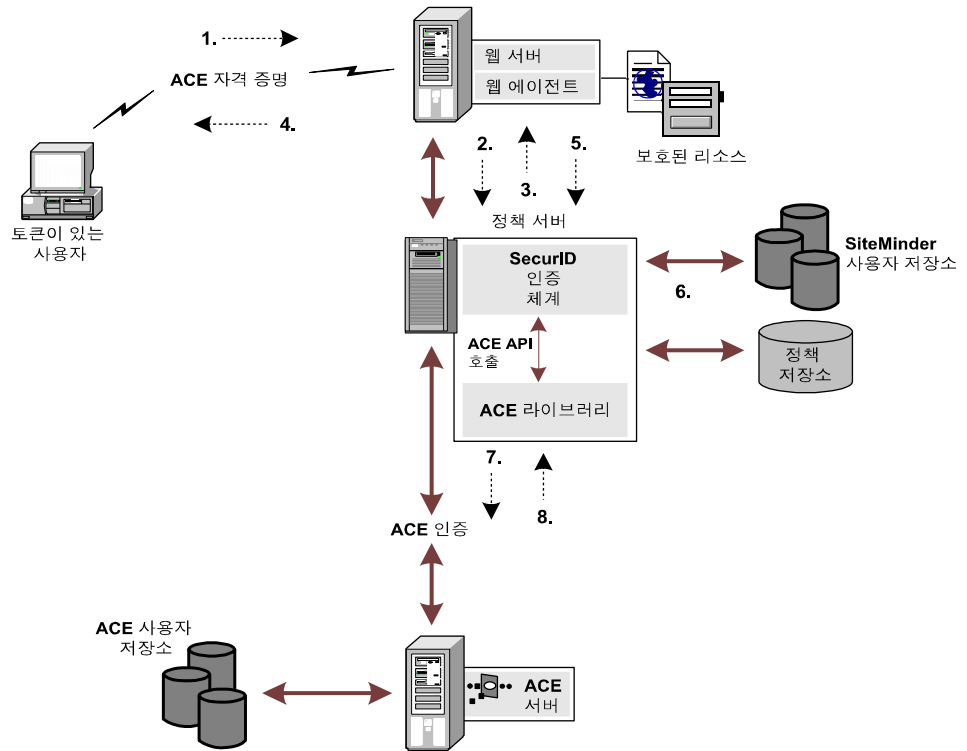
RSA ACE/서버는 RSA SecurID 토큰과 함께 작동하여 유효한 RSA Ace/에이전트를 통해 사용자 아이덴티티를 인증합니다. 또한 RSA 는 웹 에이전트와 사용자 지정 에이전트를 지원합니다. SecurID 인증 체계는 사용자 지정 ACE/에이전트의 역할을 하며 ACE/SDK 및 라이브러리를 사용합니다.

그러나 ACE/서버는 고유한 정책으로 사용자 자격 증명을 처리하고 이 정보를 ACE 사용자 저장소에 저장합니다. 정책에는 각 사용자에 대한 몇 가지 요구 사항과 제한 사항이 포함되며, ACE 관리자가 이를 언제든지 변경할 수 있습니다. 관리자는 사용자를 PIN 또는 토큰 코드를 통해 인증하도록 구성합니다. 사용자가 PIN 을 통해 인증되도록 구성된 경우에는 시스템에 토큰 코드가 필요하지 않습니다. 사용자가 토큰 코드를 통해 인증되도록 구성된 경우에는 토큰 코드와 PIN 이 필요합니다. 또한 사용자가 인증을 시도할 때 새 PIN 을 설정해야 할 수도 있습니다. 이 "새 PIN 모드"에서는 이전 PIN 과 새 PIN 이 필요합니다.

사용자를 인증하기 위해 SecurID 인증 체계는 ACE 서버와 사용자 저장소의 사용자 사이에 매핑이 필요합니다. 이 매핑은 정책 저장소에서 인증 체계 개체 특성으로 표시됩니다.

HTML 양식을 사용한 RSA ACE/SecurID 체계가 개선되어 "새 PIN 모드"에 영향을 줍니다.

다음 그림에서는 RSA ACE/서버가 정책 서버와 상호 작용하는 방식을 보여 줍니다.



이 흐름은 다음과 같습니다.

1. 사용자가 웹 페이지와 같은 리소스를 요청합니다.
2. 웹 에이전트가 리소스 보호 여부를 확인합니다.
3. 정책 서버가 요청된 리소스는 HTML 양식을 사용한 RSA ACE/SecurID 인증 체계로 보호됨을 나타냅니다.
4. 웹 에이전트가 사용자에게 자격 증명을 입력하라는 메시지를 표시합니다.
5. 사용자가 자격 증명을 입력하고 에이전트가 이를 정책 서버로 보냅니다.

6. 정책 서버가 사용자 명확성 처리를 수행하고 사용자 이름을 RSA/ACE 사용자 이름에 매핑합니다. 정책 서버는 암호 정책을 적용하지 않습니다.
7. 정책 서버가 ACE API 호출 시퀀스를 실행하여 인증 요청을 ACE/서버에 전달합니다. 이 서버는 또한 ACE/서버로 사용자의 자격 증명을 전달합니다.
8. ACE/서버가 사용자에게 PIN 을 변경해야 함을 알리고 제어를 다시 정책 서버에 반환합니다.
9. 정책 서버가 제어를 웹 에이전트에 반환하고, 그러면 에이전트는 사용자를 CGI 또는 JSP 로 리디렉션합니다.
10. CGI 또는 JSP 는 해당 HTML 양식을 생성합니다. 양식이 사용자에게 제공되고 사용자에게 사용자 이름, 이전 PIN, 새 PIN 및 새 PIN 확인의 입력이 요청됩니다.
11. 웹 에이전트가 새 자격 증명 집합을 정책 서버에 보냅니다.
12. 정책 서버가 ACE/서버에 대해 새로운 API 호출 시퀀스를 실행합니다.
13. 새 PIN 이 수락된 경우 ACE API 호출이 성공 결과를 반환합니다. 이때 사용자에게 새 PIN 을 사용하여 로그인할지 묻는 메시지가 표시되고 권한 부여 프로세스가 완료됩니다.
14. 새 PIN 이 거부된 경우 10~12 단계가 반복됩니다.

이 PIN 은 다음과 같은 조건에서 거부될 수 있습니다.

- PIN 이 너무 긴 경우
- PIN 이 너무 짧은 경우
- PIN 에 영문자가 포함된 경우

앞의 그림에서 인증은 HTML 양식으로 백엔드 PIN 정책 관련 메시지를 전달하는 것을 포함합니다. SecurID 인증 체계는 ACE/서버로 새 PIN 을 전달하기 전에 PIN 정책의 유효성을 검사합니다. ACE SDK 에는 다음과 같은 PIN 특성을 검색할 수 있는 함수 집합이 있습니다.

- 최대 길이
- 최소 길이
- 영문자와 숫자, 또는 숫자만

이 정보를 기반으로 PIN의 유효성이 검사되고 적절한 오류 메시지가 생성되어 사용자에게 표시됩니다. 유효성 검사는 다음과 같은 순서대로 수행됩니다.

- PIN이 너무 길지 않은지 확인합니다.
- PIN이 너무 짧지 않은지 확인합니다.
- PIN에 잘못된 문자가 없는지 확인합니다.

이러한 새 오류 메시지에서는 정책의 관련 부분만 사용자에게 제공됩니다. 다음 예에서는 이러한 새 메시지가 표시되는 방식을 보여 줍니다.

샘플 사용자인 Joe가 5~8 자리의 PIN을 입력해야 하는데 새 PIN으로 "poem"을 입력한 경우 다음과 같은 오류 메시지가 표시됩니다.

새 PIN이 너무 짧습니다. PIN에는 5개 이상의 문자가 포함되어야 합니다.

다음 지정된 PIN이 "novel"인 경우 다음 메시지가 표시됩니다.

새 PIN에 영문자만 포함해서는 안 됩니다.

다음 지정된 PIN이 "123412341234"인 경우 다음 메시지가 표시됩니다.

새 PIN이 너무 깁니다. PIN에는 8개 이하의 문자만 포함되어야 합니다.

SecureID 인증 체계에 의한 PIN 유효성 검사에 성공한 경우라도 ACE/서버가 새 PIN을 거부할 수 있습니다. 이 경우 사용자에게 새 자격 증명 집합을 요청하는 메시지가 표시되지만 PIN이 거부된 이유는 표시되지 않습니다. 또한 향상된 SecurID 인증 체계에서는 PIN 변경에 성공한 후 대상 웹 페이지에 대한 액세스 권한이 사용자에게 자동으로 부여됩니다.

SecurID 기본 인증 체계를 구성하는 방법

SecurID 인증 체계를 구성하려면 다음 절차를 수행하십시오.

1. [SecurID 체계 사전 요구 사항을 검토합니다](#) (페이지 383).
2. [SecurID 인증 체계를 구성합니다](#) (페이지 383).

SecurID 체계 사전 요구 사항

SecureID 인증 체계를 구성하기 전에 다음 사전 요구 사항을 충족하는지 확인하십시오.

- 다음 조건에 해당하는 경우 ACE 경로가 SecurID 파일의 위치를 가리키도록 구성하십시오.
 - ACE 환경에서 ACE Client 7.0 이상을 실행하는 경우
 - ACE 환경에서 노드 암호를 사용하지 않는 경우
 - ACE 환경에서 정책 서버가 보호하지 않는 다른 응용 프로그램을 보호하는 경우
 - ACE 환경에서 다른 타사 제품을 보호하는 경우

ACE 경로를 구성하면 정책 서버가 ACE 서버로 보내는 인증 요청이 실패하지 않습니다.

참고: SM_ACE_FAILOVER_ATTEMPTS 환경 변수는 제거되었습니다. 이 변수는 ACE 서버에 대한 장애 조치 시도를 설정하는 사용되었습니다.

SecurID 인증 체계 구성

SecurID 인증 체계를 사용하여 ACE 자격 증명으로 로그인하는 사용자를 인증할 수 있습니다.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다. 자세한 내용은 "정책 서버 개체 복제"를 참조하십시오.

다음 단계를 수행하십시오.

1. "인프라", "인증"을 차례로 클릭합니다.
2. "인증 체계"를 클릭합니다.
3. "인증 체계 만들기"를 클릭합니다.
"인증 체계 유형의 새 개체 만들기"가 선택되어 있는지 확인합니다.
"확인"을 클릭합니다.
4. 이름 및 보호 수준을 입력합니다.
5. "인증 체계 유형" 목록에서 "SecurID 템플릿"을 선택합니다.

6. ACE 사용자 ID 특성을 입력합니다.
7. 제출을 클릭합니다.

인증 체계가 저장되고 이를 영역에 할당할 수 있습니다.

SecurID HTML 양식 인증 체계를 구성하는 방법

SecurID HTML 양식 인증 체계를 구성하려면 다음 절차를 수행하십시오.

1. [SecurID HTML 양식 체계 사전 요구 사항을 검토합니다](#) (페이지 384).
2. [SecurID HTML 양식 인증 체계를 구성합니다](#) (페이지 385).

SecurID HTML 양식 체계 사전 요구 사항

SecureID HTML 양식 인증 체계를 구성하기 전에 다음 사전 요구 사항을 완료하십시오.

- Windows 정책 서버의 경우 winnt\system32 디렉터리에 ACE 구성 정보 파일(sdconf.rec)이 있어야 합니다. VAR_ACE 및 USR_ACE 변수가 각각 해당 ACE 에이전트 데이터와 prog 디렉터리를 가리켜야 합니다.
- UNIX 정책 서버의 경우 <policy server installation dir>/bin 디렉터리에 sdconf.rec 파일이 있어야 합니다. 또한 정책 서버가 ACE 에이전트가 아닌 API 라이브러리를 사용할 수 있도록 VAR_ACE 및 USR_ACE 변수가 <policy_server installation_dir>/bin 를 가리켜야 합니다.
- HTML 양식 인증을 구현할 쿠키 도메인의 웹 에이전트 서버에 사용자 지정된 .fcc 파일이 있어야 합니다. CA 는 웹 에이전트가 설치된 Samples/Forms 하위 디렉터리에 샘플 .fcc 파일을 제공합니다.
- 사용자 지정된 .unauth 파일이 웹 에이전트 서버에 있어야 합니다.

참고: .fcc 파일에 smerrorpage 지시문이 사용된 경우에는 .unauth 파일이 필요하지 않습니다.

- 정책 서버와 사용자 디렉터리 간에 디렉터리 연결이 있어야 합니다.
- 기본 HTML 양식 라이브러리가 설치되어 있어야 합니다. 이 라이브러리는 HTML 양식 인증 프로세스를 처리합니다.
 - SmAuthHTML.dll(Windows 의 경우)
 - smauthhtml.so(Solaris 의 경우)

이러한 파일은 웹 에이전트를 구성할 때 자동으로 설치됩니다.

SecurID HTML 양식 인증 체계 구성

SecurID HTML 양식 인증 체계를 사용하면 ACE 자격 증명으로 로그인하는 사용자를 사용자 지정 HTML 양식을 통해 인증할 수 있습니다.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다. 자세한 내용은 "정책 서버 개체 복제"를 참조하십시오.

다음 단계를 수행하십시오.

1. "인프라", "인증"을 차례로 클릭합니다.
2. "인증 체계"를 클릭합니다.
3. "인증 체계 만들기"를 클릭합니다.
"인증 체계 유형의 새 개체 만들기"가 선택되어 있는지 확인합니다.
"확인"을 클릭합니다.
4. 이름 및 보호 수준을 입력합니다.
5. "인증 체계 유형" 목록에서 "SecurID HTML 양식 템플릿"을 선택합니다.
6. 서버, 대상 및 ACE 특성 정보를 입력합니다.
7. 제출을 클릭합니다.

인증 체계가 저장되고 이를 영역에 할당할 수 있습니다.

SecurID 사용자의 재활성화 및 확인을 위한 SecurID HTML 양식 지원

SecurID HTML 양식 체계를 사용하여 영역을 보호하는 경우 잘못된 로그인으로 인해 일시 중지된 사용자는 사용자 지정 가능한 여러 HTML 양식을 사용하여 자신의 계정을 활성화하려고 시도할 수 있습니다. 이러한 양식의 레이아웃과 단어를 수정할 수 있지만 사용자 정보를 수집하는 태그는 수정하면 안 됩니다.

정책 서버에서 제공되는 양식은 다음을 포함합니다.

PWLogin.template

이 양식에서는 사용자가 로그인하기 위해 사용자 이름과 암호를 입력합니다.

PWNextToken.template

이 템플릿은 여러 토큰 코드를 요청하여 사용자가 유효한 SecurID 토큰을 소유하고 있는지 확인합니다.

새 사용자 계정의 활성화를 위한 SecurID HML 양식 지원

정책 서버는 관리자가 새 사용자 계정을 생성할 때와 해당 사용자가 로그인할 때 다음 양식을 사용합니다. 양식을 통해 사용자는 PIN 을 직접 생성하거나 정책 서버가 임의의 PIN 을 생성하도록 합니다.

PWSystemPIN.template

새로운 사용자의 경우나 잘못된 로그인 시도 횟수가 너무 많아 계정이 일시 중단된 사용자의 경우 이 템플릿은 새 PIN 을 획득할지 묻는 메시지를 표시합니다. 이 템플릿은 사용자의 원래 사용자 이름 및 암호를 받아들이지만 보호된 리소스에 대한 액세스 권한을 부여하는 대신 새 PIN 을 받거나 생성할 수 있는 다른 양식으로 사용자를 리디렉션합니다.

PWNewPINSelect.template

이 템플릿을 사용하면 사용자는 시스템에서 자동으로 새 PIN 이 생성되도록 할지 아니면 자신이 직접 새 PIN 을 입력할지를 지정할 수 있습니다.

PWUserPIN.template

이 템플릿을 사용하면 사용자가 새 PIN 을 입력할 수 있습니다. 사용자는 새 PIN 과 함께 올바른 사용자 이름 및 암호를 제공해야 합니다. 이 템플릿에서 \$USRMSG\$는 PIN 번호를 생성하기 위한 명령으로 대체됩니다. 예를 들면 다음과 같습니다.

PIN 은 4~8 자여야 합니다.

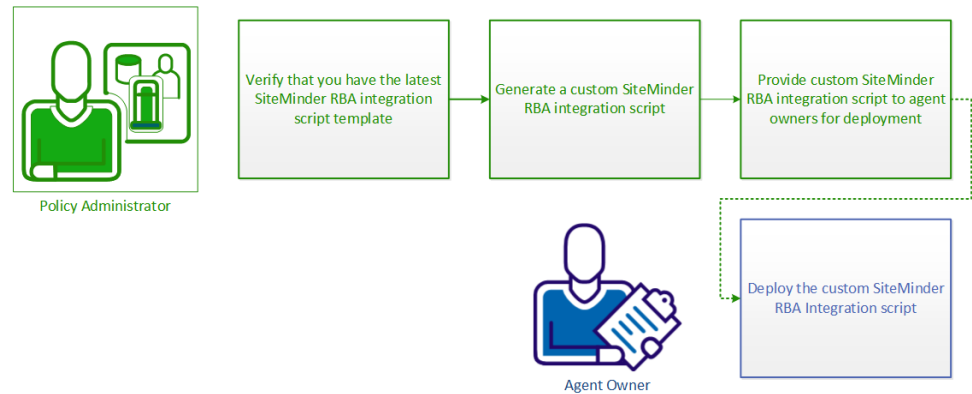
PWPINAccept.template

이 템플릿은 시스템 생성 PIN 이 새로 생성되었음을 나타냅니다. 이 템플릿에서 시스템에서 생성된 PIN 은 \$USRMSG\$ 변수를 대체합니다. 사용자가 "계속"을 클릭하는 즉시 새 PIN 을 사용하여 로그인할지 묻는 메시지가 표시됩니다.

리스크 기반 인증을 위해 SecurID HTML 양식 인증 지원을 구성하는 방법

SecurID 용 RSA 리스크 기반 인증(RBA)은 사용자 이름/암호 로그인 방식을 변경하지 않고 사용자 아이덴티티에 대한 리스크 기반 확인 기능을 제공합니다.

리스크 기반 인증(RBA)을 위해 SecurID HTML 양식 인증 지원을 구성하려면 정책 관리자와 에이전트 소유자가 협력해야 합니다. 이 시나리오는 이 둘이 모두 수행해야 하는 모든 절차를 설명합니다.



정책 관리자는 다음 절차를 수행합니다.

1. [최신 SiteMinder RBA 통합 스크립트 템플릿이 있는지 확인합니다](#) (페이지 388).
2. [사용자 지정 SiteMinder RBA 통합 스크립트를 생성합니다](#) (페이지 388).
3. [사용자 지정 SiteMinder RBA 통합 스크립트를 배포를 위해 에이전트 소유자에게 제공합니다](#) (페이지 388).

에이전트 소유자는 다음 절차를 수행합니다.

1. [각 웹 서버에 사용자 지정 SiteMinder RBA 통합 스크립트를 배포합니다](#) (페이지 389).

최신 SiteMinder RBA 통합 스크립트 템플릿이 있는지 확인

RBA 통합 스크립트는 RSA 인증 관리자와 함께 제공되는 템플릿에 기반합니다. 하지만 RSA 가 릴리스 사이에서 템플릿을 업데이트할 수 있으므로 가장 최신 템플릿을 사용해야 합니다.

다음 단계를 수행하십시오.

1. 이 링크 <https://sftp.rsa.com/human.aspx?Username=partner&password=rsasecured&arg01=859293799&arg12=downloaddirect&transaction=signon&quiet=true>를 사용하여 SiteMinder RBA 통합 스크립트 템플릿을 다운로드합니다.
2. RSA 인증 관리자 서버와 함께 제공되는 통합 스크립트 템플릿을 찾습니다.
3. 서버에 통합 템플릿이 없으면 1 단계에서 다운로드한 템플릿을 설치합니다. 그렇지 않은 경우, 템플릿의 헤더를 비교하여 더 최신 템플릿을 설치하십시오.

사용자 지정 SiteMinder RBA 통합 스크립트 생성

에이전트에 배포하기 위해 사용자 지정 RBA 통합 스크립트를 생성하려면 RSA 보안 콘솔을 사용하십시오.

다음 단계를 수행하십시오.

1. RSA 보안 콘솔에 로그인한 후 하나 이상의 에이전트에 대해 RBA 를 활성화합니다.
2. 에이전트가 사용자(RSA SecurID 또는 고정 암호 코드)를 인증하는 데 사용할 기본 방법을 선택합니다.
3. 스크립트를 생성하고 임시 디렉터리로 다운로드하려면 CA SiteMinder 템플릿을 사용합니다.

사용자 지정 SiteMinder RBA 통합 스크립트를 배포를 위해 에이전트 소유자에게 제공

RSA 보안 콘솔에서 생성한 사용자 지정 RBA 통합 스크립트는 RBA 를 지원해야 하는 각 웹 서버에 배포되어야 합니다.

사용자 지정 RBA 통합 스크립트를 각 에이전트 소유자에게 제공하고 [배포 방법](#) (페이지 389)을 알려 주십시오.

에이전트 소유자가 각 웹 서버에서 사용자 지정 SiteMinder RBA 통합 스크립트 배포

RBA 를 지원해야 하는 각 웹 서버에 정책 관리자가 제공한 사용자 지정 SiteMinder RBA 통합 스크립트를 배포하십시오.

다음 단계를 수행하십시오.

1. 에이전트 호스트에 로그인하고 기본 RSA SecurID 로그인 템플릿(smpwsservices.fcc)을 찾습니다. 이 템플릿은 에이전트 루트를 기준으로 상대 경로인 /siteminderagent/forms/ 디렉터리에 있습니다.
2. 텍스트 편집기에서 smpwsservices.fcc 를 연 다음 맨 아래에 있는 </body> 태그 바로 앞에 다음 두 줄을 추가한 후 파일을 저장합니다.

```
<script src="am_integration.js" type="text/javascript"></script>
<script>window.onload=redirectToIdP;</script>
```

중요! 필요한 경우 편집을 취소하고 편집하기 이전 상태로 돌아갈 수 있도록 편집 전에 smpwsservice.fcc 를 백업하십시오.

3. 사용자 지정 SiteMinder RBA 통합 스크립트(am_integration.js)를 /siteminderagent/forms/ 디렉터리로 복사하고 웹 서버를 다시 시작합니다.

X.509 클라이언트 인증서 인증 체계

X.509 V3 클라이언트 인증서를 구성할 수 있습니다. 클라이언트에 인증서가 설치되어 있으면 이 인증서를 사용하여 리소스를 요청하는 사용자의 아이덴티티를 확인할 수 있습니다. 인증서 인증에는 SSL 통신이 사용되며 인증서 인증과 기본 인증을 함께 사용하면 보다 높은 수준의 액세스 보안이 가능합니다.

참고: 인증서 전용 인증 체계의 경우 인증 및 권한 부여 시도에 실패하면 웹 에이전트가 HTTP 오류 403(액세스 거부됨/사용 권한 없음)을 반환합니다. 웹 에이전트에서는 사용자에게 새 인증서를 요청할 수 없기 때문입니다.

X.509 클라이언트 인증서 인증 체계는 인증서 인증을 구현합니다. X.509 클라이언트 인증서 인증을 사용하려면 사용 환경에서 SSL 통신을 처리할 수 있어야 합니다. 즉, 클라이언트 브라우저, 웹 서버 및 사용자 인증서가 인증서 인증을 수락하고 이를 수행하도록 구성되어 있어야 합니다. 이러한 태스크는 정책 서버 구성 범위를 벗어납니다.

필요한 SSL 구성 요소가 올바르게 설정된 후 X.509 인증 체계를 구성하십시오. 구성 태스크는 다음을 포함합니다.

- 웹 에이전트 구성 마법사를 실행할 때 고급 SSL 인증 체계를 선택합니다.
웹 에이전트 구성 마법사에 대한 자세한 내용은 [웹 에이전트 설치 안내서](#)를 참조하십시오.
- 관리 UI 를 사용하여 이 안내서에 설명된 X.509 인증 체계 중 하나를 구성합니다.

X.509 클라이언트 인증서 인증 체계는 다음 태스크를 수행합니다.

- 클라이언트 인증서 정보를 수집합니다.
- 사용자 인증서의 정보를 기반으로 디렉터리의 사용자를 식별합니다. 이 프로세스를 *인증서 매핑*이라고 합니다.
- 필요한 경우 CRL(인증서 해지 목록) 또는 OCSP(온라인 인증서 상태 프로토콜)를 사용하여 인증서가 유효한지 여부를 확인합니다.

추가 정보:

[X.509 클라이언트 인증서 인증 체계에 대한 인증서 매핑](#) (페이지 439)

인증서 인증을 위한 인증서 추출

사용자가 보호된 리소스를 요청할 경우 웹 에이전트는 먼저 정책 서버에 연결하여 해당 리소스를 보호하는 데 사용되고 있는 인증 체계를 확인합니다. X.509 인증 체계로 리소스를 보호하고 있는 경우 웹 에이전트는 구성된 인증 체계에 해당하는 자격 증명 수집기로 사용자의 브라우저를 리디렉션합니다. 자격 증명 수집기의 경로는 인증 체계 구성에 정의되어 있습니다.

자격 증명 수집기에 대한 연결은 SSL 보안 연결이며 웹 서버는 클라이언트 인증서를 요청하도록 구성되어 있습니다. 따라서 인증을 위해서는 브라우저가 클라이언트 인증서를 제출해야 합니다. 자격 증명 수집기 URL 의 끝에 있는 리소스 이름 및 확장명은 웹 에이전트가 웹 서버에서 사용자 인증서를 추출하도록 지시합니다. 그러면 웹 에이전트는 인증 체계에서 사용할 수 있도록 인증서를 정책 서버에 전달합니다.

SiteMinder 가 인증서 데이터를 사용하여 사용자를 식별하는 방식

웹 에이전트는 인증서 정보를 수집한 후 확인을 위해 이 데이터를 정책 서버에 전달합니다. 그러면 정책 서버는 인증서 매핑을 수행합니다. 인증서 매핑의 목적은 사용자 인증서의 주체 이름으로 사용자를 찾는 데 있습니다.

먼저 정책 서버는 정책 저장소에서 적절한 인증서 매핑을 조회합니다. 정책 서버는 인증서 발급자 DN 을 사용하여 이 매핑을 찾습니다. 발급자 DN 은 인증서 매핑 구성의 일부입니다. 정책 서버는 매핑을 찾은 후 인증서의 주체 이름을 가져오고 매핑을 적용하여 사용자 디렉터리에서 사용자 항목을 찾습니다.

정책 서버는 다음 저장소에 저장된 사용자 인증서에만 액세스할 수 있습니다.

- LDAP/AD 사용자 디렉터리
- ODBC 저장소

중요! 모든 X.509 클라이언트 인증서 인증 체계에 대해 인증서 매핑을 구성해야 합니다.

추가 정보:

[X.509 클라이언트 인증서 인증 체계에 대한 인증서 매핑 \(페이지 439\)](#)

X.509 클라이언트 인증 체계 사전 요구 사항

X.509 클라이언트 인증서 인증 체계를 구성하기 전에 다음 사전 요구 사항을 충족하십시오.

- SSL 웹 서버에 X.509 서버 인증서를 설치합니다. 인증서가 만료되지 않았는지 확인합니다.

참고: 정책 서버가 FIPS 모드에서 실행되는 경우 FIPS 승인 알고리즘만 사용하여 인증서가 생성되었는지 확인하십시오.

- 네트워크가 클라이언트 브라우저에 대한 SSL 연결(HTTPS 프로토콜)을 지원하는지 확인합니다.
- 클라이언트 브라우저용 X.509 클라이언트 인증서가 설치되어 있는지 확인합니다. 인증서가 만료되지 않았는지 확인합니다.

X.509 인증서 인증 체계 구성

SSL 환경 설정 외에, 다음 프로세스를 완료하여 인증서 인증을 구성합니다.

1. SSL 통신을 처리하도록 사용자 환경을 설정합니다. 클라이언트 브라우저, 웹 서버 및 모든 사용자 인증서가 인증서 인증을 허용하고 수행하도록 구성합니다.
2. 설치된 웹 에이전트가 SSL 인증을 처리할 수 있는지 확인합니다.
3. 관리 UI 에서 X.509 인증 체계를 구성합니다.
4. 클라이언트 인증서의 정보를 기반으로 하는 사용자를 식별하기 위한 인증서 매핑을 정의합니다.
5. (선택 사항) CRL 또는 OCSP 를 사용하여 인증서 유효성 검사를 구성합니다.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다. 자세한 내용은 "정책 서버 개체 복제"를 참조하십시오.

다음 단계를 수행하십시오.

1. "인프라", "인증"을 차례로 클릭합니다.
2. "인증 체계"를 클릭합니다.
3. "인증 체계 만들기"를 클릭합니다.
"인증 체계 유형의 새 개체 만들기"가 선택되어 있는지 확인합니다.
"확인"을 클릭합니다.
4. 이름 및 보호 수준을 입력합니다.
5. "인증 체계 유형" 목록에서 "X.509 클라이언트 인증서 템플릿"을 선택합니다.
6. SSL 자격 증명 수집기에 대한 서버 이름 및 대상 정보를 입력합니다.
7. (선택 사항) "체계 설정"에서 "인증 세션 변수 유지"를 선택합니다. 이 옵션은 인증 컨텍스트 데이터를 나중에 인증 결정에 사용할 수 있도록 세션 저장소에 저장하도록 지정합니다.
8. 제출을 클릭합니다.

인증 체계가 저장되고 이를 영역에 할당할 수 있습니다.

X.509 인증서 인증 체계가 관리 UI 에 구성되었습니다. 이제 [인증서 매핑 \(페이지 439\)](#)을 설정합니다.

X.509 클라이언트 인증서 및 기본 인증 체계

X.509 클라이언트 인증서 및 기본 인증 체계는 기본 인증과 X.509 클라이언트 인증서 인증을 결합한 것입니다. 이 인증 체계는 중요한 리소스에 대한 보안 수준을 강화해 줍니다.

사용자가 성공적으로 인증하려면 다음 두 이벤트가 발생해야 합니다.

- 사용자의 X.509 클라이언트 인증서가 확인되어야 합니다.
그리고
- 사용자가 올바른 사용자 이름 및 암호를 제공해야 합니다.

X.509 클라이언트 인증서 인증의 경우 정책 서버가 웹 에이전트에 사용자를 SSL 서버로 리디렉션하고 사용자의 인증서를 서버에 매핑하도록 지시합니다. 그런 다음 정책 서버는 사용자가 존재하는지 확인하고, 사용자의 기본 자격 증명을 확인하고, 인증서 자격 증명과 기존 자격 증명에 동일한 사용자를 나타내는지 확인합니다.

X.509 클라이언트 인증서 및 기본 체계 사전 요구 사항

X.509 클라이언트 인증서 및 기본 인증 체계를 구성하기 전에 다음 사전 요구 사항을 충족하는지 확인하십시오.

- SSL 웹 서버에 X.509 서버 인증서가 설치되어 있어야 합니다.
참고: 정책 서버가 FIPS 모드에서 실행되는 경우 FIPS 승인 알고리즘만 사용하여 인증서가 생성되었는지 확인하십시오.
- 네트워크가 클라이언트 브라우저에 대한 SSL 연결(HTTPS 프로토콜)을 지원해야 합니다.
- 클라이언트 브라우저에 X.509 클라이언트 인증서가 설치되어 있어야 합니다.
- 클라이언트 인증서와 서버 인증서 간에 트러스트가 설정되어 있어야 합니다.
- 인증서가 트러스트된 유효한 CA(인증 기관)에서 발급된 것이어야 합니다.
- 인증서 발급 CA 공개 키를 통해 발급자의 디지털 서명에 대한 유효성이 검사되어야 합니다.
- 클라이언트 인증서와 서버 인증서가 만료되지 않아야 합니다.

- 사용자의 공개 키를 통해 사용자 디지털 서명에 대한 유효성이 검사되어야 합니다.
- 클라이언트 사용자 이름 및 암호 정보가 사용자 디렉터리에 있어야 합니다.
- 정책 서버와 사용자 디렉터리 간에 디렉터리 연결이 있어야 합니다.

참고: 인증서가 필수이거나 선택 사항인 Apache 웹 서버의 경우에는 httpd.conf 파일에서 SSL Verify Depth 10 줄의 주석 처리를 제거해야 합니다.

추가 정보:

[사용자 디렉터리](#) (페이지 147)

X.509 인증서 및 기본 인증 체계 구성

인증서 인증과 기본 인증을 결합하려면 X.509 인증서 및 기본 인증 체계를 사용하십시오.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다. 자세한 내용은 "정책 서버 개체 복제"를 참조하십시오.

다음 단계를 수행하십시오.

1. "인프라", "인증"을 차례로 클릭합니다.
2. "인증 체계"를 클릭합니다.
3. "인증 체계 만들기"를 클릭합니다.
"인증 체계 유형의 새 개체 만들기"가 선택되어 있는지 확인합니다.
"확인"을 클릭합니다.
4. 이름 및 보호 수준을 입력합니다.
5. "인증 체계 유형" 목록에서 "X.509 클라이언트 인증서 및 기본 템플릿"을 선택합니다.

6. SSL 자격 증명 수집기에 대한 서버 이름 및 대상 정보를 입력합니다.
 7. (선택 사항) "체계 설정"에서 "인증 세션 변수 유지"를 선택합니다. 이 옵션은 인증 컨텍스트 데이터가 세션 저장소에 저장되도록 지정합니다.
 8. 제출을 클릭합니다.
- 인증 체계가 저장되고 이를 영역에 할당할 수 있습니다.

X.509 인증서 또는 기본 인증 체계

X.509 클라이언트 인증서 또는 기본 인증 체계에서는 기본 인증이나 X.509 클라이언트 인증서 인증을 통해 사용자 아이덴티티를 설정할 수 있습니다. 사용자가 성공적으로 인증하려면 다음 두 이벤트 중 하나가 발생해야 합니다.

- 사용자 X.509 클라이언트 인증서가 확인되어야 합니다.
- OR
- 사용자가 올바른 사용자 이름 및 암호를 제공해야 합니다.

이 체계를 사용할 경우 사용자가 보호된 리소스를 요청하면 웹 에이전트는 브라우저에 인증서를 제공하도록 요청합니다. 사용자가 인증서를 갖고 있지 않거나 "취소"를 클릭하여 인증서를 제공하지 않을 경우 웹 에이전트는 HTTP 기본 프로토콜을 사용하여 사용자에게 인증을 요청합니다. HTTP 기본 인증에서는 에이전트가 사용자 이름 및 암호를 가져올 수 있습니다.

이 체계는 X.509 인증서를 단계적으로 배포해야 하는 경우에 유용합니다. 예를 들어 사용자가 50,000 명인 회사의 경우 인증서 50,000 개를 동시에 발급하고 배포하는 작업이 번거로울 수 있습니다. 이 체계를 사용하면 인증서를 한 번에 500 개 또는 5,000 개씩 적절히 나누어 발급할 수 있습니다. 이 전환 기간 동안 이미 인증서가 있는 사용자에게 대해서는 인증서를 통해 리소스를 보호할 수 있으며, 동시에 권한 있는 다른 사용자는 디렉터리 사용자 이름 및 암호를 기반으로 리소스에 액세스할 수 있습니다.

이 체계에서는 SSL 연결을 요구하도록 기본 인증 교환을 구성하는 옵션이 제공됩니다.

참고: X.509 인증서 또는 기본 체계가 혼합된 인증서 기반 인증 체계를 여러 개 구현할 경우 브라우저 캐싱 제한으로 인해 예기치 못한 동작이 발생할 수 있습니다. 사용자가 인증서 또는 기본 인증 체계로 보호되는 영역의 리소스에 액세스하기 위해 인증서 기반 인증을 선택하지 않을 경우 브라우저는 이 결정을 자동으로 캐시합니다. 이후에 동일한 사용자가 같은 브라우저 세션에서 필수 인증서 부분(예: X.509 인증서, X.509 인증서 및 기본, X.509 인증서 및 양식)을 포함하는 인증 체계로 보호되는 리소스에 액세스하려고 하면 "사용 권한 없음" 오류 메시지가 표시됩니다.

사용자가 첫 번째 리소스에 액세스할 때 인증서 기반 인증에 필요한 인증서를 보내지 않았고 브라우저는 해당 결정을 캐시했기 때문에 사용자가 인증서가 필요한 영역에 액세스하려고 하면 자동으로 거부됩니다.

X.509 인증서 또는 기본 체계를 포함하는 인증서 기반 인증 체계로 보호되는 영역과 사용자가 인증을 위해 인증서를 보낼지 여부를 선택할 수 없는 기타 인증서 기반 체계로 보호되는 영역이 혼합된 배포 환경에서 유효한 인증서가 있는 사용자가 리소스에 액세스할 때는 인증서를 사용하도록 권장하십시오.

X.509 클라이언트 인증서 또는 기본 체계 사전 요구 사항

X.509 클라이언트 인증서 또는 기본 인증 체계를 구성하기 전에 다음 사전 요구 사항을 충족하는지 확인하십시오.

- SSL 웹 서버에 X.509 서버 인증서가 설치되어 있어야 합니다.
참고: 정책 서버가 FIPS 모드에서 실행되는 경우 FIPS 승인 알고리즘만 사용하여 인증서가 생성되었는지 확인하십시오.
- 네트워크가 클라이언트 브라우저에 대한 SSL 연결(HTTPS 프로토콜)을 지원해야 합니다.
- 클라이언트 브라우저에 X.509 클라이언트 인증서가 설치되어 있어야 합니다.
- 클라이언트 인증서와 서버 인증서 간에 트러스트가 설정되어 있어야 합니다.
- 인증서가 트러스트된 유효한 CA(인증 기관)에서 발급된 것이어야 합니다.
- 인증서 발급 CA의 공개 키를 통해 발급자의 디지털 서명에 대한 유효성이 검사되어야 합니다.

- 클라이언트 인증서와 서버 인증서가 만료되지 않아야 합니다.
- 사용자의 공개 키를 통해 사용자 디지털 서명에 대한 유효성이 검사되어야 합니다.
- 클라이언트 사용자 이름 및 암호 정보가 사용자 디렉터리에 있어야 합니다.
- 정책 서버와 사용자 디렉터리 간에 디렉터리 연결이 있어야 합니다.

참고: 인증서가 필수이거나 선택 사항인 Apache 웹 서버의 경우에는 httpd.conf 파일에서 SSL Verify Depth 10 줄의 주석 처리를 제거해야 합니다.

추가 정보:

[사용자 디렉터리](#) (페이지 147)

X.509 인증서 또는 기본 인증 체계 구성

X.509 인증서 또는 기본 인증 체계를 사용하여 인증서 인증이나 기본 인증 또는 둘 모두를 구현할 수 있습니다.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다. 자세한 내용은 "정책 서버 개체 복제"를 참조하십시오.

다음 단계를 수행하십시오.

1. "인프라", "인증"을 차례로 클릭합니다.
2. "인증 체계"를 클릭합니다.
3. "인증 체계 만들기"를 클릭합니다.
"인증 체계 유형의 새 개체 만들기"가 선택되어 있는지 확인합니다.
"확인"을 클릭합니다.
4. 이름 및 보호 수준을 입력합니다.
5. "인증 체계 유형" 목록에서 "X.509 클라이언트 인증서 또는 기본 템플릿"을 선택합니다.

6. SSL 자격 증명 수집기에 대한 서버 및 대상 정보를 입력합니다.
 7. (선택 사항) "체계 설정"에서 "인증 세션 변수 유지"를 선택합니다. 이 옵션은 인증 컨텍스트 데이터가 세션 저장소에 저장되도록 지정합니다.
 8. 제출을 클릭합니다.
- 인증 체계가 저장되고 이를 영역에 할당할 수 있습니다.

X.509 클라이언트 인증서 및 HTML 양식 인증 체계

X.509 클라이언트 인증서 및 HTML 양식 인증 체계는 HTML 양식 인증과 X.509 클라이언트 인증서 인증을 결합한 것입니다. 이 인증 체계는 중요한 리소스에 대한 보안 수준을 강화해 줍니다.

사용자가 성공적으로 인증하려면 다음 두 이벤트가 발생해야 합니다.

- 사용자의 X.509 클라이언트 인증서가 확인되어야 합니다.
그리고
- 사용자가 HTML 양식에 의해 요청된 자격 증명을 제공해야 합니다.

이 체계의 경우 인증 프로세스는 다음 단계를 따릅니다.

1. 정책 서버가 웹 에이전트에 사용자를 SSL 사용 웹 서버의 FCC로 리디렉션하도록 지시합니다.
2. 웹 에이전트가 양식을 제공합니다.
3. FCC가 인증서와 양식을 다시 정책 서버에 전달합니다.
4. 정책 서버가 인증서 매핑에 있는 사용자의 존재 여부를 확인합니다.
5. 정책 서버가 사용자의 HTML 양식 자격 증명을 확인하고 인증서 자격 증명과 HTML 양식 자격 증명이 동일한 사용자를 나타내는지 확인합니다.

X.509 클라이언트 인증서 및 HTML 양식 체계 사전 요구 사항

X.509 클라이언트 인증서 및 HTML 양식 인증 체계를 구성하기 전에 다음 사전 요구 사항을 충족하는지 확인하십시오.

- SSL 웹 서버에 X.509 서버 인증서가 설치되어 있어야 합니다.
참고: 정책 서버가 FIPS 모드에서 실행되는 경우 FIPS 승인 알고리즘만 사용하여 인증서가 생성되었는지 확인하십시오.
- 네트워크가 클라이언트 브라우저에 대한 SSL 연결(HTTPS 프로토콜)을 지원해야 합니다.
- 클라이언트 브라우저에 X.509 클라이언트 인증서가 설치되어 있어야 합니다.
- 클라이언트 인증서와 서버 인증서 간에 트러스트가 설정되어 있어야 합니다.
- 인증서가 트러스트된 유효한 CA(인증 기관)에서 발급된 것이어야 합니다.
- 인증서 발급 CA의 공개 키를 통해 발급자의 디지털 서명에 대한 유효성이 검사되어야 합니다.
- 클라이언트 인증서와 서버 인증서가 만료되지 않아야 합니다.
- 사용자의 공개 키를 통해 사용자 디지털 서명에 대한 유효성이 검사되어야 합니다.
- 양식 자격 증명 정보가 사용자 디렉터리에 있어야 합니다.
- 정책 서버와 사용자 디렉터리 간에 디렉터리 연결이 있어야 합니다.
- (Sun Java Systems) Sun Java Systems 웹 서버를 사용하는 경우 magnus.conf 파일의 StackSize 매개 변수 값을 131072 보다 큰 값으로 늘려야 합니다. 값을 변경하지 못하면 정책 서버가 양식을 사용하여 인증을 요청할 때마다 웹 서버가 코어를 덤프하고 재시작됩니다.

참고: 인증서가 필수이거나 선택 사항인 Apache 웹 서버의 경우에는 httpd.conf 파일에서 SSL Verify Depth 10 줄의 주석 처리를 제거해야 합니다.

인증서와 양식 데이터는 함께 수집되어 정책 서버에 전달됩니다.

조건	결과
인증서가 없는 경우	브라우저가 오류 500 표시

조건	결과
인증서 및 양식 자격 증명이 수락되지 않은 경우	브라우저가 오류 500 표시

추가 정보:

[사용자 디렉터리](#) (페이지 147)

에이전트 API 지원

X.509 클라이언트 인증서 및 HTML 양식 인증 체계에는 Sm_Api_Cred_SSLRequired 및 Sm_Api_Cred_FormRequired 비트가 사용됩니다.

X.509 인증서 및 HTML 양식 인증 체계 구성

인증서 인증과 HTML 양식 기반 인증을 결합하려면 X.509 인증서 및 HTML 인증 체계를 사용하십시오.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다. 자세한 내용은 "정책 서버 개체 복제"를 참조하십시오.

다음 단계를 수행하십시오.

1. "인프라", "인증"을 차례로 클릭합니다.
2. "인증 체계"를 클릭합니다.
3. "인증 체계 만들기"를 클릭합니다.
"인증 체계 유형의 새 개체 만들기"가 선택되어 있는지 확인합니다.
"확인"을 클릭합니다.
4. 이름 및 보호 수준을 입력합니다.
5. "인증 체계 유형" 목록에서 "X.509 클라이언트 인증서 및 양식 템플릿"을 선택합니다.

6. SSL 자격 증명 수집기에 대한 서버 이름 및 대상 정보를 입력합니다.
 7. (선택 사항) "체계 설정"에서 "인증 세션 변수 유지"를 선택합니다. 이 옵션은 인증 컨텍스트 데이터가 세션 저장소에 저장되도록 지정합니다.
 8. 제출을 클릭합니다.
- 인증 체계가 저장되고 이를 영역에 할당할 수 있습니다.

X.509 클라이언트 인증서 또는 HTML 양식 인증 체계

X.509 클라이언트 인증서 또는 HTML 양식 인증 체계에서는 HTML 양식 인증이나 X.509 클라이언트 인증서 인증을 통해 사용자 아이덴티티를 설정할 수 있습니다. 사용자가 성공적으로 인증하려면 다음 두 이벤트 중 하나가 발생해야 합니다.

- X.509 클라이언트 인증서가 확인되어야 합니다.
- OR
- 사용자가 HTML 양식에 요청된 자격 증명을 제공해야 합니다.

사용자가 보호된 리소스를 요청하면 웹 에이전트는 브라우저에 인증서를 제공하도록 요청합니다. 이 체계는 다음과 같은 영향을 줍니다.

조건	결과
인증서가 제공됨	인증서가 처리됨
인증서가 수락되지 않음	브라우저가 오류 500 표시
인증서가 제공되지 않음	브라우저가 양식 제공
양식이 거부됨	브라우저가 양식을 다시 요청

이 체계는 X.509 인증서를 단계적으로 배포해야 하는 경우에 유용합니다. 예를 들어 사용자가 50,000 명인 회사의 경우 인증서 50,000 개를 동시에 발급하고 배포하는 작업이 번거로울 수 있습니다. 이 체계를 사용하면 인증서를 한 번에 500 개 또는 5,000 개씩 적절히 나누어 발급할 수 있습니다. 이 전환 기간 동안 이미 인증서가 있는 사용자에게 대해서는 인증서를 통해 리소스를 보호할 수 있으며, 동시에 권한 있는 다른 사용자는 HTML 양식 자격 증명을 기반으로 리소스에 액세스할 수 있습니다.

참고: X.509 인증서 또는 양식 체계가 혼합된 인증서 기반 인증 체계를 여러 개 구현할 경우 브라우저 캐싱 제한으로 인해 예기치 못한 동작이 발생할 수 있습니다. 사용자가 인증서 또는 양식 인증 체계로 보호되는 영역의 리소스에 액세스하기 위해 인증서 기반 인증을 사용하지 않을 경우 브라우저는 이 결정을 자동으로 캐시합니다. 이후에 동일한 사용자가 같은 브라우저 세션에서 필수 인증서 부분(예: X.509 인증서, X.509 인증서 및 기본, X.509 인증서 및 양식)을 포함하는 인증 체계로 보호되는 리소스에 액세스하려고 하면 "사용 권한 없음" 오류 메시지가 표시됩니다.

사용자가 첫 번째 리소스에 액세스할 때 인증서 기반 인증에 필요한 인증서를 보내지 않았고 브라우저는 해당 결정을 캐시했기 때문에 사용자가 인증서가 필요한 영역에 액세스하려고 하면 자동으로 거부됩니다.

X.509 인증서 또는 양식 체계를 포함하는 인증서 기반 인증 체계로 보호되는 영역과 사용자가 인증을 위해 인증서를 보낼지 여부를 선택할 수 없는 기타 인증서 기반 체계로 보호되는 영역이 혼합된 배포 환경에서 유효한 인증서가 있는 사용자가 리소스에 액세스할 때는 인증서를 사용하도록 권장하십시오.

X.509 클라이언트 인증서 또는 HTML 양식 체계 사전 요구 사항

X.509 클라이언트 인증서 또는 HTML 양식 인증 체계를 구성하기 전에 다음 사전 요구 사항을 충족하는지 확인하십시오.

- SSL 웹 서버에 X.509 서버 인증서가 설치되어 있어야 합니다.
참고: 정책 서버가 FIPS 모드에서 실행되는 경우 FIPS 승인 알고리즘만 사용하여 인증서가 생성되었는지 확인하십시오.
- 네트워크가 클라이언트 브라우저에 대한 SSL 연결(HTTPS 프로토콜)을 지원해야 합니다.
- 클라이언트 브라우저에 X.509 클라이언트 인증서가 설치되어 있어야 합니다.
- 클라이언트 인증서와 서버 인증서 간에 트러스트가 설정되어 있어야 합니다.
- 인증서가 트러스트된 유효한 CA(인증 기관)에서 발급된 것이어야 합니다.
- 인증서 발급 CA의 공개 키를 통해 발급자의 디지털 서명에 대한 유효성이 검사되어야 합니다.

- 클라이언트 인증서와 서버 인증서가 만료되지 않아야 합니다.
- 사용자의 공개 키를 통해 사용자 디지털 서명에 대한 유효성이 검사되어야 합니다.
- HTML 양식에서 요청된 사용자 특성이 사용자 디렉터리에 있어야 합니다.
- 정책 서버와 사용자 디렉터리 간에 디렉터리 연결이 있어야 합니다.
- (Sun Java Systems) Sun Java Systems 웹 서버를 사용하는 경우 magnus.conf 파일의 StackSize 매개 변수 값을 131072 보다 큰 값으로 늘려야 합니다. 값을 변경하지 못하면 정책 서버가 양식을 사용하여 인증을 요청할 때마다 웹 서버가 코어를 덤프하고 재시작됩니다.

추가 정보:

[사용자 디렉터리](#) (페이지 147)

에이전트 API 지원

에이전트 API에서는 Sm_AuthApi_Cred_CertOrForm 값이 열거 형식 Sm_Api_Credentials_t에 추가되어 있습니다. Sm_Api_Credentials_t는 사용자가 Sm_AgentApi_Realm_t 구조체에서 참조되는 영역에 액세스하는데 필요한 자격 증명을 지정합니다. 이 열거 형식은 이 구조체의 nRealmCredentials 필드에 적용됩니다.

새 값은 사용자 인증에 반드시 X.509 인증서 또는 양식 기반 인증 체계를 사용하도록 지정합니다.

X.509 인증서 또는 HTML 양식 인증 체계 구성

X.509 인증서 또는 HTML 양식 인증 체계를 사용하여 인증서 인증이나 HTML 양식 기반 인증 또는 둘 모두를 구현할 수 있습니다.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다. 자세한 내용은 "정책 서버 개체 복제"를 참조하십시오.

다음 단계를 수행하십시오.

1. "인프라", "인증"을 차례로 클릭합니다.
2. "인증 체계"를 클릭합니다.
3. "인증 체계 만들기"를 클릭합니다.
"인증 체계 유형의 새 개체 만들기"가 선택되어 있는지 확인합니다.
"확인"을 클릭합니다.
4. 이름 및 보호 수준을 입력합니다.
5. "인증 체계 유형" 목록에서 "X509 클라이언트 인증서 또는 양식 템플릿"을 선택합니다.
6. 서버 및 대상 정보를 입력합니다.
7. (선택 사항) "체계 설정"에서 "Persist Authentication Scheme Data"(인증 체계 데이터 유지)를 선택합니다. 이 옵션은 인증 컨텍스트 데이터가 세션 저장소에 저장되도록 지정합니다.
8. 제출을 클릭합니다.

인증 체계가 저장되고 이를 영역에 할당할 수 있습니다.

참고: 인증서가 필수이거나 선택 사항인 Apache 웹 서버의 경우에는 `httpd.conf` 파일에서 `SSL Verify Depth 10` 행의 주석 처리를 제거합니다.

익명 인증 체계

익명 인증 체계는 네트워크에서 아직 식별되지 않은 사용자에게 액세스 권한을 제공합니다. 영역에 익명 인증 체계를 할당할 경우 액세스 제어 기능은 제공되지 않지만 사용자에게 대한 콘텐츠를 개인화할 수 있습니다.

사용자가 익명 체계를 사용하는 영역의 리소스에 액세스하면 정책 서버는 GUID(전역 고유 식별자)를 할당합니다. 이 GUID는 사용자의 브라우저에 저장되어 익명 사용자를 식별할 수 있게 해 줍니다.

익명 인증 체계를 생성할 때는 게스트의 DN(고유 이름)을 지정해야 합니다. 이 게스트 DN에 개인화된 콘텐츠를 제공하는 정책을 바인딩할 수 있습니다.

참고: 익명 체계로 보호되는 영역의 개인화된 콘텐츠는 사용자의 GUID 가 아니라 게스트 DN 을 기반으로 합니다. 익명 사용자에게는 게스트 DN 을 포함하는 정책에 따라 콘텐츠가 표시됩니다. 식별된 사용자에게는 고유한 DN 이 있으므로 익명 체계로 보호되는 동일한 리소스에 식별된 사용자가 액세스할 때는 게스트 DN 대신 고유한 DN 을 기반으로 리소스 콘텐츠가 표시됩니다.

추가 정보:

[영역](#) (페이지 555)

익명 체계 사전 요구 사항

익명 인증 체계를 구성하기 전에 다음 사전 요구 사항을 충족하는지 확인하십시오.

- 익명 사용자의 게스트 DN 이 사용자 디렉터리에 있어야 합니다.
- 정책 서버와 사용자 디렉터리 간에 디렉터리 연결이 있어야 합니다.
- 익명 인증을 통해 할당된 GUID 에 따라 사용자를 추적하려면 관리 UI 의 "전역 설정" 창에서 사용자 추적을 활성화하십시오.

참고: 사용자 추적 기능이 사용되도록 설정하는 방법에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

추가 정보:

[사용자 디렉터리](#) (페이지 147)

익명 인증 체계 구성

익명 인증 체계를 사용하여 미등록 사용자에게 특정 웹 콘텐츠에 대한 액세스 권한을 부여할 수 있습니다.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다. 자세한 내용은 "정책 서버 개체 복제"를 참조하십시오.

다음 단계를 수행하십시오.

1. "인프라", "인증"을 차례로 클릭합니다.
2. "인증 체계"를 클릭합니다.
3. "인증 체계 만들기"를 클릭합니다.
"인증 체계 유형의 새 개체 만들기"가 선택되어 있는지 확인합니다.
"확인"을 클릭합니다.
4. 이름 및 보호 수준을 입력합니다.
5. "인증 체계 유형" 목록에서 "익명 템플릿"을 선택합니다.
6. 사용자의 DN 을 입력합니다.
7. 제출을 클릭합니다.
인증 체계가 저장되고 이를 영역에 할당할 수 있습니다.

사용자 지정 인증 체계

사용하려는 인증 방법이 정책 서버에서 제공되지 않을 경우 **CA API** 를 사용하여 사용자 지정 인증 체계를 개발하십시오.

소프트웨어 개발 키트를 설치한 경우 사용자 지정 인증 체계 생성에 대한 자세한 내용은 "API Reference Guide for C"(C 용 API 참조 안내서) 및 "API Reference Guide for Java"(Java 용 API 참조 안내서)를 참조하십시오. 사용자 지정 체계를 생성한 경우 "인증" 창에서 체계를 구성하십시오.

참고: 싱글 사인온에 필요한 **smauthetsso** 사용자 지정 인증 체계를 구성하는 방법에 대한 자세한 내용은 [CA SSO/WAC 통합](#) (페이지 807)을 참조하십시오.

사용자 지정 인증 체계의 사전 요구 사항은 **CA API** 를 사용하여 체계를 생성할 때 결정됩니다. 사전 요구 사항은 인증 체계에 따라 달라집니다.

사용자 지정 체계 사전 요구 사항

사용자 지정 인증 체계의 사전 요구 사항은 **CA API** 를 사용하여 체계를 생성할 때 결정됩니다. 사전 요구 사항은 인증 체계에 따라 달라집니다.

사용자 지정 인증 체계 구성

사용자 지정 인증 체계를 사용하여 제품에서 제공하지 않는 체계를 지정할 수 있습니다.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다. 자세한 내용은 "정책 서버 개체 복제"를 참조하십시오.

다음 단계를 수행하십시오.

1. "인프라", "인증"을 차례로 클릭합니다.
2. "인증 체계"를 클릭합니다.
3. "인증 체계 만들기"를 클릭합니다.
"인증 체계 유형의 새 개체 만들기"가 선택되어 있는지 확인합니다.
"확인"을 클릭합니다.
4. 이름 및 보호 수준을 입력합니다.
5. "인증 체계 유형" 목록에서 "사용자 지정 템플릿"을 선택합니다.
체계 관련 설정이 열립니다.
6. (선택 사항) "체계 일반 설정"에서 "보호 무시 허용" 확인란을 선택합니다. 이 옵션은 라이브러리의 보호 수준이 관리 UI에서 지정된 보호 수준보다 높은 우선 순위를 갖도록 지정합니다.
7. "체계 설정"에서 인증 체계에 대한 자격 증명을 처리할 라이브러리와 라이브러리에 전달되는 매개 변수를 입력합니다.
8. (선택 사항) "체계 설정"에서 "인증 세션 변수 유지"를 선택합니다. 이 옵션을 선택하지 않으면 세션 변수가 세션 저장소에 저장되지 않습니다.
9. "제출"을 클릭합니다.
인증 체계가 저장되고 이를 영역에 할당할 수 있습니다.

OAuth 인증 체계를 구성하는 방법

이 시나리오에서는 정책 서버 관리자 및 에이전트 소유자가 OAuth 인증 체계를 구성하는 방법을 설명합니다.

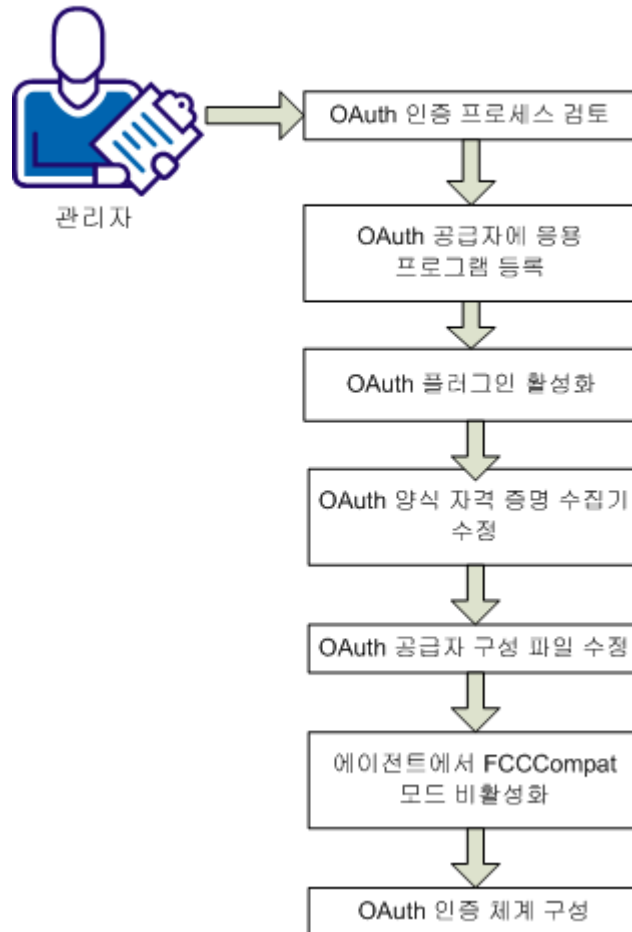
OAuth 인증 체계를 사용하면 사용자가 OAuth 공급자를 통해 자격 증명을 제출할 수 있습니다. OAuth 공급자는 사용자를 인증하고 사용자에게 대한 클레임이 포함된 인증 응답을 보냅니다. 정책 서버는 인증 응답을 확인하고 인증 프로세스를 완료하고 리소스에 대한 액세스 권한을 부여합니다.

시나리오의 목표는 사용자가 다음을 수행할 수 있게 하는 것입니다.

- OAuth 인증 프로세스가 작동하는 방식을 파악합니다.
- 필요한 에이전트 측 구성 요소를 구성합니다.
- 필요한 정책 서버 측 구성 요소를 구성합니다.

다음 그림에서는 OAuth 인증 체계를 구성하는 데 필요한 태스크를 보여줍니다.

OAuth 인증 체계를 구성하는 방법



OAuth 를 구성하려면 다음 단계를 수행하십시오.

1. [OAuth 인증 프로세스를 검토](#) (페이지 410)합니다.
2. [응용 프로그램을 OAuth 공급자에 등록합니다](#). (페이지 411)
3. [OAuth 플러그인이 사용되도록 설정](#) (페이지 413)합니다.
4. [OAuth 양식 자격 증명 수집기를 수정합니다](#). (페이지 414)
5. [OAuth 공급자 구성 파일을 수정합니다](#) (페이지 416).
6. [에이전트에서 FCCCompatMode 를 사용하지 않도록 설정](#) (페이지 421)합니다.
7. [OAuth 인증 체계를 구성합니다](#) (페이지 421).

OAuth 인증 프로세스

다음 절차에서는 OAuth 인증 체계가 작동하는 방식을 설명합니다.

1. 사용자가 리소스를 요청합니다.
2. 에이전트가 요청을 가로채고 정책 서버에 연결하여 리소스가 보호되는지 확인합니다.
3. 정책 서버에서 리소스가 OAuth 인증 체계로 보호되는지 확인합니다. 정책 서버에서 에이전트가 사용자를 OAuth FCC(양식 자격 증명 수집기)로 리디렉션하도록 요청합니다.
4. 에이전트가 사용자를 FCC 로 리디렉션합니다.
5. 사용자가 OAuth 공급자를 선택하고 공급자 사이트에서 자격 증명을 제출합니다.
6. FCC 가 사용자 식별자를 구성하여 정책 서버에 전달합니다.
7. 정책 서버가 인증 요청을 구성하여 사용자를 OAuth 공급자로 리디렉션합니다.
8. 사용자가 공급자별 자격 증명을 사용하여 OAuth 공급자에 인증됩니다.
9. 공급자가 인증 성공 응답을 FCC 로 리디렉션합니다.
10. 에이전트가 인증 응답을 정책 서버에 전달합니다.
11. 정책 서버가 공급자 인증 응답을 확인하고 이를 사용하여 첫 번째 필수 클레임 값을 결정합니다. 정책 서버는 정책 도메인의 모든 사용자 디렉터리를 검색하여 특성이 클레임 값과 일치하는 사용자를 찾습니다. 일치하는 경우 정책 서버가 사용자를 인증합니다.
참고: 인증 체계에서는 익명 모드의 인증을 지원합니다. 익명 모드에서는 정책 서버가 사용자에게 매핑하기 위해 클레임 값을 사용하지 않습니다. 정책 서버는 정책 도메인의 모든 사용자 디렉터리를 검색하여 인증 체계에서 정의한 익명 사용자와 일치하는 사용자를 찾습니다.
12. 정책 서버가 인증된 사용자의 세션 정보를 FCC 에 반환합니다.
13. FCC 가 세션 쿠키를 생성하여 웹 브라우저에 전달합니다. 사용자는 요청된 리소스로 리디렉션되고 정책 서버는 모든 권한 부여 결정을 유지 관리합니다.

응용 프로그램을 OAuth 공급자에 등록합니다.

사전 요구 사항

웹 에이전트 구성에 SecureURLs 매개 변수가 설정되어 있는지 여부와 설정된 경우 해당 값을 확인해야 합니다.

등록 프로세스의 일부는 리디렉션 URI 설정(Google) 또는 사이트 URL 설정(Facebook)의 항목을 지정하기 위한 것입니다. 이 항목의 형식은 SecureURLs 에이전트 매개 변수의 값에 따라 달라집니다. 관리 UI 에서 SecureURLs 매개 변수의 값을 확인하십시오. 이 매개 변수는 호스트 에이전트의 에이전트 구성 개체에 있습니다.

- SecureURLs 매개 변수가 Yes 로 설정되어 있으면 URL 을 다음 형식으로 입력하십시오.

`http(s)://agent_host/siteminderagent/forms/oauthcb.fcc?SMQUERYDATA=Sample`

- SecureURLs 매개 변수가 No 로 설정되어 있으면 URL 을 다음 형식으로 입력하십시오.

`http(s)://agent_host/siteminderagent/forms/oauthcb.fcc`

Google

다음 단계를 수행하십시오.

1. Google Apps 계정을 설정합니다.
2. `https://code.google.com/apis/console` 로 이동하고 로그인합니다.
3. "API Access"(API 액세스)를 선택하고 OAuth 클라이언트 ID 를 생성합니다. 클라이언트 ID 를 생성하려면 다음 정보를 입력합니다.

Home Page URL(홈 페이지 URL)

`http(s)://homepage.com`

예: `http://www.forwardinc.com`

Application type(애플리케이션 유형)

Web application(웹 애플리케이션)

Your site or hostname(사이트 또는 호스트 이름)

`http://agent_host`

예: `http://myagent.ca.com`

4. "Create clientID"(클라이언트 ID 만들기)를 클릭합니다.
5. "Redirect URI"(리디렉션 URI)의 설정을 다음 URI 로 편집합니다.

Redirect URIs(리디렉션 URI)

`http(s)://agent_host/siteminderagent/forms/oauthcb.fcc`

SecureURLs 는 설정하지 않거나 No 로 설정합니다.

또는

`http(s)://agent_host/siteminderagent/forms/oauthcb.fcc?SMQUERYDATA=Sample`

SecureURLs 는 Yes 로 설정합니다.

6. "Update"(업데이트)를 클릭합니다.

Google 등록 프로세스가 완료되었습니다.

Facebook

다음 단계를 수행하십시오.

1. Facebook 계정을 설정합니다.
2. `https://developers.facebook.com/apps` 로 이동합니다.
3. 앱 이름을 선택하고 "Continue"(계속)를 클릭합니다.
4. 표시되는 자동 가입 방지 텍스트를 입력하고 "Continue"(계속)를 클릭합니다.
5. Facebook 로그인 섹션이 있는 웹 사이트에서 다음 필드를 작성합니다.

Site URL(사이트 URL)

`http(s)://agent_host/siteminderagent/forms/oauthcb.fcc`

SecureURLs 는 설정하지 않거나 No 로 설정합니다.

또는

`http(s)://agent_host/siteminderagent/forms/oauthcb.fcc?SMQUERYDATA=Sample`

SecureURLs 는 Yes 로 설정합니다.

6. "Save changes"(변경 내용 저장)를 클릭합니다.
7. 다음 설정을 완료합니다.
 - "Domain"(도메인)을 `ca.com` 으로 설정합니다.
 - "Sandbox mode"(샌드박스 모드)를 사용하지 않도록 설정합니다.
 - "Canvas URL"(캔버스 URL)을 `https://apps.facebook.com/application_name/`으로 설정합니다.
 - "Secure canvas URL"(보안 캔버스 URL)을 `https://apps.facebook.com/application_name/`으로 설정합니다.

등록 프로세스가 진행되고 클라이언트 응용 프로그램 URL, 클라이언트 ID 및 관련 암호가 생성됩니다. OAuth 서비스가 권한 부여 코드를 가져오고 토큰에 액세스할 OAuth 권한 부여 서버 끝점 URL도 생성됩니다. 이 정보 중 일부는 OAuth 인증 체계가 올바르게 작동하기 위해 사용하는 파일을 설정할 때 필요합니다.

OAuth 플러그인이 사용되도록 설정

OAuth 플러그인은 웹 에이전트 구성 파일(WebAgent.conf) 내에서 참조됩니다. 이 플러그인은 에이전트가 OAuth 공급자와 통신하고 OAuth 공급자 인증 응답을 정책 서버에 전달할 수 있도록 합니다.

에이전트 소유자에게 필요한 플러그인이 사용되도록 설정하라고 지시하십시오.

다음 단계를 수행하십시오.

1. 웹 에이전트 호스트 시스템에 로그인합니다.
2. 웹 에이전트 구성 파일을 엽니다. 기본 파일 위치는 웹 서버 유형에 따라 달라집니다.

IIS

```
agent_home\bin\IIS
agent_home
```

에이전트 설치 경로를 지정합니다.

Oracle iPlanet(iPlanet/SunOne)

```
web_server_home/https-hostname/config
web_server_home
```

웹 서버 설치 경로를 지정합니다.

Apache, IBM HTTP 서버 및 Oracle HTTP 서버

`web_server_home/conf`

`web_server_home`

웹 서버 설치 경로를 지정합니다.

Domino(Windows)

`C:\lotus\domino`

Domino(UNIX)

`$HOME/notesdata`

3. OAuth 플러그인을 로드하는 행의 주석 처리를 제거합니다.

예:

```
#LoadPlugin="C:\Program Files\CA\webagent\bin\OAuthPlugin.dll"
```

4. 파일을 저장합니다.
5. 웹 서버를 다시 시작합니다.

OAuth 양식 자격 증명 수집기 수정

샘플 OAuth FCC 가 웹 에이전트 설치에 포함되어 있습니다. FCC 를 사용하면 사용자가 OAuth 공급자 사용자 이름을 입력하여 인증할 수 있습니다.

기본적으로 FCC 는 여러 OAuth 공급자를 표시합니다. 에이전트 소유자에게 보호되는 응용 프로그램이 지원하는 공급자만 파일에 포함하도록 FCC 를 수정하라고 지시하십시오.

다음 단계에서는 FCC 를 수정하는 방법을 설명합니다.

다음 단계를 수행하십시오.

1. 웹 에이전트 호스트 시스템에 로그인합니다.
2. 다음 위치로 이동합니다.

`agent_home\samples\forms`

`agent_home`

웹 에이전트 설치 경로를 지정합니다.

3. 텍스트 편집기에서 `oauth.fcc` 파일을 엽니다.
4. FCC 를 검토합니다. 공급자를 추가할지 제거할지를 결정합니다.
5. FCC 의 공급자 섹션을 찾습니다. 텍스트에서 `var oauth_providers` 문자열을 검색합니다.

6. `var oauth_providers` 섹션에 누락된 공급자 항목을 추가합니다. `apps` 설정 옆에 응용 프로그램 이름을 지정합니다.

다음 예제에서는 두 개의 공급자 항목 예를 보여 줍니다.

```
var oauth_providers = {
  google : {
    name : 'Google',
    image : 'images/google.gif',
    apps : 'ForwardIncGoogleApp'
  },
  facebook : {
    name : 'Facebook',
    image : 'images/facebook.gif',
    apps : 'ForwardIncFacebookApp'
  }
}
```

7. 텍스트에서 `var oauth_applications` 문자열을 검색하여 FCC의 응용 프로그램 섹션을 찾습니다. 각 응용 프로그램에 대해 다음 정보를 지정합니다.

- 응용 프로그램 이름
- 사용자가 공급자 아이콘을 클릭할 때 표시되는 레이블 텍스트입니다.
- 이미지 이미지 값은 FCC가 표시하는 공급자 아이콘의 위치입니다.

다음 예제에서는 두 개의 응용 프로그램 항목 예를 보여 줍니다. 한 항목의 이름은 `ForwardIncGoogleApp`이고 다른 항목의 이름은 `ForwardIncFacebookApp`입니다.

중요! 이러한 응용 프로그램 이름은 예제 값일 뿐입니다. 배포에는 실제 응용 프로그램 이름을 입력하십시오. 또한, 이 FCC 파일에 입력하는 응용 프로그램 이름은 [oauthproviders.xml 파일](#) (페이지 416)에 입력한 응용 프로그램 이름과 일치해야 합니다.

```
};
var oauth_applications = {

ForwardIncGoogleApp : {
  name : 'ForwardIncGoogleApp',
  label : 'Login using google application',
  image : 'images/google.ico'
}
ForwardIncFacebookApp : {
  name : 'ForwardIncFacebookApp',
  label : 'Login using facebook application',
  image : 'images/facebook.ico'
},
}
```

8. 필요하지 않은 공급자 항목을 주석 처리하여 해당 공급자를 FCC 에서 제거합니다. 공급자 이름 앞에 주석 문자열 `/*`를 입력합니다. 항목 끝에 닫는 주석 문자열 `*/`를 입력합니다. 예를 들면 다음과 같습니다.

```
/* google : {  
    name : 'ForwardIncGoogleApp',  
    image : 'images/google.gif',  
    apps : 'ForwardIncGoogleApp'  
},*/
```

9. 수정을 모두 완료한 후 스크립트를 저장합니다.
10. 웹 서버를 다시 시작합니다.

OAuth 공급자 구성 파일 수정

OAuth 공급자 구성 파일(`oauthproviders.xml`)은 정책 서버와 함께 설치됩니다. 공급자 구성 파일에는 각 공급자 및 보호되는 응용 프로그램에 대한 구성 상세 정보가 포함됩니다. 파일에 올바른 설정이 포함되지 않으면 인증이 실패합니다.

파일에 대한 정보:

- 기본적으로 이 파일에는 OAuth FCC 에서 사용할 수 있는 모든 공급자에 대한 샘플 설정이 포함되어 있습니다. 샘플 설정을 검토하고 필요에 따라 수정하십시오.

중요! 이 값은 샘플용입니다. 인증 체계를 배포하기 전에 OAuth 공급자에게 모든 구성 설정을 확인하는 것이 좋습니다.

- 공급자 구성은 여러 응용 프로그램에 공급자 구성을 재사용하기 위해 등록된 응용 프로그램 구성과는 별개입니다.
- 공급자 구성 상세 정보는 응용 프로그램 구성 상세 정보를 따라야 합니다. 각 응용 프로그램은 미리 정의된 공급자 구성 중 하나를 사용합니다.
- 각 응용 프로그램에는 해당 응용 프로그램이 등록되는 하나의 공급자에 대한 PROVIDERLINK 가 있어야 합니다.
- FCC 파일에서 공급자 설정을 추가 또는 수정하려면 또한 이 파일에서 공급자의 구성 설정을 추가하거나 수정하십시오.
- 이 파일에 입력하는 응용 프로그램 이름은 `oauth.fcc` 파일에 입력한 응용 프로그램 이름과 일치해야 합니다.
- 여러 OAuth 인증 체계를 구성하는 경우 각 체계에서 고유한 공급자 구성 파일을 사용할 수 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 위치로 이동합니다.

siteminder_home\config\properties

siteminder_home

정책 서버 설치 경로를 지정합니다.

3. 기본 공급자 구성 파일의 복사본을 백업으로 만듭니다.
4. `oauthproviders.xml` 파일을 엽니다.
5. 파일을 검토하고 필요한 OAuth 공급자 설정을 사용할 수 있는지 확인합니다. 공급자를 추가하려면 다음 단계를 수행합니다.
 - a. 기존 OAuth 공급자 노드와 모든 자식 노드를 복사합니다. 모든 공급자 노드는 다음 루트 노드 내에 포함되어 있습니다.

```
<OAuthProvider>  
</OAuthProvider>
```

- b. 새 OAuth 공급자 노드와 모든 자식 노드를 다음 루트 노드 아래에 추가합니다.

```
<TrustedOAuthProviders>  
</TrustedOAuthProviders>
```

6. 각 공급자의 설정을 구성합니다. 다음 설정 값을 업데이트합니다.

OAuth providername

이 노드의 OAuth 공급자를 식별합니다. 공급자의 이름을 입력합니다.

참고: 공급자 이름을 입력할 때는 소문자를 사용하십시오.

AuthorizationURL

이 공급자의 권한 부여 서버 끝점 URL 을 제공합니다. 이 URL 은 사용자를 성공적으로 인증한 후 권한 부여 토큰을 생성해야 합니다.

Google 예: <https://accounts.google.com/o/oauth2/auth>

Facebook 예: <https://www.facebook.com/dialog/oauth>

AccessTokenURL

액세스 토큰 끝점 URL 을 제공합니다. 사용자는 응용 프로그램 구성 상세 정보와 함께 권한 부여 코드를 교환하여 액세스 토큰에 대해 쿼리할 수 있습니다.

Google 예: <https://accounts.google.com/o/oauth2/token>

Facebook 예: https://graph.facebook.com/oauth/access_token

7. 등록된 각 응용 프로그램에 대한 설정을 구성합니다. 응용 프로그램 노드 및 모든 자식 노드는 다음 루트 노드 아래에 있습니다.

<Application>

</Application>

다음 설정 값을 업데이트합니다.

Application appname

OAuth 에 등록된 응용 프로그램에 대한 구성과 사용자 인증 구성을 식별합니다. 최종 사용자가 OAuth 인증에 대한 구성을 사용하려면 FCC 페이지에서 이 식별자를 제공해야 합니다.

예: ForwardIncGoogleApp, ForwardIncFacebookApp

중요! 이러한 응용 프로그램 이름은 예제 값일 뿐입니다. 배포에는 실제 응용 프로그램 이름을 입력하십시오. 또한, 이 파일에 입력하는 응용 프로그램 이름은 [oauth.fcc 파일](#) (페이지 414)에 입력한 응용 프로그램 이름과 일치해야 합니다.

ApplicationURL

등록된 응용 프로그램 URL 을 지정합니다. 이 설정 값을 응용 프로그램 등록 시 입력한 것과 동일한 리디렉션 URI(Google) 또는 사이트 URL(Facebook)로 업데이트합니다. 예를 들어, Google 리디렉션 URI 값이 다음과 같이 설정된 경우:

리디렉션 URI:

`https://fedserver.bizpartnerinc.ca/siteminderagent/forms/oauthcb.fcc`

이 파일에서 ApplicationURL 의 값은 다음과 같습니다.

```
</OAuthProvider>
```

```
<Application appname="ForwardIncGoogleApp">
```

```
<ApplicationURL>
```

```
<!-- HOSTNAME : WebAgent/SPS host name -->
```

```
https://fedserver.bizpartnerinc.ca/siteminderagent/forms/oauthcb.fcc
```

```
</ApplicationURL>
```

URL 의 형식은 SecureURLs 에이전트 매개 변수의 값에 따라 달라집니다. 관리 UI 에서 SecureURLs 매개 변수의 값을 확인하십시오. 이 매개 변수는 호스트 에이전트의 에이전트 구성 개체에 있습니다.

- SecureURLs 매개 변수가 Yes 로 설정되어 있으면 URL 을 다음 형식으로 입력하십시오.

```
http(s)://agent_host/siteminderagent/forms/oauthcb.fcc?SMQUERYDATA=Sample
```

예:

```
https://myagent.ca.com/siteminderagent/forms/oauthcb.fcc?SMQUERYDATA=Sample
```

- SecureURLs 매개 변수가 No 로 설정되어 있으면 URL 을 다음 형식으로 입력하십시오.

```
http(s)://agent_host/siteminderagent/forms/oauthcb.fcc
```

ClientID

OAuth 서버에 등록된 클라이언트 응용 프로그램의 식별자가 포함됩니다. 이 설정 값을 등록된 클라이언트 ID 로 업데이트합니다. 권한 부여 서버에서는 응용 프로그램이 성공적으로 등록된 경우 이 ID 값을 제공합니다.

암호

ClientID 와 연결된 암호를 나타냅니다. 이 설정 값을 ClientID 와 연결된 암호로 업데이트합니다. 권한 부여 서버에서는 응용 프로그램이 성공적으로 등록된 경우 이 값을 제공합니다.

PROVIDERLINK

응용 프로그램을 공급자와 연결합니다. 정의된 공급자의 `providername` 값을 지정합니다. 이 응용 프로그램은 OAuth 인증을 수행하는 동안 공급자 구성을 사용합니다.

예: google, facebook

범위

응용 프로그램이 사용자에게 요청하는 필수 권한 유형을 지정합니다. 예를 들어 Scope 값이 `https://www.googleapis.com/auth/userinfo.profile` 인 경우 응용 프로그램은 기본 사용자 프로필 정보에 대한 읽기 전용 권한을 부여할 수 있습니다.

이 Scope 값은 권한 부여 토큰 요청에 포함되어 전달됩니다. 클라이언트는 코드를 사용하여 UserInfoURL 특성에 지정된 리소스 URL 에 액세스할 수 있습니다. 관리자는 이 특성에 단일 값을 지정하거나 여러 값을 공백으로 구분하여 지정할 수 있습니다.

UserInfoURL

생성된 액세스 토큰으로 사용자 정보를 쿼리할 수 있는 단일 URL 이나 공백으로 구분된 여러 URL 을 지정합니다. 이 URL 은 클라이언트가 액세스를 시도하는 리소스를 나타냅니다.

UserAttribute

사용자 특성을 지정합니다. 이 값을 OAuth 사용자 정보의 사용자 식별 클레임으로 업데이트합니다. 이 특성 값은 사용자를 명확히 하는 데 사용됩니다. 예를 들어 이 사용자 특성으로 "email"을 사용할 수 있습니다.

8. 파일을 저장한 후 닫습니다.

에이전트에서 FCCCompatMode 비활성화

CAM 에이전트 구성에서 FCCCompatMode 설정을 사용하지 않도록 설정하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "인프라", "에이전트"를 차례로 클릭합니다.
3. "에이전트 구성 개체"를 클릭합니다.
4. "에이전트 구성 개체" 페이지가 표시됩니다.
5. 검색 조건을 지정하고 "검색"을 클릭합니다.

검색 조건과 일치하는 에이전트 구성 개체의 목록이 표시됩니다.

6. CAM 에이전트를 선택하고 수정합니다.

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

7. "수정"을 클릭합니다.
8. FCCCompatMode 설정을 no 로 설정합니다.
9. 변경 내용을 저장합니다.

OAuth 인증 체계 구성

관리 UI 를 사용하여 OAuth 인증 체계 개체를 구성하십시오.

네트워크에 여러 쿠키 도메인이 포함되어 있고 각 쿠키 도메인에 인증 체계가 필요한 경우 각 쿠키 도메인에서 별도의 인증 체계 개체를 구성하십시오.

참고: Solaris 플랫폼에서 작동하는 경우 **sun.security.provider.Sun** 공급자가 첫 번째 공급자로 등록되도록 **jre_root/lib/security** 디렉터리에 있는 **java.security** 파일을 수정하십시오.

다음 단계를 수행하십시오.

1. "인프라", "인증", "인증 체계"를 차례로 클릭합니다.
2. "인증 체계 만들기"를 클릭합니다.
3. 새 개체 옵션을 선택하고 "확인"을 클릭합니다.
"인증 체계 만들기" 페이지가 표시됩니다.
4. 이름 및 보호 수준을 입력합니다.
5. "인증 체계 유형" 목록에서 OAuth 템플릿을 선택합니다.
체계 관련 설정이 표시됩니다.
6. 나머지 매개 변수를 구성하고 "제출"을 클릭합니다.

중요! 프록시 설정을 변경한 경우에는 정책 서버를 다시 시작해야 합니다.

OAuth 인증 체계를 구성하는 데 필요한 태스크를 완료했습니다. 이제 정책 또는 응용 프로그램 구성 요소에서 인증 체계를 사용하여 리소스를 보호할 수 있습니다.

OpenID 인증 체계

이 시나리오는 OpenID 인증 체계의 구성하는 방법을 설명합니다.

OpenID 인증 체계를 사용하면 사용자가 OpenID 공급자를 통해 자격 증명을 제출할 수 있습니다. OpenID 공급자는 사용자를 인증하고 정책 서버로 인증 응답을 보냅니다. 정책 서버는 이 응답을 확인하고 인증 프로세스를 완료하고 리소스에 대한 액세스 권한을 부여합니다.

시나리오의 목표는 의도하는 대상자가 다음을 할 수 있게 하는 것입니다.

- OpenID 인증 프로세스가 작동하는 방식을 파악합니다.
- 인증 체계를 사용하기 위해 필요한 에이전트 측 구성 요소를 구성합니다.
- 인증 체계를 사용하기 위해 필요한 정책 서버 측 구성 요소를 구성합니다.

SiteMinder 12.52 SP1에서는 OpenID 버전 1.1 및 2.0 과 OpenID Attribute Exchange 버전 1.0 을 지원합니다.

SiteMinder 에서 OpenID 인증이 작동하는 방식

OpenID 인증 프로세스의 흐름은 다음 단계를 따릅니다.

1. 사용자가 리소스를 요청합니다.
2. 에이전트가 요청을 가로채고 정책 서버에 연결하여 리소스가 보호되는지 확인합니다.
3. 정책 서버에서 리소스가 OpenID 인증 체계로 보호되는지 확인하고 에이전트가 사용자를 OpenID FCC(양식 자격 증명 수집기)로 리디렉션하도록 요청합니다.
4. 에이전트가 사용자를 FCC 로 리디렉션합니다.
5. 사용자가 다음 태스크 중 하나를 완료합니다. FCC 가 사용자 지정된 방식에 따라 이 단계의 작업 흐름이 결정됩니다. 사용자는 다음을 수행할 수 있습니다.
 - OpenID 공급자를 선택하고 공급자 사이트에서 OpenID 자격 증명을 제출합니다.
 - OpenID 공급자를 선택하고 OpenID 사용자 이름을 제출합니다.
 - OpenID 를 선택하고 전체 OpenID 사용자 식별자를 제출합니다.
6. FCC 가 OpenID 사용자 식별자를 구성하여 정책 서버에 전달합니다.
7. 정책 서버가 OpenID 인증 요청을 구성하여 인증을 위해 사용자를 OpenID 공급자로 리디렉션합니다.
8. 사용자가 공급자별 자격 증명을 사용하여 OpenID 공급자에 인증됩니다.
9. OpenID 공급자가 성공적인 인증 요청을 FCC 로 리디렉션합니다.
10. 에이전트가 인증 응답을 정책 서버에 전달합니다.
11. 정책 서버가 공급자 인증 응답을 확인하고 이를 사용하여 첫 번째 필수 클레임 값을 결정합니다. 정책 서버는 정책 도메인의 모든 사용자 디렉터리를 검색하여 특성이 클레임 값과 일치하는 사용자를 찾습니다. 일치하는 경우 정책 서버가 사용자를 인증합니다.

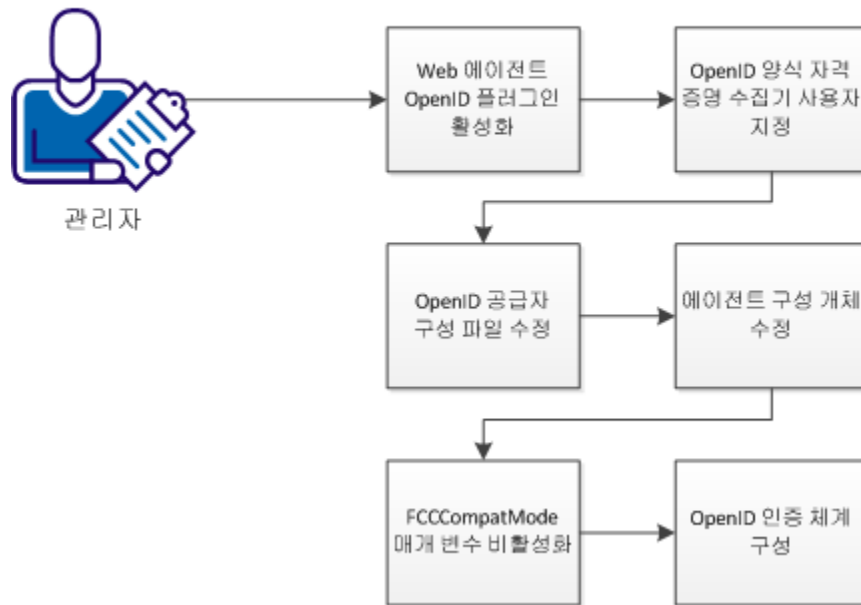
참고: 인증 체계에서는 익명 모드의 인증을 지원합니다. 익명 모드에서는 정책 서버가 사용자에게 매핑하기 위해 클레임 값을 사용하지 않습니다. 정책 서버는 정책 도메인의 모든 사용자 디렉터리를 검색하여 인증 체계에서 정의한 익명 사용자와 일치하는 사용자를 찾습니다.

12. 정책 서버가 인증된 사용자의 세션 정보를 FCC 에 반환합니다.
13. FCC 가 세션 쿠키를 생성하여 웹 브라우저에 전달합니다. 사용자는 요청된 리소스로 리디렉션되고 정책 서버는 모든 권한 부여 결정을 유지 관리합니다.

OpenID 인증 체계를 구성하는 방법

이 단원에서는 정책 서버 관리자가 OpenID 인증 체계를 구성하는 방법을 설명합니다. 다음 다이어그램에서는 필요한 태스크에 대해 설명합니다.

OpenID 인증 체계 구성 방법



다음 단계를 수행하십시오.

1. [웹 에이전트 OpenID 플러그인이 사용되도록 설정합니다](#) (페이지 425).
2. [OpenID 양식 자격 증명 수집기를 사용자 지정합니다](#) (페이지 426).
3. [OpenID 공급자 구성 파일을 수정합니다](#) (페이지 429).
4. [에이전트 구성 개체를 수정합니다](#) (페이지 432).
5. [FCCCompatMode 매개 변수를 사용하지 않도록 설정합니다](#) (페이지 433).
6. [OpenID 인증 체계를 구성합니다](#) (페이지 434).

웹 에이전트 OpenID 플러그인이 사용되도록 설정

OpenID 플러그인은 웹 에이전트 구성 파일(WebAgent.conf) 내에서 참조됩니다. 플러그인은 에이전트가 OpenID 공급자와 통신하고 OpenID 공급자 인증 응답을 정책 서버에 전달할 수 있도록 하는 데 필요합니다.

에이전트 소유자에 연결하고 소유자에게 필요한 플러그인이 사용되도록 지시하십시오.

다음 단계를 수행하십시오.

1. 웹 에이전트 호스트 시스템에 로그인합니다.
2. 웹 에이전트 구성 파일을 엽니다.

참고: 파일의 기본 위치는 웹 서버 유형에 따라 다릅니다.

- IIS

`agent_home\bin\IIS`

`agent_home`

에이전트 설치 경로를 지정합니다.

- Oracle iPlanet(iPlanet/SunOne)

`web_server_home/https-hostname/config`

`web_server_home`

웹 서버 설치 경로를 지정합니다.

- Apache, IBM HTTP 서버 및 Oracle HTTP 서버

`web_server_home/conf`

`web_server_home`

웹 서버 설치 경로를 지정합니다.

- (Windows) Domino

`C:\lotus\domino`

- (UNIX) Domino

`$HOME/notesdata`

3. OpenID 플러그인을 로드하는 행의 주석 처리를 제거합니다.

예:

```
#LoadPlugin="C:\Program Files\CA\webagent\bin\OpenIDPlugin.dll"
```

4. 파일을 저장합니다.
5. 웹 서버를 다시 시작합니다.

OpenID 양식 자격 증명 수집기 사용자 지정

샘플 OpenID FCC가 웹 에이전트 설치에 포함되어 있습니다. FCC는 사용자가 다음을 통해 인증할 수 있도록 하는 데 필요합니다.

- OpenID 공급자 사용자 이름 입력
- 전체 OpenID 식별자 입력

기본적으로 FCC는 여러 OpenID 공급자를 표시합니다. 에이전트 소유자에 연결하고 소유자에게 FCC를 수정하여 보호되는 응용 프로그램이 지원하는 공급자만 표시하도록 지시하십시오.

다음 단계를 수행하십시오.

1. 웹 에이전트 호스트 시스템에 로그인합니다.
2. 다음 위치로 이동합니다.

`agent_home\samples\forms`

`agent_home`

웹 에이전트 설치 경로를 지정합니다.

3. 텍스트 편집기에서 다음 파일을 엽니다.

`openid.fcc`

4. FCC를 검토합니다. 필요한 OpenID 공급자를 사용할 수 있는지 또는 프로필을 추가해야 하는지 확인합니다. 기본 공급자는 다음 섹션에 있습니다.

```
var providers_large
var providers_small
```

5. 필요하지 않은 공급자를 주석 처리하여 해당 공급자를 FCC에서 제거합니다. 공급자 이름에서 주석을 시작하고 프로필 끝에서 주석을 종료합니다.

예:

```
/*google : {
    name : 'Google',
    url : 'https://www.google.com/accounts/o8/id'
},*/
```

6. 공급자를 추가해야 하는 경우 크거나 작은 공급자 섹션에서 사용자 지정 공급자 ID 를 찾습니다.

예:

```


```

참고: 개별 공급자 섹션은 FCC 가 표시하는 공급자 아이콘의 크기에 해당됩니다.

- 큰 섹션에서 아이콘의 지원되는 크기는 100 x 60 픽셀입니다.
FCC 는 큰 아이콘을 최대 5 개까지 표시할 수 있습니다.
- 작은 섹션에서 아이콘의 지원되는 크기는 24 x 24 픽셀입니다.
FCC 는 작은 아이콘을 최대 11 개까지 표시할 수 있습니다.

- a. 다음 문자를 제거하여 새 공급자를 추가합니다.

```


```

- b. 레이블 및 이름 값을 업데이트합니다. 레이블 값은 사용자가 공급자 아이콘을 클릭할 때 표시되는 텍스트를 결정합니다.

예:

```


```

참고: Forward, Inc.는 설명용으로만 사용되는 가상의 회사 이름으로, 실제 회사를 가리키지 않습니다.

- c. URL 값을 업데이트합니다. URL 값은 OpenID 사용자 식별자를 나타냅니다. 정책 서버가 사용자 식별자를 OpenID 공급자에 전달합니다.

예:

```
myprovider : {  
  name : 'Foward Inc',  
  label : 'Enter your Forward Inc user name',  
  url : 'http://{username}.forwardinc.com/'  
  image : 'images/image.png'  
}
```

- d. 이미지 값을 업데이트합니다. 이미지 값은 FCC 가 표시할 공급자 아이콘의 위치를 나타냅니다.

예:

```
myprovider : {  
  name : 'Foward Inc',  
  label : 'Enter your Forward Inc user name',  
  url : 'http://{username}.forwardinc.com/'  
  image : 'images/forwardinc.png'  
}
```

- 7. 기본적으로 FCC 는 공급자 ID 가 구성되어 FCC 에서 사용되도록 설정된 순서로 공급자 아이콘을 표시합니다. 아이콘 순서를 변경하려면 공급자 ID 순서를 적절히 조정합니다.

중요! 기본 공급자 ID 는 다음 이미지 인덱스 속성을 포함합니다.

imageidx

이 속성을 제거하거나 변경하지 *마십시오*. 이 속성은 FCC 가 올바른 공급자 아이콘을 표시한다는 것을 확인합니다.

- 8. 스크립트를 저장합니다.
- 9. 웹 서버를 다시 시작합니다.

OpenID 공급자 구성 파일 수정

제품에서는 OpenID 공급자 구성 파일을 제공합니다. 이 파일은 보호되는 응용 프로그램이 지원하는 각 공급자의 구성 정보를 참조해야 합니다. 파일에 올바른 설정이 포함되지 않으면 인증이 실패합니다.

- 기본적으로 이 파일에는 OpenID FCC 에서 사용할 수 있는 모든 공급자에 대한 샘플 설정이 포함되어 있습니다. 샘플 설정을 검토하고 필요에 따라 수정하십시오.

중요! 이 값은 샘플용입니다. 인증 체계를 배포하기 전에 OpenID 공급자에게 모든 구성 설정을 확인하는 것이 좋습니다.

- FCC 에 공급자를 추가한 경우 공급자의 구성 설정을 추가하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 위치로 이동합니다.

`siteminder_home\config\properties`

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

3. 다음 단계 중 하나를 수행합니다.

- 기본 공급자 구성 파일을 엽니다.

`Openidproviders.xml`

- 기본 구성 파일을 복사하여 다른 인스턴스를 생성합니다. 구성하는 각 OpenID 인증 체계에서 자체의 공급자 구성 파일을 사용할 수 있습니다.

예: 인증 체계의 한 인스턴스에 대해서는 연방 ICAM(Identity, Credential, and Access Management) 준수를 사용하고 다른 인스턴스에는 ICAM 준수가 사용되지 않도록 설정할 수 있습니다.

4. 파일을 검토하고 필요한 OpenID 공급자 설정을 사용할 수 있는지 또는 설정을 추가해야 하는지 확인합니다.
5. 설정을 추가해야 하는 경우 다음 단계를 완료하십시오.
 - a. 기존 OpenID 공급자 노드와 모든 자식 노드를 복사합니다. 모든 필수 및 선택적 노드가 다음 노드 내에 포함되어 있습니다.

```
<OpenIDProvider>
</OpenIDProvider>
```

- b. 새 OpenID 공급자 노드와 모든 자식 노드를 다음 루트 노드에 추가합니다.

```
<TrustedOpenIDProviders>  
</TrustedOpenIDProviders>
```

6. 인증 체계에서 지원할 각 공급자에 대한 설정을 다음 노드 설명을 사용하여 구성합니다.

OpenIDProvider RequestType="value"

공급자에 대한 구성 설정의 시작을 나타냅니다.

RequestType

(선택 사항) 공급자가 지원하는 스키마 유형을 지정합니다.

유효한 값: ax 또는 sreg

기본값: ax

ProviderName

서비스를 호스트하는 OpenID 공급자의 URL 을 지정합니다. 쉼표로 구분된 공급자 URL 목록을 값에 포함할 수 있습니다.

Required Claims

OpenID 공급자가 인증 요청의 일부로 반환하는 클레임을 지정합니다. 공급자가 필수 클레임 중 일부를 제공할 수 없으면 인증이 실패합니다. 이 노드에는 하나 이상의 클레임 노드가 필요합니다.

클레임

개별 필수 클레임을 정의합니다.

URI

OpenID 공급자 클레임의 URI 형식을 지정합니다. 정책 서버는 이 값을 사용하여 인증 요청을 구성합니다.

중요! 첫 번째 필수 클레임 값이 사용자 디렉터리의 사용자 특성에 매핑되는지 확인하십시오. 정책 서버는 공급자 인증 응답을 기반으로 하는 첫 번째 필수 클레임의 값을 결정합니다. 그런 다음 정책 서버는 정책 도메인의 모든 사용자 디렉터리를 검색하여 클레임 값과 일치하는 사용자를 찾습니다. 정책 서버가 클레임 값을 사용자 특성에 매핑하지 못하는 경우 인증이 실패합니다.

값: 값은 공급자가 지원하는 스키마 유형을 따라야 합니다.

별칭

(선택 사항) URI 노드 값에 대한 사용자에게 친숙한 이름을 정의하며 URI가 저장되거나 참조되지 않게 합니다. 시스템에서는 별칭을 사용하여 클레임을 식별합니다.

값: 모든 문자열

예: 시스템에서는 세션 저장소에 있는 사용자의 이름을 반환하는 URI를 저장하지 않고 대신 클레임 이름을 전체 이름으로 참조할 수 있습니다.

참고: 세션 저장소에 저장되는 별칭에는 다음 접두사가 추가됩니다.

smopenidclaim

Optional Claims

(선택 사항) OpenID 공급자가 인증 요청의 일부로 반환할 선택적 클레임을 지정합니다. 공급자가 선택적 클레임을 제공하지 못해도 인증이 실패하지 않습니다. 이 노드에는 하나 이상의 클레임 노드가 필요합니다.

Pape

(선택 사항) ICAM 준수를 위해 필요한 속성을 정의합니다. ICAM 준수를 위한 인증 체계를 구성하는 경우 이 노드와 모든 자식 노드가 필요합니다.

max_auth_age

(선택 사항) OpenID 공급자 사용자 세션의 유효 시간을 지정합니다. 사용자 세션이 유효한 경우 OpenID 공급자는 공급자별 쿠키를 사용하여 보호된 리소스에 대해 사용자를 인증합니다. 세션이 만료되면 재인증하라는 메시지가 표시됩니다.

측정 단위: 초

기본값: 0

기본값으로 두면 사용자는 유효한 세션에 관계없이 OpenID 공급자에 대해 인증해야 합니다.

값: 값은 양의 정수여야 합니다.

정책

(선택 사항) OpenID 공급자가 따라야 하는 ICAM 정책을 쉽표로 구분된 목록으로 지정합니다. 공급자가 준수 수준을 따르지 않으면 인증이 실패합니다.

7. 파일을 저장한 후 닫습니다.

에이전트 구성 개체 수정

확장 무시 ACO 매개 변수에 대한 기본 설정을 사용하면 OpenID FCC 가 표시되지 않습니다. 관리 UI 를 사용하여 기본 설정을 수정하십시오.

다음 단계를 수행하십시오.

1. "인프라", "에이전트 구성 개체"를 차례로 클릭합니다.
2. 사용자 요청을 FCC 로 리디렉션할 에이전트에 대한 에이전트 구성 개체를 찾습니다.
3. 편집 아이콘을 클릭하여 개체를 엽니다.
4. 다음 매개 변수를 찾습니다.

IgnoreExt

5. 편집 아이콘을 클릭하고 다음 값을 추가합니다.

- .css

- .js

참고: 값을 쉽표로 구분하십시오.

예:

.class, .gif, .jpg, .jpeg, .png, .fcc, .scc, .sfcc, .ccc, .ntc, .css, .js

6. "확인"을 클릭합니다.
7. "제출"을 클릭합니다.

에이전트 구성 개체가 제외된 리소스 확장으로 업데이트됩니다.

FCCCompatMode 매개 변수를 사용하지 않도록 설정

에이전트는 이전 버전 제품과의 호환을 위해 FCCCompatMode 구성 매개 변수를 사용합니다. 최신 버전 제품(예: 12.52 SP1)의 경우 특정 기능을 사용할 때 보안 향상을 위해 이 매개 변수를 사용하지 않도록 설정해야 합니다.

참고: 이 절차에서는 정책 서버의 에이전트 구성 개체를 사용하여 중앙에서 에이전트를 구성한다고 가정합니다. 이 방법 대신 로컬 에이전트 구성 방법을 사용하는 경우에는 LocalConfig.conf 파일에서 FCCCompatMode 매개 변수를 사용하지 않도록 설정하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에서 "인프라", "에이전트 구성 개체"를 차례로 클릭합니다.
2. 원하는 에이전트 구성 개체 옆의 편집 아이콘을 클릭합니다.
3. 다음 매개 변수를 찾습니다.

FCCCompatMode

FCC/NTC 가 4.x 웹 에이전트가 보호하는 리소스 또는 타사 응용 프로그램에 양식을 제공하도록 설정합니다.

참고: FCCCompatMode 가 yes 로 설정된 경우에만 사용자 지정 인증 체계에 SMUSRMSG 가 지원됩니다.

제한: yes, no

기본값: (기존 에이전트) Yes

기본값: (프레임워크 에이전트) No

중요! 이 매개 변수를 no 로 설정하면 4.x 버전의 Netscape 브라우저가 지원되지 않습니다.

4. 값이 no 로 설정되어 있는지 확인합니다. 값이 "yes"로 설정되어 있으면 다음 단계를 계속합니다.
 - a. 매개 변수 왼쪽에 있는 편집 아이콘을 클릭합니다.
"매개 변수 편집" 대화 상자가 나타납니다.
 - b. "값" 필드를 강조 표시하고 "no"를 입력합니다.
 - c. "확인"을 클릭합니다.
"매개 변수 편집" 대화 상자가 닫힙니다.
 - d. 제출을 클릭합니다.
FCCCompatMode 매개 변수가 사용되지 않도록 설정되고 확인 메시지가 나타납니다.

OpenID 인증 체계 구성

관리 UI 를 사용하여 OpenID 인증 체계 개체를 구성합니다.

네트워크에 여러 쿠키 도메인이 포함되어 있고 각 쿠키 도메인에 인증 체계가 필요한 경우 각 쿠키 도메인에서 별도의 인증 체계 개체를 구성하십시오.

참고: Solaris 플랫폼에서 작동하는 경우 **sun.security.provider.Sun** 공급자가 첫 번째 공급자로 등록되도록 *jre_root/lib/security* 디렉터리에 있는 *java.security* 파일을 수정하십시오.

다음 단계를 수행하십시오.

1. "인프라", "인증", "인증 체계"를 차례로 클릭합니다.
2. "인증 체계 만들기"를 클릭합니다.
3. 새 개체 옵션을 선택하고 "확인"을 클릭합니다.
"인증 체계 만들기" 페이지가 표시됩니다.
4. 이름 및 보호 수준을 입력합니다.

5. "인증 체계 유형" 목록에서 **OpenID** 템플릿을 선택합니다.
체계 관련 설정이 표시됩니다.

6. 나머지 매개 변수를 구성하고 "제출"을 클릭합니다.

중요! 프록시 설정 또는 후처리 체인 설정을 변경하는 경우 정책 서버를 다시 시작하십시오.

OpenID 인증 체계를 구성하는 데 필요한 태스크를 완료했습니다. 이제 인증 체계를 정책 영역 및 EPM(Enterprise Policy Management) 응용 프로그램 구성 요소에 바인딩할 수 있습니다.

레거시 페더레이션 인증 체계

다음은 사용할 수 있는 페더레이션 인증 체계입니다.

- SAML 아티팩트 템플릿
- SAML POST 템플릿
- SAML 2.0 템플릿
- WS-Federation 템플릿

참고: 이러한 인증 체계에 대한 자세한 내용은 *레거시 페더레이션 안내서*를 참조하십시오.

가장 인증 체계

일련의 정책 서버 개체를 구성하여 권한 있는 사용자가 다른 사용자를 가장하는 것을 허용할 수 있습니다. 이 기능은 헬프 데스크 또는 고객 서비스 담당자가 고객의 문제를 해결해야 하거나 직원이 부재 중일 때 유용합니다.

가장 프로세스의 일부로 가장 인증 체계가 필요합니다. 가장 인증 체계는 권한 있는 사용자가 가장 프로세스를 시작하고, 가장할 사용자(가장 대상)를 식별하고, 가장 세션을 설정할 수 있도록 합니다. 이 인증 체계는 **HTML** 양식 인증 체계와 유사합니다.

가장 체계 사전 요구 사항

가장 인증 체계를 구성하기 전에 다음 사전 요구 사항을 충족하는지 확인하십시오.

- 가장을 구현할 쿠키 도메인의 웹 에이전트 서버에 사용자 지정된 .fcc 파일이 있어야 합니다. CA 는 웹 에이전트가 설치된 /forms 하위 디렉터리에 샘플 .fcc 파일을 제공합니다.

.fcc 파일 작성에 대한 자세한 내용은 SiteMinder FCC 파일을 참조하십시오. 가장을 위한 특정 .fcc 파일 요구 사항에 대한 자세한 내용은 [Enable Impersonation through an .fcc File](#) (페이지 695)(.fcc 파일을 통해 가장이 사용되도록 설정)을 참조하십시오.

- 정책 서버와 가장자 및 피가장자가 포함된 사용자 디렉터리 간에 디렉터리 연결이 있어야 합니다.
- 인증 프로세스를 처리하는 다음 기본 HTML 양식 라이브러리는 정책 서버에 설치됩니다.
 - smauthimpersonate.dll(Windows 의 경우)
 - smauthimpersonate.so(Solaris 의 경우)이러한 라이브러리는 인증 프로세스를 처리합니다. 이러한 파일은 정책 서버를 설치할 때 자동으로 설치됩니다.

참고: 디렉터리 매핑은 가장을 지원하지 않습니다. 가장되는 사용자인 피가장자는 도메인과 연결된 인증 디렉터리에 고유하게 존재해야 합니다. 그렇지 않으면 가장이 실패합니다.

추가 정보:

[사용자 디렉터리](#) (페이지 147)

가장 인증 체계 구성

가장 인증 체계를 사용하여 권한 있는 사용자가 다른 사용자를 가장하도록 허용할 수 있습니다.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다. 자세한 내용은 "정책 서버 개체 복제"를 참조하십시오.

다음 단계를 수행하십시오.

1. "인프라", "인증"을 차례로 클릭합니다.
2. "인증 체계"를 클릭합니다.
3. "인증 체계 만들기"를 클릭합니다.
"인증 체계 유형의 새 개체 만들기"가 선택되어 있는지 확인합니다.
"확인"을 클릭합니다.
4. 이름 및 보호 수준을 입력합니다.

5. "인증 체계 유형" 목록에서 "가장 템플릿"을 선택합니다.

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

6. 서버 이름 및 대상 정보를 입력합니다.
7. 제출을 클릭합니다.

인증 체계가 저장되고 이를 영역에 할당할 수 있습니다.

제 9 장: X.509 인증서에 대한 인증서 매핑 및 유효성 검사

이 섹션은 다음 항목을 포함하고 있습니다.

[X.509 클라이언트 인증서 인증 체계에 대한 인증서 매핑](#) (페이지 439)

[X.509 클라이언트 인증서 인증을 위한 인증서 신뢰성 검사](#) (페이지 447)

X.509 클라이언트 인증서 인증 체계에 대한 인증서 매핑

정책 서버는 인증서를 사용하여 사용자를 식별하기 위해 인증서 정보를 사용자 디렉터리의 사용자 레코드와 비교합니다. 인증서 매핑은 정책 서버가 사용자 인증서의 주체 이름을 사용하여 사용자 디렉터리에서 SiteMinder 사용자를 찾은 다음 해당 사용자를 인증하는 방식을 정의합니다.

인증서 정보가 Microsoft SQL Server, Oracle 또는 LDAP 사용자 디렉터리에 저장된 사용자에 대해 인증서 매핑을 구성할 수 있습니다.

추가 정보:

[사용자 디렉터리](#) (페이지 147)

인증서 매핑 구성

사용자 인증서 정보를 사용자 디렉터리에 저장된 정보와 비교하는 방법을 결정하려면 인증서 매핑을 구성하십시오.

다음 단계를 수행하십시오.

1. "인프라", "디렉터리"를 차례로 클릭합니다.
2. "인증서 매핑"을 클릭합니다.
3. "인증서 매핑 만들기"를 클릭합니다.

4. 인증서에 표시된 대로 정확하게 "발급자 DN"을 입력합니다. 공백이나 문자를 추가하지 마십시오.

DN 을 입력할 때 예약된 특수 문자는 백슬래시(\)로 이스케이프하십시오. 특수 문자에는 다음이 포함됩니다.

- 세미콜론(;)
- 따옴표(")
- 백슬래시(\)
- 더하기 문자(+)
- 보다 큼 문자(>)
- 보다 작음 문자(<)

DN 용으로 예약된 특수 문자에 관한 자세한 내용은 <http://www.faqs.org/rfcs/rfc2253.html> 을 참조하십시오.

참고: 관계형 데이터베이스를 정책 저장소로 사용하는 경우 발급자 DN 은 255 자를 초과할 수 없습니다. LDAP 디렉터리를 정책 저장소로 사용하는 경우 특정 디렉터리의 문자 제한을 확인하십시오.

5. 인증서가 매핑되는 디렉터리 유형을 선택합니다.

LDAP 디렉터리의 경우에는 사용자가 제시하는 인증서가 사용자 디렉터리의 사용자 기록에 저장된 인증서와 일치하는지 확인하도록 정책 서버를 구성할 수 있습니다. "디렉터리에 인증서 필요" 옵션을 사용하면 이러한 확인이 필요하도록 지정할 수 있습니다.

참고: 인증서가 저장된 사용자 기록의 특성 이름은 **usercertificate** 입니다.

6. X.509 사용자 인증서 정보를 사용자 디렉터리의 사용자 항목에 매핑하는 방법을 지정합니다. 정책 서버는 올바른 사용자 입력을 찾기 위해 다음 속성 중 하나를 사용하여 매핑을 적용할 수 있습니다.

- 단일 특성
- 사용자 지정 매핑 식
- 사용자 인증서의 전체 주체 이름

7. 목록에서 특성 이름을 선택합니다.

8. "테스트"를 클릭하여 인증서 매핑을 테스트합니다.

9. (선택 사항) "CRL 검사 수행"을 선택하고 CRL 설정을 지정합니다.

CRL 을 선택하지 않을 경우 OCSP 를 사용할 수 있습니다.

10. 제출을 클릭합니다.

인증서가 선택된 사용자 디렉터리와 매핑됩니다.

추가 정보:

[X.509 클라이언트 인증서 인증을 위한 인증서 신뢰성 검사](#) (페이지 447)

인증서 매핑 테스트

인증서 매핑을 테스트하면 정책 서버가 클라이언트 인증서를 사용자 디렉터리 특성에 매핑하는 데 사용할 검색 문자열이 표시됩니다.

다음 단계를 수행하십시오.

1. 인증서 매핑을 엽니다.

2. "매핑" 섹션에서 "테스트"를 클릭합니다.

"인증서 매핑 테스트" 창이 열립니다.

3. "디렉터리" 목록에서 사용자 디렉터리 연결을 선택합니다.

참고: "디렉터리" 목록에는 인증서 매핑을 생성할 때 선택한 유형의 기존 디렉터리 연결이 모두 포함됩니다.

"디렉터리 정보" 그룹 상자의 내용은 사용자 디렉터리 연결의 유형에 따라 달라집니다. WinNT, ODBC 및 OCI 사용자 디렉터리 연결의 경우 이 그룹 상자에는 테스트하려는 디렉터리 유형이 표시됩니다. LDAP 디렉터리 연결의 경우 이 그룹 상자에는 디렉터리 유형 및 LDAP 디렉터리 내에서 사용자 DN 을 찾는 데 사용되는 조회 시작 및 조회 끝 값도 표시됩니다.

정책 서버가 인증서 매핑을 테스트하고 "인증서 매핑 테스트" 그룹 상자에 결과를 제공합니다.

4. "닫기"를 클릭합니다.

"인증서 매핑 테스트" 그룹 상자가 닫힙니다.

사용자 지정 매핑 식

복잡한 여러 특성을 매핑할 때는 사용자 지정 매핑 식을 사용할 수 있습니다. 사용자 지정 매핑 식을 사용하면 인증서 매핑을 구성하기 위해 사용자 DN에서 추출할 여러 사용자 특성을 지정할 수 있습니다.

참고: 사용자 지정 매핑 식은 테스트 도구를 통해 인증서 기반 인증을 시뮬레이트할 때도 유용합니다.

사용자 지정 매핑 식의 구문에 적용된 구문 분석 사양은 완전한 매핑 유연성을 지원합니다. 이 구문은 인증서에서 가져올 정보와 사용자 디렉터리에서 해당 정보를 적용할 위치를 나타냅니다. 기본 구문은 다음과 같습니다.

```
UserAttribute=%{CertificateAttribute},  
UserAttribute2=%{CertificateAttribute}
```

추가 정보:

[인증서 기반 인증 테스트](#) (페이지 785)

사용자 지정 인증서 매핑에서 원치 않는 사용자 DN 조회 시작 및 끝 문자열 생략

LDAP 사용자 디렉터리에 대한 사용자 지정 인증서 매핑을 만들 때 결과 검색 쿼리 문자열에 LDAP 사용자 DN 조회 시작 및 끝 문자열이 잘못 포함됩니다. ("인증서 매핑 만들기" 창에서 지정하는 매핑 식에만 필요). 다음 예에 표시된 것처럼 결과 쿼리가 잘못되었습니다.

LDAP 사용자 DN 조회 시작

```
(samAccountName=
```

LDAP 사용자 DN 조회 끝

```
)
```

인증서 매핑 식

```
(mail=%{E})
```

결과 검색 쿼리

```
(samAccountName=(mail=%{E}))
```

검색 쿼리에서 사용자 DN 조회 시작 및 사용자 DN 조회 끝 문자열을 생략하려면 \Netegrity\SiteMinder\CurrentVersion\PolicyServer\로 이동하여 EnableCustomExprOnly 레지스트리 키를 1로 설정하십시오. 그러면 결과 검색 쿼리 문자열이 다음 예와 같이 올바르게 됩니다.

인증서 매핑 식

mail=%{E}

결과 검색 쿼리

mail=%{E}

참고: EnableCustomExprOnly 레지스트리 키가 0(기본값)이거나 이 키가 없는 경우 사용자 DN 조회 시작 및 사용자 DN 조회 끝 문자열이 결과 검색 쿼리에 포함됩니다.

LDAP 구문 검색 필터에서 논리 연산자에 대한 지원 구성

논리 연산자를 포함하는 검색 필터를 만들기 위해 LDAP 구문을 사용하려면 LegacyCertMapping 레지스트리 키를 활성화하십시오. 이 레지스트리 키가 사용되도록 설정하면 사용자가 지정된 LDAP 검색 조건을 사용하여 인증되도록 하는 인증서 매핑의 레거시 동작이 허용됩니다.

LegacyCertMapping

키 종류: DWORD

값: 0(사용 안 함) 및 1(사용)

기본값: 0

Windows 에서 이 레지스트리 키가 사용되도록 설정하려면

1. HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\PolicyServer 로 이동하고 LegacyCertMapping 을 엽니다.
2. 키 종류 값을 REG_DWORD 로 편집합니다.
3. 값을 1로 편집합니다.

참고: 0x1 이외의 값이 설정되거나 레지스트리 값이 없는 경우에는 해당 레지스트리 키가 사용되지 않도록 설정됩니다.

4. 레지스트리 키를 저장합니다.

LegacyCertMapping 이 사용되도록 설정되고 사용자 지정 매핑에 LDAP 검색 필터 구문을 사용할 수 있습니다.

UNIX 에서 이 레지스트리 키가 사용되도록 설정하려면

1. sm.registry 파일을 엽니다.
2. 파일에 다음 행을 추가합니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\  
PolicyServer=XXXXX  
LegacyCertMapping=0X1 REG_DWORD
```

3. 파일을 저장합니다.

LegacyCertMapping 이 사용되도록 설정되고 사용자 지정 매핑에 LDAP 검색 필터 구문을 사용할 수 있습니다.

사용자 지정 매핑: 예 1

사용자 인증서에 다음이 포함되어 있다고 가정합니다.

SubjectDN: CN=John Smith, UID=JSMITH, OU=development, O=CompanyA

이 경우 다음과 같은 사용자 지정 매핑을 지정할 수 있습니다.

CN=%{UID}, OU=%{OU}, O=%{O}

결과 UserDN 은 다음과 같습니다.

CN=JSMITH, OU=development, O=CompanyA

사용자 지정 매핑: 예 2

사용자 지정 매핑 구문은 다음 예와 같이 보다 복잡한 매핑도 처리합니다.

사용자 인증서에 다음이 포함되어 있다고 가정합니다.

Subject DN: CN=John Smith + UID=jsmith +EMAIL=jsmith@companyA.com,
ou=development, o=companyA

이 경우 다음과 같은 사용자 지정 매핑을 지정할 수 있습니다.

CN=%{CN.CN}+UID=%{CN.UID}, OU=%{O}

결과 UserDN 은 다음과 같습니다.

CN=John Smith+UID=JSMITH, OU=companyA

위 예의 CN 에는 여러 특성이 포함되어 있습니다. 이 구문은 "CN.CN 또는 CN.UID"를 지정하여 UserDN 의 CN 에 적용할 CN 구성 요소를 나타냅니다. 이 구문은 사용자 지정 식이 CN 의 CN 및 UID 부분 모두를 사용함을 나타냅니다.

참고: 사용자 디렉터리의 여러 특성을 명확하게 하기 위해 "+" 연산자를 사용할 수 없습니다. "+" 연산자는 사용자 디렉터리에 있는 사용자에 대한 사용자 DN의 다른 문자와 마찬가지로 사용됩니다.

사용자 지정 매핑: 예 3

정적 텍스트는 사용자 지정 식에서 대괄호 표기 외부에 배치하여 나타낼 수 있습니다.

사용자 인증서는 다음을 포함합니다.

Subject DN: CN=John Smith, UID=JSMITH, OU=development

이 경우 다음과 같은 매핑을 지정할 수 있습니다.

CN=%{UID}, OU=%{OU}, O=companyA

결과 UserDN은 다음과 같습니다.

CN=JSMITH, OU=development, O=CompanyA

템플릿 문자열 사용

템플릿 문자열은 텍스트와 해시 괄호로 묶은 식 %{...}으로 구성됩니다. 대괄호 외부의 모든 텍스트는 변경되지 않고 반환됩니다. 해시 괄호로 묶은 식은 다음 규칙에 따라 계산됩니다.

- 고유하지 않은 변수 이름(예: DN)은 반환되기 전에 확인됩니다.
- 고유한 변수 이름(예: DN.UID)은 반환되기 전에 변수 구성 요소로 확인됩니다.

인증서 일련 번호 또는 IssuerDN에 매핑

인증서 매핑은 subjectDN의 일부가 아닌 CertSerialNumber 및 IssuerDN 특성의 매핑을 지원합니다. 사용자 인증서의 subjectDN에 있는 이러한 특성은 기본 사용자 특성이나 사용자 지정 사용자 특성(예: 사용자 디렉터리의 UID 또는 CN)에 매핑될 수 있습니다.

이러한 특성을 매핑하려면 "인증서 매핑" 창의 "매핑 식" 필드에 다음 표기를 추가하십시오.

- CustomAttributeinLDAP1 = %{CertSerialNumber}

동일한 유형의 여러 특성에 대한 사용자 지정 인증서 매핑

일부 인증서의 경우 "주체 DN"에 동일한 유형의 여러 특성이 있을 수 있습니다. SiteMinder에서는 사용자 지정 인증서 매핑을 사용하여 특정 유형의 첫 번째 특성을 제외한 다른 특성을 확인하기 위한 간단한 방법을 지원합니다. 해당 구문은 다음과 같습니다.

`%{attribute_name}` - 첫 번째로 나타나는 `attribute_name` 을 확인하려는 경우

`%{attribute_nameN}` - N 번째로 나타나는 `attribute_name` 을 확인하려는 경우

예를 들어, 인증서의 주체 DN 이 다음 특성을 포함하는 경우 임의의 `sn` 특성에 대한 사용자 지정 인증서 매핑을 설정할 수 있습니다.

`CN=user,ou=dev,sn=1234,sn=2345,sn=3456,o=company,c=us`

따라서 첫 번째 `sn` 에 매핑하려면 사용자 지정 매핑으로 `%{sn}`을 입력하십시오. 두 번째 `sn` 에 매핑하려면 사용자 지정 매핑으로 `%{sn2}`를 입력하면 됩니다.

필수 특성이 아닌 특성에 매핑

개인별로 인증서가 조금씩 다를 수 있습니다. 예를 들어 일부 사용자에게는 계정 번호가 두 개 있는 반면 다른 사용자에게는 번호가 하나만 있을 수 있습니다. 이러한 경우 두 번째 특성이 있으면 두 번째 번호로 매핑할 수 있습니다. 이 작업은 다음과 같은 표기법을 사용하여 수행할 수 있습니다.

`%{attribute_name2/attribute_name}`

앞의 예에서 "주체 DN"에 두 번째 번호가 있으면 이를 사용하고 그렇지 않으면 첫 번째 계정 번호를 사용하도록 지정하려면 사용자 지정 매핑으로 `%{SN2/SN}`을 입력하면 됩니다.

이 표기법은 인증서 매핑에 허용되는 서로 다른 두 특성을 지정하는 데도 사용될 수 있습니다. 예를 들어 `SN` 을 사용하되, `SN` 이 없는 경우에는 `CN` 을 사용할 수 있도록 지정하려면 `%{SN/CN}`을 입력합니다.

X.509 클라이언트 인증서 인증을 위한 인증서 신뢰성 검사

인증서 유효성 검사는 X.509 클라이언트 인증서 인증의 선택적 기능입니다.

정책 서버는 다음 방법을 사용하여 사용자 인증서가 유효한지 여부를 확인할 수 있습니다.

- CRL(인증서 해지 목록) 검사

정책 서버는 CRL 을 사용하여 인증서가 해지되었는지 여부를 확인할 수 있습니다. 관리 UI 에서 CRL 디렉터리의 경로를 지정하거나 "CRL Distribution Points"(CRL 배포 지점)를 선택하여 CRL 을 찾을 수 있습니다.

- OCSP(온라인 인증서 상태 프로토콜) 검사

정책 서버는 단일 사용자와 관련된 OCSP 응답자에 요청을 보냅니다. OCSP 응답자는 사용자 인증서의 해지 상태를 확인하고 응답을 되보냅니다.

정책 서버가 사용할 인증서 유효성 검사 방법을 결정하는 방식은 다음과 같습니다.

- CRL 검사만 구성된 경우 정책 서버는 CRL 을 사용합니다.
- OCSP 만 구성된 경우 정책 서버는 OCSP 를 사용합니다.
- 장애 조치가 사용되도록 설정된 상태에서 CRL 검사와 OCSP 가 구성된 경우 정책 서버는 지정된 기본 유효성 검사 방법(CRL 또는 OCSP)을 먼저 사용합니다. 기본 유효성 검사 방법이 실패하면 보조 방법이 사용됩니다. 다음 요청에서는 정책 서버가 기본 방법으로 돌아갑니다.

정책 서버는 첫 번째로 받은 *양호* 또는 *해지됨* 응답을 최종적인 것으로 간주합니다. 첫 번째 유효한 응답 후에는 정책 서버가 후속 CRL 또는 OCSP 응답을 요청하지 않습니다. 또한 정책 서버는 사용자 인증서의 종합적인 상태를 확인하기 위해 CRL 및 OCSP 유효성 검사의 결과를 집계하지 않습니다.

추가 정보:

[OCSP 와 CRL 간의 장애 조치](#) (페이지 469)

유효성 검사를 구현하기 위한 사전 요구 사항

사용자 인증서의 유효성을 검사하려면 사용자가 보호된 리소스를 요청할 때 사용자를 인증하도록 X.509 클라이언트 인증서 인증 체계를 구성하십시오.

[X.509 클라이언트 인증서 인증 체계](#) (페이지 389)를 설정하기 위한 지침을 검토하십시오.

CRL 및 OCSP 를 구성하기 위한 지침은 다음에 나오는 단원에 설명되어 있습니다.

인증서 해지 목록 검사

CRL(인증서 해지 목록)은 디지털로 서명된 해지된 인증서 목록으로, 해당 인증서를 발급한 CA(인증 기관)에서 게시합니다. 인증서를 CRL 과 비교하면 인증서가 유효한지 여부를 확인할 수 있습니다.

정책 서버 인증서 매핑에 구성된 각 발급자 DN 마다 CRL 을 하나씩 사용할 수 있습니다.

정책 서버는 다음 중 한 가지 방법으로 CRL 을 가져옵니다.

- LDAP 디렉터리에서 CRL 을 가져옵니다.

정책 서버는 CRL 구성 시 지정한 LDAP 디렉터리에 대한 연결을 설정할 수 있습니다. 정책 서버는 해당 디렉터리에서 CRL 을 가져옵니다.

LDAP 디렉터리에는 여러 CRL 이 있을 수 있지만 각 인증서 매핑은 해당 매핑의 진입점으로 식별된 CRL 하나만 참조할 수 있습니다. 따라서 각 CRL 마다 진입점이 달라야 합니다.

참고: 정책 서버는 모든 사유 코드가 포함된 CRL 만 수락하고 특정 사유 코드만 포함된 CRL 은 거부합니다.

- CDP(CRL 배포 지점) 확장으로 지정된 위치에서 CRL 을 가져옵니다.

사용자 인증서에는 배포 지점 확장이 포함될 수 있습니다. CDP 확장은 CRL 을 가져올 수 있는 위치를 가리킵니다. 정책 서버는 한 CRL 에 대한 단일 항목이나 서로 다른 여러 CRL 에 대한 여러 포인터가 있는 배포 지점 확장을 지원합니다.

배포 지점에서는 HTTP, HTTPS, LDAP 등의 다양한 원본을 사용할 수 있습니다. CDP 확장에 여러 값을 갖는 배포 지점 이름을 사용하는 항목이 포함되어 있는 경우 이러한 값은 모두 동일한 CRL 을 가리켜야 합니다.

정책 서버는 CRL 을 가져온 후 필요한 검사를 수행할 수 있습니다. 관리 UI 에서 CRL 캐싱이 사용되도록 설정한 경우 정책 서버는 CRL 을 메모리에 저장할 수 있습니다. 캐싱이 사용되도록 설정하지 않을 경우 정책 서버는 인증 요청이 있을 때마다 외부에서 CRL 을 가져와야 합니다.

CRL 에 대한 사유 코드 요구 사항

정책 서버는 가능한 모든 사유 코드에 대한 해지 정보가 포함된 CRL 만 지원합니다. CRL 에 일부 사유 코드와 관련하여 해지된 인증서만 포함된 경우 정책 서버는 오류를 생성하고 해당 CRL 을 유효하지 않은 것으로 처리합니다. 정책 서버는 유효하지 않은 CRL 을 무시하고 유효한 CRL 을 찾을 때까지 사용 가능한 CRL 을 계속 찾습니다.

정책 서버는 *델타* CRL 을 유효하지 않은 CRL 로 처리합니다. 델타 CRL 에는 CA 가 전체 CRL 을 발급한 후 해지 상태가 변경된 인증서만 나열됩니다. 정책 서버는 델타 CRL 을 무시하고 유효한 CRL 을 찾을 때까지 사용 가능한 CRL 을 계속 찾습니다.

사용 가능한 모든 CRL 을 검색한 후에도 유효한 CRL 을 찾지 못할 경우에는 정책 서버가 사용자를 인증하지 않습니다.

CRL 크기 제한

정책 서버는 CRL 을 캐시합니다. 정책 서버의 기본 캐시 크기는 최대 2 MB 입니다. CRL 이 기본 캐시 크기를 초과할 경우 캐시 크기를 최대 1 GB 로 늘리십시오. 캐시 크기를 늘리려면 MaxCRLBufferMB 레지스트리 키를 추가합니다.

다음 단계를 수행하십시오.

1. 정책 서버에 액세스한 후 사용 중인 운영 체제 플랫폼에 해당하는 단계를 수행합니다.

Windows: 레지스트리 편집기를 열고

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Netegrity\SiteMinder\Cu
rrentVersion\PolicyServer 로 이동합니다.

UNIX: sm.registry 파일을 엽니다. 이 파일의 기본 위치는
siteminder_home/registry 입니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

2. 레지스트리 값 종류를 REG_DWORD 로 지정하여 MaxCrlBufferMB 를
추가합니다.

측정 단위: MB

기준: 10 진수

기본값: 2

최소값: 1

최대값: 1023

3. 다음 단계 중 하나를 완료하십시오.

Windows: 레지스트리 편집기를 종료합니다.

UNIX: sm.registry 파일을 저장합니다.

4. 정책 서버를 다시 시작합니다.

CRL 서명 확인

CRL 서명 확인은 CRL 검사의 선택적 기능입니다.

정책 서버는 인증서를 CRL 과 비교하기 전에 LDAP 디렉터리에 저장된 CA 인증서를 사용하여 CRL 의 서명을 확인합니다. 정책 서버는 관리 UI 에서 인증서 매핑에 대해 구성한 CRL 디렉터리의 DN 이나 인증서의 발급자 DN 을 기반으로 식별된 LDAP 사용자 디렉터리의 특정 항목에서 CA 인증서를 검색합니다.

CA 인증서는 정책 서버가 액세스할 수 있는 LDAP 디렉터리에 저장하십시오. 이 LDAP 디렉터리에서 **cacertificate** 라는 특성을 가진 특정 디렉터리 항목을 구성하십시오. **cacertificate** 특성은 여러 CA 인증서를 저장할 수 있는 다중값 특성입니다. CRL 이 분할되고 각 파티션이 서로 다른 CA 키로 서명된 경우 여러 CA 인증서가 필요할 수 있습니다. 정책 서버는 지정된 파티션에 대해 연결된 CA 서명 인증서에 액세스할 수 있는 경우에만 파티션의 서명을 확인할 수 있습니다.

서명 확인을 위해 정책 서버는 다음과 같은 해시 알고리즘을 사용할 수 있습니다.

- MD5
- MD2
- SHA1
- SHA2 알고리즘(SHA224, SHA256, SHA384 및 SHA512)

참고: 사용되는 서명 알고리즘은 CRL 에 지정되어 있습니다.

CA 인증서를 사용할 수 없거나 CRL 이 지원되지 않는 알고리즘으로 서명된 경우에는 CRL 확인 프로세스 중에 서명 검사가 사용되지 않도록 설정할 수 있습니다.

중요! 서명 검사가 해제된 경우 CRL 이 저장된 리포지토리가 적절하게 보호되는지 확인하십시오.

CRL 을 찾기 위한 CRL 배포 지점

CDP(CRL 배포 지점)는 CRL 위치를 가리키는 인증서 확장입니다. 정책 서버는 지정된 위치에서 CRL 을 가져와 해지된 인증서가 무엇인지 확인할 수 있습니다.

CDP 확장에 CRL 을 찾을 원본을 여러 개 지정할 수 있습니다. 각 원본에는 CRL 을 찾는 데 필요한 모든 정보가 있습니다. 정책 서버는 정보를 가져오는 다양한 옵션을 통해 CRL 을 쉽게 구할 수 있습니다. CDP 확장에 포함할 수 있는 원본은 다음과 같습니다.

- LDAP
- HTTP
- HTTPS

HTTPS 배포 지점의 경우 정책 서버는 보안 연결을 생성합니다. 이 보안 연결이 이루어지려면 유효한 CA 인증서 또는 인증서 번들(여러 인증서가 연결되어 하나의 체인을 이루는 파일)이 *policy_server_home/config* 디렉터리에 있어야 합니다. 유효한 인증서가 없으면 HTTPS 서버에 대한 연결이 실패합니다.

HTTPS 연결용 CA 인증서 파일은 PEM 형식(base64 로 인코딩)이어야 하고 이름은 **cert.pem** 이어야 합니다. 인증서가 PEM 형식이 아니면 OpenSSL 명령줄 유틸리티를 사용하여 변환합니다. **cert.pem** 파일은 CDP 확장에 구성된 SSL 웹 서버에 대한 발급자 인증서와 각 배포 지점에 대한 트러스트된 CA 인증서를 포함해야 합니다.

참고: OpenSSL 유틸리티에 대한 자세한 내용은 OpenSSL 설명서를 참조하십시오.

CDP 확장에 항목이 여러 개 있는 경우 정책 서버는 모든 사유 코드를 포함하여 성공적으로 가져온 첫 번째 CRL 을 사용하여 인증서 유효성을 검사합니다. CRL 을 가져오는 순서는 인증서에 항목이 나열된 순서와 같습니다. CDP 목록의 첫 번째 CRL 을 가져올 수 없는 경우 정책 서버는 CRL 을 가져올 수 있을 때까지 계속해서 다음 CRL 을 가져오려고 시도합니다.

정책 서버가 어떤 원본에서도 유효한 CRL 을 가져올 수 없으면 인증이 실패하고 사용자는 액세스가 거부됩니다. CRL 과 OCSP 간에 장애 조치가 사용되도록 설정할 경우에는 예외적으로 이 동작이 발생하지 않습니다. CRL 검사가 기본 유효성 검사 방법이고 이 검사가 실패한 경우 정책 서버는 차선책으로 OCSP 에 장애 조치됩니다.

참고: OCSP 구성 파일에서 [장애 조치](#) (페이지 469)가 사용되도록 설정하십시오.

"인증서 매핑" 대화 상자에서 CRL Checking(CRL 검사) 설정의 일부로 "CRL Distribution Points"(CRL 배포 지점)를 구성합니다.

분할된 CRL 의 서명 확인

다양한 CA 키가 CRL 의 서로 다른 파티션에 서명할 수 있습니다. 정책 서버는 각 파티션과 연관된 CA 서명 인증서에 액세스할 수만 있으면 모든 CRL 파티션의 서명을 확인할 수 있습니다.

분할된 CRL 사용은 CRL 을 찾기 위해 인증서 배포 지점을 사용할 때와 관련이 있습니다. 확장은 다양한 CRL 에 대한 여러 연결을 포함할 수 있으며 모든 연결은 서명이 확인되어야 합니다.

정책 서버는 LDAP 디렉터리에 저장된 CA 인증서를 사용하여 CRL 의 서명을 확인합니다. 이 LDAP 디렉터리에서 **cacertificate** 라는 특성을 가진 특정 항목을 구성하십시오. 이 특성은 다중값 특성입니다. 다양한 CA 키로 서명된 분할된 CRL 을 확인하려면 여러 CA 인증서가 필요합니다.

인증서 해지 목록 검사 구성

사용자 인증서가 해지되었는지 여부를 확인하도록 CRL 검사를 구성합니다. 이렇게 확인을 하면 클라이언트 인증서가 올바르지 않은 사용자가 보호된 리소스에 액세스하는 것을 방지할 수 있습니다.

CRL 은 LDAP 디렉터리 또는 CDP 가 지정하는 위치에서 가져올 수 있습니다. 정책 서버가 특정 LDAP 디렉터리에서 CRL 을 가져오는 경우 해당 디렉터리에 대한 연결을 구성하십시오. 이 LDAP 디렉터리는 사용자 저장소 및 CRL 저장소의 역할을 할 수 있습니다. CRL 검사를 구성하기 전에 또는 CRL 구성 프로세스 도중에 디렉터리를 구성합니다.

다음 단계를 수행하십시오.

1. "인프라", "디렉터리"를 차례로 클릭합니다.
2. "인증서 매핑"을 클릭합니다.
"인증서 매핑" 페이지가 표시됩니다.
3. "발급자 DN" 이름을 클릭하여 인증서 매핑을 선택합니다.
"인증서 매핑 보기" 페이지가 표시됩니다.
4. "수정"을 클릭합니다.
설정과 컨트롤이 활성화됩니다.
5. "CRL 검사 수행"을 선택합니다.
CRL 특정 필드와 컨트롤이 표시됩니다.
6. 정책 서버가 CRL 을 가져오는 LDAP 디렉터리의 이름을 "CRL 디렉터리" 필드에서 선택합니다.

디렉터리 이름은 관리 UI 의 "사용자 디렉터리" 섹션에서 디렉터리를 구성할 때 할당한 이름입니다. 목록에 사용자 디렉터리가 없는 경우에는 "만들기"를 클릭하여 디렉터리 연결을 추가합니다.

LDAP 디렉터리를 지정하지 않을 경우에는 정책 서버가 CRL 을 검색하는데 사용할 방법으로 "배포 지점 사용"을 선택합니다.

참고: "CRL 디렉터리" 필드에 대한 선택적 텍스트 문자열 값이 있으며 해당 문자열은 "인증서 확장에서 가져오기"입니다. CRL 검색을 위해 배포 지점을 사용하려는 경우에만 이 옵션을 선택하십시오.
7. "CRL 디렉터리"에서 사용자 디렉터리를 지정한 경우 "CRL 디렉터리"의 DN 에서 입력 항목에 대한 값을 입력합니다.

"CRL 디렉터리"의 DN 에 지정된 값은 정책 서버가 CRL 을 찾기 위해 CRL 디렉터리에서 조회하는 DN 입니다. 이 값은 "CRL 디렉터리"로 LDAP 디렉터리를 선택한 경우에만 유효합니다. CRL 을 찾기 위한 배포 지점이 사용되도록 설정한 경우 이 필드를 비워 두십시오.

8. (선택 사항) CRL의 서명을 확인하려면 "서명 확인"을 선택하십시오.

CRL의 서명 확인에 필요한 인증서를 검색하기 위해 정책 서버에는 액세스 가능한 LDAP 호스트가 필요합니다. 관리 UI에서 LDAP 호스트를 사용자 디렉터리 연결로 구성했는지 확인하십시오.

정책 서버는 CRL 배포 지점을 사용하여 CRL을 찾을 수 있습니다. 이 배포 지점이 LDAP URI인 경우 정책 서버는 CRL 서명을 확인할 수 있습니다. 배포 지점이 HTTP URI인 경우에는 인증서를 검색할 위치로 LDAP 호스트를 사용할 수 없기 때문에 "서명 확인" 옵션을 선택하지 마십시오.

9. (선택 사항) "배포 지점 사용"을 선택하여 CRL을 찾는 데 CDP 확장을 사용합니다. CRL 디렉터리를 지정하는 대신 이 옵션을 사용할 수 있습니다.

"배포 지점 사용"을 선택하고 "CRL 디렉터리"에 디렉터리를 입력하면 정책 서버는 배포 지점만 사용하여 CRL을 찾습니다. 배포 지점은 CRL 디렉터리보다 우선 순위가 높습니다.

10. 필요에 따라 나머지 설정을 지정하고 "제출"을 클릭합니다.

인증서 해지 목록 검사가 활성화됩니다.

HTTP 프록시를 통해 CRL 액세스

CRL 요청은 HTTP 연결을 통해 이루어지며, 인증서 유효성 검사를 위해 CRL 을 검색하려면 HTTP GET 요청이 필요합니다.

많은 엔터프라이즈 환경에서 HTTP 트래픽은 HTTP 프록시를 거칩니다. 정책 서버가 HTTP 프록시를 통해 CRL 을 검색할 수 있도록 하려면 정책 서버가 있는 시스템에서 `http_proxy` 환경 변수를 설정하십시오. 예를 들면 다음과 같습니다.

```
set http_proxy=http://username:password@proxy.example.org:8080
export http_proxy
```

포트 번호를 지정하지 않을 경우 SiteMinder 는 기본적으로 포트 1080 을 사용합니다.

username

프록시 서버의 로그인 사용자 이름입니다. 이 이름은 프록시 서버 구성에 포함된 유효한 사용자여야 합니다.

password

프록시 서버의 로그인 암호입니다. 이 암호는 프록시 사용자 구성에 포함된 유효한 항목이어야 합니다.

참고: 프록시를 통해 OCSP 응답자에 액세스하기 위해 이 환경 변수를 사용할 수는 없습니다.

OCSP(온라인 인증서 상태 프로토콜) 검사

OCSP(온라인 인증서 상태 프로토콜)는 사용자 인증서가 유효한지 여부를 확인하여 사용 환경 전체의 보안을 유지하는 데 유용합니다. OCSP 는 OCSP 응답자를 사용하여 X.509 클라이언트 인증서의 해지 상태를 확인합니다. OCSP 응답자는 인증서 유효성 검사 데이터를 집계하고 특정 인증서에 대한 OCSP 요청에 응답하여 실시간으로 이 확인 작업을 수행합니다.

OCSP 의 이점 중 하나는 클라이언트 측에서 최신 인증서 상태 정보를 유지하기 위해 CRL 을 계속 다운로드할 필요가 없다는 점입니다. 또한 CRL 은 크기가 클 수 있습니다.

OCSP 검사를 구현하기 위해 정책 서버는 **SMocsp.conf** 라는 텍스트 기반 구성 파일을 사용합니다. 이 파일은 **policy_server_home/config** 디렉터리에 있으며 SiteMinder OCSP 기능을 사용하려면 이 파일이 있어야 합니다.

SMocsp.conf 파일에는 하나 이상의 OCSP 응답자가 작동하는 방식을 정의하는 설정이 포함됩니다. 사용자 인증서가 유효한지 여부를 확인할 때 정책 서버는 **SMocsp.conf** 파일에서 발급자 DN 을 찾습니다. 발급자 DN 을 찾은 경우 발급자 DN 과 연결된 지정된 OCSP 응답자를 사용하여 인증서 상태 검사가 수행됩니다. 정책 서버는 OCSP 검사만 수행하고 정책 서버가 발급자 DN 을 찾은 경우 인증서가 유효하다고 간주합니다. 발급자 DN 이 없어서 인증서가 유효한 것으로 간주되므로 OCSP 유효성 검사가 필요하지 않게 됩니다.

OCSP 요청에 서명할 수 있지만 이는 선택적인 기능입니다.

OCSP 응답자가 정책 서버에 응답을 반환하면 정책 서버는 기본적으로 서명된 응답의 유효성을 검사합니다. **SMocsp.conf** 파일의 몇 가지 설정에는 응답 확인이 사용되도록 설정하는 구성이 필요합니다.

참고: 관리 UI 에서 CRL 검사가 사용되도록 설정된 경우 정책 서버는 기본적으로 **SMocsp.conf** 파일의 존재 여부에 관계없이 CRL 검사를 사용합니다. 장애 조치가 사용되도록 설정하고 OCSP 를 기본 유효성 검사 방법으로 설정한 경우에만 OCSP 가 CRL 검사보다 우선합니다. 장애 조치는 OCSP 구성 파일에서 구성됩니다.

OCSP 사전 요구 사항

인증서 유효성 검사에 OCSP 를 사용하려면 다음 구성 요소를 설정하십시오.

- CA(인증 기관) 환경을 설정하십시오.
- OCSP 응답자를 설정하십시오.
- SiteMinder 로 반환된 OCSP 응답자의 서명을 확인하는 OCSP 트러스트된 응답자 인증서를 저장하도록 LDAP 디렉터리를 구성하십시오. OCSP 트러스트된 응답자 인증서는 하나의 트러스트된 유효성 검사 인증서 또는 여러 인증서의 모음입니다.

이러한 인증서는 OCSP 트랜잭션과 별도의 통신에서 가져올 수 있습니다.

트러스트된 인증서 또는 인증서 모음을 저장하려면 관리 UI 의 "사용자 디렉터리" 섹션에서 LDAP 디렉터리를 구성하십시오. 사용자 디렉터리가 있으면 정책 서버가 사용자 디렉터리에 연결하고 인증서 또는 인증서 모음을 찾아서 응답 서명을 확인할 수 있습니다. 인증서 모음을 저장할 때는 모든 인증서가 저장되도록 디렉터리 항목에 다중 값 바이너리 특성을 사용하십시오.

OCSP 응답자에는 서명 유효성 검사 인증서와 응답이 포함될 수 있습니다. 이 경우 정책 서버는 LDAP 디렉터리의 트러스트된 인증서를 사용하여 인증서 및 응답 서명을 확인합니다.

서명 유효성 검사 인증서가 응답에 없는 경우 정책 서버는 LDAP 디렉터리의 인증서 또는 인증서 모음을 사용하여 응답의 서명을 확인합니다.

OCSP 를 구성할 때는 SMocsp.conf 파일의 ResponderCertEP 설정에 인증서 또는 인증서 모음의 위치를 지정하십시오.

정책 서버는 SHA-1 및 SHA-2 알고리즘 제품군(SHA224, SHA256, SHA384, SHA512)을 사용하여 서명된 OCSP 응답을 지원합니다.

- 사용자 인증서를 발급한 CA 인증서를 LDAP 디렉터리에 저장하십시오. 이 CA 인증서는 사용자 인증서를 확인합니다. 이 인증서를 OCSP 트러스트된 응답자 인증서를 저장하는 LDAP 디렉터리 또는 다른 LDAP 디렉터리에 저장할 수 있습니다.
- SiteMinder OCSP 구성 파일(SMocsp.conf)을 구성하십시오. 샘플 구성 파일 SMocsp.Sample.conf 가 정책 서버와 함께 설치됩니다. 이 파일을 복사하고 이름을 SMocsp.conf 로 바꾼 다음 필요에 따라 수정하십시오. UNIX 운영 플랫폼의 경우에는 파일 이름의 대/소문자 구분을 유지해야 합니다.
- (선택 사항) 정책 서버가 OCSP 요청에 서명하기 위해 사용하는 개인 키/인증서 쌍을 정책 서버에서 사용할 수 있는지 확인하십시오. 이 키/인증서 쌍을 인증서 데이터 저장소에 저장하십시오.

OCSP 구성 파일 생성

정책 서버는 OCSP 검사를 구축하는 데 `SMocsp.conf` 라는 파일을 사용합니다. 이 파일은 하나 이상의 OCSPResponder 레코드가 있는 ASCII 파일입니다.

`SMocsp.conf` 파일은 `siteminder_home/config` 디렉터리에 있어야 합니다. 구성의 편의를 위해 정책 서버와 함께 샘플 파일(`SMocsp.Sample.conf`)이 `config` 폴더에 설치됩니다. OCSP 를 환경에 맞게 구성하려면 샘플 파일을 복사하고 이름을 `SMocsp.conf` 로 바꾸십시오.

참고: UNIX 플랫폼의 경우 파일 이름의 대/소문자 구분을 유지하십시오.

다음은 하나의 OCSPResponder 항목이 있는 `SMocsp.conf` 파일의 예입니다.

참고: 이 샘플 파일은 사용 가능한 모든 설정을 보여 줍니다. 하지만 모든 설정이 필요한 것은 아닙니다.

```
[
OCSPResponder
IssuerDN C=US,ST=Massachusetts,L=Boston,O=,OU=QA,CN=Issuer,E=user@domain.com
AlternateIssuerDN C=US,ST=New York,L=Islandia,O=,OU=QA,CN=Issuer,E=user@domain.com
CACertDir 10.1.22.2:389
CACertEP uid=caroot,dc=systest,dc=com
ResponderCertDir 10.2.11.1:389
ResponderCertEP cn=OCSP,ou=PKI,ou=Engineering,o=ExampleInc,c=US
ResponderCertAttr cacertificate
ResponderLocation http://10.12.2.4:389
AIAExtension NO
HttpProxyEnabled YES
HttpProxyLocation http://10.11.2.5:80
HttpProxyUserName proxyuser1
HttpProxyPassword letmein
SignRequestEnabled YES
SignDigest SHA256
Alias defaultenterpriseprivatekey
IgnoreNonceExtension NO
PrimaryValidationMethod OCSP
EnableFailover YES
ResponderCertAlias cert1
ResponderGracePeriod 0
]
```

SMocsp.conf 파일을 수정하기 위한 지침은 다음과 같습니다.

- 설정의 이름은 대/소문자가 구분되지 않는 경우도 있습니다. 항목의 대/소문자 구분 여부는 특정한 설정에 따라 다릅니다.
- 파일의 설정이 비어 있으면 정책 서버에서 오류 메시지를 보냅니다. 이 메시지는 항목이 올바르게 않음을 나타냅니다. 정책 서버는 이 설정을 무시합니다. 설정을 비워 두려면 메시지를 무시하십시오.
- 설정 이름 앞에 공백을 두지 마십시오.

파일의 설정은 다음과 같습니다.

OCSPResponder

필수입니다. 항목이 OCSP 응답자 레코드를 나타냅니다. 각 OCSP 응답자 레코드는 OCSPResponder 라는 이름으로 시작해야 합니다.

IssuerDN

필수입니다. 인증서 발급자의 DN 을 지정합니다. 이 값은 파일의 각 OCSP 응답자 레코드에 레이블을 지정합니다.

항목: 인증서의 발급자 DN 값입니다.

AlternateIssuerDN

선택 사항입니다. 보조 IssuerDN 또는 리버스 DN 을 지정합니다.

CACertDir

필수입니다. 사용자 인증서를 발급하는 CA 인증서가 저장된 CA 인증서 디렉터리의 이름을 지정합니다.

이 디렉터리를 관리 UI 에서 SiteMinder 사용자 디렉터리로 구성하여 정책 서버가 이 디렉터리에 연결할 수 있도록 해야 합니다.

사용자 디렉터리의 올바른 IP 주소 및 포트 번호를 입력합니다.

CACertEP

필수입니다. CA 인증서가 있는 CA 인증서 디렉터리의 진입점을 지정합니다.

인증서 디렉터리의 진입점을 나타내는 문자열을 입력합니다.

ResponderCertDir

필수입니다. 응답자 인증서가 저장된 LDAP 디렉터리를 지정합니다.

이 디렉터리를 관리 UI 에서 SiteMinder 사용자 디렉터리로 구성하여 정책 서버가 이 디렉터리에 연결할 수 있도록 해야 합니다.

디렉터리의 올바른 IP 주소 및 포트 번호를 입력합니다.

ResponderCertEP

필수입니다. 응답자 인증서가 있는 LDAP 디렉터리의 진입점을 지정합니다. 응답자 인증서 디렉터리는 ResponderCertDir 설정에서 지정합니다.

서명 유효성 검사 인증서는 응답 서명 또는 중간 인증서 모음을 직접 확인하는 인증서입니다.

OCSP 응답자에는 서명 유효성 검사 인증서와 응답이 포함될 수 있습니다. 이 경우 정책 서버는 LDAP 디렉터리의 트러스트된 인증서를 사용하여 응답 서명 및 인증서를 확인합니다. 서명 유효성 검사 인증서가 응답에 없는 경우 정책 서버는 LDAP 디렉터리의 인증서 또는 인증서 모음을 사용하여 응답 서명만 확인합니다.

인증서 또는 인증서 모음이 있는 디렉터리의 진입점을 나타내는 문자열을 입력하십시오.

ResponderCertAttr

필수입니다. 정책 서버가 ResponderCertDir 설정에 지정된 응답자 인증서 디렉터리에서 응답자 인증서를 조회하기 위해 사용하는 LDAP 디렉터리 특성을 나타냅니다.

ResponderLocation

선택 사항입니다. OCSP 응답자 서버의 위치를 나타냅니다.

ResponderLocation 설정 또는 AIAExtension 설정을 사용할 수 있지만 다음 사항에 유의하십시오.

- ResponderLocation 설정이 비어 있거나 SMocsp.conf 파일에 없는 경우에는 AIAExtension 설정을 YES 로 설정하십시오. 또한 AIA 확장이 인증서에 있어야 합니다.
- ResponderLocation 설정에 값이 있고 AIAExtension 이 YES 로 설정된 경우 정책 서버는 유효성 검사에 ResponderLocation 을 사용합니다. ResponderLocation 설정은 AIAExtension 보다 우선 순위가 높습니다.
- 이 설정에 대해 지정된 OCSP 응답자가 중지되고 AIAExtension 이 YES 로 설정된 경우에는 인증이 실패합니다. 정책 서버는 인증서의 AIA 확장에 지정된 응답자를 시도하지 않습니다.

위치를 입력하는 경우 값을 *responder_server_url:port_number* 의 형식으로 입력하십시오.

응답자 서버의 URL 및 포트 번호를 입력하십시오.

AIAExtension

선택 사항입니다. 정책 서버가 유효성 검사 정보를 찾기 위해 인증서의 AIA(Authority Information Access) 확장을 사용하는지 여부를 지정합니다.

AIAExtension 또는 ResponderLocation 설정을 사용할 수 있으며 다음 사항에 유의하십시오.

- AIAExtension 이 YES 로 설정되고 ResponderLocation 이 구성되지 않은 경우 정책 서버는 인증서의 AIA 확장을 유효성 검사에 사용합니다. 확장은 인증서에 있어야 합니다.
- AIAExtension 이 YES 로 설정되고 ResponderLocation 에 값이 있는 경우 정책 서버는 ResponderLocation 을 유효성 검사에 사용합니다. ResponderLocation 설정은 AIAExtension 보다 우선 순위가 높습니다.
- AIAExtension 이 NO 로 설정된 경우 정책 서버는 ResponderLocation 설정을 사용합니다. 정책 서버는 AIA 확장이 있는 경우 이를 무시합니다.

YES 또는 NO 를 입력하십시오.

기본값: NO

HttpProxyEnabled

선택 사항입니다. OCSP 요청을 웹 서버가 아니라 프록시 서버로 전송하도록 정책 서버에 지시합니다.

YES 또는 NO 를 입력하십시오.

기본값: NO

HttpProxyLocation

선택 사항입니다. 프록시 서버의 URL 을 지정합니다. 이 값은 HttpProxyEnabled 가 YES 로 설정된 경우에만 필요합니다.

http://로 시작하는 URL 을 입력하십시오.

참고: https://로 시작하는 URL 을 입력하지 마십시오.

HttpProxyUserName

선택 사항입니다. 프록시 서버에 대한 로그인 자격 증명의 사용자 이름을 지정합니다. 이 사용자 이름은 유효한 프록시 서버 사용자의 이름이어야 합니다. 이 값은 HttpProxyEnabled 가 YES 로 설정된 경우에만 필요합니다.

영숫자 문자열을 입력하십시오.

HttpProxyPassword

선택 사항입니다. 프록시 서버 사용자 이름의 암호를 지정합니다. 이 값은 일반 텍스트로 표시됩니다. 이 값은 HttpProxyEnabled 가 YES 로 설정된 경우에만 필요합니다.

영숫자 문자열을 입력하십시오.

SignRequestEnabled

선택 사항입니다. 정책 서버에 생성된 OCSP 요청에 서명하도록 지시합니다. 서명 기능을 사용하려면 이 값을 Yes 로 설정하십시오.

이 값은 사용자 인증서 서명과 별개이며 OCSP 요청에만 사용됩니다.

참고: 이 설정은 OCSP 응답자가 서명된 요청을 요구하는 경우에만 필요합니다.

YES 또는 NO 를 입력하십시오.

기본값: NO

SignDigest

선택 사항입니다. 정책 서버가 OCSP 요청에 서명할 때 사용하는 알고리즘을 지정합니다. 이 설정은 대/소문자를 구분하지 않습니다. 이 설정은 SignRequestEnabled 설정을 YES 로 설정한 경우에만 필요합니다.

다음 옵션 중 하나를 입력하십시오. SHA1, SHA224, SHA256, SHA384, SHA512

기본값: SHA1

별칭

선택 사항입니다. OCSP 응답자에 전송되는 OCSP 요청에 서명하는 키/인증서 쌍의 별칭을 지정합니다. 이 키/인증서 쌍은 SiteMinder 인증서 데이터 저장소에 있어야 합니다.

참고: 별칭은 SignRequestEnabled 설정을 YES 로 설정한 경우에만 필요합니다.

소문자 ASCII 영숫자 문자를 사용하여 별칭을 입력하십시오.

IgnoreNonceExtension

선택 사항입니다. OCSP 요청에 nonce 를 포함하지 않도록 정책 서버에 지시합니다. nonce(한 번 사용되는 숫자)는 응답이 재사용되는 것을 방지하기 위해 인증 요청에 가끔 포함되는 고유한 숫자입니다. 이 매개 변수를 Yes 로 설정하면 정책 서버는 OCSP 요청에 nonce 를 포함하지 않습니다.

YES 또는 NO 를 입력하십시오.

기본값: NO

PrimaryValidationMethod

선택 사항입니다. 정책 서버가 인증서의 유효성을 검사하기 위해 사용할 기본 방법을 OCSP 또는 CRL 중에서 지정합니다. 이 설정은 EnableFailover 설정을 Yes 로 설정한 경우에만 필요합니다.

OCSP 또는 CRL 을 입력하십시오.

기본값: OCSP

EnableFailover

OCSP 및 CRL 인증서 유효성 검사 방법 간에 장애 조치를 수행하도록 정책 서버에 지정합니다.

YES 또는 NO 를 입력하십시오.

기본값: NO

ResponderCertAlias

(페더레이션에만 필요). OCSP 응답의 서명을 확인하는 인증서의 별칭 이름을 지정합니다. 정책 서버가 응답 서명 유효성 검사를 수행하도록 하려면 이 설정에 대한 별칭을 지정하십시오. 그렇게 하지 않으면 CA 발급자가 사용할 수 있는 OCSP 구성이 없습니다.

참고: 정책 서버는 X.509 인증서 인증에 이 설정을 사용하지 않습니다.

별칭 이름을 지정하는 문자열을 입력하십시오.

SMocsp.conf 파일이 로드된 후 각 발급자에게 OCSP 구성이 있는지 여부를 확인할 수 있습니다. 다음은 샘플 상태 메시지입니다.

SMocsp.conf 파일이 로드되었습니다.

다음 발급자 별칭에 대해 OCSP 구성이 추가되었습니다:

```
ocspcacert  
ocspcacert1  
ocspcacert2
```

상태 메시지의 발급자 별칭은 데이터 저장소에 CA 인증서를 추가할 때 관리 UI에서 지정한 별칭을 가리킵니다. 발급자 별칭이 목록에 없으면 SMocsp.conf 및 cds.log 파일을 확인하십시오. 로그 파일은 *siteminder_home\log*에 있습니다.

RevocationGracePeriod

(선택 사항) 인증서 해지 후 무효화를 지연할 기간(일)을 지정합니다. OCSP 유예 기간은 구성이 갑자기 중지되지 않도록 사용자에게 인증서를 업데이트할 시간을 부여합니다. 값이 0이면 인증서가 해지될 때 즉시 무효화됩니다.

이 필드에 값을 지정하지 않으면 정책 서버는 관리 UI의 기본 해지 유예 기간 설정을 사용합니다. "인프라" > "X509 인증서 관리" > "인증서 관리"로 이동하여 기본 설정을 확인할 수 있습니다.

기본값: 0

OCSP 검사 구성

사용자가 유효하지 않은 클라이언트 인증서로 보호된 리소스에 액세스할 수 없도록 OCSP 검사를 구성하십시오.

참고: OCSP 검사가 사용되도록 설정하기 전에 사용 환경에 [인증서 인증](#) (페이지 389)을 설정하십시오.

정책 서버는 SHA-1 및 SHA-2 알고리즘 제품군(SHA224, SHA256, SHA384, SHA512)을 사용하여 서명된 OCSP 응답을 지원합니다.

장애 조치가 사용되지 않는 경우 OCSP 검사를 구성하려면

1. `policy_server_home/config` 로 이동합니다.

샘플 파일 `SMocsp.Sample.conf` 는 정책 서버와 함께 `config` 디렉터리에 설치됩니다.

2. 샘플 구성 파일을 복사하고 이름을 `SMocsp.conf` 로 지정합니다.

UNIX 플랫폼에서는 파일 이름의 대/소문자가 구분되지만 Windows 플랫폼에서는 그렇지 않습니다.

3. 텍스트 편집기에서 파일을 엽니다.

4. 인증서 매핑에 지정된 IssuerDN 과 일치하는 각 IssuerDN 에 대해 고유 OCSPResponder 항목을 이 파일에 추가합니다.

중요! 각 발급자 DN 에 대해 응답자 레코드를 구성하지 않을 경우 정책 서버는 인증서의 유효성을 확인하지 않고 사용자를 인증합니다.

5. 파일을 저장합니다.

6. 정책 서버를 다시 시작합니다.

7. 관리 UI 에 로그인합니다.

8. "인프라", "디렉터리"를 차례로 선택합니다.

9. "인증서 매핑" 옵션을 확장합니다.

10. "인증서 매핑 만들기" 또는 "인증서 매핑 수정"을 선택합니다.

"인증서 매핑" 대화 상자가 열립니다.

11. 유효성 검사 방법으로 OCSP 만 사용하려는 경우 "CRL 검사 수행" 확인란의 선택을 취소합니다. 장애 조치를 사용하려는 경우에는 CRL 검사 기능을 사용해야 합니다.

사용자 인증서의 발급자가 인증서 매핑과 일치하고 CRL 검사 기능이 사용되는 경우 정책 서버는 OCSP 가 아니라 CRL 검사를 사용합니다. 장애 조치가 사용되도록 설정할 경우에는 예외적으로 CRL 검사가 OCSP 보다 우선하지 않을 수 있습니다. [장애 조치가 사용될](#) (페이지 469) 경우 정책 서버는 구성된 기본 유효성 검사 방법을 사용합니다.

12. 변경 내용을 저장한 다음 관리 UI 를 종료합니다.

13. (선택 사항) 정책 서버가 OCSP 요청에 서명하도록 구성합니다.

이제 OCSP 가 사용되도록 설정되었습니다. OCSP 가 사용되지 않도록 설정하려면 `SMocsp.conf` 파일의 이름을 변경하십시오.

HTTP 프록시를 통해 OCSP 응답자에 액세스

OCSP 요청은 HTTP 연결을 통해 이루어지며, 인증서 유효성 검사를 위해 OCSP 응답자에 요청하려면 HTTP GET 이 필요합니다.

많은 엔터프라이즈 환경에서 HTTP 트래픽은 HTTP 프록시를 거칩니다. 정책 서버가 HTTP 프록시를 통해 OCSP 요청을 보내도록 하려면 `SMocsp.conf` 파일에서 프록시 설정을 구성하십시오.

다음 단계를 수행하십시오.

1. 기존 `SMocsp.conf` 파일을 편집하거나 정책 서버 `config` 디렉터리 `policy_server_home/config` 에 이 파일을 생성합니다.
2. 다음과 같이 설정을 편집합니다.

- `HttpProxyEnabled YES`
- `HttpProxyLocation proxy_server_URL`
- `HttpProxyUserName user_login_name`
- `HttpProxyPassword password_for_login`

각 값을 설정하는 방법을 알아보려면 OCSP 구성 파일 생성 방법을 검토하십시오.

3. 정책 서버를 다시 시작합니다.

OCSP 요청 서명을 위한 사전 요구 사항 구성(선택 사항)

정책 서버는 SiteMinder 인증서 인증 체계를 사용할 때 OCSP 요청에 서명할 수 있습니다. 요청 서명은 OCSP 응답자가 서명된 요청서를 요구할 경우에만 필요합니다.

다음 단계를 수행하십시오.

OCSP 서명을 구성하기 전에 다음 사전 요구 사항 태스크를 완료하십시오.

1. [OCSP 검사](#) (페이지 456)를 구성합니다.
2. 요청에 서명하는 키/인증서 쌍을 인증서 데이터 저장소에 추가합니다. 관리 UI 를 사용하여 이 태스크를 수행합니다.

키/인증서 쌍을 추가할 때 별칭을 지정합니다. 정책 서버는 별칭을 사용하여 인증서 데이터 저장소의 인증서 항목을 식별합니다. 별칭을 지정할 때 다음 제한 사항에 주의하십시오.

- 인증서를 단일 별칭으로 한 번만 저장하십시오. 동일한 인증서를 다른 별칭으로 저장하려고 하면 실패합니다. 여러 응답자가 동일한 서명 인증서를 사용하는 경우 동일한 별칭을 사용하십시오.
- 지정하는 별칭 값은 `SMocsp.conf` 파일의 별칭 설정 값과 일치해야 합니다.
- 인증서 별칭의 이름에는 제한이 없지만 첫 번째 별칭은 `defaultenterpriseprivatekey` 여야 합니다.
- 별칭은 다음 조건을 충족해야 합니다.
 - 모두 소문자 USA ASCII 여야 합니다.
 - 영숫자 문자를 사용해야 합니다.

참고: 개인 키는 RSA 키여야 합니다.

OCSP 요청 서명 구성

정책 서버는 SiteMinder 인증서 인증 체계를 사용할 때 요청에 서명하고 응답을 확인할 수 있습니다.

다음 단계를 수행하십시오.

1. `SMocsp.conf` 파일을 편집기에서 엽니다. 이 파일은 `policy_server_home/config` 디렉터리에 있습니다.
2. `SMocsp.conf` 파일에 각 응답자에 대한 다음 항목을 추가합니다.

SignRequestEnabled

정책 서버에 OCSP 요청에 서명하도록 지시합니다.

제한: Yes 또는 No

서명 기능을 사용하려면 이 값을 Yes 로 설정하십시오.

서명 기능이 사용되지 않도록 설정하려면 기본값인 No 를 그대로 두십시오.

기본값: No - 응답자 레코드에 `SignRequestEnabled` 항목이 없는 경우 정책 서버가 OCSP 요청에 서명할 수 없습니다.

SignDigest

OCSP 요청에 서명하는 데 사용할 알고리즘을 나타냅니다.

옵션:

- SHA1
- SHA224
- SHA256
- SHA384
- SHA512

SignDigest 는 대/소문자를 구분하지 않습니다.

기본값: SHA1

별칭

정책 서버가 서명 키/인증서 쌍을 검색할 별칭을 나타냅니다.
별칭에는 소문자 USA ASCII 영숫자만 사용할 수 있습니다.

3. SMocsp.conf 파일을 저장합니다.
4. 정책 서버를 다시 시작합니다.

이제 OCSP 요청에 대한 서명 기능이 사용됩니다.

OCSP 와 CRL 간의 장애 조치

정책 서버는 인증서 유효성 검사 메커니즘으로 OCSP 와 CRL 을 사용할 수 있습니다. 두 메커니즘을 모두 구성할 경우 정책 서버가 두 메커니즘 간에 장애 조치 기능을 사용하도록 구성할 수 있습니다. 장애 조치 기능을 사용하면 두 인증서 유효성 검사 메커니즘 중 하나를 사용할 수 없게 되더라도 인증에 실패하지 않으므로 유용합니다.

인증서 검사에 대한 장애 조치를 구현하려면 OCSP 구성 파일(SMocsp.conf)에서 기본 유효성 검사 방법을 지정하십시오. 기본 유효성 검사 방법을 사용할 수 없는 경우 정책 서버는 보조 유효성 검사 방법을 사용하여 요청을 완료합니다. 다음 요청에서는 정책 서버가 기본 방법으로 돌아가고, 오류가 발생하지 않는 한 이 방법을 사용합니다.

OCSP 를 기본 유효성 검사 방법으로 구성할 경우

기본 방법이 OCSP 인데 OCSP 응답자를 사용할 수 없으면 정책 서버는 대신 CRL 을 사용하여 인증서 유효성 검사를 수행합니다.

OCSP 응답자가 양호 또는 해지됨 응답 표시기를 반환하는 한 장애 조치가 OCSP 기능보다 우선하지 않습니다. 응답 표시기가 "알 수 없음"인 경우에는 CRL 검사로 장애 조치됩니다.

OCSP 을 기본 유효성 검사 방법으로 구성할 경우 정책 서버 동작은 다음과 같습니다.

OCSP 인증서 유효성 검사	장애 조치 사용 안 함	장애 조치 사용
유효	사용자 인증됨	사용자 인증이 OCSP 결과만을 기반으로 합니다. CRL 검사는 필요하지 않습니다.
해지됨	사용자가 인증되지 않음	사용자가 인증되지 않습니다. CRL 검사는 필요하지 않습니다.
알 수 없음 또는 응답 없음	사용자가 인증되지 않음	CRL 검사가 수행됩니다.

CRL 검사를 기본 유효성 검사 방법으로 구성할 경우

기본 방법이 CRL 검사인데 CRL 을 검색할 수 없으면 정책 서버는 OCSP 응답자로 장애 조치합니다. 이 경우 CRL 디렉터리 서버에 대한 연결을 사용할 수 없으면 정책 서버는 OCSP 만 사용합니다. CRL 이 유효 응답을 반환할 경우 정책 서버는 OCSP 를 사용하지 않습니다.

참고: 장애 조치가 사용되지 않고 CRL 검사와 OCSP 가 모두 구성된 경우 정책 서버는 인증서 유효성 검사에 CRL 검사만 사용합니다.

CRL 을 기본 유효성 검사 방법으로 구성할 경우 정책 서버 동작은 다음과 같습니다.

CRL 인증서 유효성 검사	장애 조치 사용 안 함	장애 조치 사용
유효	사용자 인증됨	검사가 첫 번째로 유효한 CRL 결과를 기반으로 합니다. 추가 CRL 검사가 필요하지 않습니다.
해지됨	사용자가 인증되지 않음	추가 CRL 또는 OCSP 검사가 필요하지 않습니다.
응답 없음/검색 실패	CDP 확장을 사용할 수 있는 경우 정책 서버는 CRL 을 성공적으로 검색할 때까지 각 배포 지점을 순차적으로 시도합니다. 인증서가 유효 또는 해지됨 상태인 경우에는 해당 상태에 대한 설명을 참조하십시오. 모든 사유 코드가 포함된 CRL 이 검색되지 않을 경우 정책 서버는 기본적으로 사용자를 인증하지 않습니다.	CDP 확장을 사용할 수 있는 경우 정책 서버는 CRL 을 성공적으로 검색할 때까지 각 배포 지점을 순차적으로 시도합니다. 인증서가 유효 또는 해지됨 상태인 경우에는 해당 상태에 대한 설명을 참조하십시오. 모든 사유 코드가 포함된 CRL 이 검색되지 않을 경우 OCSP 가 사용됩니다.

OCSP 와 CRL 간의 장애 조치 구성

정책 서버는 인증서 유효성 검사 메커니즘으로 OCSP 와 CRL 을 모두 사용할 수 있으며 이 둘 간의 장애 조치 기능이 사용되도록 설정할 수 있습니다. 장애 조치 기능이 사용되도록 설정하기 전에 관리 UI 에서 CRL 검사를 구성하고 SMocsp.conf 파일을 생성하여 OCSP 를 구성하십시오. 장애 조치가 작동하기 위해서는 CRL 검사와 OCSP 검사가 사용되도록 설정해야 합니다.

다음 단계를 수행하십시오.

1. SMocsp.conf 파일을 편집기에서 엽니다. 이 파일은 `policy_server_home/config` 디렉터리에 있습니다.
2. 각 응답자 레코드에 대해 다음 항목을 추가하거나 수정합니다.

EnableFailover

SiteMinder 가 기본 유효성 검사 방법에서 보조 방법으로 장애 조치되도록 설정합니다.

장애 조치를 사용하려면 이 값을 Yes 로 설정하십시오.

장애 조치가 사용되지 않도록 설정하려면 기본값인 No 를 그대로 두십시오. 장애 조치를 구성하지 않을 경우 OCSP 응답자가 유효성 검사를 수행할 수 없으면 트랜잭션이 실패합니다.

제한: YES 또는 NO

기본값: No

PrimaryValidationMethod

정책 서버가 다른 방법을 시도하기 전에 먼저 사용할 인증서 유효성 검사 방법을 나타냅니다.

EnableFailover 가 YES 로 설정되고 이 설정의 값이 OCSP 인 경우 정책 서버는 OCSP 유효성 검사를 먼저 사용합니다. OCSP 응답자에서 응답이 없거나 응답 표시기가 "알 수 없음"이면 정책 서버는 CRL 로 장애 조치합니다.

이 설정 값이 CRL 이면 정책 서버는 OCSP 유효성 검사가 구성되어 있더라도 이를 무시하고 CRL 을 사용합니다. CRL 을 가져올 수 없거나 CRL 이 만료되었으면 정책 서버는 OCSP 로 장애 조치합니다.

제한: OCSP, CRL

기본값: OCSP

3. 변경 내용을 SMocsp.conf 파일에 저장합니다.
4. 정책 서버를 다시 시작합니다.

인증서 유효성 검사 문제 해결

상세 추적 로깅을 사용하면 X.509 인증서 인증과 유효성 검사의 문제를 손쉽게 해결할 수 있습니다.

일반적인 OCSP 및 CRL 메시지에 추가하여, 정책 서버는 또한 장애 조치 이벤트에 대한 정보도 로깅합니다. 장애 조치 이벤트가 발생할 경우 정책 서버는 인증서 유효성 검사 오류와 관련된 진단 메시지와 장애 조치를 설명하는 메시지를 로깅합니다. 이 메시지는 OCSP에 연결할 수 없어 현재 CRL을 사용 중임을 나타내거나, CRL을 가져오기 못해 정책 서버가 OCSP 검사로 장애 조치되었음을 나타낼 수 있습니다.

OCSP 및 CRL 로그 메시지를 보려면 정책 서버 관리 콘솔에서 "프로파일러"를 사용하여 인증 추적 로깅이 사용되도록 설정하십시오.

기본 템플릿 파일인 `smtracedefault.txt`를 수정하여 정책 서버가 추적 로깅에 포함할 구성 요소 및 데이터 필드를 결정할 수 있습니다.

다음 `smtracedefault.txt` 파일에는 추적 로그에서 인증서 유효성 검사를 진단하기 위해 파일에 포함하는 것이 좋은 몇 가지 구성 요소가 나와 있습니다.

components: Login_Logout/Authentication, Login_Logout/Certificates, Login_Logout/Receive_Request, IsAuthorized/Policy_Evaluation, IsAuthorized/Receive_Request, Directory_Access, LDAP/Ldap_Error_Messages

data: Date, PreciseTime, SrcFile, Function, ReturnValue, Message, User, Directory, SearchKey, ErrorString, ErrorValue, AuthStatus, AuthReason, CertSerial, SubjectDN, IssuerDN, CertDistPt, UserDN, Data, HexadecimalData, CallDetail, Returns, Result

OCSP 서명의 경우에만 서명 유효성을 검사할 때 추적 메시지가 사용되도록 설정할 수 있습니다.

OCSP 서명에 대한 추적을 활성화하려면:

1. `policy_server_home/config`로 이동합니다.
`policy_server_home`은 정책 서버를 설치한 디렉터리입니다.
2. 텍스트 편집기에서 `JVMOptions` 파일을 엽니다.
3. `-DOCSP_PS_TRACE` 설정을 추가하고 해당 값을 다음과 같이 `true`로 설정합니다.
`-DOCSP_PS_TRACE=true`

4. 파일을 저장합니다.
5. 정책 서버를 다시 시작합니다.

OcspCertKeyRetriever.log 라는 추적 파일이 다음과 같은 정책 서버의 현재 작업 디렉터리에 기록됩니다.

Windows: system32

Unix: siteminder 또는 siteminder/bin

제 10 장: 강력한 인증

이 섹션은 다음 항목을 포함하고 있습니다.

[자격 증명 선택기 소개](#) (페이지 475)

[자격 증명 선택기 사용 사례](#) (페이지 476)

[사용 사례에 대한 자격 증명 선택기 솔루션](#) (페이지 479)

[프론트엔드 인증 체계 설정](#) (페이지 479)

[성공하지 못한 인증 시도 관리](#) (페이지 489)

[백엔드 처리 설정](#) (페이지 490)

[샘플 응용 프로그램 보호](#) (페이지 497)

[자격 증명 선택기 솔루션 테스트](#) (페이지 503)

자격 증명 선택기 소개

자격 증명 선택기는 강력한 인증 솔루션입니다. 사용자는 자격 증명 선택기를 사용하여 보호된 리소스에 액세스하는 데 필요한 인증 자격 증명의 유형을 선택할 수 있습니다. 정책 서버는 사용자 인증 컨텍스트를 기반으로 권한 부여를 결정한 다음 동일한 싱글 사인온 환경에서 사용자 응답을 생성할 수 있습니다.

자격 증명 선택기 기능은 SiteMinder 로 보호되는 임의의 응용 프로그램이 사용할 수 있는 독립 실행형 구성 요소로 구현됩니다.

자격 증명 선택기 사용 사례

이 사용 사례에서 사용자는 보호된 리소스에 대한 액세스 권한을 요청할 때 다양한 자격 증명을 선택하여 각기 다른 수준의 액세스 권한을 얻을 수 있습니다. 사용자가 보호되는 샘플 응용 프로그램을 요청하면 다음과 같은 로그인 대화 상자가 표시됩니다.

Password And/Or Certificate Username: Password: ☐ Use an X.509 client certificate Login	SecurID Authentication Username: SecurID PIN: Login
Windows Authentication Login	SafeWord Authentication Username: Login

각 대화 상자의 로그인 단추를 누르면 각기 다른 자격 증명이 제출됩니다. 사용자의 환경은 사용자가 제공하는 자격 증명의 유형에 따라 달라집니다. 사용자는 다음 인증 유형 중 하나를 선택할 수 있습니다.

- 암호 및/또는 인증서 인증
- Windows 인증
- SecureID 인증
- SafeWord 인증

성공적으로 인증되고 권한이 부여된 사용자는 샘플 응용 프로그램에 액세스할 수 있으며 이때 응용 프로그램에는 사용자가 로그인하는 데 사용한 인증 체계의 유형과 인증 수준을 알려 주는 인사말이 표시됩니다.

추가 정보

[암호 및/또는 인증서 인증을 사용한 액세스 요청](#) (페이지 477)

[SafeWord 인증을 사용한 액세스 요청](#) (페이지 478)

[SecurID 인증을 사용한 액세스 요청](#) (페이지 478)

[Windows 인증을 사용한 액세스 요청](#) (페이지 478)

암호 및/또는 인증서 인증을 사용한 액세스 요청

로그인 대화 상자의 "Password And/Or Certificate"(암호 및/또는 인증서) 섹션에서 사용자는 다음 자격 증명 조합 중 하나를 선택할 수 있습니다.

- HTML 양식에 입력된 사용자 이름과 암호만
- X.509 클라이언트 인증서만
- 사용자 이름/암호와 X.509 클라이언트 인증서

사용자가 올바른 사용자 이름 및 암호만 제공할 경우 다음 메시지가 표시됩니다.

```
Greetings, SampleUser!
Your authentication level is 5
You have used username/password authentication
```

사용자가 "X.509 client certificate"(X.509 클라이언트 인증서) 확인란만 선택할 경우 브라우저에 구성된 클라이언트 인증서 중 하나를 선택하라는 메시지가 표시됩니다. 정책 서버가 인증서를 인식하면 다음 메시지가 표시됩니다.

```
Greetings, SampleUser!
Your authentication level is 10.
You have used X.509 client certificate authentication
```

"Password And/Or Certificate"(암호 및/또는 인증서) 옵션을 사용할 경우 사용자가 제공하는 자격 증명에 따라 다양한 수준의 인증 수준이 제공됩니다. 암호 및/또는 인증서 옵션과 유사할 수 있는 X.509 인증서 또는 양식 인증 체계는 사용자가 제공하는 인증서의 유형을 구분하지 않습니다. 따라서 사용자가 제공하는 자격 증명에 상관없이 보호 수준은 동일합니다.

사용자 이름과 암호가 모두 제공되고 "X.509 client certificate"(X.509 클라이언트 인증서) 확인란이 선택된 경우 사용자에게 클라이언트 인증서를 요구하는 메시지가 표시됩니다. 정책 서버가 인증서를 인식하고 인증서가 사용자가 제공하는 사용자 이름과 일치하는 경우 다음과 같은 메시지가 표시됩니다.

```
Greetings, SampleUser!
Your authentication level is 15
You have used X.509 client certificate and username/password authentication
```

Windows 인증을 사용한 액세스 요청

사용자가 보호된 리소스를 요청할 때 Windows 도메인에 로그인되어 있는 경우 다음과 같은 메시지가 표시됩니다.

```
Greetings, SampleUser!  
Your authentication level is 5  
You have used the Windows domain authentication
```

사용자가 Windows 도메인에 로그인되어 있지 않은 경우에는 Windows 도메인 자격 증명을 요구하는 메시지가 표시됩니다.

SecurID 인증을 사용한 액세스 요청

사용자가 보호된 리소스를 요청할 때 SecurID 인증을 위한 올바른 사용자 이름과 SecurID PIN 을 제공하는 경우 다음과 같은 메시지가 표시됩니다.

```
Greetings, SampleUser!  
Your authentication level is 20  
You have used the SecurID authentication
```

SafeWord 인증을 사용한 액세스 요청

사용자가 SafeWord 인증을 위해 사용자 이름만 제공한 경우 2 단계 프로세스가 수행됩니다. 즉, SiteMinder 가 사용자 이름을 SafeWord 서버에 전달하고 서버는 사용자 인증 요청에 사용할 자격 증명을 확인합니다. SafeWord 는 로그인당 최대 네 개의 인증자를 지원합니다. 인증자는 암호를 사용하는 고정 인증자이거나 토큰 카드 핀을 사용하는 동적 인증자일 수 있습니다.

액세스에 성공할 경우 다음 메시지가 표시됩니다.

```
Greetings, SampleUser!  
Your authentication level is 20  
You have used the SafeWord authentication
```

사용 사례에 대한 자격 증명 선택기 솔루션

이 사용 사례에 대한 자격 증명 선택기를 설정하려면 다음 구성 요소를 구성하십시오.

- 프론트엔드 인증 체계에서 사용자가 보호된 샘플 응용 프로그램을 요청할 때 표시되는 로그인 대화 상자를 렌더링하는 데 사용되는 FCC(양식 자격 증명 수집기). `selectlogin.fcc` 라고 하는 샘플 FCC 는 웹 에이전트를 설치할 때 함께 설치됩니다.
- 관리 UI 에서 구성
 - 자격 증명 선택기를 사용할 응용 프로그램에 노출되는 프론트엔드 인증 체계
 - 사용자가 선택할 수 있는 각 자격 증명 유형에 대한 여러 백엔드 인증 체계. 백엔드 처리란 자격 증명 선택기와 상호 작용하는 기능만을 나타냅니다. 최종 사용자는 이러한 기능에 대해 알지 못합니다.
 - 자격 증명 선택기의 백엔드 처리를 나타내는 영역, 규칙, 응답 및 정책을 포함하는 특수하게 구성된 정책 도메인
- 백엔드 처리를 나타내는 정책 도메인에 대해 진입점의 역할을 하는 웹 에이전트
- 프론트엔드 인증 체계를 사용하는 샘플 응용 프로그램. 이 사용 사례의 경우 샘플 응용 프로그램은 사용자에게 인사말 메시지를 표시합니다. 이 메시지는 사용자가 로그인할 때 선택하는 자격 증명에 따라 달라집니다.

프론트엔드 인증 체계 설정

프론트엔드 인증 체계는 양식 자격 증명 수집기(FCC)인 `selectlogin.fcc` 를 사용하여 보호된 리소스에 대한 액세스를 요청하는 데 사용되는 로그인 선택 화면을 생성합니다. FCC 는 에이전트에 대한 FCC 지시문을 동적으로 구성하므로 에이전트가 인증 체계 선택 항목에 적절하게 사용자를 리디렉션할 수 있습니다.

참고: `selectlogin.fcc` 는 자격 증명 선택기가 사용하는 샘플입니다. 인증 선택 항목 및 HTML 서식 집합은 특성 상황에 따라 달라집니다.

FCC(양식 자격 증명 수집기) 사용

FCC 형식은 웹 에이전트가 자격 증명을 수집하여 정책 서버로 전달하는 데 사용하는 고유한 형식입니다. FCC 는 헤더와 본문으로 구성됩니다.

FCC 헤더 설명

FCC 헤더는 각 줄에 하나씩 있는 FCC 지시문의 목록입니다. FCC 지시문의 구문은 다음과 같습니다.

@<directive>[=<value>]

값에는 **%parameter%** 형식으로 지정되는 % 대체 항목이 포함될 수 있습니다. 매개 변수는 자격 증명이 제출될 때 POST 작업에서 FCC 파일과 함께 전달됩니다.

FCC 지시문의 집합은 제한됩니다. 이 예에서 가장 중요한 지시문은 다음과 같습니다.

@target

웹 에이전트가 정책 서버에 전달해야 하는 리소스 URL 입니다.

@username

웹 에이전트가 정책 서버에 전달해야 하는 사용자 이름입니다.

@password

웹 에이전트가 정책 서버에 전달해야 하는 암호입니다.

@smagentname

웹 에이전트가 정책 서버에 전달해야 하는 에이전트 이름입니다. 에이전트 구성에서 **EncryptAgentName** 매개 변수가 **yes** 로 설정된 경우 이 이름은 암호화됩니다.

모든 FCC 지시문이 헤더에 나열되어야 하는 것은 아닙니다. 많은 지시문에는 다음과 같이 암시적 기본값이 있습니다.

- @target=%target%
- @username=%username%
- @password=%password%
- @smagentname=%smagentname%

FCC 본문 설명

FCC 본문에는 HTML 이나 그 밖에 웹 브라우저가 읽을 수 있는 형식이 포함됩니다. FCC 본문은 사용자가 자격 증명을 제공할 때 웹 브라우저에 표시됩니다.

본문에는 `$$parameter$$` 형식의 대체 항목이 포함될 수 있습니다. 매개 변수 이름은 GET 작업에서 FCC 파일과 함께 전달되는 알려진 매개 변수 집합에 속해 있어야 합니다.

이 예에서 중요한 지시문은 다음과 같습니다.

`$$target$$`

사용자가 요청한 리소스 URL 입니다.

`$$smagentname$$`

에이전트 이름입니다. 에이전트 구성에서 `EncryptAgentName` 매개 변수가 `yes` 로 설정된 경우 이 이름은 암호화됩니다.

프런트엔드 인증을 위한 `selectlogin.fcc` 파일 구성

웹 에이전트를 설치한 경우 `selectlogin.fcc` 파일이 샘플 FCC 로 포함되어 있습니다. 프런트엔드 인증 체계는 `selectlogin.fcc` 파일을 사용하여 사용자가 보호된 리소스를 요청할 때 나타나는 로그인 대화 상자를 표시합니다.

사용자가 리소스를 요청하면 웹 에이전트는 요청된 URL 을 정책 서버에 전달합니다. 대부분의 경우 웹 에이전트가 전달하는 리소스 URL 은 사용자가 요청한 리소스 URL 과 동일합니다. 인증 체계에 대해 정의된 FCC 파일은 `$$target$$`(GET 매개 변수)을 `%target%(POST 매개 변수)`으로 전달하고 `@target=%target%` 지시문을 사용하여 요청된 URL 이 전달될 수 있도록 합니다. 예를 들면 다음과 같습니다.

```
<!-- some HTML code -->
<form name="Login" method="POST">
<!-- some HTML code -->
<input type="hidden" name="target" value="$$target$$">
<!-- more HTML code -->
</form>
<!-- more HTML code -->
```

참고: `@target=%target%` 지시문은 기본적으로 사용됩니다.

이 경우 `%target%` 매개 변수의 값을 다음 값으로 바꾸면 `selectlogin.fcc` 파일이 작동합니다.

```
/path/redirect.ext?authtype=type&target=$$target$$
```

redirect.ext

`target` 매개 변수에 제공된 URL 로 리디렉션되는 간단한 스크립트입니다. 예를 들어 `redirect.asp` 또는 `redirect.jsp` 와 같은 값을 사용합니다. 또는 리디렉션 스크립트의 URL 이 제공된 자격 증명에 의존하는 한 동일한 실제 파일을 노출하는 다른 가상 디렉터리나 다른 리디렉션 스크립트 파일을 사용할 수 있습니다.

type

사용자가 선택하는 자격 증명에 의해 결정되는 문자열입니다.

다른 인증 체계가 다른 리디렉션 URL 을 보호하는 경우 선택한 인증 체계는 FCC 가 수집하는 자격 증명을 처리합니다. 선택한 인증 체계는 사용자 인증 수준을 포함한 사용자 세션을 구성합니다. 리디렉션 스크립트 리소스에 대해 인증되고 권한이 부여된 사용자는 원래 요청한 리소스로 리디렉션됩니다.

참고: 싱글 사인온이 적용되고 사용자 보호 수준이 프론트엔드 인증 체계의 보호 수준보다 높거나 같은 경우 원래 리소스에 대해 사용자 세션의 유효성이 검사됩니다. 사용자에게 권한이 부여되는지 여부는 정책 구성에 따라 달라지며, 사용자의 인증 컨텍스트가 검사될 수 있습니다. 예를 들어 특정 리소스에 액세스하는 데 최소 보호 수준이나 특정 조건이 필요할 수 있습니다.

Selectlogin.fcc 구성 상세 정보

`selectlogin.fcc` 파일에서 다양한 인증 체계를 구성할 수 있습니다. 다음 목록은 일부 체계에 대한 구성 상세 정보를 보여 줍니다.

- 인증서 및 양식 체계에는 SSL 연결을 통한 포스트가 필요합니다. 프론트엔드 인증 체계가 SSL 연결을 사용하지 않는 경우 에이전트가 GET 요청이 획득한 것과 동일한 `selectlogin.fcc` URL 에 포스트할 수 없습니다.

다음 JavaScript 코드를 사용하여 URL 을 SSL URL 로 변환할 수 있습니다.

```
arr = document.URL.split("://");  
document.Login.action = "https://" + arr[1];
```

- SafeWord 2 단계 인증을 지원하려면 클라이언트 쪽에서 최초 챌린지 양식에서 수집된 사용자 이름을 두 번째 챌린지 때 기억해야 합니다. 에이전트 설치에도 포함되어 있는 `safeword.fcc` 파일은 `@smtransient` FCC 지시문을 사용하여 사용자 이름을 임시 쿠키에 보관합니다. 동일한 지시문을 `selectlogin.fcc` 파일에서 사용할 수도 있지만, 그러면 사용자가 다른 자격 증명을 선택할 경우에도 쿠키가 생성됩니다. 따라서 이 경우에는 다음과 같이 `safeword.fcc` 파일에 포스트하도록 `action` 인수를 수정하는 것이 좋습니다.

```
document.Login.action = "safeword.fcc";
```

- Windows 인증 체계는 FCC 파일을 사용하지 않습니다. Windows 인증 체계의 경우 웹 서버에는 없지만 에이전트가 인식하는 특정 의사 리소스(pseudo-resource) URL 을 사용합니다. Windows 인증이 작동하도록 하려면 다음과 같이 `action` 인수를 동일한 의사 리소스(pseudo-resource) URL 로 설정하십시오.

```
document.Login.action = "/siteminderagent/ntlm/creds.ntc";
```

- SecurID 인증 체계는 FCC 를 사용하지 않지만 에이전트가 SecurID 자격 증명을 `selectlogin.fcc` 파일에 직접 포스트할 수 있습니다. 따라서 `action` 인수를 수정할 필요가 없습니다.
- 작업 URL 은 다른 웹 서버에서 호스트할 수 있습니다. 하지만 SiteMinder 관련 리소스 URL(FCC, SCC, NTC)이 인식되고 올바르게 처리되도록 이 다른 웹 서버 또한 에이전트로 보호되어야 합니다.

참고: SCC 의사 리소스(pseudo-resource) URL 은 인증서 전용 인증에 사용됩니다.

샘플 selectlogin.fcc 파일

아래에는 HTML 서식이 없는 간단한 `selectlogin.fcc` 파일이 나옵니다. `smquerydata` 및 `postpreservationdata` 에 대한 숨겨진 입력 필드는 각각 GET 및 POST 매개 변수를 전달하는 데 필요합니다.

`smauthreason` 매개 변수는 정책 서버가 인증 챌린지와 함께 제공하는 사유 코드를 보관합니다.

샘플 selectlogin.fcc 파일은 다음과 같습니다.

```
@username=%USER%
@smretries=0

<html>
<head>
  <script language="JavaScript">
    function submitForm(form)
    {
      authtype = "none";

      if (form == 1)
      {
        document.Login.USER.value      = document.Login.USER1.value;
        document.Login.PASSWORD.value = document.Login.PASSWORD1.value;

        if (!document.Login.UseCert.checked)
        {
          // username/password only
          authtype = "form";
        }
        else if (document.Login.USER.value == "" &&
                  document.Login.PASSWORD.value == "")
        {
          // certificate only
          authtype = "cert";
        }
        else
        {
          // username/password and certificate
          authtype = "certform";

          // This option requires posting over SSL.
          arr = document.URL.split("://");
          document.Login.action = "https://" + arr[1];
        }
      }
    }
  </script>
</head>
<body>
```



```
else if (form == 2)
{
    // SecurID authentication
    authtype = "securid";
    document.Login.USER.value = document.Login.USER2.value;
    document.Login.PASSWORD.value = document.Login.PASSWORD2.value;
}
else if (form == 3)
{
    // Safeword authentication
    authtype = "safeword";
    document.Login.USER.value = document.Login.USER3.value;
    document.Login.PASSWORD.value = "";

    // POST to safeword.fcc, for additional processing.
    // NOTE: This forces the web agent to POST to safeword.fcc
    // even if the authentication scheme's URL parameter
    // is set to selectlogin.fcc for redirection purposes.
    document.Login.action = "safeword.fcc";
}
else if (form == 4)
{
    // Authenticate with the current Windows login credentials
    authtype = "windows";
    document.Login.USER.value = "";
    document.Login.PASSWORD.value = "";

    // POST to creds.ntc (required by the Windows authentication scheme).
    document.Login.action = "/siteminderagent/ntlm/creds.ntc";
}
// Generate the target, depending on the user's choice of credentials.
// This sample uses redirect.asp, but it could also be redirect.jsp, redirect.pl,
etc.
// This sample uses the following format:
/auth/redirect.asp?authtype=<choice>&target=<original target>
// Other formats are also possible, e.g.:
/auth-<choice>/redirect.asp?target=<original
    target>
// The helper realms' resource filters must be defined accordingly (see the tech
note).
```

```
// Check if the target is not already in the same format. The user may
// have been redirected back to selectlogin.fcc upon authentication failure,
// if the authentication scheme's URL parameter is set to selectlogin.fcc.
if ("$$target$$.indexOf("/auth/redirect.asp?authtype=") == 0 &&
    "$$target$$.indexOf("&target=") > 0)
{
    // This must be a redirect. Extract the original target, but not
    // the authtype parameter, because the user may have made a different
    // choice of credentials this time.
    trgarr = "$$target$$.split("&target=");
    document.Login.target.value = "/auth/redirect.asp?authtype=" + authtype +
"&target=" + trgarr[1];
}
else
{
    // This is not a redirect. Pass $$target$$ as a URL query parameter.
    document.Login.target.value = "/auth/redirect.asp?authtype=" + authtype +
"&target=$$target$$";
}

document.Login.submit();
}
function resetCredFields()
{
    document.Login.PASSWORD.value = "";
    document.Login.PASSWORD1.value = "";
    document.Login.PASSWORD2.value = "";
}
</script>
</head>

<body onLoad="resetCredFields();">
<center>
<form name="Login" method="POST">
    <input type="hidden" name="USER">
    <input type="hidden" name="PASSWORD">
    <input type="hidden" name="smagentname" value="$$smagentname$$">
    <input type="hidden" name="smauthreason" value="$$smauthreason$$">
    <input type="hidden" name="smquerydata" value="$$smquerydata$$">
    <input type="hidden" name="postpreservationdata"
value="$$postpreservationdata$$">
    <input type="hidden" name="target">
```

```
<!-- Some table formatting throughout -->
<!-- Authentication Choice: Password And/Or Certificate -->
  <input type="text"      name="USER1">
  <input type="password" name="PASSWORD1">
  <input type="button"   value="Login" onClick="submitForm(1);">

<!-- Authentication Choice: Windows Authentication -->
  <input type="button"   value="Login" onClick="submitForm(4);">

<!-- Authentication Choice: SecurID Authentication -->
  <input type="text"      name="USER2">
  <input type="password" name="PASSWORD2">
  <input type="button"   value="Login" onClick="submitForm(2);">

<!-- Authentication Choice: SafeWord Authentication -->
  <input type="text"      name="USER3">
  <input type="button"   value="Login" onClick="submitForm(3);">
<!-- More table formatting -->
</form>
</center>
</body>
</html>
```

프런트엔드 인증 체계 구성

인사말을 생성하는 샘플 응용 프로그램을 보호하는 프런트엔드 인증 체계를 구성하십시오. 이를 위해서는 AuthChannel 인증 체계를 구성합니다.

AuthChannel 인증 체계의 예는 다음 그림을 참조하십시오.

General

Name: AuthChannel **Description:** Auth scheme for

Scheme Common Setup

Authentication Type Style: HTML Form Template

Protection Level: 1 [1-1,000,higher i]

☐ Password Policies enabled for this Authentication Scheme

Scheme Setup

Web Server Name auth.sample.com

☐ Use SSL Connection

Target /siteminderagent/forms/selectlogin.fcc

☐ Allow this Scheme to save credentials

"AuthChannel Authentication Scheme"(AuthChannel 인증 체계)은 다음과 같이 설정됩니다.

인증 유형 스타일

HTML 양식 템플릿

보호 수준

1

프런트엔드 인증 체계의 보호 수준은 구성의 다른 체계보다 낮아야 하므로 AuthChannel 체계의 보호 수준은 1로 설정됩니다. 보호되는 리소스를 액세스하기 위해 사용자가 로그인할 때 선택하는 인증 체계는 해당 사용자의 실제 보호 수준을 결정합니다. 사용자가 다시 원래 요청한 리소스로 리디렉션되더라도 프런트엔드 체계의 낮은 보호 수준으로 인해 사용자에게 인증이 다시 요청되지 않습니다.

웹 서버 이름

auth.sample.com

샘플 응용 프로그램이 있는 웹 서버를 지정합니다.

대상

/siteminderagent/forms/selectlogin.fcc

이 대상은 `selectlogin.fcc` 파일을 가리킵니다. `selectlogin.fcc` 파일은 웹 에이전트 설치에 포함된 샘플 파일입니다.

성공하지 못한 인증 시도 관리

인증 체계가 사용자를 거부하는 경우 이 사용자는 해당 인증 체계에 대한 `Target` 매개 변수에 지정된 URL 로 리디렉션됩니다.

상황에 가장 적합하게 다음 동작을 구성하십시오.

- 인증 체계를 다시 선택할 수 있도록 하는 대신 동일한 인증 체계에 대한 자격 증명을 다시 제출하라는 메시지가 사용자에게 표시되도록 합니다.
- 사용자가 원래 로그인 화면으로 돌아가서 선택을 반복할 수 있도록 합니다. 이 동작을 구성하려면 해당하는 경우 `selectlogin.fcc` 를 각 인증 체계에 대한 `Target` 매개 변수로 지정하십시오.

`selectlogin.fcc` 파일이 아닌 다른 FCC 파일에 포스트해야 하는 특정 자격 증명을 선택할 경우 `selectlogin.fcc` 에서 HTML 양식에 대한 `action` 매개 변수를 원하는 FCC 파일 URL 로 설정하십시오. 예를 들어 다음 명령은 `action` 매개 변수를 `safeword.fcc` 파일로 설정합니다.

```
document.Login.action = "safeword.fcc";
```

기본 인증 체계와 같이 `Target` 매개 변수가 없는 체계를 사용하는 경우 사용자 환경은 인증에 성공할 경우와 동일합니다. 하지만 사용자가 다시 챌린지되어야 하는 경우 이 챌린지는 기본 인증 체계에 기반합니다. 따라서 HTML 양식이 아닌 입력 대화 상자가 사용됩니다.

참고: SafeWord 기본 체계는 SafeWord HTML 양식 체계와 달리 2 단계 인증과 여러 인증자를 지원하지 않습니다.

백엔드 처리 설정

자격 증명 선택기를 사용하려면 백엔드 처리를 위해 다음 구성 요소가 필요합니다.

- 각 로그인 자격 증명 선택을 위한 인증 체계
- 백엔드 구성 요소가 포함된 정책 도메인
- 각 인증 체계를 사용하는 영역
- 각 영역에 대한 규칙
- 인증 컨텍스트를 설정하고 리소스 액세스 권한을 부여하는 정책

백엔드 처리를 위한 인증 체계 설정

백엔드 처리를 위한 몇 가지 인증 체계를 설정해야 합니다. 사용자에게 제공되는 각 자격 증명 선택 항목마다 하나씩 설정하십시오. 사용자는 이러한 체계를 사용하여 보호된 리소스에 액세스하기 위해 제공하는 자격 증명의 유형을 선택할 수 있습니다.

다음은 각 자격 증명 유형에 대한 인증 체계입니다.

- HTML 양식 인증 체계
- X.509 클라이언트 인증서 인증 체계
- X.509 클라이언트 인증서 및 양식 인증 체계
- SecurID HTML 양식 인증 체계
- SafeWord HTML 양식 인증 체계
- Windows 인증 체계

참고: 기본 인증 체계는 정책 서버를 설치할 때 기본적으로 설정되는 체계입니다.

백엔드 처리를 위한 정책 도메인 설정

자격 증명 선택기 백엔드 처리를 나타내도록 정책 도메인을 구성하십시오. 이 솔루션에서는 정책 도메인을 **BackendAuth** 라고 합니다.

백엔드 정책 도메인에 대한 영역 구성

구성된 각 백엔드 인증 체계마다 영역을 하나씩 정의하십시오. 각 영역에는 다음과 같이 정의된 리소스 필터가 필요합니다.

`/auth/redirect.asp?authtype=type&target=`

type

다음 값 중 하나가 될 수 있습니다.

form	사용자 이름/암호 인증
cert	인증서 인증
certform	인증서 및 양식 인증
securid	SecurID 인증
safeword	SafeWord 인증
windows	Windows 인증

참고: 이러한 유형은 이 사용 사례의 목적에 맞게 선택된 것입니다. 이러한 특정 값 외의 다른 값도 선택할 수 있지만 유형은 `selectlogin.fcc` 파일이나 `selectlogin.fcc` 템플릿을 기반으로 하는 다른 FCC 파일의 `authtype` 값에 해당해야 합니다. 또한 영역 리소스 필터가 FCC 파일의 리디렉션 대상과 일치해야 합니다.

다음 창에는 영역이 나열되어 있습니다.



영역을 보호하는 웹 에이전트는 동일할 수는 있지만 동일할 필요는 없습니다. 이 솔루션에서는 단일 웹 에이전트를 사용하지만 여러 웹 에이전트가 사용되는 경우에는 웹 에이전트가 특정 요구 사항을 충족해야 합니다.

다음은 자격 증명 선택기 기능의 일부로 영역을 보호하는 에이전트가 충족해야 하는 요구 사항입니다.

- 영역을 보호하는 모든 웹 에이전트 간에 싱글 사인온이 구성되어야 합니다. 즉, 모든 웹 에이전트가 동일한 쿠키 도메인에 있거나 동일한 쿠키 공급자를 사용해야 합니다.
- FCC 파일의 `@smagentname` 지시문 값이 원래 요청한 리소스를 보호하는 하나 이상의 웹 에이전트에 대한 예상 값과 일치해야 합니다.

예상 값은 `AgentName` 매개 변수 값이거나, `AgentName` 매개 변수에 값이 할당되지 않은 경우 `DefaultAgentName` 매개 변수 값입니다. 에이전트 구성에서 `EncryptAgentName` 매개 변수가 `yes` 로 설정된 경우 이 값은 암호화되어야 합니다.

`@smagentname` 지시문을 설정하는 한 가지 방법은 각 웹 에이전트를 동일한 명명 속성으로 구성하는 것입니다. 각 웹 에이전트가 하나의 에이전트 구성 개체를 공유해도 됩니다. 또 다른 방법은 이름이 암호화되지 않은 경우 FCC 파일에서 `@smagentname` 지시문을 프로그래밍 방식으로 구성하는 것입니다.

중요! `@smagentname` 지시문이 잘못 구성된 경우 정책 서버 로그에 "No realm received in request"(요청에서 받은 영역 없음)라는 오류 메시지가 표시될 수 있습니다.

- `selectlogin.fcc` 파일이 생성하는 새 대상에 대해 두 번째 `IsProtected` 호출이 수행되도록 하려면 `FCCForcelsProtected` 매개 변수를 `yes` 로 설정해야 합니다. 에이전트가 이 URL 쿼리 매개 변수를 무시하지 않도록 방지하려면 `IgnoreQueryData` 매개 변수를 `No` 로 설정하십시오.

백엔드 정책 도메인에 대한 규칙 만들기

`BackendAuth` 정책 도메인에 대해 구성하는 각 영역에서 다음 두 규칙을 구성하십시오.

- `OnAuthAccept` 규칙
- 웹 에이전트 작업 규칙(이 예의 경우 `GET` 작업 규칙 사용)

두 규칙 모두에 대해 "리소스" 필드의 값으로 별표(*)를 구성하십시오.

예를 들어 BackendAuth 정책 도메인의 Form 영역에 대한 규칙은 다음과 같습니다.

OnAuthAccept

리소스: /auth/redirect.asp?authtype=form&target=*

작업: OnAuthAccept

GetRule

리소스: /auth/redirect.asp?authtype=form&target=*

작업: Get

백엔드 정책 도메인에 대한 AuthContext 응답 구성

BackendAuth 도메인에서 각 인증 체계에 대한 AuthContext 응답을 구성하십시오. 이러한 각 응답에는 OnAuthAccept 이벤트에서만 평가되는 AuthContext 응답 특성이 포함되어 있습니다. 해당 값은 SiteMinder 세션 티켓에 SM_AUTHENTICATIONCONTEXT 사용자 특성 값으로 추가됩니다. 하지만 이 값은 클라이언트에 사용자 응답으로 반환되지는 않습니다.

이 예의 경우 응답 목록은 다음과 같습니다.

에이전트 유형 설명		
이름		
Form	웹 에이전트	사용자 이름/암호 인증용 AuthContext
Certificate	웹 에이전트	인증서 인증용 AuthContext
CertandForm	웹 에이전트	인증서 및 양식 인증용 AuthContext
SecurID	웹 에이전트	SecurID 인증용 AuthContext
SafeWord	웹 에이전트	SafeWord 인증용 AuthContext
Windows	웹 에이전트	Windows 인증용 AuthContext

참고: 응답 특성 값은 80 바이트 길이로 잘립니다.

AuthContext 응답 특성을 구성하려면

WebAgent-OnAuthAccept-Session-AuthContext 응답 특성 유형을 선택하십시오.

다음 그림에서는 WebAgent-OnAuthAccept-Session-AuthContext 특성 유형을 사용하여 AuthContext 응답 특성을 생성하는 예를 보여 줍니다.

Attribute WebAgent-OnAuthAccept-Session-AuthContext						
Value Type Text						
Response Form Response						
Attribute Setup						
<table border="1"> <tr> <th>Attribute Kind</th> <th>Attribute Fields</th> </tr> <tr> <td> ☒ Static ☐ User Attribute ☐ DN Attribute ☐ Active Response </td> <td> Variable Name Variable Value username/password HTTP Variable Name Response Variable Name </td> </tr> <tr> <td>Allow Nested Groups ☐</td> <td></td> </tr> </table>	Attribute Kind	Attribute Fields	☒ Static ☐ User Attribute ☐ DN Attribute ☐ Active Response	Variable Name Variable Value username/password HTTP Variable Name Response Variable Name	Allow Nested Groups ☐	
Attribute Kind	Attribute Fields					
☒ Static ☐ User Attribute ☐ DN Attribute ☐ Active Response	Variable Name Variable Value username/password HTTP Variable Name Response Variable Name					
Allow Nested Groups ☐						
Advanced						
Script username/password						

그림에 표시된 대로 AuthContext 응답 특성 유형은 정적입니다. 레거시 페더레이션을 사용 중인 경우 향상된 캡슐화를 위해 정적 특성을 지정하여 상수 또는 리터럴 값을 정의할 수 있습니다. 상수 값에는 문자열이 포함됩니다.

SiteMinder 변수 및 활성 식을 사용하면 보다 유연하게 AuthContext 응답 특성을 구성할 수 있습니다. 여기에는 또한 SAML 어설션의 인증 타임스탬프, 해시 값 또는 둘 모두가 포함될 수 있습니다.

다음 그룹 상자에서는 이 솔루션에 대해 구성된 결과 응답 중 하나를 보여 줍니다. 이 특성은 Form 응답에 대한 특성입니다.

Domain BackendAuth

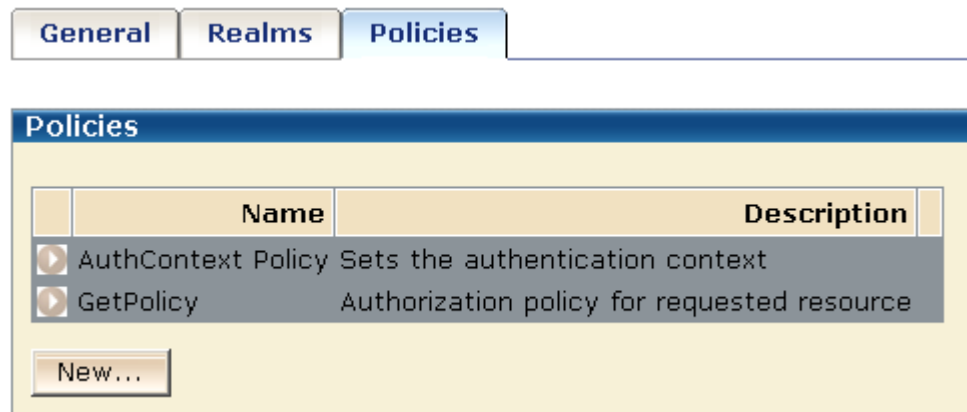
Attribute List		
	Agent Type Attribute Name	Value
	WebAgent-OnAuthAccept-Session-AuthContext	username/password

백엔드 자격 증명 선택에 대한 정책 구성

이 예에서는 BackendAuth 도메인에 대한 다음 두 가지 정책을 구성하십시오.

- 사용자 인증 컨텍스트를 설정하기 위한 정책
- 웹 에이전트 작업에 대한 정책

다음 그림에서는 이 두 가지 정책을 보여 줍니다.



인증 컨텍스트 정책 만들기

AuthContext 정책은 SiteMinder 세션 티켓에 인증 및 유효성 검사에 사용되는 인증 컨텍스트를 설정합니다. 이 정책에서 각 영역의 OnAuthAccept 규칙은 해당 응답과 쌍으로 연결되어 보호된 리소스에 대한 액세스를 허용합니다. 예를 들어 Form 영역에 대한 OnAuthAccept 규칙은 Form 응답과 쌍으로 연결되고 SafeWord 영역에 대한 OnAuthAccept 규칙은 SafeWord 응답과 쌍으로 연결됩니다.

사용자 인증과 사용자 유효성 검사는 OnAuthAccept 이벤트이므로 각 유효성 검사 이후 세션 티켓의 인증 컨텍스트를 덮어쓰게 될 수 있습니다. 인증 컨텍스트 특성을 업데이트하는 기능은 예를 들어 특성 값에 카운터가 포함되는 경우와 같은 일부 경우에 유용할 수 있습니다. 그러나 자격 증명 선택기를 사용하는 이 솔루션에서는 세션 티켓을 덮어쓰지 않도록 인증 컨텍스트가 비어 있는 경우에만 AuthContext 정책이 실행되도록 구성됩니다. 따라서 사용자가 선택하는 자격 증명이 기억됩니다.

세션 티켓에서 SM_AUTHENTICATIONCONTEXT 을 가져오도록 AuthContext 정책에 활성 식을 작성하는 방법으로 인증 컨텍스트가 덮어쓰기되지 않도록 방지하십시오.

레거시 페더레이션을 사용 중인 경우 **AuthContext** 이라는 사용자 컨텍스트 변수를 생성하고 **AuthContext** 정책에서 해당 변수를 사용하여 세션 티켓에서 **SM_AUTHENTICATIONCONTEXT** 특성을 검색하는 활성 식을 정의할 수 있습니다.

General	
• Name:	AuthContext
Description:	

Attributes	
Variable Type	UserContext

Variable Information	
Return Type	String

Context Item	
Item	User Property
• Property	SM-AUTHENTICATIONCONTEXT
• DN	
• Buffer Size	80

AuthContext 정책에서 **AuthContext** 변수를 사용하여 활성 식을 정의하십시오.

General	Users	Rules	Expression						
<table border="1"> <thead> <tr> <th colspan="2">Expression</th> </tr> </thead> <tbody> <tr> <td>Expression</td> <td>(AuthContext=="")</td> </tr> <tr> <td colspan="2"> Edit </td> </tr> </tbody> </table>				Expression		Expression	(AuthContext=="")	Edit	
Expression									
Expression	(AuthContext=="")								
Edit									

보호 정책 만들기

인증된 사용자에게 요청된 리소스에 대한 권한을 부여하려면 **BackendAuth** 도메인에 두 번째 정책이 있어야 합니다. 이 정책은 리소스를 보호할 뿐 아니라 이 도메인의 인증 컨텍스트 정책이기도 합니다.

보호 정책이 인증된 사용자에게 리디렉션 대상에 대한 권한을 부여하도록 구성하십시오. 이 작업은 **redirect.asp** 파일의 **GET** 작업입니다. 정책 이름을 **GetPolicy** 로 지정하십시오.

GetPolicy 에는 관련 규칙이 포함됩니다.

규칙	영역
GetRule	Form
GetRule	Certificate
GetRule	CertandForm
GetRule	SecureID
GetRule	SafeWord
GetRule	Windows

샘플 응용 프로그램 보호

자격 증명 선택기를 사용하려면 구성 요소의 프런트엔드 인증 체계를 사용하여 **SiteMinder** 응용 프로그램의 보호된 영역을 구성하십시오. 응용 프로그램을 보호하는 정책에는 사용자 인증 수준과 인증 컨텍스트를 기반으로 하는 제한이 있을 수 있습니다.

이 솔루션의 샘플 응용 프로그램은 인증되고 권한이 부여된 사용자에게 표시할 인사말 메시지를 생성합니다.

이 인사말을 생성하는 파일에는 다음과 같은 코드가 있습니다.

```
<html>
<head></head>
<body>

<h3>
<p>Greetings, <%=Request.ServerVariables("HTTP_USERNAME") %>!
<p>Your authentication level is <%=Request.ServerVariables("HTTP_AUTHLEVEL") %>
<p>You have used <%=Request.ServerVariables("HTTP_AUTHCONTEXT") %>
authentication
</h3>

</body>
</html>
```

로그인 대화 상자에서 다른 인증 옵션을 선택할 경우의 결과 액세스 수준과 인사말은 다음과 같이 달라집니다.

```
Greetings, SampleUser!
Your authentication level is 5
You have used username/password authentication

Greetings, SampleUser!
Your authentication level is 10.
You have used X.509 client certificate authentication

Greetings, SampleUser!
Your authentication level is 5
You have used Windows domain authentication
```

샘플 응용 프로그램에는 서로 다른 영역에 포함된 네 종류의 리소스가 있습니다. 각 영역은 프런트엔드 인증 체계로 구성되어야 합니다.

샘플 응용 프로그램의 영역 및 규칙

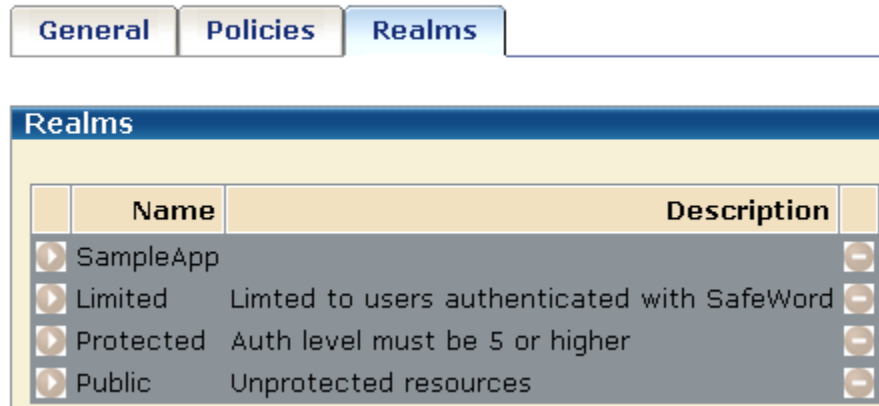
이 예의 경우 다음 네 가지 영역이 샘플 응용 프로그램을 구성하는 다양한 리소스를 보호합니다.

- 공용 리소스가 포함된 영역
- 수준 5 이상의 인증이 필요한 리소스가 포함된 영역

- 수준 15 이상의 인증이 필요한 리소스가 포함된 영역
- SafeWord 로 인증된 사용자만 사용할 수 있는 리소스가 포함된 영역

다음 그림에서는 이러한 영역을 보여 줍니다.

Modify Domain: *SampleApp*



보호된 영역은 다음 그림과 같이 AuthChannel 프런트엔드 인증 체계로 구성되어 있습니다.

The image shows a configuration window with two tabs: 'General' and 'Resource'.
 In the 'General' tab, there is a 'Name' field with the value 'Protected'.
 In the 'Resource' tab, there is an 'Agent' dropdown menu set to 'sampleagent'. Below it is a 'Resource Filter' field containing '/protected/'. The 'Effective Resource' field displays 'sampleagent/protected/'. Under 'Default Resource Protection', the 'Protected' radio button is selected. At the bottom, the 'Authentication Scheme' dropdown is set to 'AuthChannel'.

SampleAgentGroup에는 샘플 응용 프로그램에 진입점을 제공하는 웹 에이전트가 포함될 수 있습니다.

다음은 자격 증명 선택기 기능의 일부로 영역을 보호하는 에이전트가 충족해야 하는 요구 사항입니다.

- 영역을 보호하는 모든 웹 에이전트 간에 싱글 사인온이 구성되어야 합니다. 즉, 모든 웹 에이전트가 동일한 쿠키 도메인에 있거나 동일한 쿠키 공급자를 사용해야 합니다.
- FCC 파일의 @smagentname 지시문 값이 원래 요청한 리소스를 보호하는 하나 이상의 웹 에이전트에 대한 예상 값과 일치해야 합니다.

예상 값은 AgentName 매개 변수 값이거나, AgentName 매개 변수에 값이 할당되지 않은 경우 DefaultAgentName 매개 변수 값입니다. 에이전트 구성에서 EncryptAgentName 매개 변수가 yes로 설정된 경우 이 값은 암호화되어야 합니다.

@smagentname 지시문을 설정하는 한 가지 방법은 각 웹 에이전트를 동일한 명명 속성으로 구성하는 것입니다. 각 웹 에이전트가 하나의 에이전트 구성 개체를 공유해도 됩니다. 또 다른 방법은 이름이 암호화되지 않은 경우 FCC 파일에서 @smagentname 지시문을 프로그래밍 방식으로 구성하는 것입니다.

중요! @smagentname 지시문이 잘못 구성된 경우 정책 서버 로그에 "No realm received in request"(요청에서 받은 영역 없음)라는 오류 메시지가 표시될 수 있습니다.

- `selectlogin.fcc` 파일이 생성하는 새 대상에 대해 두 번째 `IsProtected` 호출이 수행되도록 하려면 `FCCForcelsProtected` 매개 변수를 `yes` 로 설정해야 합니다. 에이전트가 이 URL 쿼리 매개 변수를 무시하지 않도록 방지하려면 `IgnoreQueryData` 매개 변수를 `No` 로 설정하십시오.

샘플 응용 프로그램을 보호하는 정책에 대한 규칙

샘플 응용 프로그램 리소스가 포함된 영역에 대한 규칙 유형을 구성할 수 있습니다.

샘플 응용 프로그램을 보호하도록 정책 구성

보호된 리소스에 액세스하려면 `GetProtected` 정책에 보호 수준 5 이상이 필요합니다. 이 보호 수준 제한을 적용하려면 `GetProtected` 정책에 SiteMinder 세션 티켓에서 `SM_AUTHENTICATIONLEVEL` 을 검색하는 활성 식을 작성합니다.

참고: 이 인증 수준 제한은 암호 인증 수준 1 만 지원하는 사용자 지정 웹 에이전트에서 응용 프로그램을 보호하기 위한 것입니다.

레거시 페더레이션을 사용 중인 경우 `AuthLevel` 이라는 사용자 컨텍스트 변수를 생성하고 `GetProtected` 정책에서 해당 변수를 사용하여 세션 티켓에서 `SM_AUTHENTICATIONLEVEL` 특성을 검색하는 활성 식을 정의할 수 있습니다.

Create Policy: GetProtected

Module Domain: [BackendAuth](#) > Create Policy: GetProtected

General Users Rules **Expression**

Expression

Expression

Edit

샘플 응용 프로그램에 대한 응답 구성

이 예에서 인사말 메시지를 표시하는 샘플 응용 프로그램은 다음 세 개의 HTTP 헤더 변수를 사용합니다.

- HTTP_USERNAME
- HTTP_AUTHLEVEL
- HTTP_AUTHCONTEXT

이러한 헤더는 다음 응답과 함께 클라이언트에 반환됩니다.

General

Name: SampleResponse

Description: Username, Auth level, Auth Cont

Attributes

Agent Type

☐ Radius
 ☒ SiteMinder

Agent Type

Web Agent

Domain SampleApp

Attribute List

	Agent Type	Attribute Name	Value	
▶	WebAgent-HTTP-Header-Variable	UserName=<%userattr="SM_USERSESSIONUNIVID"%>		⊖
▶	WebAgent-HTTP-Header-Variable	AuthContext=<%userattr="SM_AUTHENTICATIONCONTEXT"%>		⊖
▶	WebAgent-HTTP-Header-Variable	AUTHLEVEL=<%userattr="SM_AUTHENTICATIONLEVEL"%>		⊖

특성 값은 "응답 특성" 창에서 지정합니다.

자격 증명 선택기 솔루션 테스트

이 사용 사례에 설명된 다양한 구성 요소를 설정한 경우 자격 증명 선택기 기능을 테스트할 수 있습니다. 이 테스트를 통해 지정하는 자격 증명에 따라 다른 인사말이 표시되는지 확인해야 합니다.

다음 단계를 수행하십시오.

1. 샘플 응용 프로그램에 대한 링크를 클릭하는 등의 방법으로 샘플 응용 프로그램에 액세스를 시도합니다.

`selectlogin.fcc` 파일에 정의된 로그인 화면이 표시됩니다.

2. 로그인하는 데 사용할 자격 증명 유형을 하나 입력합니다.

입력한 자격 증명에 적절한 인사말이 표시됩니다. 예를 들어 사용자 이름과 SecurID PIN 을 입력한 경우 다음과 같은 인사말이 표시됩니다.

```
Greetings, SampleUser!  
Your authentication level is 20  
You have used the SecurID authentication
```

3. 응용 프로그램을 종료하고 샘플 응용 프로그램에 다시 액세스해 봅니다.
4. 이전 단계에서 입력한 것과는 다른 자격 증명 집합을 입력합니다.

지정한 자격 증명에 적절한 인사말 메시지가 표시됩니다.

자격 증명 선택기를 성공적으로 테스트했습니다.

제 11 장: 응용 프로그램 개체에서 웹 응용 프로그램에 대한 보안 정책 정의

이 섹션은 다음 항목을 포함하고 있습니다.

[응용 프로그램 개체를 사용한 리소스 보안의 장점 \(페이지 505\)](#)

[응용 프로그램 개체에서 웹 응용 프로그램에 대한 보안 정책을 정의하는 방법 \(페이지 506\)](#)

[응용 프로그램 개체를 사용하여 응용 프로그램 보안 정책을 정의하기 위한 사용 사례 \(페이지 518\)](#)

응용 프로그램 개체를 사용한 리소스 보안의 장점

응용 프로그램 개체는 SiteMinder 와 관련된 개념 및 개체 유형에 대해 자세히 알지 못하는 사용자도 비즈니스 응용 프로그램을 보호할 수 있게 해주는 액세스 관리 모델을 제공합니다. 이 모델을 EPM(Enterprise Policy Management)이라고도 합니다.

응용 프로그램 개체는 응용 프로그램 보안 컨텍스트에서 정책 구성을 제공합니다. 응용 프로그램 개체를 생성하고 기본값이 없는 구성 설정에 대해 데이터를 제공하기만 하면 응용 프로그램을 보호할 수 있습니다. 그 외의 설정은 필요할 때 수정하면 되므로 응용 프로그램 개체를 사용하면 정책 구성 작업을 보다 간단하게 수행할 수 있습니다. 다른 설정을 조작하여 응용 프로그램 보호 기능을 좀 더 세부적으로 정의할 수 있지만 이러한 조작이 꼭 필요하지는 않습니다.

도메인 기반 정책에 익숙한 관리자라면 응용 프로그램 지향 개념과 기본 정책 개체 간에 특정한 관계가 있음을 잘 알고 있을 것입니다. 이러한 관계는 관리 UI 에 반영되어 있으며 다음 표에 나와 있습니다.

응용 프로그램 대화 상자 및 그룹 상자	기본 SiteMinder 구성 요소
일반 설정	정책 도메인 정의
구성 요소	영역 정의
리소스	규칙 지정
응용 프로그램 역할	정책 사용자 정의

응용 프로그램 역할은 응용 프로그램 개체에 정의된 리소스 또는 리소스 그룹에 대한 액세스 권한이 있는 사용자 집합을 정의합니다. 역할은 다음 속성을 가질 수 있습니다.

- 역할은 구성된 사용자 디렉터리의 모든 사용자를 포함할 수 있습니다.
- 역할은 선택한 그룹, 조직, 일치하는 사용자 특성이 있는 사용자로 제한할 수 있습니다.
- 역할은 명명되거나 명명되지 않은 식을 사용하여 지정될 수 있습니다.

응용 프로그램 개체를 사용하면 다음과 같은 이점이 있습니다.

응용 프로그램 중심 접근 방식

응용 프로그램의 중심은 대부분의 기업이 액세스 관리를 바라보는 관점과 밀접한 관련이 있습니다.

일관된 보안 적용 모델

응용 프로그램 개체의 보안 적용 모델은 보다 도메인 중심적인 모델에서 구현하는 것과 다르지 않지만 도메인 관련 구성 요소는 구성에서 숨겨집니다.

단순한 보안

리소스 보안이 단순해집니다. 응용 프로그램, 보호가 필요한 응용 프로그램 리소스 및 액세스가 허용되는 응용 프로그램 역할을 지정하기만 하면 됩니다. 보안 정책을 설정하기 위해 한 구성 요소의 모든 측면을 검토하거나 수정할 필요가 없습니다.

향상된 위임

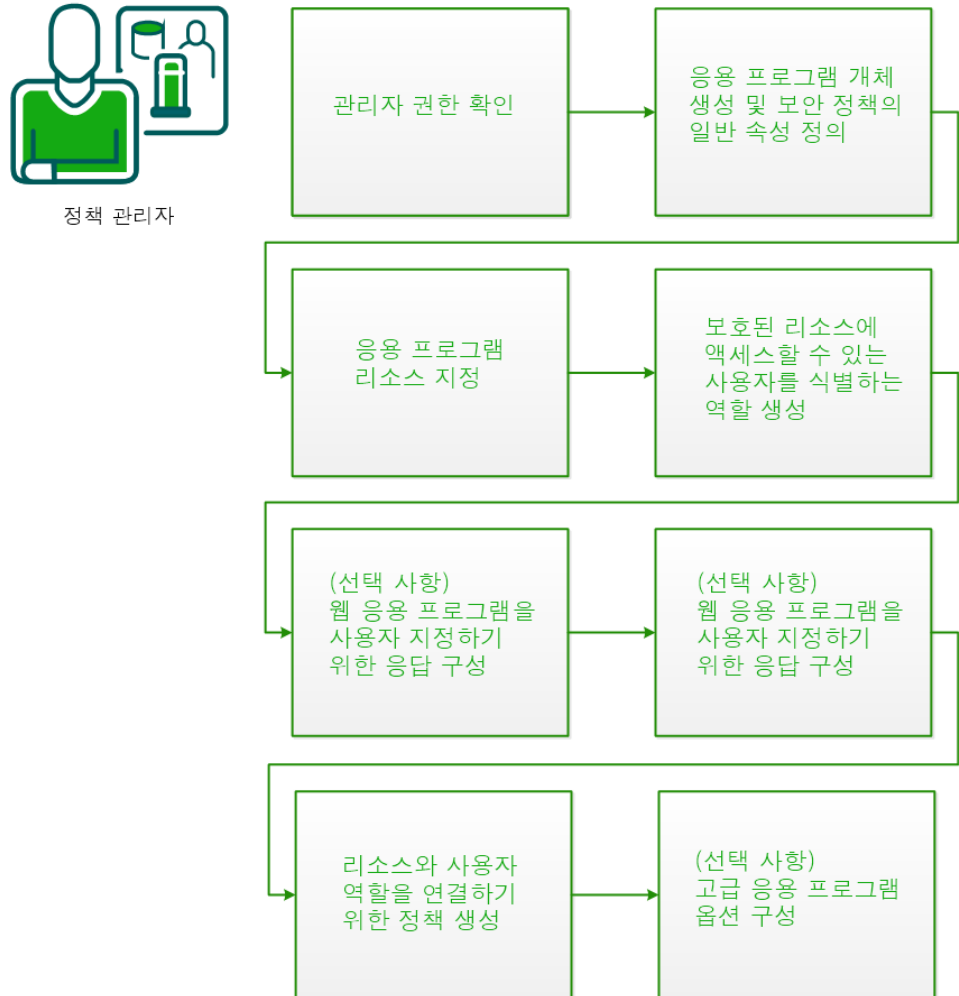
관리자는 SiteMinder에 대한 전문 지식 없이도 응용 프로그램에 대한 액세스 권한을 부여할 수 있습니다. 따라서 선임 보안 관리자는 액세스 관리 업무를 다른 관리자에게 위임할 수 있습니다.

응용 프로그램 개체에서 웹 응용 프로그램에 대한 보안 정책을 정의하는 방법

응용 프로그램 개체는 웹 응용 프로그램(또는 웹 사이트)에 대한 완전한 보안 정책을 정의할 수 있는 직관적인 방법을 제공합니다. 응용 프로그램 개체는 리소스를 사용자 역할과 연결하여 사용자별로 액세스할 수 있는 리소스를 결정하는 권한 정책을 지정합니다.

참고: 응용 프로그램 개체는 정책 도메인 및 하위 개체에서 구성할 수 있는 정책 정보(즉, 영역, 규칙, 규칙 그룹, 응답 및 정책)를 정의합니다.

응용 프로그램 개체에서 웹 응용 프로그램에 대한
보안 정책 정의 방법



응용 프로그램 개체에서 웹 응용 프로그램에 대한 보안 정책을 정의하려면 다음 절차를 수행하십시오.

1. [관리 권한을 확인합니다](#) (페이지 508).
2. [응용 프로그램 개체를 생성하고 보안 정책의 일반 속성을 정의합니다](#) (페이지 508).
3. [응용 프로그램 리소스를 지정합니다](#) (페이지 510).

4. [보호된 리소스에 액세스할 수 있는 사용자를 식별하는 역할을 생성합니다](#) (페이지 511).
5. [\(선택 사항\) 웹 응용 프로그램을 사용자 지정하도록 응답을 구성합니다](#) (페이지 511).
6. [\(선택 사항\) 웹 응용 프로그램을 사용자 지정하도록 응답 그룹을 구성합니다](#) (페이지 512).
7. [리소스를 사용자 역할에 연결할 정책을 생성합니다](#) (페이지 513).
8. [\(선택 사항\) 고급 응용 프로그램 옵션을 구성합니다](#). (페이지 514)

관리 권한 확인

응용 프로그램 보안 정책을 구현하려면 필요한 관리 권한이 있어야 합니다. 관리자에게는 다음과 같은 응용 프로그램 관련 권한이 부여될 수 있습니다.

응용 프로그램 관리

응용 프로그램 관리 권한이 있으면 응용 프로그램과 해당 구성 요소를 생성하고, 수정하고, 삭제할 수 있습니다.

정책 관리

정책 관리 권한이 있으면 응용 프로그램과 연결된 리소스, 역할 및 정책을 정의할 수 있습니다.

필요한 권한이 없는 경우 SiteMinder 슈퍼 사용자에게 문의하십시오.

응용 프로그램 개체 생성 및 보안 정책의 일반 속성 정의

응용 프로그램 개체를 생성하고 응용 프로그램 개체가 정의하는 보안 정책의 다음과 같은 일반 속성을 구성하십시오.

- 하나 이상의 구성 요소-보안 요구 사항이 유사한 관련 응용 프로그램 리소스(일반적으로 공용 위치에 있는 리소스)의 그룹입니다. 예를 들어 마케팅 정보는 네트워크의 /marketing 디렉터리에 있습니다.
- 리소스를 사용할 수 있는 권한이 부여된 사용자의 디렉터리

다음 단계를 수행하십시오.

1. 관리 UI에 로그인합니다.
2. "정책", "응용 프로그램"을 차례로 클릭합니다.
3. "응용 프로그램"을 클릭합니다.
4. "응용 프로그램 만들기"를 클릭합니다.
"응용 프로그램 만들기" 페이지가 표시됩니다.
5. 응용 프로그램의 이름과 설명을 입력합니다.
6. "구성 요소" 섹션에서 보안 요구 사항이 유사한 하나 이상의 관련 리소스 그룹을 정의합니다. 각 구성 요소에 대해 다음 단계를 수행합니다.
 - a. "구성 요소 만들기"를 클릭합니다.
 - b. 구성 요소의 이름을 입력합니다.
 - c. "에이전트/에이전트 그룹 조회"를 클릭합니다.
 - d. 에이전트 또는 에이전트 그룹을 선택하고 "확인"을 클릭합니다.
 - e. "리소스 필터" 필드에서 보호할 리소스의 루트 URL을 입력합니다.
 - f. 리소스가 기본적으로 보호되는지 여부를 지정합니다.
 - g. 리소스를 요청하는 사용자의 아이덴티티 유효성을 검사하는 데 사용할 인증 체계를 지정합니다.
7. "사용자 디렉터리" 섹션에서 다음 단계를 수행하여 응용 프로그램 리소스를 사용할 수 있는 권한이 부여된 사용자의 디렉터리를 선택합니다.
 - a. "추가/제거"를 클릭합니다.
 - b. "사용 가능한 구성원"의 목록에서 하나 이상의 사용자 디렉터리를 선택하고 오른쪽 방향 화살표를 클릭합니다.
사용자 디렉터리가 "사용 가능한 구성원" 목록에서 제거되고 "선택한 구성원" 목록에 추가됩니다.
참고: 한 번에 여러 구성원을 선택하려면 **Ctrl** 키를 누른 채 추가 구성원을 클릭하십시오. 구성원 블록을 선택하려면 첫 번째 구성원을 클릭한 다음 **Shift** 키를 누른 채 블록의 마지막 구성원을 클릭하십시오.
 - c. "확인"을 클릭합니다.
선택한 사용자 디렉터리가 "응용 프로그램 만들기" 페이지의 "사용자 디렉터리" 아래에 나열됩니다.

8. "확인"을 클릭합니다.
 9. 제출을 클릭합니다.
- 응용 프로그램 개체가 생성됩니다.

응용 프로그램 리소스 지정

보호할 응용 프로그램 구성 요소를 정의한 후에는 각 구성 요소 내에서 보호할 특정 리소스를 지정하십시오.

다음 단계를 수행하십시오.

1. "응용 프로그램 만들기" 페이지에서 "리소스" 탭을 클릭합니다.
 2. 여러 구성 요소를 생성한 경우 "컨텍스트 루트 선택" 드롭다운 목록에서 보호할 리소스의 루트 URL("일반" 탭의 "리소스 필터"로 지정됨)을 선택합니다.
 3. "만들기"를 클릭합니다.
 4. 리소스의 이름을 입력합니다.
 5. "리소스" 필드에 보호할 리소스를 입력합니다. 특정 파일을 지정하거나, 정규식을 사용하여 리소스 일치의 유연성을 높입니다.
"유효 리소스"가 업데이트되어 리소스가 포함됩니다.
 6. "리소스" 필드에 정규식을 사용한 경우 "정규식" 옵션을 설정합니다.
 7. "작업" 섹션에서 지정된 리소스에 대해 수행되어 정책 서버가 요청을 처리하도록 하는 작업의 유형을 선택합니다.
"작업 목록"이 선택한 작업 유형에 적절한 작업으로 채워집니다.
 8. 작업을 하나 이상 선택합니다.
 9. "확인"을 클릭합니다.
리소스가 생성됩니다.
 10. 웹 응용 프로그램의 각 리소스에 대해 2~9 단계를 반복합니다.
- 이제 웹 응용 프로그램 리소스가 정의되었습니다.

보호된 리소스에 액세스할 수 있는 사용자를 식별하는 역할 생성

웹 응용 프로그램 구성 요소 및 리소스를 정의한 후에는 특정 리소스에 액세스할 수 있는 사용자 집합을 정의하는 역할을 지정하십시오.

다음 단계를 수행하십시오.

1. "응용 프로그램 만들기" 페이지에서 "역할" 탭을 클릭합니다.
2. "역할 만들기"를 클릭합니다.
3. "역할 유형의 새 개체 만들기" 옵션이 선택되어 있는지 확인하고 "확인"을 클릭합니다.
4. 역할의 이름과 설명(선택 사항)을 입력합니다.
5. 해당 역할이 구성된 사용자 디렉터리의 "모든 사용자"에게 적용되는지, "선택한 사용자"에게만 적용되는지를 지정합니다.

참고: "모든 사용자" 옵션을 설정하면 "사용자 설정" 및 "고급" 섹션이 적용되지 않으며 더 이상 표시되지 않습니다.

6. "사용자 설정" 그룹 상자에서 사용자를 선택하여 역할의 구성원을 정의하는 그룹, 조직 및 사용자 특성 식을 정의합니다.
7. "확인"을 클릭합니다.
8. 필요한 각 추가 역할에 대해 2~7 단계를 반복합니다.

(선택 사항) 웹 응용 프로그램을 사용자 지정하도록 응답 구성

텍스트, 사용자 특성, DN 특성, 활성 응답 또는 정의된 변수의 런타임 값을 정책 서버에서 에이전트로 전달하도록 응답을 구성하십시오. 웹 응용 프로그램은 응답 데이터를 사용하여 사용자 지정된 콘텐츠를 표시하거나 세부적인 액세스 제어를 위한 권한을 결정할 수 있습니다. 응답 데이터는 SiteMinder 설정을 변경하거나 사용자를 다른 리소스로 리디렉션하는 데도 사용될 수 있습니다.

다음 단계를 수행하십시오.

1. "응용 프로그램 만들기" 페이지에서 "응답" 탭을 클릭합니다.
2. "응답 만들기"를 클릭합니다.
3. 응답의 이름을 입력합니다.

4. 하나 이상의 응답 특성을 생성합니다. 각 응답 특성에 대해 다음 단계를 수행합니다.
 - a. "응답 특성 만들기"를 클릭합니다.
 - b. 구성할 특성 유형을 선택합니다. 예를 들어 **WebAgent-HTTP-Header-Variable** 특성 유형을 선택합니다.
 - c. "특성 종류"를 선택합니다.
"특성 필드"의 상세 정보가 지정한 특성 종류에 맞게 업데이트됩니다.
 - d. "특성 필드"에서 상세 정보를 입력합니다.
 - e. (선택 사항) "스크립트" 필드에서 특성을 편집합니다.
참고: "고급" 섹션에서 특성을 편집할 경우 "특성 설정" 섹션이 닫힙니다.
 - f. "캐시 값"(기본값) 또는 "값 재계산 간격"(초)을 지정합니다.
참고: 입력할 수 있는 최대 시간 제한은 3600 초입니다.
 - g. "확인"을 클릭합니다.
응답 특성이 "특성 목록"에 추가됩니다.
5. "확인"을 클릭합니다.
응답이 생성됩니다.

(선택 사항) 웹 응용 프로그램을 사용자 지정하도록 응답 그룹 구성

하나의 개체에 여러 응답을 결합하려면 응답 그룹을 구성하십시오. 응용 프로그램 정책을 생성하면 여러 응답을 해당 정책 내의 단일 리소스에 보다 쉽게 연결할 수 있습니다.

다음 단계를 수행하십시오.

1. "응용 프로그램 만들기" 페이지에서 "응답" 탭을 클릭합니다.
2. "응답 그룹 만들기"를 클릭합니다.
3. 응답 그룹의 이름을 입력합니다.

4. "추가/제거"를 클릭합니다.

"응답 그룹 구성원" 페이지가 표시됩니다.

참고: "사용 가능한 구성원" 열에 응용 프로그램 개체에 정의된 모든 응답 및 응답 그룹이 나열됩니다.

5. "사용 가능한 구성원" 목록에서 응답 또는 응답 그룹을 하나 이상 선택하고 오른쪽 방향 화살표를 클릭합니다.

응답이 "사용 가능한 구성원" 목록에서 제거되고 "선택한 구성원" 목록에 추가됩니다.

참고: 한 번에 여러 구성원을 선택하려면 **Ctrl** 키를 누른 채 추가 구성원을 클릭하십시오. 구성원 블록을 선택하려면 첫 번째 구성원을 클릭한 다음 **Shift** 키를 누른 채 블록의 마지막 구성원을 클릭하십시오.

6. "확인"을 클릭합니다.

선택된 응답이 응답 그룹에 추가됩니다.

7. "확인"을 클릭합니다.

응답 그룹이 생성됩니다.

리소스를 사용자 역할과 연결하도록 정책 구성

각 리소스에 액세스할 수 있는 권한이 있는 사용자를 정의하려면 응용 프로그램 정책에서 리소스와 사용자 역할을 연결하십시오. 또한 리소스가 액세스될 때 권한 부여 에이전트에 데이터를 반환하려는 경우에는 정책에서 응답과 리소스를 연결하십시오.

다음 단계를 수행하십시오.

1. "응용 프로그램 만들기" 페이지에서 "정책" 탭을 클릭합니다.

"정책" 탭에는 두 개의 테이블이 있는데, 하나는 리소스 및 역할을 나열하고 다른 하나는 리소스 및 응답을 나열합니다.

2. 리소스 테이블에서 각 리소스와 연결할 역할을 선택합니다. 선택한 역할의 사용자에게만 해당 리소스에 액세스할 수 있는 권한이 부여됩니다.

3. 응답 테이블에서 각 리소스와 연결할 응답 및 응답 그룹을 선택합니다. 연결된 리소스가 액세스될 때 선택한 응답에 정의된 데이터가 반환됩니다.

참고: 역할/리소스 테이블 항목을 선택하기 전에는 응답 테이블에 응답이 표시되지 않습니다.

4. 제출을 클릭합니다.
확인 화면이 표시됩니다. 응용 프로그램 보안 정책이 생성됩니다.

(선택 사항) 고급 응용 프로그램 옵션 구성

응용 프로그램 보안 정책에 대해 다음과 같은 고급 옵션을 구성할 수도 있습니다.

- [사용자 지정 특성을 구성하여 메타데이터 추가](#) (페이지 514)
- [신뢰 수준 구성](#) (페이지 515)
- [CA DataMinder 콘텐츠 분류 구성](#) (페이지 516)
- [고급 정책 구성 요소 구성](#) (페이지 517)

(선택 사항) 사용자 지정 특성을 구성하여 응용 프로그램에 대한 메타데이터 추가

사용자 지정 특성을 정의하여 응용 프로그램에 대한 고유 식별 메타데이터를 추가할 수 있습니다. 메타데이터는 응용 프로그램을 생성한 사용자의 이름 또는 응용 프로그램의 용도와 같은 정보를 추가하여 응용 프로그램을 설명합니다.

다음 단계를 수행하십시오.

1. "응용 프로그램 만들기" 페이지에서 "사용자 지정 특성" 탭을 클릭합니다.
"사용자 지정 특성" 탭에는 기존 메타데이터의 이름과 값이 포함된 테이블이 표시됩니다.
2. "만들기"를 클릭합니다.
"사용자 지정 특성" 테이블에 빈 항목이 추가됩니다.
3. 추가할 메타데이터의 이름과 값을 입력합니다.

4. "만들기"를 클릭합니다.

사용자 지정 특성이 테이블에 추가되고 비어 있는 새 항목이 추가됩니다.

5. 추가할 각 사용자 지정 특성에 대해 3~4 단계를 반복합니다.

응용 프로그램에서 신뢰 수준 구성

SiteMinder 가 지원되는 위험 분석 엔진과 통합되는 경우 신뢰 수준을 응용 프로그램 개체에 사용할 수 있습니다. 신뢰 수준은 사용자 인증의 일부로 완료된 위험 평가의 결과를 포함하도록 응용 프로그램을 확장합니다. 정책 서버에서는 권한 부여 결정을 할 때 이러한 결과를 사용할 수 있습니다.

신뢰 수준을 다음 개체에 적용할 수 있습니다.

- 응용 프로그램 구성 요소

응용 프로그램 구성 요소에서 구성하는 신뢰 수준은 해당 구성 요소와 연결된 모든 리소스에 적용됩니다. 신뢰 수준은 기본적인 응용 프로그램 설정에서 제공하는 것보다 더 높은 수준의 세분성을 나타냅니다. 응용 프로그램 구성 요소의 고급 설정을 사용하여 신뢰 수준을 적용할 수 있습니다.

참고: 신뢰 수준을 응용 프로그램 구성 요소에 적용하려면 신뢰 수준 지원을 활성화해야 합니다. 자세한 내용은 *SiteMinder 구현 안내서*를 참조하십시오.

- 응용 프로그램 역할

응용 프로그램 역할의 일부로 구성하는 신뢰 수준을 통해 좀 더 세부적으로 권한 부여 결정을 내릴 수 있습니다. 신뢰 수준은 리소스에 액세스할 수 있는 사용자 그룹을 좀 더 자세하게 정의하는 데 사용할 수 있는 활성 구성 요소를 나타냅니다. 신뢰 수준은 기본적인 역할 구성원 자격이 제공하는 것보다 더 높은 수준의 세분성을 나타냅니다. 역할에 신뢰 수준을 추가하려면 `SM_USER_CONFIDENCE_LEVEL` SiteMinder 생성 특성을 참조하는 명명된 식을 사용하십시오.

참고: 신뢰 수준을 응용 프로그램에 적용하는 기능은 이전 릴리스부터 계속 지원되므로 기본적으로 활성화되어 있습니다.

응용 프로그램에 CA DataMinder 콘텐츠 분류 구성

SiteMinder 와 CA DataMinder 가 통합된 경우 응용 프로그램 개체에 콘텐츠 분류를 사용할 수 있습니다. 콘텐츠 분류는 사용자가 요청하는 콘텐츠 유형을 포함하도록 응용 프로그램을 확장합니다. 정책 서버는 CA DataMinder 콘텐츠 분석 결과에 따라 권한 부여를 결정할 수 있습니다.

참고: 응용 프로그램 구성 요소에 콘텐츠 분류를 적용하려면 사용 환경에서 CA DataMinder 통합이 사용되도록 설정해야 합니다. 자세한 내용은 *SiteMinder 구현 안내서*를 참조하십시오.

다음 개체에 CA DataMinder 콘텐츠 분류를 적용할 수 있습니다.

- 응용 프로그램 구성 요소:
 - 응용 프로그램 구성 요소에 적용하는 콘텐츠 분류는 해당 구성 요소와 연관된 모든 리소스에 적용됩니다.
 - 기본적으로 CA DataMinder Content Classification Service 는 응용 프로그램 구성 요소에 모든 콘텐츠 분류를 제공합니다. 정책 서버가 권한 부여를 결정할 때 하나 이상의 분류를 무시하도록 하려면 응용 프로그램에서 해당 분류를 제거하십시오.
 - SiteMinder 관리자는 콘텐츠 분류를 관리할 수 없습니다. 변경이 필요한 경우 CA DataMinder 관리자와 상의하여 변경하십시오.
- 응용 프로그램 역할:
 - 응용 프로그램 역할에 콘텐츠 분류를 적용하면 더 세부적으로 권한 부여를 결정할 수 있습니다. 콘텐츠 분류는 리소스에 액세스할 수 있는 하나 이상의 사용자 그룹을 추가로 정의하는 데 사용할 수 있는 활성 구성 요소를 나타냅니다. 콘텐츠 분류는 기본 역할 구성원 자격이 제공하는 상위 수준의 세분성을 나타냅니다.
 - 역할과 콘텐츠 분류 간의 관계는 누적 적용됩니다. 사용자가 동일한 응용 프로그램에서 여러 역할의 구성원일 경우 해당 역할과 연결된 모든 문서에 액세스할 수 있습니다.

응용 프로그램에 대한 고급 정책 구성 요소 구성

응용 프로그램 개체는 다음 유형의 사용자가 SiteMinder 구성 요소의 기본 설정을 수정할 수 있는 구성 옵션을 제공합니다.

- r12 이전의 SiteMinder 릴리스에서 사용되는 정책 디자인과 인터페이스에 익숙하고 정책의 여러 가지 측면을 세부적으로 조정하려는 사용자
- 정책에서 기본 설정이 제공하는 것보다 더 높은 수준의 세분성을 원하는 사용자
- 응용 프로그램 개체를 사용하여 구현한 정책이 조직의 요구 사항 또는 조직에서 준수해야 하는 규정을 충족하는지 여부를 결정하려는 감사자 및 기타 사용자

다음 단계를 수행하십시오.

1. "응용 프로그램"을 클릭합니다.
2. "응용 프로그램 만들기"를 클릭합니다.
3. "일반" 및 "구성 요소" 섹션에 정보를 입력하고 "고급 설정"을 클릭합니다.

"구성 요소 수정" 페이지가 표시됩니다. "구성 요소 수정" 페이지에는 정책 영역의 고급 기능 및 세션이 포함되어 있습니다. 예를 들어 신뢰 수준 지원이 사용되도록 설정한 경우 구성 요소에 최소 신뢰 수준을 추가할 수 있습니다.
4. 다음 단계 중 하나를 수행합니다.
 - 구성 요소에 대해 하나 이상의 고급 설정을 구성합니다.
 - 레거시 권한 부여 디렉터리 매핑을 선택합니다.
 - 하위 구성 요소를 생성하려면 "하위 구성 요소 만들기"를 클릭하여 "구성 요소 만들기" 화면을 엽니다. 하위 구성 요소를 만드는 작업은 하위 또는 중첩된 영역을 만드는 것과 같습니다.
5. 완료되면 "확인"을 클릭하여 변경 내용을 저장하고 응용 프로그램의 나머지 부분을 계속 구성합니다.

응용 프로그램 개체를 사용하여 응용 프로그램 보안 정책을 정의하기 위한 사용 사례

다음 사용 사례를 검토하여 응용 프로그램 개체를 통해 응용 프로그램 보안 정책을 정의하는 방법을 알아보십시오.

- [웹 포털 보호를 위한 응용 프로그램 보안 정책](#) (페이지 518)
- [역할 기반 응용 프로그램 보안 정책](#) (페이지 523)
- [사용자 매핑 및 명명된 식을 사용한 응용 프로그램 보안 정책](#) (페이지 531)
- [CA DataMinder 콘텐츠 분류 기반 응용 프로그램 보안 정책](#) (페이지 541)

웹 포털 보호를 위한 응용 프로그램 보안 정책

이 사용 사례에서 소프트웨어 회사인 **sample-software-company.com**에는 자사 및 자사 제품에 대한 정보를 대중에게 제공하는 웹 포털이 있습니다.

누구든지 제약 없이 기본 홈 페이지와 홍보 자료, 백서 등의 제품 정보 페이지에 액세스할 수 있습니다. 웹 포털의 이 영역에는 보안 정책이 필요하지 않습니다. 그러나 소프트웨어 다운로드 영역은 등록된 고객만 액세스할 수 있도록 제한됩니다. 각 고객에게는 LDAP 디렉터리 서버에 저장된 사용자 이름 및 암호가 할당됩니다.

다음 사용 사례에서는 등록된 고객만 액세스할 수 있도록 응용 프로그램 보안 정책으로 제한된 소프트웨어 다운로드 영역을 보호하는 방법을 보여줍니다.

상황:

- SiteMinder 환경에는 등록된 모든 고객에 대한 사용자 이름 및 암호가 저장되는 단일 LDAP 디렉터리 서버가 포함되어 있습니다.
- 고객이 소프트웨어 다운로드 영역에 액세스하려면 먼저 사용자 이름 및 암호로 인증해야 합니다.

해결책:

이 사용 사례를 해결하려면 다음 절차를 수행하십시오.

1. 보호가 필요한 웹 포털을 식별하고 고객 정보가 들어 있는 디렉토리를 선택합니다.
2. 포털의 소프트웨어 다운로드 영역에 대한 개별 리소스를 생성합니다.
3. 등록된 고객 역할을 생성합니다.
4. 등록된 고객 역할에 리소스를 연결하여 응용 프로그램 보안 정책을 생성합니다.

웹 포털 식별 및 사용자 디렉토리 선택

웹 포털에 대한 응용 프로그램 보안 정책에서는 보호할 리소스의 최상위 위치와 리소스 사용 권한이 있는 사용자의 디렉토리를 지정해야 합니다.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다. 자세한 내용은 "정책 서버 개체 복제"를 참조하십시오.

다음 단계를 수행하십시오.

1. "정책", "응용 프로그램"을 차례로 클릭합니다.
2. "응용 프로그램"을 클릭합니다.
"응용 프로그램" 페이지가 표시됩니다.
3. "응용 프로그램 만들기"를 클릭합니다.
"응용 프로그램 만들기" 페이지가 표시됩니다.
4. 응용 프로그램의 이름과 설명을 입력합니다. 다음 예에서처럼 용도나 기능을 기억하는 데 도움이 되는 고유 값을 제공합니다.

이름

샘플 소프트웨어 회사 포털

설명

다운로드 영역을 제외하고 포털의 모든 부분에 대한 액세스를 허용합니다.

5. "구성 요소"에 구성 요소의 이름을 제공하고 보호할 리소스가 포함된 디렉터리를 지정합니다. 이 웹 포털 사용 사례에서는 다음의 예를 사용합니다.

구성 요소 이름

다운로드

에이전트 유형

웹 에이전트

에이전트

포털 에이전트

리소스 필터

/downloads

참고: 하위 구성 요소는 주 구성 요소를 저장한 후에만 생성할 수 있습니다.

6. 나머지 설정은 기본값을 사용합니다.
7. "사용자 디렉터리"에서 "추가/제거"를 클릭합니다.
"사용자 디렉터리 선택" 페이지가 표시됩니다.
8. 해당 사용자가 포함된 디렉터리를 선택한 다음 오른쪽 화살표를 클릭하여 디렉터리를 "사용 가능한 구성원" 열에서 "선택한 구성원" 열로 이동합니다.
9. "확인"을 클릭합니다.
"일반" 탭으로 돌아갑니다.
10. 제출을 클릭합니다.
웹 포털 응용 프로그램이 식별되고 디렉터리가 선택됩니다.

웹 포털 리소스 만들기

리소스와 사용자 디렉터리의 위치를 지정한 후에는 보호할 웹 포털의 하위 디렉터리에 있는 개별 리소스를 지정해야 합니다.

다음 단계를 수행하십시오.

1. "리소스" 탭을 클릭합니다.
리소스 목록이 나타납니다.
2. "만들기"를 클릭합니다.
"응용 프로그램 리소스 만들기" 창이 열립니다.
3. "일반" 그룹 상자의 필드에 값을 입력합니다. 다음 예와 같이 용도나 기능을 쉽게 알아볼 수 있는 값을 선택합니다.

이름

다운로드 영역

설명

등록된 고객에게만 제공되는 소프트웨어 다운로드

리소스

*

4. "유효 리소스"가 보호할 항목과 일치하는지 확인합니다. 이 사용 사례의 경우 유효 리소스는 다음과 같습니다.

유효 리소스

/downloads/*

이 문자열은 **downloads** 디렉터리의 모든 리소스가 보호되도록 지정합니다.

5. 작업 그룹 상자의 "Web Agent Actions"(웹 에이전트 작업) 옵션 단추가 선택되어 있는지 확인하고 "작업" 목록에서 다음 항목을 클릭합니다.

■ Get

■ Post

6. "확인"을 클릭합니다.

웹 포털 리소스가 생성되어 리소스 목록에 표시됩니다.

웹 포털 역할 만들기

웹 포털 리소스를 지정한 후에는 웹 포털의 등록된 고객에게 적용할 역할을 생성하십시오. 역할은 리소스를 사용자 그룹과 연결합니다.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다. 자세한 내용은 "정책 서버 개체 복제"를 참조하십시오.

다음 단계를 수행하십시오.

1. "역할" 탭을 클릭합니다.
2. "역할 만들기"를 클릭합니다.
3. "Create a new object of type Role"(역할 유형의 새 개체 만들기) 단추가 선택되어 있는지 확인하고 "확인"을 클릭합니다.
"역할 만들기" 창이 열립니다.
4. "일반" 그룹 상자의 필드에 값을 입력합니다. 다음 예와 같이 용도나 기능을 쉽게 알아볼 수 있는 값을 선택합니다.

이름

등록된 고객

설명

소프트웨어 다운로드에 액세스할 수 있는 등록된 고객

역할 적용 대상

모든 사용자

참고: 이 옵션을 설정하면 "사용자 설정" 및 "고급" 그룹 상자가 적용되지 않으며 더 이상 표시되지 않습니다.

5. "확인"을 클릭합니다.
등록된 고객 역할이 생성됩니다.

웹 포털 정책 만들기

리소스 및 역할을 생성한 후에는 보호할 웹 포털의 리소스를 웹 포털의 리소스에 액세스할 사용자의 역할과 연결하십시오. 이렇게 하면 응용 프로그램을 보호하는 정책이 생성됩니다.

다음 단계를 수행하십시오.

1. "정책" 탭을 클릭합니다.
2. "Software Downloads"(소프트웨어 다운로드) 행의 "Registered Customers"(등록된 고객) 역할을 선택합니다.
이 역할을 선택하면 등록된 고객만 웹 포털의 소프트웨어 다운로드 영역에 액세스할 수 있도록 지정됩니다.
3. 제출을 클릭합니다.
확인 화면이 표시됩니다. 웹 포털에 대한 응용 프로그램 보안 정책이 생성되었습니다.

리소스 목록 표시

다음 라디오 단추 중 하나를 클릭하여 표시되는 리소스 목록을 정렬할 수 있습니다.

이름

리소스를 지정할 때 제공한 이름에 따라 리소스를 정렬합니다.

예: 소프트웨어 다운로드

Filter

보호할 실제 리소스에 따라 리소스를 정렬합니다.

예: *(별표는 모든 리소스를 나타냄)

역할 기반 응용 프로그램 보안 정책

이 사용 사례에서는 `acme-financial.com` 이라는 금융 서비스 회사에 복리 후생 및 성과 관리를 처리하는 내부 인사 응용 프로그램이 있다고 가정합니다. 이 응용 프로그램의 복리 후생 부분은 모든 직원이 액세스할 수 있지만 성과 관리 부분은 관리자에게만 액세스가 허용됩니다.

다음 절차에서는 EPM 모델을 응용 프로그램 역할과 함께 사용하여 인사 응용 프로그램의 보안 정책을 생성하는 방법을 자세히 설명합니다.

상황:

- SiteMinder 환경에 AcmeLDAP 라는 사용자 LDAP 디렉터리가 하나 있습니다.
- 이 사용자 디렉터리는 모든 직원과 관리자인 직원을 식별합니다. 이러한 직원은 디렉터리에 다음과 같이 정의되어 있습니다.
 - group:cn=employees,ou=Groups,o=acme-financial.com
 - group:cn=managers,ou=Groups,o=acme-financial.com
- 관리자를 포함한 직원은 기본 인증 체계를 사용하여 인증되어야 합니다.

역할 기반 응용 프로그램 보안을 위한 해결책:

이 사용 사례를 해결하려면 다음 단계를 완료하십시오.

1. 응용 프로그램을 생성합니다.
2. 역할 조건을 충족하는 사용자를 배치할 사용자 디렉터리를 선택합니다.
3. 주 응용 프로그램의 하위 구성 요소인 리소스를 지정합니다.
4. 응용 프로그램에 대한 액세스 권한이 필요한 역할을 두 개 정의합니다.
5. 리소스와 역할을 응용 프로그램 정책에 결합합니다.

보호가 필요한 응용 프로그램 식별

이 사용 사례에서는 인사 관리 응용 프로그램의 여러 부분에 대해 서로 다른 액세스 권한을 설정합니다. 이를 위해서는 기본 응용 프로그램 아래의 디렉터리를 식별하고 적절한 액세스 권한을 구성합니다.

예제 인사 관리 응용 프로그램을 보호하려면

1. "정책", "응용 프로그램"을 차례로 클릭합니다.
2. "응용 프로그램"을 클릭합니다.
"응용 프로그램" 페이지가 표시됩니다.
3. "응용 프로그램 만들기"를 클릭합니다.
"응용 프로그램 만들기" 페이지가 표시됩니다.
4. "일반" 탭을 클릭합니다.

5. "일반"에서 다음 필드의 값을 입력합니다. 이 사용 사례에서는 다음 데이터를 지정합니다.

이름

HR 응용 프로그램

설명

내부 인사 관리 응용 프로그램을 식별합니다.

6. "구성 요소"에 다음 필드의 값을 입력합니다. 이 사용 사례에서는 다음 데이터를 지정합니다.

구성 요소 이름

혜택

에이전트 유형

웹 에이전트

에이전트

hrportal 에이전트

리소스 필터

/benefits

기본 리소스 보호

보호됨

인증 체계

기본

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

참고: 하위 구성 요소는 주 구성 요소를 저장한 후에만 생성할 수 있습니다.

7. 보호되는 리소스와 연결된 사용자 디렉터리를 지정합니다.
SiteMinder에서는 역할 조건과 일치하는 사용자를 이 디렉터리에서 찾습니다.
 - a. "추가/제거"를 클릭합니다.
 - b. "사용 가능한 구성원" 상자에서 "Employees"(직원)를 선택하고 오른쪽 화살표를 클릭하여 이 그룹을 "선택한 구성원" 상자로 이동합니다.
 - c. "확인"을 클릭합니다.

이제 인사 관리 응용 프로그램이 식별됩니다.

응용 프로그램 리소스 지정

보호할 기본 응용 프로그램의 하위 영역을 지정한 후에는 해당 하위 디렉터리 내에서 응용 프로그램 정책으로 보호할 특정 리소스를 지정할 수 있습니다.

이 사용 사례에서는 다음 두 개의 리소스를 보호합니다.

- 복리 후생 관리
- 성과 평가

기본 응용 프로그램의 특정 리소스 또는 기능을 지정하려면

1. "리소스" 탭을 클릭합니다.
2. "만들기"를 클릭합니다.
"리소스" 창이 열립니다.
3. "일반" 그룹 상자의 필드에 값을 입력합니다. 이 사용 사례에서는 다음 값을 입력하십시오.

이름

복리 후생 관리

설명

직원이 자신의 복리 후생을 관리할 수 있음

4. "특성" 그룹 상자의 필드에 값을 입력합니다. 이 사용 사례에서는 다음 값을 입력하십시오.

리소스

managebenefits.jsp

5. 2~4 단계를 반복하되 다음 정보를 입력합니다.

이름

성과 평가

설명

관리자가 직원에 대한 평가 보고서 및 연봉 협상안을 작성할 수 있음

리소스

salaryincrease.jsp

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

이제 성과 관리 응용 프로그램과 연결된 리소스가 정의되었습니다.

직원 역할 만들기

보호가 필요한 응용 프로그램의 특정 구성 요소를 정의한 후에는 특정 리소스에 대한 액세스 권한이 있는 사용자 집합을 정의하는 역할을 지정하십시오. 모든 직원에게 적용할 역할을 생성하십시오.

다음 단계를 수행하십시오.

1. "역할" 탭을 클릭합니다.
2. "역할 만들기"를 클릭합니다.
"역할 만들기" 창이 나타납니다.
3. "만들기" 옵션이 선택되어 있는지 확인하고 "확인"을 클릭합니다.

4. "일반" 그룹 상자의 필드에 값을 입력합니다. 이 사용 사례에서는 다음 값을 입력하십시오.

이름

Employees

설명

Acme Financial Services 의 모든 직원

역할 적용 대상

모든 사용자

참고: 이 옵션을 설정하면 "사용자 설정" 및 "고급" 그룹 상자가 적용되지 않으며 더 이상 표시되지 않습니다.

5. "확인"을 클릭합니다.

관리자 역할 만들기

보호가 필요한 응용 프로그램의 특정 구성 요소를 정의한 후에는 특정 리소스에 대한 액세스 권한이 있는 사용자 집합을 정의하는 역할을 지정하십시오. 관리자용 역할을 생성하십시오.

다음 단계를 수행하십시오.

1. "역할" 탭을 클릭합니다.
2. "만들기"를 클릭합니다.
"역할 만들기" 창이 나타납니다.
3. "만들기" 옵션이 선택되어 있는지 확인하고 "확인"을 클릭합니다.
4. "일반" 그룹 상자의 필드에 값을 입력합니다. 이 사용 사례에서는 다음 값을 입력하십시오.

이름

Managers

설명

Acme Financial Services 의 관리자

역할 적용 대상

선택한 사용자

5. "역할 적용 대상" 옵션이 "선택한 사용자"로 선택되어 있고 "사용자 설정" 및 "고급" 그룹 상자가 표시되는지 확인합니다.

6. "사용자 설정" 그룹 상자에서 사용자를 선택하여 관리자 역할의 사용자 집합을 정의합니다. 이 사용 사례에서는 "구성원 그룹" 테이블에서 다음 항목을 선택합니다.

`cn=managers,ou=Groups,o=acme-financial.com`

이 항목은 회사 사용자 디렉터리에 있는 관리자 그룹을 지정합니다.

7. "확인"을 클릭합니다.

응답을 사용하여 응용 프로그램에 데이터 제공

Acme Financial Services 직원에 대한 인사 응용 프로그램을 보다 편리하게 사용할 수 있도록 직원의 복리 후생 레코드에 직원 ID 를 제공하는 응답을 구성할 수 있습니다.

직원 ID 를 제공하는 응답을 생성하려면

1. "응용 프로그램 응답" 대화 상자를 클릭합니다.
2. "응답 만들기"를 클릭합니다.
"응답 만들기" 대화 상자가 열립니다.
3. 다음과 같이 필드에 데이터를 입력합니다.

이름

직원 ID

설명

직원 ID 를 나열합니다.

4. "응답 특성 만들기"를 클릭합니다.
"응답 특성 만들기" 대화 상자가 열립니다.
5. 다음과 같이 필드에 데이터를 입력합니다.

특성

WebAgent-HTTP-Header-Variable

특성 종류

사용자 특성

특성 필드-변수 이름

Personnel_Key

특성 필드-변수 값

EmployeeID

6. 다른 모든 필드의 경우 기본값을 그대로 둡니다.
7. 기본 "응답" 탭으로 돌아갈 때까지 "확인"을 계속 클릭합니다.

직원 ID 응답이 생성되었습니다. 직원이 자신의 복리 후생 정보를 볼 때 이 응답의 데이터가 인사 응용 프로그램에 반환되고 이 직원의 복리 후생 레코드에 해당 고객 ID 가 표시됩니다.

역할 기반 정책 설정

리소스 및 역할을 정의한 후에는 이러한 개체를 응용 프로그램 보안 정책으로 그룹화할 수 있습니다.

다음 단계를 수행하십시오.

1. "정책" 탭을 클릭합니다.
"정책" 창이 열리고 구성된 리소스 및 역할이 나열된 표가 표시됩니다. 이 표를 사용하여 어떤 역할에 어떤 리소스에 대한 액세스 권한을 부여할 수 있는지 빠르게 확인할 수 있습니다.
2. 다음 단계를 수행하십시오.
 - a. 모든 직원이 자신의 복리 후생을 관리하도록 허용하는 정책을 만들려면 "복리 후생 관리" 행에서 "직원" 역할을 선택하십시오.
 - b. 관리자만 성과 평가에 액세스하도록 허용하는 정책을 만들려면 "성과 평가" 행에서 "관리자" 역할을 선택하십시오.
3. 제출을 클릭합니다.

인사 응용 프로그램에 대해 역할을 기반으로 하는 두 개의 보안 정책을 생성했습니다.

참고: 리소스 또는 역할을 편집하려면 "정책" 창이 아니라 해당하는 탭에서 변경 작업을 수행하십시오.

응용 프로그램을 설명하는 메타데이터 포함

Acme-financial.com에서는 내부 인사 응용 프로그램에 대한 설명 정보를 제공하려고 합니다. 사용자 지정 특성을 사용하여 응용 프로그램을 설명하는 메타데이터를 정의할 수 있습니다.

Acme-financial에서 원하는 정보는 응용 프로그램과 응용 프로그램이 완료된 날짜입니다.

다음 단계를 수행하십시오.

1. "사용자 지정 특성" 탭을 클릭합니다.
"사용자 지정 특성" 대화 상자가 열립니다.
2. "만들기"를 클릭합니다.
"이름" 및 "값" 필드가 포함된 표가 나타납니다.
3. 사용자 지정 특성 표의 필드에 값을 입력합니다. 이 사용 사례에서는 다음 값을 입력하십시오.

이름

App_Completed

값

2007_11_22

4. "만들기"를 클릭하여 표에 행을 하나 더 추가하고 다음 값을 입력합니다.

이름

용도

값

Human_Resource_Mgmt

5. 제출을 클릭합니다.

사용자 매핑 및 명명된 식을 사용한 응용 프로그램 보안 정책

이 사용 사례에서는 한 소매 의류업체가 고객이 신용 한도를 초과한 경우 웹에서 신용 구매를 할 수 없도록 하는 역할을 정의하려고 한다고 가정합니다. 회사 정책에 고객의 신용 한도는 1,000 달러로, 직원의 신용 한도는 2,000 달러로 명시되어 있습니다.

특성 매핑, 명명된 식(가상 사용자 특성 및 사용자 클래스) 및 역할을 사용하여 회사 신용 정책을 충족하는 응용 프로그램 보안 정책을 생성할 수 있습니다.

상황:

- SiteMinder 환경에 사용자 디렉터리가 두 개 있습니다.
- 디렉터리 A에는 직원이 저장됩니다. 직원은 고객이 될 수도 있습니다. 따라서 디렉터리 A는 직원이면서 동시에 다음에 속하는 고객을 식별합니다.

`group:cn=Customers,ou=Groups,o=acme.com`

- 디렉터리 B에는 고객만 저장됩니다. 디렉터리 B에는 고객을 식별하는 사용자 특성이 없는데, 디렉터리 B에 사용자를 저장한다는 것은 사용자가 곧 고객임을 의미하기 때문입니다.

해결책:

1. 특성 매핑을 정의합니다.
2. 명명된 식을 작성합니다.
3. 고급 식에 특성 매핑을 사용하여 역할을 설정합니다.
4. 응답을 생성하여 응용 프로그램을 추가로 사용자 지정합니다.
5. 응용 프로그램 보안 정책을 생성합니다.

두 개의 사용자 디렉터리에 대한 매핑 설정

이 소매업체에서는 두 개의 디렉터리를 유지 관리합니다. 두 사용자 디렉터리 모두에서 고객을 식별하는 유니버설 체계를 생성하려면 관리 UI에서 생성하는 특성 매핑을 사용하십시오.

이 사용 사례에 대한 특성 매핑을 생성하려면

1. 디렉터리 A에 대한 그룹 구성원 자격 특성을 생성합니다.
 - 특성 이름을 **IsCustomer**로 지정합니다.
 - IsCustomer를 cn=Customers,ou=Groups,o=acme.com으로 정의합니다.
2. 디렉터리 B에 대한 상수 특성을 생성합니다.
 - 특성 이름을 **IsCustomer**로 지정합니다.
 - IsCustomer를 **"TRUE"**로 정의합니다.

IsCustomer를 사용하면 동일한 사용자 정보의 공통 보기가 생성됩니다. 식에서 IsCustomer를 참조하여 사용자가 고객인지 여부를 확인할 수 있습니다.

특성 매핑을 구성하는 방법에 대한 자세한 내용은 [특성 매핑 정의](#) (페이지 248) 단원을 참조하십시오.

명명된 식을 정의하여 신용 한도 확인

SiteMinder는 명명된 식을 사용하여 각 사용자의 신용 한도와 계정 잔액을 계산할 수 있습니다. 식으로 고객의 신용 한도가 초과되었는지 여부도 확인할 수 있습니다.

이 사용 사례에 대한 명명된 식을 정의하려면

1. 고객과 직원의 신용 한도를 각각 1,000 달러와 2,000 달러로 계산하는 가상 사용자 특성을 정의합니다.
 - 특성 이름을 **#CreditLimit**로 지정합니다.
 - #CreditLimit를 다음과 같이 정의합니다.

`IsCustomer?1000:2000`

이 계산에는 SiteMinder에서 지원되는 식 구문이 포함되어 있습니다.

- 계정 데이터베이스에서 계정 잔액을 검색하는 가상 사용자 특성을 정의합니다.

- 특성 이름을 **#Balance** 로 지정합니다.
- 이 특성을 다음과 같이 정의합니다.

```
(MyLibrary.GetBalance(""))
```

이 특성 정의는 의류 소매업체에서 정의한 활성 식입니다.

- 고객의 신용 한도가 초과되었는지 여부를 확인하는 사용자 클래스 식을 생성합니다.

- 특성 이름을 **@IsUnderCreditLimit** 로 지정합니다.
- 이 특성을 다음과 같이 정의합니다.

```
(#Balance > #CreditLimit)
```

가상 사용자 특성 및 사용자 클래스 식 생성에 대한 자세한 내용은 [명명된 식 정의](#) (페이지 229) 단원을 참조하십시오.

온라인 쇼핑 응용 프로그램 보호

이 사용 사례에서는 웹 기반 쇼핑 응용 프로그램에 대해 특정 조건이 적용되는 액세스 권한을 설정하고자 합니다.

웹 기반 쇼핑 응용 프로그램을 보호하려면

- "정책", "응용 프로그램"을 차례로 클릭합니다.
- "응용 프로그램"을 클릭합니다.
"응용 프로그램" 페이지가 표시됩니다.
- "응용 프로그램 만들기"를 클릭합니다.
"응용 프로그램 만들기" 페이지가 표시됩니다.
- "일반" 탭을 클릭합니다.
- 다음 필드의 값을 입력합니다. 이 사용 사례에서는 다음 데이터를 지정합니다.

이름

온라인 카탈로그

설명

의류 상점 웹 기반 쇼핑 응용 프로그램을 식별합니다.

6. "구성 요소"에 다음 필드의 값을 입력합니다. 이 사용 사례에서는 다음 데이터를 지정합니다.

구성 요소 이름

카탈로그

에이전트 유형

웹 에이전트

에이전트

웹 소매 에이전트

리소스 필터

/webcatalog

기본 리소스 보호

보호됨

인증 체계

기본

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

참고: 하위 구성 요소는 주 구성 요소를 저장한 후에만 생성할 수 있습니다.

7. 보호되는 리소스와 연결된 사용자 디렉터리를 지정합니다.
SiteMinder에서는 역할 조건과 일치하는 사용자를 이 디렉터리에서 찾습니다.
- "추가/제거"를 클릭합니다.
 - "사용 가능한 구성원" 상자에서 **IsCustomer** 를 선택하고 오른쪽 화살표를 클릭하여 이 그룹을 "선택한 구성원" 상자로 이동합니다.

IsCustomers 가 의류 상점과 연결된 두 디렉터리 모두의 사용자에게 매핑됩니다.
 - 제출을 클릭합니다.

이제 온라인 카탈로그라는 응용 프로그램을 생성했습니다.

보호가 필요한 리소스 지정

이 사용 사례에서는 신용 한도를 초과하는 사용자는 거래를 마칠 수 없도록 결제 프로세스를 보호하고자 합니다. 따라서 앞서 만든 온라인 카탈로그 응용 프로그램에 리소스를 추가하십시오.

웹 기반 쇼핑 응용 프로그램의 특정 리소스를 보호하려면

1. "정책", "응용 프로그램"을 차례로 클릭합니다.
2. "응용 프로그램"을 클릭합니다.
"응용 프로그램" 페이지가 표시됩니다.
3. 검색 조건을 지정하고 "검색"을 클릭합니다.
조건과 일치하는 응용 프로그램이 표시됩니다.
4. 수정할 응용 프로그램의 이름을 클릭합니다. 이 사용 사례에서는 "온라인 카탈로그"를 클릭합니다.
"응용 프로그램 보기" 페이지가 표시됩니다.
5. 페이지를 아래로 스크롤하고 "수정"을 클릭합니다.
설정과 컨트롤이 활성화됩니다.
6. "리소스" 탭을 선택합니다.
7. "만들기"를 클릭합니다.
"리소스 만들기" 페이지가 표시됩니다.
8. 다음 필드의 값을 입력합니다. 이 사용 사례에서는 다음 값을 입력하십시오.

이름

결제

설명

구입 총액을 계산하고 결제할 수 있습니다.

9. "특성"에서 다음 필드의 값을 입력합니다. 이 사용 사례에서는 다음 값을 입력하십시오.

리소스

`total_charges.jsp`

10. "작업"에서 웹 에이전트 작업을 선택하고 **Get** 및 **Post** 작업을 선택합니다.
11. "확인"을 클릭합니다.

Checkout 이라는 리소스를 생성했습니다.

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

고객 역할 구성

웹 포털 리소스를 정의했으면 고객이 신용 한도를 초과하지 않는 한 웹 기반 구매를 할 수 있도록 하는 응용 프로그램 역할을 생성하십시오.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다. 자세한 내용은 "정책 서버 개체 복제"를 참조하십시오.

이 신용 기반 역할을 생성하려면

1. "역할" 탭을 클릭합니다.
2. "역할 만들기"를 클릭합니다.
"역할 만들기" 대화 상자가 나타납니다.
3. "만들기" 옵션이 선택되어 있는지 확인하고 "확인"을 클릭합니다.
"역할 만들기" 대화 상자가 열립니다.

4. "일반" 그룹 상자의 필드에 값을 입력합니다. 이 사용 사례에서는 다음 값을 입력하십시오.

이름

PurchasewithCredit

설명

고객이 구매 시 신용으로 결제한다는 것을 나타냅니다.

역할 적용 대상

선택한 사용자

5. "Advanced Expression"(고급 식) 그룹 상자에 식을 입력합니다. 이 사용 사례에서는 다음을 입력합니다.

사용자 식

@IsUnderCreditLimit

역할 식은 두 가상 사용자 특성 식인 #Balance 와 #CreditLimit 를 함께 사용하여 사용자가 신용 한도를 초과했는지 여부를 계산합니다.

6. "확인"을 클릭합니다.

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

두 명명된 식을 조합한 결과 값을 갖는 PurchasewithCredit 이라는 역할을 생성했습니다.

응답을 사용하여 응용 프로그램 사용자 지정

이 소매 의류업체에서는 고객에게 보다 개인화된 환경을 제공하기 위해 신용 한도가 초과된 고객이 신용 한도 증액을 신청할 수 있도록 하는 응답을 구성할 수 있습니다. 고객의 신용 한도가 초과된 경우 이 응답은 신용 한도 증액을 신청할 수 있는 신용 응용 프로그램으로 고객을 리디렉션합니다.

응답을 생성하려면

1. "응답" 탭을 클릭합니다.

2. "응답 만들기"를 클릭합니다.

"응답 만들기" 대화 상자가 열립니다.

3. 다음과 같이 필드에 데이터를 입력합니다.

이름

CreditNotice

설명

신용 한도가 초과되었음을 사용자에게 알립니다.

4. "응답 특성 만들기"를 클릭합니다.
"응답 특성 만들기" 대화 상자가 열립니다.
5. 필드 및 설정 값을 다음과 같이 입력합니다.

특성

WebAgent-OnReject-Redirect

특성 종류

정적

특성 필드-변수 값

http://catalog.retailcorp.com/credit_notice.jsp

6. 다른 모든 필드의 경우 기본값을 그대로 둡니다.
7. "확인"을 클릭합니다.

CreditNotice 라는 응답이 생성되었으며 이제 신용 한도가 초과된 고객에게는 이 응답이 보내집니다.

쇼핑 응용 프로그램에 대한 보안 정책 구성

리소스, 역할 및 응답을 정의한 후에는 웹 기반 쇼핑 응용 프로그램을 보호하는 정책을 구성하십시오.

다음 단계를 수행하십시오.

1. "정책" 탭을 클릭합니다.
"정책" 대화 상자가 열리고 표에 Checkout 리소스와 PurchaseWithCredit 역할이 표시됩니다.
2. Checkout 리소스에 대해 PurchaseWithCredit 역할을 선택합니다.
이 쌍은 신용 한도가 초과되지 않은 한 모든 고객이 해당 상점의 신용카드를 사용하여 구매할 수 있도록 하는 정책을 설정합니다. 또한 역할을 선택하면 응답 표가 채워집니다.

3. Checkout 리소스에 대해 CreditNotice 응답을 선택합니다.

이제 지출 제한을 정의하는 역할을 기반으로 온라인 카탈로그 응용 프로그램에 대한 보안 정책이 생성되었습니다. 또한 응답이 정책과 연결되어 한도 초과 후에도 계속 구매하는 고객에게 이 응답이 보내집니다.

응용 프로그램을 설명하는 메타데이터 제공

소매 의류업체에서 온라인 카탈로그 응용 프로그램에 대한 설명 정보를 제공하려고 합니다. 사용자 지정 특성을 사용하여 응용 프로그램을 설명하는 메타데이터를 제공할 수 있습니다.

이 소매 의류업체에서는 응용 프로그램이 온라인 카탈로그 전용임을 알리고 응용 프로그램 관리자의 전자 메일 주소를 표시하려고 합니다.

온라인 카탈로그 응용 프로그램에 대한 메타데이터를 지정하려면

1. "사용자 지정 특성" 탭을 클릭합니다.
"사용자 지정 특성" 대화 상자가 열립니다.
2. "만들기"를 클릭합니다.
"이름" 및 "값" 필드가 포함된 표가 나타납니다.
3. 사용자 지정 특성 표의 필드에 값을 입력합니다. 이 사용 사례에서는 다음 값을 입력하십시오.

이름

App_Function

값

online_retail

4. "만들기"를 클릭하여 표에 행을 하나 더 추가하고 다음 값을 입력합니다.

이름

Admin_email

값

jdoe@retailcorp.com

5. 제출을 클릭합니다.

응용 프로그램 보안 정책을 생성하는 데 관련된 사용 가능한 모든 태스크를 완료했습니다.

CA DataMinder 콘텐츠 분류 기반 응용 프로그램 보안 정책

이 사용 사례에서는 Forward Inc.라는 금융 서비스 회사가 Microsoft SharePoint 를 배포했습니다. 이 회사는 다음을 수행하려고 합니다.

- 모든 직원에게 SharePoint 에 대한 액세스 권한을 제공합니다.
- 직원 보상 정보가 포함된 문서에 대한 액세스를 제한합니다. 인사 부서의 직원만 직원 보상 정보가 포함된 문서에 액세스할 수 있습니다.

참고: Forward, Inc.는 설명용으로만 사용되는 가상의 회사 이름으로, 실제 회사를 가리키지 않습니다.

다음은 CA DataMinder 콘텐츠 분류가 포함된 응용 프로그램을 구성하여 직원 보상 정보를 보호하는 보안 정책을 만드는 자세한 방법입니다.

상황:

- SiteMinder 환경에 LDAP 사용자 디렉터리가 하나 있습니다. 디렉터리 이름은 ForwardLDAP 입니다.
- 사용자 디렉터리는 인사 부서의 직원을 포함한 모든 직원을 식별합니다. 사용자 디렉터리는 다음과 같이 인사 부서 직원을 식별합니다.
`cn=human resources,o=forwardinc.com`
- 모든 직원은 기본 인증 체계를 사용하여 인증해야 합니다.
- 단일 SharePoint 사이트가 배포되었습니다.
 - SharePoint 사이트의 루트 URL 은 다음과 같습니다.
`usecase.forwardinc.com/SitePages/Home.aspx`
 - Shared Documents 디렉터리의 URL 은 다음과 같습니다.
`usecase.forwardinc.com/Shared Documents`

해결책:

1. Shared Documents 디렉터리를 보호합니다.
2. 모든 문서 리소스를 보호합니다.
3. Human Resources 역할을 생성합니다.
4. Human Resources 역할을 기반으로 하는 정책을 설정합니다.

Shared Documents 디렉터리 보호

이 사용 사례에서는 SharePoint 환경에서 보호하려고 하는 최상위 지점이 Shared Documents 디렉터리입니다. SharePoint 사이트(usecase.forwardinc.com/SitePages/Home.aspx)는 모든 직원이 액세스할 수 있도록 보호되지 않은 상태로 둡니다.

다음 단계를 수행하십시오.

1. "정책", "응용 프로그램"을 차례로 클릭합니다.
2. "응용 프로그램"을 클릭합니다.
3. "응용 프로그램 만들기"를 클릭합니다.
4. "DLP 서버 사용"을 선택합니다.
5. "일반" 섹션에서 필요한 값을 입력합니다. 이 사용 사례에서는 다음 데이터를 지정합니다.

이름

SharePoint 사이트

6. "구성 요소" 섹션에 필요한 값을 입력합니다. 이 사용 사례에서는 다음 데이터를 지정합니다.

구성 요소 이름

Shared Documents

에이전트

SharePoint

리소스 필터

[/usecase.forwardinc.com/Shared Documents](http://usecase.forwardinc.com/Shared Documents)

7. "사용자 디렉터리" 섹션에서 "추가/제거"를 클릭하여 응용 프로그램 정책에서 사용할 수 있는 모든 사용자 디렉터리의 목록을 표시합니다.
8. 사용자 디렉터리를 선택하고 "확인"을 클릭합니다. 이 사용 사례에서는 다음 사용자 디렉터리를 지정합니다.

ForwardLDAP

9. "DLP 분류" 섹션에서 구성 요소에 추가하지 않을 콘텐츠 분류가 있으면 제거합니다. 이 사용 사례에서는 분류를 제거하지 마십시오.
10. "제출"을 클릭하여 응용 프로그램을 저장합니다.

모든 문서 리소스 보호

이 사용 사례에서는 Shared Documents 디렉터리의 모든 문서를 보호하려고 합니다. 응용 프로그램에 리소스를 추가하여 모든 문서 리소스를 보호합니다.

다음 단계를 수행하십시오.

1. "정책", "응용 프로그램"을 차례로 클릭합니다.
2. "응용 프로그램"을 클릭합니다.
3. 검색 조건을 지정하고 "검색"을 클릭합니다.
4. 수정할 응용 프로그램을 식별하고 수정 아이콘을 클릭합니다. 이 사용 사례에서는 다음 응용 프로그램을 수정합니다.

SharePoint 사이트

5. "리소스" 탭을 선택하고 "만들기"를 클릭합니다.
6. 다음 필드의 값을 입력합니다. 이 사용 사례에서는 다음 값을 입력하십시오.

이름

모든 문서

리소스

/*

7. 규칙이 실행되기 위해 발생해야 하는 이벤트 유형 및 작업을 선택합니다. 이 사용 사례에서는 다음 이벤트 유형을 선택하십시오.
 - 웹 에이전트 작업
 - Connect
 - Delete
 - Get
 - Head
 - Options
 - Post
 - Put
 - Trace

8. "확인"을 클릭하여 리소스를 저장합니다.
9. "제출"을 클릭하여 리소스를 구성 요소에 추가합니다.

Human Resources 역할 만들기

이 사용 사례에서는 인사 부서 직원만 보상 정보가 포함된 문서에 액세스할 수 있도록 하는 역할을 생성하려고 합니다.

다음 단계를 수행하십시오.

1. "정책", "응용 프로그램"을 차례로 클릭합니다.
2. "응용 프로그램"을 클릭합니다.
3. 검색 조건을 지정하고 "검색"을 클릭합니다.
4. 수정할 응용 프로그램을 식별하고 수정 아이콘을 클릭합니다. 이 사용 사례에서는 다음 응용 프로그램을 수정합니다.

SharePoint 사이트

5. "역할" 탭을 선택하고 "역할 만들기"를 클릭합니다.
6. 다음 옵션을 선택합니다.

Create a new object of type role(역할 유형의 새 개체 만들기)

7. "확인"을 클릭합니다.
8. "일반" 섹션에 값을 입력합니다. 이 사용 사례에서는 다음 값을 입력하십시오.

이름

Human Resources

설명

직원 보상 정보가 포함된 문서에 액세스할 수 있는 역할

9. 역할을 사용 가능한 디렉터리의 모든 사용자에게 적용할지, 특정 사용자에게 적용할지를 지정합니다. 이 사용 사례에서는 다음 옵션을 선택합니다.

선택한 사용자

10. "사용자 설정" 섹션에서 역할 구성원을 정의합니다. 이 사용 사례에서는 "구성원 그룹" 섹션에서 다음 조직을 선택합니다.

cn=human resources,o=forwardinc.com

11. "DLP 분류" 섹션에서 역할에 콘텐츠 분류를 추가합니다. 이 사용 사례에서는 다음 값을 선택하십시오.
 - US Employee Compensation Information(영국 직원 보상 정보)
 - UK Employee Compensation Information(영국 직원 보상 정보)
12. "확인"을 클릭하여 역할을 저장합니다.
13. "제출"을 클릭하여 역할을 응용 프로그램에 추가합니다.

Human Resources 역할을 기반으로 하는 정책 설정

이 사용 사례에서는 직원 보상 정보가 포함된 문서를 보호하는 정책을 생성하려고 합니다.

다음 단계를 수행하십시오.

1. "정책", "응용 프로그램"을 차례로 클릭합니다.
2. "응용 프로그램"을 클릭합니다.
3. 검색 조건을 지정하고 "검색"을 클릭합니다.
4. 수정할 응용 프로그램을 식별하고 수정 아이콘을 클릭합니다. 이 사용 사례에서는 다음 응용 프로그램을 수정합니다.

SharePoint 사이트

5. "정책" 탭을 선택합니다.
6. "모든 문서" 리소스에 대해 "Human Resources" 역할을 선택합니다.
7. "제출"을 클릭합니다.

인사 부서 직원만 직원 보상 정보가 포함된 SharePoint 문서에 액세스할 수 있도록 하는 정책이 생성됩니다.

제 12 장: 도메인

이 섹션은 다음 항목을 포함하고 있습니다.

[정책 도메인 개요](#) (페이지 547)

[도메인 및 사용자 구성원](#) (페이지 549)

[정책 도메인을 구성하는 방법](#) (페이지 549)

[도메인에 CA Identity Manager 환경 추가](#) (페이지 553)

[도메인에 대한 전역 정책 처리가 사용되지 않도록 설정](#) (페이지 554)

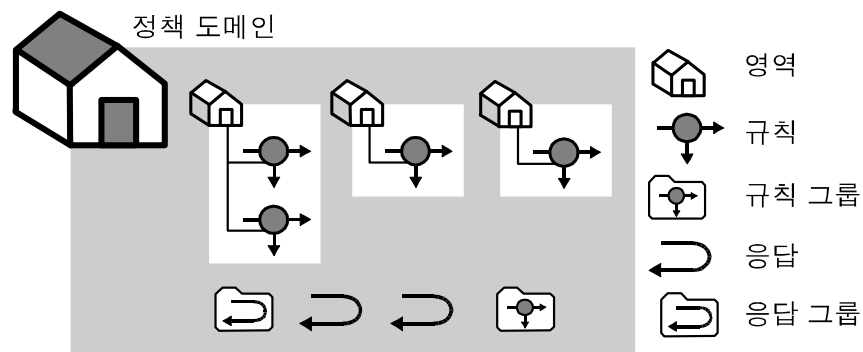
[도메인 수정](#) (페이지 554)

[도메인 삭제](#) (페이지 554)

정책 도메인 개요

정책 도메인은 하나 이상의 사용자 디렉터리와 연결된 리소스를 논리적으로 그룹화한 것입니다. 또한 정책 도메인에는 정책 도메인 내의 개체를 변경할 수 있는 관리자 계정이 하나 이상 필요합니다. 정책 도메인에는 영역, 규칙, 응답 및 정책이 필요하고, 선택적으로 규칙 그룹과 응답 그룹이 포함됩니다. 적절한 권한이 있는 관리자가 한 명 이상의 관리자에게 정책 도메인을 할당합니다.

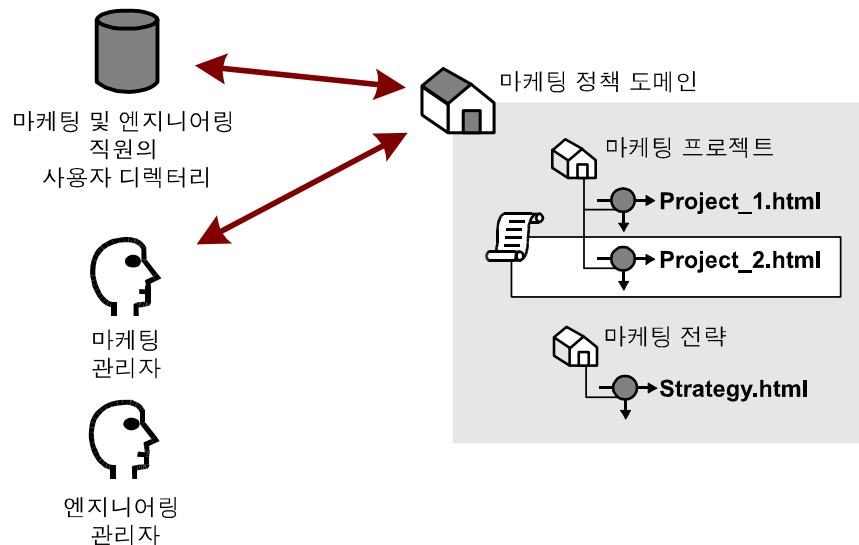
정책 도메인의 리소스는 하나 이상의 영역으로 그룹화할 수 있습니다. 영역은 공통적인 보안(인증) 요구 사항이 있는 리소스의 집합입니다. 리소스에 대한 리소스 제어 액세스를 포함하는 영역과 관련된 규칙입니다. 다음 다이어그램에서는 영역과 영역에 연결된 규칙과 함께 규칙 그룹, 응답 그룹 및 응답 쌍도 포함된 작은 정책 도메인을 보여 줍니다.



정책 도메인의 영역 및 규칙을 그룹화하면 리소스에 대한 보안 도메인을 조직에 제공할 수 있습니다. 정책 단위에서는 정책 도메인 내에 정책 도메인의 리소스에 대한 액세스를 제어하는 정책을 생성하는 방법을 알아봅니다.

아래의 샘플 다이어그램에서는 마케팅 정책 도메인에 지정된 마케팅 정책 관리자가 마케팅 전략 및 마케팅 프로젝트 영역을 관리할 수 있습니다. 이 정책 도메인은 마케팅 정책 도메인에 대한 관리 권한이 없는 엔지니어링 관리자가 마케팅 부서에 속한 리소스를 제어할 수 없도록 합니다. 그러나 마케팅 정책 도메인은 엔지니어링 사용자가 포함된 사용자 디렉터리와 연결되어 있습니다.

따라서 마케팅 부서의 관리자가 마케팅 정책 도메인 내에서 엔지니어링 직원이 **Project_2.html** 리소스에 액세스할 수 있도록 하는 정책을 생성할 경우 엔지니어링 사용자가 이 리소스에 액세스할 수 있습니다.



추가 정보:

[정책](#) (페이지 621)

도메인 및 사용자 구성원

정책 도메인은 도메인 개체의 컨테이너 역할을 할 뿐 아니라 사용자 디렉터리에도 연결합니다. 정책 서버는 대상 리소스가 있는 영역의 요구 사항을 기반으로 사용자를 인증합니다. 사용자를 인증하기 위해 정책 서버는 사용자가 정의되어 있는 사용자 디렉터리를 찾아야 합니다. 정책 서버는 영역이 속해 있는 정책 도메인을 찾아 이 작업을 수행합니다. 정책 도메인에서 정책 서버는 정책 도메인의 검색 순서에 지정된 사용자 디렉터리를 쿼리합니다.

검색 순서는 정책 도메인에 대한 사용자 디렉터리 연결을 추가할 때 정의됩니다. 디렉터리 연결을 추가하는 순서에 따라 정책 서버가 사용자를 검색하는 데 사용하는 순서가 결정됩니다. 예를 들어 WinNT 디렉터리의 사용자 데이터를 LDAP 디렉터리에 마이그레이션하려는 회사의 정책 도메인을 설정할 경우 정책 서버가 새 LDAP 디렉터리에서 먼저 검색한 다음 WinNT 사용자 디렉터리에서 검색하도록 하려면 정책 도메인에 대한 LDAP 디렉터리 연결을 먼저 추가한 다음 WinNT 사용자 디렉터리 연결을 추가하십시오.

정책 도메인을 구성하는 방법

하나 이상의 사용자 디렉터리가 포함된 논리적 리소스 그룹을 생성하도록 도메인을 구성하십시오. 도메인을 구성하려면 다음을 수행해야 합니다.

- 사용자 인증을 위한 사용자 디렉터리를 하나 이상 할당
- 보안 정책에 따라 리소스를 그룹화하기 위한 영역을 하나 이상 생성

참고: 나중에 영역을 추가해야 하는 경우 정책 도메인의 속성을 편집하면 됩니다.

새 정책 도메인을 구성하는 과정은 다음 단계로 이루어집니다.

1. [정책 도메인 구성](#) (페이지 550)
2. [사용자 디렉터리 할당](#) (페이지 550)
3. [영역 생성](#) (페이지 551)

정책 도메인 구성

논리적 리소스 그룹화를 보호하기 위한 정책 도메인을 생성하십시오.

다음 단계를 수행하십시오.

1. "정책", "도메인", "도메인"을 클릭합니다.
2. "도메인 만들기"를 클릭합니다.
3. 정책의 이름과 설명을 입력합니다.
4. 사용자 디렉터리와 영역을 추가합니다.
5. 제출을 클릭합니다.

정책 도메인을 정의했습니다.

사용자 디렉터리 할당

하나 이상의 사용자 디렉터리를 정책 도메인에 추가할 수 있습니다. 정책 서버는 사용자가 입력하는 자격 증명을 사용자 디렉터리에 저장된 자격 증명과 비교하여 사용자를 인증합니다. 정책 서버는 사용자 디렉터리를 정책 도메인에 나열된 순서대로 검색합니다.

다음 단계를 수행하십시오.

1. "정책", "도메인", "도메인"을 클릭합니다.
2. 검색 조건을 지정하고 "검색"을 클릭합니다.
검색 조건과 일치하는 도메인의 목록이 표시됩니다.
3. 수정할 도메인의 이름을 클릭합니다.
4. "수정"을 클릭합니다.
설정과 컨트롤이 활성화됩니다.
5. "일반" 탭에서 "추가/제거"를 클릭합니다.
"사용자 디렉터리 선택" 페이지가 표시됩니다.

6. "사용 가능한 구성원"의 목록에서 하나 이상의 사용자 디렉터리를 선택하고 오른쪽 방향 화살표를 클릭합니다.

사용자 디렉터리가 "사용 가능한 구성원" 목록에서 제거되고 "선택한 구성원" 목록에 추가됩니다.

참고: 한 번에 여러 구성원을 선택하려면 **Ctrl** 키를 누른 채 추가 구성원을 클릭하십시오. 구성원 블록을 선택하려면 첫 번째 구성원을 클릭한 다음 **Shift** 키를 누른 채 블록의 마지막 구성원을 클릭하십시오.

7. "확인"을 클릭합니다.

선택된 사용자 디렉터리가 "사용자 디렉터리" 아래에 나열됩니다.

참고: 새 사용자 디렉터를 생성하고 도메인에 추가하려면 "만들기"를 클릭하십시오.

8. 제출을 클릭합니다.

선택된 사용자 디렉터리가 정책 도메인에 추가됩니다.

영역 생성

영역은 도메인에 생성되고 웹 에이전트와 연결됩니다. 영역에서는 리소스 필터를 사용하여 보안 요구 사항이 비슷하며 공통 인증 체계를 공유하는 리소스를 그룹화합니다.

SiteMinder 웹 에이전트로 영역 구성

도메인을 생성할 때 도메인에 하나 이상의 영역을 생성하고 이를 웹 에이전트 또는 에이전트 그룹과 연결할 수 있습니다. 영역은 보안 요구 사항이 비슷하며 공통 인증 체계를 공유하는 리소스를 그룹화합니다.

다음 단계를 수행하십시오.

1. "정책", "도메인", "영역"을 클릭합니다.
2. "영역 만들기"를 클릭합니다.
3. 도메인을 선택하고 "다음"을 클릭합니다.
4. 영역의 이름과 설명을 입력합니다.
5. 줄임표 단추를 클릭하고 에이전트를 선택합니다.
6. 웹 에이전트 또는 에이전트 그룹을 선택하고 "확인"을 클릭합니다.
7. 나머지 리소스 속성을 지정합니다.

8. 새 규칙을 생성하거나 기존 규칙을 삭제합니다.
9. 새 하위 영역을 생성하거나 기존 하위 영역을 삭제합니다.
10. 세션 속성을 지정합니다.
11. 영역이 처리해야 하는 이벤트의 유형과 인증 디렉터리 매핑을 지정합니다.
12. "마침"을 클릭합니다.
영역이 생성됩니다.

추가 정보:

[정책 서버 개체 복사](#) (페이지 10)

RADIUS 에이전트로 영역 구성

도메인을 생성할 때 도메인에 하나 이상의 영역을 생성하고 이를 Radius 에이전트 또는 에이전트 그룹과 연결할 수 있습니다. 영역은 보안 요구 사항이 비슷하며 공통 인증 체계를 공유하는 리소스를 그룹화합니다.

참고: 관리 UI에서는 RADIUS 에이전트로 보호되는 영역을 구성할 수 있습니다. 이러한 영역에는 SiteMinder 웹 에이전트 영역에 필요한 것과 동일한 정보가 모두 필요하지는 않습니다.

다음 단계를 수행하십시오.

1. "정책", "도메인", "영역"을 클릭합니다.
2. "영역 만들기"를 클릭합니다.
3. 도메인을 선택하고 "다음"을 클릭합니다.
4. 영역의 이름과 설명을 입력합니다.
5. 줄임표 단추를 클릭하고 에이전트를 선택합니다.
6. RADIUS 에이전트 또는 에이전트 그룹을 선택하고 "확인"을 클릭합니다.
7. 나머지 리소스 속성을 지정합니다.

8. 새 규칙을 생성하거나 기존 규칙을 삭제합니다.
9. 세션 속성을 지정합니다.
10. "마침"을 클릭합니다.

영역이 만들어지고 선택된 RADIUS 에이전트 또는 에이전트 그룹과 연결됩니다.

추가 정보:

[정책 서버 개체 복사](#) (페이지 10)

도메인에 CA Identity Manager 환경 추가

도메인에 CA Identity Manager 환경 및 관련 사용자 디렉토리를 추가하면 정책에서 CA Identity Manager 역할을 사용할 수 있게 됩니다.

다음 단계를 수행하십시오.

1. "정책", "도메인", "도메인"을 클릭합니다.
2. 검색 조건을 지정하고 "검색"을 클릭하여 필요한 도메인을 찾습니다.
3. 환경을 추가할 도메인의 이름을 클릭합니다.
4. "수정"을 클릭합니다.
5. 환경에 연결된 사용자가 도메인에 바인딩되어 있지 않은 경우 관련 사용자 디렉토리를 추가합니다.
6. "IDM 환경" 섹션에서 "추가/제거"를 클릭합니다.
7. 필요한 "IDM 환경"을 선택하고 "확인"을 클릭합니다.
8. 제출을 클릭합니다.

CA Identity Manager 환경이 도메인에 추가됩니다. 환경에 연결된 역할을 도메인에서 생성된 모든 정책에 사용할 수 있게 됩니다.

도메인에 대한 전역 정책 처리가 사용되지 않도록 설정

전역 정책을 사용하면 모든 도메인의 특정 리소스 및 이벤트에 응답을 연결할 수 있습니다. 기본적으로 전역 정책은 정책 도메인의 모든 리소스에 적용됩니다.

다음 단계를 수행하십시오.

1. 도메인을 엽니다.
2. "전역 정책 적용" 확인란의 선택을 취소하고 "제출"을 클릭합니다.
전역 정책이 더 이상 이 도메인의 리소스에 적용되지 않습니다.

도메인 수정

정책 또는 가맹 도메인과 연결된 이름, 설명, 사용자 디렉터리 연결 및 관리자를 변경할 수 있습니다. 도메인의 다른 모든 기능은 부수적 구성에 따라 결정됩니다.

도메인 삭제

중요! 도메인을 삭제하면 도메인에 바인딩된 도메인 사용자 디렉터리, 관리자 연결 및 개체(예: 규칙, 영역, 응답, 정책 또는 가맹)가 모두 삭제됩니다.

삭제된 모든 개체는 짧은 시간 내에 캐시에서 제거될 수 있습니다.

제 13 장: 영역

이 섹션은 다음 항목을 포함하고 있습니다.

[영역 개요](#) (페이지 555)

[신뢰 수준 소개](#) (페이지 556)

[에이전트, 영역 및 규칙별로 리소스 식별](#) (페이지 557)

[중첩된 영역](#) (페이지 559)

[요청 처리에서의 영역](#) (페이지 561)

[영역 구성](#) (페이지 561)

[영역 수정](#) (페이지 564)

[영역 삭제](#) (페이지 564)

[중첩된 영역 구성](#) (페이지 564)

[리소스 캐시에서 단일 영역 플러시](#) (페이지 565)

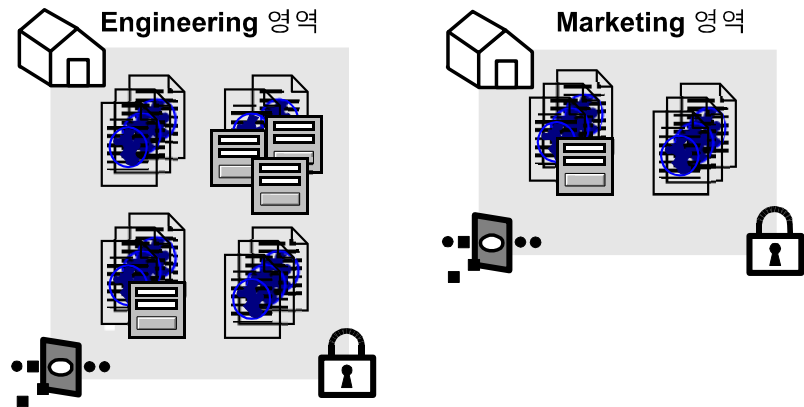
영역 개요

복잡한 리소스 집합은 보안 정책을 생성할 수 있도록 논리적으로 그룹화해야 합니다. 리소스에 대한 기본 SiteMinder 그룹이 영역입니다.

영역은 보안 요구 사항에 따라 그룹화된 정책 도메인 내의 리소스 클러스터입니다. 영역은 일반적으로 네트워크의 공용 위치에 있는 리소스에 대해 정의됩니다. 예를 들어 네트워크의 /marketing 디렉터리에 있는 마케팅 정보는 회사의 마케팅 조직에 있는 관리자가 제어하는 정책 도메인의 영역으로 구성될 수 있습니다.

영역의 콘텐츠는 에이전트가 보호합니다. 사용자가 영역 내에 있는 리소스를 요청할 경우 관련 에이전트가 사용자의 인증 및 권한 부여를 처리합니다. 영역에 따라 인증 방법이 달라집니다.

다음 다이어그램에서는 두 영역의 콘텐츠를 보여 줍니다.



각 영역에는 HTML 파일, 양식 또는 응용 프로그램 등의 리소스가 포함되어 있습니다. 또한 각 영역은 에이전트 및 인증 체계와 연결되어 있습니다.

신뢰 수준 소개

SiteMinder 가 지원되는 위험 분석 엔진과 통합되는 경우 신뢰 수준을 사용하여 영역을 구성할 수 있습니다. 신뢰 수준은 보호되는 리소스를 요청하는 사용자가 적합할 가능성을 의미하는 자격 증명 보장을 나타냅니다.

다음 사항을 고려하십시오.

- 신뢰 수준은 0~1000 사이의 숫자를 기반으로 합니다. 신뢰 수준이 높을수록 자격 증명의 보장 수준이 높아집니다.
- 두 가지 액세스 관리 모델을 사용하여 신뢰 수준을 권한 부여 결정에 적용할 수 있습니다. 자세한 내용은 [정책에서 신뢰 수준 구성](#) (페이지 624) 및 [응용 프로그램에서 신뢰 수준 구성](#) (페이지 515)을 참조하십시오.
- 신뢰 수준을 생성하는 인증 체계에서 사용자를 인증하는 경우 신뢰 수준이 사용자의 세션 티켓에 삽입됩니다. 사용자는 정책 또는 응용 프로그램이 사용자에게 적용되는 한 이 값 이상의 신뢰 수준이 필요한 모든 리소스에 액세스할 수 있습니다.

- 신뢰 수준을 계산할 때 사용되는 요소는 위험 분석 엔진에서 자격 증명 보장을 결정하기 위해 사용하는 데이터를 기반으로 합니다.

참고: SiteMinder에서는 CA Arcot WebFort 및 CA Arcot Risk의 온프레미스 구축 환경 및 CA Arcot A-OK의 호스트된 구축 환경과의 통합을 지원합니다.

에이전트, 영역 및 규칙별로 리소스 식별

SiteMinder가 보호하는 리소스는 다음과 같이 식별됩니다.

[에이전트] [영역 리소스 필터] [규칙 리소스]

에이전트

에이전트는 보호된 리소스의 영역이 하나 이상 포함된 서버를 모니터링합니다.

영역 리소스 필터

영역에 포함된 리소스를 지정하는 문자열(예: 디렉터리의 상대 경로)입니다. 최상위 영역의 경우에는 파일 또는 응용 프로그램을 제공하는 서버를 기준으로 리소스를 지정합니다. 영역이 중첩되어 있는 경우에는 부모 영역을 기준으로 리소스를 지정합니다.

예를 들어 다음과 같이 웹 서버의 문서 루트 바로 아래에 있는 디렉터리의 콘텐츠가 영역에 포함될 수 있습니다.

```
<document_root>/HR
```

이때 영역 리소스 필터를 다음과 같이 지정할 수 있습니다.

```
/HR
```

규칙 리소스

규칙이 적용되는 리소스를 지정하는 문자열 또는 정규식입니다. 리소스가 포함된 영역을 기준으로 리소스를 지정합니다. 예를 들어 영역 리소스 필터가 디렉터리 이름으로 끝나는 경우 규칙 리소스에는 다음과 같이 영역 디렉터리의 하위 디렉터리와 하위 디렉터리의 파일 이름도 포함될 수 있습니다.

```
/Managers/PayRanges.html
```

와일드카드를 사용하여 규칙의 사양을 확장할 수 있습니다. 예를 들면 다음과 같습니다.

```
/Managers/*
```

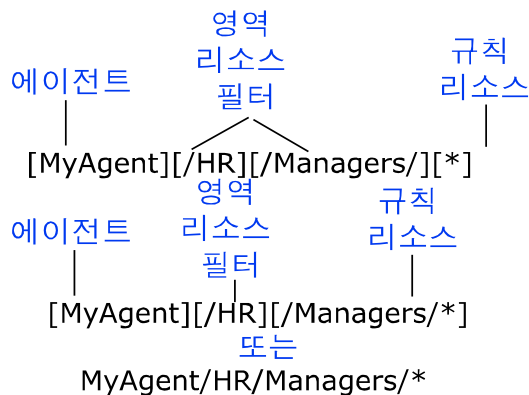
이 세 개의 요소를 조합하여 다음과 같은 경우를 가정해 보십시오.

- MyAgent 라는 에이전트가 myorg.org 도메인의 MyHost 호스트에 있는 웹 서버를 보호합니다.
- 영역에 다음 웹 서버 디렉터리의 콘텐츠를 포함하려고 합니다.

<document_root>/HR

- HR 디렉터리에는 **Managers** 라는 하위 디렉터리가 포함되어 있으며 이 하위 디렉터리의 모든 파일을 보호하려고 합니다.

다음 그림에서는 정책 서버에 대한 유효 리소스를 보여 줍니다.



Managers 라는 디렉터리는 /HR 영역 아래에 중첩된 영역으로 구성할 수 있습니다.

사용자가 **Managers** 하위 디렉터리 아래의 보호된 페이지인 **PayRanges.html**에 액세스하려면 다음을 수행해야 합니다.

1. 리소스를 지정합니다.

<http://MyHost.myorg.org/HR/Managers/PayRanges.html>

2. 리소스에 액세스할 수 있는 권한이 부여된 사용자의 자격 증명을 제공합니다. 관리자는 정책을 사용하여 리소스에 액세스할 수 있는 권한이 부여된 사용자를 지정합니다.

보호되지 않은 영역, 규칙 및 정책

기본적으로 영역은 "보호됨" 상태로 생성됩니다. 대부분의 경우 영역을 "보호 안 함" 상태로 변경하는 대신 보호된 영역을 사용해야 합니다. 보호된 영역에서는 모든 리소스가 액세스에 대해 보호됩니다. 액세스를 허용하려면 규칙을 정의한 다음 이를 정책에 포함해야 합니다.

"보호 안 함" 상태로 영역을 생성할 경우 SiteMinder 에서 해당 영역의 리소스를 보호하려면 먼저 규칙을 구성해야 합니다. 보호되지 않은 영역의 리소스에 대한 규칙을 생성하면 지정된 리소스만 보호됩니다. 리소스가 보호된 후에는 사용자가 해당 리소스에 액세스할 수 있도록 하는 규칙을 정책에 추가해야 합니다. 영역에 있는 리소스의 일부만 권한 없는 액세스로부터 보호해야 하는 경우에는 보호되지 않은 영역을 사용할 수 있습니다.

다음은 보호되지 않은 영역을 설정할 때 필요한 작업의 예입니다.

작업	보호 상태
리소스 필터 /dir 를 사용하여 영역 1 이라는 보호되지 않은 영역을 생성합니다.	/dir 와 하위 디렉터리에 포함된 리소스는 보호되지 않습니다.
영역 1 에 file.html 리소스에 대한 Rule1 을 생성합니다.	/dir/file.html 파일은 보호되지만 /dir 의 나머지 콘텐츠는 보호되지 않습니다.
Policy1 을 생성하고 Rule1 과 User1 을 이 정책에 바인딩합니다.	User1 은 /dir/file.html 에 액세스할 수 있습니다. 다른 모든 사용자는 이 보호된 파일에 액세스할 수 없습니다.

참고: 익명 인증 체계를 사용하는 영역의 사용자를 추적하려면 영역이 보호된 영역이어야 합니다. 익명 체계에 대한 자세한 내용은 [익명 인증 체계](#) (페이지 404)를 참조하십시오.

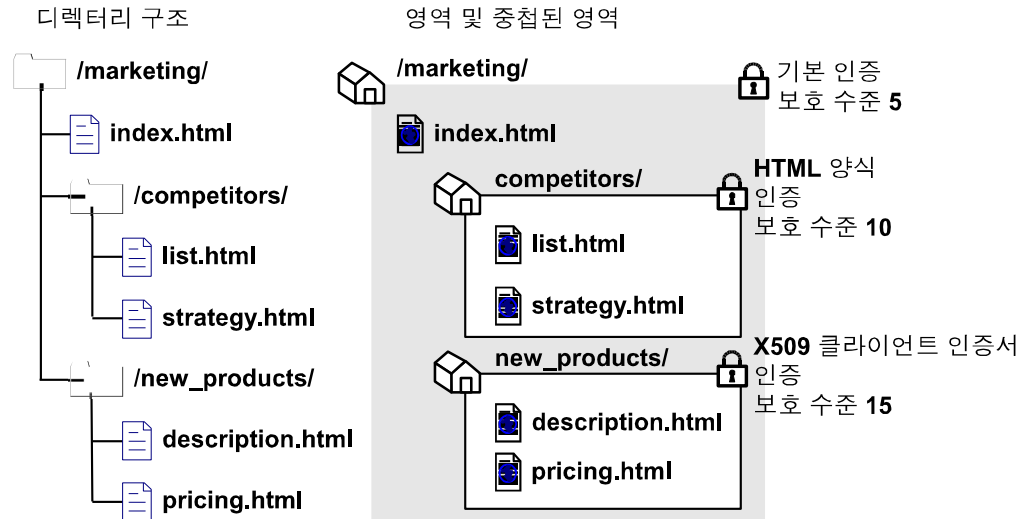
중첩된 영역

파일 및 폴더의 디렉터리가 파일 시스템의 콘텐츠를 나타내는 것처럼 영역은 리소스의 그룹을 나타냅니다. 중첩된 영역을 사용하면 디렉터리 트리에서 하위 위치에 있는 리소스의 보호 수준을 높일 수 있습니다. 기존 영역 아래에 중첩된 영역을 생성할 수 있습니다. 그런 다음 중첩된 영역에 보호 수준이 더 높은 인증 체계를 할당할 수 있습니다.

기본적으로 자식 영역의 리소스에 액세스하려면 사용자에게 부모 영역의 리소스와 자식 영역의 리소스에 대한 권한이 부여되어야 합니다. 정책 서버의 기본 동작을 전역적으로 변경하여, 부모 영역 또는 자식 영역 중 하나에 대한 권한이 부여된 사용자가 자식 영역의 리소스에 항상 액세스할 수 있도록 허용할 수도 있습니다. 그러나 **and** 논리에서 보안 수준이 낮은 **or** 논리로 변경하는 것은 권장되지 않습니다. **or** 논리로 변경하려면 "중첩된 보안 사용" 확인란의 선택을 취소하십시오.

참고: 최상위 영역을 포함하여 중첩된 구조의 영역에는 익명 인증 체계를 할당하지 마십시오. 익명 인증 체계로 보호된 리소스의 경우 특정 사용자에게 권한을 부여할 수 없으므로 **and** 논리가 실패합니다.

다음 예에서는 중첩된 영역을 사용하여 보안 수준을 높이는 방법을 보여줍니다.



위 그림에 표시된 영역 구조에서 영역은 리소스의 파일 구조와 유사합니다. 중첩된 각 영역에는 부모 영역과는 다른 인증 체계가 있습니다. 각 자식 영역의 인증 체계는 부모 영역의 인증 체계보다 보호 수준이 높으므로 사용자는 트리의 하위 수준에 있는 리소스에 액세스할 때 다시 인증해야 합니다. 이 예를 구현하려면 각 영역에 대해 규칙을 생성해야 합니다. 그런 다음 각 정책에 규칙이 하나 포함되고 자식 영역의 리소스에 액세스해야 하는 사용자가 부모 영역의 리소스에도 액세스할 수 있도록 해당하는 정책을 생성해야 합니다.

참고: "시스템 및 도메인 개체 관리" 권한이 있는 관리자만 영역을 생성, 편집 및 삭제할 수 있습니다. 그러나 "도메인 개체 관리" 권한이 있는 관리자도 자신이 관리하는 정책 도메인의 기존 영역 아래에 있는 중첩된 영역을 생성, 편집 및 삭제할 수 있습니다.

요청 처리에서의 영역

사용자가 리소스를 요청하면 정책 서버는 일치하는 가장 긴 영역을 사용하여 리소스 보호 여부를 확인하고, 리소스가 보호된 리소스일 경우 사용자의 아이덴티티를 설정하는 데 사용해야 하는 인증 체계를 확인합니다. 일치하는 가장 긴 영역은 요청된 리소스 경로와 일치하는 가장 낮은 그룹 수준의 중첩된 영역 그룹(또는 중첩된 영역이 사용되지 않는 경우 단일 영역)에 있을 수 있는 리소스 필터로 구성됩니다.

예

이전 단원의 예를 사용할 경우, `/marketing/competitors/list2.html` 위치에 있는 `list2.html` 이라는 파일은 중첩된 영역 `/marketing/competitors/`와 일치합니다. `/marketing/competitors/` 영역에는 HTML 양식 인증 체계가 연결되어 있으므로 정책 서버가 `list2.html`에 대한 인증을 처리할 때 사용자는 HTML 양식을 통해 인증됩니다.

같은 예에서 `current_budget.html` 이라는 파일은 `/marketing/budgets/current_budget.html` 위치에 있습니다. `/budget` 디렉터리는 중첩된 영역에서 명시적으로 호출되지 않으므로 이 리소스에 대해 일치하는 가장 긴 영역은 `/marketing/`입니다. 따라서 사용자는 기본 사용자 이름 및 암호 인증 체계를 통해 인증됩니다.

영역 구성

영역은 네트워크의 특정 위치에 있는 리소스 그룹입니다. 영역의 콘텐츠는 에이전트가 보호합니다. 사용자가 영역 내에 있는 리소스를 요청할 경우 관련 에이전트가 사용자의 인증 및 권한 부여를 처리합니다. 영역에 따라 인증 방법이 지정됩니다.

가맹 에이전트를 포함하여 모든 유형의 SiteMinder 에이전트에 대해 영역을 구성할 수 있습니다.

SiteMinder 웹 에이전트로 보호되는 영역 구성

사용자가 웹 서버를 통해 액세스하는 리소스 그룹을 보호하도록 영역을 구성할 수 있습니다.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다.

다음 단계를 수행하십시오.

1. "정책", "도메인", "영역"을 클릭합니다.
2. "영역 만들기"를 클릭합니다.
3. "도메인" 목록에서 도메인을 선택하고 "다음"을 클릭합니다.
4. 영역의 이름과 설명을 입력합니다.
5. 줄임표 단추를 클릭하고 에이전트를 선택합니다.
6. SiteMinder 웹 에이전트 또는 에이전트 그룹을 선택하고 "확인"을 클릭합니다.
7. 나머지 리소스 속성을 지정합니다.
8. 새 규칙을 생성하거나 기존 규칙을 삭제합니다.
9. 새 하위 영역을 생성하거나 기존 하위 영역을 삭제합니다.
10. 세션 속성을 지정합니다.
11. 영역이 처리해야 하는 이벤트 유형과 디렉터리 매핑을 지정합니다.
12. 영역의 모든 리소스에 적용할 최소 신뢰 수준을 지정합니다.

참고: 영역에 신뢰 수준을 적용하려면 SiteMinder 를 지원되는 위험 분석 엔진과 통합하고 신뢰 수준 지원이 사용되도록 설정해야 합니다. 자세한 내용은 [구현 안내서](#)를 참조하십시오.

13. "마침"을 클릭합니다.

선택된 SiteMinder 웹 에이전트 또는 에이전트 그룹과 연결된 영역이 생성됩니다.

추가 정보:

[정책 서버 개체 복사](#) (페이지 10)

RADIUS 에이전트로 보호되는 영역 구성

사용자가 웹 서버를 통해 액세스하는 리소스 그룹을 보호하도록 영역을 구성할 수 있습니다.

참고: 관리 UI에서는 RADIUS 에이전트로 보호되는 영역을 구성할 수 있습니다. 이러한 영역에는 SiteMinder 웹 에이전트 영역에 필요한 것과 동일한 정보가 모두 필요하지는 않습니다.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다.

다음 단계를 수행하십시오.

1. "정책", "도메인", "영역"을 클릭합니다.
2. "영역 만들기"를 클릭합니다.
3. "도메인" 목록에서 도메인을 선택하고 "다음"을 클릭합니다.
4. 영역의 이름과 설명을 입력합니다.
5. 줄임표 단추를 클릭하고 에이전트를 선택합니다.
6. RADIUS 에이전트 또는 에이전트 그룹을 선택하고 "확인"을 클릭합니다.
7. 나머지 리소스 속성을 지정합니다.
8. 새 규칙을 생성하거나 기존 규칙을 삭제합니다.
9. 세션 속성을 지정합니다.
10. "마침"을 클릭합니다.

선택된 RADIUS 에이전트 또는 에이전트 그룹과 연결된 영역이 생성됩니다.

추가 정보:

[정책 서버 개체 복사](#) (페이지 10)

영역 수정

기존 영역을 수정할 경우 다음 항목은 변경할 수 없습니다.

- 에이전트

기존 영역이 있는 서버를 보호하는 에이전트는 변경할 수 없습니다.
에이전트를 변경해야 하는 경우에는 영역을 삭제하고 새 에이전트로 영역을 다시 생성해야 합니다.

- 리소스 필터

기존 영역의 리소스 필터는 변경할 수 없습니다. 리소스 필터를 변경해야 하는 경우에는 영역을 삭제하고 새 리소스 필터로 영역을 다시 생성해야 합니다.

참고: 정책 서버 개체의 수정 및 삭제에 대한 자세한 내용은 정책 서버 개체 관리를 참조하십시오.

영역 삭제

영역을 삭제하면 해당 영역과 연관된 중첩된 영역까지 모두 삭제됩니다. 또한 삭제한 영역 및 중첩된 영역과 연관된 규칙도 삭제됩니다. 연관된 중첩된 영역까지 모두 제거하려면 부모 영역만 삭제하면 됩니다. 중첩된 영역을 삭제하기 위해 개별적으로 선택하지 않아도 됩니다.

참고: 정책 서버 개체의 수정 및 삭제에 대한 자세한 내용은 정책 서버 개체 관리를 참조하십시오.

중첩된 영역 구성

도메인 개체 관리 권한을 가진 관리자는 부모 영역이 관리자 범위 내의 도메인과 연결된 경우 부모 영역 내에 중첩된 영역을 생성할 수 있습니다.

참고: SiteMinder 웹 에이전트로 보호되는 영역 아래에서만 중첩된 영역을 생성할 수 있습니다.

다음 단계를 수행하십시오.

1. "정책", "도메인", "영역"을 클릭합니다.
2. 검색 조건을 지정하고 "검색"을 클릭합니다.

3. 수정할 영역의 이름을 클릭합니다.
4. "수정"을 클릭합니다.
설정과 컨트롤이 활성화됩니다.
5. "하위 영역"에서 "하위 영역 만들기"를 클릭합니다.
6. 영역의 이름과 설명을 입력합니다.
7. 리소스 필터의 경로를 입력합니다.

참고: 중첩된 영역의 리소스 필터가 부모 영역의 리소스 필터에 추가됩니다. 예를 들어 부모 영역의 필터가 /marketing 이고 중첩된 영역의 필터가 /data 인 경우 전체 필터는 <agent_of_the_parent_realm>/marketing/data 입니다.

참고: 리소스 필터에서는 별표(*) 및 물음표(?) 문자가 와일드카드가 아니라 리터럴 문자로 취급됩니다.

8. 세션 속성을 지정합니다.
9. 다음의 고급 설정을 지정합니다.
 - 권한 부여 디렉터리 매핑
 - 이벤트 처리
10. "확인"을 클릭합니다.
새로 생성된 하위 영역이 부모 영역에 추가됩니다.
11. 제출을 클릭합니다.
새로 생성된 하위 영역과 연결된 영역이 생성됩니다.

리소스 캐시에서 단일 영역 플러시

SiteMinder에서는 사용자가 보호된 리소스에 액세스할 때 영역 정보를 캐시합니다. 이를 통해 SiteMinder에서는 최근 사용한 리소스를 추적하여 네트워크 성능을 향상시킵니다. 하지만 영역의 보안 요구 사항 또는 콘텐츠를 변경할 경우에는 SiteMinder 리소스 캐시에서 영역을 플러시해야 합니다.

참고: "시스템 및 도메인 개체 관리" 관리 권한이 있는 경우에는 "캐시 관리" 대화 상자를 사용하여 리소스 캐시에서 모든 영역을 플러시할 수 있습니다.

다음 단계를 수행하십시오.

1. "정책", "도메인", "영역"을 클릭합니다.
2. 검색 조건을 지정하고 "검색"을 클릭합니다.
3. 수정할 영역의 이름을 클릭합니다.
4. "수정"을 클릭합니다.
설정과 컨트롤이 활성화됩니다.
5. "영역의 리소스 플러시"에서 "플러시"를 클릭합니다.
SiteMinder 가 리소스 캐시에서 영역을 플러시합니다.

제 14 장: 규칙

이 섹션은 다음 항목을 포함하고 있습니다.

[규칙 개요](#) (페이지 567)

[웹 에이전트 작업을 위한 규칙 구성](#) (페이지 575)

[인증 이벤트 작업을 위한 규칙 구성](#) (페이지 576)

[권한 부여 이벤트 작업을 위한 규칙 구성](#) (페이지 577)

[가장 이벤트 작업을 위한 규칙 구성](#) (페이지 579)

[리소스 일치 및 정규식](#) (페이지 579)

[규칙을 사용하거나 사용하지 않도록 설정](#) (페이지 581)

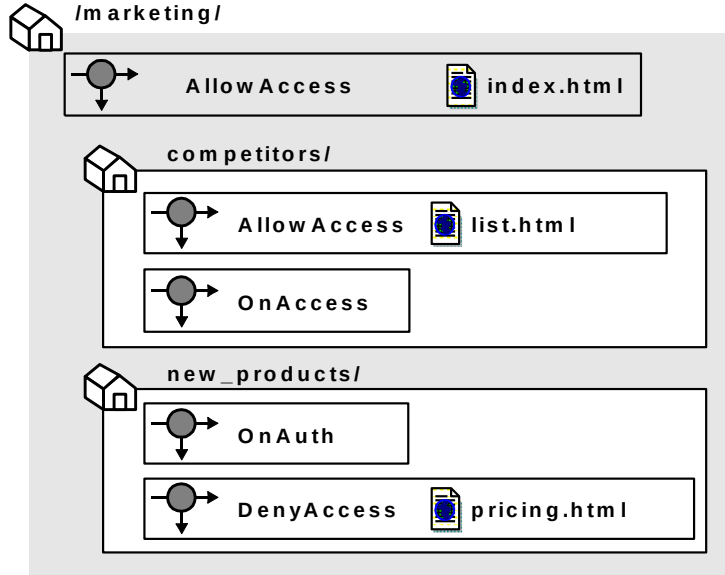
[고급 규칙 옵션](#) (페이지 582)

[규칙 삭제](#) (페이지 584)

규칙 개요

규칙은 특정 리소스를 식별하고 리소스에 대한 액세스를 허용 또는 거부합니다. 인증 또는 권한 부여 이벤트가 발생할 때 규칙을 사용하여 응답을 트리거할 수도 있습니다. 규칙을 생성할 때는 규칙을 특정 영역과 연결해야 합니다.

다음 다이어그램에서는 다양한 영역 및 중첩된 영역 및 영역에 연결된 규칙을 보여 줍니다.



위 다이어그램에서 각 영역과 중첩된 영역의 리소스에는 특정 규칙이 연결되어 있습니다. 영역의 모든 리소스 또는 영역의 일부 리소스에 단일 규칙을 연결할 수도 있습니다. 이렇게 하려면 리소스 일치 또는 정규식을 사용하여 리소스를 지정합니다.

규칙이 정책의 일부로 작동하는 방식

정책은 규칙, 사용자 및 응답을 함께 바인딩하여 리소스를 보호합니다. 규칙은 정책의 일부로, 보호되는 리소스와 규칙이 실행되도록 하는 작업 유형을 정확히 결정합니다.

예를 들어 웹 서버가 **HTML** 페이지에 대한 요청에 응답하는 데 사용하는 **GET** 작업에 대해 영역의 모든 **HTML** 파일이 보호되도록 하는 규칙을 지정할 수 있습니다. 사용자의 브라우저가 리소스에 액세스하려고 하면 규칙이 실행되고 해당 규칙이 포함된 정책에 따라 사용자가 선택한 리소스를 볼 수 있는지 여부가 결정됩니다.

정책 서버가 규칙을 처리하는 방식

정책 서버는 정책에 정의된 사용자, 규칙 및 응답 간의 관계에 따라 규칙을 평가합니다. 사용자가 보호된 리소스에 액세스하면 정책 서버는 정책에 포함된 규칙을 처리하여 사용자에게 해당 리소스에 대한 권한을 부여할지 여부, 인증 및 권한 부여 이벤트를 처리해야 하는지 여부, 그리고 응답을 생성하여 SiteMinder 에이전트에 반환할지 여부를 결정해야 합니다.

정책 서버는 권한 부여 이벤트를 처리할 때 보호된 리소스와 일치하는 가장 긴 리소스 필터가 포함된 영역을 찾습니다. 그런 다음 정책 서버는 해당 영역과 연결된 규칙만 실행합니다. 이 예에서는 사용자가 관리자이고 다음과 같은 보호된 리소스에 액세스하려고 한다고 가정합니다.

`/company/employees/managers/performance/`

다음 영역에는 보호된 리소스와 일치하는 리소스 필터가 있습니다.

영역 이름	영역 설명	리소스 필터
회사	고객, 직원, 공급업체	<code>/company/</code>
회사 직원	모든 직원	<code>/company/employees/</code>
회사 관리자	모든 관리자	<code>/company/employees/managers/</code>
성과 관리	관리자와 팀 구성원	<code>/company/employees/managers/performance/</code>

일치하는 가장 긴 리소스 필터가 있는 영역은 "성과 관리"입니다. 정책 서버는 권한 부여 이벤트에 대한 응답으로 "성과 관리" 영역과 연결된 모든 규칙을 실행합니다.

중첩된 영역을 배포할 때 정책 서버는 처리 중 사용할 수 있도록 일치하는 영역이 포함된 순위 지정 목록을 보관합니다. 일치하는 규칙이 리소스에 대한 액세스를 거부하면 처리가 중지되고 정책 서버는 해당 액세스 거부 규칙과 연결된 응답을 SiteMinder 에이전트에 반환합니다.

정책 서버는 실행되는 모든 일치 규칙에서 응답을 수집합니다. 규칙을 기반으로 한 응답 수집을 마치면 정책 서버는 중복 응답을 삭제합니다.

중첩된 영역을 사용하는 배포 환경에서 정책 서버는 일치하는 모든 규칙에 대한 누적된 응답이 포함된 전체 목록을 수집합니다. **OnAuthAccept** 규칙의 경우 정책 서버는 전체 응답 목록을 **SiteMinder** 에이전트에 반환합니다. **OnAuthReject** 규칙의 경우 정책 서버는 가장 낮은 중첩된 영역의 규칙과 연결된 응답만 **SiteMinder** 에이전트에 반환합니다. **OnAuthReject** 규칙은 정책에 바인딩된 사용자에게 대해서만 실행됩니다.

규칙 및 중첩된 영역

중첩된 영역은 기존 영역 내에 생성된 영역입니다. 중첩된 영역에는 부모 영역 또는 최상위 영역이 있으며, 중첩된 영역은 부모 영역의 자식으로 간주됩니다. 중첩된 영역을 생성할 때 자식 영역의 리소스를 보호하기 위한 별도의 규칙을 생성할 수도 있습니다. 기존 규칙을 복사하여 다른 영역에 추가하고 규칙의 이름을 변경할 수도 있습니다.

추가 정보:

[중첩된 영역](#) (페이지 559)

규칙 작업

규칙의 작업은 규칙을 실행하기 위해 발생해야 하는 작업을 결정합니다. 정책 서버가 규칙에 지정된 작업이 발생한 것을 확인하면 규칙이 실행됩니다. 규칙은 사용하도록 설정된 기존 정책에 포함되어야 합니다. 예를 들어 정책에 **HTML** 페이지에 대한 액세스를 허용하는 규칙이 포함되어 있고 이 정책에 특정 디렉터리에 있는 사용자가 지정된 경우, 디렉터리에 나열된 사용자 중 한 명이 리소스에 액세스하려고 하면 정책 서버는 요청을 처리하기 위해 규칙이 실행되어야 하는지 확인합니다.

규칙이 실행되면 정책 서버는 규칙에 지정된 작업을 규칙이 포함된 정책의 구성 방식에 따라 처리합니다. 예를 들어 사용자가 정책에 지정된 그룹에 속하지 않는 경우 **HTML** 페이지에 대한 **HTTP Get** 작업을 허용하는 규칙이 리소스에 대한 해당 사용자의 액세스를 허용하지 않습니다.

추가 정보:

[정책 개요](#) (페이지 621)

웹 에이전트 작업

웹 에이전트 작업과 관련된 규칙은 지정된 HTTP 작업 중 하나가 발생할 경우 해당 규칙에 지정된 리소스에 대한 액세스를 허용하거나 거부합니다.

액세스 허용을 지정하는 규칙이 실행되는 경우 SiteMinder 는 인증 작업이 성공할 때 지정된 리소스에 사용자가 액세스할 수 있도록 합니다. 반면에 액세스 거부를 지정하는 규칙이 실행되는 경우 SiteMinder 는 인증된 사용자에게 대한 액세스를 거부합니다. 액세스 거부 규칙을 정책에 추가하면 리소스에 액세스할 수 없는 특정 개인 또는 그룹을 거부하여 추가 보안 계층을 제공할 수 있습니다. 기본 설정은 "액세스 허용"입니다.

액세스 거부 규칙은 액세스 허용 규칙보다 우선 순위가 높습니다. 사용자가 리소스에 액세스를 시도할 때 액세스 거부 규칙과 액세스 허용 규칙이 실행되면 액세스 거부 규칙이 모든 액세스 허용 규칙보다 우선 적용됩니다.

웹 에이전트 규칙 작업은 다음과 같습니다.

- HEAD
- GET
- POST
- PUT
- DELETE
- TRACE
- OPTIONS

WSS 에이전트 작업

WSS 에이전트용으로 다음 두 개의 추가 웹 에이전트 규칙 작업을 사용할 수 있습니다.

ProcessSOAP

SOAP 봉투로 래핑된 수신 XML 메시지를 지원합니다.

ProcessXML

SOAP 봉투로 래핑되지 않고 수신 원시 XML 메시지를 지원합니다.

인증 이벤트

인증 이벤트는 SiteMinder 가 사용자 아이덴티티를 설정하려고 할 때 발생합니다. 인증 이벤트는 규칙 작업으로 정책 서버가 인증 프로세스의 특정 시점에서 규칙을 실행하도록 합니다.

인증 이벤트는 사용자가 On-Auth 이벤트를 포함하는 규칙으로 보호되는 리소스에 액세스할 때 발생합니다. 웹 에이전트 작업이나 권한 부여 이벤트와 달리 인증 이벤트는 항상 전체 영역에 적용됩니다. 영역의 일부에만 적용되는 On-Auth 규칙은 생성할 수 없습니다.

다음은 사용할 수 있는 인증 이벤트의 목록입니다.

OnAuthAccept

인증이 성공한 경우 발생합니다. 이 이벤트를 사용하면 인증 성공 후 사용자를 리디렉션할 수 있습니다.

OnAuthAcceptCredentials

로그인 단계 중에만 발생합니다. 사용자 자격 증명이 제공되고 새 세션이 생성됩니다.

OnAuthReject

On-Auth-Reject 규칙을 포함하는 정책에 바인딩된 사용자에게 대해 인증이 실패한 경우 발생합니다. 이 이벤트는 인증이 실패한 후 사용자를 리디렉션하는 데 사용될 수도 있습니다.

OnAuthAccept 및 OnAuthReject 이벤트는 인증 시점(사용자가 사용자 이름 및 암호를 입력할 때)과 유효성 검사 시점(사용자 정보를 찾기 위해 사용자 쿠키를 읽을 때)에 모두 실행됩니다. 하지만 다음과 같은 몇 가지 특수한 작업은 인증 시점에만 발생합니다.

영역 시간 만료 재정의(EnforceRealmTimeouts 가 사용되지 않는 경우)

웹 에이전트가 EnforceRealmTimeouts 옵션을 지원하며 이 옵션이 사용되도록 설정된 경우가 아니면, 사용자의 유효 시간 만료 및 최대 시간 만료는 사용자가 마지막으로 인증한 영역에 대한 값으로 유지됩니다. 이 값은 사용자가 자격 증명을 다시 입력해야 하는 경우에만 변경됩니다.

리디렉션

무한 리디렉션 루프를 방지하기 위해 리디렉션은 인증 시에만 허용됩니다.

사용자 암호에 대한 액세스

암호는 **SMSESSION** 쿠키에 저장되지 않으므로 이 작업은 사용자가 실제로 암호를 입력할 때(인증 시)에만 사용 가능합니다.

참고: **OnAuth** 이벤트의 결과는 영역마다 다릅니다. 예를 들어 사용자가 영역 A에서 영역 B로 이동하며 영역 A에서 **OnAuthAccept** 헤더를 가지고 있는 경우 영역 B에서는 이 헤더를 사용할 수 없습니다. 사용자가 다시 영역 A로 돌아가면 헤더가 다시 설정됩니다.

OnAuthAttempt

SiteMinder가 사용자를 알 수 없어 이 사용자가 거부된 경우 발생합니다. 예를 들어 등록되지 않은 사용자는 먼저 등록 페이지로 리디렉션될 수 있습니다.

OnAuthChallenge

사용자 지정 챌린지-응답 인증 체계가 활성화된 경우(예: 토큰 코드) 발생합니다.

OnAuthUserNotFound

이 이벤트는 활성 응답을 트리거하는 데만 사용됩니다. 활성 응답이 아닌 다른 응답을 트리거하려면 이 이벤트를 사용하지 마십시오.

인증 이벤트 작업을 포함하는 규칙은 정책에서 **SiteMinder** 응답과 짝을 이룰 수 있습니다. 사용자가 인증되거나 거부되면 정책 서버는 해당 **On-Auth** 규칙과 연관된 응답을 다시 요청 에이전트로 전달합니다.

참고: **SiteMinder** 성능을 최적화하고 웹 에이전트가 정책 서버에서 정적 정보를 가져와야 하는 횟수를 제한할 수 있습니다. 성능을 최적화하려면 **OnAuthAccept** 인증 이벤트 기반 규칙을 설정하고 정적 정보를 반환하는 응답을 생성하십시오. 정책에서 규칙과 응답을 바인딩하면 정책에 지정된 사용자에게 규칙이 실행됩니다. 정적 응답은 성공적으로 인증한 사용자에게만 반환됩니다.

권한 부여 이벤트

권한 부여 이벤트는 **SiteMinder**가 사용자에게 리소스에 대한 액세스 권한이 부여되는지 여부를 확인할 때 발생합니다. 권한 부여 이벤트는 규칙 작업으로 정책 서버가 권한 부여 프로세스의 특정 시점에서 규칙을 실행하도록 합니다.

다음은 사용할 수 있는 권한 부여 이벤트의 목록입니다.

OnAccessAccept

성공적인 권한 부여의 결과로 발생합니다. 이 이벤트는 리소스에 대한 액세스 권한이 부여된 사용자를 리디렉션하는 데 사용할 수 있습니다.

OnAccessReject

실패한 권한 부여의 결과로 발생합니다. 이 이벤트는 리소스에 대한 액세스 권한이 부여되지 않은 사용자를 리디렉션하는 데 사용할 수 있습니다.

권한 부여 이벤트 작업을 포함하는 규칙은 정책에서 SiteMinder 응답과 짝을 이룰 수 있습니다. 사용자가 권한을 부여받거나 거부되면 정책 서버는 해당 On-Access 규칙과 연결된 응답을 다시 요청 에이전트로 전달합니다.

가장 이벤트

가장을 사용하면 권한 있는 사용자가 권한 있는 사용자의 세션을 종료하지 않고도 다른 사용자의 역할을 가장할 수 있습니다. 가장 이벤트는 리소스에 액세스할 때 가장 세션을 시작하는 데 사용됩니다.

가능한 가장 이벤트는 다음과 같습니다.

ImpersonationStart

적절한 정책에 포함된 경우 이 이벤트가 포함된 규칙은 가장 세션이 시작될 수 있도록 합니다.

ImpersonationStartUser

적절한 정책에 포함된 경우 이 이벤트가 포함된 규칙은 사용자 집합을 가장할 수 있도록 합니다.

고급 규칙 옵션

"고급" 옵션을 사용하여 추가 규칙 설정을 정의할 수 있습니다.

시간 제한

규칙이 실행되어야 할 때와 실행되지 않아야 할 때를 지정합니다.

활성 규칙

외부 비즈니스 논리를 기반으로 동적 권한 부여를 허용합니다.

추가 정보:

[규칙에 시간 제한 추가](#) (페이지 582)

웹 에이전트 작업을 위한 규칙 구성

지정된 웹 에이전트 작업에 대한 응답으로 적용되며 규칙으로 보호되는 리소스에 대한 액세스를 허용하거나 거부하는 규칙을 생성할 수 있습니다.

참고: CA SOA Security Manager XML Agent 에 대한 규칙도 생성할 수 있습니다. 이 에이전트 유형에 대한 규칙을 생성할 때는 ProcessSOAP 및 ProcessXML 의 두 가지 추가적인 규칙 작업을 사용할 수 있습니다. 자세한 내용은 *CA SOA Security Manager Policy Configuration Guide*(CA SOA Security Manager 정책 구성 안내서)를 참조하십시오.

다음 단계를 수행하십시오.

1. "정책", "도메인", "규칙"을 클릭합니다.
2. "규칙 만들기"를 클릭합니다.
3. 목록에서 도메인을 선택한 후 "다음"을 클릭합니다.
4. 규칙으로 보호할 리소스가 포함된 영역을 선택하고 "다음"을 클릭합니다.

참고: 보호할 리소스에 대한 영역이 없는 경우에는 해당 리소스를 보호하기 위한 규칙을 생성할 수 없습니다.

5. 규칙의 이름과 설명을 입력합니다.

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

6. 규칙으로 보호할 리소스를 입력합니다.

"유효 리소스"가 업데이트되어 리소스가 포함됩니다.

7. 규칙이 보호된 리소스에 대한 액세스를 허용할지 아니면 거부할지 지정합니다.

8. 웹 에이전트 작업을 선택합니다.

"작업 목록"이 HTTP 작업으로 채워집니다.

9. 하나 이상의 HTTP 작업을 선택합니다.

10. (선택 사항) "고급"에서 시간 제한이나 활성 규칙 또는 둘 모두를 지정합니다.
11. "마침"을 클릭합니다.
웹 에이전트 작업에 대한 규칙이 생성됩니다.

인증 이벤트 작업을 위한 규칙 구성

사용자가 리소스에 액세스하기 위한 인증이 이루어질 때 수행되는 작업을 제어하는 인증 이벤트 작업에 대한 규칙을 구성할 수 있습니다.

규칙이 만들어질 영역은 인증 이벤트를 처리할 수 있어야 합니다. "인증 이벤트 처리" 옵션이 선택되어 있는지 확인합니다.

다음 단계를 수행하십시오.

1. "정책", "도메인", "규칙"을 클릭합니다.
2. "규칙 만들기"를 클릭합니다.
3. 목록에서 도메인을 선택한 후 "다음"을 클릭합니다.
4. 규칙으로 보호할 리소스가 포함된 영역을 선택하고 "다음"을 클릭합니다.

참고: 보호할 리소스에 대한 영역이 없는 경우에는 해당 리소스를 보호하기 위한 규칙을 생성할 수 없습니다.

5. 규칙의 이름과 설명을 입력합니다.

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

6. 인증 이벤트를 선택합니다.

"작업 목록"이 인증 이벤트로 채워집니다.

참고: 인증 이벤트는 영역 전체에 적용되므로 "리소스" 필드는 비활성화됩니다. "액세스 허용" 및 "액세스 거부" 옵션 역시 인증 이벤트에 적용되지 않으므로 비활성화됩니다.

7. 하나 이상의 인증 이벤트를 선택합니다.
8. (선택 사항) "고급"에서 시간 제한 또는 활성 규칙 설정을 지정합니다.
9. "마침"을 클릭합니다.

규칙이 저장되고 지정된 영역 및 리소스에 적용됩니다.

권한 부여 이벤트 작업을 위한 규칙 구성

권한 부여 이벤트는 사용자가 인증된 후에 발생합니다. 사용자가 요청한 리소스에 대해 권한이 부여되었는지 여부를 기준으로 하여 SiteMinder 호출이 응답할 수 있도록 권한 부여 규칙을 구성합니다. 사용자가 자신의 권한에 따라 액세스가 허용 또는 거부될 때 적절한 이벤트가 트리거됩니다.

규칙이 만들어질 영역은 권한 부여 이벤트를 처리할 수 있어야 합니다. "권한 부여 이벤트 처리" 옵션이 선택되어 있는지 확인합니다.

다음 단계를 수행하십시오.

1. "정책", "도메인", "규칙"을 클릭합니다.
2. "규칙 만들기"를 클릭합니다.
3. 목록에서 도메인을 선택한 후 "다음"을 클릭합니다.
4. 규칙으로 보호할 리소스가 포함된 영역을 선택하고 "다음"을 클릭합니다.

참고: 보호할 리소스에 대한 영역이 없는 경우에는 해당 리소스를 보호하기 위한 규칙을 생성할 수 없습니다.

5. 규칙의 이름과 설명을 입력합니다.

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

6. 규칙으로 보호할 리소스를 입력합니다.

"유효 리소스"가 업데이트되어 리소스가 포함됩니다.

7. 권한 부여 이벤트를 선택합니다.

"작업 목록"이 권한 부여 이벤트로 채워집니다.

참고: "액세스 허용" 및 "액세스 거부" 옵션은 비활성화됩니다. 권한 부여 이벤트에는 이러한 옵션이 적용되지 않기 때문입니다.

8. 하나 이상의 권한 부여 이벤트를 선택합니다.
9. (선택 사항) "고급"에서 시간 제한이나 활성 규칙 또는 둘 모두를 설정합니다.
10. 제출을 클릭합니다.

규칙이 저장되고 지정된 영역 및 리소스에 적용됩니다.

OnAccessReject 규칙에 대한 정책 고려 사항

OnAccessReject 이벤트가 포함된 전역 규칙을 생성할 때는 OnAccessReject 규칙에 의해 발생하는 특수한 상황과 전역 정책이 정책 서버에서 처리되는 방식을 고려하십시오.

OnAccessReject 규칙은 GET/POST 규칙과 동일한 정책에 있는 경우에는 실행되지 않습니다. 사용자가 인증되면 SiteMinder 는 사용자의 아이덴티티를 확인합니다. 따라서 OnAccessReject 규칙과 GET/POST 규칙이 동일한 정책에 있는 경우에는 리소스에 대한 액세스가 허용된 사용자와 OnAccessReject 이벤트에서 리디렉션되는 사용자가 동일하게 됩니다. 해당 사용자는 액세스가 허용되었으므로 거부 이벤트가 적용되지 않습니다.

이 모순을 해결하려면 OnAccessReject 규칙에 대한 별도의 정책(다른 이벤트 규칙도 포함될 수 있음)을 생성하고 이 정책을 적용할 사용자를 지정하십시오.

예를 들어 LDAP 사용자 디렉터리에서 User1 이 리소스에 액세스할 수 있어야 하고 ou=People, o=company.com 그룹의 다른 모든 사용자는 OnAccessReject 페이지로 리디렉션되어야 하는 경우, 다음 두 개의 정책이 필요합니다.

정책 1

User1 의 액세스를 허용하는 GET/POST 규칙을 포함합니다.

정책 2

OnAccessReject 규칙과 리디렉션 응답을 포함하고 ou=People, o=company.com 그룹을 지정합니다.

User1 은 권한이 부여되었으므로 User1 이 리소스에 액세스할 때는 OnAccessReject 규칙이 실행되지 않습니다. 그러나 ou=People, o=company.com 그룹에 있는 다른 모든 사용자의 경우에는 리소스에 대한 액세스 권한이 부여되지 않았으므로 OnAccessReject 규칙이 실행됩니다.

가장 이벤트 작업을 위한 규칙 구성

리소스에 액세스할 때 가장 세션을 시작하기 위한 가장 이벤트에 대한 규칙을 구성할 수 있습니다.

다음 단계를 수행하십시오.

1. "정책", "도메인", "규칙"을 클릭합니다.
2. "규칙 만들기"를 클릭합니다.
3. 목록에서 도메인을 선택한 후 "다음"을 클릭합니다.
4. 규칙으로 보호할 리소스가 포함된 영역을 선택하고 "다음"을 클릭합니다.

참고: 보호할 리소스에 대한 영역이 없는 경우에는 해당 리소스를 보호하기 위한 규칙을 생성할 수 없습니다.

5. 규칙의 이름과 설명을 입력합니다.

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

6. 규칙으로 보호할 리소스를 입력합니다.

"유효 리소스"가 업데이트되어 리소스가 포함됩니다.

7. 가장 이벤트를 선택합니다.

"작업 목록"이 가장 이벤트로 채워집니다.

참고: "액세스 허용" 및 "액세스 거부" 옵션은 비활성화됩니다. 가장 이벤트에는 이러한 옵션이 적용되지 않기 때문입니다.

8. 하나 이상의 가장 이벤트를 선택합니다.
9. (선택 사항) "고급"에서 시간 제한이나 활성 규칙 또는 둘 모두를 설정합니다.
10. "마침"을 클릭합니다.

규칙이 저장되고 지정된 영역 및 리소스에 적용됩니다.

리소스 일치 및 정규식

규칙에서는 리소스 일치와 정규식 일치를 사용하여 영역의 리소스를 지정할 수 있습니다.

표준 리소스 일치

기본적으로 규칙에 대한 리소스 일치는 와일드카드로 수행됩니다.

다음 표에서는 리소스 일치에 대해 지원되는 문자를 설명합니다.

문자	사용
*	와일드카드(*)는 문자열의 모든 문자를 일치시키는 데 사용됩니다. 식 *.html 은 index.html, out.html 등과 같이 확장명이 .html 인 모든 파일과 일치합니다.
?	물음표(?)는 문자열의 단일 문자와 일치합니다. 식 lmn?p 는 하위 문자열 lmnop, lmneq 등과 일치합니다.

리소스 일치를 위한 정규식

정규식을 사용하면 리소스 일치의 유연성이 향상됩니다. 정규식 일치를 사용하려면 SiteMinder "규칙" 대화 상자에서 "정규식" 확인란을 선택하십시오.

정규식은 문자열 일치를 위해 사용되는 텍스트 패턴입니다. 다음 표에서는 정규식에 사용되는 구문의 예를 보여 줍니다.

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

문자	결과
$\wedge$	줄의 시작 부분에서만 일치
$\$$	줄의 끝 부분에서만 일치
A^*	A 와 0 번 이상 일치(확장)
A^+	A 와 1 번 이상 일치(확장)
$A?$	A 와 1 번 또는 0 번 일치(확장)
$A\{n\}$	A 와 정확히 n 번 일치(확장)
$A\{n,\}$	A 와 n 번 이상 일치(확장)
$A\{n,m\}$	A 와 n 번 이상 m 번 이하 일치(확장)
$A^*?$	A 와 0 번 이상 일치(축소)
$A^+?$	A 와 1 번 이상 일치(축소)
$A??$	A 와 0 번 또는 1 번 일치(축소)
AB	순서대로 A 및 B 와 일치
$A B$	A 또는 B 와 일치
$\backslash 1$	첫 번째 괄호 안의 하위 식에 대한 후참조
$\backslash n$	n 번째 괄호 안의 하위 식에 대한 후참조

제한: 각 정규식에는 해당 식 자체를 포함하여 하위 식을 10 개까지만 포함할 수 있습니다. 하위 식의 개수는 정규식의 왼쪽 괄호(여는 괄호) 수와 식 자체의 왼쪽 괄호 한 개를 더한 수와 같습니다.

규칙을 사용하거나 사용하지 않도록 설정

규칙이 사용되도록 설정하여 SiteMinder 가 지정된 리소스를 보호하도록 하거나, 규칙이 사용되지 않도록 설정하여 SiteMinder 가 지정된 리소스를 보호하지 않도록 할 수 있습니다.

규칙이 사용되는 경우에는 해당 규칙이 포함된 정책이 이미 생성되었고 해당 규칙에 액세스하려는 사용자가 정책에 지정된 그룹의 구성원이 아닌 한 아무도 보호된 리소스에 액세스할 수 없습니다. 정책이 적용되기 전에 리소스에 대한 액세스를 허용하려면 규칙이 사용되지 않도록 설정하면 됩니다.

다음 단계를 수행하십시오.

1. 규칙을 엽니다.
2. 규칙을 사용하려면 "사용" 확인란을 선택하고, 사용하지 않으려면 "사용" 확인란의 선택을 취소합니다.
3. 제출을 클릭합니다.
규칙이 저장됩니다.

고급 규칙 옵션

"규칙" 창의 "고급" 그룹 상자에서는 추가 규칙 설정을 정의할 수 있습니다. 이 그룹 상자에서 시간 제한과 활성 규칙을 설정할 수 있습니다. 시간 제한과 활성 규칙은 다음 단원에서 설명합니다.

규칙에 시간 제한 추가

SiteMinder 에서 규칙을 실행하는 시간을 지정하는 시간 제한을 구성합니다.

예를 들어 시간 제한을 월요일 - 금요일, 오전 9 시 - 오후 5 시 사이로 구성하면 SiteMinder 가 지정된 시간 동안에만 규칙을 실행하도록 지정됩니다. 규칙이 실행되도록 설정되면 사용자가 리소스에 액세스할 수 있습니다. 지정된 시간 범위가 아니면 리소스를 사용할 수 없습니다.

참고: SiteMinder 가 여러 표준 시간대 간에 시간을 처리하는 방법에 대한 자세한 내용은 웹 에이전트 및 정책 서버에서 시간이 계산되는 방식을 참조하십시오.

다음 단계를 수행하십시오.

1. "시간 제한" 그룹 상자에서 "설정"을 클릭합니다.

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

2. 시작 날짜와 만료 날짜를 지정합니다.

3. "Hourly Restrictions"(시간별 제한) 표에서 시간 제한을 지정합니다.

참고: 각 확인란은 1 시간을 나타냅니다. 확인란을 선택하면 해당 시간 동안 규칙이 실행되고 지정된 리소스에 규칙이 적용됩니다. 확인란의 선택을 취소하면 해당 시간 동안 규칙이 실행되지 않고 지정된 리소스에 규칙이 적용되지 않습니다.

4. "확인"을 클릭합니다.

시간 제한이 저장되고 규칙 설정이 나타납니다.

활성 규칙 구성

외부 비즈니스 논리를 기반으로 동적 권한 부여에 대한 활성 규칙을 구성합니다. 정책 서버가 고객이 제공한 공유 라이브러리에서 함수를 호출합니다. 이 공유 라이브러리는 소프트웨어 개발 키트에서 제공되는 권한 부여 API에 지정된 인터페이스를 준수해야 합니다.

다음 단계를 수행하십시오.

1. "활성 규칙" 그룹 상자의 필드에서 라이브러리 이름, 함수 이름 및 함수 매개 변수를 지정합니다.

활성 규칙 문자열이 "활성 규칙" 필드에 표시됩니다.

2. 제출을 클릭합니다.

활성 규칙이 저장됩니다.

규칙 삭제

규칙을 삭제하면 해당 규칙이 포함된 정책에서 이 규칙이 자동으로 제거됩니다. 그러나 정책은 시스템에 유지됩니다. 삭제된 규칙 없이도 정책이 작동하는지 확인하십시오.

참고: 정책에는 규칙이 하나 이상 포함되어야 합니다.

규칙 그룹에 포함된 규칙을 삭제할 경우 삭제된 규칙이 규칙 그룹에서 제거되는 데는 몇 초 정도 걸릴 수 있습니다. 또한 삭제된 모든 개체가 짧은 시간 내에 캐시에서 제거될 수도 있습니다.

참고: 정책 서버 개체의 수정 및 삭제에 대한 자세한 내용은 정책 서버 개체 관리를 참조하십시오.

제 15 장: 규칙 그룹

이 섹션은 다음 항목을 포함하고 있습니다.

[규칙 그룹 개요](#) (페이지 585)

[규칙 그룹 만들기](#) (페이지 586)

[규칙을 규칙 그룹에 추가](#) (페이지 587)

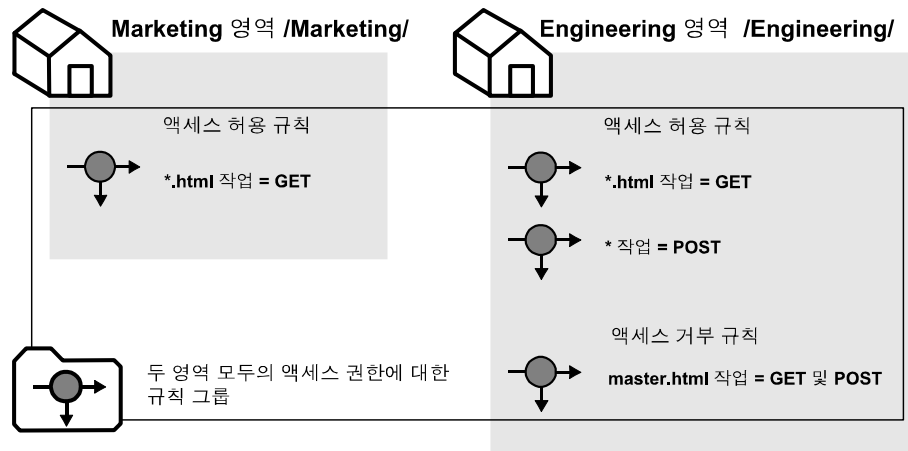
[규칙 그룹 수정](#) (페이지 587)

[규칙 그룹 삭제](#) (페이지 588)

규칙 그룹 개요

규칙 그룹은 SiteMinder 정책에 바인딩할 수 있는 규칙 집합입니다. 규칙 그룹을 사용하여 동일한 정책에 적용할 규칙의 그룹을 조합할 수 있습니다. 예를 들어 웹 사이트의 다양한 리소스에 대한 GET 작업을 허용하는 여러 규칙이 있는 경우 모든 리소스를 포함하는 규칙 그룹을 생성할 수 있습니다. 이러한 규칙을 포함할 정책을 구성할 경우 모든 규칙을 개별적으로 추가하는 대신 단일 규칙 그룹을 정책에 추가할 수 있습니다.

정책에 규칙 그룹을 포함할 경우 그룹의 각 규칙은 그룹의 다른 규칙과는 독립적으로 평가되고 적용됩니다.



위 다이어그램에서는 Marketing 영역과 Engineering 영역 모두에 대한 규칙이 포함된 규칙 그룹을 보여 줍니다. 정책에 네 개의 모든 규칙을 개별적으로 포함하는 대신 규칙 그룹을 사용할 수 있습니다.

추가 정보:

[정책 개요](#) (페이지 621)

규칙 그룹 만들기

규칙 그룹을 생성하여 도메인에 추가할 수 있습니다.

다음 단계를 수행하십시오.

1. "정책", "도메인", "규칙 그룹"을 클릭합니다.
2. "규칙 그룹 만들기"를 클릭합니다.
3. "확인"을 클릭합니다.
4. 도메인을 선택하고 "다음"을 클릭합니다.
5. 규칙 그룹의 이름과 설명을 입력합니다.
6. Radius 또는 SiteMinder 및 에이전트 유형을 선택합니다.
7. "그룹 구성원"에서 "추가/제거"를 클릭합니다.

지정된 도메인 및 지정된 에이전트 유형과 연결된 영역에 정의된 모든 규칙이 "사용 가능한 구성원" 열에 나열됩니다. 에이전트 유형이 "일반 RADIUS"인 경우 "사용 가능한 구성원" 열에는 RADIUS 에이전트가 지원하는 모든 규칙이 나열됩니다.

8. "사용 가능한 구성원" 목록에서 하나 이상의 규칙을 선택하고 오른쪽 방향 화살표를 클릭합니다.

한 번에 여러 구성원을 선택하려면 Ctrl 키를 누른 채 추가 구성원을 클릭하십시오. 구성원 블록을 선택하려면 첫 번째 구성원을 클릭한 다음 Shift 키를 누른 채 블록의 마지막 구성원을 클릭하십시오.

9. "확인"을 클릭합니다.
10. "마침"을 클릭합니다.

규칙 그룹이 생성됩니다.

규칙을 규칙 그룹에 추가

동일한 도메인에 있고 에이전트 유형이 동일한 규칙 그룹에 규칙을 추가할 수 있습니다.

다음 단계를 수행하십시오.

1. "정책", "도메인", "규칙 그룹"을 클릭합니다.
2. 검색 조건을 지정하고 "검색"을 클릭합니다.
3. 수정할 규칙 그룹의 이름을 클릭합니다.
4. "수정"을 클릭합니다.

설정과 컨트롤이 활성화됩니다.

5. "그룹 구성원"에서 "추가/제거"를 클릭합니다.

참고: 지정된 도메인 및 지정된 에이전트 유형과 연결된 영역에 정의된 모든 규칙이 "사용 가능한 구성원" 열에 나열됩니다. 에이전트 유형이 "일반 RADIUS"인 경우 "사용 가능한 구성원" 열에는 RADIUS 에이전트가 지원하는 모든 규칙이 나열됩니다.

6. "사용 가능한 구성원" 목록에서 하나 이상의 규칙을 선택하고 오른쪽 방향 화살표를 클릭합니다.

참고: 한 번에 여러 구성원을 선택하려면 Ctrl 키를 누른 채 추가 구성원을 클릭하십시오. 구성원 블록을 선택하려면 첫 번째 구성원을 클릭한 다음 Shift 키를 누른 채 블록의 마지막 구성원을 클릭하십시오.

7. "확인"을 클릭합니다.
8. 제출을 클릭합니다.

선택된 규칙이 규칙 그룹에 추가됩니다.

규칙 그룹 수정

SiteMinder 에이전트의 에이전트 유형과 RADIUS 에이전트의 공급업체 유형을 제외하고 규칙 그룹의 모든 속성을 수정할 수 있습니다. 에이전트 유형이나 공급업체 유형을 변경하려면 규칙 그룹을 삭제하고 새 규칙 그룹을 생성하십시오.

참고: 정책 서버 개체의 수정 및 삭제에 대한 자세한 내용은 정책 서버 개체 관리를 참조하십시오.

규칙 그룹 삭제

규칙 그룹을 삭제하면 그룹만 삭제되고 그룹에 포함된 규칙은 삭제되지 않습니다.

참고: 정책 서버 개체의 수정 및 삭제에 대한 자세한 내용은 정책 서버 개체 관리를 참조하십시오.

제 16 장: 응답 및 응답 그룹

이 섹션은 다음 항목을 포함하고 있습니다.

[응답](#) (페이지 589)

[응답 구성](#) (페이지 592)

[개방 형식 쿠키를 생성하는 웹 에이전트 응답을 생성하는 방법](#) (페이지 601)

[SiteMinder 생성 사용자 특성](#) (페이지 610)

[응답 그룹](#) (페이지 617)

응답

응답은 정책 서버에서 SiteMinder 에이전트로 정적 텍스트, 사용자 특성, DN 특성, 사용자 지정 활성 응답 또는 정의된 변수의 런타임 값을 전달합니다. 응답은 서블릿, 웹 응용 프로그램 또는 기타 사용자 지정 응용 프로그램에서 사용자 지정 콘텐츠를 표시하거나 SiteMinder 설정을 변경하거나 사용자를 다른 리소스로 리디렉션하는 데 사용될 수 있습니다. 웹 응용 프로그램에서 작업 중인 경우에는 세부적인 액세스 제어를 위한 권한으로 응답을 사용할 수 있습니다.

정책에는 사용자 및 사용자 그룹에 바인딩된 규칙 및 응답이 포함됩니다. 정책에서 응답은 특정 규칙 또는 규칙 그룹에 바인딩됩니다. 규칙이 실행되면 연결된 응답이 SiteMinder 에이전트에 정보를 반환합니다.

응답은 이름/값 쌍의 형태를 지닙니다. 규칙이 트리거되면 정책 서버는 쌍으로 연결된 응답을 SiteMinder 에이전트에 반환합니다.

예를 들어 사용자가 보호된 웹 페이지에 액세스하려고 하는데 해당 페이지의 내용을 볼 수 있는 권한이 부여되어 있지 않으면 응답을 통해 사용자에게 액세스 권한이 없음을 나타내는 HTML 페이지로 사용자가 리디렉션되고 시스템 관리자에 문의하기 위한 상세 정보가 제공됩니다.

웹 에이전트의 경우 SiteMinder 는 규칙에 명명된 웹 리소스 또는 응용 프로그램에서 응답을 사용할 수 있도록 HTTP 헤더 변수나 HTTP 쿠키 변수에 응답 특성을 추가합니다. RADIUS 환경에서는 응답이 RADIUS 클라이언트에 반환됩니다.

응답 유형

응답은 하나 이상의 응답 특성에 대한 컨테이너입니다. 응답 특성은 정책 서버가 응답을 처리한 후 **SiteMinder** 에이전트가 받는 항목입니다. 가능한 응답 특성은 응답의 유형에 따라 달라집니다.

다음과 같은 유형의 응답을 사용할 수 있습니다.

- 웹 에이전트 응답
- RADIUS 응답

참고: 소프트웨어 개발 키트와 별도로 제공되는 **SiteMinder API** 를 사용하여 사용자 지정 에이전트의 응답 유형과 응답 특성을 생성할 수 있습니다. 자세한 내용은 "**API Reference Guide for C**"(C 용 API 참조 안내서)를 참조하십시오.

웹 에이전트 응답

웹 에이전트 응답은 **SiteMinder** 웹 에이전트가 사용할 수 있는 이름/값 쌍을 제공하는 **SiteMinder** 응답입니다. 이러한 응답에는 **HTTP** 헤더 변수, 쿠키 변수 및 리디렉션용 **URL** 에 대한 특성이 포함될 수 있습니다.

RADIUS 응답

RADIUS 응답은 RADIUS 에이전트가 사용할 수 있는 값을 제공하는 **SiteMinder** 응답입니다. 이러한 응답에는 지원되는 모든 RADIUS 특성에 대한 응답 특성이 포함될 수 있습니다.

추가 정보:

[RADIUS 에이전트 응답 특성](#) (페이지 591)

응답 특성

각 **SiteMinder** 응답에는 하나 이상의 응답 특성이 포함됩니다. 이러한 특성은 응답의 유형에 따라 달라집니다. 다음 단원에서는 각 응답 유형에 사용할 수 있는 응답 특성에 대해 설명합니다.

eTrust SOA Security Manager 웹 에이전트 응답 특성

SiteMinder 웹 에이전트 응답 특성에 추가하여 eTrust SOA Security Manager 는 WSS 에이전트에서만 사용 가능한 다음과 같은 웹 에이전트 응답 특성을 제공합니다.

WebAgent-SAML-Session-Ticket-Variable

[set AGENT value for your book]가 SAML 어설션을 생성하는 데 사용하는 정책 서버 데이터를 제공합니다. 이 데이터는 연결된 응답 특성에 지정된 대로 XML 메시지 HTTP 나 SOAP 봉투 헤더 또는 쿠키에 삽입됩니다.

SAML 세션 티켓 응답을 구성할 경우 정책 서버는 응답 데이터를 생성합니다. 이 데이터는 [set AGENT value for your book]에 어설션을 작성하는 방법을 알려 줍니다. [set AGENT value for your book]는 세션 티켓과 웹 서비스 소비자의 공개 키(선택 사항)를 암호화하고 응답 데이터도 암호화합니다. 그런 다음 에이전트는 어설션을 생성합니다. 에이전트는 어설션을 웹 서비스로 전송합니다. 토큰은 [set AGENT value for your book]에서 해당 에이전트 키로만 암호화 및 암호 해독할 수 있습니다.

WebAgent-WS-Security-Token

연결된 응답 특성에 지정된 대로 [set AGENT value for your book]가 WS-보안 사용자 이름, X509v3 또는 SAML 토큰을 생성하는 데 사용하는 정책 서버 데이터를 제공합니다. 이러한 토큰은 SOAP 메시지 헤더에 추가됩니다.

WS-보안 응답을 구성할 경우 정책 서버는 응답 데이터를 생성합니다. 이 데이터는 [set AGENT value for your book]에 토큰을 작성하는 방법을 알려 줍니다. 그러면 에이전트는 토큰을 생성하여 SOAP 요청에 추가하고 이를 웹 서비스로 전송합니다.

RADIUS 에이전트 응답 특성

RADIUS 에이전트 응답 특성은 RADIUS 에이전트가 해석할 수 있는 응답 특성입니다. SiteMinder 가 지원하는 모든 응답 특성은 RADIUS 프로토콜이 지원하는 특성을 설명하는 RFC(Request for Comments) 2138 에 설명된 특성에 해당합니다.

응답 및 디렉터리 매핑

디렉터리 매핑을 사용하여 응용 프로그램 개체 구성 요소 또는 영역에서 개별 권한 부여 사용자 디렉터리를 지정할 수 있습니다. 개별 권한 부여 디렉터리를 정의할 경우 사용자는 한 디렉터리에 포함된 정보를 기반으로 인증되고 다른 디렉터리에 포함된 정보를 기반으로 권한이 부여됩니다.

응답을 생성하여 인증(OnAuth) 이벤트와 연결할 경우 사용자 디렉터리에서 검색되는 모든 정보가 인증 디렉터리에서 검색됩니다. 권한 부여(OnAccess) 이벤트를 생성할 경우 사용자 디렉터리에서 검색되는 모든 정보가 권한 부여 디렉터리에서 검색됩니다.

응답 구성

에이전트 유형 및 특성 목록을 지정하여 응답을 생성할 수 있습니다. 응답은 지정된 특성을 포함하여 지정된 에이전트로 전송됩니다.

다음 단계를 수행하십시오.

1. "정책", "도메인", "응답"을 클릭합니다.
2. "응답 만들기"를 클릭합니다.
3. 도메인을 선택하고 "다음"을 클릭합니다.
4. 응답의 이름과 설명을 입력합니다.
5. Radius 또는 SiteMinder 및 에이전트 유형을 선택합니다.
6. (선택 사항) "응답 특성 만들기"를 클릭하여 응답 특성을 생성하고 특성 목록에 추가합니다.
7. "마침"을 클릭합니다.
응답이 생성됩니다.

응답 특성 구성

각 SiteMinder 응답에는 응답 특성이 하나 이상 포함될 수 있습니다. 응답 특성은 정책 서버가 SiteMinder 에이전트에 전달하는 정보의 일부를 식별합니다. 각 SiteMinder 에이전트 유형마다 서로 다른 응답 특성을 허용할 수 있습니다.

참고: SiteMinder 에서 CA Single Sign-On 으로 의 싱글 사인온이 사용되도록 설정하는 데 필요한 smetssocookie 웹 에이전트 활성 응답 특성을 구성하는 방법에 대한 자세한 내용은 smetssocookie 웹 에이전트 활성 응답 특성 구성을 참조하십시오.

응답 특성 유형

SiteMinder 에서는 여러 응답 특성 유형을 지원합니다. 응답 특성 유형에 따라 SiteMinder 가 특성에 적절한 콘텐츠를 제공하는 방식이 달라집니다.

SiteMinder 응답에 응답 특성을 추가할 때 다음 유형의 응답 특성을 지정할 수 있습니다.

정적

일정하게 유지되는 데이터를 반환합니다.

SiteMinder 응답의 일부로 문자열을 반환하려면 정적 특성을 사용하십시오. 이 응답 유형은 웹 응용 프로그램에 정보를 제공하는 데 사용할 수 있습니다. 예를 들어 웹 사이트의 사용자 지정된 특정 콘텐츠가 사용자 그룹에 있는 경우 정적 응답 특성 `show_button = yes` 가 응용 프로그램에 전달될 수 있습니다.

사용자 특성

사용자 디렉터리의 사용자 항목에서 프로필 정보를 반환합니다.

LDAP, WinNT, Microsoft SQL Server 또는 Oracle 사용자 디렉터리에서 사용자 특성을 검색할 수 있습니다.

참고: 정책 서버가 사용자 디렉터리 특성의 값을 응답 특성으로 반환하도록 하려면 SiteMinder 사용자 디렉터리 창에서 사용자 디렉터리를 구성하십시오.

DN 특성

LDAP, Microsoft SQL Server 또는 Oracle 사용자 디렉터리의 디렉터리 개체에서 프로필 정보를 반환합니다.

사용자 DN 의 일부인 사용자 그룹 및 OU(조직 단위)가 DN 특성으로 처리될 수 있는 디렉터리 개체 특성의 예입니다.

예를 들어 DN 특성을 사용하여 한 사업부의 사용자 구성원 자격을 기반으로 이 사용자의 회사 사업부를 반환할 수 있습니다.

참고: 정책 서버가 DN 특성의 값을 응답 특성으로 반환하도록 하려면 SiteMinder 사용자 디렉터리 창에서 사용자 디렉터리를 구성하십시오.

활성 응답

SiteMinder 권한 부여 API 를 기반으로 하는 고객이 제공한 라이브러리에서 값을 반환합니다.

활성 응답은 외부 원본의 정보를 반환하는 데 사용됩니다. 정책 서버가 고객이 제공한 공유 라이브러리의 함수를 호출하게 하면 활성 응답이 생성됩니다. 이 공유 라이브러리는 권한 부여 API(소프트웨어 개발 키트와 별도로 제공)를 준수합니다.

참고: 반환된 값이 유효한지 확인하십시오. 응답 특성을 구성할 때 응답 특성에 대한 올바른 값 유형이 "응답 특성" 창에 표시됩니다.

변수 정의

런타임에 지정된 변수의 값을 변환합니다.

이미 정의된 변수 목록에서 변수를 선택 및 사용하려면 "변수 정의"를 선택하십시오.

세션 변수

세션 변수 값을 반환합니다.

응답이 인증 요청의 일부인 경우 SiteMinder 는 세션 저장소나 메모리에서 값을 검색합니다.

식

관리자가 식을 제공할 수 있습니다.

예를 들어 관리자는 인증서 issuerDN 특성에서 특정 문자열을 추출하여 새 세션 변수로 저장하도록 응답 특성을 구성할 수 있습니다.

웹 에이전트 응답 특성 구성

"응답" 창의 "특성" 그룹 상자에서 "SiteMinder" 및 "웹 에이전트"를 선택하여 SiteMinder 웹 에이전트에 대한 응답 특성을 생성할 수 있습니다. 웹 에이전트 응답 특성은 HTTP 헤더 변수, 쿠키 변수, 다른 리소스로의 리디렉션, 텍스트 및 시간 만료 값을 지원합니다.

참고: SOA Security Manager 를 구매하여 설치한 경우 WebAgent-SAML-Session-Ticket-Variable 응답 특성을 생성할 수 있습니다. 자세한 내용은 *CA SOA Security Manager Policy Configuration Guide*(CA SOA Security Manager 정책 구성 안내서)를 참조하십시오.

다음 단계를 수행하십시오.

1. "응답 특성 만들기"를 클릭합니다.
2. 응답 특성을 선택합니다.
3. 특성 유형을 선택합니다.
"특성 필드"의 상세 정보가 지정한 특성 유형에 맞게 업데이트됩니다.
4. "특성 필드"에서 상세 정보를 입력합니다.

참고: 응답에서 사용할 수 있는 자동으로 생성된 SiteMinder 사용자 특성 목록은 [SiteMinder 생성 사용자 특성](#) (페이지 610)에 있습니다.

5. (선택 사항) "스크립트" 필드에서 특성을 편집합니다.
참고: "고급" 섹션에서 특성을 편집할 경우 "특성 설정" 섹션이 닫힙니다.
6. "캐시 값" 또는 "값 재계산 간격"을 초 단위로 지정합니다.
참고: 입력할 수 있는 최대 시간 제한은 3600 초입니다.
7. 제출을 클릭합니다.

응답 특성 만들기 태스크가 처리를 위해 제출되고 해당 응답 특성이 "응답" 페이지의 "특성 목록"에 추가됩니다.

RADIUS 응답 특성 구성

"응답" 창의 "특성" 그룹 상자에서 "RADIUS" 및 "RADIUS 공급업체"를 선택하여 RADIUS 에이전트에 대한 응답 특성을 생성할 수 있습니다. RADIUS 응답 특성은 RADIUS 프로토콜이 지원하는 모든 특성을 지원합니다.

다음 단계를 수행하십시오.

1. "응답 특성 만들기"를 클릭합니다.
2. 응답 특성을 선택합니다.
3. 특성 유형을 선택합니다.
"특성 필드"의 상세 정보가 지정한 특성 유형에 맞게 업데이트됩니다.
4. "특성 필드"에서 상세 정보를 입력합니다.

참고: 응답에서 사용할 수 있는 자동으로 생성된 SiteMinder 사용자 특성 목록은 [SiteMinder 생성 사용자 특성](#) (페이지 610)에 있습니다.

5. (선택 사항) "스크립트" 필드에서 특성을 편집합니다.

참고: "고급" 섹션에서 특성을 편집할 경우 "특성 설정" 섹션이 닫힙니다.

6. "캐시 값" 또는 "값 재계산 간격"을 초 단위로 지정합니다.

참고: 입력할 수 있는 최대 시간 제한은 3600 초입니다.

7. 제출을 클릭합니다.

응답 특성 만들기 태스크가 처리를 위해 제출되고 해당 응답 특성이 "응답" 페이지의 "특성 목록"에 추가됩니다.

응답의 변수 개체 사용

변수 개체를 응답 특성에 통합하여 변수 개체를 포함하는 응답을 생성할 수 있습니다. 응답 특성에 변수 개체를 사용하여 요청에 대한 권한 부여 중에 평가되는 동적 정보를 포함할 수 있습니다.

참고: 응답에 포함된 변수 개체는 요청에 대한 권한 부여 중에만 평가되고 인증 프로세스 중에는 평가되지 않습니다. 변수가 포함된 응답은 권한 부여 이벤트에만 사용할 수 있습니다.

응답에는 여러 응답 특성이 포함될 수 있습니다. 각 응답 특성에는 변수 개체가 하나씩 포함됩니다. HTTP 헤더 및 쿠키 변수와 마찬가지로 SiteMinder 변수 개체도 이름/값 쌍입니다. 그러나 SiteMinder 변수 개체는 런타임에 변수 개체 값을 조회하는 데 변수 개체 이름이 사용된다는 점에서 HTTP 헤더 및 쿠키 변수와 다릅니다. 응답 특성의 경우 결과 이름/값 쌍이 HTTP 헤더나 쿠키 변수에 반환될 수 있습니다.

변수가 포함된 응답 특성 구성

응답에는 변수 개체에 따라 값이 결정되는 응답 특성이 하나 이상 포함될 수 있습니다. 각 응답 특성에는 변수 개체가 하나씩 포함됩니다. 각 변수 개체는 이름-값 쌍입니다. 변수 개체의 이름은 런타임에 변수 개체의 값을 조회하는 데 사용됩니다. SiteMinder 는 결과 이름-값 쌍을 웹 에이전트에 전달합니다.

다음 단계를 수행하십시오.

1. 응답 구성의 설명에 따라 응답을 생성합니다.
2. "특성" 섹션에서 "에이전트 유형"으로 "SiteMinder" 및 "웹 에이전트"를 선택합니다.

3. "특성 목록" 섹션에서 "응답 특성 만들기"를 클릭합니다.
4. "특성 유형" 섹션의 드롭다운 목록에서 응답 특성을 선택합니다.
5. "특성 종류" 섹션에서 응답 특성의 유형을 선택합니다.
6. "특성 필드" 섹션의 "변수 이름" 필드에 변수 개체의 이름을 입력합니다.

참고: 이 필드가 필수 필드인 경우 SiteMinder 는 이 이름을 이름-값 쌍의 형태로 웹 에이전트에 전달합니다.

7. 선택한 응답 특성 유형에 대해 "특성 필드" 그룹 섹션에서 다음 필드를 완성합니다.

정적

"변수 값" 필드에 정적 변수의 값을 지정합니다.

사용자 특성

"특성 이름" 필드에 사용자 특성의 이름을 지정합니다.

DN 특성

"DN 사양" 필드에 사용자 또는 사용자 그룹의 DN 을, "특성 이름" 필드에 사용자 특성의 이름을 지정합니다.

(선택 사항) "조회"를 클릭하여 지정한 사용자 디렉터리에서 사용자 또는 사용자 그룹 집합을 검색하고 하나를 선택합니다.

(선택 사항) "중첩된 그룹 허용" 확인란을 선택합니다.

활성 응답

라이브러리 이름 및 라이브러리 함수 이름을 지정합니다. 필요한 경우 "라이브러리 이름", "함수 이름" 및 "매개 변수" 필드에 매개 변수 이름을 지정합니다.

참고: 라이브러리는 SiteMinder 권한 부여 API 을 기반으로 해야 합니다.

변수 정의

"조회"를 클릭하여 "변수" 필드의 기존 변수 개체를 선택합니다.

세션 변수

관리자가 값을 가져올 수 있는 세션 변수의 이름을 지정합니다.

식

특성에서 값을 추출하여 새 세션 변수로 저장하는 식을 지정합니다.

참고: SiteMinder 는 "특성 필드" 섹션의 필드에 제공된 정보를 사용하여 이름-값 쌍의 형태로 웹 에이전트에 전달할 값을 결정합니다.

8. "확인"을 클릭합니다.

응답 특성이 저장됩니다.

응답 특성에 포함할 사용자 선택

"사용자 조회" 창에서 응답 특성에 포함할 사용자 집합 또는 사용자 그룹을 하나 선택하여 사용자 디렉터리 하나를 선택하고 이 디렉터리에서 사용자 및 사용자 그룹 목록을 검색할 수 있습니다.

다음 단계를 수행하십시오.

1. "특성 설정" 그룹 상자에서 "특성 종류"로 "DN 특성"을 선택합니다.
"특성 필드" 그룹 상자가 확장되어 "DN 사양" 필드가 포함됩니다.
2. "특성 필드" 그룹 상자에서 "조회"를 클릭합니다.
3. 목록에서 사용자 디렉터리 하나의 이름을 선택하고 "검색"을 클릭합니다.
4. (선택 사항) "검색 유형"을 선택하고 "실행"을 클릭합니다.

특성-값

"사용자/그룹" 대화 상자의 필드에서 특성 이름 및 값을 지정합니다.

식

"사용자/그룹" 대화 상자의 "식" 필드에서 검색 식을 지정합니다.

참고: "재설정"을 클릭하면 검색 결과를 지울 수 있습니다.

5. 목록에서 사용자 집합 또는 사용자 그룹 하나를 선택하고 "확인"을 클릭합니다.
6. "확인"을 클릭합니다.

"응답 특성" 창이 다시 열리고 "특성 필드" 그룹 상자의 "DN 사양" 필드에 사용자 집합 또는 사용자 그룹이 추가됩니다.

변수 조회를 사용하여 변수 선택

"변수 선택" 창을 사용하여 기존 변수 개체 목록에서 변수 개체를 하나 선택할 수 있습니다.

다음 단계를 수행하십시오.

1. "특성 설정" 그룹 상자에서 "특성 종류"로 "변수 정의"를 선택합니다.
2. "특성 필드" 그룹 상자에서 "조회"를 클릭합니다.
3. 목록에서 변수 개체를 하나 선택하고 "확인"을 클릭합니다.

"응답 특성 만들기" 창이 다시 열리고 "특성 필드" 그룹 상자의 "변수" 필드에 변수 개체의 이름이 표시됩니다.

응답 특성 캐싱 구성

응답은 요청 에이전트에 값을 반환합니다. 에이전트에 반환되는 데이터는 고정값이거나 시간 경과에 따라 변경되는 값일 수 있습니다. SiteMinder 에이전트를 사용하여 리소스를 보호하는 경우 관련 정책이 실행될 때마다 값을 다시 계산할 필요가 없도록 에이전트가 고정 데이터의 값을 캐싱할 수 있습니다.

예를 들어 고객의 계정 번호는 고정값인 반면 고객의 계정 잔액은 거래가 있을 때마다 변경됩니다. 따라서 계정 번호는 한 번 검색한 후에 캐싱해 두는 것이 더 효율적입니다. 그러나 계정 잔액의 경우에는 정보를 최신 상태로 유지하기 위해 정기적으로 잔액을 다시 계산해야 할 수 있습니다.

참고: SiteMinder 는 RADIUS 응답 특성을 캐싱하지 않습니다.

다음 단계를 수행하십시오.

1. 응답을 엽니다.
"특성 목록" 그룹 상자에 연결된 응답 특성이 나열됩니다.
2. 원하는 응답 특성의 왼쪽에 있는 편집 아이콘을 클릭합니다.
3. "특성 캐싱" 그룹 상자에서 캐시 설정을 지정합니다.
4. 제출을 클릭합니다.
캐시 설정이 저장됩니다.

응답 편집

에이전트 유형을 제외한 모든 응답 속성을 편집할 수 있습니다. 에이전트 유형을 변경하려면 응답을 삭제하고 새 응답을 생성해야 합니다.

참고: 정책 서버 개체의 수정 및 삭제에 대한 자세한 내용은 정책 서버 개체 관리를 참조하십시오.

응답 삭제

응답을 삭제하면 연결된 모든 정책에서 해당 응답이 제거됩니다.

삭제된 모든 개체는 짧은 시간 내에 캐시에서 제거될 수 있습니다.

참고: 정책 서버 개체의 수정 및 삭제에 대한 자세한 내용은 정책 서버 개체 관리를 참조하십시오.

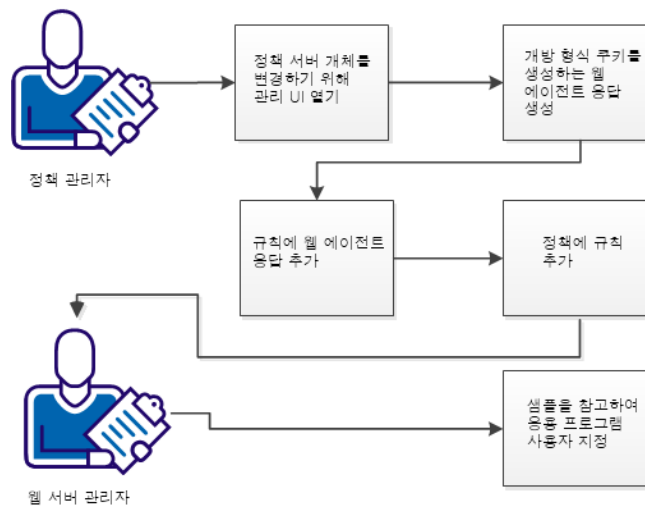
개방 형식 쿠키를 생성하는 웹 에이전트 응답을 생성하는 방법

조직에서 개방 형식 쿠키를 사용하는 경우 개방 형식 쿠키를 생성하도록 정책 서버의 에이전트 응답을 구성할 수 있습니다.

중요! SiteMinder 는 개방 형식 쿠키만 생성합니다. SiteMinder 는 응용 프로그램이 개방 형식 쿠키에 대해 변경한 내용을 인식하지 못합니다. 따라서 처리 중 발생하는 이벤트 순서에 따라 SiteMinder 가 개방 형식 쿠키를 덮어쓸 수도 있습니다. SiteMinder 는 사용자가 로그아웃할 때 개방 형식 쿠키를 자동으로 제거할 수 없습니다.

개방 형식 쿠키를 생성하도록 SiteMinder 를 구성한 후에는 웹 서버 관리자가 웹 응용 프로그램을 사용자 지정하여 개방 형식 쿠키의 정보를 사용할 수 있도록 해야 합니다. 제공된 샘플을 사용하십시오.

개방 형식 쿠키를 생성하는 웹 에이전트
응답 생성 방법



다음 단계를 수행하십시오.

1. [정책 서버 개체를 변경하기 위해 관리 UI 를 엽니다](#) (페이지 85).
2. [개방 형식 쿠키를 생성하는 웹 에이전트 응답을 생성합니다](#) (페이지 603).
3. [규칙에 웹 에이전트 응답을 추가합니다](#) (페이지 608).
4. [정책에 규칙을 추가합니다](#) (페이지 609).
5. [샘플을 참조하여 응용 프로그램을 사용자 지정합니다](#) (페이지 610).

정책 서버 개체 변경

관리 UI 를 열어 정책 서버의 개체를 변경합니다.

다음 단계를 수행하십시오.

1. 브라우저에서 다음 URL 을 엽니다.

`https://host_name:8443/iam/siteminder/adminui`

host_name

정규화된 관리 UI 호스트 시스템 이름을 지정합니다.

2. "사용자 이름" 필드에 SiteMinder 슈퍼 사용자 이름을 입력합니다.
3. "암호" 필드에 SiteMinder 슈퍼 사용자 계정 암호를 입력합니다.

참고: 슈퍼 사용자 계정 암호에 달러 -기호(\$) 문자가 있으면 달러 기호 문자의 각 인스턴스를 \$DOLLAR\$로 바꾸십시오. 예를 들어 SiteMinder 슈퍼 사용자 계정 암호가 \$password 이면 "암호" 필드에 \$DOLLAR\$password 를 입력하십시오.

4. "서버" 드롭다운 목록에 올바른 서버 이름 또는 IP 주소가 나타나는지 확인합니다.
5. "로그인"을 선택합니다.

개방 형식 쿠키를 생성하는 웹 에이전트 응답 생성

관리 UI 를 사용하여 개방 형식 쿠키를 생성하는 웹 에이전트 응답을 생성합니다.

다음 단계를 수행하십시오.

1. "정책", "도메인", "응답", "응답 만들기"를 차례로 클릭합니다.
2. 개방 형식 쿠키를 발급할 도메인에 해당하는 옵션 단추를 클릭합니다.
3. "다음"을 클릭합니다.
4. 다음 단계를 수행하여 개방 형식 쿠키를 생성하는 응답을 생성합니다.
 - a. 응답의 이름과 설명(선택 사항)을 입력합니다.
 - b. 다음 설정을 확인합니다.
 - SiteMinder 옵션 단추가 선택되어 있는지 확인합니다.
 - "웹 에이전트"가 "에이전트 유형" 드롭다운 목록에 나타나는지 확인합니다.
 - c. "응답 특성 만들기"를 클릭합니다.
 - d. "특성" 드롭다운 목록을 클릭하고 다음 값을 선택합니다.

WebAgent-HTTP-Open-Format-Cookie

- e. 다음 필드를 작성하십시오.

쿠키 이름

개방 형식 쿠키에 HTTP 헤더 변수로 반환되는 이름을 지정합니다.

제한: 인쇄 가능한 모든 ASCII 문자(!부터 ~까지 포함.; = 또는 공백 제외)

쿠키 도메인 범위

개방 형식 쿠키에 설정된 섹션(각 섹션의 문자는 섹션 사이의 마침표로 구분됨) 수를 지정합니다.

이 값이 0으로 설정되면 개방 형식 쿠키에 가장 특정한 쿠키 도메인이 사용됩니다. 즉, `myserver.example.com`이라는 쿠키 도메인 대신 `example.com` 도메인이 사용되고

`myserver.metals.example.org` 대신 `.metals.example.org` 도메인이 사용됩니다. 반대로 "쿠키 도메인 범위" 값이 2로 설정되면 쿠키 도메인은 각각 `.example.com`과 `.example.org`가 됩니다.

이 설정은 개방 형식 쿠키에 고유합니다. SiteMinder 에이전트가 사용하는 `CookieDomainScope` 매개 변수는 이와 다릅니다.

제한: 0, 2 또는 2보다 큰 수

예: 개방 형식 쿠키 도메인이 `division.example.com`인 경우를 가정해 봅니다. `server.division.example.com`에 대한 쿠키 도메인 범위를 설정하려면 "쿠키 도메인 범위" 필드 값을 3으로 설정합니다.

기본값: 2

활성화 시간

개방 형식 쿠키가 유효한 시간(초)을 지정합니다. 이 값은 HTTP 헤더 변수로 반환됩니다.

제한: 0보다 큰 양수

쿠키 경로

개방 형식 쿠키에 사용되는 경로를 지정합니다. 이 설정은 개방 형식 쿠키에 고유합니다. SiteMinder 에이전트가 사용하는 CookiePath 매개 변수는 이와 다릅니다.

쿠키 경로 범위

개방 형식 쿠키에 사용되는 경로의 범위를 정의하는 숫자를 지정합니다.

이 설정은 개방 형식 쿠키에 고유합니다. SiteMinder 에이전트가 사용하는 CookiePathScope 매개 변수는 이와 다릅니다.

제한: 0 이상

암호화 알고리즘

개방 형식 쿠키를 암호화하는 데 사용되는 암호화 알고리즘을 지정합니다. 3DES 암호화 키는 192 비트(24 바이트) 키 길이로 제한됩니다.

제한: AES128/CBC/PKCS5Padding, AES192/CBC/PKCS5Padding, AES256/CBC/PKCS5Padding, 3DES_EDE/CBC/PKCS5Padding

기본값: 3DES_EDE/CBC/PKCS5Padding

참고: 128-비트보다 긴 키를 사용하려면 Sun JCE(Java Cryptography Extension) Unlimited Strength Jurisdiction Policy Files 를 설치하십시오. 이 파일은 <http://java.sun.com/javase/downloads/index.jsp> 에서 다운로드할 수 있습니다.

암호화 암호

개방 형식 쿠키를 암호화하는 데 사용되는 암호를 지정합니다.

- f. 키를 생성하려면 "암호화 키 생성"을 클릭합니다. 사용자 고유의 기존 키를 입력해도 됩니다.

암호화 키가 다음 필드에 나타납니다.

암호화 키

개방 형식 쿠키와 함께 사용되는 암호화 키를 식별합니다. 고유한 키를 입력하거나 "암호화 암호" 필드의 값을 기반으로 키를 생성합니다. 이 키는 응용 프로그램에서 개방 형식 쿠키의 암호를 해독하는 데도 사용됩니다. 여기에서 설정되거나 수정된 키를 응용 프로그램에 복사하십시오.

제한: 16진수 문자만 사용합니다.

- g. 개방 형식 쿠키에 추가할 특성에 해당하는 확인란을 클릭합니다. 다음 목록에서 선택합니다.

참고: 인증 프로세스 중에 사용할 수 있는 값 중 일부는 권한 부여 프로세스 중에는 사용되지 않습니다. 이 경우 인증 프로세스에 사용되는 개방 형식 쿠키의 정보를 이후 권한 부여 중에 덮어쓰게 됩니다.

SM_USERNAME

개방 형식 쿠키에 사용자 DN(사용자 고유 이름) 값을 추가합니다.

SM_USERLOGINNAME

개방 형식 쿠키에 사용자가 로그인하는 데 사용하는 사용자 이름의 값을 추가합니다.

SM_USERIPADDRESS

사용자의 IP 주소(인증 또는 권한 부여에 존재하는 주소)를 개방 형식 쿠키에 추가합니다.

SM_USERSESSIONIP

사용자가 세션을 처음 인증 및 연결했을 때 사용한 IP 주소를 개방 형식 쿠키에 추가합니다.

SM_USERGROUPS

개방 형식 쿠키에 사용자 그룹을 추가합니다.

SM_USER_CONFIDENCE_LEVEL

개방 형식 쿠키에 영역의 위험 점수 또는 신뢰 수준을 추가합니다.

SM_AUTHENTICATIONNAME

개방 형식 쿠키에 인증 체계의 이름을 추가합니다.

제한: 인증 단계 중에만 사용할 수 있습니다.

SM_AUTHENTICATIONTYPE

개방 형식 쿠키에 인증 체계 유형을 추가합니다.

제한: 인증 단계 중에만 사용할 수 있습니다.

SM_AUTHENTICATIONLEVEL

개방 형식 쿠키에 인증 체계에 정의된 보호 수준을 추가합니다.

- h. (선택 사항) 사용자 디렉터리에서 개방 형식 쿠키에 포함할 값이 있는 다른 특성을 추가합니다.
- i. 다음 특성 캐싱 옵션 중 하나를 선택하십시오.

캐시 값

에이전트가 특성 값을 한 번 계산한 다음 정책 서버의 값을 캐시하도록 지정합니다. 긴 시간 동안 정적으로 유지되는 특성에 이 옵션 단추를 사용하십시오.

값 다시 계산 간격

응답 값을 다시 계산하기 전까지의 경과 시간(초)을 지정합니다. 값이 0이면 "캐시 값"과 동일합니다.

- 5. "확인"을 클릭합니다.
- 6. "마침"을 클릭합니다.

개방 형식 쿠키를 생성하는 웹 에이전트 응답이 생성됩니다.

규칙에 웹 에이전트 응답 추가

다음 규칙 유형 중 *하나*에 개방 형식 쿠키를 생성하는 웹 에이전트 응답을 추가해야 합니다.

- OAuthAccept
- OnAccessAccept

위의 두 유형을 모두 사용하되 각 규칙에서 하나의 유형만 허용하려면 서로 다른 규칙을 생성하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에서 "정책" "도메인", "규칙", "규칙 만들기"를 차례로 클릭합니다.
2. 개방 형식 쿠키를 발급할 도메인에 해당하는 옵션 단추를 클릭합니다.
3. "다음"을 클릭합니다.
4. 개방 형식 쿠키를 발급할 영역을 선택합니다.
5. "다음"을 클릭합니다.
6. "규칙 만들기"를 클릭합니다.
7. 다음 단계를 수행하여 규칙을 생성합니다.
 - a. 구체적인 이름과 설명(선택 사항)을 입력합니다.
 - b. 다음 항목을 지정합니다.
 - 영역 및 리소스
 - 허용/거부 및 사용/사용 안 함
 - c. 다음 옵션 단추 중 하나를 클릭합니다.
 - 인증 이벤트
 - 권한 부여 이벤트
 - d. 다음 목록에서 적절한 값이 표시되는지 확인합니다.
 - 인증 이벤트의 경우 "작업" 드롭다운 목록에 OAuthAccept 가 나타나야 합니다.
 - 권한 부여 이벤트의 경우 "작업" 드롭다운 목록에 OnAccessAccept 가 나타나야 합니다.
 - e. (선택 사항) 규칙에 원하는 시간 제한을 추가합니다.
8. "마침"을 클릭합니다.

웹 에이전트 응답이 규칙에 추가됩니다.

9. (선택 사항) 6~8 단계를 반복하여 추가 규칙을 생성합니다.

정책에 규칙 추가

기존 정책에 규칙을 추가하십시오. 규칙은 개방 형식 쿠키를 생성하는 응답과 연결됩니다.

다음 단계를 수행하십시오.

1. 관리 UI 에서 "정책", "도메인", "도메인 정책"을 차례로 클릭합니다.
2. 규칙을 추가할 정책의 편집 아이콘을 클릭합니다.
"일반" 탭이 선택된 상태로 "정책 수정:" 화면이 나타납니다.
3. "규칙" 탭을 클릭합니다.
4. "규칙 추가"를 클릭합니다.
사용 가능한 규칙 목록이 나타납니다.
5. 정책에 추가할 규칙의 확인란을 클릭합니다.
6. "확인"을 클릭합니다.
7. "제출"을 클릭합니다.
규칙이 정책에 추가되고 확인 메시지가 나타납니다.

샘플을 참조하여 응용 프로그램 사용자 지정

응용 프로그램을 사용자 지정하기 위한 샘플 응용 프로그램 및 추가 정보 파일이 제공됩니다. 웹 서버 관리자는 개방 형식 쿠키를 사용할 수 있도록 응용 프로그램을 수정할 때 이러한 샘플을 참조할 수 있습니다.

다음 목록에서 응용 프로그램 유형에 적절한 디렉터리를 선택하십시오.

- *installation_directory*\SiteMinder\samples\SmOpenFormatCookie\Java(Java)
- *installation_directory*\SiteMinder\samples\SmOpenFormatCookie\dotnet(.NET)

installation_directory

정책 서버가 설치된 파일 시스템의 위치를 지정합니다.

참고: 사용자가 로그아웃할 때 SiteMinder 가 열린 형식 쿠키를 자동으로 제거할 수는 없지만 쿠키를 제거하는 샘플 스크립트가 별도 시나리오에서 제공됩니다.

SiteMinder 생성 사용자 특성

다음 목록에는 SiteMinder 가 자동으로 생성하는 사용자 특성이 나와 있습니다. 이러한 특성은 웹 에이전트 응답의 응답 특성으로 지정할 수 있으며 명명된 식에서 사용할 수 있습니다.

%SM_USER

웹 에이전트는 모든 요청에 대해 SM_USER http 헤더 변수에 사용자 이름을 넣습니다. 웹 에이전트는 다음 항목 중 하나에 해당될 경우 SM_USER 헤더 변수의 값을 설정하지 않습니다.

- 사용자가 사용자 이름을 제공하지 않는 경우(예: 인증서 기반 인증)
- 사용자 이름을 알 수 없는 경우

%SM_USER_CONFIDENCE_LEVEL

사용자가 인증 체계를 통해 인증되고 인증 체계에서 신뢰 수준을 생성하는 경우 이 특성은 정수(0~1000)를 포함합니다. 인증 체계에서 이 정수를 사용자의 세션 티켓에 삽입합니다. 신뢰 수준이 높을수록 자격 증명의 보장 수준이 높아집니다. 신뢰 수준이 0 이면 자격 증명이 전혀 보장되지 않음을 나타냅니다. 자격 증명이 전혀 보장되지 않으면 SiteMinder 가 요청된 리소스에 대한 액세스를 거부합니다.

참고: 자세한 내용은 [신뢰 수준 소개](#) (페이지 556)를 참조하십시오.

%SM_USERDN

인증된 사용자에 대해 웹 에이전트는 정책 서버에서 결정한 DN 을 사용하여 이 http 헤더 변수를 채웁니다. 인증서 기반 인증의 경우 이 특성을 통해 사용자를 식별할 수 있습니다.

%SM_USERNAME

인증된 사용자에 대해 이 특성은 SiteMinder 에서 식별하는 사용자 DN 을 포함합니다. 인증되지 않은 사용자에 대해 이 특성은 사용자가 로그인 시도 중에 지정하는 사용자 ID 를 포함합니다.

%SM_USERIMPERSONATORNAME

인증 체계에서 가장을 수행하는 경우 이 특성은 SiteMinder 가 인증하는 사용자 DN 을 포함합니다.

%SM_USERLOGINNAME

이 특성은 사용자가 로그인 시도 중에 지정하는 사용자 ID 를 포함합니다.

%SM_USERIPADDRESS

이 특성은 인증 또는 권한 부여 시 사용자의 IP 주소를 포함합니다.

%SM_USERPATH

인증된 사용자에 대해 이 특성은 사용자 디렉터리 정의에 지정된 디렉터리 네임스페이스와 디렉터리 서버 및 SiteMinder 가 식별하는 사용자 DN 을 나타내는 문자열을 포함합니다. 예를 들면 다음과 같습니다.

```
"LDAP://123.123.0.1/uid=scarter,ou=people,o=airius.com"
```

인증되지 않은 사용자에 대해 이 특성은 SM_USERNAME 과 동일한 값을 포함합니다.

%SM_USERPASSWORD

이 특성은 사용자가 로그인 시도 중에 지정하는 암호를 포함합니다. 이 특성은 OnAuthAccept 이벤트를 통해 성공적인 인증 후에만 사용할 수 있습니다. 값은 인증 시에만 반환되고 권한 부여 시에는 반환되지 않습니다.

%SM_TRANSACTIONID

이 특성은 에이전트에서 생성하는 트랜잭션 ID 를 포함합니다.

%SM_USERSESSIONSPEC

사용자의 세션 티켓입니다.

%SM_USERSESSIONID

이 특성은 이미 인증된 사용자의 세션 ID 또는 SiteMinder 가 성공적인 인증 시 사용자에게 할당하는 세션 ID 를 포함합니다.

%SM_USERSESSIONIP

이 특성은 (세션 설정 시) 초기 사용자 인증 중에 사용된 IP 주소를 포함합니다.

%SM_USERSESSIONUNIVID

이 특성은 사용자의 유니버설 ID 를 포함합니다. 유니버설 ID 디렉터리 특성이 사용자 디렉터리 정의에 지정되지 않은 경우 값은 기본적으로 사용자의 DN 으로 설정됩니다.

%SM_USERSESSIONDIRNAME

이 특성은 정책 서버에서 사용하도록 구성된 사용자 디렉터리의 이름을 포함합니다.

%SM_USERSESSIONDIROID

이 특성은 정책 서버에서 사용하도록 구성된 사용자 디렉터리의 개체 ID 를 포함합니다.

%SM_USERSESSIONTYPE

이 특성은 사용자의 세션 유형을 포함합니다. 값은 다음 중 하나입니다.

- 2 - 세션
- 1 - 아이덴티티

%SM_USERLASTLOGINTIME

이 특성은 사용자가 마지막으로 로그인하고 인증된 시간(GMT 사용)을 포함합니다. 이 응답 특성은 OnAuthAccept 인증 이벤트에 대해서만 사용할 수 있습니다. 이 특성은 다음 두 조건을 모두 충족할 경우에만 값을 포함합니다.

- 암호 서비스가 사용되도록 설정되었습니다.
- 사용자가 SiteMinder 를 통해 한 번 이상 로그인했습니다.

%SM_USERPREVIOUSLOGINTIME

이 특성은 마지막 로그인 이전에 성공한 로그인 시간(GMT 사용)을 포함합니다. 이 응답 특성은 OnAuthAccept 인증 이벤트에 대해서만 사용할 수 있습니다. 이 특성은 암호 서비스가 사용되도록 설정된 경우에만 값을 포함합니다.

%SM_USERGROUPS

이 특성은 사용자가 속하는 그룹을 포함합니다. 사용자가 중첩 그룹에 속할 경우 이 특성은 계층에서 가장 아래의 그룹을 포함합니다.

사용자가 속한 모든 중첩 그룹에 대해 SM_USERNESTEDGROUPS 를 사용합니다.

예:

사용자가 "지급 계정" 그룹에 속하고 이 "지급 계정"이 "회계" 그룹에 포함된 경우 SM_USERGROUPS 에 "지급 계정" 그룹이 포함됩니다. "지급 계정"과 "회계" 그룹을 모두 원할 경우에는 SM_USERNESTEDGROUPS 를 사용하십시오.

%SM_USERNESTEDGROUPS

이 특성은 사용자가 속한 중첩 그룹을 포함합니다. 계층의 최하위 그룹에 대해서만 SM_USERGROUPS 를 사용합니다.

예:

사용자가 "지급 계정" 그룹에 속하고 이 "지급 계정"이 "회계" 그룹에 포함된 경우 SM_USERNESTEDGROUPS 에 "회계" 및 "지급 계정" 그룹이 포함됩니다. "회계" 그룹만 원할 경우 SM_USERGROUPS 를 사용하십시오.

%SM_USERSCHEMAATTRIBUTES

이 특성은 DN 과 관련된 사용자 특성 또는 사용자와 관련된 속성을 포함합니다. 사용자 디렉터리가 SQL 데이터베이스일 경우 SM_USERSCHEMAATTRIBUTES 는 테이블에서 사용자 데이터가 저장된 열의 이름을 포함합니다. 예를 들어 SmSampleUsers 스키마를 사용할 경우 SM_USERSCHEMAATTRIBUTES 는 SmUser 테이블에 있는 열의 이름을 포함합니다.

%SM_USERPOLICIES

사용자가 리소스에 대해 권한이 부여되고 사용자 권한 부여를 제공하는 정책이 있을 경우 이 특성은 이러한 정책의 이름을 포함합니다.

예: 물품을 구매하려면 "구매자" 정책과 관련된 사용자여야 합니다. 정책 서버에서 물품을 구매할 권한을 부여하는 경우 SM_USERPOLICIES 에 "구매자"라는 이름이 포함됩니다.

%SM_USERPRIVS

사용자가 리소스에 대해 인증되거나 권한이 부여되면 SM_USERPRIVS 는 모든 정책 도메인에서 이 사용자에게 적용되는 모든 정책에 대한 모든 응답 특성을 포함합니다.

%SM_USERREALMPRIVS

사용자가 특정 영역의 리소스에 대해 인증되거나 권한이 부여되면 SM_USERREALMPRIVS 는 이 영역의 모든 규칙에 대한 모든 응답 특성을 포함합니다.

예:

"장비 구매"라는 영역이 있고, 이 영역 아래에 "신용확인"이라는 규칙이 있습니다. 이 규칙은 다음과 같은 응답 특성으로 구매자의 신용 한도를 반환하는 응답과 관련됩니다.

limit = \$15000

구매자가 5000 달러 상당의 장비를 구매하려고 하면 규칙이 실행됩니다. SM_USERREALMPRIVS 는 "장비 구매" 영역 아래 모든 규칙에 대한 모든 응답 특성을 포함하게 됩니다.

%SM_AUTHENTICATIONLEVEL

사용자가 리소스에 대해 인증될 경우 이 특성은 사용자가 인증된 인증 체계의 보호 수준을 나타내는 정수(0~1000)를 포함합니다.

%SM_USERDISABLEDSTATE

이 특성은 사용자가 비활성화된 이유의 비트 마스크를 나타내는 십진수를 포함합니다. 이러한 비트는 SDK의 일부인 `SmApi.h`의 `Sm_Api_DisabledReason_t` 데이터 구조 아래에 정의되어 있습니다.

예를 들어 비활성 `Sm_Api_Disabled_Inactivity`의 결과로 사용자가 비활성화될 수 있습니다. `Sm_Api_DisabledReason_t`에서 `Sm_Api_Disabled_Inactivity` 이유는 0x00000004 값에 해당됩니다. 따라서 이 경우 `SM_USERDISABLEDSTATE`는 4입니다.

사용자는 여러 가지 이유로 비활성화될 수 있습니다.

%SM_USER_APPLICATION_ROLES

CA Identity Manager를 구매했을 경우 이 특성을 응답에 사용할 수 있습니다. 이 특성은 사용자에게 할당되거나 위임된 모든 역할의 목록을 포함합니다. 응용 프로그램 이름이 지정된 경우에는 해당 응용 프로그램과 관련된 역할만 응답 특성에 반환됩니다.

응답 특성 이름은 "응답 특성" 창의 "변수 이름" 필드에 입력합니다. 응답 특성 이름의 구문은 다음과 같습니다.

`SM_USER_APPLICATION_ROLES[:application_name]`

여기서 `application_name`은 Identity Manager에 정의된 응용 프로그램의 이름으로, 선택 사항입니다.

`application_name` 값을 정책 서버 관리자에게 전달해야 합니다. 응용 프로그램 이름은 관리 UI에 자동으로 전달되지 않습니다.

참고: Identity Manager 역할에 대한 자세한 내용은 *CA Identity Manager Operations Guide*(CA Identity Manager 작업 안내서)를 참조하십시오.

%SM_USER_APPLICATION_TASKS

CA Identity Manager(Identity Manager)를 구매했을 경우 이 특성을 응답에 사용할 수 있습니다. 이 특성은 사용자에게 할당되거나 위임된 모든 태스크의 목록을 포함합니다. 응용 프로그램 이름이 지정된 경우에는 해당 응용 프로그램과 관련된 태스크만 응답 특성에 반환됩니다.

응답 특성 이름은 "응답 특성" 창의 "변수 이름" 필드에 입력합니다. 응답 특성 이름의 구문은 다음과 같습니다.

`SM_USER_APPLICATION_TASKS[:application_name]`

여기서 *application_name* 은 Identity Manager 에 정의된 응용 프로그램의 이름으로, 선택 사항입니다.

application_name 값을 정책 서버 관리자에게 전달해야 합니다. 응용 프로그램 이름은 관리 UI 에 자동으로 전달되지 않습니다.

참고: Identity Manager 태스크에 대한 자세한 내용은 *CA Identity Manager Operations Guide*(CA Identity Manager 작업 안내서)를 참조하십시오.

추가 정보:

[웹 에이전트 응답 특성 구성](#) (페이지 594)

SiteMinder 생성 응답 특성의 사용 여부

다음 표에서는 인증, 권한 부여 및 가장 이벤트 도중 SiteMinder 생성 응답 특성의 사용 여부를 보여 줍니다.

응답 특성	인증 및 권한 부여 이벤트					가장 이벤트
	GET/PUT	시점: 인증 승인	시점: 인증 거부	시점: 액세스 승인	시점: 액세스 거부	
SM_USER_CONFIDENCE_LEVEL	예	예	예	예	예	아니요
SM_USERNAME	예	예	예	예	예	아니요
SM_USERPATH	예	예	예	예	예	아니요
SM_USERIPADDRESS	예	예	예	예	예	아니요
SM_USERPASSWORD	아니요	예	예	아니요	아니요	아니요
SM_TRANSACTIONID	예	아니요	아니요	예	예	아니요
SM_USERSESSIONID	예	예	아니요	예	예	아니요
SM_USERSESSIONSPEC	예	아니요	아니요	예	예	아니요
SM_USERSESSIONIP	예	예	예	예	예	아니요
SM_USERSESSIONUNIVID	예	예	아니요	예	예	아니요

응답 특성	인증 및 권한 부여 이벤트					가장 이벤트
	GET/PUT	시점: 인증 승인	시점: 인증 거부	시점: 액세스 승인	시점: 액세스 거부	
SM_USERSESSIONDIRNAME	예	예	아니요	예	예	아니요
SM_USERSESSIONDIROID	예	예	아니요	예	예	아니요
SM_USERSESSIONTYPE	예	예	아니요	예	예	아니요
SM_USERLASTLOGINTIME	아니요	예	아니요	아니요	아니요	아니요
SM_USERGROUPS	예	예	아니요	예	예	아니요
SM_USERNESTEDGROUPS	예	예	아니요	예	예	아니요
SM_USERSCHEMAATTRIBUTES	예	예	예	예	예	아니요
SM_USERLOGINNAME	아니요	예	예	아니요	아니요	아니요
SM_USERIMPERSONATORNAME	아니요	아니요	아니요	아니요	아니요	예
SM_USERDISABLEDSTATE	예	예	아니요	예	예	아니요
SM_USERPOLICIES	아니요	아니요	아니요	예	아니요	아니요
SM_USERREALMPRIVS	예	아니요	아니요	아니요	아니요	아니요
SM_USERPRIVS	예	아니요	아니요	아니요	아니요	아니요

응답 그룹

응답 그룹은 정책 내의 단일 규칙에 적용할 수 있도록 논리적으로 그룹화된 응답 모음입니다. 응답 그룹과 쌍으로 연결된 규칙이 실행되면 응답 그룹 내의 모든 관련 응답이 실행됩니다.

응답 그룹을 사용하면 여러 응답을 단일 개체로 결합할 수 있습니다. 또한 정책을 생성할 때 해당 정책 내의 단일 규칙과 여러 응답을 보다 쉽게 연결할 수 있습니다.

응답 그룹 구성

응답 집합을 정책의 한 규칙에 적용하는 응답 그룹을 생성할 수 있습니다.

다음 단계를 수행하십시오.

1. "정책", "도메인", "응답 그룹"을 클릭합니다.
2. "응답 그룹 만들기"를 클릭합니다.
3. "확인"을 클릭합니다.
4. 도메인을 선택하고 "다음"을 클릭합니다.
5. 응답 그룹의 이름과 설명을 입력합니다.
6. Radius 또는 SiteMinder 및 에이전트 유형을 선택합니다.

참고: 지정된 에이전트 유형은 그룹에 있는 응답의 에이전트 유형에 해당해야 합니다. 지정된 에이전트 유형의 응답만 그룹에 포함할 수 있습니다.

7. "그룹 구성원"에서 "추가/제거"를 클릭합니다.

참고: 지정된 에이전트 유형에 대해 지정된 도메인에 정의된 모든 응답이 "사용 가능한 구성원" 열에 나열됩니다. 에이전트 유형이 "일반 Radius"인 경우 "사용 가능한 구성원" 열에는 Radius 에이전트가 지원하는 모든 응답이 나열됩니다.

8. "사용 가능한 구성원" 목록에서 하나 이상의 응답을 선택하고 오른쪽 방향 화살표를 클릭합니다.

응답이 "사용 가능한 구성원" 목록에서 제거되고 "선택한 구성원" 목록에 추가됩니다.

참고: 한 번에 여러 구성원을 선택하려면 Ctrl 키를 누른 채 추가 구성원을 클릭하십시오. 구성원 블록을 선택하려면 첫 번째 구성원을 클릭한 다음 Shift 키를 누른 채 블록의 마지막 구성원을 클릭하십시오.

9. "확인"을 클릭합니다.
선택된 응답이 응답 그룹에 추가됩니다.
10. "마침"을 클릭합니다.
응답 그룹이 생성됩니다.

응답 그룹에 응답 추가

동일한 에이전트 유형의 응답을 응답 그룹에 추가할 수 있습니다. 이 경우 모든 응답이 동일한 도메인에 있어야 합니다.

다음 단계를 수행하십시오.

1. 응답 그룹을 엽니다.
2. "그룹 구성원" 그룹 상자에서 "추가/제거"를 클릭합니다.

"응답 선택" 그룹 상자가 열립니다. "사용 가능한 구성원" 열에는 지정된 에이전트 유형 또는 **RADIUS** 공급업체 유형과 함께 선택한 도메인에서 사용할 수 있는 응답이 포함되어 있습니다.

참고: "일반 **RADIUS**"를 지정한 경우 "사용 가능한 구성원" 열에는 **RADIUS** 에이전트가 지원하는 모든 응답이 나열됩니다.

3. 응답을 "선택한 구성원" 열로 이동하여 그룹에 포함하고 "확인"을 클릭합니다.

"응답 그룹" 창이 열립니다. 선택한 규칙이 "그룹 구성원" 그룹 상자에서 열립니다.

4. 제출을 클릭합니다.
응답 그룹이 저장됩니다.

응답 그룹 수정

에이전트 유형을 제외한 모든 응답 그룹 속성을 수정할 수 있습니다.

에이전트 유형을 변경하려면 응답 그룹을 삭제하고 새 응답 그룹을 생성하십시오.

참고: 정책 서버 개체의 수정 및 삭제에 대한 자세한 내용은 정책 서버 개체 관리를 참조하십시오.

응답 그룹 삭제

응답 그룹을 삭제하면 그룹만 삭제되고 그룹에 포함된 개별 응답은 삭제되지 않습니다.

참고: 정책 서버 개체의 수정 및 삭제에 대한 자세한 내용은 정책 서버 개체 관리를 참조하십시오.

제 17 장: 정책

이 섹션은 다음 항목을 포함하고 있습니다.

[정책 개요](#) (페이지 621)

[정책을 구성하는 방법](#) (페이지 625)

정책 개요

정책은 사용자가 리소스와 상호 작용하는 방법을 정의합니다. 관리 UI 에서 정책을 만들려면 다음 속성을 식별하는 개체를 연결(바인딩)합니다.

- 사용자
- 리소스
- 리소스와 관련된 작업

정책은 정책 도메인에 저장됩니다. 정책을 구성할 때 정책 도메인의 사용 가능한 사용자 디렉터리에서 사용자 및 그룹을 선택할 수 있습니다.

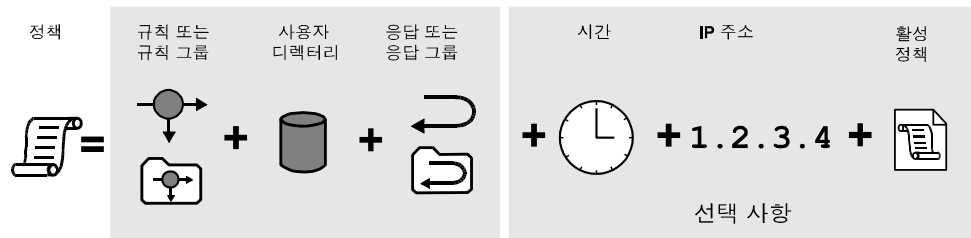
정책 서버는 규칙을 통해 리소스를 식별합니다. 정책을 생성할 때 정책에 포함할 리소스를 지정하는 규칙을 선택할 수 있습니다.

정책의 사용자와 리소스를 식별한 후에는 해당 사용자가 지정된 리소스에 액세스할 때 발생하는 작업을 지정할 수 있습니다. 이러한 작업은 응답의 형태로 이루어집니다. 정책은 다음과 같은 일을 수행하는 응답을 포함할 수 있습니다.

- 리소스에 대한 액세스 허용 또는 거부
- 사용자 세션 시간 사용자 지정
- 사용자를 다른 리소스로 리디렉션
- 사용자 디렉터리에 포함된 특성에 기반하여 사용자가 받는 콘텐츠를 사용자 지정합니다.

고급 정책은 특정 시간이나 특정 사용자 IP 주소로 제한될 수 있습니다. 이렇게 하면 리소스 그룹의 관리자가 리소스를 더욱 세부적으로 제어할 수 있습니다.

다음 다이어그램에서는 정책에 포함될 수 있는 모든 요소를 보여 줍니다.



규칙/규칙 그룹

정책에는 규칙 또는 규칙 그룹이 하나 이상 포함되어야 합니다. 규칙은 정책에 포함된 특정 리소스를 식별합니다.

사용자

정책에서는 정책의 영향을 받는 사용자 또는 사용자 그룹을 지정해야 합니다. 이러한 사용자 또는 사용자 그룹에 대한 연결은 "사용자 디렉터리" 화면에서 구성해야 합니다. 정책이 있는 정책 도메인에 포함된 디렉터리의 사용자 또는 사용자 그룹만 정책에 연결될 수 있습니다.

응답

응답은 사용자가 규칙에 지정된 리소스에 액세스할 때 트리거되는 작업을 정의합니다. 응답을 통해 다른 응용 프로그램에서 사용하거나 콘텐츠를 사용자 지정할 수 있도록 사용자 디렉터리의 특성을 반환할 수 있습니다. 또한 응답을 통해 인증 및 권한 부여 이벤트를 기반으로 작업을 트리거할 수도 있습니다.

(선택 사항) IP 주소

정책은 특정 사용자 IP 주소로 제한될 수 있습니다. 정책에 IP 주소 제한을 추가한 경우 사용자가 정책에 지정되지 않은 IP 주소에서 리소스에 액세스하려고 하면 해당 사용자에게 대해 정책이 실행되지 않으므로 액세스가 허용 또는 거부되지 않거나 응답이 처리되지 않습니다.

(선택 사항) 시간 제한

정책은 특정 날짜이나 시간 범위로 제한될 수도 있습니다. 시간 제한이 있는 정책은 지정된 시간 외에는 실행되지 않으므로 보호된 리소스에 대한 액세스가 허용 또는 거부되지 않거나 응답이 처리되지 않습니다.

(선택 사항) 활성 정책

활성 정책을 사용하여 SiteMinder 외부의 비즈니스 논리를 정책 정의에 포함할 수 있습니다. SiteMinder 는 활성 정책을 통해 SiteMinder API 를 사용하여 생성된 사용자 지정 소프트웨어와 상호 작용할 수 있습니다.

정책 바인딩

정책 바인딩은 사용자를 정책과 연결하는 데 사용되는 방법입니다. 정책 서버는 정책에 포함된 사용자 또는 그룹이 생성한 정책 바인딩의 일부인 사용자에게 대해서만 정책을 확인합니다.

정책 서버가 보호된 리소스에 대한 사용자의 액세스 시도를 확인하려면 먼저 사용자가 인증되어야 합니다. SiteMinder 는 사용자를 인증할 때 사용자의 컨텍스트를 설정합니다. 사용자 컨텍스트는 사용자 본인에 대한 정보와 해당 사용자가 리소스에 액세스할 때 갖게 되는 권한에 대한 정보를 제공합니다.

예를 들어 사용자가 **Employees** 라는 사용자 디렉터리의 그룹에 속하는 경우 이 사용자가 인증될 때 정책 서버는 **Employees** 그룹에 사용자의 구성원 자격에 대한 정책 바인딩을 생성합니다. 이 사용자가 **Employees** 그룹 구성원의 액세스를 허용하는 정책의 규칙으로 보호된 리소스에 액세스하려고 할 때 SiteMinder 는 사용자의 정책 바인딩을 사용하여 사용자에게 권한을 부여할 수 있습니다.

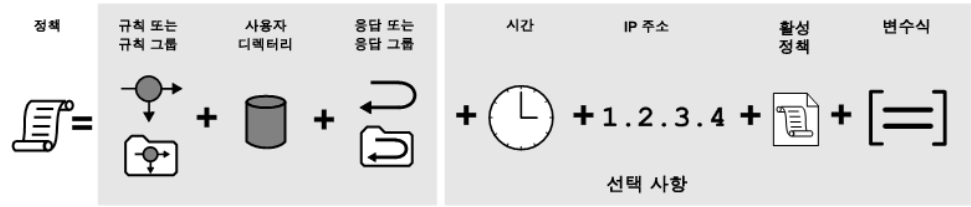
정책의 식

eTelligent 규칙은 정책 식에 여러 변수를 사용할 수 있도록 해 줍니다.

식은 런타임에 평가되는 동적 정보를 포함하도록 정책을 확장합니다. 식에 변수 개체를 사용하면 정책으로 보호된 리소스에 대한 권한을 확인하는 부울 조건 집합을 생성할 수 있습니다.

활성 정책 식에 변수 개체를 사용하려면 정책 개체를 구성하고 "식" 대화 상자를 사용하여 적절한 부울 식을 작성해야 합니다. 이 인터페이스는 정책에 LDAP 식 추가에 설명된 LDAP 검색 식 편집기와 유사합니다.

참고: 다음 그림과 같이 정책 개체가 지원하는 다른 데이터에 식을 추가할 수도 있습니다.



참고: 활성 식과 명명된 식은 동일하지 않습니다. 두 유형의 식은 모두 런타임에 평가되지만 다음과 같은 차이점이 있습니다.

- 활성 식은 부울 식인 반면, 명명된 식은 문자열, 숫자 또는 부울 값을 반환할 수 있습니다.
- 활성 식은 있는 그대로 참조되고 사용할 때마다 다시 입력해야 하는 반면, 명명된 식은 이름으로 참조되며 어느 위치에서나 참조되고 재사용될 수 있습니다.

추가 정보:

[변수](#) (페이지 629)

정책에서 신뢰 수준 구성

SiteMinder가 지원되는 위험 분석 엔진과 통합되는 경우 신뢰 수준을 정책에 사용할 수 있습니다. 신뢰 수준은 사용자 인증의 일부로 완료된 위험 평가의 결과를 포함하도록 정책을 확장합니다. 정책 서버에서는 권한 부여 결정을 할 때 이러한 결과를 사용할 수 있습니다.

신뢰 수준을 다음 개체에 적용할 수 있습니다.

- 정책 영역
영역에서 구성하는 신뢰 수준은 해당 영역과 연결된 모든 리소스(규칙)에 적용됩니다. 신뢰 수준을 정책 영역에 적용하려면 신뢰 수준 지원을 활성화해야 합니다.

■ 활성 정책 식

활성 정책 식으로 구성하는 신뢰 수준은 해당 정책과 연결된 리소스(규칙)에만 적용됩니다. 활성 정책 식을 사용하면 보다 세부적으로 권한 부여 결정을 내릴 수 있습니다. 활성 정책 식을 사용하여 신뢰 수준을 적용하는 기능은 이전 릴리스부터 계속 지원되므로 기본적으로 활성화되어 있습니다.

참고: SiteMinder에서는 CA Arcot WebFort 및 CA Arcot Risk의 온 프레미스 구축 환경 및 CA Arcot A-OK의 호스트된 구축 환경과의 통합을 지원합니다.

정책을 구성하는 방법

정책을 구성하는 과정은 다음 단계로 이루어집니다.

참고: "Scripting interface for Perl"(Perl 스크립팅 인터페이스)을 사용하여 정책을 생성할 수도 있습니다. 자세한 내용은 *Programming Guide for Perl*(Perl 프로그래밍 안내서)을 참조하십시오.

다음 단계를 수행하십시오.

1. [정책을 생성합니다](#) (페이지 625).
2. [정책에 사용자를 추가합니다](#) (페이지 627).
3. [정책에 규칙을 하나 이상 추가합니다](#) (페이지 627).
4. (선택 사항) 규칙에 응답 또는 응답 그룹을 연결합니다.
5. (선택 사항) 규칙에 전역 응답을 연결합니다.
6. (선택 사항) 고급 정책 옵션을 구성합니다.

정책 생성

새 도메인이나 기존 도메인에 정책을 추가하는 방법으로 정책을 생성하십시오. 정책은 사용자와 리소스 간의 관계를 정의합니다.

다음 단계를 수행하십시오.

1. "정책", "도메인"을 차례로 클릭합니다.
2. "도메인"을 클릭합니다.
3. 수정할 도메인의 이름을 클릭합니다.

4. "수정"을 클릭합니다.
5. "정책" 탭을 클릭합니다.
6. "만들기"를 클릭합니다.
7. 정책의 이름과 설명을 입력합니다.
8. (선택 사항) 항상 사용자를 다시 인증하도록 할 리소스가 정책으로 보호되는 경우 "아이덴티티 유효성 검사" 확인란을 선택합니다. 예를 들어 한 은행 계좌에서 다른 은행 계좌로 이체하기 전에 항상 사용자를 다시 인증하도록 하려면 "아이덴티티 유효성 검사" 확인란을 선택합니다. 그러면 사용자가 다시 인증해야만 이체할 수 있습니다. 이 설정을 사용하면 SiteMinder 세션이 아직 유효한 상태에서 사용자가 화면 앞을 떠나더라도 사용자를 보호할 수 있습니다. 현재 SiteMinder 세션은 영향을 받지 않습니다.

참고: 이 설정을 사용하려면 정책 서버 및 에이전트에서 추가 구성이 필요합니다. 자세한 내용은 기술 자료 문서, *시나리오: 중요한 리소스에 대해 재인증 요구*를 참조하십시오.
9. "사용자" 탭을 클릭합니다.
10. 사용자나 사용자 그룹 또는 둘 모두를 정책에 추가하고 "제출"을 클릭합니다.
11. 제출을 클릭합니다.

처리를 위해 "도메인 수정" 태스크가 제출됩니다.

정책에 사용자 추가

정책에 개별 사용자, 사용자 그룹 또는 둘 모두를 추가한 다음 추가한 사용자와 정책 간에 정책 바인딩을 생성할 수 있습니다. 사용자가 보호된 리소스에 액세스하려고 하면 정책은 사용자가 정책 바인딩의 일부인지 확인한 다음 정책에 포함된 규칙을 실행하여 사용자가 리소스에 액세스할 수 있도록 허용된 사용자인지 여부를 확인합니다.

다음 단계를 수행하십시오.

1. "사용자" 페이지로 이동합니다.

2. 사용자 디렉터리의 사용자 또는 그룹을 정책에 추가합니다.

각 사용자 디렉터리 그룹 상자 내에서 "구성원 추가", "항목 추가" 및 "모두 추가"를 선택할 수 있습니다. 정책에 사용자를 추가하는 데 사용하는 방법에 따라 사용자를 추가할 수 있는 대화 상자가 열립니다.

참고: "구성원 추가"를 선택하는 경우 "사용자/그룹" 창이 열립니다. 개별 사용자는 자동으로 표시되지 않습니다. 검색 유틸리티를 사용하여 디렉터리 중 하나에서 특정 사용자를 찾을 수 있습니다.

오른쪽 화살표(>)를 클릭하여 사용자 또는 그룹을 편집하거나 빼기 기호(-)를 클릭하여 사용자 또는 그룹을 삭제할 수 있습니다.

3. 아무 방법이나 사용하여 개별 사용자, 사용자 그룹 또는 둘 다를 선택하고 "확인"을 클릭합니다.

"사용자 디렉터리" 페이지가 다시 열리면서 새 사용자가 나열됩니다.

정책에 사용자를 바인딩하는 태스크가 완료되었습니다.

정책에 규칙 추가

규칙은 정책에 포함된 특정 리소스와 규칙이 실행될 때 해당 리소스에 대한 액세스를 허용할지 거부할지를 나타냅니다. 응답은 규칙이 실행될 때 수행할 작업을 나타냅니다.

참고: 정책에 규칙 또는 규칙 그룹을 하나 이상 추가하십시오.

다음 단계를 수행하십시오.

1. "정책", "규칙"으로 이동합니다.
"규칙" 페이지가 열립니다.
2. "규칙 추가"를 클릭합니다.
"사용 가능한 규칙" 창이 열립니다.
3. 정책에 추가할 개별 규칙, 규칙 그룹 또는 둘 모두를 선택하고 "확인"을 클릭합니다.
"규칙" 섹션에 추가된 규칙 및 그룹의 목록이 표시됩니다.
4. (선택 사항) 규칙을 응답 또는 응답 그룹과 연결합니다.

참고: 정책에서 규칙 또는 규칙 그룹을 제거하려면 "규칙" 섹션의 규칙 오른쪽에 있는 빼기 기호(-)를 클릭하십시오. 규칙을 생성하려면 "사용 가능한 규칙" 창에서 "새 규칙"을 클릭하십시오.

제 18 장: 변수

이 섹션은 다음 항목을 포함하고 있습니다.

[eTelligent 규칙](#) (페이지 629)

[변수 개요](#) (페이지 634)

[웹 서비스 변수](#) (페이지 637)

[변수 만들기](#) (페이지 641)

eTelligent 규칙

정책 식이라고 하는 세부적인 액세스 제어 조건을 사용할 수 있도록 하는 변수를 정의하려면 eTelligent 규칙을 사용하십시오.

정책 식은 정책 특성으로 구현됩니다. 정책 식에는 연산자와 런타임에, 즉 사용자가 웹 사이트의 보호된 리소스에 액세스하려고 시도할 때 평가되는 고객 정의 변수가 포함됩니다.

변수는 기업 내의 로컬 정보나 웹 서비스가 제공하는 원격 정보를 저장할 수 있습니다.

eTelligent 규칙이 제공하는 변수는 관리 UI 에서 사용할 수 있습니다. 정책 식을 통해 변수 개체를 정의한 후 정책 논리에 통합할 수 있습니다. SiteMinder 응답 개체에 변수를 포함할 수도 있습니다.

eTelligent 규칙에 대한 구성 요소 요구 사항

eTelligent 규칙을 사용하려면 다음과 같은 구성 요소가 필요합니다.

- 웹 에이전트
- (선택 사항) 웹 에이전트 옵션 팩

웹 에이전트 옵션 팩은 POST 변수를 사용하려는 경우에만 필요합니다.

eTelligent 규칙의 이점

eTelligent 규칙의 이점은 다음과 같습니다.

- 복잡성을 줄여 주고 사용자 지정 코드가 필요하지 않도록 합니다.
SiteMinder 관리자는 응용 프로그램 코드가 아닌 그래픽 도구를 사용하여 정책 식에 권한 부여 액세스를 정의합니다. 백엔드 비즈니스 응용 프로그램 액세스 제어 정보가 SiteMinder 정책 서버에 중앙 집중화되므로 이를 통합하고 조정할 필요가 없습니다.
- 보안 정책에서 비즈니스 데이터를 동적으로 사용할 수 있습니다.
보안 리소스에 대한 액세스 제어 정의는 로컬 사용자 정보와 사용자의 구매 주문 수량과 같이 외부에서 수신 정보를 기반으로 합니다.
- 권한 부여 결정을 위해 다양한 유형의 정보를 조합할 수 있습니다.
웹 브라우저 양식 데이터, 정책 서버에 로컬로 저장되는 사용자 컨텍스트 데이터, 서비스 부서를 통해 얻은 원격 데이터 등을 정책 식에 유연하게 조합할 수 있습니다.
- 트랜잭션 관련 결정을 온라인으로 수행할 수 있습니다.
보호된 리소스에 액세스하기 위해 권한 부여가 필요할 때마다 백엔드 비즈니스 응용 프로그램으로 돌아갈 필요가 없습니다.
- XML 기반 타사 보안 데이터를 사용할 수 있습니다.
eTelligent 규칙은 표준 XML 프로토콜을 사용하여 트러스트된 서비스 부서와 통신하므로 선택할 수 있는 웹 서비스 공급자의 범위가 넓어집니다.
- 부울 논리를 사용할 수 있습니다.
SiteMinder 보안 관리자는 논리 연산자와 함께 변수를 사용하여 정의식을 정의합니다.
- 필요한 정책 수를 최소화할 수 있습니다.
논리 기반의 정책 식을 사용하기 때문에 필요한 정책 수가 적어 정책 관리를 최소화할 수 있습니다.

eTelligent 규칙을 구성하는 방법

eTelligent 규칙을 구성하려면 다음 태스크를 수행하십시오.

1. 다음 eTelligent 규칙 속성 파일을 구성합니다.
 - JVMOptions.txt
 - LoggerConfig.properties
2. 변수를 구성합니다.
3. eTelligent 규칙 변수를 사용하는 정책 식을 구성합니다.

eTelligent 규칙 속성 파일

다음과 같은 속성 파일이 eTelligent 규칙에 필요합니다.

- JVMOptions.txt

이 파일은 eTelligent 규칙에 대한 JVM 을 구성하는 데 필요합니다. 이 파일이 설치된 위치는 *policy_server_home/config/*입니다.

- LoggerConfig.properties

이 파일은 eTelligent 규칙의 로깅을 구성하는 데 필요합니다. 이 파일이 설치된 위치는 다음과 같습니다.

policy_server_home/config/properties

추가 정보:

[JVMOptions.txt 파일](#) (페이지 631)

[LoggerConfig.properties 파일 수정](#) (페이지 632)

JVMOptions.txt 파일

JVMOptions.txt 파일에는 정책 서버가 eTelligent 규칙을 지원하는 데 사용되는 Java Virtual Machine 을 생성할 때 사용하는 설정이 포함되어 있습니다.

누락된 클래스와 관련된 오류가 발생하면 JVMOptions.txt 파일에서 클래스 경로 지시문을 수정할 수 있습니다. JVMOptions.txt 파일에 포함된 설정에 대한 자세한 내용은 Java 설명서를 참조하십시오.

LoggerConfig.properties 파일 수정

정책 서버에서 **LoggerConfig.properties** 파일을 사용하여 **SiteMinder** 서비스를 명령줄에서 시작할 때 사용되는 로깅 기능을 지정할 수 있습니다. 서비스가 정책 서버 관리 콘솔에서 시작될 때는 이 파일에 포함된 속성이 사용되지 않습니다. 디버깅을 위해 더 많은 출력을 보려면 이 파일을 수정하십시오.

다음은 **LoggerConfig.properties** 파일의 예입니다.

```
// LoggingOn can be Y, N
LoggingOn=Y

// LogLevel can be one of LOG_LEVEL_NONE, LOG_LEVEL_ERROR,
LOG_LEVEL_INFO, LOG_LEVEL_TRACE
LogLevel=LOG_LEVEL_TRACE

// If LogFileName is set Log output will go to the file named
LogFileName=affwebserv.log

// AppendLog can be Y, N. Y means append output to LogFileName if
specified
AppendLog=Y

// AlwaysWriteToSystemStreams can be Y, N.
// Y means log messages are written to System.out
// or System.err regardless of what the logger streams are
// set to. If the logger streams are set to System.out
// or System.err log messages will be written multiple times.
// This facilitates logging messages to System.out/System.err
// and a file simultaneously.
AlwaysWriteToSystemStreams=N

// DateFormatPattern can be any valid input to java.text.DateFormat
constructor.
// See the Java documentation for java.text.DateFormat for details
// If not specified, the default format for the default locale is used
DateFormatPattern=MMM d, yyyy h:mm:ss.S a
```

이 파일의 설정은 다음과 같습니다.

LoggingOn

로깅을 사용하거나 사용하지 않도록 설정합니다. 로깅을 사용하려면 이 매개 변수를 **Y** 로 설정하십시오. 로깅을 사용하지 않으려면 이 매개 변수를 **N** 으로 설정하십시오.

LogLevel

로그에 포함되는 상세 정보 수준을 나타냅니다. LogLevel 은 다음 값 중 하나가 될 수 있습니다.

LOG_LEVEL_NONE

로깅된 메시지가 없습니다.

LOG_LEVEL_ERROR

오류 메시지만 기록됩니다.

LOG_LEVEL_INFO

오류 메시지와 경고가 기록됩니다.

LOG_LEVEL_TRACE

오류 메시지, 경고, 그리고 문제 추적에 유용한 일반적인 처리 정보가 기록됩니다.

LogFileName

LogFileName 이 설정된 경우 모든 로그가 이 매개 변수에 명명된 파일로 출력됩니다.

AppendLog

시작 시 기존 파일에 로깅 정보를 추가할지 또는 시작 시 새 파일을 생성할지를 나타냅니다. LogFileName 매개 변수에 지정된 파일에 출력을 추가하려면 이 매개 변수를 Y 로 설정하십시오. 시작 시 새 파일을 생성하려면 이 매개 변수를 N 으로 설정하십시오.

AlwaysWriteToSystemStreams

로거 스트림의 설정에 관계없이 System.out 또는 System.err 에 메시지를 로깅하려면 이 매개 변수를 Y 로 설정하십시오. 로거 스트림이 System.out 또는 System.err 로 설정된 경우에는 로그 메시지가 여러 번 기록됩니다. 이렇게 하면 System.out/System.err 와 또 하나의 파일에 메시지를 동시에 로깅할 수 있습니다.

DateFormatPattern

DateFormatPattern 은 java.text.DateFormat 생성자에 대한 유효한 입력일 수 있습니다. java.text.DateFormat 에 대한 자세한 내용은 Java 설명서를 참조하십시오.

지정되지 않은 경우 기본 로캘의 기본 형식이 사용됩니다.

변수 개요

정책 서버는 요청의 권한 부여 단계로 통합할 수 있는 값으로 변수 개체를 확인합니다. 변수 개체의 값은 동적 데이터의 결과이며 런타임에 평가됩니다. 변수는 정책 및 응답의 기능을 확장하기 위한 유연한 도구를 제공합니다.

변수 유형

다음과 같은 유형의 변수를 사용할 수 있습니다.

- [정적 변수](#) (페이지 634)
- [요청 컨텍스트 변수](#) (페이지 634)
- [사용자 컨텍스트 변수](#) (페이지 635)
- [양식 Post 변수](#) (페이지 635)
- [웹 서비스 변수](#) (페이지 636)

정적 변수

정적 변수는 간단한 이름/특정 형식의 값(예: 문자열, 부울 등) 쌍으로 구성됩니다. 정적 변수의 주요 이점은 적절한 프로그래밍 실례를 구현할 수 있다는 것입니다. 상수 값을 정책에서 사용할 때마다 반복하지 않고 정적 변수는 여러 정책에서 사용할 수 있는 하나의 데이터를 제공합니다.

요청 컨텍스트 변수

처리된 각 요청은 요청 컨텍스트를 설정합니다. 이 컨텍스트는 다음과 같은 속성을 식별합니다.

작업

요청에 지정된 작업 유형(예: GET 또는 POST)을 나타냅니다.

리소스

요청된 리소스(예: /directory_name/)를 나타냅니다.

서버

요청에 지정된 전체 서버 이름(예: `server.example.com`)을 나타냅니다.

요청 컨텍스트 변수는 이와 같은 정보를 캡처하여 정책 식 또는 응답에 포함할 수 있도록 해 줍니다. 이 변수 유형의 주요 이점은 프로그래밍 논리를 사용하지 않고도 세부적인 요청 컨텍스트 정보를 제공할 수 있다는 것입니다.

사용자 컨텍스트 변수

정책 서버가 디렉터리의 항목을 기준으로 사용자를 인증하면 사용자 컨텍스트가 생성됩니다. 사용자 컨텍스트는 사용자 디렉터리에 대한 정보와 인증된 사용자와 관련된 디렉터리의 내용으로 구성됩니다.

사용자 컨텍스트 변수는 디렉터리 연결의 특성을 기반으로 하거나 디렉터리의 내용을 기반으로 할 수 있습니다. 이 변수 유형의 주요 이점은 프로그래밍 논리를 사용하지 않고도 특정 사용자 컨텍스트를 기반으로 규칙을 자유롭게 정의할 수 있다는 것입니다.

양식 Post 변수

HTML 양식은 주로 백엔드 응용 프로그램이 요구하는 정보를 수집하는 데 사용됩니다. 양식 **Post** 변수를 사용하면 HTML 양식으로 입력되어 포스트된 정보를 캡처할 수 있습니다. 예를 들어, 응용 프로그램과 연결된 비즈니스 로직이 HTML 로그인 양식에 지정된 구매 주문서 금액을 요구하는 경우, 사용자가 제공하는 구매 주문의 값을 수집하기 위해 양식 **Post** 변수를 만드십시오. 그러면 이 변수를 정책에 사용할 수 있습니다.

중요: EJB 및 서블릿 에이전트는 양식 **Post** 변수를 지원하지 않습니다. EJB 또는 서블릿 에이전트에서 실행되는 정책에 양식 **Post** 변수를 사용하지 마십시오.

이 변수 유형의 주요 이점은 기업이 백엔드 서버 응용 프로그램에 보안 논리를 포함하도록 하는 대신 정책 서버가 정책 식의 일부로 **POST** 데이터를 사용할 수 있다는 점입니다. HTTP **POST** 변수를 사용하면 에이전트와 정책 서버 간의 효율적인 네트워크 사용이 가능합니다. 에이전트는 정책 서버가 권한 부여 처리 중에 HTTP 변수 정보를 사용할 수 있도록 HTTP 스트림에서 해당 정보를 추출합니다.

웹 서비스 변수

웹 서비스 변수를 사용하면 웹 서비스에서 검색한 정보를 캡처하여 정책 또는 응답에 사용할 수 있습니다. 이 유형의 변수를 통해 정책 서버 관리자는 웹 서비스에서 실시간으로 제공하는 동적 고객 정보를 바탕으로 정책을 정의하는 주요 이점을 누릴 수 있습니다.

추가 정보:

[웹 서비스 변수](#) (페이지 637)

정책에 변수 사용

변수를 사용하면 정책 식으로 작성할 수 있는 광범위한 동적 데이터를 캡처하여 정책에 비즈니스 논리를 포함할 수 있습니다. 관리 UI에서 변수 개체를 정의할 때 "정책" 대화 상자의 "식" 탭에서 이러한 변수를 식에 사용할 수 있습니다. 여러 변수 개체와 부울 연산자를 사용하여 정책의 복잡한 비즈니스 논리를 캡처하는 식을 작성할 수 있습니다.

예를 들어 응용 프로그램에 대한 액세스를 허용하기 위해 사용자의 계정 유형 및 신용 점수의 값을 필요로 하는 식이 정책에 포함될 수 있습니다. 계정 유형이 "골드"이고 신용 점수가 특정 값 이상인 사용자만 리소스에 액세스할 수 있도록 하는 식을 정책에 정의할 수 있습니다. 이 예에는 두 개의 변수가 필요하며 이들은 식으로 결합되어야 합니다.

추가 정보:

[정책의 식](#) (페이지 623)

응답에 변수 사용

응답에 변수를 사용할 수 있습니다. 관리 UI에서 변수 개체를 정의한 경우 응답에 이러한 변수를 사용할 수 있습니다. 응답 값은 런타임에 정책 서버가 변수 개체의 값을 확인할 때 생성됩니다.

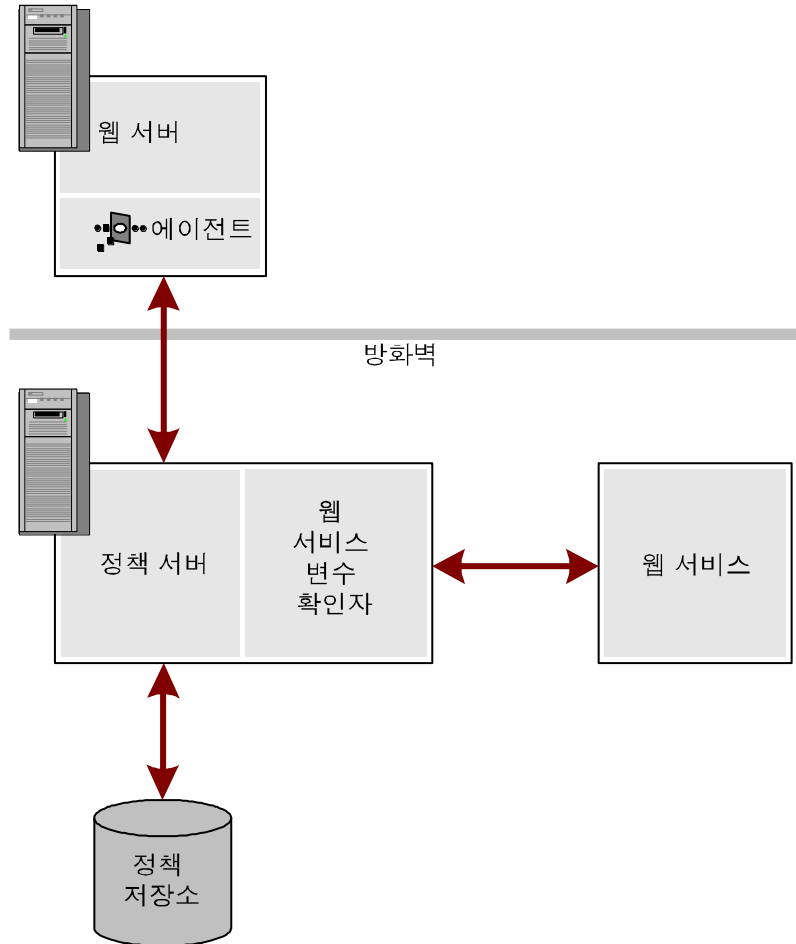
웹 서비스 변수

웹 서비스 변수는 웹 서비스의 동적 데이터를 **SiteMinder** 정책에 포함하는 방법을 제공합니다. 웹 서비스 변수는 웹 서비스를 호출하여 확인됩니다. 정책 서버는 웹 서비스 변수 정의에 지정된 대로 **SOAP** 요청 문서를 보내고 회신으로 **SOAP** 응답 문서를 받습니다. 정책 서버는 **SOAP** 응답 문서에서 웹 서비스 변수 값을 추출합니다.

SOAP(Simple Object Access Protocol)는 다음과 같은 세 부분으로 이루어진 XML 기반 경량 프로토콜입니다.

- 메시지 내용 및 처리 방법을 설명하는 프레임워크를 정의하는 봉투
- 응용 프로그램 정의 데이터 형식의 인스턴스를 표현하는 인코딩 규칙 집합
- 원격 프로시저 호출 및 응답을 나타내는 규칙

다음 그림에서는 배포된 SiteMinder가 인트라넷 내 웹 서비스의 웹 서비스 변수를 확인하는 방법을 보여 줍니다. 웹 서비스는 방화벽에서 정책 서버와 같은 쪽에 있습니다.



이 시나리오에서 웹 서비스 변수가 권한 부여 요청과 연관되어 있으면 해당 웹 서비스 변수는 웹 서비스 변수 확인자를 호출하여 정책 서버 측에서 확인됩니다. 웹 서비스 변수 확인자는 동일한 프로세스 공간에서 실행됩니다.

사용자는 웹 서비스 변수를 정의할 때 웹 서비스에 보낼 SOAP 문서, 인증 자격 증명 및 기타 매개 변수를 지정합니다.

확인자는 지정된 SOAP 문서를 웹 서비스에 보내고, 응답에서 변수 값을 추출해 정책 서버로 전달하여 권한 부여 요청을 완료하도록 합니다.

정책 서버와 웹 서비스 사이에 방화벽이 있더라도 둘 간의 통신을 허용하도록 구성할 수 있습니다. 정책 서버가 요청을 발급하고 응답을 읽기 때문에 방화벽은 정책 서버에서 웹 서비스로의 아웃바운드 요청을 허용하는 데만 필요합니다.

정책 서버와 웹 서비스 간에 보안 **SSL** 연결을 구성하면 웹 서비스에서 정책 서버로의 인바운드 요청을 허용할 수 있습니다. **SSL** 연결에서는 웹 서비스에 있는 서버 측 인증서와 정책 서버 측에 구성된 트러스트된 인증 기관 목록을 사용합니다.

웹 서비스 변수에 대한 구성 요소 요구 사항

웹 서비스 변수에는 세션 저장소가 필요합니다.

참고: 세션 저장소 구성에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오. 세션 저장소 업그레이드에 대한 자세한 내용은 *SiteMinder 업그레이드 안내서*를 참조하십시오.

웹 서비스 변수를 확인할 때의 보안 요구 사항

웹 서비스 변수의 보안을 위해서는 정책 서버와 웹 서비스 간에 **SSL** 연결이 필요합니다. 또한 **WS**-보안 헤더를 웹 서비스가 인식하도록 구성된 사용자 이름 토큰과 함께 포함할 수 있습니다. **WS**-보안은 보안 토큰 전파, 메시지 무결성 및 서명과 암호화를 통한 기밀성을 제공하는 **SOAP** 확장의 표준 집합입니다.

웹 서비스 변수의 보안 확인을 위해 필요한 사항:

- 정책 서버가 알려진 아이덴티티(웹 서비스 계정)를 대신하여 웹 서비스에 **SOAP** 요청을 수행해야 합니다. 이 모델은 **SiteMinder**가 사용자 디렉터리의 특성에 액세스하는 데 사용하는 모델과 비슷합니다.
- 웹 서비스 자격 증명이 포함된 **WS**-보안 헤더에 암호의 **base-64-encoded SHA-1** 다이제스트가 포함되도록 구성할 수 있습니다.
- 웹 서비스 변수에서 서버 측 인증서를 사용한 **SSL** 연결을 사용하도록 구성할 수 있습니다. 이를 위해서는 정책 서버가 트러스트된 **CA** 목록을 사용하여 구성되어야 합니다.

참고: SSL 연결의 경우 웹 서비스에 대한 서버 측 인증서를 구성하십시오. 정책 서버에서 트러스트된 CA의 목록을 구성하십시오. 트러스트된 CA를 구성하려면 인증 기관 및 웹 서비스 변수에서 설명하는 인증서 데이터 저장소를 사용하십시오.

웹 서비스 변수 확인자 구성

정책 서버가 웹 서비스 변수를 확인하기 위해서는 웹 서비스 변수 확인자가 웹 서비스에 연결되도록 구성하십시오. 웹 서비스 구성 요소에는 두 가지 범주가 있습니다.

- 정책 서버와 웹 서비스가 모두 방화벽의 같은 쪽에 있는 경우
- 정책 서버와 웹 서비스 사이에 방화벽이 있지만 이 둘 간의 단방향 통신(정책 서버에서 웹 서비스로의 아웃바운드 요청)만 허용하도록 구성된 경우

웹 서비스 변수 기능을 사용하려면 먼저 SmKeyTool 명령줄 유틸리티를 사용하여 정책 서버에 트러스트된 CA 목록을 구성해야 합니다. 부하 분산 또는 장애 조치 구성에 여러 정책 서버가 사용되는 경우 각 정책 서버에 동일한 트러스트된 CA 목록이 구성되어 있어야 합니다.

기본 구성 설정은 SiteMinder/Config/properties 디렉터리의 WebServiceConfig.properties 파일에 제공됩니다. 이 속성은 수정할 수 있습니다.

샘플 WebServiceConfig.properties 구성 파일

```
# Netegrity Web Service Variable Resolver properties configuration file:
# This file must be in the classpath that is used when the policy server runs.
# ResolutionTimeout is the amount of time the resolver will at most wait to resolve
all Web Service variables related to a given request.
#
# This setting is intended to end sessions that are waiting on a web service that is
not responding. The time that the Web Agent will typically wait before responding is
typically 60 sec (but may be changed # in the future), which means this setting should
be 60000 or greater to cancel transactions that cannot be returned.
ResolutionTimeout=75000
# MaxThreadCount is the maximal number of active threads running within the Web Service
variables resolver.
MaxThreadCount=10
```

인증 기관 및 웹 서비스 변수

웹 서비스 변수를 확인할 때 SSL 연결을 사용하려면 트러스트된 CA(인증 기관)의 목록을 구성하십시오. 정책 서버는 웹 서비스에 연결할 때 CA를 사용합니다.

인증서 데이터 저장소의 목록을 구성하려면 관리 UI를 사용하십시오.

변수 만들기

정책 또는 응답에서 사용할 수 있도록 변수를 생성할 수 있습니다. 변수는 도메인 개체입니다. 특정 정책 도메인 내에 변수를 생성하거나, smobjimport 도구를 사용하여 도메인으로 변수를 가져올 수 있습니다.

정책 도메인으로 개체를 가져오는 방법에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

추가 정보:

[도메인](#) (페이지 547)

정적 변수 만들기

정책 또는 응답에서 사용할 수 있도록 정적 변수를 생성할 수 있습니다.

참고: 확인된 변수의 값은 1K 보다 작아야 합니다.

다음 단계를 수행하십시오.

1. "정책", "도메인"을 차례로 클릭합니다.
2. "변수"를 클릭합니다.
3. "변수 만들기"를 클릭합니다.

"Create a new object of type Variable"(변수 유형의 새 개체 만들기) 옵션이 선택되어 있는지 확인합니다.

4. "확인"을 클릭합니다.
5. 목록에서 도메인을 선택한 후 "다음"을 클릭합니다.
6. "이름" 필드에 변수 이름을 입력합니다.

7. "변수 유형" 목록에서 "정적"을 선택합니다.

"정적 변수" 설정이 열립니다.

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

8. "변수 정보"에서 변수의 값과 데이터 형식을 지정합니다.

9. "제출"을 클릭합니다.

변수가 도메인의 "변수" 탭에 표시됩니다. 이제 변수를 정책 식 또는 응답에 사용할 수 있습니다.

요청 컨텍스트 변수 만들기

정책 또는 응답에서 사용할 수 있도록 요청 컨텍스트 변수를 생성할 수 있습니다.

참고: 확인된 변수의 값은 1K 보다 작아야 합니다.

다음 단계를 수행하십시오.

1. "정책", "도메인"을 차례로 클릭합니다.
2. "변수"를 클릭합니다.
3. "변수 만들기"를 클릭합니다.

"Create a new object of type Variable"(변수 유형의 새 개체 만들기) 옵션이 선택되어 있는지 확인합니다.

4. "확인"을 클릭합니다.
5. 목록에서 도메인을 선택한 후 "다음"을 클릭합니다.
6. "이름" 필드에 변수 이름을 입력합니다.

참고: "요청 컨텍스트" 변수 이름은 백분율 문자(%)로 시작해야 합니다.

예: %REQUEST_ACTION

7. "변수 유형" 목록에서 "요청 컨텍스트"를 선택합니다.

요청 컨텍스트 설정이 열립니다.

8. "속성" 목록에서 변수 값을 선택합니다.
9. "확인"을 클릭합니다.

변수가 도메인의 "변수" 탭에 표시됩니다. 이제 변수를 정책 식 또는 응답에 사용할 수 있습니다.

사용자 컨텍스트 변수 만들기

정책 또는 응답에서 사용할 수 있도록 사용자 컨텍스트 변수를 생성할 수 있습니다.

참고: 확인된 변수의 값은 1K 보다 작아야 합니다.

다음 단계를 수행하십시오.

1. "정책", "도메인"을 차례로 클릭합니다.
2. "변수"를 클릭합니다.
3. "변수 만들기"를 클릭합니다.

"Create a new object of type Variable"(변수 유형의 새 개체 만들기) 옵션이 선택되어 있는지 확인합니다.

4. "확인"을 클릭합니다.
5. 목록에서 도메인을 선택한 후 "다음"을 클릭합니다.
6. "이름" 필드에 변수 이름을 입력합니다.

참고: 사용자 컨텍스트 변수 이름은 백분율 문자(%)로 시작해야 합니다.

예: %SM_USERPATH

7. "변수 유형" 목록에서 "사용자 컨텍스트"를 선택합니다.
"사용자 컨텍스트" 설정이 열립니다.
8. "항목" 목록에서 변수의 값을 제공하는 사용자 컨텍스트 부분을 선택합니다.
9. (세션 변수에 필요) 변수로 나타내는 데이터의 형식(부울, 숫자, 문자열 또는 날짜)을 "반환 유형" 필드에 지정합니다.
다른 "항목" 목록 선택의 경우 "반환 유형" 값은 "문자열" 또는 "부울"로 적절하게 미리 설정되어 있으며 이는 사용자가 구성할 수 없습니다.
10. (사용자 속성, 디렉터리 항목 및 세션 변수에 필요) 변수 값을 제공하는 사용자 특성 또는 디렉터리의 이름을 "속성" 필드에 입력합니다.

11. (사용자 속성, 디렉터리 항목 및 세션 변수에 필요) 변수를 저장하기 위한 버퍼의 크기(바이트 단위)를 "버퍼" 필드에 입력합니다.
12. (디렉터리 항목에 필요) 디렉터리 항목의 고유 이름을 "DN" 필드에 입력합니다.
13. 제출을 클릭합니다.
변수가 도메인의 "변수" 탭에 표시됩니다. 이제 변수를 정책 식 또는 응답에 사용할 수 있습니다.

사용자 컨텍스트 변수를 처리할 때 다중 값 사용자 특성 결과를 지원하도록 구성

기본적으로, 디렉터리에서 지정된 사용자 속성의 값을 가져오도록 구성된 사용자 컨텍스트 변수는 단일 값 사용자 특성만 지원합니다.

사용자 컨텍스트 변수를 처리할 때 다중 값 사용자 특성 결과를 지원하도록 정책 서버를 구성할 수 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버를 중지합니다.
2. 텍스트 편집기에서 다음 파일을 엽니다.
`ps_install_dir\config\properties\scriptActiveExpConfig.properties`
3. 파일에서 임의의 위치에 다음 항목을 포함하는 줄을 추가합니다.
`ALLOW_MULTIVALUSERATTR=1`
4. 파일을 저장하고 텍스트 편집기를 종료합니다.
5. 정책 서버 시작

양식 Post 변수 만들기

양식 Post 변수를 생성하여 정책에서 사용할 수 있습니다.

참고: 확인된 변수의 값은 1K 보다 작아야 합니다.

다음 단계를 수행하십시오.

1. "정책", "도메인"을 차례로 클릭합니다.
2. "변수"를 클릭합니다.
3. "변수 만들기"를 클릭합니다.

"Create a new object of type Variable"(변수 유형의 새 개체 만들기)
옵션이 선택되어 있는지 확인합니다.

4. "확인"을 클릭합니다.
5. 목록에서 도메인을 선택한 후 "다음"을 클릭합니다.
6. "이름" 필드에 변수 이름을 입력합니다.
7. "변수 유형" 목록에서 "Post"를 선택합니다.

양식 Post 설정이 열립니다.

8. "양식 필드 이름" 필드에 양식에 포함된 POST 변수의 이름을 입력합니다.
9. "확인"을 클릭합니다.

변수가 도메인의 "변수" 탭에 표시됩니다. 이제 정책 식에 변수를 사용할 수 있습니다.

웹 서비스 변수 만들기

정책 또는 응답에서 사용할 수 있도록 웹 서비스 변수를 생성할 수 있습니다.

참고: 확인된 변수의 값은 1K 보다 작아야 합니다.

다음 단계를 수행하십시오.

1. "정책", "도메인"을 차례로 클릭합니다.
2. "변수"를 클릭합니다.
3. "변수 만들기"를 클릭합니다.

"Create a new object of type Variable"(변수 유형의 새 개체 만들기) 옵션이 선택되어 있는지 확인합니다.

4. "확인"을 클릭합니다.
5. 목록에서 도메인을 선택한 후 "다음"을 클릭합니다.
6. "이름" 필드에 변수 이름을 입력합니다.
7. "변수 유형" 목록에서 "웹 서비스"를 선택합니다.
웹 서비스 설정이 표시됩니다.
8. "반환 유형" 목록에서 데이터 형식을 선택합니다.
9. URL 필드에 웹 서비스 URL 을 입력합니다.
10. "XPath" 필드에 XPath 쿼리를 입력합니다.

참고: 정책 서버는 이 쿼리를 사용하여 웹 서비스가 반환하는 SOAP 문서에서 웹 서비스 변수의 값을 추출합니다.

11. (선택 사항) "웹 서비스 자격 증명"에서 "자격 증명 필요" 옵션을 선택하고 정책 서버가 웹 서비스에 연결할 때 사용할 사용자 이름과 암호를 지정합니다.
12. (선택 사항) "SOAP 문서" 섹션에서 다음 단추를 클릭하여 기존 변수를 SOAP 메시지에 추가합니다.

변수

13. (선택 사항) "HTTP 헤더"에서 "추가"를 클릭하여 HTTP 헤더를 웹 서비스 변수와 연결합니다.
14. "마침"을 클릭합니다.
변수가 도메인의 "변수" 탭에 나타나므로 이제 정책 식이나 응답에 사용할 수 있습니다.

제 19 장: 키 및 인증서 관리

인증서 및 개인 키 사용

다음 태스크에는 개인 키와 인증서가 필요합니다.

- 페더레이션 구성 요소는 전체 세션 또는 특정 어설션 콘텐츠의 서명, 유효성 검사, 암호화 또는 암호 해독에 개인 키/인증서 쌍을 사용합니다.
- 페더레이션 구성 요소는 아티팩트 싱글 사인온에 대한 백 채널 인증에 클라이언트 인증서를 사용합니다.
- SSL 연결을 설정하는 경우(SSL 서버 인증서)

개인 키/인증서 쌍과 페더레이션 기능을 위한 단일 인증서는 CDS(인증서 데이터 저장소)에 저장됩니다. 인증서 데이터 저장소는 정책 저장소와 같은 곳에 배치됩니다. 동일한 정책 저장소에 대한 공통의 뷰를 공유하는 모든 정책 서버는 동일한 키, 인증서, CDS 구성 CRL(인증서 해지 목록) 및 OCSP 응답자에 액세스할 수 있습니다.

SSL 서버 인증서는 SSL 서버 인증서가 설치된 웹 서버에 저장됩니다. SSL 서버 인증서는 인증서 데이터 저장소에 저장되지 않습니다.

인증서 데이터 저장소의 각 키/인증서 쌍, 클라이언트 인증서 및 트러스트된 인증서마다 각각 고유한 별칭이 있어야 합니다. 별칭은 인증서 저장소의 모든 개인 키/인증서 쌍 또는 단일 인증서를 고유하게 참조하는 데 사용됩니다. 인증서 데이터 저장소는 여러 키/인증서 쌍과 단일 인증서를 저장할 수 있습니다. 페더레이션 환경에서는 파트너가 여러 개 있을 수 있습니다. 파트너가 여러 개인 경우 각 파트너마다 다른 쌍을 사용할 수 있습니다.

서명 별칭이 서명 어설선에 대해 구성된 경우 어설선 생성기는 해당 별칭과 연결된 키를 사용하여 어설선에 서명합니다. 구성된 서명 별칭이 없으면 어설선 생성기는 **defaultenterpriseprivatekey** 별칭의 키를 사용하여 어설선에 서명합니다. 어설선 생성기가 기본 엔터프라이즈 개인 키를 찾지 못한 경우에는 처음 발견된 개인 키를 사용하여 어설선에 서명합니다.

중요! 여러 개의 키를 저장하려는 경우에는 추가하는 첫 번째 키를 **defaultenterpriseprivatekey** 별칭을 사용하여 정의한 다음 이후 키를 추가하십시오.

지정된 정책 서버가 응답을 서명하거나 서명하고 확인할 수 있습니다. 서명 및 확인을 위한 키와 인증서를 동일한 인증서 데이터 저장소에 추가할 수 있습니다.

관리 UI 를 사용하여 인증서 데이터 저장소의 콘텐츠를 관리할 수 있습니다.

다음과 같은 유형의 키/인증서 쌍과 단일 인증서가 인증서 데이터 저장소에 저장됩니다.

Function	개인 키/인증서 쌍	Certificate (공개 키)	CA 인증서	클라이언트 인증서
어설선, 인증 요청, SLO 요청 및 응답에 서명	X			
서명된 어설선, 인증 요청 및 SLO 요청/응답 확인		X		
어설선, 이름 ID 및 특성을 암호화 (SAML 2.0 전용)		X		
어설선, 이름 ID 및 특성을 암호 해독 (SAML 2.0)	X			
아티팩트 백 채널의 클라이언트 인증에 대한 자격 증명 역할 수행				X
다른 인증서 및 인증서 해지 목록 확인			X	
SSL 연결을 사용하여 웹 서비스 변수 확인			X	

추가 정보:[서명 및 확인 작업](#) (페이지 651)[SSL 연결에 대한 인증서](#) (페이지 652)

서명 및 확인 작업

정책 서버는 서명 및 확인 태스크에 개인 키/인증서 쌍을 사용합니다. 개인 키/인증서 쌍은 어설션, 어설션 응답 또는 인증 요청에 서명하는 데 사용됩니다. 서명되는 특정 메시지는 실행 중인 트랜잭션과 사용 중인 페더레이션 프로필에 따라 달라집니다.

모든 서명 트랜잭션 전에 어설션에 서명하는 파트너는 개인 키/인증서 쌍과 연결된 인증서(공개 키)를 파트너에 전송합니다. 이 교환은 대역외 통신의 일부로 수행됩니다. 파트너는 인증서를 사용하여 서명을 확인합니다.

트랜잭션이 발생할 때 기본적으로 어설션 당사자가 어설션에 인증서를 포함합니다. 하지만 확인 프로세스 중에 파트너는 파트너 사이트에 저장하는 인증서를 사용하여 서명의 유효성을 검사합니다.

SAML 2.0 싱글 로그아웃의 경우 로그아웃을 시작하는 측이 요청에 서명하고 요청을 받는 측이 서명을 확인합니다. 이와 반대로 받는 측은 SLO 응답에 서명하고 이니시에이터가 응답을 확인합니다.

암호화/암호 해독 작업

SAML 2.0 의 경우 전체 어설션, NameID 또는 기타 특성을 암호화하도록 정책 서버를 구성할 수 있습니다. 암호화가 사용되도록 설정하면 어설션 당사자는 신뢰 당사자가 데이터를 암호화하기 위해 보내는 인증서(공개 키)를 사용합니다. 트랜잭션 이전에 신뢰 당사자는 대역외 교환에서 인증서를 어설션 당사자에게 보냅니다. 신뢰 당사자는 개인 키/인증서 쌍을 사용하여 데이터를 암호 해독합니다.

참고: SAML 1.1 및 WS-페더레이션은 어설션 데이터의 암호화를 지원하지 않습니다.

SSL 연결에 대한 인증서

정책 서버는 다음과 같은 방식으로 SSL 연결을 사용합니다.

- 페더레이션 통신의 경우

SAML HTTP-아티팩트 백 채널 또는 일반 페더레이션 통신에 SSL 을 사용하도록 설정할 수 있습니다. SSL 연결을 설정하려면 신뢰 당사자는 CA 인증서를 서명된 SSL 서버 인증서와 연결해야 합니다.

SSL 서버 인증서는 SSL 연결에 보안을 적용합니다. CA 인증서는 SSL 서버 인증서가 트러스트되었는지 확인합니다.

- ICAS 의 경우

SSL 연결을 사용하도록 설정하여 신뢰 당사자의 양식 자격 증명 수집기 파일을 보호하십시오. SSL 서버 인증서를 신뢰 당사자 웹 사이트에서 인증서 데이터 저장소로 가져옵니다. 서버 인증서는 SSL 연결에 보안을 적용합니다.

- 웹 서비스 변수의 경우

웹 서비스 변수 확인에 SSL 연결을 사용하도록 설정할 수 있습니다.

참고: SSL 서버 인증서는 해당 인증서가 설치된 웹 서버에 저장됩니다. SSL 서버 인증서는 인증서 데이터 저장소에 저장되지 않습니다.

아티팩트 백 채널에 보안을 적용하기 위한 인증서

아티팩트 바인딩을 사용하여 싱글 사인온을 구축하려면 신뢰 당사자는 어설션에 대한 요청을 어설션 당사자의 SiteMinder 에 전송합니다. 어설션 요청은 어설션 검색 서비스(SAML 1.1) 또는 아티팩트 레졸루션 서비스(SAML 2.0)로 보내집니다. 검색 서비스는 신뢰 당사자가 제공한 아티팩트를 사용하여 어설션을 검색합니다. SiteMinder 는 응답을 다시 백 채널을 통해 신뢰 당사자로 보냅니다. 백 채널은 어설션 수행 측과 신뢰 당사자 사이의 보안 연결입니다. 반면에 웹 브라우저 통신은 프런트 채널을 통해 수행됩니다.

다음 인증 방법 중 하나를 사용하여 백 채널과 검색 서비스를 권한 없는 액세스로부터 보호하십시오.

- 기본
- SSL 을 통한 기본 인증
- X.509 클라이언트 인증서

X.509 클라이언트 인증서를 인증 방법으로 사용하는 경우 신뢰 당사자는 클라이언트 인증서를 자격 증명으로 제공해야 합니다. 이 자격 증명을 통해 신뢰 당사자는 어설션을 검색하는 어설션 당사자의 서비스에 액세스할 수 있습니다.

인증 방법을 선택할 때는 다음 사항을 고려하십시오.

- 백 채널에 SSL 연결을 사용하는 방법을 고려하십시오. 트러스트된 CA 가 서명한 SSL 서버 인증서로 SSL 연결에 보안을 적용하십시오.

공통 루트 및 중간 CA 인증서의 기본 집합이 인증서 데이터 저장소와 함께 제공됩니다. CA 가 서명한 다른 서버 인증서를 사용하려면 CA 인증서를 저장소에 트러스트된 CA 인증서로 가져옵니다.

페더레이션은 백 채널 요청을 처리할 때 SSL-클라이언트를 사용합니다. 어설션 당사자의 웹 서버는 다음 암호화를 통해 SSL 버전 TLSV1_1 및 TLSV1_2 를 사용하도록 구성될 수 있습니다.

- RSA_With_AES_128_CBC_SHA256
- RSA_With_AES_256_CBC_SHA256

이러한 암호화는 FIPS 모드와 비 FIPS 모드에서 모두 지원됩니다. SHA256 사용 여부는 SP 서버 측에서 결정됩니다. 페더레이션에는 알고리즘 선택을 위한 구성이 없습니다. 따라서 관리자는 어설션 당사자의 서버가 적절하게 구성되어 있는지 확인해야 합니다.

- 연결을 설정하기 위해 X.509 클라이언트 인증서가 필요한 경우 신뢰 당사자에 키/인증서 쌍이 있어야 하며, 그렇지 않으면 클라이언트 인증서 인증이 실패합니다. 클라이언트 인증서가 어설션 당사자의 인증서 데이터 저장소에 있는지 확인하십시오. 신뢰 당사자가 어설션에 대한 요청을 보낼 때는 클라이언트 인증서가 검색 서비스에 액세스하기 위한 신뢰 당사자 자격 증명의 역할을 합니다.

인증서 데이터 저장소에서 지원하는 형식

인증서 데이터 저장소는 다음 형식을 지원합니다.

- 개인 키는 다음 형식으로 지원되며 DER 또는 PEM 인코딩되어야 합니다.
 - PKCS1
 - PKCS5
 - PKCS8
 - PKCS12RSA 키만 지원됩니다.
- 공개 인증서는 다음과 같은 X.509 인증서 형식으로 지원됩니다.
 - V1
 - V2
 - V3
- 공개 인증서는 다음 인코딩 형식으로 지원됩니다.
 - DER
 - Base64
 - PEM

트러스트된 인증서 및 키/인증서 쌍 가져오기

키/인증서 쌍과 트러스트된 인증서는 여러 페더레이션 SSO 와 기타 기능에 영향을 줍니다. 키 및 인증서를 사용하는 태스크를 실행하려면 이러한 항목이 인증서 데이터 저장소에 있어야 합니다.

인증서 데이터 저장소에 키/인증서 쌍이 없는 경우에는 다음 두 가지 옵션을 사용할 수 있습니다.

- 기존 파일(.p12 또는 .pfx)에서 키/인증서 쌍을 가져옵니다.
- 키/인증서 쌍을 생성합니다.

새 키/인증서 쌍을 생성하려면 트러스트된 인증 기관에 인증서를 요청한 다음 기관에서 반환한 서명된 인증서 응답을 가져옵니다.

추가 정보:

[인증서 및 개인 키 사용](#) (페이지 649)

[기존 파일에서 키/인증서 쌍 가져오기](#) (페이지 655)

[키 및 인증서 쌍을 생성하는 방법](#) (페이지 656)

기존 파일에서 키/인증서 쌍 가져오기

인증서 데이터 저장소에 키/인증서 쌍이 없는 경우 기존 .p12 또는 .pfx 파일에서 가져옵니다.

정책 서버는 가져온 인증서를 트러스트된 인증서로 처리합니다. 단, 자체 서명된 인증서는 예외적으로 다음 지침에 따라 처리됩니다.

- 정책 서버는 V3 자체 서명 인증서를 CA 인증서로 식별합니다. 이 경우 V3 자체 서명 인증서는 CA 인증서로 처리됩니다. 이 동작은 인증서/개인 키 대화 상자에서 가져오기를 시작하더라도 수행됩니다.
- 정책 서버는 다음과 같은 경우 인증서를 트러스트된 인증서로 처리합니다.
 - 정책 서버가 V3 자체 서명 인증서를 CA 인증서로 식별하지 않는 경우
 - 인증서가 V1 자체 서명 인증서인 경우

다음 단계를 수행하십시오.

1. 관리 UI에 로그인합니다.
2. "인프라", "X509 인증서 관리", "트러스트된 인증서 및 개인 키"를 선택합니다.
3. "새로 가져오기"를 클릭하고 마법사의 단계를 따릅니다.

4. 마법사를 진행할 때 다음 사항을 참조하십시오.

- 키와 인증서가 들어 있는 단일 파일을 가져오거나, 키 파일과 인증서 파일을 개별적으로 가져올 수 있습니다. 사용하는 파일에 해당하는 옵션 단추를 선택하십시오.
- 자체 서명된 인증서를 인증 기관 인증서로서 가져오려면 "Use as CA"(CA 로 사용) 옵션 단추를 "예"로 설정하십시오. 인증서는 CA 인증서로서 가져오기되며 파트너 관계를 구성할 때(예: 서명 또는 암호화를 위해 구성할 때)는 사용할 수 없습니다.
그렇지 않은 경우, 기본값인 "아니요" 설정을 선택하여 파트너 관계를 구성할 때 사용 가능한 트러스트된 인증서로서 인증서를 가져오십시오.
- DER(바이너리) 형식의 트러스트된 인증서 파일의 경우 파일에는 하나 이상의 인증서가 포함될 수 있습니다. PEM(base 64) 형식의 트러스트된 인증서 파일의 경우 파일당 하나의 인증서가 필요합니다.
- .p12 파일을 사용할 때는 암호를 입력해야 합니다.
- 인증서 데이터 저장소에 추가하려는 각 항목에 대해 해당 항목과 연결하려는 별칭을 입력하십시오. 여러 항목을 선택하는 경우 각 항목마다 고유한 별칭이 필요합니다.

5. "확인" 단계에서 정보를 검토하고 "마침"을 클릭합니다.

키/인증서 쌍을 인증서 데이터 저장소로 가져왔습니다.

키 및 인증서 쌍을 생성하는 방법

인증서 데이터 저장소에 키/인증서 쌍이 없는 경우에는 새 키/인증서 쌍을 생성할 수 있습니다.

다음 단계를 수행하십시오.

1. 인증서 요청을 생성하고 요청을 트러스트된 인증 기관에 보냅니다.
2. 기관으로부터 서명된 인증서 응답을 가져옵니다.

인증서 요청 생성

인증서 데이터 저장소에 키/인증서 쌍이 없는 경우에는 트러스트된 인증 기관에 새로 요청하십시오. CA 에서 서명된 인증서 응답을 반환하면 이를 인증서 데이터 저장소로 가져오십시오.

인증서 요청을 생성하면 정책 서버는 개인 키 및 자체 서명 인증서 쌍을 생성합니다. 정책 서버는 이 쌍을 인증서 데이터 저장소에 저장합니다. 생성된 요청을 사용하여 인증 기관에 연결하고 CA 인증서 요청 양식을 기입하십시오. 그런 다음 생성된 요청의 내용을 양식에 붙여 넣으십시오.

CA에서는 일반적으로 PKCS #7 형식으로 서명된 인증서 응답을 생성합니다. 서명된 인증서 응답을 인증서 데이터 저장소로 가져올 수 있습니다. 서명된 인증서 응답을 가져온 후에 별칭이 동일한 기존 자체 서명 인증서가 대체됩니다.

다음 단계를 수행하십시오.

1. 관리 UI에 로그인합니다.
2. "인프라", "X509 인증서 관리", "트러스트된 인증서 및 개인 키"를 선택합니다.
3. "인증서 요청"을 클릭합니다.
4. 필수 필드를 기입합니다.
5. "저장"을 클릭합니다.

PKCS #10 사양을 따르는 파일이 생성됩니다.

브라우저에서 인증서 요청이 포함된 파일을 저장할지 아니면 열지를 묻는 메시지가 표시됩니다. 이 파일을 저장하지 않더라도(즉, 파일을 열고 텍스트를 추출하더라도) 정책 서버는 개인 키 및 자체 서명 인증서 쌍을 생성합니다. 개인 키에 대한 새 요청 파일을 가져오려면 "CSR 생성" 기능을 사용하여 새 인증서 서명 요청을 생성하십시오.

서명된 인증서 응답 가져오기

인증서 요청을 작성하고 이를 인증 기관에 전송하면 인증 기관에서 서명된 인증서 응답을 발급합니다.

서명된 인증서를 인증 데이터 저장소로 가져와서 동일한 별칭을 가진 기존의 자체 서명된 인증서 항목을 이 서명된 인증서로 바꾸십시오.

다음 단계를 수행하십시오.

1. "인프라", "X509 인증서 관리", "트러스트된 인증서 및 개인 키"를 선택합니다.
2. 목록에서 업데이트할 자체 서명된 인증서를 찾습니다.

3. 자체 서명된 항목 옆의 "작업", "인증서 업데이트"를 선택합니다.
4. 원하는 파일을 찾아 이동합니다. 사용 가능한 파일은 다음과 같습니다.
 - 서명된 인증서와 해당 인증서 체인이 포함된 .p7 또는 .p7b 파일
 - 인증서 체인 없이 서명된 인증서가 있는 .cer 또는 .crt 파일(base64 PEM 파일)
5. 적절한 항목을 선택합니다.
6. 인증서 정보를 검토한 다음 "마침"을 클릭합니다.

서명된 인증서를 인증서 데이터 저장소로 가져오게 되고 자체 서명된 인증서가 대체됩니다.

새 인증서 서명 요청 생성

CSR(인증서 서명 요청)은 디지털 아이덴티티 인증서를 신청하기 위해 인증 기관에 보내는 메시지입니다. 개인 키를 생성한 후 CSR 를 생성할 수 있습니다. CSR 에는 공개 키가 포함되어 있습니다.

자체 서명되거나 CA 서명된 개인 키/인증서 쌍에 대한 새 CSR 를 생성할 수 있습니다. 개인 키는 항상 기존 개인 키를 수정하지 않고 동일한 CSR 를 생성합니다. 기존 개인 키에 대한 새 요청을 생성하는 이유는 다음과 같습니다.

- 개인 키/자체 서명 인증서 쌍에 대해 생성된 원래 요청이 더 이상 없는 경우
- 인증서가 만료되어 새 인증서가 필요한 경우. 이 경우에는 인증 기관에 제출하기 위한 새로운 CSR 사본이 필요합니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "인프라", "X509 인증서 관리", "트러스트된 인증서 및 개인 키"를 선택합니다.
3. 새 CSR 을 원하는 개인 키 항목에 대해 "작업", "CSR 생성"을 선택합니다.
PKCS #10 사양을 따르는 파일이 생성됩니다.
4. 메시지가 표시되면 CSR 을 저장합니다.

5. (선택 사항) CA 서명된 인증서가 필요한 경우 인증 기관에 문의합니다. 요청을 제출하기 위해 해당 인증 기관이 요구하는 절차를 따르십시오. 이전 단계에서 저장한 PKCS#10 파일을 요청에 사용합니다.

인증서 요청 프로세스를 완료하면 인증 기관에서 서명된 인증서 응답을 발급합니다. 이 인증서를 인증서 데이터 저장소로 가져옵니다. 그러면 정책 서버는 별칭이 같은 기존 인증서 항목을 새로 가져온 인증서로 바꿉니다.

인증서 데이터 저장소에서 인증서 업데이트

키/인증서 쌍과 독립 실행형 인증서를 다음과 같은 방법으로 업데이트할 수 있습니다.

- 기존 인증서를 삭제하고 새 트러스트된 인증서를 가져와서 만료되는 트러스트된 인증서를 업데이트합니다. 새 인증서는 인증서 데이터 저장소의 만료 인증서와 일치해야 합니다.
- 서명되고 트러스트된 인증서 또는 PKCS7 서명된 응답을 가져와서 인증서를 업데이트합니다. 새 인증서는 인증서 데이터 저장소의 만료 인증서와 일치해야 합니다.
- 인증서를 PKCS#12 파일의 인증서로 업데이트합니다. 새 개인 키 및 인증서 쌍은 인증서 데이터 저장소의 만료되는 키/인증서 쌍과 일치해야 합니다.

새 인증서가 유효해야만 정책 서버가 이를 사용하여 만료되는 인증서를 업데이트할 수 있습니다. 인증서를 가져오면 즉시 인증서가 업데이트되고 사용 가능하게 됩니다. 유효 간격에 따라 확인한 결과 새 인증서가 유효하지 않으면 정책 서버는 새 인증서를 사용할 수 없습니다.

트러스트된 인증서만 가져오려면 PEM 또는 DER 인코딩의 인증서가 포함된 파일을 사용하십시오. 이러한 파일 유형의 표준 확장명은 *.crt 또는 *.cer 입니다. 파일이 .p12 또는 .pfx 로 끝나면 키/인증서 쌍이 포함된 인증서 데이터 저장소 파일로 처리됩니다. 마지막으로 파일이 .p7 또는 .p7b 로 끝나면 서명된 응답 파일로 처리됩니다. 다른 파일은 모두 인증서 파일로 취급되며 SiteMinder 는 여기에서 인증서 로드를 시도합니다.

참고: 페더레이션 환경의 인증서를 업데이트하는 경우 만료되는 인증서를 사용하는 페더레이션 개체는 업데이트할 필요가 없습니다.

인증서 및 키 데이터 내보내기

개인 키/인증서 쌍을 내보내고 이를 페더레이션 파트너로 전송할 수 있습니다. 파트너는 인증서를 사용하여 인증서의 연결된 개인 키로 생성된 디지털 서명을 확인할 수 있습니다.

중요! 백업 중 개인 키를 내보낼 경우 다른 사람과 공유하지 마십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "인프라", "X509 인증서 관리", "트러스트된 인증서 및 개인 키"를 선택합니다.
3. 내보낼 항목에 대해 "작업", "내보내기"를 선택합니다.
4. 내보낸 데이터에서 생성하고자 하는 파일의 형식을 선택합니다.
5. 파일 형식을 선택합니다.
6. "Export"(내보내기)를 클릭합니다.

로컬 시스템에서 파일을 열거나 저장하라는 메시지가 표시됩니다.

키 또는 인증서를 나타내는 인코딩된 파일 콘텐츠가 생성됩니다.

인증 기관(CA) 인증서 사용

페더레이션 시스템은 인증 기관 인증서를 사용하여 다음 항목을 확인합니다.

- SAML HTTP-아티팩트 백 채널에 보안을 적용하는 SSL 연결에 대한 SSL 서버 인증서가 트러스트된 인증서인지 여부
- HTTP-아티팩트 싱글 사인온의 경우 SSL 연결로 백 채널에 보안을 적용하십시오. 페더레이션 시스템의 포함된 웹 서버는 인증 기관의 인증서를 확인하여 SSL 연결이 트러스트된 인증서로 보안 적용되는지 확인할 수 있습니다. 이 인증서는 인증서 데이터 저장소에 저장되어야 합니다.
- 인증서 해지 목록이 유효한지 여부.

CRL 은 인증 기관에서 가져옵니다. CRL 의 유효성을 검사하려면 해당 CA 의 인증서가 필요합니다. CRL 은 런타임에 사용되기 위해 데이터 저장소에 저장됩니다.

이를 위해 공통 루트 및 중간 CA 인증서의 기본 집합이 제품과 함께 제공됩니다.

CA 인증서 가져오기

공통 루트 및 중간 CA 인증서의 집합이 제품에 포함되어 있습니다. 인증서 데이터 저장소에 없는 CA 인증서를 사용하려면 해당 CA 인증서를 가져오십시오.

가져오는 모든 인증서는 CA 인증서로 취급됩니다. 자체 서명된 인증서는 예외입니다.

- 시스템이 V3 자체 서명 인증서를 비 CA 인증서로 식별하는 경우 인증서는 트러스트된 인증서로 취급됩니다. 이 동작은 "CA 인증서 가져오기" 대화 상자에서 가져오기를 시작한 경우에도 적용됩니다.
- 시스템이 V1 자체 서명된 인증서를 식별하는 경우 인증서는 CA 인증서로 취급됩니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "인프라", "X509 인증서 관리", "인증 기관"을 차례로 선택합니다.
3. "새로 가져오기"를 클릭합니다.

4. 마법사의 단계에 따라 새 항목을 가져옵니다.
5. 인증서 정보를 검토한 다음 "마침"을 클릭합니다.

CA 인증서를 인증서 데이터 저장소로 가져왔습니다. 변경 내용은 가져오기가 완료된 직후 적용됩니다.

중요! 시스템에서 사용 중인 인증서에 대한 트러스트 체인의 일부인 CA 인증서는 삭제할 수 없습니다. 사용 중인 CA 인증서를 삭제하려고 하면 인증서를 삭제할 수 없다는 오류 메시지가 표시됩니다.

CRLs 를 사용하여 인증서 유효성 확인

CRL(인증서 해지 목록)은 인증 기관에서 해당 구독자에게 발급됩니다. 이 목록에는 무효화되거나 해지된 인증서의 일련 번호가 포함되어 있습니다. 서버에 액세스 요청이 수신되면 서버는 CRL 을 기반으로 액세스를 허용하거나 거부합니다.

페더레이션은 인증서 기능에 CRL 을 이용할 수 있습니다. SiteMinder 가 CRL 을 사용하려면 인증서 데이터 저장소가 현재 CRL 에 연결되어야 합니다. SiteMinder 가 해지된 파트너 인증서를 사용하려고 하면 오류 메시지가 표시됩니다. 레거시 페더레이션의 경우 이 오류 메시지는 SAML 어설션에 포함됩니다. 이 메시지는 인증이 실패했음을 나타냅니다.

참고: 페더레이션 기능은 X.509 인증 체계와는 다른 방식으로 CRL 사용을 구현합니다. 이 인증 체계에서는 CRL 을 저장하는 독립 LDAP 디렉터리를 사용하며, 인증서 데이터 저장소는 사용하지 않습니다.

SiteMinder 는 다음과 같은 CRL 기능을 지원합니다.

- 파일 기반 CRL 또는 LDAP CRL

SiteMinder 는 CRL 을 인증서 데이터 저장소에 저장합니다. 파일 기반 CRL 은 Base64 또는 바이너리 형식으로 인코딩되어야 합니다. LDAP CRL 은 바이너리 형식으로 인코딩되어야 합니다. 또한 LDAP CRL 은 다음 특성 중 하나에 CRL 데이터를 포함해야 합니다.

- certificateRevocationList;binary
- authorityRevocationList;binary

인증 기관에서는 LDAP CRL 을 게시할 때 RFC4522 및 RFC4523 에 따라 CRL 데이터를 바이너리 형식으로 반환해야 합니다. 그렇지 않으면 SiteMinder 가 CRL 데이터를 사용할 수 없습니다.

- 파일 기반 CRL 의 PEM 및 DER 인코딩 형식
- LDAP CRL 의 DER 인코딩 형식

SiteMinder 는 CRL 을 기준으로 SSL 서버 인증서의 유효성을 검사하지 않습니다. SiteMinder 웹 에이전트가 설치된 웹 서버가 SSL 서버 인증서를 관리합니다.

시스템의 각 루트 CA 마다 CRL 이 필요하지는 않습니다. 루트 CA 에 대한 CRL 이 없는 경우 해당 CA 가 서명한 모든 인증서가 트러스트된 인증서인 것으로 간주합니다.

인증서 관리를 위한 CRL 추가

CRL 을 사용하여 유효한 인증서만 PKI 기능에 사용되도록 하십시오. CRL 에 대하여 인증서의 유효성을 확인하십시오.

중요! SiteMinder 는 바이너리 인코딩에서 LDAP CRL 을 명시적으로 요청합니다. 또한 CRL 데이터를 *certificateRevocationList;binary* 또는 *authorityRevocationList;binary* 라는 LDAP 특성에 저장해야 합니다. CA(인증 기관)가 LDAP CRL 을 게시할 경우 RFC4522 및 RFC4523 에 따라 CRL 데이터를 바이너리 형식으로 반환해야 합니다. 그렇지 않으면 SiteMinder 가 CRL 데이터를 사용할 수 없습니다.

CRL 을 사용하려면 CRL 위치가 필요합니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "인프라", "X509 인증서 관리", "인증서 유효성"을 선택합니다.
3. "추가"를 클릭합니다.
"해지 목록 구성" 대화 상자가 열립니다.
4. CRL 의 별칭과 인증서 해지 목록의 위치(URL)를 지정합니다.
위치는 파일 CRL 의 파일 경로와 LDAP CRL 의 LDAP 검색 경로여야 합니다.
5. "저장"을 클릭합니다.

CRL 이 인증서 데이터 저장소에 추가됩니다.

CRL 업데이트

CRL 을 업데이트하여 사용 중인 인증서 데이터가 최신 상태인지 확인하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "인프라", "X509 인증서 관리", "인증서 유효성"을 선택합니다.
3. 목록에서 CRL 을 삭제합니다.
4. 다음 단계 중 하나를 수행하여 CRL 을 추가합니다.
 - "추가"를 클릭하여 새 CRL 파일 또는 LDAP 위치에 대한 설정을 완료합니다. "저장"을 클릭합니다.
 - 다시 "인증서 관리" 대화 상자로 돌아갑니다. 기본 "CRL 업데이트 간격" 설정에 대한 값을 지정합니다. 다음 CRL 업데이트 시점에 인증서 데이터 저장소가 자동으로 구성된 파일 또는 LDAP 위치로 가서 CRL 을 다시 로드합니다.

OCSP 를 사용하여 인증서 유효성 확인

일부 기능을 사용하려면 인증서 데이터 저장소의 인증서에 대한 인증서 유효성 검사가 필요합니다. 12.52 SP1 에서 페더레이션 기능은 인증서 데이터 저장소를 사용합니다. 이 기능에는 HTTP-아티팩트 백 채널 보호, SAML 메시지 확인 및 SAML 메시지 암호화가 포함됩니다.

인증서 데이터 저장소는 인증서의 유효성을 검사하기 위해 OCSP 서비스를 사용할 수 있습니다. OCSP 는 CA(인증 기관)가 필요 시 인증서 유효성 검사를 제공하기 위해 제공하는 HTTP 서비스를 사용합니다.

참고: 페더레이션 기능은 X.509 인증 체계와는 다른 방식으로 OCSP 사용을 구현합니다. 이 인증 체계에서는 독립 LDAP 디렉터리를 사용하여 OCSP 응답자 인증서를 저장하며, 인증서 데이터 저장소는 사용하지 않습니다.

기본적으로 인증서 데이터 저장소에서 인증서의 해지 상태는 검사되지 않습니다. OCSP 응답자를 통해 해지 상태를 확인하려면 OCSP 업데이트 유틸리티(OCSPUpdater)를 사용하십시오. OCSPUpdater 는 사용되도록 설정된 경우 구성된 OCSP 응답자에 대한 해지 상태를 5 분마다 확인합니다. 이 기본 주기는 구성할 수 있습니다.

OCSPUpdater 를 구성할 때는 다음 구성 요소를 사용합니다.

- SMocsp.conf 파일

OCSPUpdater 는 OCSP 응답자 구성에 SMocsp.conf 파일을 사용합니다. 인증서를 발급하는 각 CA(인증 기관)마다 자체 OCSP 응답자가 있습니다. SMocsp.conf 파일에서 인증서 데이터 저장소의 각 CA 인증서에 대한 모든 OCSP 응답자를 포함하십시오.

OCSPUpdater 를 사용하려면 SMocsp.conf 파일이 있어야 합니다.

참고: SMocsp.conf 파일은 X.509 인증서 인증 체계가 자체 OCSP 구현을 구성하기 위해 사용하는 것과 동일한 파일입니다.

- XPSConfig 유틸리티

XPSConfig 를 사용하면 OCSPUpdater 의 사용 여부 및 업데이트 빈도 설정과 같은 동작을 사용자 지정할 수 있습니다. 사용자 지정은 OCSPUpdater 를 실행 중인 정책 서버에 로컬로 적용됩니다. OCSPUpdater 는 배포에서 하나의 정책 서버에서만 사용되도록 설정하십시오.

OCSP 및 CRL 검사 간 장애 조치

인증서 데이터 저장소는 OCSP 에서 CRL 유효성 검사로의 장애 조치를 지원합니다. CRL 및 OCSP 검사를 구성하면 둘 사이의 장애 조치를 사용할 수 있습니다.

페더레이션 기능은 확장이 인증서에 있더라도 장애 조치가 구성된 인증서 배포 지점 확장을 지원하지 않습니다.

추가 정보:

[X.509 클라이언트 인증서 인증을 위한 인증서 신뢰성 검사](#) (페이지 447)

제 20 장: 전역 정책, 규칙 및 응답

이 섹션은 다음 항목을 포함하고 있습니다.

[전역 정책](#) (페이지 667)

[전역 정책을 구성하는 방법](#) (페이지 672)

[전역 정책을 사용하거나 사용하지 않도록 설정](#) (페이지 682)

[전역 활성 정책 구성](#) (페이지 682)

[전역 정책에 사용할 수 있는 IP 주소](#) (페이지 683)

[전역 정책 시간 제한 추가 및 제거](#) (페이지 685)

전역 정책

표준 정책은 단일 정책 도메인의 컨텍스트에서 생성됩니다. 대규모 프로덕션 환경에는 수천 개의 도메인이 포함되어 있을 수 있습니다. 이러한 환경에서는 많은 도메인에 공통적인 동작(정책이 나타내는 동작)을 정의하는 것이 유용할 수 있습니다. 표준 정책을 사용하려면 동일한 동작이 필요한 각 도메인에 대해 동일한 정책을 다시 생성해야 합니다. 전역 정책을 사용하면 정책과 관련 규칙 및 응답을 모든 도메인에 적용되는 시스템 수준 개체로 구성할 수 있습니다.

다음 용어는 전역 정책을 설명하는 데 사용됩니다.

액세스 규칙

액세스 규칙은 리소스에 대한 액세스를 허용하거나 거부합니다. 전역 정책에는 액세스 규칙이 포함되지 않습니다. 전역 정책에는 이벤트 규칙만 추가됩니다.

이벤트 규칙

이벤트 규칙은 인증 또는 권한 부여 이벤트가 발생할 때 호출됩니다. 모든 도메인에서 공통적으로 구현되는 동작은 이벤트 규칙과 연결되며 전역 정책에 포함될 수 있습니다.

전역 정책

시스템 개체로 정의되는 정책입니다.

전역 규칙

시스템 개체로 정의되는 규칙입니다.

전역 응답

시스템 개체로 정의되는 응답입니다.

정책 링크

정책 정의에 사용되는 논리적 엔터티입니다. 이 엔터티는 규칙/응답 쌍으로 구성됩니다. 정책에는 정책 링크가 하나 이상 포함될 수 있습니다.

전역 정책 개체 특성

다음 단원에서는 전역 정책 개체의 특성을 설명하고, 전역이 아닌 표준 정책 개체와 비교했을 때의 기본적인 유사점과 차이점을 간략하게 설명합니다.

표준 응답과 비교한 전역 응답

차이점

- 시스템 수준에서 정의됩니다. 시스템 수준 관리자만 전역 응답을 정의할 수 있습니다.
- 이러한 응답은 변수 기반 특성을 사용할 수 없습니다.
- 모든 전역 또는 도메인별 정책에서 사용됩니다.
- 특정 에이전트 유형과 연관됩니다.
- 이러한 응답은 응답 그룹에 추가할 수 없습니다. 전역 응답 그룹은 금지됩니다.

유사점

- 이러한 응답은 활성 식을 사용할 수 있습니다.
- 응답은 특정 정책에 지정된 경우에만 반환됩니다.

표준 규칙과 비교한 전역 규칙

차이점

- 시스템 수준에서 정의됩니다. 시스템 수준 관리자만 전역 규칙을 정의할 수 있습니다.
- 전역 규칙에 대한 필터는 특정 영역에 바인딩되지 않습니다. 전역 규칙에 대한 필터는 절대 필터입니다. 정규식은 허용됩니다.
- 특정 에이전트 또는 에이전트 그룹에 바인딩됩니다. 에이전트는 규칙이 생성될 때 명시적으로 지정됩니다.

- SiteMinder 에이전트에만 사용할 수 있습니다. RADIUS 에이전트는 인증 및 권한 부여 이벤트를 지원하지 않으므로 RADIUS 에이전트에는 전역 규칙을 연결할 수 없습니다.
- 인증 또는 권한 부여 이벤트에 대해서만 정의됩니다.
- 전역 정책에서만 사용됩니다.
- 이러한 규칙은 규칙 그룹에 추가할 수 없습니다. 전역 규칙 그룹은 존재하지 않습니다.
- 이러한 전역 정책 처리를 사용하는 모든 도메인의 리소스에 대해 실행될 수 있습니다.

표준 정책과 비교한 전역 정책

차이점

- 시스템 수준에서 정의됩니다. 시스템 수준 관리자만 전역 정책을 정의할 수 있습니다.
- 모든 사용자에게 바인딩됩니다. 전역 정책에서 특정 사용자를 포함하거나 제외할 수 없습니다.

참고: 개별 도메인에 대해 전역 정책 처리를 사용하거나 사용하지 않도록 명시적으로 설정할 수 있습니다.

- 전역 규칙, 전역 응답 및 이러한 전역 개체의 그룹을 사용해서만 정의됩니다.
- 이러한 정책은 변수 기반 특성 또는 변수 식을 사용할 수 없습니다.
- 이러한 정책은 허용/거부 액세스 규칙을 포함할 수 없습니다. 전역 정책에는 이벤트 규칙만 허용됩니다.
- 이러한 정책은 전역 정책에서 특정 리소스/영역을 포함하거나 제외할 수 없습니다. 이러한 전역 정책은 관련 도메인에서 정책에 대해 정의된 하나 이상의 규칙 필터와 일치하는 모든 리소스에 적용됩니다.
- Java 정책 관리 API 를 통해서도 지원되지 않습니다.

유사점

- 이러한 정책은 활성 식을 사용할 수 있습니다.
- 특정 에이전트와 연관됩니다. 하지만 동일 유형의 모든 에이전트를 포함하는 그룹을 생성하고 이 그룹에 전역 규칙을 바인딩할 수는 있습니다.

전역 정책이 처리될 때는 실행된 전역 규칙에 대해 정의된 응답이 다른 응답 목록에 추가됩니다. 전역 규칙은 다음과 같은 조건을 충족하는 경우에 실행됩니다.

- 액세스할 리소스가 전역 규칙에 대해 정의된 절대 리소스 필터와 일치합니다.
- 발생한 이벤트가 전역 규칙에 대해 정의된 것과 같습니다.
- 규칙에 대해 지정된 동일한 에이전트/에이전트 그룹이 리소스를 보호합니다.
- 액세스할 리소스/영역이 전역 정책 처리를 사용하는 도메인에 속합니다.

중요! 다음 조건이 충족될 때 표준 정책이 전역 정책보다 우선 적용됩니다.

- 도메인에 대해 전역 정책 처리가 활성화되어 있습니다.
- 표준 규칙 및 전역 규칙 모두가 동일한 에이전트 또는 그룹에 바인딩되어 있습니다.

추가 정보:

[도메인에 대한 전역 정책 처리가 사용되지 않도록 설정 \(페이지 554\)](#)

SiteMinder 전역 정책 개념

이 제품은 정책 기반 액세스 제어 모델을 사용합니다. 정책은 특정 리소스에 대한 사용자의 액세스 유형과 사용자가 리소스에 액세스할 때 발생하는 작업을 정의합니다. 각 표준 정책은 여러 사용자와 여러 리소스 사이를 연결합니다. 정책은 사용자, 규칙, 응답을 바인딩하여 리소스를 보호하도록 설계되었습니다. 모든 정책에서는 정책이 적용되는 사용자나 사용자 그룹을 지정해야 합니다. 사용자는 정책에 포함되거나 정책에서 제외될 수 있습니다.

표준 정책에는 규칙 또는 규칙 그룹이 하나 이상 포함되어야 합니다. 규칙은 보호되는 리소스와 규칙이 트리거되도록 유발하는 동작 유형을 결정합니다. 규칙은 문자열 기반 *리소스 필터*와 *작업*의 조합을 사용하여 정책에 포함된 리소스를 식별합니다. 필터는 *영역 필터*와 *규칙 필터*로 구성됩니다.

정책 개체에는 시스템 수준 개체와 도메인 수준 개체라는 두 가지 유형이 있습니다. 전역이 아닌 표준 정책에서는 모든 정책 개체가 특정 도메인의 컨텍스트에서 생성되어야 합니다. 그러나 전역 정책은 제품 배포 환경의 모든 도메인에 적용될 수 있는 시스템 수준 정책입니다. 시스템 수준 권한이 있는 관리자는 전역 규칙과 전역 응답이 포함된 전역 정책을 정의할 수 있습니다. 이러한 전역 정책은 모든 도메인의 모든 리소스에 적용될 수 있습니다.

전역 개체는 도메인별로 적용되는 표준 개체와 유사합니다. 전역 정책 정의에 있는 전역 개체의 역할은 도메인 관련 정책 개체와 다릅니다. 그러나 전역 도메인이나 전역 영역 개체는 없습니다.

전역 정책 처리

다음 조건을 충족할 경우 전역 정책에 포함된 모든 전역 규칙이 실행됩니다.

- 요청된 리소스가 전역 정책 처리가 사용되지 않는 도메인에 속해 있습니다.
- 요청된 리소스가 전역 규칙에 대해 정의된 절대 리소스 필터와 일치합니다. 전역 규칙에 대한 필터가 영역이 아닌 규칙에서 획득되었습니다.
- 발생하는 이벤트가 전역 규칙에 대해 정의된 것과 동일합니다.
- 동일한 에이전트 또는 그룹이 규칙에 대해 정의된 요청된 리소스를 보호합니다.

인증 또는 권한 부여 이벤트가 발생할 때마다 실행된 전역 규칙에 대해 정의된 응답이 다른 응답 목록에 추가됩니다.

전역 정책을 구성하는 방법

전역 정책은 전역 규칙 개체와 응답 특성을 포함한 전역 응답 개체로 구성됩니다. 전역 정책을 생성하는 절차는 다음과 같습니다.

1. 인증 이벤트에 대한 전역 규칙 생성 또는 권한 부여 이벤트에 대한 전역 규칙 생성
2. 전역 응답 구성
3. [전역 웹 에이전트 응답 특성 구성](#) (페이지 679)
4. [전역 정책 구성](#) (페이지 680)

중요! 동일한 리소스에 영향을 주는 전역 정책과 도메인별 정책을 모두 구성할 수 있습니다. 예를 들어 액세스 제어를 위한 도메인별 정책과 표준 응답 집합을 제공하는 전역 정책을 구성할 수 있습니다. 그러나 전역 정책이 작동하려면 도메인별 정책에 포함된 영역이 이벤트 처리를 허용하도록 구성되어 있어야 합니다.

전역 규칙

전역 규칙은 전역 정책의 일부로, 전역 정책의 처리를 트리거하는 리소스 및 이벤트를 정의합니다. 전역 규칙은 도메인별 규칙과 유사합니다. 전역 규칙은 인증 또는 권한 부여 이벤트와 연결되어야 합니다. 전역 허용/거부 액세스 규칙은 사용할 수 없습니다.

인증 이벤트에 대한 전역 규칙

인증 이벤트가 포함된 전역 규칙을 사용하여 사용자가 리소스에 액세스하기 위해 인증할 때 발생하는 동작(On-Auth 이벤트)을 제어할 수 있습니다.

참고: OnAuth 이벤트의 결과는 영역마다 다릅니다. 예를 들어 사용자가 영역 A에서 영역 B로 이동하며 영역 A에서 OnAuthAccept 헤더를 갖고 있었던 경우 영역 B에서는 이 헤더를 사용할 수 없습니다. 사용자가 다시 영역 A로 돌아가면 헤더가 다시 설정됩니다.

다음은 사용할 수 있는 On-Auth 이벤트의 목록입니다.

On-Auth-Accept

인증이 성공한 경우 발생합니다. 이 이벤트를 사용하면 인증 성공 후 사용자를 리디렉션할 수 있습니다.

On-Auth-Reject

On-Auth-Reject 규칙을 포함하는 정책에 바인딩된 사용자에게 대해 인증이 실패한 경우 발생합니다. 이 이벤트는 인증이 실패한 후 사용자를 리디렉션하는 데 사용될 수도 있습니다.

OnAuthAccept 및 OnAuthReject 이벤트는 인증 시점(사용자가 사용자 이름 및 암호를 입력할 때)과 유효성 검사 시점(사용자의 쿠키를 읽을 때)에 모두 실행됩니다. 하지만 다음과 같은 몇 가지 특수한 작업은 인증 시점에만 발생합니다.

영역 시간 만료 재정의(EnforceRealmTimeouts 가 사용되지 않는 경우)

EnforceRealmTimeouts 옵션을 지원하는 버전의 웹 에이전트가 있고 해당 옵션이 사용하도록 설정된 경우가 아니면 사용자에게 대한 유효 시간 만료 및 최대 시간 만료는 사용자가 마지막으로 인증된 영역에 대한 값으로 유지되며 사용자가 자격 증명을 다시 입력해야 하는 경우에만 변경됩니다.

리디렉션

리디렉션은 여러 가지 이유로 인증 시에만 허용되지만 가장 실용적인 점 중 하나는 OnAuth 리디렉션이 유효성 검사 시에도 허용된 경우 무한 리디렉션 루프를 매우 손쉽게 구성할 수 있다는 점입니다.

사용자 암호에 대한 액세스

암호는 SMSESSION 쿠키에 저장되지 않으므로 이 작업은 사용자가 실제로 암호를 입력할 때(인증 시)에만 사용 가능합니다.

On-Auth-Attempt

사용자가 제품에서 인식되지 않는 사용자라서 거부된 경우에 발생합니다. 예를 들어 등록되지 않은 사용자는 먼저 등록 페이지로 리디렉션될 수 있습니다.

On-Auth-Challenge

사용자 지정 챌린지-응답 인증 체계가 활성화된 경우(예: 토큰 코드) 발생합니다.

사용자가 인증되거나 거부되면 정책 서버는 해당 On-Auth 규칙과 연결된 전역 응답을 다시 요청 에이전트로 전달합니다.

추가 정보:

[전역 응답 개체](#) (페이지 678)

인증 이벤트에 대한 전역 규칙 만들기

사용자가 리소스에 액세스하기 위한 인증이 이루어질 때 수행되는 작업을 제어하기 위한 인증 이벤트에 대한 전역 규칙을 생성할 수 있습니다.

다음 단계를 수행하십시오.

1. "정책", "전역"을 차례로 클릭합니다.
2. "전역 규칙"을 클릭합니다.
3. "전역 규칙 만들기"를 클릭합니다.
4. 전역 규칙 이름을 입력합니다.
5. "영역" 및 "리소스"에서 에이전트 및 리소스 설정을 지정합니다.

참고: 동일한 리소스와 연결된 도메인 관련 규칙을 사용하여 에이전트 그룹을 지정하면 시스템 성능이 저하될 수 있습니다. 전역 규칙에 의해 생성된 리소스를 복제하는 도메인 관련 규칙을 고려하십시오. 정책 서버가 정보를 다시 요청 에이전트에 전달하기 전에 중복 응답을 자동으로 삭제하므로 에이전트에는 하나의 응답만 반환됩니다.

6. 인증 이벤트를 선택합니다.
 7. "작업" 목록에서 OnAuth 이벤트를 선택합니다.
 8. "제출"을 클릭합니다.
- 전역 규칙이 저장됩니다.

권한 부여 이벤트에 대한 전역 규칙

SiteMinder 는 SiteMinder 권한 부여 이벤트가 포함된 전역 규칙을 사용하여 사용자에게 요청한 리소스에 대한 권한이 부여되었는지 여부를 기반으로 응답을 호출할 수 있습니다. 리소스를 보호하는 규칙에 On-Access 이벤트가 포함된 경우 권한 부여 이벤트는 사용자가 인증된 후에 발생합니다. 사용자가 자신의 권한에 따라 액세스가 허용 또는 거부될 때 적절한 이벤트가 트리거됩니다.

다음은 사용할 수 있는 On-Access 이벤트의 목록입니다.

On-Access-Accept

성공적인 권한 부여의 결과로 발생합니다. 이 이벤트는 리소스에 대한 액세스 권한이 부여된 사용자를 리디렉션하는 데 사용할 수 있습니다.

On-Access-Reject

실패한 권한 부여의 결과로 발생합니다. 이 이벤트는 리소스에 대한 액세스 권한이 부여되지 않은 사용자를 리디렉션하는 데 사용할 수 있습니다.

사용자가 권한을 부여받거나 거부되면 정책 서버는 해당 On-Access 규칙과 연결된 응답을 다시 요청 에이전트로 전달합니다.

OnAccessReject 규칙에 대한 정책 고려 사항

OnAccessReject 이벤트가 포함된 전역 규칙을 생성할 때는 OnAccessReject 규칙에 의해 발생하는 특수한 상황과 전역 정책이 정책 서버에서 처리되는 방식을 고려하십시오.

OnAccessReject 규칙은 GET/POST 규칙과 동일한 정책에 있는 경우에는 실행되지 않습니다. 사용자가 인증되면 SiteMinder 는 사용자의 아이덴티티를 확인합니다. 따라서 OnAccessReject 규칙과 GET/POST 규칙이 동일한 정책에 있는 경우에는 리소스에 대한 액세스가 허용된 사용자와 OnAccessReject 이벤트에서 리디렉션되는 사용자가 동일하게 됩니다. 해당 사용자는 액세스가 허용되었으므로 거부 이벤트가 적용되지 않습니다.

이 모순을 해결하려면 OnAccessReject 규칙에 대한 별도의 정책(다른 이벤트 규칙도 포함될 수 있음)을 생성하고 이 정책을 적용할 사용자를 지정하십시오.

예를 들어 LDAP 사용자 디렉터리에서 User1 이 리소스에 액세스할 수 있어야 하고 ou=People, o=company.com 그룹의 다른 모든 사용자는 OnAccessReject 페이지로 리디렉션되어야 하는 경우, 다음 두 개의 정책이 필요합니다.

정책 1

User1 의 액세스를 허용하는 GET/POST 규칙을 포함합니다.

정책 2

OnAccessReject 규칙과 리디렉션 응답을 포함하고 ou=People, o=company.com 그룹을 지정합니다.

User1 은 권한이 부여되었으므로 User1 이 리소스에 액세스할 때는 OnAccessReject 규칙이 실행되지 않습니다. 그러나 ou=People, o=company.com 그룹에 있는 다른 모든 사용자의 경우에는 리소스에 대한 액세스 권한이 부여되지 않았으므로 OnAccessReject 규칙이 실행됩니다.

권한 부여 이벤트에 대한 전역 규칙 만들기

사용자가 리소스에 액세스하기 위한 인증이 이루어질 때 수행되는 작업을 제어하기 위한 권한 부여 이벤트에 대한 전역 규칙을 생성할 수 있습니다.

다음 단계를 수행하십시오.

1. "정책", "전역"을 차례로 클릭합니다.
2. "전역 규칙"을 클릭합니다.
3. "전역 규칙 만들기"를 클릭합니다.
4. 전역 규칙 이름을 입력합니다.
5. "영역" 및 "리소스"에서 에이전트 및 리소스 설정을 지정합니다.

참고: 동일한 리소스와 연결된 도메인 관련 규칙을 사용하여 에이전트 그룹을 지정하면 시스템 성능이 저하될 수 있습니다. 전역 규칙에 의해 생성된 리소스를 복제하는 도메인 관련 규칙을 고려하십시오. 정책 서버가 정보를 다시 요청 에이전트에 전달하기 전에 중복 응답을 자동으로 삭제하므로 에이전트에는 하나의 응답만 반환됩니다.

6. 권한 부여 이벤트를 선택합니다.
7. "작업" 목록에서 OnAccess 이벤트를 선택합니다.
8. 제출을 클릭합니다.

전역 규칙을 사용하거나 사용하지 않도록 설정

사용자가 지정된 리소스를 액세스할 때 규칙이 실행되도록 하려면 전역 규칙을 활성화하십시오. 사용자가 지정된 리소스를 액세스할 때 규칙이 실행되지 않도록 하려면 전역 규칙을 비활성화하십시오.

다음 단계를 수행하십시오.

1. 전역 규칙을 엽니다.
2. 다음 태스크 중 하나를 수행합니다.
 - "사용" 확인란을 선택하여 규칙을 활성화하십시오.
 - "사용" 확인란의 선택을 취소하여 규칙을 비활성화하십시오.
3. 제출을 클릭합니다.

규칙이 저장됩니다.

전역 규칙에 시간 제한 추가

특정 시간으로 한정하려면 전역 정책에 시간 제한을 추가하십시오. 사용자가 지정된 기간 이외에 리소스를 액세스하려고 시도하면 정책이 시행되지 않습니다.

다음 단계를 수행하십시오.

1. 전역 정책을 엽니다.
2. "시간 제한" 그룹 상자에서 "설정"을 클릭합니다.
3. 시작 날짜와 만료 날짜를 지정합니다.
4. "Hourly Restrictions"(시간별 제한) 표에서 시간 제한을 지정합니다.

참고: 각 확인란은 1 시간을 나타냅니다. 확인란을 선택하면 해당 시간 중에 규칙이 실행됩니다. 규칙은 지정된 리소스에 적용됩니다. 확인란의 선택을 취소하면 규칙이 해당 시간 중에 실행되지 않습니다. 규칙은 지정된 리소스에 적용되지 않습니다.

5. "확인"을 클릭합니다.

추가 정보:

[규칙에 시간 제한 추가](#) (페이지 582)

활성 전역 규칙 구성

외부 비즈니스 논리를 기반으로 동적 권한 부여에 대한 활성 규칙을 구성합니다. 정책 서버가 고객이 제공한 공유 라이브러리에서 함수를 호출합니다. 이 공유 라이브러리는 소프트웨어 개발 키트에서 제공되는 권한 부여 API에 지정된 인터페이스를 준수해야 합니다.

다음 단계를 수행하십시오.

1. "활성 규칙" 그룹 상자의 필드에서 라이브러리 이름, 함수 이름 및 함수 매개 변수를 지정합니다.
활성 규칙 문자열이 "활성 규칙" 필드에 표시됩니다.
2. 제출을 클릭합니다.
활성 규칙이 저장됩니다.

전역 규칙 삭제

전역 규칙을 삭제하면 사용하는 모든 전역 정책에서 규칙이 자동으로 제거됩니다. 전역 정책은 시스템에 유지됩니다. 삭제된 규칙 없이도 전역 정책이 작동하는지 확인하십시오.

모든 전역 정책에는 규칙이 하나 이상 포함되어야 합니다.

전역 응답 개체

전역 응답은 사용자에게 반환되는 특성을 정의하는 전역 정책의 일부입니다. 이러한 특성은 사용자가 전역 규칙에 지정된 인증 또는 권한 부여 이벤트를 트리거한 후에 반환됩니다.

참고: 도메인 정책에 전역 응답을 사용할 수 있습니다. 전역 응답이 반환되도록 하려면 도메인별 정책이나 전역 정책에 전역 응답을 추가해야 합니다. 정책 내에서 전역 응답은 도메인별 응답과 마찬가지로 처리됩니다.

전역 응답 구성

전역 응답을 구성하여 연결된 전역 규칙에서 인증 또는 권한 부여 이벤트가 수행된 후 반환되는 특성을 정의할 수 있습니다.

다음 단계를 수행하십시오.

1. "정책", "전역"을 차례로 클릭합니다.
2. "전역 응답"을 클릭합니다.
3. "전역 응답 만들기"를 클릭합니다.
4. 전역 응답 이름을 입력합니다.
5. 에이전트 유형 목록에서 에이전트 유형을 선택합니다.
6. 제출을 클릭합니다.

전역 응답이 저장됩니다. 이제 응답에 응답 특성을 추가할 수 있습니다.

전역 응답에 대한 응답 특성

각 SiteMinder 전역 응답에는 응답 특성이 하나 이상 포함될 수 있습니다. 응답 특성은 정책 서버가 SiteMinder 에이전트에 전달하는 정보의 일부를 식별합니다. 각 SiteMinder 에이전트 유형마다 서로 다른 응답 특성을 허용할 수 있습니다.

전역 응답 특성 유형

SiteMinder에서는 여러 응답 특성 유형을 지원합니다. 응답 특성의 유형에 따라 정책 서버가 응답 특성의 올바른 값을 찾는 위치가 결정됩니다. 전역 응답에 대해 구성할 수 있는 응답 특성의 유형은 도메인별 응답에 대해 구성할 수 있는 응답 특성의 유형과 동일합니다.

전역 웹 에이전트 응답 특성 구성

정책 서버가 SiteMinder 에이전트에 전달하는 정보의 일부를 저장하도록 응답 특성을 구성할 수 있습니다. 웹 에이전트 응답 특성은 HTTP 헤더 변수, 쿠키 변수, 다른 리소스로의 리디렉션, 텍스트 및 시간 만료 값을 지원합니다. 웹 에이전트 응답 특성 유형에 대한 자세한 내용은 [웹 에이전트 구성 안내서](#)를 참조하십시오.

참고: CA SOA Security Manager를 구매한 경우 "CA SOA Security Manager Policy Configuration Guide"(CA SOA Security Manager 정책 구성 안내서)에서 WebAgent-SAML-Session-Ticket-Variable 응답 특성 유형에 대한 정보를 찾을 수 있습니다.

다음 단계를 수행하십시오.

1. "응답 특성 만들기"를 클릭합니다.
2. 응답 특성을 선택합니다.
3. 특성 유형을 선택합니다.

"특성 필드"의 상세 정보가 지정한 특성 유형에 맞게 업데이트됩니다.

4. "특성 필드"에서 상세 정보를 입력합니다.

참고: 응답에서 사용할 수 있는 자동으로 생성된 SiteMinder 사용자 특성 목록은 [SiteMinder 생성 사용자 특성](#) (페이지 610)에 있습니다.

5. (선택 사항) "스크립트" 필드에서 특성을 편집합니다.

참고: "고급" 섹션에서 특성을 편집할 경우 "특성 설정" 섹션이 닫힙니다.

6. "캐시 값" 또는 "값 재계산 간격"을 초 단위로 지정합니다.

참고: 입력할 수 있는 최대 시간 제한은 3600 초입니다.

7. 제출을 클릭합니다.

응답 특성 만들기 태스크가 처리를 위해 제출되고 해당 응답 특성이 "응답" 페이지의 "특성 목록"에 추가됩니다.

전역 정책 개체를 구성하는 방법

전역 정책을 구성하려면 다음 절차를 완료해야 합니다.

1. 전역 정책 만들기
2. [전역 정책에 전역 규칙 추가](#) (페이지 681)
3. (선택 사항) [전역 규칙을 응답과 연결](#) (페이지 681)

전역 정책 만들기

전역 정책을 생성하여 사용자가 리소스와 상호 작용하는 방법을 정의할 수 있습니다.

다음 단계를 수행하십시오.

1. "정책", "전역"을 차례로 클릭합니다.
2. "전역 정책"을 클릭합니다.
3. "전역 정책 만들기"를 클릭합니다.
4. 전역 정책 이름을 입력합니다.
5. 전역 규칙 및 전역 응답을 추가합니다.
6. 제출을 클릭합니다.

전역 정책에 전역 규칙 추가

전역 규칙은 전역 정책에 포함된 특정 리소스를 나타냅니다. 전역 정책에 전역 규칙을 하나 이상 추가하십시오.

다음 단계를 수행하십시오.

1. "규칙" 탭을 클릭합니다.

"규칙" 그룹 상자가 열립니다.

2. "규칙 추가"를 클릭합니다.

"사용 가능한 규칙" 창이 열리고 사용 가능한 전역 규칙의 목록이 표시됩니다.

참고: 필요한 전역 규칙이 나타나지 않을 경우 "New Rule"(새 규칙)을 클릭하십시오. 이 방법으로 생성하는 규칙은 전역 정책에 추가됩니다.

3. 추가할 전역 규칙을 선택하고 "확인"을 클릭합니다.

"규칙" 그룹 상자에 선택한 규칙 및 규칙 그룹의 목록이 표시됩니다.

4. (선택 사항) 규칙을 응답 또는 응답 그룹과 연결합니다.

전역 규칙을 응답과 연결

전역 응답은 규칙이 실행될 때 발생하는 작업을 나타냅니다. 규칙이 실행되면 연결된 응답도 실행됩니다.

다음 단계를 수행하십시오.

1. 응답을 연결할 전역 규칙에 대해 "응답 추가"를 클릭합니다.

2. 응답, 응답 그룹 또는 전역 응답을 선택하고 "확인"을 클릭합니다.

참고: 필요한 응답이 없는 경우 "새 응답"을 클릭하여 응답을 생성하십시오.

전역 정책을 사용하거나 사용하지 않도록 설정

관리 UI 에서 전역 정책을 사용하거나 사용하지 않도록 설정할 수 있습니다. 기본적으로 전역 정책을 생성하면 해당 정책이 사용되도록 설정됩니다. 전역 정책에 포함된 모든 전역 규칙은 사용자가 해당 규칙에 지정된 리소스에 액세스하려고 시도할 때 실행됩니다.

전역 정책을 사용하지 않을 경우에는 정책에 포함된 규칙이 실행되지 않습니다.

다음 단계를 수행하십시오.

1. 관리 UI 에서 정책을 엽니다.
2. "사용" 확인란을 선택하거나 선택 취소합니다.
확인란을 선택하면 정책을 사용할 수 있습니다. 확인란을 선택 취소하면 정책을 사용할 수 없습니다. 해제된 정책은 실행되지 않습니다.
3. 제출을 클릭합니다.
정책이 저장됩니다.

전역 활성 정책 구성

활성 정책은 외부 비즈니스 논리를 기반으로 한 동적 권한 부여에 사용됩니다. 활성 정책은 정책 서버가 고객이 제공한 공유 라이브러리의 함수를 호출하도록 함으로써 권한 부여 결정에 포함됩니다.

이 공유 라이브러리는 소프트웨어 개발 키트와는 별도로 제공되는 권한 부여 API 에 지정된 인터페이스를 따라야 합니다.

참고: 자세한 내용은 "API Reference Guide for C"(C 용 API 참조 안내서)를 참조하십시오.

전역 정책에 대한 활성 정책을 구성하는 과정은 도메인별 정책에 대한 활성 정책을 구성하는 과정과 동일합니다.

다음 단계를 수행하십시오.

1. 전역 정책을 엽니다.
2. "고급" 그룹 상자에서 "활성 정책 편집" 확인란을 선택합니다.
활성 정책 설정이 나타납니다.

3. "라이브러리 이름" 필드에 공유 라이브러리의 이름을 입력합니다.
4. 활성 정책을 구현할 공유 라이브러리의 함수 이름을 입력합니다.
5. 제출을 클릭합니다.
정책이 저장됩니다.

전역 정책에 사용할 수 있는 IP 주소

사용자가 다음과 같은 항목에서 보호된 리소스를 액세스할 때 전역 정책이 실행되도록 구성할 수 있습니다.

- IP 주소
- 호스트 이름
- 서브넷 마스크
- IP 주소 범위

예를 들어, IP 주소의 범위를 지정하면 해당 IP 주소에서 로그인한 사용자만 보호된 리소스에 액세스할 수 있습니다.

전역 정책에 대한 단일 IP 주소 지정

단일 IP 주소를 지정하면 지정된 IP 주소에서 리소스를 액세스하는 사용자에 대해서만 전역 정책이 실행됩니다.

다음 단계를 수행하십시오.

1. 정책을 엽니다.
2. "IP 주소" 그룹 상자에서 "추가"를 클릭합니다.
3. "단일 호스트" 옵션 단추를 선택합니다.
단일 호스트와 관련된 설정이 나타납니다.
4. IP 주소를 입력한 다음 "확인"을 클릭합니다.

IP 주소 그룹 상자에 해당 IP 주소가 나타납니다.

참고: IP 주소를 모르면 "DNS 조회"를 클릭하고 정규화된 호스트 이름을 입력하여 IP 주소를 조회하십시오.

5. 제출을 클릭합니다.
정책이 저장됩니다.

전역 정책에 대한 호스트 이름 추가

호스트 이름을 지정하여 해당 호스트에서 보호되는 리소스에 액세스하는 사용자에게 대해서만 정책이 실행되도록 할 수 있습니다.

다음 단계를 수행하십시오.

1. 정책을 엽니다.
2. "IP 주소" 그룹 상자에서 "추가"를 클릭합니다.
3. "호스트 이름" 옵션 단추를 선택합니다.
호스트 이름과 관련된 설정이 나타납니다.
4. 호스트 이름을 입력한 다음 "확인"을 클릭합니다.
호스트 이름이 "IP 주소" 그룹 상자에 나타납니다.
5. 제출을 클릭합니다.
정책이 저장됩니다.

전역 정책에 대한 서브넷 마스크 추가

서브넷 마스크를 지정하여 해당 서브넷 마스크에서 보호된 리소스에 액세스하는 사용자에게 대해서만 정책이 실행되도록 할 수 있습니다.

다음 단계를 수행하십시오.

1. 정책을 엽니다.
2. "IP 주소" 그룹 상자에서 "추가"를 클릭합니다.
IP 주소 관련 설정이 나타납니다.
3. 서브넷 마스크 옵션 단추를 선택합니다.
이 서브넷 마스크와 관련된 설정이 나타납니다.
4. "IP 주소" 필드에 IP 주소를 입력합니다.
참고: IP 주소를 모르면 "DNS 조회"를 클릭하고 정규화된 호스트 이름을 입력하여 IP 주소를 조회하십시오.
5. "서브넷 마스크" 필드에 서브넷 마스크를 입력합니다.

6. "확인"을 클릭합니다.
서브넷 마스크가 "IP 주소" 그룹 상자에 나타납니다.
7. 제출을 클릭합니다.
정책이 저장됩니다.

전역 정책에 대한 IP 주소 범위 추가

IP 주소 범위를 지정하면 해당 IP 주소 범위에서 보호된 리소스를 액세스하는 사용자에게 대해서만 정책이 실행됩니다.

다음 단계를 수행하십시오.

1. 정책을 엽니다.
2. "IP 주소" 그룹 상자에서 "추가"를 클릭합니다.
IP 주소 관련 설정이 나타납니다.
3. "범위" 옵션 단추를 선택합니다.
IP 주소 범위 관련 설정이 나타납니다.
4. "시작" 필드에 시작 IP 주소를 입력합니다.
참고: IP 주소를 모르면 "DNS 조회"를 클릭하고 정규화된 호스트 이름을 입력하여 IP 주소를 조회하십시오.
5. "끝" 필드에 끝 IP 주소를 입력합니다.
6. "확인"을 클릭합니다.
"IP 주소" 그룹 상자에 IP 주소 범위가 나타납니다.
7. 제출을 클릭합니다.
정책이 저장됩니다.

전역 정책 시간 제한 추가 및 제거

전역 정책에 시간 제한을 추가할 수 있습니다. 시간 제한을 추가할 경우 해당 제한 시간에 지정된 기간 동안에만 전역 정책이 실행됩니다. 제한 시간으로 지정된 기간이 지나면 사용자가 정책과 연결된 리소스에 액세스하려고 할 때 전역 정책이 실행되지 않습니다.

참고: 시간 제한은 정책 서버가 설치된 서버의 시스템 클럭을 기준으로 합니다.

다음 단계를 수행하십시오.

1. 정책을 엽니다.
2. "시간" 그룹 상자에서 "설정"을 클릭합니다.

"시간 제한" 창이 나타납니다.

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

3. 시작 날짜와 만료 날짜를 지정합니다.
4. "Hourly Restrictions"(시간별 제한) 표에서 시간 제한을 지정합니다.

참고: 각 확인란은 1 시간을 나타냅니다. 확인란을 선택하면 해당 시간 동안 규칙이 실행되고 지정된 리소스에 규칙이 적용됩니다. 확인란의 선택을 취소하면 해당 시간 동안 규칙이 실행되지 않고 지정된 리소스에 규칙이 적용되지 않습니다.

5. "확인"을 클릭합니다.
시간 제한이 저장됩니다.

제 21 장: 가장

가장은 권한 있는 사용자가 다음과 같은 작업을 수행할 수 있는 방법을 제공합니다.

- 권한 있는 사용자의 세션을 중지하지 않고 다른 사용자의 역할을 수행합니다.
- 임시로 다른 사용자의 아이덴티티를 사용합니다.

사용자는 다른 사용자로 가장할 때 현재 사용자 암호를 제공할 필요가 없습니다.

다음 용어는 가장을 설명하는 데 사용됩니다.

가장된 세션

다른 사용자의 아이덴티티를 가장할 목적으로 생성되는 사용자 세션입니다.

가장 대상

권한 있는 사용자가 아이덴티티를 사용하는 대상 사용자입니다.

가장 주체

다른 사용자의 아이덴티티를 가장할 수 있는 권한 있는 사용자입니다.

가장 인증 체계

권한 있는 사용자가 가장 주체의 아이덴티티를 유지하면서 다른 사용자의 아이덴티티를 가장할 수 있게 해 주는 사용자 인증 방법입니다.

세션

사용자 세션이라고도 합니다. 이 용어는 인증 후부터 로그아웃할 때까지의 시간을 나타냅니다.

세션 사양

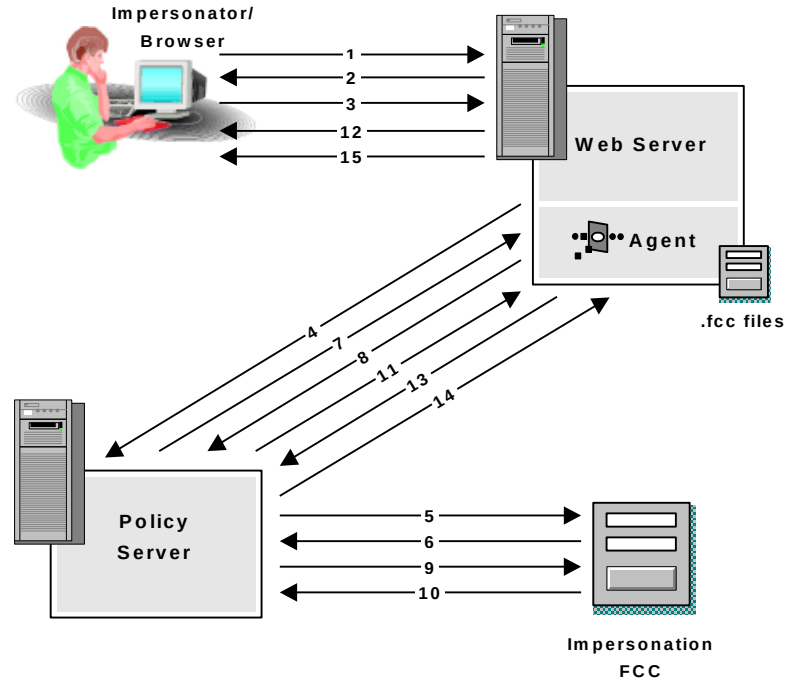
세션 사양은 또한 세션 티켓 또는 세션 사양이라고도 부릅니다. 세션 사양은 고유한 형식으로 구성된 정보로서 사용자와 현재 세션의 성격을 설명합니다.

SMSESSION

정책 서버의 세션 사양을 포함하는 웹 에이전트 쿠키의 이름입니다.

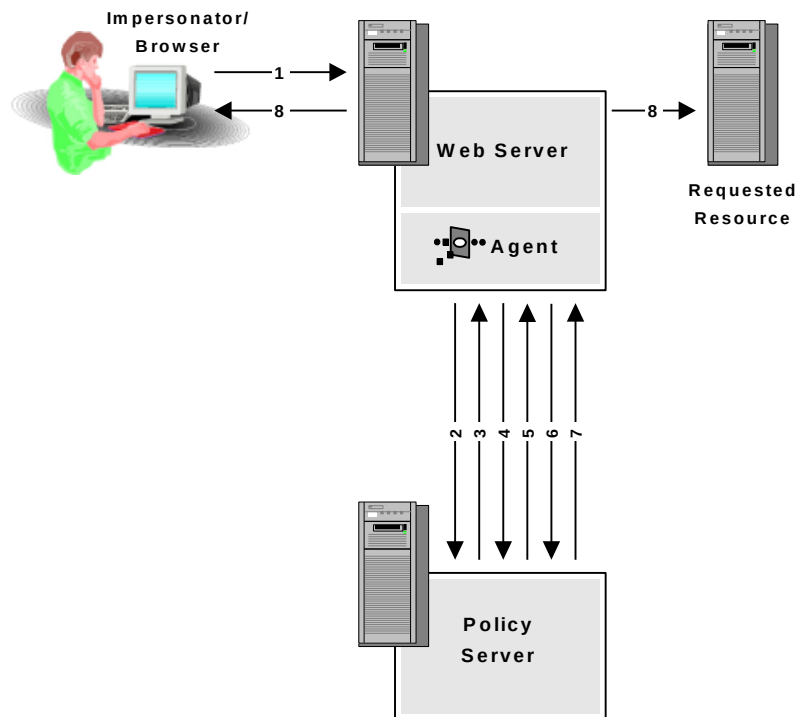
가장 세션이 시작되는 방법

다음 그림은 권한 있는 사용자가 가장 세션을 시작하는 방법을 프로세스별로 설명합니다.



1. 이전에 인증된 가장 주체가 가장 .fcc 파일에 액세스하여 사용자를 가장하려고 시도합니다.
2. .fcc가 보호되지 않거나 CSR의 액세스가 허용되지 않습니다(결정 내용은 표시되지 않음). 웹 에이전트는 단계에서 요구된 양식(.fcc)을 제공합니다. FCC에는 가장 인증 체계에 의해 보호되는 영역에 있는 대상을 나타내도록 구성된 숨은 양식 필드가 있습니다.
3. 가장 주체는 가장될 사용자의 이름을 나타냅니다.
4. 웹 에이전트는 .fcc의 대상 필드를 사용하여 영역을 파악합니다.
5. 정책 서버는 가장 인증 체계에서 필요한 자격 증명을 결정합니다.
6. 필요한 자격 증명이 반환됩니다.
7. 정책 서버는 .fcc 대상을 보호하기 위해 사용 중인 영역을 나타냅니다.
8. 웹 에이전트는 가장 주체의 세션 사양을 암호로서 사용하여 가장된 사용자를 인증합니다.

9. 가장 인증 체계의 기능이 제공된 자격 증명(가장 대상 이름 및 가장 주체의 세션 사양)을 보유한 사용자를 인증하기 위해 호출됩니다. 가장 주체의 세션 사양의 유효성이 검사됩니다. 정책 서버는 사용자를 명확히 하고 가장 세션을 인증합니다.
10. 정책 서버가 `ImpersonateStart` 이벤트에 연결된 이벤트 정책이 있음을 확인합니다. 가장 주체에 적용되는 정책이 있는 경우 가장 대상에 적용되는 정책에 바인딩된 `ImpersonateStartUser` 이벤트가 있는지 파악하기 위해 유사한 검사가 수행됩니다. 응답은 두 정책 중 하나의 규칙에 연결될 수 있습니다.
11. 가장 주체가 가장 인증 체계를 사용하여 인증된 후에는 이제 임의 응용 프로그램에서 사용자를 가장하려고 시도할 수 있습니다.
참고: 가장 주체가 어떠한 리소스에도 액세스하지 않았으므로 가장이 수행되지 않았습니다.
세션 사양이 웹 에이전트로 반환됩니다. 여기에는 가장 대상의 `DN` 및 가장 주체의 `DN`, 그리고 가장 주체와 가장 대상이 모두 있는 디렉터리가 포함됩니다.
웹 에이전트가 기존 `SMSESSION` 을 `SMSESSION` 으로 이동시키고 `FFC` 의 `@pushsession` 지시문으로 인해 새 `SMSESSION` 쿠키를 새 세션 사양과 동일하게 설정합니다.
12. 웹 에이전트가 가장 대상이 `.fcc` 대상 리소스에 대해 권한이 있는지 여부를 파악합니다.
13. 정책 서버가 가장 대상이 `.fcc` 대상 리소스에 대해 권한이 있음을 나타냅니다.
14. 가장 주체가 가장 `.fcc` 에 지정된 리소스에 액세스합니다. 예를 들어, 이것은 가장 주체 및 가장 대상의 `DN` 을 나타내는 `.jsp` 페이지일 수 있습니다.



1. 가장 주체(이제 사용자를 가장하고 있음)가 새 응용 프로그램으로 이동합니다.
2. 에이전트가 정책 서버를 호출하여 해당 리소스가 보호되는지 확인합니다.
3. 가장 주체가 요청된 리소스에 액세스합니다.
4. 리소스가 보호되어 있고 가장 주체의 웹 브라우저에 이 쿠키 도메인에 대한 **SMSESSION** 쿠키가 있으므로 웹 에이전트는 정책 서버를 호출하여 세션 사양의 유효성을 검사합니다.
5. 세션 사양이 현재 인증 로직에 따라 유효성 검사되는 동시에, 유효성 검사 로직이 세션 사양의 콘텐츠로 인해 가장이 발생한다고 파악할 수 있으므로 가장 주체 및 사용자에게 대한 추가 검사가 수행됩니다. 가장 주체는 **ImpersonateStart** 이벤트에 대한 규칙이 있는 현재 영역의 이벤트 정책에 바인딩되어야 합니다. 사용자는 가장될 수 있는 사용자에게 적용되는 **ImpersonateStartUser** 이벤트에 대한 유사한 정책에 바인딩되어야 합니다.
6. 웹 에이전트는 사용자가 리소스에 대해 권한 부여된 경우 정책 서버를 묻습니다.

7. 정책 서버는 인증 응답으로 응답합니다. 인증 응답이 액세스가 허용되었거나 여러 이유(이 리소스에 대한 규칙이 호출되지 않았거나, 해당 사용자에게 액세스가 명시적으로 거부되었거나, 인증 수준이 너무 낮거나, 세션이 만료된 경우 등등)로 인해 액세스가 거부되었음을 나타낼 수 있습니다. 이러한 모든 액세스 거부 이유는 사용자 경험을 반영합니다. 하지만 보호 수준은 가장된 세션에 대해 적용되지 않습니다.
8. 요청된 리소스가 반환됩니다.

가장에 대한 보안 고려 사항

가장 주체의 세션 사양은 임의 고객의 세션 사양과 같이 처리됩니다. 주요 차이점은 가장 주체의 고유 이름과 가장 주체가 원래 인증된 사용자 디렉터리가 추가 필드로 제공된다는 점입니다. 추가 필드는 다음을 수행합니다.

- 가장된 모든 리소스 액세스가 추가 확인을 통해 전달되도록 합니다.
- 정책 서버가 감사를 위해 가장된 활동을 기록합니다.

가장된 세션 사양은 가장 체인을 방지하는 데도 사용됩니다. 정책 서버는 가장 주체 DN 및 사용자 디렉터리의 필드가 사용 중인 것으로 확인될 추가 가장을 허용하지 않고 로그인 시도를 거부합니다. 따라서 여러 가장 주체가 동시에 같은 가장 대상을 가장하여 제한된 리소스에 액세스할 수 없게 됩니다.

인증 체계 보호 수준의 효과

가장 주체가 원래 인증된 보호 수준은 가장 중에 확인되지 않습니다. 일반적으로는 더 높은 수준에서 인증 체계가 보호하는 새 영역의 리소스에 액세스할 때 사용자에게 새 자격 증명이 요청됩니다. 그러나 가장 주체는 권한 있는 사용자이므로 가장 세션 중에는 이러한 유형의 요청이 발생하지 않습니다. 보호 수준은 영역의 리소스에 액세스하는 데 사용되는 자격 증명의 강도를 나타내기 위한 것입니다. 가장 중에 가장되는 사용자에게 고유한 자격 증명은 없습니다. 따라서 가장 수준은 고려되지 않습니다.

참고: 가장된 세션이 종료되면 보호 수준이 정상적으로 적용됩니다.

세션 유희 시간 만료

가장된 세션 도중 가장 주체의 원래 세션이 만료될 수 있습니다. 이는 가장 주체가 원래 인증되었던 영역의 유희 시간 만료 값에 따라 결정됩니다. 가장 주체가 원래 유희 시간 만료 값을 초과하면 가장 세션이 가장 주체의 원래 세션과 함께 종료됩니다. 이 문제를 방지하려면 가장 주체가 일반적으로 인증되는 영역의 세션 유희 만료 시간을 늘리십시오.

가장 제한

가장을 수행하려면 가장 주체 및 가장 대상이 가장 영역의 정책에 바인딩되어야 합니다. 가장 주체 정책은 `ImpersonateStart` 이벤트에 대해 호출되는 규칙이 있어야 하며, 가장 대상 정책은 `ImpersoanteStartUser` 이벤트에 대해 호출되어야 합니다.

가장 영역 및 이벤트

가장은 가장 프로세스를 시작하도록 구성된 영역에서 시작됩니다. 가장 주체가 가장 영역의 리소스를 요청하면 가장 주체가 가장 인증 체계의 인증을 받게 됩니다. 체계는 가장 주체에게 양식을 통해 자격 증명을 요구합니다. 일반적인 사용자 이름과 암호를 요구하지 않고, 대신 양식은 가장 주체가 가장 대상의 사용자 이름을 제공할 것을 요청합니다. 양식의 FCC 파일 내에는 암호를 가장 주체의 현재 세션 사양으로 설정하는 로직이 있습니다.

정책 서버는 가장 인증 체계를 사용하여 가장 주체의 현재 세션이 유효한지 확인합니다. 그런 다음 정책 서버는 가장 영역과 관련된 정책 도메인에 포함된 디렉터리에서 가장될 사용자를 찾으려고 시도합니다. 정책 서버가 사용자를 찾으면 인증이 진행됩니다.

정책 서버가 디렉터리에서 가장을 찾으면 해당 가장 주체가 가장할 권한이 있는지, 그리고 가장 대상이 가장될 수 있는지 여부를 확인합니다. 이러한 권한은 정책, 규칙 및 두 가장 이벤트를 사용하여 구성 및 시행됩니다.

가장 이벤트는 인증 및 권한 부여 이벤트와 유사하지만 피동적으로 호출되지 않습니다. 정책은 가장 주체와 가장 대상을 모두 가장 주체 이벤트 규칙에 명시적으로 바인딩해야 합니다. 정책이 없거나 해당 가장 주체 및 가장 대상에 대한 가장 주체 이벤트 규칙을 포함하지 않는 경우 가장은 허용되지 않습니다.

가장은 가장 이벤트에 대한 정책 및 규칙을 사용하여 임의 영역에서 허용 또는 허용되지 않을 수 있습니다. 영역은 모든 가장을 허용하지 않거나 가능한 가장 주체 및 가장 대상을 제한하도록 구성될 수 있습니다.

가장 구성

엔터프라이즈에서 가장을 구현하려면 여러 정책 서버 개체를 구성해야 합니다. 여러 개체를 조합하면 한 사용자가 다른 사용자로 가장(impersonate)하는 데 필요한 인증 및 정책 권한을 제공할 수 있습니다. 가장을 위해서는 다음 개체가 필요합니다.

인프라 개체:

에이전트

가장에는 웹 에이전트 및 관련 정책 서버 에이전트 개체가 필요합니다.

참고: 가장을 구현하려면 배포에 하나 이상의 웹 에이전트가 설치되어 있어야 합니다.

인증 체계

가장은 가장 템플릿에 기반한 인증 체계 개체가 필요합니다.

사용자 디렉터리

가장은 가장 주체(Impersonator)와 가장 대상(Impersonatee)을 포함한 사용자 저장소를 가리키는 하나 이상의 사용자 디렉터리 개체가 필요합니다. 특성 값 또는 그룹 구성원 자격으로 인해 두 사용자는 고유해야 합니다.

도메인

가장은 사용자 디렉터리 개체를 포함하는 정책 도메인 개체가 필요합니다.

도메인 개체:

영역

가장은 최소 두 개의 구성된 영역 개체가 필요합니다. 하나의 영역은 가장 대상이 액세스할 수 있는 리소스를 포함합니다. 다른 영역은 가장 영역이며, 가장 세션을 초기화하는 데 필요한 리소스 및 규칙을 포함합니다.

규칙

가장은 액세스 제어 규칙이 필요합니다. 또한, 가장 주체가 가장 세션을 시작하기 위해 `ImpersonateStart` 이벤트를 사용한 규칙이 있어야 합니다. 사용자가 가장될 수 있도록 `ImpersonateStartUser` 이벤트를 사용한 규칙이 있어야 합니다.

정책

리소스를 보호하는 정책에 추가하여, 가장은 가장 영역에서 리소스에 대한 액세스를 허용하기 위해 추가 정책이 필요합니다. 이러한 정책은 사용자를 가장 주체로서 인식하고 가장 대상 수를 제한합니다.

startimp.fcc 를 사용하도록 에이전트 구성

가장 세션을 호출하려면 FCC 파일(샘플 `startimp.fcc` 등)이 가장 인증 체계에 지정되어야 하고 웹 에이전트에 의해 처리되어야 합니다. 기본적으로 웹 에이전트는 `.fcc` 파일 확장명을 사용하는 파일을 보호하지 않습니다.

웹 에이전트가 가장 세션의 초기화를 허용하려면 다음 두 개 옵션 중 하나가 필요합니다.

- `.fcc` 확장명이 무시되지 않도록 웹 에이전트가 구성되어야 합니다.
- 가장을 호출하기 위해 사용된 `.fcc` 파일은 다른 (무시되지 않는) 파일 확장명(예: `.ifcc`)을 사용해야 합니다.

가장 인증 체계 구성

가장은 가장 인증 체계를 필요로 합니다. 이 체계는 가장 주체가 가장 프로세스를 시작하기 위한 방법으로서 사용됩니다. 가장 세션을 시작하기 위해 가장 주체는 가장 인증 체계가 보호하는 리소스인 `.fcc` 파일을 직접 액세스합니다.

추가 정보:

[가장 인증 체계](#) (페이지 435)

.fcc 파일을 통한 가장 활성화

가장에 있어 중요한 사항은 인증 프로세스가 적절한 인증 체계 및 .fcc 파일을 사용하는 것입니다. 가장 인증 체계를 활성화하는 .fcc 파일은 웹 에이전트를 통해 설치됩니다. 이 파일은 .fcc 확장명으로 끝나야 합니다. 이 확장명을 사용하는 파일은 웹 에이전트에 의한 특별 처리의 이점을 누릴 수 있습니다. 가장 인증 체계는 HTML 양식 인증 체계와 유사합니다.

가장 주체는 체계에 대한 .fcc 파일을 직접 액세스하여 가장 인증 체계를 호출할 수 있습니다. 적절한 인증 체계는 .fcc 파일의 대상 매개 변수를 통해 호출됩니다. 이 값은 @target 지시문으로 사용하거나 대상(숨은 양식 게시 변수)을 적절한 웹 페이지로 설정하여 .fcc 파일에 하드 코드될 수 있습니다.

참고: 대상 리소스는 반드시 가장 인증 체계가 보호하는 영역에 있어야 합니다.

가장을 위한 .fcc 요구 사항

가장 프로세스를 시작하는 FCC 는 또한 @smpushsession=true 지시문으로 포함해야 합니다. 이 지시문은 세션 쿠키가 가장된 사용자의 세션 사양을 보유할 수 있도록 다른 쿠키에 현재 세션 쿠키 콘텐츠를 저장하도록 웹 에이전트에게 지시합니다.

인증이 수행되기 위해서는 가장 인증 체계를 처리하는 웹 에이전트에 적절한 자격 증명이 있어야 합니다. 사용자 이름은 가장되는 사용자의 사용자 이름입니다. 암호는 가장 주체의 세션 사양으로 설정되어야 하며, 필요한 경우 추가 특성을 앞에 추가해야 합니다. 양식이 게시될 때 쿠키 또는 헤더의 콘텐츠를 지시문으로 대체하는 FCC 의 기능이 이 용도로 사용됩니다. 이 기능을 사용하여 FCC 는 @password 지시문을 필요한 경우 다른 데이터와 함께 사용자 세션 사양으로 설정합니다.

가장 프로세스를 끝내기 위해 가장 인증 체계에 의해 보호되는 영역에 또 다른 .fcc 파일이 포함될 수 있습니다. 이 .fcc 파일은 가장 프로세스를 시작하는 데 사용된 제한된 영역의 리소스를 가리키도록 @target 지시문을 설정해야 합니다. 또한, @smredirect 지시문은 인증 프로세스를 중단시키기 위해 동일한 리소스로 설정되어야 합니다. 마지막으로, 원래 세션 쿠키를 복원하기 위해 @smpopsession=true 지시문이 사용되어야 합니다.

가장을 위한 FCC 지시문

가장을 위한 .fcc 파일을 만들 때는 파일에 다음 지시문이 사용되어야 합니다.

@logout

이 지시문은 SiteMinder 에서 사용자를 로그아웃시키고 SMSESSION 쿠키를 제거합니다.

@smheaders

이 지시문은 FCC 네임스페이스에 HTTP 요청 헤더를 추가합니다. 가장을 위해 이 지시문은 암호로서 사용할 수 있도록 세션 사양 헤더 SMSERVERSESSIONSPEC(또는 SM_SERVERSESSIONSPEC. SMSERVERSESSIONSPEC 및 LegacyVariables 에 대한 설명 참조)의 콘텐츠를 FCC 네임스페이스에 제공합니다.

@smpushsession

이 지시문은 사용자가 다른 사용자로 “가장”한 다음 원래 세션으로 돌아가도록 허용합니다. 이 지시문은 "true"로 설정되어야 합니다.

@smpopsession

이 지시문은 @smpushsession 이 사용된 이후에 원래 세션으로 돌아갑니다. 이 설정은 "true"로 설정되어야 합니다.

@smredirect

이 지시문은 요청을 지정된 대상으로 리디렉션합니다.

@target

이 지시문은 URL 처리 후 어디로 리디렉션할지를 FCC 에게 알려 줍니다.

@password

이 지시문은 정책 서버로 전달할 암호의 콘텐츠를 지정합니다.

@smaltcreds

사용자 지정 인증 체계가 4KB 보다 큰 자격 증명을 보내도록 허용합니다. 이것은 @password 지시문이 사용된 것과 동일한 방식으로 사용될 수 있습니다. @smaltcreds 를 사용하여 자격 증명에 FCC 에 게시된 경우 그 값은 4k 바이트로 제한된 암호 필드를 피하여 바이트 버퍼로서 로그인 중에 정책 서버로 전달됩니다. @smaltcreds 지시문은 기존 인증 체계와 함께 사용할 수 없지만 사용자 지정 인증에 대해서는 사용할 수 있습니다. 사용자 지정 인증 체계의 개발자들은 로그인 중에 에이전트 API 를 통해 전달된 사용자 자격 증명 구조의 IpszCertBinary 필드에서 @smaltcreds 자격 증명을 찾는 인증 체계 라이브러리를 코딩해야 합니다.

@username

이 지시문은 정책 서버로 전달할 사용자 이름을 지정합니다.

% 및 \$ 대체 기능

"%" 및 "\$\$" 기능은 Perl 의 스칼라 변수와 유사한 데이터 대체에 사용됩니다. "%NAME%"는 POST 에서 "NAME"과 관련된 데이터로 "NAME"을 대체하는 데 사용됩니다. "\$\$NAME\$\$"는 GET 에서 "NAME"과 관련된 데이터로 "NAME"을 대체하는 데 사용됩니다.

FCC 를 사용한 세션 사양 획득

웹 에이전트는 일련의 헤더에 세션 사양을 저장하여 모든 요청에서 이 사양을 포함시킵니다. 세션 사양 헤더는 여러 FCC 지시문을 사용하여 암호로서 제출될 수 있습니다. @smheaders 지시문은 FCC 의 네임스페이스에 SMSERVERSESSIONSPEC 헤더를 포함하기 위해 사용됩니다. @password 지시문은 SMSERVERSESSIONSPEC 헤더의 콘텐츠에 암호를 설정하기 위해 사용됩니다.

SM_SERVERSESSIONSPEC/SMSERVERSESSION 헤더는 DisableSessionVars 가 웹 에이전트 구성 파일에서 기본값인 false 로 설정된 경우에만 사용할 수 있습니다.

참고: LegacyVariables 웹 에이전트 매개 변수가 Yes 로 설정되면 헤더는 SM_SERVERSESSIONSPEC 가 됩니다. **참고:** LegacyVariables 웹 에이전트 매개 변수가 No 로 설정되면 헤더는 SMSERVERSESSIONSPEC 가 됩니다. LegacyVariables 매개 변수는 IIS 6.0 웹 서버의 웹 에이전트에 대해 지원되지 않습니다. IIS 6.0 의 웹 에이전트의 경우 SMSERVERSESSIONSPEC 가 항상 올바른 헤더입니다.

가장을 위한 예제 .fcc 파일

다음 .fcc 파일은 가장 프로세스를 시작하기 위해 가장 주체에 의해 직접 호출되거나 가장 인증 체계에 의해 호출됩니다.

```
@username=%USER%
@smheaders=%SMSERVERSESSIONSPEC%
@password=%SMSERVERSESSIONSPEC%
@smpushsession=true

<html>
<head><title>Sample Impersonation Form</title></head>
<body>
<h3> Please enter your Impersonation Information</h3>
<form method=post><table>
<tr>
<td>User Name:</td>
<td><input type=text name=USER></td>
</tr>
<tr>
<td><input type=hidden name=target value="server.example.com/app/
impersonatee/successimp.htm ">
<td><input type=submit></td></tr>
</table></form></body>
</html>
```

다음 .fcc 파일은 원래 세션으로 돌아가기 위해 가장 주체에 의해 호출됩니다.

```
@smpopsession=true
@target=/impersonators/end.htm
@smredirect=/impersonators/end.htm
```

FCCCompatMode 의 영향

기존 웹 에이전트가 fcccompatmode 를 기본적으로 yes 로 설정하지만 프레임워크 웹 에이전트는 fcccompatmode 를 no 로 설정합니다. 이 모드가 yes 로 설정되면 웹 에이전트는 가장 요청을 처리할 수 있습니다. 하지만 모드가 no 로 설정된 경우 웹 에이전트가 가장 요청을 처리하려면 다음 두 개의 요구 사항이 충족되어야 합니다.

- 웹 에이전트 구성 매개 변수 EncryptAgentName 이 false 로 설정되어야 합니다.
- 웹 에이전트 구성 매개 변수 AgentName 이 가장을 시작하는 fcc 파일에 코딩되거나 가장 세션이 시작되었을 때 에이전트로 전달된 쿼리 데이터에 코딩되어야 합니다.

가장 이벤트 구성

가장 이벤트는 권한 있는 사용자가 다른 사용자로 가장할 수 있도록 허용하기 위해 구성되어 정책에 포함되어야 하는 규칙 이벤트입니다.

가장을 사용하려면 다음 각각의 가장 이벤트 중 최소 하나 이상을 구성해야 합니다.

ImpersonateStart

적절한 정책에 포함된 경우 이 이벤트가 포함된 규칙은 가장 세션이 시작될 수 있도록 합니다.

ImpersonateStartUser

적절한 정책에 포함된 경우 이 이벤트가 포함된 규칙은 사용자 집합을 가장할 수 있도록 합니다.

가장에 대한 정책 구성

가장이 올바르게 기능하도록 하려면 여러 정책을 구성해야 합니다.

가장을 시작하는 리소스에 대해 다음 항목이 필요합니다.

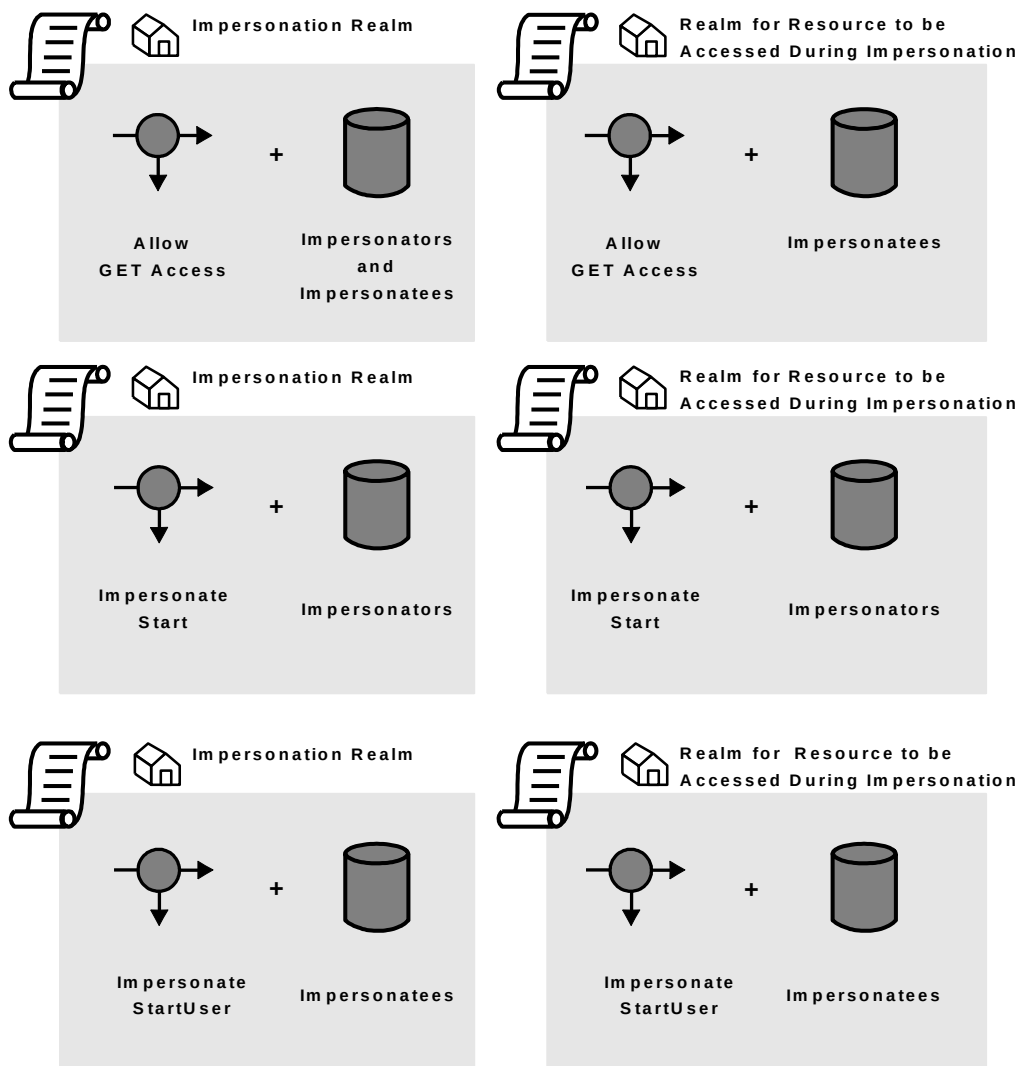
- 가장 주체 및 가장 대상 모두에 대한 액세스 제어 정책 예: 가장 주체 및 가장 대상 모두에 대한 GET 액세스 규칙을 포함하는 정책
- ImpersonationStart 규칙 및 가장 주체를 포함하는 가장 정책
- ImpersonationStartUser 규칙 및 가장 대상을 포함하는 가장 정책

가장 주체가 리소스에 액세스하려면 다음 항목이 필요합니다.

- 가장 대상에 대한 액세스 제어 정책 예: 가장 대상에 대한 GET 액세스 규칙을 포함하는 정책
- ImpersonationStart 규칙 및 가장 주체를 포함하는 가장 정책
- ImpersonationStartUser 규칙 및 가장 대상을 포함하는 가장 정책

참고: 가장 주체가 액세스할 수 있는 각 리소스에 대해 정책이 있어야 합니다.

다음 그림은 가장 주체가 리소스에 액세스하기 위해 필요한 최소 정책을 보여 줍니다:



추가 정보:

[정책](#) (페이지 621)

다중 쿠키 도메인 지원

사이트가 여러 쿠키 도메인으로 구성된 경우 서로 다른 쿠키 도메인에 있는 리소스 사이에서 이동할 때 가장 주체의 아이덴티티가 혼동될 수 있습니다. 이 문제를 해결하기 위해 현재 사용 중인 것을 제외하고 모든 쿠키 도메인에서 **SMSESSION** 쿠키가 삭제되어야 합니다. 이 작업은 가장을 시작하고 끝내는 데 사용되는 양식을 수정하는 방법으로 수행되어야 합니다. 이러한 양식은 현재 사용 중인 것을 제외하고 모든 쿠키 도메인에서 **SMSESSION** 쿠키를 삭제하기 위해 서버 쪽 코드를 호출하는 HTML 또는 스크립트가 추가되어야 합니다.

예를 들어, `yourcompany.com`, `subsidiaryA.com`, `subsidiaryB.com` 에 설치된 웹 에이전트를 가정합니다. 가장을 수행하는 웹 에이전트는 `yourcompany.com` 도메인에 있을 수 있습니다. 가장을 시작 및 끝내는 .fcc 파일은 가장이 올바르게 기능하도록 쿠키 도메인에서 **SMSESSION** 쿠키를 삭제하기 위해 `subsidiaryA.com` 및 `subsidiaryB.com` 에서 서버 쪽 기능(예: JSP 페이지)을 호출해야 합니다.

가장의 샘플 구현

이 섹션에서는 간단한 가장 구현에 대해 설명합니다. 가장을 구현하기 위해 필요한 최소 정책 서버 개체는 다음과 같습니다.

인프라 개체:

에이전트

가장에는 웹 에이전트 및 관련 정책 서버 에이전트 개체가 필요합니다.

참고: 가장을 구현하려면 배포에 하나 이상의 SiteMinder 웹 에이전트가 설치되어 있어야 합니다. 웹 에이전트 설치에 대한 자세한 내용은 *웹 에이전트 설치 안내서*를 참조하십시오.

인증 체계

가장 인증 체계 템플릿에 기반한 가장 인증 체계가 필요합니다. 이 섹션에서 정의된 샘플의 경우 인증 체계의 이름은 "Impersonation Auth"입니다.

사용자 디렉터리

가장은 가장 주체(Impersonator)와 가장 대상(Impersonatee)을 포함한 사용자 저장소를 가리키는 하나 이상의 사용자 디렉터리 개체가 필요합니다. 특성 값 또는 그룹 구성원 자격으로 인해 두 사용자는 고유해야 합니다.

도메인

정책 도메인이 필요합니다. 이 섹션에서 정의된 샘플의 경우 정책 도메인의 이름은 "Impersonation Domain"입니다.

도메인 개체:

영역

이 섹션에서 설명된 샘플의 경우 "Impersonation" 및 "App1"의 두 개의 영역이 필요합니다. "Impersonation" 영역은 "Impersonation Auth" 인증 체계를 사용해야 합니다. "App1" 영역은 임의의 인증 체계를 사용할 수 있습니다.

규칙

이 섹션에서 설명된 샘플의 경우 "Get" 작업에 대해 모든 리소스의 액세스를 허용하는 "Impersonation" 영역에서 규칙을 구성해야 합니다. 즉, 규칙에 대한 "리소스" 필드에 별표를 입력해야 합니다. 또한 가장 이벤트에 대한 규칙도 구성해야 합니다. 한 규칙은 가장 주체가 해당 정책에 포함된 경우 가장을 허용하고, 다른 규칙은 다른 해당 규칙에 포함된 경우 가장 대상이 가장되도록 허용합니다.

규칙

"Impersonation" 영역에 있는 것과 유사한 규칙 집합을 "App1" 영역에 만들어야 합니다.

정책

이 섹션에서 설명된 샘플의 경우 6 개의 정책이 필요합니다. "Impersonation" 영역에 있는 각 규칙에 대해 한 정책이 정의되어야 하고, "App1" 영역에 있는 각 규칙에 대해 또 다른 한 정책이 정의되어야 합니다.

샘플 가장 구현 평가

모든 필요한 정책 서버 개체가 갖춰지면 관리자가 다음을 수행하여 가장 세션을 시작합니다.

1. 가장 주체가 될 관리자가 보호된 네트워크에 로그인합니다.
2. 관리자가 자격 증명을 제공하고 인증 및 권한 부여됩니다.
3. 관리자가 웹 브라우저를 사용하여 `imp.fcc` 파일에 액세스합니다.
4. 관리자가 가장될 사람의 사용자 ID 를 입력하도록 요청받습니다.
관리자가 또한 가장될 사용자에게 대한 추가 정보를 제공하도록 요청받을 수 있습니다.
5. 관리자가 정보를 제출합니다.
6. 정책 서버가 다음을 파악하기 위해 가장에 대해 정의된 정책을 사용합니다.
 - 해당 관리자가 가장 주체로 작업하도록 허용되었는지 여부
 - 해당 사용자가 가장될 수 있는지 여부
7. 둘 모두 허용되면 가장 주체가 가장 대상으로 가장합니다.

참고: 사용자 지정 배포(.jsp 페이지, 서블릿 등) 없이 가장 세션은 감사 로깅을 사용하여 추적할 수 있습니다. 하지만 기업이 일부 사용자 지정 웹 응용 프로그램을 만들어 가장 세션을 모니터링하고 추적하면 추가적인 이점이 있을 수 있습니다.

가장 프로세스를 시작하기 위한 양식

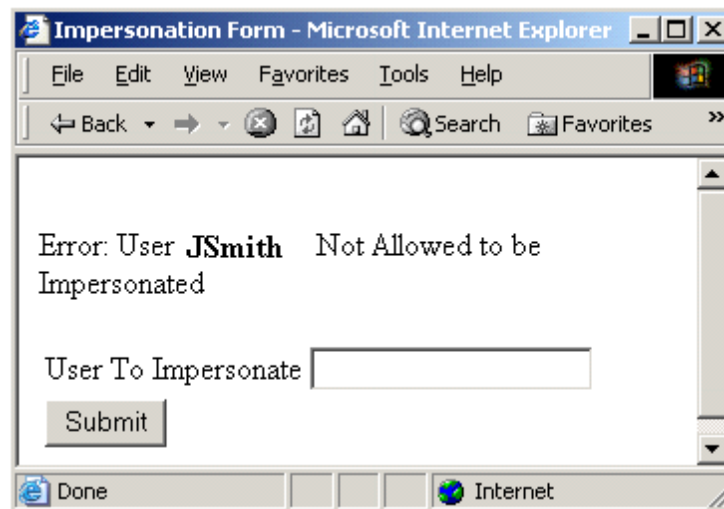
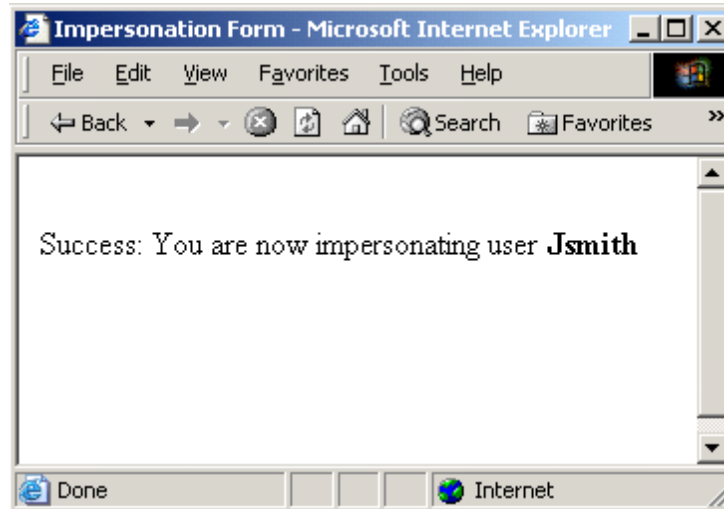
가장은 엔터프라이즈에 적절한 인터페이스를 위해 사용자 지정되어야 하는 여러 웹 기반 양식을 필요로 합니다. 양식은 가장 프로세스를 호출하는 `.fcc` 파일이 제공해야 하는 기본 요소를 포함하고 있습니다.

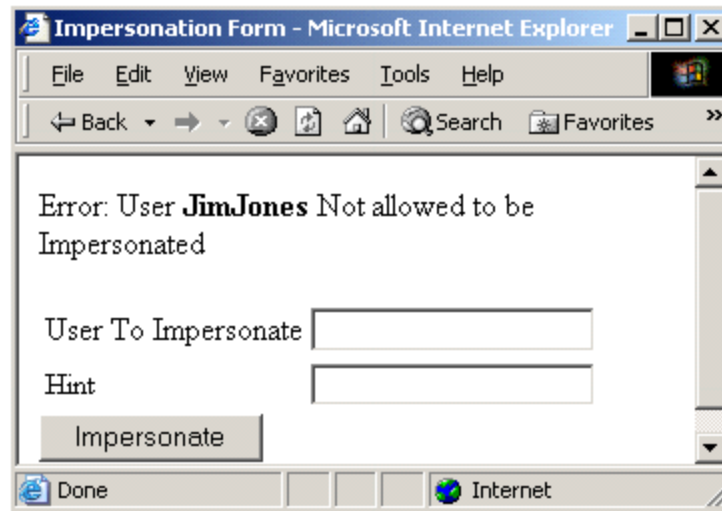
힌트 필드는 가장 대상을 명확히 하는 데 사용될 수 있는 추가 특성을 요구하도록 가장을 구성하는 것이 가능함을 나타냅니다. 힌트는 추가 특성의 목록으로서 가장 인증 체계에서 구성 가능합니다. 추가 특성은 직원 번호 또는 사용자 디렉터리에서 사용자를 고유하게 정의하는 기타 다른 사용자 특성과 같은 정보를 포함할 수 있습니다.

가장 결과 양식

가장 시도의 결과는 성공 또는 실패한 가장 시도를 모두 나타내는 양식으로서 커뮤니케이션되어야 합니다.

참고: 다음 양식은 각 양식의 기본 요구 사항을 설명하기 위해 제공됩니다. 모든 가장 양식은 사용자 지정되어 .fcc 파일에서 참조되어야 합니다.

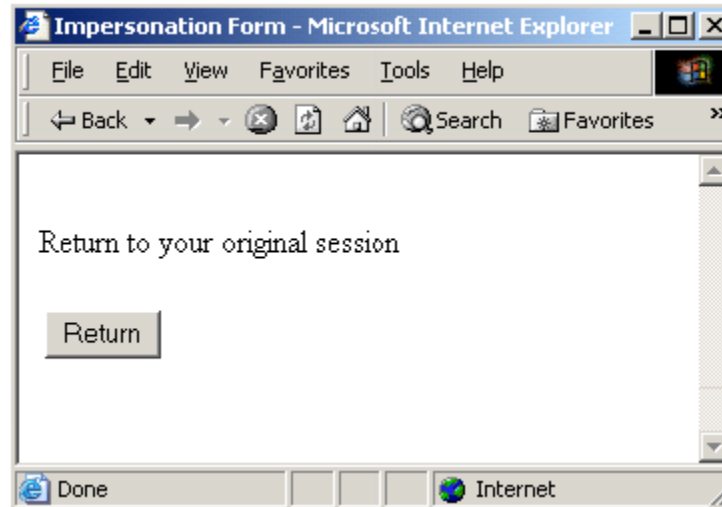




가장 로그오프 양식

가장 세션을 끝내기 위한 양식은 반드시 구성해야 합니다.

참고: 다음 양식은 기본 요구 사항을 설명하기 위해 제공됩니다. 가장 양식은 사용자 지정되어 .fcc 파일에서 참조되어야 합니다.



제 22 장: 암호 정책

이 섹션은 다음 항목을 포함하고 있습니다.

[암호 서비스 개요](#) (페이지 707)

[암호 정책을 구성하는 방법](#) (페이지 708)

[CA Directory 암호 정책 제어](#) (페이지 718)

[사용자가 직접 암호 변경](#) (페이지 718)

[암호 정책 문제 해결](#) (페이지 720)

암호 서비스 개요

암호 서비스는 보호된 리소스에 대한 보안 수준을 강화해 줍니다. 암호 서비스는 FCC(양식 자격 증명 수집기)와 사용자 지정 가능한 HTML 양식을 사용하여 다음 항목 내의 사용자 암호를 관리합니다.

- 사용자 디렉터리
- 사용자 디렉터리의 일부

참고: 저장소 암호 서비스 지원에 대한 자세한 내용은 "12.52 SP1 SiteMinder Platform Support Matrix"(12.52 SP1 SiteMinder 플랫폼 지원표)를 참조하십시오. 에이전트 및 암호 서비스에 대한 자세한 내용은 [웹 에이전트 구성 안내서](#)를 참조하십시오.

암호 정책을 사용하여 사용자 암호를 관리하고, 필요한 경우 사용자가 암호를 변경할 수 있도록 설정하십시오.

- 암호 정책은 다음 항목을 제어하는 규칙 및 제한 사항을 정의합니다.
 - 암호 만료
 - 조합
 - 용도

참고: 사용자 디렉터리 전체 또는 일부에 암호 정책을 여러 개 적용할 수 있습니다. SiteMinder 는 각 정책에 대해 지정된 우선 순위에 따라 정책을 적용합니다.

- 사용자가 보호된 리소스에 액세스하려고 하면 **SiteMinder** 가 암호 정책을 호출하고 사용자의 자격 증명을 평가합니다. 정책 확인 결과 암호가 만료된 경우 **SiteMinder** 는 다음 작업을 수행할 수 있습니다.
 - 해당 사용자 계정을 비활성화하여 무단 액세스를 방지합니다. 비활성화된 계정은 **SiteMinder** 관리자가 다시 활성화해야 합니다.
 - 사용자가 암호를 변경하도록 합니다.

암호 정책을 사용하면 관리자가 개입할 필요 없이 암호 조합 규칙을 적용할 수 있습니다. 암호 서비스를 통해 다음 작업을 수행할 수 있습니다.

- 지정한 시기에 사용자가 암호를 변경하도록 합니다.
- 사용자가 암호를 변경할 수 있도록 설정합니다.

암호 정책을 구성하는 방법

보호된 리소스에 대한 보안 수준을 강화하도록 암호 정책을 구성하십시오.

암호 정책을 구성하려면 다음 절차를 완료하십시오.

1. [암호 정책을 만듭니다](#) (페이지 709).
2. (선택 사항) 암호 만료를 구성합니다.
3. (선택 사항) 암호 조합을 구성합니다.
4. (선택 사항) 암호 정규식을 구성합니다.
5. (선택 사항) 암호 제한을 구성합니다.
6. (선택 사항) 고급 암호 옵션을 구성합니다.

암호 정책 고려 사항

기업에서 암호 정책을 구현하려는 경우에는 다음 사항을 고려하십시오.

- **SiteMinder** 에 사용자 디렉터리에 대한 읽기/쓰기 권한이 있어야 합니다. 이러한 권한에는 해당 디렉터리 내의 일부 특성을 단독으로 사용하여 암호 및 암호 관련 정보를 저장할 수 있는 권한이 포함됩니다.
- 암호의 유효성을 검사하려면 추가 사용자 디렉터리 검색이 필요하므로 암호 정책은 **SiteMinder** 성능에 영향을 줄 수 있습니다. 사용자 디렉터리 전체가 아니라 일부만 검색하도록 구성된 암호 정책도 성능에 영향을 줄 수 있습니다.

- 사용자 디렉터리에 네이티브 암호 정책이 있는 경우 이 정책은 다음 조건을 충족해야 합니다.
 - SiteMinder 암호 정책보다 덜 제한적임
 - 사용 안 함

그렇지 않으면 네이티브 암호 정책이 SiteMinder에 알리지 않고 암호를 수락하거나 거부할 수 있습니다. 따라서 SiteMinder가 해당 암호를 관리할 수 없습니다.
 - 기본적으로 사용자가 암호를 변경할 때 잘못된 정보를 입력하면 SiteMinder는 일반적인 오류 메시지를 반환합니다. 이 메시지에 오류 원인은 포함되지 않습니다. 이 기본 동작을 변경하여 변경에 실패한 이유를 사용자에게 알려 주려면 DisallowForceLogin 레지스트리 키를 생성하여 사용하십시오.
 - 여러 정책 서버에서 암호 정책을 사용하는 경우에는 모든 서버의 시스템 시간을 동기화하십시오. 시간을 동기화하면 계정이 비활성화되거나 강제 암호 변경이 중간에 종료되지 않도록 할 수 있습니다.
- 참고:** 자세한 내용은 *SiteMinder 정책 서버 구성 안내서*를 참조하십시오.

암호 정책 만들기

암호 정책을 생성하여 보호되는 리소스에 추가적인 보안 계층을 제공할 수 있습니다.

다음 단계를 수행하십시오.

1. "정책", "암호"를 차례로 클릭합니다.
2. "암호 정책"을 클릭합니다.
3. "암호 정책 만들기"를 클릭합니다.

암호 정책 설정이 표시됩니다.

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

4. 정책 이름을 입력합니다.
5. 정책을 적용할 사용자 디렉터리를 "디렉터리" 목록에서 선택합니다.
6. 정책을 전체 디렉터리에 적용할지 아니면 디렉터리 일부에 적용할지를 지정합니다.

7. (선택 사항) 정책이 디렉터리의 일부에만 적용되는 경우 "조회"를 클릭하여 해당 부분을 지정합니다.
8. (선택 사항) 사용자가 암호 정책에서 잘못된 것으로 간주되는 암호를 "리디렉션 URL" 필드에 입력할 경우 사용자를 리디렉션할 FCC의 위치를 지정합니다.

리디렉션 FCC를 에이전트와 동일한 서버에서 호스트하려면 다음 기본값을 그대로 사용합니다.

`/siteminderagent/forms/smpwservices.fcc`

특정 서버의 모든 호스트에 대해 리디렉션 FCC를 호스트하려면 다음과 같이 지정합니다.

`http://server_name:port/siteminderagent/forms/smpwservices.fcc`

SSL을 통해 특정 서버의 모든 호스트에 대해 리디렉션 FCC를 호스트하려면 다음과 같이 지정합니다.

`https://server_name:port/siteminderagent/forms/smpwservices.fcc`

9. 만료 날짜, 조합, 식, 제한 또는 고급 설정을 구성하여 원하는 암호 로직이 반영되도록 정책을 구성합니다.

참고: FQDN(정규화된 도메인 이름)을 사용하여 특정 서버로 리디렉션하도록 에이전트를 구성하고 리디렉션 FCC를 사용자 지정 또는 지역화하는 방법에 대한 자세한 내용은 [웹 에이전트 구성 안내서](#)를 참조하십시오.

암호 만료 구성

암호가 만료될 경우 트리거되어 정책 서버가 사용자 계정을 비활성화하고 필요한 경우 사용자를 새 웹 페이지로 리디렉션하도록 하는 이벤트를 정의하려면 암호 만료 설정을 구성하십시오. 이러한 이벤트의 예로는 여러 번의 로그인 시도 실패와 계정 비활성화가 포함됩니다.

참고: 만료 설정은 선택 사항입니다. 만료 설정을 사용하지 않으려면 해당 필드를 비워 두십시오.

암호 만료를 구성하려면

1. "만료" 탭을 클릭합니다.

암호 만료 설정이 열립니다.

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

2. "만료" 그룹 상자의 "성공한 로그인 추적", "실패한 로그인 추적" 및 "로그인 추적 실패에 대한 인증" 확인란을 선택하여 사용자 로그인 추적 설정을 지정합니다.

참고: 계정 비활성 상태에 따라 계정을 비활성화하려면 "성공한 로그인 추적" 확인란을 선택해야 합니다. 실패한 로그인 시도 횟수에 따라 계정을 비활성화하려면 "실패한 로그인 추적" 확인란을 선택해야 합니다.

3. "변경하지 않으면 암호 만료" 그룹 상자에서 암호를 변경해야 하는 빈도를 결정하는 설정을 지정합니다.

4. "잘못된 암호" 그룹 상자에서 잘못된 암호를 시도할 수 있는 횟수를 결정하는 설정을 지정합니다.

5. "비활성 상태에서 암호 만료" 그룹 상자에서 암호가 비활성 상태로 유지될 수 있는 기간을 결정하는 설정을 지정합니다.

참고: 비활성 상태에서 암호가 만료되도록 구성할 필요가 없는 경우에는 성능을 위해 이 옵션을 설정하지 않는 것이 좋습니다.

6. "제출"을 클릭하여 암호 정책을 저장하거나, 다른 탭을 클릭하여 암호 정책 관련 작업을 계속 수행합니다.

암호 조합 구성

새로 생성되는 암호의 문자 조합을 제어하려면 암호 조합 규칙을 구성하십시오.

참고: 조합 규칙은 선택 사항입니다. 조합 규칙을 사용하지 않으려면 해당 필드를 비워 두십시오.

암호 조합 제한을 구성하려면

1. "조합" 탭을 클릭합니다.

암호 조합 설정이 열립니다.

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

2. "최소 길이" 및 "최대 길이" 필드에 암호의 최소 및 최대 문자 길이를 입력합니다.
3. "최대 값" 필드에 암호에 연속으로 나타날 수 있는 최대 문자 수를 입력합니다.
4. 각 "콘텐츠 최소값" 그룹 상자에서 허용 가능한 문자 유형 및 최소 요구 사항을 지정합니다.
5. "제출"을 클릭합니다.

암호 정규식

암호에 정규식 일치를 사용하면 각 암호와 일치하거나 일치하지 않아야 유효한 것으로 간주되는 문자열 일치에 사용되는 텍스트 패턴을 지정할 수 있습니다.

예를 들어 암호의 첫 자는 숫자이지만 마지막 자는 숫자가 아니어야 하는 경우 이 요구 사항을 적용하여 모든 암호를 확인하는 정규식을 구성할 수 있습니다.

정규식 구문

다음 표에서는 암호 일치를 위한 정규식을 구성하는 데 사용할 수 있는 문자를 설명합니다. 이 구문은 영역을 지정할 때 리소스 일치에 대해 지원되는 정규식 구문과 일치합니다.

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

정규식 구문은 다음과 같습니다.

문자	결과
\	메타 문자(예: '*')를 나타내는 데 사용됨
\\	단일 '\' 문자와 일치
(A)	하위 식 그룹화(패턴 평가 순서에 영향을 줌)
[abc]	단순한 문자 클래스(대괄호 내의 모든 문자가 대상 문자와 일치함)
[a-zA-Z]	범위가 있는 문자 클래스(대괄호 내의 모든 문자 범위가 대상 문자와 일치함)
[^abc]	부정 문자 클래스
.	새 줄이 아닌 모든 문자와 일치
^	줄의 시작 부분에서만 일치
\$	줄의 끝 부분에서만 일치
A*	A 와 0 번 이상 일치(확장)
A+	A 와 1 번 이상 일치(확장)
A?	A 와 1 번 또는 0 번 일치(확장)
A*?	A 와 0 번 이상 일치(축소)
A+?	A 와 1 번 이상 일치(축소)
A??	A 와 0 번 또는 1 번 일치(축소)
AB	순서대로 A 및 B 와 일치
A B	A 또는 B 와 일치
\1	첫 번째 괄호 안의 하위 식에 대한 후참조
\n	n 번째 괄호 안의 하위 식에 대한 후참조

제한: 각 정규식에는 해당 식 자체를 포함하여 하위 식을 10 개까지만 포함할 수 있습니다. 하위 식의 개수는 정규식의 왼쪽 괄호(여는 괄호) 수와 식 자체의 왼쪽 괄호 한 개를 더한 수와 같습니다.

정규식 일치 구성

정규식을 구성하여 문자열 일치에 사용되는 텍스트 패턴을 지정할 수 있습니다. 암호와 일치하거나 일치하지 않아야 식이 유효한 것으로 간주됩니다. 각 정규식 항목은 설명 태그와 식 정의로 구성되는 이름/값 쌍입니다.

암호에 대한 정규식 일치는 선택 사항입니다. 정규식을 사용하려면 암호와 일치하거나 일치하지 않아야 하는 식에 대한 항목을 지정하기만 하면 됩니다. 식 일치가 필요하지 않으면 정규식 항목을 생성하지 마십시오.

암호에 대한 정규식을 구성하려면

1. "암호 정책" 대화 상자에서 "정규식" 탭을 선택합니다.
"정규식" 그룹 상자에 빈 표가 표시됩니다.
2. "추가"를 클릭하여 식을 추가합니다.
"암호 정규식" 대화 상자가 열립니다.
3. 다음 라디오 단추 중 하나를 선택합니다.
 - 일치해야 함
이 옵션을 선택할 경우 암호와 일치해야 하는 정규식을 정의하십시오.
 - 불일치해야 함
이 옵션을 선택할 경우 암호와 일치하지 않아야 하는 각 정규식에 대한 항목을 추가하십시오.
4. 필드에 값을 입력합니다.
참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.
5. "확인"을 클릭합니다.
정규식이 표에 추가됩니다. "불일치해야 함"을 선택한 경우 "불일치" 열에 확인란이 표시됩니다.

암호 제한 구성

암호 사용에 제한을 두려면 암호 제한을 구성하십시오. 제한 사항에는 다음이 포함됩니다.

- 사용자가 암호를 다시 사용할 수 있을 때까지 기다려야 하는 시간
- 이전에 사용한 암호와 새 암호의 차이

보안 위험 요소이거나 사용자의 개인 정보를 포함한다고 판단되는 단어를 사용자가 지정하지 못하게 할 수도 있습니다.

참고: 제한은 선택 사항입니다. 제한을 사용하지 않으려면 해당 필드를 비워 두십시오.

암호 제한을 구성하려면

1. "제한" 탭을 클릭합니다.

암호 제한 설정이 열립니다.

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

2. "재사용" 그룹 상자에서 이전 암호를 다시 사용하려면 시간이 얼마나 경과해야 하는지 및/또는 새 암호를 얼마나 생성해야 하는지를 지정합니다.

참고: 두 조건을 모두 지정할 경우 각 조건이 충족되어야 사용자가 암호를 다시 사용할 수 있습니다.

예: 암호 정책에 따라 사용자가 특정 암호를 다시 사용하려면 365 일이 경과하고 그 사이 12 개의 암호를 지정해야만 한다고 가정합니다. 1 년이 지날 때까지 사용자가 암호를 여섯 개만 제공했다면 이후 암호를 여섯 개 더 제공해야 첫 번째 암호를 다시 사용할 수 있습니다.

3. "변경 필요" 그룹 상자에서 새 암호가 이전 암호와 얼마나 달라야 하는지를 지정합니다.
4. "프로필 특성" 그룹 상자에서 암호 정책이 사용자 프로필에 저장된 개인 정보와 비교할 연속 문자 수를 지정합니다.
5. "사전" 그룹 상자에서 금지된 암호가 포함된 사용자 정의 사전의 경로와 사전에 있는 값과 비교할 문자열의 길이를 지정합니다.
6. "적용"을 클릭하여 변경 내용을 저장하거나, "확인"을 클릭하여 변경 내용을 저장하고 관리 UI로 돌아갑니다.

고급 암호 옵션 구성

제출된 암호를 유효성 검사 및 저장 전에 전처리하도록 지정하려면 고급 암호 정책 옵션을 구성하십시오. 고급 암호 정책을 사용하면 정책에 우선 순위를 할당할 수 있으므로 동일한 사용자 디렉터리 또는 네임스페이스에 적용되는 여러 암호 정책의 예측 가능한 평가가 가능해집니다.

참고: 전처리 옵션은 선택 사항입니다. 사용자 디렉터리 또는 네임스페이스에 할당될 수 있는 각 암호 정책에 대해 고유한 암호 정책 평가 우선 순위를 지정해야 합니다.

고급 암호 옵션을 구성하려면

1. "고급" 탭을 클릭합니다.

고급 암호 정책 설정이 열립니다.

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

2. "암호 전처리" 그룹 상자에서 제출된 암호를 평가 및 저장 전에 처리하기 위한 옵션을 지정합니다.

참고: 동일한 사용자 디렉터리 또는 네임스페이스에 적용되는 각 암호 정책에 대해 동일한 전처리 옵션을 지정해야 합니다.

3. (선택 사항) 암호 정책이 동일한 사용자 디렉터리 또는 네임스페이스에 적용되는 여러 정책 중 하나인 경우 "암호 정책 우선 순위" 그룹 상자에서 암호 정책 우선 순위를 지정합니다.

참고: 평가 우선 순위의 범위는 0~999 입니다(999 가 가장 높음).

암호 서비스를 위해 리디렉션 시 로그인 ID 제거

암호 서비스 처리 중에는 사용자 요청이 여러 번 리디렉션됩니다. 요청이 리디렉션될 때는 사용자가 입력한 로그인 ID(일반적으로 사용자 이름)가 기본적으로 요청 URL 에 추가됩니다. 기본 브라우저 동작을 수정하여 로그인 ID(사용자 이름)가 리디렉션에 추가되지 않도록 하려면 다음 절차 중 하나를 수행하십시오.

Windows 에서 암호 서비스를 위해 리디렉션 시 로그인 ID 를 제거하려면

1. 다음 레지스트리 키를 추가합니다.
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\PolicyServer\DisallowUsernameInURL
2. DWORD 값을 다음 값 중 하나로 설정합니다.
 - 0 - 요청 URL 에 UID 를 추가하는 기본 동작을 적용합니다.
 - 1 - 요청 URL 에 UID 가 추가되지 않도록 기본 동작을 변경합니다.

UNIX 에서 암호 서비스를 위해 리디렉션 시 로그인 ID 를 제거하려면

1. 다음 위치로 이동합니다.
<policy-server-install-dir>/registry/
2. 텍스트 편집기에서 다음 파일을 엽니다.
sm.registry
3. 다음 레지스트리 키를 추가합니다.
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\PolicyServer\DisallowUsernameInURL
4. DWORD 값을 다음 값 중 하나로 설정합니다.
 - 0 - 요청 URL 에 UID 를 추가하는 기본 동작을 적용합니다.
 - 1 - 요청 URL 에 UID 가 추가되지 않도록 기본 동작을 변경합니다.

CA Directory 암호 정책 제어

CA Directory 암호 정책을 따르도록 정책 서버를 구성할 수 있습니다. 적절하게 구성된 웹 에이전트와 함께 웹 에이전트 정책 서버는 디렉터리 암호 정책에 기반한 최종 사용자가 구성한 경고 및 알림을 보낼 수 있습니다.

다음과 같은 CA Directory 암호 정책이 지원됩니다.

- 네이티브 암호 만료
- 이 기능을 사용하려면 다음 옵션 중 *하나*를 수행하십시오.
 - 암호 만료에 대한 정책 서버 암호 정책을 설정하지 마십시오.
 - CA directory 암호 정책의 설정보다 덜 제한되도록 만료 및 경고에 대한 정책 설정을 구성하십시오.
- 사용자 계정 잠금 설정
CA Directory 설정을 사용하는 경우 정책 서버 계정 잠금 기능을 비활성화하십시오.
- 암호 만료 경고
- 남은 유예 로그인 알림. 클라이언트가 유예 로그인 메시지에 대한 암호 메시지 코드를 인식할 수 있는 경우
정책 서버에는 남은 유예 로그인의 개념이 없습니다.

CA Directory 암호 정책을 사용하도록 허용하려면:

1. 사용자가 있는 CA Directory 를 참조하는 SiteMinder 암호 정책을 정의합니다.
2. XPSConfig 도구를 사용하여 구성 매개 변수 **CA.SM::\$LdapEnablePwdCtrlSupport** 를 true 로 설정합니다.
이 도구의 사용 방법은 XPSConfig 지침을 참조하십시오.

사용자가 직접 암호 변경

사용자가 직접 암호를 변경하는 기능을 사용하면 관리자가 개입할 필요 없이 최종 사용자가 직접 자신의 암호를 변경할 수 있습니다. 사용자는 링크를 클릭하여 "암호 변경 요청" 양식에 액세스한 후 암호를 변경할 수 있습니다.

암호 변경 링크 추가

사용자가 암호를 변경할 수 있도록 하려면 정책 서버 관리자가 HTML 페이지에 암호 변경 링크를 추가해야 합니다. 예를 들어 관리자가 로그인 페이지에 이 링크를 추가하면 사용자는 로그인 시 암호를 변경할 수 있습니다.

참고: 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.

암호 직접 변경

자신의 암호를 변경하려는 사용자는 다음을 수행해야 합니다.

1. "암호 변경"을 클릭합니다.
"암호 변경 요청" 양식이 표시됩니다.
2. 요청된 정보를 입력하고 "암호 변경" 단추를 클릭합니다.
관리 UI 에서 사용자의 암호가 변경되었음을 나타내는 "암호 변경 정보" 페이지가 별도로 표시됩니다.

암호 변경 허용 오류 메시지

기본적으로 사용자가 암호를 변경할 때 잘못된 정보를 입력하면 SiteMinder 는 일반적인 오류 메시지를 반환합니다. 이 메시지에 오류 원인은 포함되지 않습니다.

기본 동작을 변경하여 암호 변경에 실패한 이유를 사용자에게 명시적으로 알려 줄 수 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 액세스하여 다음 중 하나를 수행합니다.
 - a. Windows: 레지스트리 편집기를 열고
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\PolicyServer 로 이동합니다.
 - b. (UNIX) sm.registry 파일을 엽니다. 이 파일의 기본 위치는
siteminder_home/registry 입니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

2. 다음 설정을 사용하여 DisallowForceLogin 을 생성합니다.

키 종류: REG_DWORD

값: 0 또는 1

0

(기본값) SiteMinder 가 일반 오류 메시지를 반환합니다. 이 동작은 기본 SiteMinder 동작과 일치합니다.

1

SiteMinder 가 명시적 오류 원인을 반환합니다.

참고: 1 또는 0 이 아닌 값은 지원되지 않습니다.

3. 다음 작업 중 하나를 수행하십시오.
 - (Windows) 레지스트리 편집기를 종료합니다.
 - (UNIX) 레지스트리 파일을 저장합니다.
4. 정책 서버를 다시 시작합니다.

암호 정책 문제 해결

다음 단원에서는 암호 정책을 구현할 때 발생할 수 있는 문제를 설명하고 해결책을 제공합니다.

새 사용자 암호가 거부됨

증상:

사용자 지정 암호가 항상 거부됩니다.

해결책:

암호 정책이 너무 엄격하거나 잘못 구성되었을 수 있습니다. 콘텐츠 최소값 및 암호 길이 조합 설정의 일관성을 확인하십시오.

사용자 계정이 잘못 비활성화됨

증상:

사용자 계정이 허용되는 로그인 시도 실패 횟수를 초과하지 않았는데도 비활성화됩니다.

해결책:

잘못된 암호 설정을 확인하십시오. 암호를 일정 횟수 이상 연속해서 잘못 입력할 경우 계정을 비활성화하기 위한 설정 값이 너무 낮을 수 있습니다.

이 값을 너무 낮게 설정하면 서로 다른 사용자 디렉터리에 있는 둘 이상의 사용자가 동일한 사용자 이름을 사용할 경우 문제가 발생할 수 있습니다. 정책 서버는 사용자 권한 부여를 시도할 때 로그인에 해당하는 모든 사용자 이름을 확인한 다음 암호가 일치하는지 확인합니다. 암호가 일치하지 않는 사용자 이름이 발견되면 정책 서버는 해당 사용자에게 대해 실패한 시도를 기록합니다. 실패한 시도 횟수가 잘못된 암호 설정에 지정된 횟수를 초과하면 계정이 비활성화됩니다.

사용자 계정이 중간에 비활성화됨

증상:

다중 정책 서버 환경에서 사용자 계정이 중간에 비활성화됩니다.

해결책

정책 서버 간에 시간 차이가 없는지 확인하십시오.

암호 변경이 강제 적용됨

증상:

다중 정책 서버 환경에서 사용자 계정에 변경된 암호가 너무 빠르게 적용됩니다.

해결책:

정책 서버 간에 시간 차이가 없는지 확인하십시오.

LDAP 사용자가 비활성화되지 않음

증상:

암호 정책이 LDAP 사용자를 비활성화하지 않습니다.

해결책:

다음을 확인하십시오.

- 정책이 바인딩된 LDAP 디렉터리가 쓰기 가능한지 확인하십시오. LDAP 디렉터리의 각 사용자 레코드에 암호를 저장할 수 있어야 합니다.
- 사용자 디렉터리 설정에서 암호 특성, 암호 데이터 및 비활성화된 플래그 사용자 프로필 특성이 올바른지 확인하십시오. 암호 특성, 암호 데이터 및 비활성화된 플래그 사용자 프로필 특성의 구성에 대한 자세한 내용은 [디렉터리 특성 개요](#) (페이지 150)를 참조하십시오.

Active Directory 사용자가 암호를 변경할 수 없음

증상:

Active Directory 사용자 디렉터리에 저장된 사용자가 자신의 암호를 변경할 수 없습니다.

해결책:

다음을 확인하십시오.

- 정책이 바인딩된 Active Directory 사용자 디렉터리에 보안 SSL 연결이 구성되었는지 확인하십시오.
- 정책이 바인딩된 Active Directory 사용자 디렉터리가 unicodePWD 암호 특성을 사용하도록 구성되었는지 확인하십시오.

암호가 올바르지 않다는 메시지가 표시되지 않음

증상:

사용자가 현재 암호가 잘못 포함된 암호 변경 요청을 제출할 경우 현재 암호가 잘못되었다는 메시지를 표시하는 "암호 변경 정보" 화면이 열리지 않습니다. 대신 정책 서버가 사용자를 다음과 같이 리디렉션합니다.

- On-Auth-Reject-Redirect 응답이 사용자 디렉터리에 대해 구성된 정책에 바인딩되지 않은 경우 메시지를 표시하지 않고 로그인 화면으로 리디렉션합니다.
- On-Auth-Reject-Redirect 응답이 사용자 디렉터리에 대해 구성된 정책에 바인딩된 경우 이 응답과 연결된 URL 로 리디렉션합니다.

해결책:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\PolicyServer 에 있는 DisallowForceLogin 레지스트리 키가 사용되도록 설정하십시오.

DisallowForceLogin

변경 요청에 포함된 현재 암호가 잘못된 경우 현재 암호를 다시 입력할 수 있는 "암호 변경 정보" 화면으로 사용자를 리디렉션합니다.

키 종류: REG_DWORD

값: 0(사용 안 함) 또는 1(사용)

기본값: 0(사용 안 함)

참고: 이 레지스트리 키를 사용할 경우 0 또는 1 이 아닌 값은 지원되지 않으며 이러한 값을 사용하면 정의되지 않은 동작이 발생합니다.

제 23 장: DeviceDNA™를 사용한 고급 세션 보증

이 섹션은 다음 항목을 포함하고 있습니다.

[DeviceDNA™를 사용한 고급 세션 보증 구성 방법](#) (페이지 725)

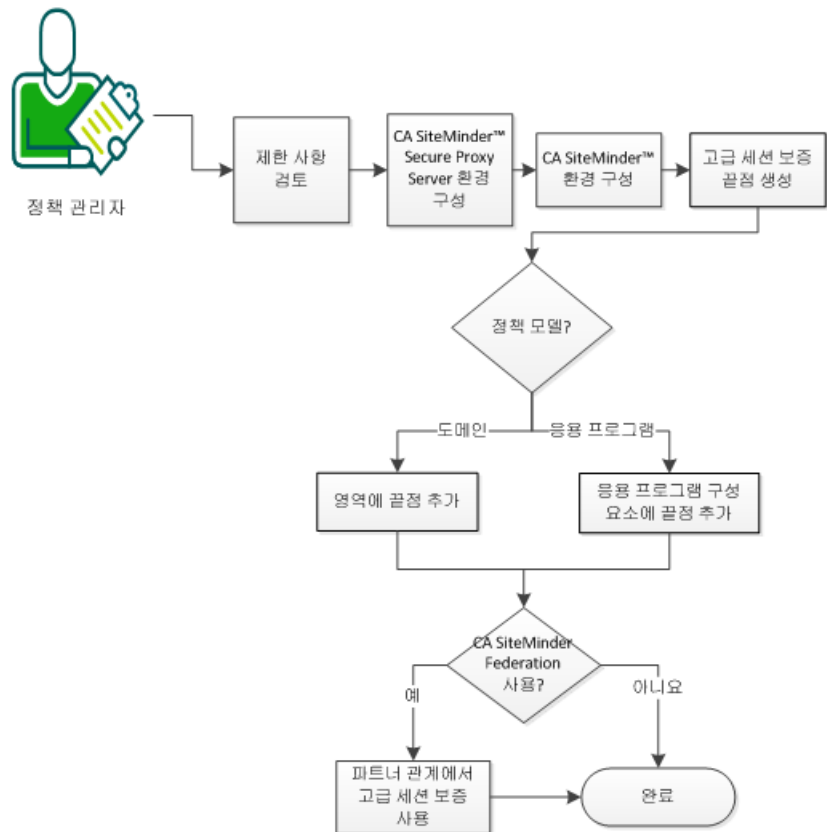
[업그레이드 중 DeviceDNA™를 사용한 고급 세션 보증 구성 방법](#) (페이지 737)

DeviceDNA™를 사용한 고급 세션 보증 구성 방법

DeviceDNA™를 사용한 고급 세션 보증은 권한 없는 사용자가 훔친 쿠키를 사용하여 적법한 세션을 가로채는 것을 방지하는 데 도움을 줍니다. 세션 클라이언트는 제품이 사용자 시스템에서 수집하는 고유 DeviceDNA™를 사용하여 유효성이 검사됩니다. 이러한 유효성 검사를 통해 세션을 시작한 클라이언트가 액세스를 요청하는 클라이언트와 동일한지 확인됩니다. DeviceDNA™가 없는 사용자는 보호된 리소스에 대한 액세스가 거부됩니다.

다음 그림은 DeviceDNA™를 사용한 고급 세션 보증을 구성하는 방법을 설명합니다.

DeviceDNA™를 사용한 고급 세션 보증 구성 방법



다음 단계를 수행하십시오.

1. [제한 사항을 검토합니다](#) (페이지 728).
2. [CA SiteMinder® for Secure Proxy Server 환경을 구성합니다](#) (페이지 730).
3. [SiteMinder 환경을 구성합니다](#) (페이지 731).
4. [세션 보증 끝점을 생성합니다](#) (페이지 732).
5. 다음 목록에서 정책 모델에 적절한 단계를 선택합니다.
 - 정책 도메인의 경우 [끝점을 영역에 추가합니다](#) (페이지 734).
 - 응용 프로그램(EPM)의 경우 [끝점을 응용 프로그램 구성 요소에 추가합니다](#) (페이지 735).
6. CA SiteMinder® Federation 의 경우 [파트너 관계에서 고급 세션 보증을 활성화합니다](#) (페이지 736).

DeviceDNA™를 사용한 고급 세션 보증 제한 사항

DeviceDNA™를 사용한 고급 세션 보증은 다음 항목을 지원하지 *않습니다*.

Web 2.0 클라이언트

Web 2.0 응용 프로그램은 CA SiteMinder® for Secure Proxy Server 로 리디렉션할 수 없는 웹 요청을 생성하는 AJAX 등의 기술에 기반하여 구축됩니다. Web 2.0 클라이언트에는 비 브라우저 기반 클라이언트(예: 모바일 장치의 Flickr 클라이언트)가 포함되어 있습니다. 두 경우 모두 인증 흐름 응용 프로그램을 호스트하는 CA SiteMinder® for Secure Proxy Server 인스턴스로 리디렉션할 수 없는 요청이 발생할 수 있습니다. 이러한 상황으로 인해 DeviceDNA™를 사용한 고급 세션 보증은 Web 2.0 클라이언트에서 지원되지 않습니다. Web 2.0 응용 프로그램의 로그인 페이지를 보호할 수 있습니다. 하지만 AJAX 와 관련된 요청을 비롯한 일부 요청은 DeviceDNA™를 사용한 고급 세션 보증으로 보호할 수 없습니다.

사용자 지정 에이전트

SiteMinder SDK 로 생성한 에이전트는 DeviceDNA™를 사용한 고급 세션 보증을 지원하지 않습니다.

JavaScript 및 쿠키를 지원하지 않는 클라이언트

CA SiteMinder® for Secure Proxy Server 의 DeviceDNA™ 스크립트는 웹 클라이언트와 관련된 정보를 추출하는 JavaScript 입니다. 이 클라이언트 정보는 세션을 장치 또는 클라이언트와 연결합니다. JavaScript 에 대한 지원 없이는 DeviceDNA™를 수집할 수 없으므로 DeviceDNA™를 사용한 고급 세션 보증이 세션을 장치 또는 클라이언트와 연결할 수 없습니다. DeviceDNA™를 사용한 고급 세션 보증은 텔넷 또는 Lynx 같은 클라이언트에서 지원되지 않습니다.

POST 보존

DeviceDNA™를 사용한 고급 세션 보증은 CA SiteMinder® for Secure Proxy Server 의 인증 흐름 응용 프로그램에 대한 리디렉션을 사용하여 작동합니다. 이 응용 프로그램에는 DeviceDNA™ 스크립트가 포함되어 있습니다. 인증 흐름 응용 프로그램은 현재 POST 데이터를 지원하지 않습니다. 따라서 POST 요청이 인증 흐름 응용 프로그램으로 리디렉션되지 않습니다.

공유 워크스테이션

공유 워크스테이션에서는 모든 사용자의 DeviceDNA™ 서명이 동일합니다. 예를 들어 한 사용자가 유효한 SMSESSION 쿠키를 공유 워크스테이션의 다른 사용자로부터 가로챘다고 가정합니다. 가로챈 사용자가 훔친 SMSESSION 쿠키를 동일한 공유 워크스테이션에서 재생하는 경우 차이점이 감지되지 *않습니다*. DeviceDNA™를 사용한 고급 세션 보증은 가로챈 사용자가 훔친 SMSESSION 쿠키를 *다른* 장치에서 재생하려고 할 때 보호 기능을 제공합니다.

인증 및 권한 부여 웹 서비스

웹 서비스 클라이언트 응용 프로그램은 에이전트 API 호출에서 받은 리디렉션 또는 응답을 푸시하는 인증 및 권한 부여 웹 서비스를 처리합니다. 하지만 호출하는 클라이언트는 DeviceDNA™를 사용한 고급 세션 보증 흐름과 관련된 리디렉션을 처리할 수 *없습니다*.

CA SiteMinder® Federation

다음 구성은 DeviceDNA™를 사용한 고급 세션 보증을 지원하지 *않습니다*.

- SAML 2.0 파트너 관계의 SP 측
- 파트너 관계의 IdP 측에서 SAML 2.0 HTTP-POST 바인딩

에이전트 구성 매개 변수

다음 에이전트 구성 매개 변수는 DeviceDNA™를 사용한 고급 세션 보증을 지원하지 *않습니다*.

- SecureURL
- TargetAsRelativeURI

참고: DeviceDNA™를 사용한 고급 세션 보증을 사용하는 경우 이러한 매개 변수를 설정하지 마십시오. 이러한 매개 변수에 일반적으로 포함되는 대상 URL 은 DeviceDNA™를 사용한 고급 세션 보증에서 사용하는 토큰 요청에 이미 포함되어 있습니다.

응답 특성

다음 응답 특성은 DeviceDNA™를 사용한 고급 세션 보증을 지원하지 *않습니다*.

- OnAuthAccept

DeviceDNA™를 사용한 고급 세션 보증을 위한 CA SiteMinder® for Secure Proxy Server 환경 구성

DeviceDNA™를 사용한 고급 세션 보증 기능을 사용하려면 CA SiteMinder® for Secure Proxy Server 가 작동해야 합니다.

1. 다음 태스크 중 *하나*를 수행합니다.

- CA SiteMinder® for Secure Proxy Server 가 설치되지 않은 경우 12.52 SP1 버전을 설치합니다.
- CA SiteMinder® for Secure Proxy Server 가 설치된 경우 12.52 SP1 로 업그레이드합니다.

참고: CA SiteMinder® for Secure Proxy Server 의 설치 및 업그레이드에 대한 자세한 내용은 CA SiteMinder® for Secure Proxy Server 관리 안내서를 참조하십시오. 또한 온라인에서 [설치 비디오](#)도 참조할 수 있습니다.

2. SSL 을 사용하도록 CA SiteMinder® for Secure Proxy Server 를 구성합니다.
3. CA SiteMinder® for Secure Proxy Server 와 정책 서버 사이에서 포트 번호 7658 을 엽니다.
4. CA SiteMinder® for Secure Proxy Server 설치 또는 업그레이드에서 고급 인증 서버 암호화 키를 기록합니다. 현재 환경의 SiteMinder 정책 서버에서 나중에 이 키가 필요합니다.
5. 여러 쿠키 도메인을 사용하는 싱글 사인온 환경의 경우 쿠키 공급자 도메인의 FQDN(정규화된 도메인 이름)이 필요합니다. 구성 마법사를 실행할 때 이 FQDN 을 ServerName 설정에 사용합니다. 예를 들어 쿠키 도메인이 sso.example.com 일 경우 CA SiteMinder® for Secure Proxy Server 구성 마법사에서 ServerName 의 값을 sso.example.com 으로 설정합니다.
6. CA SiteMinder® for Secure Proxy Server 에 대한 IgnoreExt 구성 매개 변수에 다음 값을 추가합니다.

.sac

7. 다음 단계에 따라 JVM 을 JSafeJCE 보안 공급자와 함께 구성하여 암호화를 사용하도록 설정합니다.
 - a. CA SiteMinder® for Secure Proxy Server 컴퓨터에 로그인합니다.
 - b. Oracle 웹 사이트에서 사용하는 Java 버전에 대한 "Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files" 패키지를 다운로드하십시오.
 - c. 다음 위치로 이동합니다.

Windows

`JVM_HOME\lib\security`

UNIX

`JVM_HOME/lib/security`

JVM_HOME

JRE(Java Runtime Environment)가 JDK에서 설치된 위치를 정의합니다.

- d. "JCE Unlimited Strength Jurisdiction Policy Files" 패키지의 파일을 사용하여 다음 파일을 패치하십시오.
 - local_policy.jar
 - US_export_policy.jar
 JVM 이 구성되었습니다.

DeviceDNA™를 사용한 고급 세션 보증을 위한 SiteMinder 환경 구성

DeviceDNA™를 사용한 고급 세션 보증을 사용하려면 SiteMinder 환경에서 일부 구성 요소 및 설정이 필요합니다.

다음 단계를 수행하십시오.

1. 정책 서버를 12.52 SP1 버전으로 설치하거나 업그레이드합니다.
참고: 이전 버전에서 업그레이드한 경우 환경에 있는 각 정책 서버에서 정책 서버 구성 마법사를 실행하십시오.
2. 세션 저장소가 없을 경우 세션 저장소를 하나 구성합니다.
3. 정책 서버와 CA SiteMinder® for Secure Proxy Server 사이에서 포트 번호 7658 을 엽니다.

DeviceDNA™를 사용한 고급 세션 보증 끝점 만들기

DeviceDNA™를 사용한 고급 세션 보증은 DeviceDNA™ 정보를 수집하기 위해 CA SiteMinder®for Secure Proxy Server 에서 호스트되는 인증 흐름 응용 프로그램 끝점으로 사용자를 자동 리디렉션합니다. 이러한 DeviceDNA™ 정보는 사용자 세션의 유효성을 검사합니다.

성능상의 이유로 인해 조직에서 각 지역마다 하나의 끝점을 만들 것을 권장합니다. 예를 들어, 뉴욕과 시카고에 사무소가 있는 경우 각 사무소마다 하나의 끝점을 만드십시오.

정책 또는 응용 프로그램에 DeviceDNA™를 사용한 고급 세션 보증을 추가하기 전에 CA SiteMinder®for Secure Proxy Server 에서 이러한 끝점을 구성하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에서 "정책", "전역", "세션 보증 끝점"을 클릭합니다.
2. "세션 보증 끝점 생성"을 클릭합니다.
3. 구체적인 이름과 설명(선택 사항)을 입력합니다.

4. 다음 필드를 작성하십시오.

웹 서버 이름

사용자를 인증하기 위해 DeviceDNA™를 수집하는 CA SiteMinder® for Secure Proxy Server 서버의 이름을 지정합니다.

Port(포트)

CA SiteMinder® for Secure Proxy Server 가 리디렉션을 위해 수신 대기하는 포트 번호를 지정합니다. 보안 연결(SSL 사용)을 사용하도록 이 포트를 구성하십시오.

기본값: 443

대상

사용자가 자동으로 리디렉션되는 CA SiteMinder® for Secure Proxy Server 의 URL 을 지정합니다. 이 서버는 사용자의 DeviceDNA™를 수집합니다. 제품은 이 DeviceDNA™를 사용하여 사용자와 관련된 세션의 유효성을 검사합니다.

DeviceDNA™ 새로 고침 간격

사용자와 관련된 DeviceDNA™가 유효한 상태로 유지되는 기간(초)을 지정합니다. 올바른 DeviceDNA™가 없는 사용자는 고급 세션 보증 끝점으로 리디렉션되고, 여기서 서버가 사용자에 대한 현재 DeviceDNA™를 획득합니다.

DeviceDNA™ 새로 고침 간격은 DeviceDNA™의 수집에 적용됩니다. DeviceDNA™ 새로 고침 간격이 만료된 후 발생하는 모든 요청은 DeviceDNA™를 수집하기 위해 인증 흐름 응용 프로그램으로 리디렉션됩니다.

DeviceBinder 는 세션과 관련된 사용자를 식별하는 세션 속성입니다. DeviceBinder 및 클라이언트 쪽 장치 ID 는 인증 프로세스 중 연결되었습니다. 고유 DeviceHash 및 만료 시간이 이 속성을 구성합니다.

기본값: 300 초(5 분)

5. 제출을 클릭합니다.

영역에 끝점 추가

DeviceDNA™를 사용한 고급 세션 보증을 사용하여 영역에 있는 리소스를 보호하려면 이 영역에 하나의 세션 보증 끝점을 추가하십시오.

참고: DeviceDNA™를 사용한 고급 세션 보증이 작동하기 위해 영역이 영구적일 필요는 없습니다.

다음 단계를 수행하십시오.

1. 관리 UI 에서 "정책", "도메인", "영역"을 차례로 클릭합니다.
2. 원하는 영역의 편집 아이콘을 클릭합니다.
3. "세션" 아래에서 "고급 세션 보증" 옆의 "사용" 확인란을 클릭합니다.
4. "끝점 조회"를 클릭합니다.
5. 원하는 끝점을 선택합니다.
6. "확인"을 클릭합니다.
7. 제출을 클릭합니다.
8. 세션 보증 기능을 사용하여 보호할 리소스가 있는 기타 영역에 대해 2 - 6 단계를 반복합니다.

응용 프로그램 구성 요소에 끝점 추가

DeviceDNA™를 사용한 고급 세션 보증을 사용하여 응용 프로그램의 구성 요소를 보호하려면 고급 세션 보증 끝점 *하나*를 관련 응용 프로그램의 구성 요소에 추가하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에서 "정책", "응용 프로그램"을 클릭합니다.
응용 프로그램 목록이 나타납니다.
2. 원하는 응용 프로그램의 편집 아이콘을 클릭합니다.
"응용 프로그램 수정:" 대화 상자가 표시됩니다.
3. 다음 단계 중 *하나*를 수행합니다.
 - 응용 프로그램에 단 하나의 구성 요소만 있는 경우 "고급 설정"을 클릭하십시오.
 - 응용 프로그램에 여러 구성 요소가 있는 경우 원하는 구성 요소의 편집 아이콘을 클릭하십시오. "고급 설정"을 클릭하십시오.
4. "세션" 아래에서 "고급 세션 보증" 옆의 "사용" 확인란을 선택합니다.
5. "끝점 조회"를 클릭합니다.
끝점의 목록이 표시됩니다.
6. 원하는 끝점을 선택합니다.
7. "확인"을 클릭합니다.
8. 제출을 클릭합니다.
"응용 프로그램 수정" 대화 상자가 닫히고 확인 메시지가 표시됩니다.
9. 세션 보증 기능을 사용하여 보호할 리소스가 있는 기타 응용 프로그램에 대해 2 - 7 단계를 반복합니다.

파트너 관계에서 DeviceDNA™를 사용한 고급 세션 보증 활성화

CA SiteMinder® Federation 를 사용하는 경우 다음 파트너 관계에서 DeviceDNA™를 사용한 고급 세션 보증을 활성화할 수도 있습니다.

- SP-IdP 파트너 관계의 IdP 측(HTTP-리디렉션 바인딩만 해당)
- 소비자-생산자 파트너 관계의 생산자 측
- RP-AP 파트너 관계의 AP 측

다음 단계를 수행하십시오.

1. 관리 UI 에서 "페더레이션", "파트너 관계 페더레이션", "파트너 관계"를 클릭합니다.
2. 원하는 파트너 관계의 왼쪽에 있는 "작업" 단추를 클릭한 다음 "비활성화"를 클릭합니다.
3. 동일한 "작업" 단추를 다시 클릭한 다음 "수정"을 선택합니다.
4. "SSO 및 SLO" 탭을 클릭합니다.
5. 다음 확인란을 클릭합니다.

세션 보증 사용

영역(정책 도메인 모델) 또는 구성 요소(응용 프로그램 모델)에 지정된 리소스를 보호합니다. 특정 CA SiteMinder® Federation 파트너 관계의 인증 요청을 보호할 수도 있습니다. 세션 보증 끝점은 사용자로부터 DeviceDNA™를 수집하여 세션의 유효성을 검사합니다.

제한: 이 기능은 세션 보증 끝점이 필요합니다.

끝점의 목록이 표시됩니다.

6. 원하는 끝점의 확인란을 클릭합니다.
7. "저장"을 클릭합니다.
8. 원하는 다른 파트너 관계에 대해 2 - 7 단계를 반복합니다.
9. (로컬 인증 모드만 해당) 인증 URL(Redirect.jsp)과 연결되는 영역에서 DeviceDNA™를 사용한 고급 세션 보증을 활성화합니다.

SM--Related 로그 파일

"DeviceDNA™를 사용한 고급 세션 보증"과 관련된 트랜잭션은 다음 로그 파일에 기록됩니다.

정책 서버

xps-*.audit - 이 기능의 구성 설정에 대한 변경 사항

smaccesslog4 - 이 기능과 관련된 인증 및 권한 부여 작업

고급 인증 서버에 대한 시작 로그:

caauthminderstartup

cariskminderstartup

cariskmindercasemgmtserverstartup

고급 인증 서버에 대한 런타임 로그:

caauthminder

cariskminder

cariskmindercasemgmtserver

CA SiteMinder® for Secure Proxy Server 서버(고급 인증 흐름 응용 프로그램)

arcotuds.log - UDS 서비스에 대한 로그 파일

CAWebFlowLog.txt - 인증 흐름 응용 프로그램에 대한 로그 파일

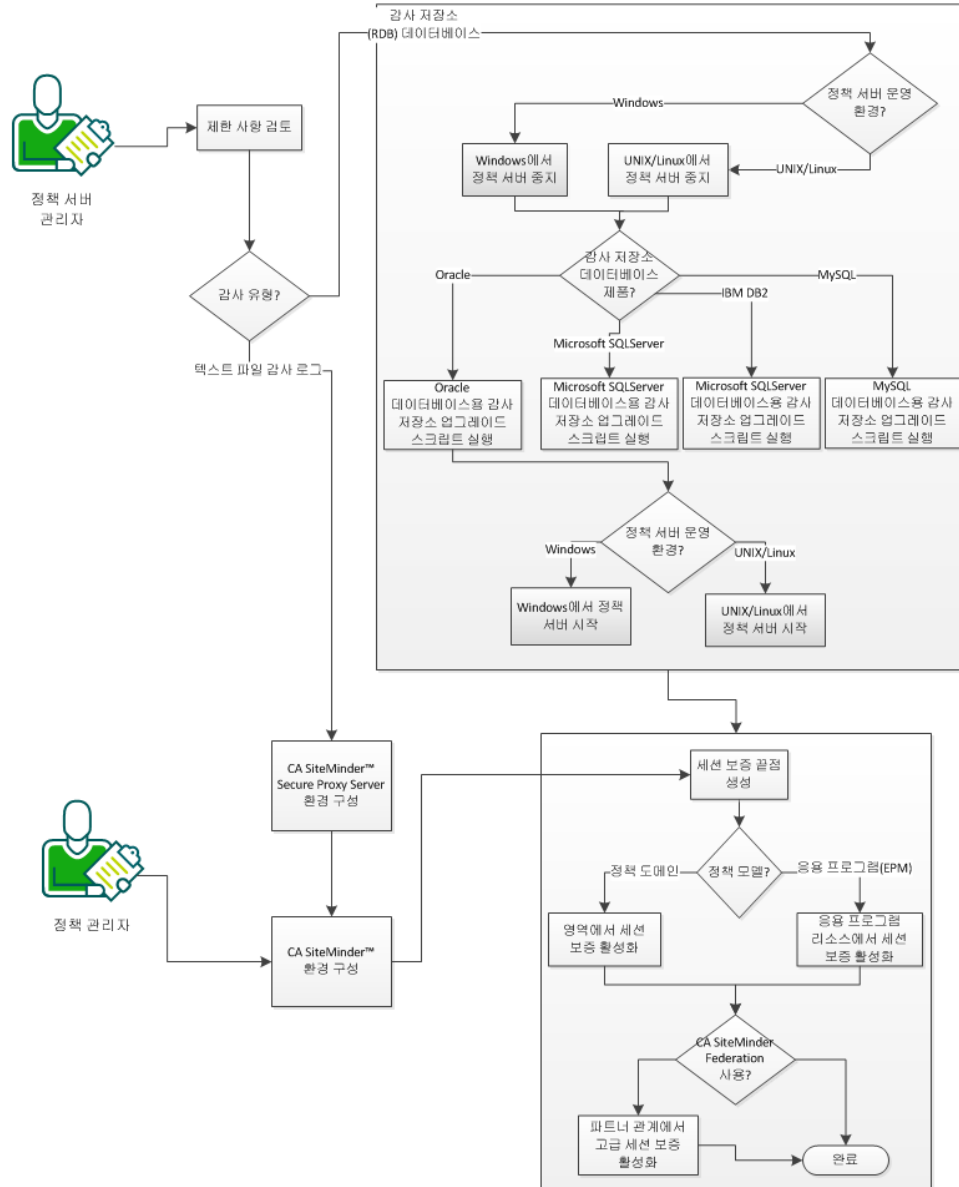
UIApplog.txt - UIApp(인증 흐름 응용 프로그램 실행 프로세스의 일부)에 대한 로그

업그레이드 중 DeviceDNA™를 사용한 고급 세션 보증 구성 방법

DeviceDNA™를 사용한 고급 세션 보증은 권한 없는 사용자가 훔친 쿠키를 사용하여 적법한 세션을 가로채는 것을 방지하는 데 도움을 줍니다. 세션 클라이언트는 제품이 사용자 시스템에서 수집하는 고유 DeviceDNA™를 사용하여 유효성이 검사됩니다. 이러한 유효성 검사를 통해 세션을 시작한 클라이언트가 액세스를 요청하는 클라이언트와 동일한지 확인됩니다. DeviceDNA™가 없는 사용자는 보호된 리소스에 대한 액세스가 거부됩니다.

다음 그림은 업그레이드 중 DeviceDNA™를 사용한 고급 세션 보증을 구성하는 방법을 설명합니다.

업그레이드 중 Device DNA™를 사용한 고급 세션 보증 구성 방법



다음 단계를 수행하십시오.

1. [제한 사항을 검토합니다](#) (페이지 728).
2. 다음 단계 중 *하나*를 수행합니다.
 - 관계형 데이터베이스에 감사 로그를 저장하는 경우 3 단계로 가십시오.
 - 텍스트 파일로 감사 로그를 저장하는 경우 4 단계로 가십시오.
3. 다음 단계를 사용하여 감사 저장소(데이터베이스)를 업그레이드합니다.
 - a. 다음 단계 중 *하나*를 사용하여 정책 서버를 중지합니다.
 - [Windows 운영 환경에서 정책 서버를 중지합니다](#) (페이지 742).
 - [UNIX/Linux 운영 환경에서 정책 서버를 중지합니다](#) (페이지 743).
 - b. 다음 절차 중 *하나*를 사용하여 데이터베이스에 적절한 업그레이드 스크립트를 실행 (페이지 743)합니다.
 - [Oracle 데이터베이스용 감사 저장소 업그레이드 스크립트를 실행합니다](#) (페이지 744).
 - [SQL Server 데이터베이스용 감사 저장소 업그레이드 스크립트를 실행합니다](#) (페이지 745).
 - [IBM DB2 데이터베이스용 감사 저장소 업그레이드 스크립트를 실행합니다](#) (페이지 747).
 - [MySQL 데이터베이스용 감사 저장소 업그레이드 스크립트를 실행합니다](#) (페이지 748).
 - c. 다음 절차 중 *하나*를 사용하여 정책 서버를 시작합니다.
 - [Windows 운영 환경에서 정책 서버를 시작합니다](#) (페이지 749).
 - [UNIX/Linux 운영 환경에서 정책 서버를 시작합니다](#) (페이지 750).
4. [CA SiteMinder® for Secure Proxy Server 환경을 구성합니다](#) (페이지 730).
5. [SiteMinder 환경을 구성합니다](#) (페이지 731).
6. [세션 보증 끝점을 생성합니다](#) (페이지 732).
7. 다음 목록에서 정책 모델에 적절한 단계를 선택합니다.
 - 정책 도메인의 경우 [끝점을 영역에 추가합니다](#) (페이지 734).
 - 응용 프로그램(EPM)의 경우 [끝점을 응용 프로그램 구성 요소에 추가합니다](#) (페이지 735).
8. CA SiteMinder® Federation 의 경우 [파트너 관계에서 고급 세션 보증을 활성화합니다](#) (페이지 736).

DeviceDNA™를 사용한 고급 세션 보증 제한 사항

DeviceDNA™를 사용한 고급 세션 보증은 다음 항목을 지원하지 *않습니다*.

Web 2.0 클라이언트

Web 2.0 응용 프로그램은 CA SiteMinder® for Secure Proxy Server 로 리디렉션할 수 없는 웹 요청을 생성하는 AJAX 등의 기술에 기반하여 구축됩니다. Web 2.0 클라이언트에는 비 브라우저 기반 클라이언트(예: 모바일 장치의 Flickr 클라이언트)가 포함되어 있습니다. 두 경우 모두 인증 흐름 응용 프로그램을 호스트하는 CA SiteMinder® for Secure Proxy Server 인스턴스로 리디렉션할 수 없는 요청이 발생할 수 있습니다. 이러한 상황으로 인해 DeviceDNA™를 사용한 고급 세션 보증은 Web 2.0 클라이언트에서 지원되지 않습니다. Web 2.0 응용 프로그램의 로그인 페이지를 보호할 수 있습니다. 하지만 AJAX 와 관련된 요청을 비롯한 일부 요청은 DeviceDNA™를 사용한 고급 세션 보증으로 보호할 수 없습니다.

사용자 지정 에이전트

SiteMinder SDK 로 생성한 에이전트는 DeviceDNA™를 사용한 고급 세션 보증을 지원하지 않습니다.

JavaScript 및 쿠키를 지원하지 않는 클라이언트

CA SiteMinder® for Secure Proxy Server 의 DeviceDNA™ 스크립트는 웹 클라이언트와 관련된 정보를 추출하는 JavaScript 입니다. 이 클라이언트 정보는 세션을 장치 또는 클라이언트와 연결합니다. JavaScript 에 대한 지원 없이는 DeviceDNA™를 수집할 수 없으므로 DeviceDNA™를 사용한 고급 세션 보증이 세션을 장치 또는 클라이언트와 연결할 수 없습니다. DeviceDNA™를 사용한 고급 세션 보증은 텔넷 또는 Lynx 같은 클라이언트에서 지원되지 않습니다.

POST 보존

DeviceDNA™를 사용한 고급 세션 보증은 CA SiteMinder® for Secure Proxy Server 의 인증 흐름 응용 프로그램에 대한 리디렉션을 사용하여 작동합니다. 이 응용 프로그램에는 DeviceDNA™ 스크립트가 포함되어 있습니다. 인증 흐름 응용 프로그램은 현재 POST 데이터를 지원하지 않습니다. 따라서 POST 요청이 인증 흐름 응용 프로그램으로 리디렉션되지 않습니다.

공유 워크스테이션

공유 워크스테이션에서는 모든 사용자의 DeviceDNA™ 서명이 동일합니다. 예를 들어 한 사용자가 유효한 SMSESSION 쿠키를 공유 워크스테이션의 다른 사용자로부터 가로챘다고 가정합니다. 가로챈 사용자가 훔친 SMSESSION 쿠키를 동일한 공유 워크스테이션에서 재생하는 경우 차이점이 감지되지 *않습니다*. DeviceDNA™를 사용한 고급 세션 보증은 가로챈 사용자가 훔친 SMSESSION 쿠키를 *다른* 장치에서 재생하려고 할 때 보호 기능을 제공합니다.

인증 및 권한 부여 웹 서비스

웹 서비스 클라이언트 응용 프로그램은 에이전트 API 호출에서 받은 리디렉션 또는 응답을 푸시하는 인증 및 권한 부여 웹 서비스를 처리합니다. 하지만 호출하는 클라이언트는 DeviceDNA™를 사용한 고급 세션 보증 흐름과 관련된 리디렉션을 처리할 수 *없습니다*.

CA SiteMinder® Federation

다음 구성은 DeviceDNA™를 사용한 고급 세션 보증을 지원하지 *않습니다*.

- SAML 2.0 파트너 관계의 SP 측
- 파트너 관계의 IdP 측에서 SAML 2.0 HTTP-POST 바인딩

에이전트 구성 매개 변수

다음 에이전트 구성 매개 변수는 DeviceDNA™를 사용한 고급 세션 보증을 지원하지 *않습니다*.

- SecureURL
- TargetAsRelativeURI

참고: DeviceDNA™를 사용한 고급 세션 보증을 사용하는 경우 이러한 매개 변수를 설정하지 마십시오. 이러한 매개 변수에 일반적으로 포함되는 대상 URL 은 DeviceDNA™를 사용한 고급 세션 보증에서 사용하는 토큰 요청에 이미 포함되어 있습니다.

응답 특성

다음 응답 특성은 DeviceDNA™를 사용한 고급 세션 보증을 지원하지 *않습니다*.

- OnAuthAccept

Windows 정책 서버 중지

계속하기 전에 정책 서버를 중지하십시오. 정책 서버를 중지하면 다음과 같은 결과가 발생합니다.

- 정책 서버가 사용 환경에서 일시적으로 제거됩니다.
- 권한 부여 또는 인증 결정이 필요한 에이전트가 중지된 정책 서버에 연결할 수 없게 됩니다. 이러한 에이전트는 사용 가능한 다른 정책 서버에 여전히 연결할 수 있습니다.
- 모든 로깅 작업이 중지됩니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.

참고: 관리자 권한이 있는 계정을 사용하십시오.

2. "시작", "프로그램", "SiteMinder", "SiteMinder 정책 서버 관리 콘솔"을 차례로 클릭합니다.
3. "중지" 단추를 클릭합니다.
4. "확인"을 클릭합니다.

정책 서버가 중지되고 콘솔이 닫힙니다.

UNIX 정책 서버 중지

정책 서버를 중지하면 다음과 같은 결과가 발생합니다.

- 정책 서버가 사용 환경에서 일시적으로 제거됩니다.
- 권한 부여 또는 인증 결정이 필요한 에이전트가 중지된 정책 서버에 연결할 수 없게 됩니다. 이러한 에이전트는 사용 가능한 다른 정책 서버에 여전히 연결할 수 있습니다.
- 모든 로깅 작업이 중지됩니다.

다음 단계를 수행하십시오.

1. 정책 서버를 원래 설치한 사용자 계정으로 정책 서버를 호스트하는 시스템에 로그인합니다.
2. 다음 작업 중 *하나*를 수행하여 모든 정책 서버 프로세스를 중지합니다.
 - 관리 콘솔을 열고 "상태" 탭을 클릭한 다음 "중지" 단추를 클릭합니다.
 - 다음 스크립트를 사용합니다. 이 스크립트는 UNIX 감독 기능도 중지하므로 프로세스가 자동으로 다시 시작되지 않습니다.

`installation_path/siteminder/stop-all`

정책 서버는 모든 UNIX 감독 기능 작업을

`installation_directory/log/smexec.log` 파일에 로깅합니다. 로그 항목은 항상 기존 로그 파일에 추가됩니다.

감사 저장소 업그레이드 스크립트

정책 서버를 중지한 후 데이터베이스 공급업체에 적절한 감사 저장소 업그레이드 스크립트를 실행하십시오. 다음 목록에서 스크립트를 선택하십시오.

- [Oracle 데이터베이스](#) (페이지 744)
- [Microsoft SQL Server 데이터베이스](#) (페이지 745)
- [IBM DB2 데이터베이스](#) (페이지 747)
- [MySQL 데이터베이스](#) (페이지 748)

Oracle 데이터베이스용 감사 저장소 업그레이드 스크립트 실행

정책 서버를 중지한 후에 감사 로그 스키마를 업그레이드하십시오. 이 업그레이드는 스크립트를 사용하여 수행됩니다.

다음 단계를 수행하십시오.

1. sqlplus 또는 다른 Oracle 유틸리티를 사용하여 정책 서버 데이터베이스 정보를 관리하는 사용자로 Oracle 데이터베이스에 로그인합니다.

참고: SYS 또는 SYSTEM 사용자로 CA SiteMinder 스키마를 업그레이드하지 않는 것이 좋습니다. 필요한 경우 SMOWNER 와 같은 Oracle 데이터베이스 사용자를 생성하고 이 사용자로 스키마를 업그레이드하십시오.

2. 12.5 에서 업그레이드하는 경우 다음 스크립트를 가져오십시오.

```
$NETE_PS_ROOT/db/SQL/sm_oracle_logs_upgrade_12.5_to_12.51.sql
```

3. 다음 스크립트를 가져옵니다.

```
$NETE_PS_ROOT/db/SQL/sm_oracle_logs_upgrade_12.51_to_12.52.sql
```

참고: 일부 환경 변수는 Oracle 이 제공하는 SQL 유틸리티에서 동작하지 않을 수 있습니다. 이 유틸리티를 사용하여 스크립트를 가져오는 동안 문제가 발생하면 명시적 경로를 지정하십시오.

감사 저장소 스키마가 업그레이드됩니다.

4. 다음 절차 중 *하나*를 사용하여 정책 서버를 시작합니다.
 - [Windows 운영 환경에서 정책 서버를 시작합니다](#) (페이지 749).
 - [UNIX/Linux 운영 환경에서 정책 서버를 시작합니다](#) (페이지 750).

Microsoft SQL Server 데이터베이스용 감사 저장소 업그레이드 스크립트 실행

정책 서버를 중지한 후에 감사 로그 스키마를 업그레이드하십시오. 이 업그레이드는 스크립트를 사용하여 수행됩니다.

다음 단계를 수행하십시오.

1. 다음 태스크 중 *하나*를 수행합니다.
 - 12.5 버전에서 업그레이드하는 경우 2 단계로 가십시오.
 - 12.51 버전에서 업그레이드하는 경우 10 단계로 가십시오.
 2. 텍스트 편집기에서 다음 파일을 엽니다.


```
installation_directory\db\SQL\sm_mssql_logs_upgrade_12.5_to_12.51.sql
```
 3. **installation_directory**
 4. 정책 서버가 설치된 파일 시스템의 위치를 지정합니다.
 5. 전체 파일의 내용을 복사합니다.
 6. 쿼리 분석기를 시작하고 정책 서버 데이터베이스를 관리하는 사용자로 로그인합니다.
 7. 데이터베이스 목록에서 데이터베이스 인스턴스를 선택합니다.
 8. **sm_mssql_logs_upgrade_12.5_to_12.51.sql** 파일의 스키마를 쿼리에 붙여 넣습니다.
 9. 쿼리를 실행합니다.
 10. 텍스트 편집기에서 다음 파일을 엽니다.


```
installation_directory\db\SQL\sm_mssql_logs_upgrade_12.51_to_12.52.sql
```

installation_directory

정책 서버가 설치된 파일 시스템의 위치를 지정합니다.
 11. 전체 파일의 내용을 복사합니다.
 12. 쿼리 분석기를 시작하고 정책 서버 데이터베이스를 관리하는 사용자로 로그인합니다.
 13. 데이터베이스 목록에서 데이터베이스 인스턴스를 선택합니다.
 14. **sm_mssql_logs_upgrade_12.51_to_12.52.sql** 파일의 스키마를 쿼리에 붙여 넣습니다.
 15. 쿼리를 실행합니다.
- 감사 저장소 스키마가 업그레이드됩니다.

16. 다음 절차 중 *하나*를 사용하여 정책 서버를 시작합니다.

- [Windows 운영 환경에서 정책 서버를 시작합니다](#) (페이지 749).
- [UNIX/Linux 운영 환경에서 정책 서버를 시작합니다](#) (페이지 750).

IBM DB2 데이터베이스용 감사 저장소 업그레이드 스크립트 실행

SiteMinder 감사 로그 스키마를 업그레이드합니다. 이 업그레이드는 스크립트를 사용하여 수행됩니다.

다음 단계를 수행하십시오.

1. 정책 서버를 호스트하는 시스템에 로그인합니다.
2. 다음 디렉터리로 이동합니다.

`installation_directory\db\tier2\DB2\`

`installation_directory`

정책 서버가 설치된 파일 시스템의 위치를 지정합니다.

3. 다음 태스크 중 *하나*를 수행합니다.
 - 12.5 버전에서 업그레이드하는 경우 4 단계로 가십시오.
 - 12.51 버전에서 업그레이드하는 경우 6 단계로 가십시오.
4. 다음 파일을 열고 내용을 텍스트 편집기에 복사합니다.

`sm_db2_log_upgrade_12.5_to_12.51.sql`

5. 내용을 쿼리에 붙여 넣고 쿼리를 실행합니다.

참고: 쿼리 실행에 대한 자세한 내용은 IBM 설명서를 참조하십시오.

감사 저장소 스키마가 업그레이드됩니다.

6. 다음 파일을 열고 내용을 텍스트 편집기에 복사합니다.

`sm_db2_log_upgrade_12.51_to_12.52.sql`

7. 내용을 쿼리에 붙여 넣고 쿼리를 실행합니다.

참고: 쿼리 실행에 대한 자세한 내용은 IBM 설명서를 참조하십시오.

감사 저장소 스키마가 업그레이드됩니다.

8. 다음 절차 중 *하나*를 사용하여 정책 서버를 시작합니다.
 - [Windows 운영 환경에서 정책 서버를 시작합니다](#) (페이지 749).
 - [UNIX/Linux 운영 환경에서 정책 서버를 시작합니다](#) (페이지 750).

MySQL 데이터베이스용 감사 저장소 업그레이드 스크립트 실행

SiteMinder 감사 로그 스키마를 업그레이드합니다. 이 업그레이드는 스크립트를 사용하여 수행됩니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 위치로 이동합니다.

`installation_directory\db\tier2\MySQL`

`installation_directory`

정책 서버가 설치된 파일 시스템의 위치를 지정합니다.

3. 다음 태스크 중 *하나*를 수행합니다.
 - 12.5 버전에서 업그레이드하는 경우 4 단계로 가십시오.
 - 12.51 버전에서 업그레이드하는 경우 9 단계로 가십시오.
4. 텍스트 편집기에서 다음 파일을 엽니다.

`sm_mysql_logs_upgrade_12.5_to_12.51.sql`

5. 다음 행을 찾습니다.

```
DROP FUNCTION IF EXISTS `databaseName`.`getdate` $$  
CREATE FUNCTION `databaseName`.`getdate` () RETURNS DATE
```

6. 'databaseName'의 각 인스턴스를 감사 저장소로 작동하는 데이터베이스의 이름으로 바꿉니다.
7. 전체 파일의 내용을 복사합니다.
8. 파일 내용을 쿼리에 붙여 넣고 쿼리를 실행합니다.
9. 텍스트 편집기에서 다음 파일을 엽니다.

`sm_mysql_logs_upgrade_12.51_to_12.52.sql`

10. 다음 행을 찾습니다.

```
DROP FUNCTION IF EXISTS `databaseName`.`getdate` $$  
CREATE FUNCTION `databaseName`.`getdate` () RETURNS DATE
```

11. 'databaseName'의 각 인스턴스를 감사 저장소로 작동하는 데이터베이스의 이름으로 바꿉니다.
 12. 전체 파일의 내용을 복사합니다.
 13. 파일 내용을 쿼리에 붙여 넣고 쿼리를 실행합니다.
- 감사 저장소 스키마가 업그레이드됩니다.

14. 다음 절차 중 *하나*를 사용하여 정책 서버를 시작합니다.

- [Windows 운영 환경에서 정책 서버를 시작합니다](#) (페이지 749).
- [UNIX/Linux 운영 환경에서 정책 서버를 시작합니다](#) (페이지 750).

Windows 정책 서버 시작

정책 서버를 시작합니다. 정책 서버를 시작하면 다음과 같은 결과가 발생합니다.

- 에이전트는 권한 부여 또는 인증 결정을 위해 정책 서버에 연결합니다.
- 로깅이 시작됩니다.

다음 단계를 수행하십시오.

1. "시작", "프로그램", "SiteMinder", "SiteMinder 정책 서버 관리 콘솔"을 차례로 클릭합니다.
"상태" 탭이 선택된 상태로 콘솔이 열립니다.
2. "시작" 단추를 클릭합니다.
3. "확인"을 클릭합니다.
정책 서버가 시작됩니다.

UNIX 정책 서버 시작

정책 서버를 시작하면 다음과 같은 결과가 발생합니다.

- 에이전트는 권한 부여 또는 인증 결정을 위해 정책 서버에 연결합니다.
- 로깅이 시작됩니다.

다음 작업 중 *하나*를 수행하여 모든 정책 서버 프로세스를 시작합니다.

- 관리 콘솔을 열고 "상태" 탭을 클릭한 다음 "시작" 단추를 클릭합니다.
- 다음 스크립트를 사용합니다. 이 스크립트는 UNIX 감독 기능도 시작합니다.

```
installation_path/siteminder/start-all
```

정책 서버는 모든 UNIX 감독 기능 작업을

`installation_directory/log/smexec.log` 파일에 로깅합니다. 로그 항목은 항상 기존 로그 파일에 추가됩니다.

DeviceDNA™를 사용한 고급 세션 보증을 위한 CA SiteMinder® for Secure Proxy Server 환경 구성

DeviceDNA™를 사용한 고급 세션 보증 기능을 사용하려면 CA SiteMinder® for Secure Proxy Server 가 작동해야 합니다.

1. 다음 태스크 중 *하나*를 수행합니다.

- CA SiteMinder® for Secure Proxy Server 가 설치되지 않은 경우 12.52 SP1 버전을 설치합니다.
- CA SiteMinder® for Secure Proxy Server 가 설치된 경우 12.52 SP1 로 업그레이드합니다.

참고: CA SiteMinder® for Secure Proxy Server 의 설치 및 업그레이드에 대한 자세한 내용은 CA SiteMinder® for Secure Proxy Server 관리 안내서를 참조하십시오. 또한 온라인에서 [설치 비디오](#)도 참조할 수 있습니다.

2. SSL 을 사용하도록 CA SiteMinder® for Secure Proxy Server 를 구성합니다.
3. CA SiteMinder® for Secure Proxy Server 와 정책 서버 사이에서 포트 번호 7658 을 엽니다.
4. CA SiteMinder® for Secure Proxy Server 설치 또는 업그레이드에서 고급 인증 서버 암호화 키를 기록합니다. 현재 환경의 SiteMinder 정책 서버에서 나중에 이 키가 필요합니다.
5. 여러 쿠키 도메인을 사용하는 싱글 사인온 환경의 경우 쿠키 공급자 도메인의 FQDN(정규화된 도메인 이름)이 필요합니다. 구성 마법사를 실행할 때 이 FQDN 을 ServerName 설정에 사용합니다. 예를 들어 쿠키 도메인이 sso.example.com 일 경우 CA SiteMinder® for Secure Proxy Server 구성 마법사에서 ServerName 의 값을 sso.example.com 으로 설정합니다.
6. CA SiteMinder® for Secure Proxy Server 에 대한 IgnoreExt 구성 매개 변수에 다음 값을 추가합니다.

.sac

7. 다음 단계에 따라 JVM 을 JSafeJCE 보안 공급자와 함께 구성하여 암호화를 사용하도록 설정합니다.
 - a. CA SiteMinder® for Secure Proxy Server 컴퓨터에 로그인합니다.
 - b. Oracle 웹 사이트에서 사용하는 Java 버전에 대한 "Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files" 패키지를 다운로드하십시오.
 - c. 다음 위치로 이동합니다.

Windows

`JVM_HOME\lib\security`

UNIX

`JVM_HOME/lib/security`

JVM_HOME

JRE(Java Runtime Environment)가 JDK에서 설치된 위치를 정의합니다.

- d. "JCE Unlimited Strength Jurisdiction Policy Files" 패키지의 파일을 사용하여 다음 파일을 패치하십시오.
 - local_policy.jar
 - US_export_policy.jarJVM 이 구성되었습니다.

DeviceDNA™를 사용한 고급 세션 보증을 위한 SiteMinder 환경 구성

DeviceDNA™를 사용한 고급 세션 보증을 사용하려면 SiteMinder 환경에서 일부 구성 요소 및 설정이 필요합니다.

다음 단계를 수행하십시오.

1. 정책 서버를 12.52 SP1 버전으로 설치하거나 업그레이드합니다.

참고: 이전 버전에서 업그레이드한 경우 환경에 있는 각 정책 서버에서 정책 서버 구성 마법사를 실행하십시오.
2. 세션 저장소가 없을 경우 세션 저장소를 하나 구성합니다.
3. 정책 서버와 CA SiteMinder® for Secure Proxy Server 사이에서 포트 번호 7658 을 엽니다.

DeviceDNA™를 사용한 고급 세션 보증 끝점 만들기

DeviceDNA™를 사용한 고급 세션 보증은 DeviceDNA™ 정보를 수집하기 위해 CA SiteMinder®for Secure Proxy Server 에서 호스트되는 인증 흐름 응용 프로그램 끝점으로 사용자를 자동 리디렉션합니다. 이러한 DeviceDNA™ 정보는 사용자 세션의 유효성을 검사합니다.

성능상의 이유로 인해 조직에서 각 지역마다 하나의 끝점을 만들 것을 권장합니다. 예를 들어, 뉴욕과 시카고에 사무소가 있는 경우 각 사무소마다 하나의 끝점을 만드십시오.

정책 또는 응용 프로그램에 DeviceDNA™를 사용한 고급 세션 보증을 추가하기 전에 CA SiteMinder®for Secure Proxy Server 에서 이러한 끝점을 구성하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에서 "정책", "전역", "세션 보증 끝점"을 클릭합니다.
2. "세션 보증 끝점 생성"을 클릭합니다.
3. 구체적인 이름과 설명(선택 사항)을 입력합니다.

4. 다음 필드를 작성하십시오.

웹 서버 이름

사용자를 인증하기 위해 DeviceDNA™를 수집하는 CA SiteMinder® for Secure Proxy Server 서버의 이름을 지정합니다.

Port(포트)

CA SiteMinder® for Secure Proxy Server 가 리디렉션을 위해 수신 대기하는 포트 번호를 지정합니다. 보안 연결(SSL 사용)을 사용하도록 이 포트를 구성하십시오.

기본값: 443

대상

사용자가 자동으로 리디렉션되는 CA SiteMinder® for Secure Proxy Server 의 URL 을 지정합니다. 이 서버는 사용자의 DeviceDNA™를 수집합니다. 제품은 이 DeviceDNA™를 사용하여 사용자와 관련된 세션의 유효성을 검사합니다.

DeviceDNA™ 새로 고침 간격

사용자와 관련된 DeviceDNA™가 유효한 상태로 유지되는 기간(초)을 지정합니다. 올바른 DeviceDNA™가 없는 사용자는 고급 세션 보증 끝점으로 리디렉션되고, 여기서 서버가 사용자에 대한 현재 DeviceDNA™를 획득합니다.

DeviceDNA™ 새로 고침 간격은 DeviceDNA™의 수집에 적용됩니다. DeviceDNA™ 새로 고침 간격이 만료된 후 발생하는 모든 요청은 DeviceDNA™를 수집하기 위해 인증 흐름 응용 프로그램으로 리디렉션됩니다.

DeviceBinder 는 세션과 관련된 사용자를 식별하는 세션 속성입니다. DeviceBinder 및 클라이언트 쪽 장치 ID 는 인증 프로세스 중 연결되었습니다. 고유 DeviceHash 및 만료 시간이 이 속성을 구성합니다.

기본값: 300 초(5 분)

5. 제출을 클릭합니다.

영역에 끝점 추가

DeviceDNA™를 사용한 고급 세션 보증을 사용하여 영역에 있는 리소스를 보호하려면 이 영역에 하나의 세션 보증 끝점을 추가하십시오.

참고: DeviceDNA™를 사용한 고급 세션 보증이 작동하기 위해 영역이 영구적일 필요는 없습니다.

다음 단계를 수행하십시오.

1. 관리 UI 에서 "정책", "도메인", "영역"을 차례로 클릭합니다.
2. 원하는 영역의 편집 아이콘을 클릭합니다.
3. "세션" 아래에서 "고급 세션 보증" 옆의 "사용" 확인란을 클릭합니다.
4. "끝점 조회"를 클릭합니다.
5. 원하는 끝점을 선택합니다.
6. "확인"을 클릭합니다.
7. 제출을 클릭합니다.
8. 세션 보증 기능을 사용하여 보호할 리소스가 있는 기타 영역에 대해 2 - 6 단계를 반복합니다.

응용 프로그램 구성 요소에 끝점 추가

DeviceDNA™를 사용한 고급 세션 보증을 사용하여 응용 프로그램의 구성 요소를 보호하려면 고급 세션 보증 끝점 *하나*를 관련 응용 프로그램의 구성 요소에 추가하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에서 "정책", "응용 프로그램"을 클릭합니다.
응용 프로그램 목록이 나타납니다.
2. 원하는 응용 프로그램의 편집 아이콘을 클릭합니다.
"응용 프로그램 수정:" 대화 상자가 표시됩니다.
3. 다음 단계 중 *하나*를 수행합니다.
 - 응용 프로그램에 단 하나의 구성 요소만 있는 경우 "고급 설정"을 클릭하십시오.
 - 응용 프로그램에 여러 구성 요소가 있는 경우 원하는 구성 요소의 편집 아이콘을 클릭하십시오. "고급 설정"을 클릭하십시오.
4. "세션" 아래에서 "고급 세션 보증" 옆의 "사용" 확인란을 선택합니다.
5. "끝점 조회"를 클릭합니다.
끝점의 목록이 표시됩니다.
6. 원하는 끝점을 선택합니다.
7. "확인"을 클릭합니다.
8. 제출을 클릭합니다.
"응용 프로그램 수정" 대화 상자가 닫히고 확인 메시지가 표시됩니다.
9. 세션 보증 기능을 사용하여 보호할 리소스가 있는 기타 응용 프로그램에 대해 2 - 7 단계를 반복합니다.

파트너 관계에서 DeviceDNA™를 사용한 고급 세션 보증 활성화

CA SiteMinder® Federation 를 사용하는 경우 다음 파트너 관계에서 DeviceDNA™를 사용한 고급 세션 보증을 활성화할 수도 있습니다.

- SP-IdP 파트너 관계의 IdP 측(HTTP-리디렉션 바인딩만 해당)
- 소비자-생산자 파트너 관계의 생산자 측
- RP-AP 파트너 관계의 AP 측

다음 단계를 수행하십시오.

1. 관리 UI 에서 "페더레이션", "파트너 관계 페더레이션", "파트너 관계"를 클릭합니다.
2. 원하는 파트너 관계의 왼쪽에 있는 "작업" 단추를 클릭한 다음 "비활성화"를 클릭합니다.
3. 동일한 "작업" 단추를 다시 클릭한 다음 "수정"을 선택합니다.
4. "SSO 및 SLO" 탭을 클릭합니다.
5. 다음 확인란을 클릭합니다.

세션 보증 사용

영역(정책 도메인 모델) 또는 구성 요소(응용 프로그램 모델)에 지정된 리소스를 보호합니다. 특정 CA SiteMinder® Federation 파트너 관계의 인증 요청을 보호할 수도 있습니다. 세션 보증 끝점은 사용자로부터 DeviceDNA™를 수집하여 세션의 유효성을 검사합니다.

제한: 이 기능은 세션 보증 끝점이 필요합니다.

끝점의 목록이 표시됩니다.

6. 원하는 끝점의 확인란을 클릭합니다.
7. "저장"을 클릭합니다.
8. 원하는 다른 파트너 관계에 대해 2 - 7 단계를 반복합니다.
9. (로컬 인증 모드만 해당) 인증 URL(Redirect.jsp)과 연결되는 영역에서 DeviceDNA™를 사용한 고급 세션 보증을 활성화합니다.

SM--Related 로그 파일

"DeviceDNA™를 사용한 고급 세션 보증"과 관련된 트랜잭션은 다음 로그 파일에 기록됩니다.

정책 서버

xps-*.audit - 이 기능의 구성 설정에 대한 변경 사항

smaccesslog4 - 이 기능과 관련된 인증 및 권한 부여 작업

고급 인증 서버에 대한 시작 로그:

caauthminderstartup

cariskminderstartup

cariskmindercasemgmtserverstartup

고급 인증 서버에 대한 런타임 로그:

caauthminder

cariskminder

cariskmindercasemgmtserver

CA SiteMinder® for Secure Proxy Server 서버(고급 인증 흐름 응용 프로그램)

arcotuds.log - UDS 서비스에 대한 로그 파일

CAWebFlowLog.txt - 인증 흐름 응용 프로그램에 대한 로그 파일

UIApplog.txt - UIApp(인증 흐름 응용 프로그램 실행 프로세스의 일부)에 대한 로그

제 24 장: SiteMinder 테스트 도구

이 섹션은 다음 항목을 포함하고 있습니다.

[테스트 도구 개요](#) (페이지 759)

[테스트 환경 에이전트 구성](#) (페이지 760)

[기능 테스트 실행](#) (페이지 772)

[명령 스크립트 파일에 기록된 테스트를 재생하여 재발 테스트 수행](#) (페이지 777)

[스트레스 테스트 실행](#) (페이지 778)

[인증서 기반 인증 테스트](#) (페이지 785)

테스트 도구 개요

SiteMinder 테스트 도구는 에이전트와 정책 서버 간의 상호 작용을 시뮬레이트하는 유틸리티로, 정책 서버의 기능을 테스트합니다. 테스트 중 테스트 도구는 에이전트의 역할을 하여 실제 에이전트와 동일하게 정책 서버에 요청합니다. 따라서 SiteMinder 구성을 배포하기 전에 테스트할 수 있습니다.

SiteMinder 테스트 도구는 Windows 시스템에서만 사용할 수 있습니다. 테스트 도구를 사용하면 Windows 기반 웹 에이전트와 RADIUS 에이전트를 제한 없이 애플레이트할 수 있습니다. SiteMinder 테스트 도구는 모든 플랫폼의 정책 서버에 연결할 수 있지만, Solaris 에서 실행되는 4.x 이후 버전 웹 에이전트는 SiteMinder 테스트 도구를 사용하여 테스트할 수 없습니다. SiteMinder 5.x 이상의 웹 에이전트에 대해 정책을 테스트하려면 다음 작업 중 하나를 수행하십시오.

- Perl 스크립팅 인터페이스를 사용하여 웹 에이전트를 등록하고 테스트합니다.
- SiteMinder 웹 에이전트를 설치 및 구성하고 수동으로 테스트합니다.

SiteMinder 테스트 도구는 다음 세 가지 유형의 테스트를 수행합니다.

기능 테스트

정책을 테스트하여 올바르게 구성되었는지 확인합니다.

재발 테스트

정책 저장소 마이그레이션이나 새로운 기능 구현과 같은 변경 내용이 SiteMinder 에 영향을 주는지 여부를 테스트합니다.

스트레스 테스트

많은 요청이 정책 서버로 수신될 때의 정책 서버 성능을 테스트합니다.

참고: 스크립팅 인터페이스를 사용하여 정책을 테스트할 수도 있습니다. Programming Guide for Perl(Perl 프로그래밍 안내서)을 참조하십시오.

테스트 환경 에이전트 구성

"SiteMinder 에이전트" 그룹 상자에서 테스트 도구가 테스트 중에 시뮬레이트하는 에이전트를 구성할 수 있습니다.

테스트 도구가 시뮬레이트하는 에이전트는 관리 UI 에서 구성해야 합니다.

에이전트 정보를 구성하려면 다음 옵션을 지정하십시오.

에이전트 유형

다음 에이전트 유형 중 하나를 지정합니다.

버전 4

SiteMinder 4.x 에이전트를 시뮬레이트합니다.

버전 5

SiteMinder 5.x 에이전트를 시뮬레이트합니다.

참고: 시스템에서 테스트 도구를 사용하여 SiteMinder 5.x 웹 에이전트를 시뮬레이트하려면 해당 시스템에서 smreghost.exe 응용 프로그램을 실행해야 합니다. smreghost.exe 파일은 웹 에이전트에 포함되어 있으며 웹 에이전트 설치 안내서에 설명되어 있습니다. 이 파일은 <Policy Server install dir>/siteminder/bin 에도 있습니다.

RADIUS

RADIUS 장치를 시뮬레이트합니다.

에이전트 이름

관리 UI 에 표시되는 에이전트 이름을 입력합니다. 이 필드는 버전 4 및 버전 5 에이전트 시뮬레이션 모두에 대해 필수입니다.

암호

에이전트의 공유 암호를 입력합니다. 에이전트를 생성할 때 입력한 공유 암호와 일치해야 합니다. "암호"는 버전 4 및 RADIUS 에이전트 시뮬레이션 모두에 대해 필수입니다.

(선택 사항) 서버

에이전트가 있는 서버의 전체 이름을 입력합니다. 예를 들어 정책 서버에서 `http://www.myorg.org` 를 테스트하려면 이 필드에 `www.myorg.org` 를 입력합니다. 이 필드는 버전 4 에이전트 시뮬레이션에 사용될 수 있습니다.

SmHost.conf 경로

시뮬레이트할 버전 5 에이전트에 대한 설정이 포함된 `SmHost.conf` 파일의 경로를 입력합니다. "찾아보기" 단추를 사용하여 `SmHost.conf` 파일을 검색할 수 있습니다.

Windows 에서 테스트 도구 시작

정책 서버 기능을 테스트하려면 테스트 도구를 시작하십시오.

중요! Windows Server 2008 에서 테스트 도구에 액세스하려면 관리자 권한으로 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

다음 단계를 수행하십시오.

다음 방법 중 하나를 사용하십시오.

- SiteMinder 프로그램 그룹에서 SiteMinder 테스트 도구를 선택합니다.
- 명령 창에서 `policy_server_home\bin` 으로 이동하고 다음 명령을 입력합니다.

```
smttest
```

UNIX 에서 테스트 도구 시작

정책 서버 기능을 테스트하려면 테스트 도구를 시작하십시오.

다음 단계를 수행하십시오.

1. 명령 창을 열고 `policy_server_home/bin` 으로 이동합니다.
2. 다음 명령을 입력합니다.

```
./smtest
```

참고: UNIX 에서 테스트 도구를 실행하려면 X 디스플레이 서버가 실행 중이어야 합니다. 필요한 경우 명령 창에 다음을 입력하여 이 디스플레이를 사용하도록 설정하십시오.

```
export DISPLAY=n.n.n.n:0.0  
n.n.n.n
```

정책 서버 호스트 시스템의 IP 주소를 지정합니다.

FIPS 전용 환경에서 테스트 도구를 사용하는 방법

FIPS 마이그레이션 또는 FIPS 전용 모드로 구성된 정책 서버는 AES(Advanced Encryption Standard) 알고리즘을 사용하여 중요한 데이터를 암호화합니다. [대화형](#) (페이지 768) 테스트를 실행 중인 경우 테스트 도구는 필요에 따라 FIPS 호환 알고리즘을 사용하여 FIPS 전용 모드 정책 서버와 통신합니다.

그러나 기본적으로 테스트 도구는 [기록](#) (페이지 768) 모드에서 명령 스크립트 파일을 생성할 때 중요한 데이터를 암호화하는 데 FIPS 호환 알고리즘을 사용하지 *않습니다*. 따라서 비 FIPS 알고리즘으로 암호화된 데이터가 포함된 명령 스크립트는 FIPS 전용 모드 정책 서버를 테스트하기 위해 재생할 수 없습니다.

FIPS 마이그레이션 또는 FIPS 전용 모드 정책 서버에 대해 테스트를 기록하고 재생하려면 다음 절차 중 하나를 수행하십시오.

- [명령줄 옵션을 사용하여 특정 FIPS 모드에서 테스트 도구 시작](#)
(페이지 763)
- [CA SM PS FIPS140 환경 변수를 설정하여 기본 FIPS 모드 정의](#)
(페이지 765)

참고: 명령줄 옵션을 사용해도 테스트 도구가 시작되지 않는 경우 CA_SM_PS_FIPS140 환경 변수에 정의된 FIPS 모드가 사용됩니다. CA_SM_PS_FIPS140 이 설정되지 않은 경우 테스트 도구는 기본적으로 FIPS 호환 모드를 사용합니다.

명령줄 옵션을 사용하여 특정 FIPS 모드에서 테스트 도구 시작

특정 FIPS 모드에서 테스트 도구를 열어 기록 또는 재생하려면 **-cf** 명령줄 옵션을 사용하여 테스트 도구를 시작하십시오.

다음 단계를 수행하십시오.

1. 명령 창을 열고 다음 위치 중 하나로 이동합니다.
 - `policy_server_home\bin(Windows)`
 - `policy_server_home/bin(UNIX)`
2. 다음 명령을 입력합니다.

```
smtest -cf FIPSmode [command_script]
```

FIPSmode

정책 서버의 FIPS 모드와 일치하도록 다음 FIPS 모드 중 하나를 지정합니다.

- COMPAT(기본값)
- MIGRATE
- ONLY

참고: *FIPSmode* 값은 대/소문자를 구분하지 않습니다.

command_script

(선택 사항) 재생할 명령 스크립트 파일의 경로 이름을 지정합니다.

각 *FIPSmode* 설정에 대해 테스트 도구는 다음과 같이 동작합니다.

COMPAT

다음과 같은 방식으로 작동하도록 테스트 도구를 구성합니다.

- 명령 스크립트 파일을 기록할 때 비 **FIPS** 알고리즘을 사용하여 중요한 데이터를 암호화합니다.
- 테스트를 재생할 때 비 **FIPS** 또는 **FIPS** 알고리즘을 사용하여 명령 스크립트 파일에 기록된 중요한 데이터의 암호를 해독합니다.

MIGRATE

다음과 같은 방식으로 작동하도록 테스트 도구를 구성합니다.

- 명령 스크립트 파일을 기록할 때 **FIPS** 알고리즘을 사용하여 중요한 데이터를 암호화합니다.
- 테스트를 재생할 때 비 **FIPS** 또는 **FIPS** 알고리즘을 사용하여 명령 스크립트 파일에 기록된 중요한 데이터의 암호를 해독합니다.

ONLY

다음과 같은 방식으로 작동하도록 테스트 도구를 구성합니다.

- 명령 스크립트 파일을 기록할 때 **FIPS** 알고리즘을 사용하여 중요한 데이터를 암호화합니다.
- "기본 재생" 또는 "고급 재생" 모드에서 테스트를 재생할 때 **FIPS** 알고리즘만 사용하여 명령 스크립트 파일에 기록되는 중요한 데이터의 암호를 해독합니다.

CA_SM_PS_FIPS140 환경 변수를 설정하여 기본 FIPS 모드 정의

CA_SM_PS_FIPS140 환경 변수를 정의하여 테스트 도구 및 다른 로컬 SiteMinder 구성 요소의 기본 FIPS 모드를 구성하십시오.

참고: -cf 명령줄 옵션을 사용하여 테스트 도구가 시작된 경우에는 CA_SM_PS_FIPS140 환경 변수가 무시됩니다.

다음 단계를 수행하십시오.

1. 다음 단계 중 하나를 완료하십시오.

- (Windows) 관리 UI 호스트 시스템에 관리 사용자로 로그인합니다.
- (UNIX) 관리 UI 호스트 시스템에 관리 UI 를 설치한 사용자로 로그인합니다.

2. 다음 환경 변수를 설정합니다.

CA_SM_PS_FIPS140=*FIPSmode*

FIPSmode

정책 서버의 FIPS 모드와 일치하도록 다음 FIPS 모드 중 하나를 지정합니다.

- COMPAT(기본값)
- MIGRATE
- ONLY

참고: 환경 변수 설정에 대한 자세한 내용은 해당 OS 설명서를 참조하십시오.

3. 관리 UI 를 실행하는 Windows 또는 UNIX 셸이 CA_SM_PS_FIPS140 변수를 올바르게 인식하는지 확인합니다.

각 *FIPSmode* 환경 설정에 대해 테스트 도구는 다음과 같이 동작합니다.

COMPAT

다음과 같은 방식으로 작동하도록 테스트 도구를 구성합니다.

- 명령 스크립트 파일을 기록할 때 비 FIPS 알고리즘을 사용하여 중요한 데이터를 암호화합니다.
- 테스트를 재생할 때 비 FIPS 또는 FIPS 알고리즘을 사용하여 명령 스크립트 파일에 기록된 중요한 데이터의 암호를 해독합니다.

MIGRATE

다음과 같은 방식으로 작동하도록 테스트 도구를 구성합니다.

- 명령 스크립트 파일을 기록할 때 FIPS 알고리즘을 사용하여 중요한 데이터를 암호화합니다.
- 테스트를 재생할 때 비 FIPS 또는 FIPS 알고리즘을 사용하여 명령 스크립트 파일에 기록된 중요한 데이터의 암호를 해독합니다.

ONLY

다음과 같은 방식으로 작동하도록 테스트 도구를 구성합니다.

- 명령 스크립트 파일을 기록할 때 FIPS 알고리즘을 사용하여 중요한 데이터를 암호화합니다.
- 테스트를 재생할 때 비 FIPS 또는 FIPS 알고리즘을 사용하여 명령 스크립트 파일에 기록된 중요한 데이터의 암호를 해독합니다.

정책 서버 식별

테스트 도구를 실행하려면 "SiteMinder 에이전트" 그룹 상자에 지정된 에이전트와의 상호 작용을 시뮬레이트할 때 사용할 정책 서버에 대한 정보가 필요합니다. 선택한 에이전트 유형에 따라 필요한 정보가 조금씩 다릅니다.

버전 4 에이전트 및 RADIUS 에이전트 시뮬레이션을 위한 정책 서버 설정

버전 4 에이전트 및 RADIUS 에이전트 시뮬레이션을 실행하려면 테스트에 사용할 정책 서버의 IP 주소 및 포트 정보를 지정해야 합니다. 여러 정책 서버 환경을 시뮬레이트하려는 경우 정책 서버의 작동 방식을 지정할 수 있습니다.

버전 4 에이전트 및 RADIUS 에이전트 시뮬레이션을 위해 정책 서버를 설정하려면

1. 필요에 따라 다음 정책 서버 옵션을 지정합니다.

정책 서버

지정하는 정책 서버가 주 정책 서버인지, 보조 정책 서버인지를 나타냅니다.

IP 주소

정책 서버의 IP 주소를 지정합니다. 기본적으로 이 필드에는 로컬 시스템의 IP 주소가 들어 있습니다.

권한 부여 포트, 인증 포트, 계정 포트

권한 부여, 인증 및 계정 설정 요청에 사용되는 TCP 포트를 지정합니다. 이러한 필드는 정책 서버의 기본 포트 번호로 채워져 있습니다.

시간 만료

테스트 도구가 정책 서버의 응답을 기다려야 하는 시간(초)을 표시합니다.

2. 다음 작동 모드 중 하나를 선택합니다.

장애 조치

장애 조치를 사용합니다. 장애 조치 중에 테스트 도구는 요청을 초기 정책 서버로 보냅니다. 초기 정책 서버가 실패하면 테스트 도구는 요청을 보조 정책 서버로 리디렉션합니다.

라운드 로빈

라운드 로빈 부하 분산을 사용합니다. 라운드 로빈 부하 분산은 요청을 주 정책 서버와 보조 정책 서버로 분산합니다. 각 연결에 대해 테스트 도구는 두 정책 서버에 번갈아 연결합니다.

3. "연결"을 클릭하여 테스트 도구가 정책 서버에 연결할 수 있는지 확인합니다.

테스트 도구가 연결되면 IsProtected 및 DoManagement 표시등이 녹색으로 바뀝니다.

참고: 정책 서버 연결을 테스트하기 전에 에이전트를 지정해야 합니다.

버전 5 에이전트에 필요한 정책 서버 정보

버전 5 에이전트를 시뮬레이트하려는 경우 테스트에 사용할 정책 서버의 IP 주소 및 포트 정보를 지정하거나 정책 저장소의 호스트 구성 개체에 포함된 정책 서버 정보를 사용할 수 있습니다.

기본적으로 테스트 도구가 SmHost.conf 파일을 사용하여 정책 서버에 대한 초기 연결을 설정할 때는 정책 저장소에서 정책 서버 정보가 검색됩니다. 정책 서버 정보를 수동으로 지정하려면 "무시" 확인란을 선택하고 [버전 4 에이전트 및 RADIUS 에이전트 시뮬레이션을 위한 정책 서버 설정](#) (페이지 766)에 설명된 대로 정책 서버 정보를 입력합니다.

"SiteMinder 에이전트" 그룹 상자에서 테스트 도구가 테스트 중에 시뮬레이트하는 에이전트를 구성할 수 있습니다.

테스트 모드 선택

다음 목록에 나온 테스트 모드 중 하나를 사용하여 테스트 실행 및 결과 표시 방식을 결정하십시오. 선택하는 테스트 모드에 따라 스크립트 정보를 지정해야 할 수도 있습니다.

Interactive(대화형)

데이터를 입력하고, 테스트를 실행하고, "서버 응답" 섹션에 바로 표시되는 결과를 볼 수 있습니다.

Record(기록) (페이지 774)

테스트 결과를 일반 텍스트 명령 스크립트 파일에 기록하는 스크립트 생성 기능과 대화형 작업을 결합합니다.

기본 재생 (페이지 777)

"기록" 모드에서 생성된 명령 스크립트 파일을 사용하여 일련의 테스트를 자동화합니다. 재발 테스트에 적합합니다.

Advanced Playback(고급 재생) (페이지 781)

수동으로 구성된 스레드 제어 파일을 사용하여 복잡한 테스트를 자동화합니다. 스트레스 테스트에 적합합니다.

리소스 정보 지정

테스트를 수행할 대상 리소스를 지정할 수 있습니다. 리소스를 제공하면 브라우저에서 URL 을 입력하는 사용자가 시뮬레이트됩니다.

리소스 정보를 지정하려면 다음 옵션의 값을 제공하십시오.

Resource

영역에 구성되어 있고 SiteMinder 가 보호하고 있는 리소스의 상대 경로를 입력합니다. 이 경로는 웹 서버 게시 디렉터리에 상대적인 경로(예: /protected/)입니다.

작업

테스트하려는 규칙에 지정된 에이전트 작업, 인증 이벤트 또는 권한 부여 이벤트를 입력합니다.

"SiteMinder 에이전트" 그룹 상자에서 테스트 도구가 테스트 중에 시뮬레이트하는 에이전트를 구성할 수 있습니다.

사용자 자격 증명 지정

정책을 통해 사용자를 인증하거나 권한을 부여할 수 있는지 여부를 테스트하려면 테스트 도구에 사용자 자격 증명을 제공해야 합니다.

사용자 자격 증명을 지정하려면 다음 필드를 채워주세요.

사용자 이름

리소스에 액세스하는 데 사용할 사용자 이름을 입력합니다.

Password

"사용자 이름"에 입력한 사용자의 암호를 입력합니다.

CHAP Password(CHAP 암호)

RADIUS CHAP 인증 체계를 사용할 경우 이 확인란을 선택합니다.

Certificate File(인증서 파일)

보호된 리소스에 대한 사용자 인증을 위해 인증서가 필요한 경우 테스트 도구가 인증서 인증을 시뮬레이트할 수 있도록 인증서 파일을 제공해야 합니다.

"SiteMinder 에이전트" 그룹 상자에서 테스트 도구가 테스트 중에 시뮬레이트하는 에이전트를 구성할 수 있습니다.

인코딩 사양 설정

인코딩 사양 필드에 언어 인코딩 매개 변수를 지정할 수 있습니다. 테스트 도구는 이 매개 변수를 사용하여 웹 에이전트와 동일한 방식으로 헤더를 인코딩한 후 인코딩된 응답 특성 데이터를 "특성" 필드에 표시합니다.

언어 인코딩에 대한 자세한 내용은 "웹 에이전트 구성 안내서"를 참조하십시오.

인코딩 사양을 설정하려면 다음과 같이 인코딩 사양 값을 입력하십시오.

encoding_spec, wrapping_spec

설명:

- encoding_spec 은 UTF-8, Shift-JIS, EUC-J 또는 ISO-2022 JP 인코딩 유형 중 하나를 나타내는 텍스트 문자열입니다.
- wrapping_spec 은 래핑 사양으로, RFC-2047 이어야 합니다.

참고: 이 필드를 비워 둘 경우 기본값은 래핑을 사용하지 않는 UTF-8 입니다.

"SiteMinder 에이전트" 그룹 상자에서 테스트 도구가 테스트 중에 시뮬레이트하는 에이전트를 구성할 수 있습니다.

테스트 도구 설정 파일에 테스트 구성 저장 및 로드

에이전트, 리소스, 사용자 정보 등 사용자가 제공한 정보를 다시 입력할 필요가 없도록 이러한 값을 테스트 도구 설정 파일에 저장할 수 있습니다. 그런 다음 이러한 값을 언제든지 다시 로드할 수 있습니다.

테스트 도구에서 지정된 현재 값을 저장하려면

1. "설정 저장" 단추를 클릭합니다.
2. "다른 이름으로 저장" 대화 상자에서 테스트 도구 설정의 위치와 이름을 입력하고 "저장"을 클릭합니다.

파일이 .ini 파일 확장명으로 저장됩니다.

테스트 도구 설정 파일에서 저장된 값을 검색하려면

1. "설정 로드" 단추를 클릭합니다.
2. "열기" 대화 상자에서 테스트 도구 설정 파일의 위치와 이름을 입력하고 "열기"를 클릭합니다.

참고: 명령 스크립트에서 테스트 도구 설정 파일을 로드할 수도 있습니다.

(선택 사항) 정책 서버에 대한 테스트 도구 연결 조정

테스트 도구 설정 파일(.ini)을 편집하고 다음 매개 변수를 추가하여 테스트 도구가 정책 서버에 연결하는 방식을 조정하십시오.

MaxConnections:

테스트 도구가 정책 서버에 대해 설정할 수 있는 최대 연결 수를 지정합니다.

MinConnections:

테스트 도구가 정책 서버에 대해 설정할 수 있는 최소 연결 수를 지정합니다.

ConnectionsStep:

새 연결을 설정해야 하는 경우 테스트 도구가 한 번에 열 수 있는 새 소켓 수를 지정합니다(최대값: MaxConnections 에 지정된 값).

다음 단계를 수행하십시오.

1. 명령 스크립트 파일에서 "SM Agent or Radius:" 매개 변수의 값을 확인하고 다음 단계 중 하나를 수행합니다.
 - "SM Agent or Radius" 값이 **SM Agent v4** 로 설정되어 있는 경우 3 단계로 진행합니다.
 - "SM Agent or Radius" 값이 **SM Agent v5** 로 설정되어 있는 경우 명령 스크립트 파일에 값이 **1** 인 "Override Bootstrap:" 매개 변수를 추가합니다.
2. 명령 스크립트 파일의 "Agent Name" 매개 변수 값이 테스트 도구 설정 파일의 "Agent name" 매개 변수와 동일한지 확인합니다. 동일하지 않은 경우 새 매개 변수가 무시되고 기본값 MaxConnections=20 및 ConnectionStep=2 가 사용됩니다.
3. 텍스트 편집기에서 테스트 도구 설정 파일을 엽니다.
4. 파일의 다른 매개 변수와 동일한 형식을 사용하여 필수 매개 변수를 해당 하나씩 추가합니다. 즉, 행의 24 열부터 매개 변수 값을 입력합니다.
5. 테스트 도구 설정 파일을 저장하고 닫습니다.

기능 테스트 실행

SiteMinder 테스트 도구를 사용하면 실제 환경을 시뮬레이트한 환경에서 정책 기능을 테스트할 수 있습니다. 기능 테스트를 수행하려면 다음 조건이 충족되어 있어야 합니다.

- 정책 서버가 구성되어 있고 실행 중입니다.
- SiteMinder 에이전트가 관리 UI에 구성되어 있습니다.

참고: 테스트 도구를 사용하여 SiteMinder 에이전트 v5.x를 시뮬레이트할 경우 에이전트에 4.x 지원이 사용되도록 설정되어 있어야 합니다.

- 정책 도메인에 사용자 디렉터리(유형은 관계없음)가 구성되어 있습니다.
- 규칙과 사용자를 연결하는 정책이 있습니다.

SiteMinder에서는 다음 기능 테스트를 수행할 수 있습니다.

IsProtected

지정된 리소스가 정책을 통해 보호되고 있는지 여부를 나타냅니다.

IsAuthenticated

정책 서버가 사용자 디렉터리에 대해 사용자 자격 증명 집합을 인증할 수 있는지 여부를 나타냅니다.

사용자 자격 증명에 인증되면 정책 서버는 이 자격 증명을 사용자 디렉터리의 항목과 비교합니다. 자격 증명에 항목과 일치하면 정책 서버는 세션 티켓을 만들고 사용자를 인증합니다.

"실제" SiteMinder 배포 환경에서는 인증된 사용자가 추가 요청을 하면 SiteMinder가 디렉터리에 대해 사용자 자격 증명을 다시 확인하는 대신 사용자의 세션 티켓이 유효한지 확인합니다. 기본적으로 테스트 도구는 사용자가 세션 티켓을 가지고 있는지 여부에 관계없이 IsAuthenticated 테스트가 실행될 때마다 사용자를 인증합니다.

IsAuthenticated 테스트를 실행하기 전에 테스트 도구의 "설명" 필드에 "유효성 검사"를 입력하여 테스트 도구가 사용자 세션 티켓의 유효성을 검사하도록 구성할 수 있습니다. 하지만 세션 티켓의 유효성을 검사하려면 먼저 SiteMinder가 사용자를 인증해야 합니다.

참고: "Interactive"(대화형) 모드("반복 횟수" 필드 사용) 및 "Playback"(재생) 모드로 테스트를 여러 개 실행할 경우 "유효성 검사"를 지정할 수 있습니다.

IsAuthorized

정책 서버가 정책을 기반으로 사용자에게 권한을 부여할 수 있는지 여부를 나타냅니다.

이러한 테스트는 위에 나온 순서대로 실행해야 합니다. 예를 들어 **IsProtected** 를 **IsAuthenticated** 보다 먼저 실행해야 합니다. 이 순서는 **SiteMinder** 가 사용자의 액세스 권한을 확인하기 위해 사용하는 단계를 반영합니다.

기능 테스트를 실행하는 동안 테스트 도구를 사용하여 다음 태스크를 수행할 수도 있습니다.

DoAccounting

가장 최근의 계정 서버 트랜잭션을 로깅합니다.

DoManagement

에이전트 캐시를 지우는 캐시 플러시 명령 등의 에이전트 명령을 요청합니다. **DoManagement** 를 실행하면 테스트 도구가 정책 서버에서 최신 정보를 받을 수 있습니다.

기능 테스트를 실행하려면

1. 테스트 환경을 구성합니다.

참고: 스크립팅 인터페이스를 사용하여 정책을 테스트할 수도 있습니다. *Programming Guide for Perl*(Perl 프로그래밍 안내서)을 참조하십시오.

2. (선택 사항) "명령" 그룹 상자의 "반복 횟수" 필드에서 원하는 테스트 실행 횟수를 지정합니다.
3. "명령" 그룹 상자에서 다음 중 실행할 테스트를 하나 선택합니다.
 - **IsProtected**
 - **IsAuthenticated**
 - **IsAuthorized**
4. **IsAuthenticated** 테스트를 실행하려고 하며, 테스트 도구에서 사용자 디렉터리에 대해 사용자 자격 증명을 인증하는 대신 인증된 사용자의 세션 티켓이 유효한지 검사하려면 "설명" 필드에 "유효성 검사"를 입력합니다.

참고: 사용자 세션 티켓의 유효성을 검사하려면 먼저 사용자가 인증되어야 합니다. 사용자가 인증되면 **SiteMinder** 는 해당 사용자의 세션 티켓을 생성합니다.

(선택 사항) 재발 및 스트레스 테스트를 위해 명령 스크립트 파일에 테스트 기록

"기록" 모드에서 테스트를 실행하는 경우 테스트 도구는 테스트 명령과 테스트 결과를 일반 텍스트 명령 스크립트 파일에 기록합니다. 이 파일은 나중에 재생 모드로 테스트를 반복할 때 입력 파일로 사용할 수 있습니다.

여러 테스트를 동일한 명령 스크립트 파일에 기록할 수 있습니다. 테스트 결과는 파일의 끝에 추가됩니다. 그런 다음 재발 테스트에 이 스크립트 파일을 사용할 수 있습니다.

다음 단계를 수행하십시오.

1. "기록" 테스트 모드를 선택합니다.
2. 명령 스크립트 파일의 경로와 파일 이름을 입력합니다. 테스트 결과는 이 파일의 "출력 스크립트" 필드에 저장됩니다.
3. 필요한 경우 기록된 테스트를 실행할 횟수를 "반복 횟수" 필드에 입력합니다.
4. 필요한 경우 명령 스크립트 파일에 추가할 설명을 "설명" 필드에 입력합니다.
5. 테스트를 하나 이상 실행합니다.
6. 기록을 중지하려면 새 테스트 모드를 지정하십시오.

추가 정보:

[FIPS 전용 환경에서 테스트 도구를 사용하는 방법](#) (페이지 762)

기능 테스트 결과

이 단원의 표에서는 각 기능 테스트 유형의 결과에 대해 설명합니다.

isProtected 의 상태	결과
성공	"메시지" 필드에 "보호됨"이 표시됩니다. 이는 테스트 도구가 정책 서버에 연결되었으며 리소스가 정책에 의해 보호되고 있음을 의미합니다. 또한 다음 필드가 정책 서버에서 반환된 값으로 채워집니다. 영역 이름 리소스가 포함된 영역의 이름입니다. 영역 OID 영역 개체 식별자입니다. 자격 증명 리소스를 보호하는 데 사용되는 인증 체계입니다. 리디렉션 인증 체계에 사용되는 리디렉션 문자열(지정된 경우)입니다. 모든 인증서와 HTML 양식 기반 체계는 이 문자열을 반환합니다. 이 문자열은 일반적으로 양식을 표시할 위치를 에이전트에 알려 줍니다.
실패	"메시지" 필드에 "오류" 또는 "보호되지 않음"이 표시됩니다. "오류"는 테스트 도구가 정책 서버에 연결할 수 없음을 나타내고, "보호되지 않음"은 지정된 리소스가 정책에 의해 보호되고 있지 않음을 나타냅니다. 테스트가 실패한 경우 다음과 같이 하십시오. 정책이 올바르게 구성되었는지 확인합니다. 인증 서버 로그에서 디버깅 정보를 확인합니다.

isAuthenticated 의 상태 결과

성공	"메시지" 필드에 "인증됨"이 표시되고 다음 필드가 정책 서버에서 반환된 값으로 채워집니다. 세션 ID SiteMinder 가 할당한 고유 세션 ID 입니다. 정책 서버는 이 ID 를 사용하여 세션 정보가 저장된 쿠키를 식별합니다. 특성 정책 서버가 응답으로 되돌려 보내는 특성입니다. 예를 들면 다음과 같습니다. ID 길이 ASCII 형식 16진수 형식 4> id 215 len 005 'LDAP:' - '4c 44 41 50 3a' 이 응답에서는 사용자가 인증된 사용자 디렉터리의 이름을 나타냅니다. 참고: 사용자가 제공한 정보를 제거하지 않고 "특성" 필드에 표시된 응답을 지우려면 "재설정"을 클릭하십시오. 원인 테스트 결과와 관련된 사유 코드입니다. 이 필드는 SiteMinder SDK 를 통해 개발자에게 정보를 제공하는 데 사용됩니다. 사유 코드는 SmApi.h 에 나와 있습니다.
실패	"메시지" 필드에 "인증되지 않음"이 표시됩니다. 테스트가 실패한 경우 다음과 같이 하십시오. 유효한 사용자 자격 증명을 사용하고 있는지 확인합니다. 인증 서버 로그에서 디버깅 정보를 확인합니다.

IsAuthorized 의 상태 결과

성공	"메시지" 필드에 "인증됨"이 표시되고 "세션 ID" 필드에 SiteMinder 가 할당한 세션 ID 가 표시됩니다. 이 ID 는 세션 정보가 저장된 쿠키를 식별합니다.
실패	"메시지" 필드에 "권한이 부여되지 않음"이 표시됩니다. 테스트가 실패한 경우 다음과 같이 하십시오. 정책이 올바르게 구성되었는지 확인합니다. 권한 부여 서버 로그에서 디버깅 정보를 확인합니다.

평균 경과 시간 계산

테스트가 완료되면 "명령" 그룹 상자의 "경과 시간" 필드에 테스트 실행에 소요된 시간이 표시됩니다. 시스템 성능에 기록이 있을 수 있으므로 여러 테스트의 평균 경과 시간을 계산하면 더 정확한 결과를 얻을 수 있습니다.

평균 경과 시간을 구하려면

1. "반복 횟수" 필드에 원하는 테스트 실행 횟수를 지정합니다.
지정한 횟수만큼 테스트가 실행된 후 총 경과 시간이 표시됩니다.
2. 총 경과 시간을 테스트 실행 횟수로 나눠 평균 경과 시간을 계산합니다.

명령 스크립트 파일에 기록된 테스트를 재생하여 재발 테스트 수행

재발 테스트를 수행하면 정책 저장소 업그레이드나 새로운 기능 구현과 같은 변경 내용이 SiteMinder에 영향을 주는지 여부를 테스트할 수 있습니다. 재발 테스트를 실행하려면 현재 환경에서 테스트를 한 번 실행하고 변경 작업 후에 테스트를 다시 실행합니다. 두 테스트의 결과를 비교하면 해당 변경 내용이 SiteMinder에 영향을 주는지 확인할 수 있습니다.

재발 테스트를 수행하려면

1. ["기록" 모드에서 기능 테스트를 하나 이상 실행합니다](#) (페이지 774).
2. "모드" 그룹 상자에서 "기본 재생"을 선택합니다.
3. "입력 스크립트" 필드에 명령 스크립트 파일의 이름을 입력합니다.
이 파일 이름은 "기록" 모드에서 "출력 스크립트" 필드에 입력한 값과 일치해야 합니다.
4. "출력 스크립트" 필드에 출력 파일 이름을 지정합니다.
5. "명령" 그룹 상자에서 "스크립트 실행"을 클릭합니다.
명령 스크립트 파일이 실행되고 출력 스크립트 파일이 생성됩니다.

추가 정보:

[FIPS 전용 환경에서 테스트 도구를 사용하는 방법](#) (페이지 762)

스트레스 테스트 실행

테스트 도구를 사용하여 정책 서버가 요청을 동시에 여러 개 수신할 때의 SiteMinder 성능을 테스트할 수 있습니다. 스트레스 테스트를 사용하면 여러 에이전트가 동시에 정책 서버에 연결하거나 단일 에이전트가 여러 스레드에서 정책 서버와 통신하는 상황을 시뮬레이션할 수 있습니다.

스트레스 테스트는 "고급 재생" 모드로 실행됩니다. 테스트 도구는 실행할 테스트와 테스트 실행 횟수를 지정하는 스레드 제어 파일에서 명령을 수신합니다. 스레드 제어 파일의 명령을 실행한 후 테스트 결과가 출력 파일에 기록됩니다.

스레드 제어 파일 구성

스트레스 테스트를 위해 복잡한 테스트를 자동화하려면 스레드 제어 파일을 구성하여 실행할 명령 스크립트 파일, 반복 횟수, 스레드 수 등을 정의하십시오. 스레드 제어 파일에는 테스트 도구 자체의 스크립팅 언어로 된 여러 명령 줄과 주석이 있으며 각 줄의 맨 앞에는 # 기호가 있습니다.

기본 지침은 다음 형식입니다.

command_script_file_name, *repetition_count*, *thread_count*, [*max_time_in_seconds*]

command_script_file_name

이전에 기록된 명령 스크립트 파일의 경로 이름을 지정합니다.

repetition_count

테스트 도구가 명령 스크립트를 실행하는 횟수를 지정합니다.

thread_count

테스트 도구가 명령 스크립트를 실행하기 위해 시작하는 동시 스레드의 수를 지정합니다.

max_time_in_seconds

(선택 사항) 테스트 기간에 대한 제한 시간(초)을 지정합니다. 경과된 테스트 시간이 이 제한 시간을 초과하면 구성된 반복 횟수에 도달했는지 여부에 상관없이 재생이 중지됩니다.

예를 들면 다음과 같습니다.

```
# c:\temp\test_data.txt, 8, 6, 120
```

이 줄은 다음을 지정합니다.

- 입력 명령 스크립트는 c:\temp\test_data.txt 입니다.
- 테스트 도구가 스크립트를 8 번 실행합니다.
- 6 개의 동시 스레드가 스크립트를 실행합니다.
- 120 초 후에는 반복 횟수가 8 번에 도달했는지 여부에 상관없이 테스트가 종료됩니다.

테스트 도구는 테스트 출력을 파일에 씁니다. 출력 파일 이름은 입력 파일 이름 뒤에 `_out#`을 추가한 형식으로 지정되며 여기서 #은 증분되는 스레드 번호입니다. 예를 들어 위 테스트의 출력 파일은

c:\temp\test_data.txt_out1 부터 c:\temp\test_data.txt_out6 까지입니다.

테스트 도구 스크립팅 언어에는 다음 표에 나오는 것과 같이 스크립트 파일 출력을 제어하기 위한 명령이 포함되어 있습니다. 아래 그림에서는 샘플 스레드 제어 파일을 보여 줍니다.

명령	설명
.report	테스트 결과가 요약된 최종 보고서를 출력 파일로 생성합니다. 이 보고서에 각 서버 요청의 상태는 포함되지 않습니다. 이 값이 기본값입니다.
.reportsread	응답 시간 스프레드 보고서가 포함된 파일을 생성합니다. 파일 이름은 <code>command_script_stats_spread</code> (예: <code>isprotected-record.txt_stats_spread</code>)입니다.
.output	각 서버 요청의 상태를 포함하여 전체 결과가 요약된 최종 보고서를 출력 파일로 생성합니다.
.viewstats	최종 통계를 텍스트 편집기에 표시합니다.
.verbose	각 서버 요청에 대한 상세 정보가 포함된 출력 파일을 생성합니다.

명령	설명
<code>.brief</code>	각 서버 요청에 대한 간략한 결과가 포함된 출력 파일을 생성합니다. 이 옵션은 <code>.output</code> 명령과 함께 사용할 경우에만 유효합니다.
<code>.sleep</code>	테스트 도구가 지정된 시간(밀리초) 동안 일시 중지할 수 있도록 합니다. 이는 간헐적인 서버 요청을 시뮬레이트합니다.
<code>.userselectionmode</code>	사용자 이름이 순서대로 사용되는지 아니면 무작위로 선택되는지를 결정합니다. 유효한 값은 0(순차적)과 1(무작위)입니다. 자세한 내용은 (선택 사항) 테스트에서 사용자 이름이 처리되는 방식 구성 (페이지 782)을 참조하십시오.
<code>.randomseed</code>	각 테스트에서 이름이 의사 무작위 순서로 스레드 순서까지 반복될 수 있습니다. 자세한 내용은 (선택 사항) 테스트에서 사용자 이름이 처리되는 방식 구성 (페이지 782)을 참조하십시오.
<code>.connect settings_file</code>	테스트 도구 설정 파일의 정보로 테스트 도구를 초기화하여 시뮬레이트된 에이전트 하나를 사용하도록 다중 스레드 테스트를 설정합니다. 기본 다중 스레드 테스트는 시뮬레이트된 에이전트 여러 개로 구성되며 각 스레드에 시뮬레이트된 에이전트가 하나씩 사용됩니다. 이 옵션을 사용하면 시뮬레이트된 에이전트 하나와 스레드 여러 개를 사용하도록 테스트를 설정할 수도 있습니다.
<code>.disconnect</code>	테스트 도구 초기화를 해제하여 시뮬레이트된 에이전트의 다중 스레드 테스트가 종료되었음을 나타냅니다.

스레드 제어 파일 예

```
.output  
  
.connect c:\test\smtest.ini  
.brief  
c:\temp\test_data1.txt, 2, 3  
.verbose  
.sleep 5000  
c:\temp\test_data1.txt, 2, 2  
.brief  
c:\temp\test_data1.txt, 3, 4  
.connect smtest.ini  
c:\temp\test_data1.txt, 5, 6  
.disconnect
```

"고급 재생" 모드에서 스레드 제어 파일을 실행하여 스트레스 테스트 수행

"고급 재생" 테스트 모드를 사용하여 스레드 제어 파일에 정의된 스트레스 테스트를 실행하십시오.

다음 단계를 수행하십시오.

1. "모드" 그룹 상자에서 "고급 재생"을 선택합니다.
2. "Control"(제어) 필드에 스레드 제어 파일의 이름을 입력합니다.
3. "명령" 그룹 상자에서 "Run Script"(스크립트 실행)를 클릭합니다.

스레드 제어 파일이 실행되고 출력 스크립트 파일이 생성됩니다.

(선택 사항) 테스트에서 사용자 이름이 처리되는 방식 구성

다음 세 개의 매개 변수는 테스트에서 사용자 이름이 처리되는 방식을 구성합니다.

34 UserCount:

(명령 스크립트 파일에서 정의됨) 테스트 시 인증 및 권한 부여에 사용되는 AAAAAA, BAAAAA ~ ZZZZZZ 형식의 사용자 수를 지정합니다. UserCount 매개 변수가 설정되어 있는 경우 UserName 매개 변수는 무시됩니다.

참고: 이 매개 변수가 무시되더라도 Username 매개 변수는 여전히 필요하므로 삭제하지 마십시오.

명령 스크립트 파일의 다른 매개 변수와 동일한 형식으로 UserCount 매개 변수를 추가하십시오. 즉, 행의 24 열부터 전체 매개 변수 이름("34 " 접두사 포함) 및 매개 변수 값을 입력하십시오.

예를 들면 다음과 같습니다.

```
34 UserCount:          1000
```

.userselectionmode

(스레드 제어 파일에서 정의됨) 사용자 이름이 순차적으로 선택되는지 무작위로 선택되지를 결정합니다. 유효한 값은 1 및 2 입니다.

1 로 설정된 경우 UserCount 매개 변수로 지정된 값에 도달할 때까지 테스트 단계가 각 사용자 이름으로 순차적으로 실행됩니다. 반복 횟수에 도달하거나 최대 시간이 경과될 때까지 사용자 이름은 반복해서 "AAAAAA"로 되돌아갑니다.

2(기본값)로 설정된 경우 사용자가 무작위로 선택됩니다.

.randomseed

(스레드 제어 파일에서 정의됨) 0 이 아닌 정수 값으로 구성된 경우 사용자 이름이 "UserCount" 매개 변수의 값으로 인덱싱될 때까지 "AAAAAA" 범위의 사용자 이름 집합에서 사용자 이름이 무작위 순서로 선택됩니다. 따라서 각 테스트에서 이름이 의사 무작위 순서로 스레드 순서까지 반복될 수 있습니다.

.randomseed 를 지정하지 않으면 현재 시간이 사용됩니다.

(선택 사항) 안정적 로드를 시뮬레이트하기 위해 정책 서버 요청 간 대기 시간 구성

요청이 일정한 간격으로 정책 서버에 전송되는 안정적 로드를 시뮬레이트하려면 스레드 제어 파일에 다음 매개 변수를 구성하십시오.

.sleepbetweenrequests

스레드별로 정책 서버에 전송되는 각 요청 사이의 대기 시간(밀리초)을 지정합니다.

예를 들어 .sleepbetweenrequests 매개 변수가 5(밀리초)로 설정되면 각 스레드에서 초당 약 200 회의 요청이 정책 서버에 전송됩니다.

참고: 실제 요청 빈도는 요청이 완료되는 데 걸리는 시간, 각 스레드에서 이용하는 CPU 시간 및 외부 요인과 같은 여러 요소의 영향을 받을 수 있습니다.

(선택 사항) 재생 테스트 결과를 CSV 형식의 파일에 기록하도록 테스트 도구 구성

다음 시스템 환경 변수를 설정하여 모든 재생 테스트 결과를 CSV(쉼표로 구분된 값) 형식의 파일에 기록하도록 테스트 도구를 구성할 수 있습니다.

SMTESTCSVFILE

테스트 도구가 재생 테스트 결과를 기록할 CSV 파일의 경로 이름을 지정합니다. 재생 테스트 결과는 지정된 파일의 시작 부분에 있는 헤더 행을 사용하여 쉼표로 구분된 형식으로 작성됩니다.

파일이 이미 있는 경우 해당 파일이 추가됩니다. 스레드 제어 파일에 여러 번의 기록 재생이 지정된 경우에는 결과가 집계됩니다.

보고서 보기

스트레스 테스트를 실행하면 결과가 요약된 보고서가 생성됩니다. 이 보고서에는 다음 정보가 포함됩니다.

- 테스트 시작 및 완료 시간
- 총 경과 시간
- 최소, 최대 및 평균 요청 시간

- 총 요청 수
- 처리량
- 테스트 실행 횟수 및 테스트 결과

이 보고서는 스레드 제어 파일이 있는 디렉터리에 저장됩니다. 보고서 이름은 스레드 제어 파일 이름 뒤에 `_stats` 가 추가된 형식입니다. 예를 들어 스레드 제어 파일이 `thread.txt` 일 경우 보고서 이름은 `thread.txt_stats` 입니다.

Control File: C:\temp\control.txt
Started at: 0:02:05.481
Finished at: 0:03:22.672
Total Elapsed: 0:00:01.396

Minimum Request Time: 0:00:00.400
Maximum Request Time: 0:00:05.498
Average Request Time: 0:00:01.396

Total Requests 234
Throughput (Req/Sec): 3.241

Request	Count	Yes	No	Timeout	Error
IsProtected	78	72	0	0	6
IsAuthenticated	78	78	0	0	0
IsAuthorized	78	72	0	6	0
Total:	234	222	0	6	6

인증서 기반 인증 테스트

SiteMinder 테스트 도구는 사용자 인증 및 권한 부여를 시뮬레이트합니다. 인증서 기반 인증 체계를 사용하려면 추가 구성을 수행해야 합니다.

다양한 인증서 생성 도구로 인해 발급자 DN의 형식이나 기타 인증서 특성에 차이가 있을 수 있습니다.

예를 들어 IIS 웹 서버에서 `certutil.exe`를 사용하여 생성된 인증서의 발급자 DN에는 상태를 나타내기 위해 `ST=`가 사용될 수 있습니다. 하지만 Oracle iPlanet 웹 서버에서 OpenSSL 도구를 사용하여 생성된 인증서의 발급자 DN에는 상태를 나타내기 위해 `S=`가 사용될 수 있습니다.

참고: 특정 인증서 생성 도구에서 사용되는 실제 값에 대한 자세한 내용은 해당 인증서 생성 도구의 공급업체에서 제공하는 설명서를 참조하십시오.

인증서 기반 인증 체계를 테스트하려면 정책 서버에서 인증서 매핑을 구성하여 다양한 인증서 생성 도구로 생성된 인증서를 처리할 수 있도록 하십시오.

사용자 지정 매핑이 필요한 인증서 특성

일반적인 몇 가지 인증서 특성은 인증서를 생성하는 데 사용된 타사 도구(예: `certutil.exe` 또는 OpenSSL)에 따라 조금씩 다릅니다. 다음 특성의 차이점으로 인해 SiteMinder 테스트 도구에서 오류가 발생할 수 있습니다.

전자 메일 주소

인증서 생성 도구의 공급업체에 따라 `E` 나 `Email`로 표시됩니다.

미국 주

인증서 생성 도구의 공급업체에 따라 `S` 나 `ST`로 표시됩니다.

사용자 ID 번호

인증서 생성 도구의 공급업체에 따라 `UID` 나 `UserID`로 표시됩니다.

참고: 특정 인증서 생성 도구에서 사용되는 실제 값에 대한 자세한 내용은 해당 인증서 생성 도구의 공급업체에서 제공하는 설명서를 참조하십시오.

테스트를 위한 사용자 지정 특성 매핑

브라우저 및 웹 서버에서 제대로 작동하는 인증서 인증 체계라도 SiteMinder 테스트 도구 사용 시 오류가 발생하는 경우가 있습니다. 인증 로그에는 인증서에 사용된 발급자 DN 형식과 발급자 DN의 형식이 달라야 한다고 나옵니다.

이 문제는 사용된 인증서 생성 도구의 유형에 따라 발급자 DN 및 기타 특성이 다를 경우에 발생합니다. 예를 들어 IIS 웹 서버의 certutil.exe 프로그램은 발급자 DN에서 주 이름의 약어로 ST=를 사용할 수 있습니다. 반면 Oracle iPlanet 웹 서버의 OpenSSL 도구는 주 이름의 약어로 S=를 사용할 수 있습니다.

참고: 특정 인증서 생성 도구에서 사용되는 실제 값에 대한 자세한 내용은 해당 인증서 생성 도구의 공급업체에서 제공하는 설명서를 참조하십시오.

이는 [사용자 지정 매핑이 필요한 인증서 특성](#) (페이지 785)에 나오는 다른 특성의 경우에도 마찬가지입니다.

이 문제를 해결하려면 각 발급자 DN 형식에 대한 매핑을 정책 서버에 생성하도록 관리자에게 요청하십시오. 이렇게 하면 정책 서버가 서로 다른 인증서 생성 도구로 생성된 발급자 DN 형식을 허용할 수 있습니다.

발급자 DN 매핑

certutil.exe 및 OpenSSL 등의 인증서 생성 도구가 발급자 DN을 생성하는 방식에는 약간의 차이점이 있습니다. 예를 들어 한 도구는 다음과 같은 발급자 DN을 생성할 수 있습니다.

```
CN=Personal Freemail RSA 2000.8.30, OU=Certificate Services, O=Thawte, L=Cape Town, S=Western Cape, C=ZA
```

다른 도구는 다음과 같은 발급자 DN을 생성할 수 있습니다.

```
CN=Personal Freemail RSA 2000.8.30, OU=Certificate Services, O=Thawte, L=Cape Town, ST=Western Cape, C=ZA
```

여러 형식을 지원하려면 사용 환경의 모든 발급자 DN 형식에 대한 매핑을 정책 서버에 생성하도록 관리자에게 요청하십시오.

참고: 특정 인증서 생성 도구에서 사용되는 실제 값에 대한 자세한 내용은 해당 인증서 생성 도구의 공급업체에서 제공하는 설명서를 참조하십시오.

사용자 지정 인증서 매핑 만들기

SiteMinder 정책 서버의 인증서 매핑 기능을 사용하여 인증서에 대한 사용자 지정 매핑을 제공할 수 있습니다.

참고: 다음 절차에서는 개체를 생성하고 있다고 가정합니다. 기존 개체의 속성을 복사하여 개체를 생성할 수도 있습니다. 자세한 내용은 "정책 서버 개체 복제"를 참조하십시오.

인증서 매핑에 사용자 지정 특성을 생성하고 사용하려면

1. "인프라", "디렉터리"를 차례로 클릭합니다.
2. "인증 매핑", "인증서 매핑 만들기"를 차례로 클릭합니다.
"인증서 매핑 만들기" 창이 열립니다.
3. "Create a new object"(새 개체 만들기)가 선택되어 있는지 확인하고 "확인"을 클릭합니다.

인증서 매핑 설정이 열립니다.

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

4. "발급자 DN" 필드에 전체 발급자 DN 을 입력합니다.
5. "매핑" 그룹 상자에서 "사용자 지정" 라디오 단추를 선택합니다.
"매핑 식" 필드가 열립니다.

6. 사용자 지정 매핑 식을 입력합니다.

이 표기법은 인증서 매핑에 허용되는 서로 다른 두 특성을 지정하는 데 사용됩니다.

■ 전자 메일:

%{E/Email}

■ ST:

%{S/ST}

■ 사용자 ID:

%{UID/UserID}

참고: 사용자 지정 매핑 식에 대한 자세한 내용은 [사용자 지정 매핑이 필요한 인증서 특성](#) (페이지 785)을 참조하십시오.

7. "제출"을 클릭합니다.

사용자 지정 매핑이 저장됩니다. 이제 정책 서버가 발급자 DN 에서 전자 메일 특성이 서로 다르게 나타나는 다양한 유형의 인증서 생성 도구(예: certutil.exe 및 OpenSSL) 및 SiteMinder 테스트 도구의 요청을 처리할 수 있습니다. [사용자 지정 매핑이 필요한 인증서 특성](#) (페이지 785)에 언급된 다른 특성에 대해서도 이 과정을 따를 수 있습니다.

추가 정보:

[X.509 클라이언트 인증서 인증 체계에 대한 인증서 매핑](#) (페이지 439)

제 25 장: 에이전트 구성 문제 해결

영어가 아닌 입력 문자에 정크 문자가 포함됨

UNIX/Linux 에 해당

증상

영어가 아닌 일부 입력 문자가 콘솔 창에 올바르게 표시되지 않습니다.

해결 방법

콘솔 창의 터미널 설정을 확인하십시오. 콘솔이 입력 문자의 높은(8) 비트를 삭제하지 않는지 확인하십시오. 다음 명령을 실행합니다.

```
stty -istrip
```

고급 인증 서버의 오류 메시지

증상

사용자에게 다음과 같은 내용의 브라우저 오류가 나타납니다.

내부 오류가 발생했습니다. 브라우저를 닫은 후 다시 엽니다. 문제가 계속되면 헬프 데스크에 문의하십시오.

해결 방법

다음 항목을 확인하십시오.

- RiskMinder 서비스가 시작되고 정책 서버에서 실행되고 있는지 확인합니다.
- 다음 로그 파일을 검토하여 RiskMinder 가 READY 상태인지 확인합니다.
`siteminder_installation_directory\..\aas\logs\cariskminderstartup.log`
- CA SiteMinder® for Secure Proxy Server 를 다시 시작합니다.
- DeviceDNA™가 수집되고 있지 않을 경우 다음 단계를 수행합니다.
 - a. JSafeJCE 보안 공급자를 사용하도록 JVM 을 구성합니다.
 - b. CA SiteMinder® for Secure Proxy Server 를 다시 시작합니다.

추가 정보:

[DeviceDNA™를 사용한 고급 세션 보증을 위한 CA SiteMinder® for Secure Proxy Server 환경 구성 \(페이지 730\)](#)

"토큰이 없습니다." 오류

증상

CA SiteMinder® for Secure Proxy Server 의 흐름 응용 프로그램 로그 파일에 다음 오류가 표시됩니다.

토큰이 없습니다...

해결 방법

다음 항목을 확인합니다.

- 에이전트가 사용되도록 설정되었는지 확인합니다.
- 정책 서버가 세션 저장소에 연결되어 있는지 확인합니다.

부록 A: SSL 인증 체계 문제 해결

이 섹션은 다음 항목을 포함하고 있습니다.

[개요](#) (페이지 791)

[SSL 구성](#) (페이지 792)

[SSL 문제 해결](#) (페이지 796)

개요

SSL 고급 인증 체계를 구성하려면 웹 서버가 SSL 을 사용하도록 올바르게 구성되어 있어야 합니다. SSL 연결을 통한 인증 체계를 구성할 때 발생하는 많은 문제는 SSL 구성 문제일 수 있습니다. 따라서 SSL 을 통한 인증 체계의 문제를 해결하는 첫 번째 단계는 SSL 이 올바르게 구성되어 있고 작동하는지 확인하는 것입니다. 이러한 구성 요소를 개별적으로 분석할 수 있도록 에이전트와의 상호 작용 없이 구성을 확인하십시오.

SSL 연결 기능 확인

SSL 을 통한 인증 체계의 문제를 해결하는 첫 번째 단계는 SSL 이 올바르게 구성되어 있고 작동하는지 확인하는 것입니다.

다음 단계를 수행하십시오.

1. SSL 을 통한 인증 체계를 사용할 영역을 보호하는 에이전트가 사용되지 않도록 설정합니다.
2. 인증서가 있는 브라우저를 사용하여 다음 URL 중 하나로 이동합니다.
 - `https://web_server_name:port`(Netscape 웹 서버)
 - `https://web_server_name:port/<SSL Virtual Directory>`(IIS 웹 서버)
 - `https://web_server_name:port`(Apache 기반 웹 서버)

이 SSL 연결이 인증서가 필요하도록 구성된 경우 인증서를 선택해야 합니다.

SSL 구성

제품을 사용하기 전에 SSL 을 구성하고 제대로 동작하는지 확인하십시오. SSL 연결을 설정하려면 수신 인증서의 인증 기관을 트러스트할 수 있어야 합니다. 예를 들어 브라우저가 VeriSign 에서 서명된 인증서를 제공하는 경우 VeriSign 인증 기관이 웹 서버에 설치되고 트러스트되어 있어야 합니다. 제공되는 클라이언트 인증서를 트러스트하는 것 외에 서버 자체에서도 클라이언트에 인증서를 제공해야 합니다. 클라이언트는 인증서를 발급한 인증 기관을 트러스트해야 합니다. 이렇게 설정하면 상호 인증이 가능합니다. 이러한 인증서를 설치한 후에는 필요에 따라 웹 서버에서 SSL 을 사용하고 인증서를 요구하도록 구성할 수 있습니다.

SSL 구성 정보에 대한 자세한 내용은 웹 서버 소프트웨어와 함께 제공된 설명서를 참조하십시오. 이 단원에는 SSL 연결을 설정할 수 있도록 웹 서버와 브라우저를 구성하기 위한 단계별 지침이 포함되어 있습니다.

Netscape 에서 웹 서버가 클라이언트 인증서를 트러스트하도록 설정

웹 서버에 인증 기관이 이미 설치되어 있는 경우 다음 단원으로 이동하십시오. 그렇지 않은 경우 SSL 웹 서버에 인증 기관의 인증서를 설치하십시오.

다음 단계를 수행하십시오.

1. 인증 기관의 인증서를 가져와서 화면에 유지하거나 파일에 저장합니다.
2. "Netscape Server Administration"(Netscape 서버 관리)에서 "Keys & Certificates"(키 및 인증서)를 선택합니다.
3. "Install Certificate"(인증서 설치)를 클릭합니다.
4. "Certificate For"(인증서 대상) 필드에서 "Server Security Chain"(서버 보안 체인)에 데이터를 입력합니다.
5. "Certificate Name"(인증서 이름) 필드에 설명을 입력합니다.
6. 인증 기관 인증서를 파일에 저장한 경우 "Message is in this file"(메시지가 포함된 파일) 필드에 파일 이름을 입력합니다. 그렇지 않은 경우 "Message text (with headers)"(메시지 텍스트(헤더 포함)) 옵션 "Message text (with headers)"(메시지 텍스트(헤더 포함)) 필드에 인증서를 붙여 넣으십시오.
7. "OK"(확인)를 클릭하고 웹 서버를 다시 시작합니다.

SSL 을 사용하도록 Netscape 웹 서버 구성

인증서를 요청하여 Netscape 웹 서버에서 SSL 을 구성하십시오.

다음 단계를 수행하십시오.

1. "Netscape Server Administration"(Netscape 서버 관리)에서 "Admin Preferences"(관리 기본 설정)를 클릭합니다.
2. "Encryption On/Off"(암호화 설정/해제)를 클릭하고 암호화가 설정되었는지 확인합니다.
3. 인증서 또는 기본 인증 체계를 사용하는 인증서를 실행 중인 경우에는 인증서를 요구하십시오. "Encryption Preferences"(암호화 기본 설정) 설정에서 "Require Certificates"(인증서 요구)를 "On"(설정)으로 설정하십시오. 인증서가 설치된 브라우저에서 `https://servername:port` 에 연결할 수 있는지 확인하십시오.

참고: "Certificate"(인증서) 또는 "Basic Authentication Scheme"(기본 인증 체계)에 대해서는 "Required Certificates"(인증서 요구)를 설정하지 마십시오.

Netscape 인증 기관에 대한 트러스트 설정

웹 서버에 인증 기관이 설치되어 있는 경우 두 인증 기관 간의 트러스트를 설정할 수 있습니다.

다음 단계를 수행하십시오.

1. "Netscape Server Administration"(Netscape 서버 관리)에서 "Keys & Certificates"(키 및 인증서)를 선택합니다.
2. "Manage Certificates"(인증서 관리)를 선택합니다.
3. "Certificate Authority"(인증 기관)를 선택합니다. 인증서에 대한 상세 정보를 제공하는 대화 상자가 표시됩니다.
4. "Trust"(트러스트)를 선택합니다.
5. "OK"(확인)를 클릭하고 웹 서버를 다시 시작합니다.

Windows 에서 웹 서버가 클라이언트 인증서를 트러스트하도록 설정

적절한 인증 기관 인증서를 설치하여 클라이언트 인증서를 트러스트하십시오.

SSL 웹 서버에는 각 인증 기관의 인증서가 있어야 합니다. 주요 인증 기관은 이미 설치되어 있을 것입니다. 인증서 스냅인을 사용하여 Windows 운영 환경에서 인증서를 구성할 수 있습니다.

SSL 을 사용하도록 IIS 웹 서버 구성

웹 서버에서 보안 포트가 사용되도록 설정되어 있는지 확인하십시오. 보안 포트는 일반적으로 포트 443 입니다. 관리 콘솔에서 웹 서버를 마우스 오른쪽 단추로 클릭하고 "속성"을 클릭한 다음 "웹 사이트" 탭에서 SSL 포트를 확인할 수 있습니다. 포트 번호가 설치되어 있어야 합니다.

고급 인증 체계는 웹 서버에 가상 디렉터리를 생성합니다. 이러한 디렉터리는 특정 인증 체계에 필요한 SSL 및 인증서를 요구하도록 자동으로 구성됩니다. 그러나 테스트 용도로 테스트 가상 디렉터리를 생성할 수도 있습니다. "디렉터리 보안" 탭의 "보안 통신"을 통해 이 가상 디렉터리가 인증서를 요구하도록 구성할 수 있습니다.

`https://servername:port/virtual directory` - 브라우저에 인증서를 요청하도록 합니다.

IIS 웹 서버 인증서 설치

아직 웹 서버용 키를 생성하지 않았으면 생성하십시오. 이 작업은 관리 콘솔의 "키 관리자"를 통해 수행합니다. 다음을 수행하여 "키 관리자"에 액세스합니다.

참고: 이 과정은 IIS 3 과 IIS 4 에서 약간 차이가 있습니다.

IIS 웹 서버 인증서를 설치하려면

1. 관리 콘솔에서 웹 서버를 마우스 오른쪽 단추로 클릭하고 "속성"을 선택합니다.
2. "디렉터리 보안" 탭을 클릭합니다.
3. "보안 통신" 패널에서 "키 관리자"를 클릭합니다.

4. "키"에서 "새 키 만들기"를 선택하면 마법사가 나머지 과정을 안내합니다.
키를 생성한 후에는 위의 단계에서 생성한 파일을 사용하여 인증서를 요청할 수 있습니다. "인증 기관"으로 이동하여 이 서버의 인증서를 요청합니다. 인증서를 받으려면 1 단계에서 생성된 인증서 요청 정보를 붙여 넣어야 합니다. 인증서를 받은 후에는 다시 관리 콘솔의 "디렉터리 보안"으로 이동하고 "키 관리자"를 클릭하여 다음 단계에 설명된 대로 키에 대한 인증서를 설치하십시오.
5. 키 이름을 마우스 오른쪽 단추로 클릭하고 "인증서 설치"를 선택합니다.
6. 웹 서버를 다시 시작합니다.

Apache 에서 웹 서버가 클라이언트 인증서를 트러스트하도록 설정

웹 서버에 인증 기관이 이미 설치되어 있는 경우 다음 단원으로 이동하십시오. 그렇지 않은 경우 다음과 같이 SSL 웹 서버에 인증 기관의 인증서를 설치하십시오.

다음 단계를 수행하십시오.

1. 다음 Apache 구성 요소를 다운로드하여 빌드합니다.
 - Apache
 - OpenSSL
 - Mod_SSL
 - Mod_so - 이 모듈은 Apache 의 일부로 포함되어 있지만 웹 서버를 구축할 때 사용되도록 설정해야 합니다.
 - RSAREf-2.0
2. 인증 기관 인증서를 `apache/conf/ssl.crt` 디렉터리에 x509 b64 형식으로 복사합니다.
3. `apache/conf/ssl.crt` 디렉터리에서 `make` 를 실행합니다.
4. 웹 서버를 다시 시작합니다.

Apache 웹 서버 인증서 설치

Apache 웹 서버에 인증서를 설치하기 위한 과정은 개별 구성에 따라 달라집니다. 이러한 구성 요소를 구성하는 방법에 대한 자세한 내용은 `Mod_SSL` 및 `OpenSSL` 설명서를 참조하십시오.

SSL 문제 해결

다음 단원에서는 SSL 인증 체계를 처리할 때 발생하는 가장 일반적인 문제에 대해 자세히 설명합니다.

인증서에 대한 메시지가 표시되지 않음

인증서에 대한 메시지가 표시되지 않으면 SSL 이 올바르게 구성되었는지 확인하십시오. 에이전트가 설치되어 있으면 에이전트가 사용되지 않도록 설정하십시오. 첫 번째 단계는 간단한 SSL 연결을 확인하는 것입니다.

다음 단계를 수행하십시오.

1. SSL 을 통한 인증 체계를 사용할 영역을 보호하는 에이전트가 사용되지 않도록 설정합니다.
2. 인증서가 있는 브라우저를 사용하여 다음 URL 중 하나로 이동합니다.
 - `https://web_server_name:port`(Netscape 웹 서버)
 - `https://web_server_name:port/<SSL Virtual Directory>`(IIS 웹 서버)
 - `https://web_server_name:port`(Apache 웹 서버)

이 SSL 연결이 인증서가 필요하도록 구성된 경우 인증서를 선택해야 합니다.

이전 절차를 수행한 후에도 인증서 메시지가 표시되지 않음

인증서 메시지가 여전히 표시되지 않을 경우 다음 단계를 추가로 수행하십시오.

- 모든 Firefox 브라우저가 항상 인증서를 묻도록 구성되었는지 확인합니다.
- 모든 웹 서버가 SSL 을 사용하고 인증서를 요구하도록 구성되었는지 확인합니다.
- 제품에서 사용되는 각각의 가상 디렉터리에 대해 다음 설정을 확인합니다.
- 웹 서버 인증서가 만료되었는지 확인합니다.
- 브라우저 인증서가 유효한지 확인합니다.

모든 Firefox 브라우저가 항상 인증서를 묻도록 구성되었는지 확인

동일한 인증서를 자동으로 전달하도록 Firefox 웹 브라우저를 구성할 수 있습니다. 이 설정을 사용하면 인증서를 선택하라는 메시지가 표시되지 않고 인증서를 사용한 SSL 연결이 구성됩니다.

다음 단계를 수행하십시오.

1. Firefox 브라우저의 "Firefox" 메뉴에서 "Options"(설정)를 선택합니다.
2. "고급"을 클릭합니다.
3. "Encryption"(암호화) 탭을 클릭합니다.
4. "Certificates"(인증서) 섹션에서 "Ask me every time"(항상 물어 보기) 옵션이 설정되었는지 확인합니다.

모든 웹 서버가 SSL 을 사용하고 인증서를 요구하도록 구성되었는지 확인

Netscape 웹 서버의 경우

1. "Netscape Server Administration"(Netscape 서버 관리)에서 "Admin Preferences"(관리 기본 설정)를 클릭합니다.
2. "Encryption On/Off"(암호화 설정/해제)를 클릭하고 암호화가 설정되어 있는지 확인한 다음 "OK"(확인)를 클릭합니다.
3. "Encryption Preferences"(암호화 기본 설정)를 클릭하고 "Require Certificates"(인증서 요구)가 설정되어 있는지 확인합니다.
4. 웹 서버를 다시 시작합니다.

IIS 웹 서버의 경우

가상 디렉터리 SMGetCredCert, SMGetCredCertOptional 및 SMGetCredNoCert 가 생성되고 올바르게 설정되어 있는지 확인합니다.

- SMGetCredCert - "Require Certificates"(인증서 요구)가 선택됩니다.
- SMGetCredCertOptional - "Accept Certificates"(인증서 승인)가 선택됩니다.
- SMGetCredNoCert - "Do not accept certificates"(인증서를 승인하지 않음)가 선택됩니다.

참고: SiteMinder SSL 인증 설정의 일부로 SiteMinder 는 인증 체계에 필요한 SSL 연결 유형에 따라 SSL 가상 디렉터리를 구성합니다.

각 SiteMinder 가상 디렉터리에 대해 다음 설정 확인

다음 단계를 수행하십시오.

IIS 웹 서버의 경우

1. 관리 콘솔에서 가상 디렉터리를 마우스 오른쪽 단추로 클릭하고 "속성"을 선택합니다.
2. "디렉터리 보안" 탭을 클릭합니다.
3. "Edit Secure Communications"(보안 통신 편집)를 클릭합니다.

Apache 웹 서버의 경우

httpd.conf 파일에서 SSLVerifyClient 를 다음과 같이 설정하십시오.

- SSL 을 통한 기본 인증의 경우: SSLVerifyClient none
- 인증서 또는 기본 인증의 경우: SSLVerifyClient optional
- 인증서/인증서 및 기본 인증의 경우: SSLVerifyClient require

참고: 인증서가 필수이거나 선택 사항인 Apache 기반 웹 서버의 경우에는 httpd.conf 파일에서 "SSL Verify Depth 10" 줄의 주석 처리를 제거해야 합니다.

웹 서버의 인증서 만료 확인

Netscape 서버

1. "Netscape Server Administration"(Netscape 서버 관리)에서 "Keys & Certificates"(키 및 인증서)를 클릭합니다.
2. "Manage Certificates"(인증서 관리)를 클릭합니다.
3. "ServerCert"를 클릭합니다.
4. 인증서가 트러스트되었고 만료되지 않았는지 확인합니다.

IIS 서버

1. 관리 콘솔에서 웹 서버를 마우스 오른쪽 단추로 클릭하고 "속성"을 선택합니다.
2. "디렉터리 보안" 탭을 클릭합니다.
3. "보안 통신" 패널에서 "키 관리자"를 클릭합니다.

4. 키를 선택합니다. 속성을 보고 키가 만료되지 않았는지 확인하십시오.
5. 웹 서버를 다시 시작합니다.

Apache 서버

Apache 웹 서버 인증서가 만료되면 서버가 시작될 때 오류 메시지가 표시됩니다.

브라우저 인증서 유효성 확인

인증서가 누락되었거나 유효하지 않을 경우 인증서 메시지를 받지 못할 수 있습니다.

웹 브라우저를 열고 브라우저 인증서의 유효성을 확인하십시오.

인증서 메시지가 표시된 후 인증 실패 메시지가 표시됨

Apache 웹 서버

- SSL 웹 서버에 제공된 인증서의 인증 기관이 포함되어 있는지 확인하십시오.
- SSL 웹 서버가 해당 인증서의 인증 기관을 트러스트하는지 확인하십시오.
- SSL Verify Depth 10 줄의 주석 처리가 제거되었는지 확인하십시오.

Netscape 웹 서버

인증서의 인증 기관이 표시되고 인증서에 대한 트러스트가 만료되지 않았는지 확인하십시오. 누락 또는 만료된 경우 새 인증 기관 인증서를 설치하십시오.

IIS 웹 서버

인증서가 표시되고 유효한지 확인하십시오. 누락 또는 만료된 경우 새 인증서를 설치하십시오. 대상 디렉터리로 이동할 수 있으면 인증서가 올바르게 설치됩니다.

정책 서버 및 웹 에이전트의 구성이 올바른지 확인

정책 서버 및 웹 에이전트의 구성을 확인하십시오.

다음 단계를 수행하십시오.

1. 정책 서버가 올바르게 생성되었는지 확인합니다.
2. 웹 에이전트에 올바른 정책 서버 정보가 포함되어 있는지 확인합니다.
3. 웹 에이전트가 사용되도록 설정되어 있는지 확인합니다.
4. 웹 에이전트와 정책 서버를 다시 시작합니다.

SiteMinder 정책이 액세스를 허용해야 하는데 SSL 인증 실패 메시지가 표시됨

이 상황은 여러 구성 오류로 인해 발생할 수 있습니다. 일반적인 오류에는 다음이 포함됩니다.

- SSL 서버가 클라이언트 인증서를 요구하도록 구성되어 있지 않습니다. 따라서 클라이언트가 인증서를 전달하지 않으므로 제품의 인증 프로세스가 사용되지 않습니다. 웹 에이전트의 로깅 옵션이 사용되도록 설정하여 이러한 상황을 확인할 수 있습니다. 적절한 로그에는 해당 사용자가 알 수 없는 사용자로 나타납니다. 이 문제를 해결하려면 SSL 웹 서버에서 "Require Certificates"(인증서 요구)를 설정하십시오.
- 정책이 올바르게 생성되지 않았습니다. 해당 정책과 관련된 사용자를 확인하십시오.
- Apache 웹 서버의 경우 SSL Verify Depth 가 올바르게 설정되어 있고 주석 처리가 제거되어 있는지 확인하십시오.

구성 요소를 찾을 수 없다는 오류 메시지가 표시됨

이 오류는 인증 체계 매개 변수가 잘못 구성된 경우에 발생합니다. 리더렉션이 올바르게 구성되지 않았으므로 웹 서버가 SSL 웹 에이전트 구성 요소를 찾을 수 없습니다.

추가 정보:

[인증 체계](#) (페이지 287)

인증서 또는 기본 인증을 실행 중인데 기본 자격 증명을 입력할 수 없음

Netscape 웹 서버에서 인증서 또는 기본 체계를 실행하려면 웹 서버에 암호화 기능이 설정되어 있어야 하지만 인증서는 필요하지 않습니다.

"Netscape Server Administration"(Netscape 서버 관리)의 "Encryption Preferences"(암호화 기본 설정)에서 "Require Certificates"(인증서 요구)가 "No"(아니요)로 설정되어 있는지 확인하십시오.

부록 B: LanMan 사용자 디렉터리

이 섹션은 다음 항목을 포함하고 있습니다.

[LanMan 사용자 디렉터리 정보](#) (페이지 803)

[LanMan 디렉터리 연결 사전 요구 사항](#) (페이지 804)

[LanMan 디렉터리 연결 구성](#) (페이지 804)

[Windows 사용자 디렉터리에 대한 장애 조치](#) (페이지 806)

[LanMan 사용자 디렉터리 검색 조건](#) (페이지 806)

LanMan 사용자 디렉터리 정보

Windows 환경에서 정책 서버는 Microsoft ADSI(Active Directory 서비스 인터페이스) 계층을 통해 디렉터리 서비스의 리소스를 열거하고 관리합니다. 이 계층은 분산 컴퓨팅 환경에서 다양한 네트워크 공급자의 디렉터리 서비스 기능을 추상화합니다. 그러나 현재 버전의 ADSI에는 정책 서버의 성능에 부정적인 영향을 줄 수 있는 고유한 제한 사항이 있습니다.

ADSI를 사용할 경우 모든 Windows 디렉터리 요청은 항상 PDC(기본 도메인 컨트롤러)를 먼저 통과해야 합니다. 따라서 PDC가 처리해야 하는 네트워크 트래픽이 늘어납니다. 이 문제를 해결하기 위한 사용자 지정 솔루션은 정책 서버가 PDC를 바이패스하여 Windows 디렉터리 요청을 BDC(백업 도메인 컨트롤러)로 전달하는 것입니다. 정책 서버는 LanMan 디렉터리 연결을 사용하여 이러한 유형의 사용자 지정 솔루션을 처리합니다.

LanMan 사용자 디렉터리 연결 옵션을 사용하면 Windows 레지스트리에서 각 사용자 디렉터리 조회에 사용되는 BDC의 장애 조치 목록을 지정할 수 있습니다. 정책 서버는 LanMan 디렉터리 연결을 사용하여 Windows 디렉터리 요청을 레지스트리 목록의 첫 번째 활성 BDC로 보냅니다. LanMan 연결은 PDC를 무시합니다.

LanMan 디렉터리 연결 사전 요구 사항

정책 서버가 LanMan 디렉터리 연결을 사용하여 Windows 디렉터리의 사용자 데이터에 액세스하려면 먼저 다음 조건을 충족해야 합니다.

- 정책 서버 설치 디렉터리에 SmDsLanman.dll 파일이 있어야 합니다. 기본 위치는 다음과 같습니다.

installation_directory\netegrity\siteminder\bin

- LanMan 디렉터리에 대한 연결을 구성하십시오.

추가 정보:

[LanMan 디렉터리 연결 구성](#) (페이지 804)

LanMan 디렉터리 연결 구성

LanMan 사용자 디렉터리를 구성할 수 있습니다. 다음 프로세스에는 정책 서버에 대한 사용자 디렉터리 연결을 생성하는 단계가 나와 있습니다.

1. [LanMan 디렉터리 연결에 대한 레지스트리 키를 구성합니다](#) (페이지 805).
2. LanMan 사용자 디렉터리 연결을 구성합니다.

LanMan 디렉터리 연결에 대한 레지스트리 키 구성

LanMan 디렉터리 연결을 구성하는 첫 번째 절차는 적절한 레지스트리 키를 구성하는 것입니다.

다음 단계를 수행하십시오.

1. Windows "시작" 메뉴에서 "실행"을 선택합니다.
2. **regedit** 를 입력하고 "확인"을 클릭합니다.
3. 다음 레지스트리 키를 수정합니다.
 - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Ds 에서 NameSpaces 키는 다음 문자열 값으로 설정되어 있습니다.
"LDAP:,ODBC:,OCI:,WinNT:,Custom:,AD:"
 - NameSpaces 레지스트리 키의 값 데이터에 문자열 Lanman 을 추가합니다.
4. 다음 레지스트리 키를 생성합니다.
 \HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Ds\Lanman_DC
5. Lanman_DC 키 아래에 NT 도메인 이름의 레지스트리 키를 생성합니다.
 \HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Ds\Lanman_DC\<NT_domain_name>
 예를 들면 다음과 같습니다.
 \HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Ds\Lanman_DC\MyDomain
6. 새로 생성된 NT 도메인 키 아래에 DWORD 유형의 NumUserDir 라는 레지스트리 값을 생성합니다. 값 데이터에 대해 이 NT 도메인의 사용자 디렉터리에 대한 실제 개별 집합 수(최대 16 개)를 입력합니다.
7. BDC 의 각 장애 조치 목록에 대해 UserDir0, UserDir1, ..., UserDirN 이라는 문자열 레지스트리 값을 0 부터 시작하여 순서대로 생성합니다.
8. 각 장애 조치 목록에 해당하는 쉼표로 구분된 문자열을 입력합니다.
 SmDsLanman 이 목록을 읽고 각 장애 조치 목록에서 NT 사용자 및 그룹을 조회할 첫 번째 활성 BDC 를 찾습니다.
9. 다른 NT 도메인에 대해 5~7 단계를 반복합니다.
10. 정책 서버 서비스를 다시 시작합니다.

LanMan 사용자 디렉터리 연결 구성

정책 서버가 LanMan Directory 사용자 저장소와 통신할 수 있도록 사용자 디렉터리 연결을 구성할 수 있습니다.

다음 단계를 수행하십시오.

1. "인프라", "디렉터리"를 차례로 클릭합니다.
2. "사용자 디렉터리"를 클릭합니다.
3. "사용자 디렉터리 만들기"를 클릭합니다.
4. 사용자 디렉터리의 이름과 설명을 입력합니다.
5. "네임스페이스" 목록에서 LanMan 을 선택합니다.
6. 레지스트리 키에서 구성한 NT 도메인의 이름을 "Domain Controller Key"(도메인 컨트롤러 키) 필드에 입력합니다.
7. 제출을 클릭합니다.

Windows 사용자 디렉터리에 대한 장애 조치

LanMan 사용자 디렉터리 연결에 대해 생성하는 레지스트리 키 목록에 따라 장애 조치 순서가 결정됩니다.

LanMan 사용자 디렉터리 검색 조건

LanMan 디렉터리 연결은 일종의 Windows 사용자 디렉터리 연결입니다. LanMan 디렉터리 연결 기능은 일반 Windows 연결과 유사합니다. 유일한 차이점은 어떤 실제 도메인 컨트롤러가 요청을 처리하는지 여부입니다. 이 구성은 사용자 디렉터리 검색의 실행 절차에는 영향을 주지 않습니다.

추가 정보:

[사용자 디렉터리 검색](#) (페이지 226)

부록 C: CA SSO/WAC 통합

이 섹션은 다음 항목을 포함하고 있습니다.

[CA SSO/WAC 통합 개요](#) (페이지 807)

[SiteMinder 및 CA SSO 통합 아키텍처 예](#) (페이지 808)

[SiteMinder 및 CA SSO 통합 사전 요구 사항](#) (페이지 814)

[SiteMinder 에서 CA SSO 로의 싱글 사인온 구성](#) (페이지 815)

[CA SSO 클라이언트에서 SiteMinder 로의 싱글 사인온 구성](#) (페이지 817)

[CA SSO 에서 SiteMinder 로의 싱글 사인온 구성](#) (페이지 818)

[smetssockie 웹 에이전트 활성 응답 특성 구성](#) (페이지 821)

[smauthetssso 사용자 지정 인증 체계 구성](#) (페이지 822)

CA SSO/WAC 통합 개요

이 제품은 CA SSO 환경에 싱글 사인온 기능을 제공합니다. 사용자는 두 제품 모두에서 환경에 로그인합니다. 인증된 후에는 사용자는 두 환경 모두에 액세스할 수 있습니다. 모든 인증된 사용자는 권한이 있는 한 자격 증명을 다시 입력하지 않고도 두 환경의 보호된 리소스에 액세스할 수 있습니다. 사용자 권한 부여는 각 환경 내에서 적용되는 정책을 기반으로 합니다.

사용자가 보안 리소스에 액세스할 수 있도록 허용할 때 두 제품은 사용자 자격 증명을 각각 자체 세션 저장소에 보관합니다. 또한 이러한 제품은 별도로 유지 관리되는 자체적인 독립 세션 자격 증명을 가지고 있습니다. 이러한 자격 증명에 다른 저장소에 있으므로 정책 서버 및 CA SSO 정책 서버는 동일한 쿠키 도메인의 일부여야 합니다. 이들은 또한 사용자 또는 인증 저장소를 공유해야 합니다.

싱글 사인온 구성에서 두 정책 서버는 동일하거나 다른 컴퓨터에 위치할 수 있습니다. 이 제품에는 웹 에이전트, CA SiteMinder[®] for Secure Proxy Server 또는 둘 모두가 포함될 수 있습니다. 사용 중인 환경을 기반으로 하는 에이전트나 CA SiteMinder[®] for Secure Proxy Server 를 사용해야 합니다. CA SSO 제품은 eTrust Web Access Control(WAC) 에이전트를 사용합니다. 제품에서 싱글 사인온을 사용하기 위해 현재 환경을 수정할 필요는 없습니다.

추가 정보:

[SiteMinder 및 CA SSO 통합 아키텍처 예](#) (페이지 808)

SiteMinder 및 CA SSO 통합 아키텍처 예

다음은 SiteMinder 환경과 CA SSO 환경 간의 싱글 사인온을 보여 주는 예입니다.

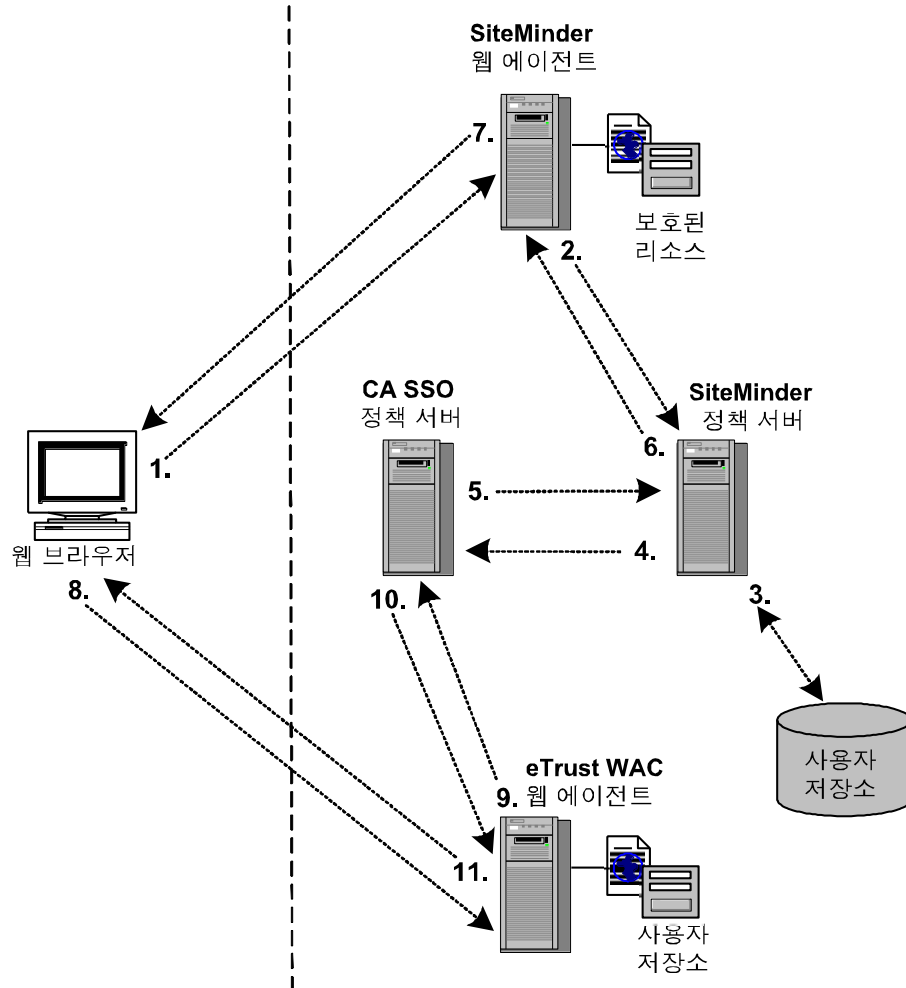
1. 사용자가 웹 브라우저를 사용하여 SiteMinder 에 대해 인증한 다음 CA SSO 로 보호된 리소스에 액세스합니다([예 1: 사용자가 CA SSO 로 보호된 리소스보다 SiteMinder 로 보호된 리소스에 먼저 액세스하는 경우](#) (페이지 809) 참조).
2. 사용자가 데스크톱 CA SSO 클라이언트를 통해 CA SSO 에 대해 인증한 다음 웹 브라우저를 사용하여 SiteMinder 로 보호된 리소스에 액세스합니다([예 2: 인증된 CA SSO 클라이언트 사용자가 SiteMinder 리소스에 액세스하는 경우](#) (페이지 811) 참조).
3. 사용자가 웹 브라우저를 사용하여 CA SSO 에 대해 인증한 다음 SiteMinder 로 보호된 리소스에 액세스합니다([예 3: 사용자가 SiteMinder 로 보호된 리소스보다 CA WAC 로 보호된 리소스에 먼저 액세스하는 경우](#) (페이지 813) 참조).

추가 정보:

[CA SSO 클라이언트에서 SiteMinder 로의 싱글 사인온 구성](#) (페이지 817)

사용자가 CA SSO 로 보호된 리소스보다 SiteMinder 로 보호된 리소스에 먼저 액세스하는 경우

다음 예에서는 사용자가 WAC 로 보호된 리소스보다 SiteMinder 로 보호된 리소스에 먼저 액세스하는 경우를 보여 줍니다.

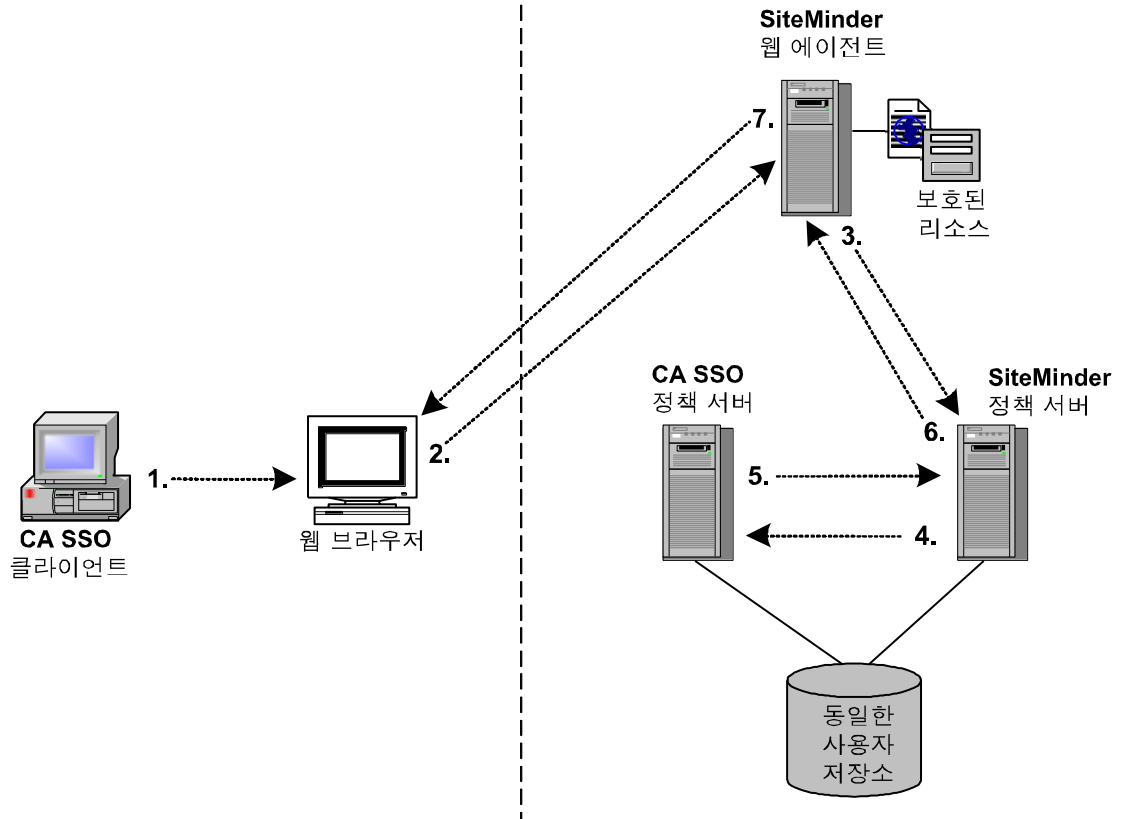


1. 사용자가 SiteMinder 로 보호된 리소스에 액세스하려고 하면 SiteMinder 웹 에이전트/CA SiteMinder® for Secure Proxy Server 가 요청을 가로챍니다. 사용자가 에이전트/SPS 에 인증 자격 증명을 제공합니다.
2. 웹 에이전트/CA SiteMinder® for Secure Proxy Server 가 유효성 검사를 위해 자격 증명을 정책 서버에 전달합니다.
3. 정책 서버는 사용자의 자격 증명 유효성을 확인합니다.
4. 인증에 성공한 후 정책 서버가 CA SSO 정책 서버에 사용자에 대한 CA SSO 쿠키를 발급하여 반환해 줄 것을 요청합니다.

5. CA SSO 정책 서버가 사용자의 유효성을 검사하고 사용자의 CA SSO 웹 인증 자격 증명을 정책 서버에 전달합니다.
6. SiteMinder 정책 서버가 CA SSO 웹 인증 자격 증명을 SiteMinder 웹 에이전트/CA SiteMinder® for Secure Proxy Server 에 전달합니다.
7. SiteMinder 웹 에이전트/CA SiteMinder® for Secure Proxy Server 가 사용자 브라우저에 CA SSO 웹 인증 및 SiteMinder 쿠키를 설정합니다. 리소스가 사용자에게 표시됩니다.
8. 사용자가 CA SSO 리소스에 액세스하려고 하면 eTrust WAC 웹 에이전트가 요청을 가로칩니다.
9. eTrust WAC 웹 에이전트가 CA SSO 정책 서버를 통해 사용자의 CA SSO 웹 인증 쿠키 자격 증명의 유효성을 검사합니다.
10. CA SSO 정책 서버가 사용자에게 유효한 자격 증명이 있음을 eTrust WAC 웹 에이전트에 알려 줍니다.
11. eTrust WAC 웹 에이전트가 CA SSO 로 보호된 리소스에 대한 사용자 액세스를 허용합니다.

인증된 CA SSO 클라이언트 사용자가 SiteMinder 리소스에 액세스하는 경우

다음 예에서는 인증된 CA SSO 클라이언트 사용자가 SiteMinder 로 보호된 리소스에 액세스하는 경우를 보여 줍니다.



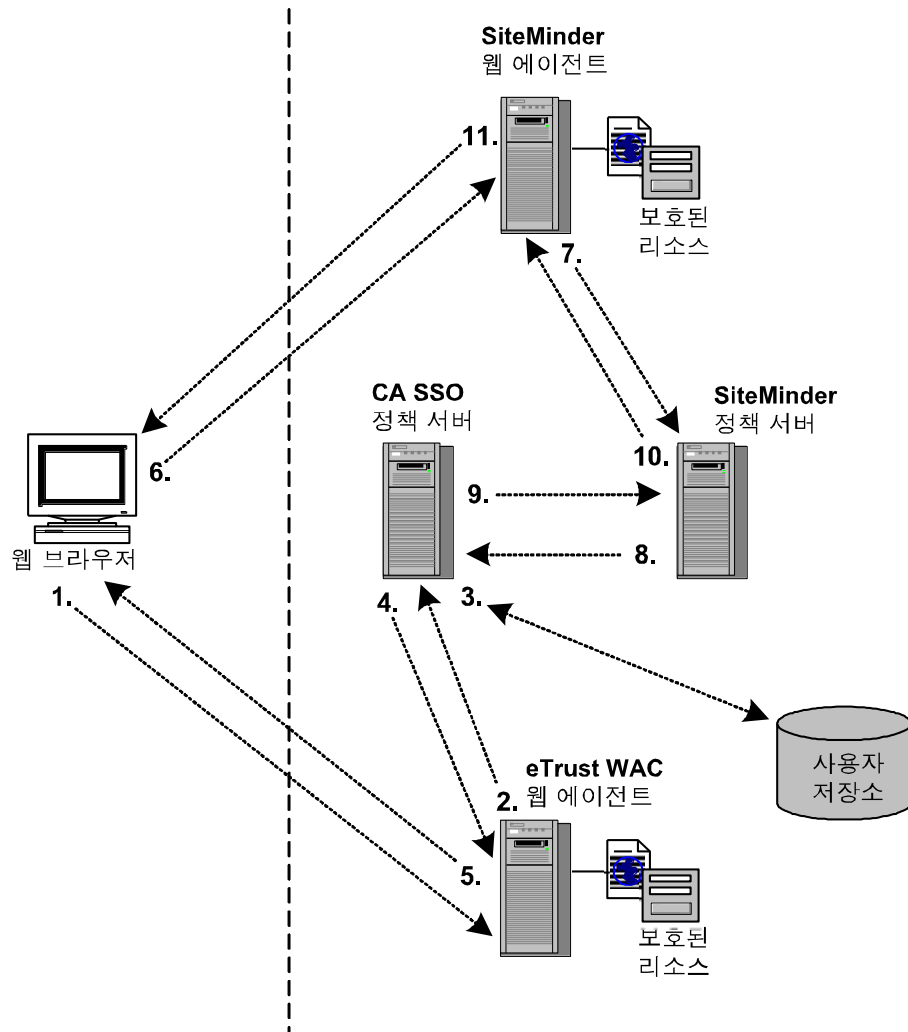
1. 인증된 CA SSO 클라이언트 사용자가 웹 브라우저를 시작합니다. 이때 CA SSO 클라이언트는 브라우저에 CA SSO 웹 인증 쿠키를 설정합니다.
2. 사용자가 웹 브라우저를 사용하여 SiteMinder 로 보호된 리소스에 대한 액세스하려고 하면 SiteMinder 웹 에이전트/CA SiteMinder® for Secure Proxy Server 가 요청을 가로칩니다.
3. SiteMinder 웹 에이전트/CA SiteMinder® for Secure Proxy Server 가 CA SSO 웹 인증 쿠키를 SiteMinder 정책 서버에 전달합니다.
4. SiteMinder 정책 서버가 CA SSO 웹 인증 쿠키를 CA SSO 정책 서버에 전달합니다.
5. CA SSO 정책 서버가 CA SSO 웹 인증 쿠키의 유효성을 검사하고 SiteMinder 정책 서버에 사용자 이름을 반환합니다.

6. SiteMinder 정책 서버가 SiteMinder 사용자 저장소에서 반환된 사용자 이름을 확인한 다음 해당하는 SiteMinder 쿠키를 발급하여 SiteMinder 웹 에이전트/CA SiteMinder® for Secure Proxy Server 에 반환합니다.
7. SiteMinder 웹 에이전트/CA SiteMinder® for Secure Proxy Server 가 SiteMinder 및 CA SSO 환경에 필요한 인증 쿠키 자격 증명이 있는 사용자에게 요청된 리소스를 반환합니다.

사용자가 SiteMinder 로 보호된 리소스보다 eTrust WAC 로 보호된 리소스에 먼저 액세스하는 경우

다음 예에서는 사용자가 제품으로 보호된 리소스보다 WAC 로 보호된 리소스에 먼저 액세스하는 경우를 보여 줍니다.

참고: 이 예에서는 환경에서 IIS6 WAC 에이전트를 사용한다고 가정합니다. IIS6 WAC 에이전트는 다음 예가 지원하는 유일한 플랫폼입니다.



1. 사용자가 CA SSO 로 보호된 리소스에 액세스하려고 하면 eTrust WAC 웹 에이전트가 요청을 가로칩니다. 사용자가 에이전트에 인증 자격 증명을 제공합니다.
2. 에이전트가 유효성 검사를 위해 자격 증명을 CA SSO 정책 서버에 전달합니다.

3. CA SSO 정책 서버는 사용자의 자격 증명이 유효한지 확인합니다.
4. CA SSO 정책 서버가 사용자의 eTrust SSO 웹 자격 증명을 eTrust WAC 웹 에이전트에 전달합니다.
5. eTrust WAC 웹 에이전트가 사용자의 웹 브라우저에서 CA SSO 웹 인증 쿠키를 설정합니다.
6. 사용자가 보호된 리소스에 액세스하려고 하면 웹 에이전트/CA SiteMinder® for Secure Proxy Server 가 요청을 가로칩니다.
7. 웹 에이전트/CA SiteMinder® for Secure Proxy Server 가 사용자의 CA SSO 웹 인증 자격 증명을 정책 서버에 전달합니다.
8. 정책 서버가 사용자의 CA SSO 웹 인증 자격 증명을 eTrust SSO 정책 서버에 전달합니다.
9. CA SSO 정책 서버가 사용자의 CA SSO 웹 인증 자격 증명의 유효성을 검사합니다. 그런 다음 CA SSO 정책 서버가 사용자 이름을 정책 서버로 다시 전달합니다.
10. 정책 서버가 사용자 저장소에서 반환된 사용자 이름을 확인한 다음 해당하는 쿠키를 발급하여 에이전트/CA SiteMinder® for Secure Proxy Server 에 반환합니다.
11. 웹 에이전트/CA SiteMinder® for Secure Proxy Server 가 사용자의 브라우저에서 쿠키를 설정합니다. 이 프로세스는 사용자가 요청된 리소스를 액세스할 수 있게 해 줍니다.

SiteMinder 및 CA SSO 통합 사전 요구 사항

SiteMinder 와 CA SSO 간의 싱글 사인온 통합을 구성하려면 먼저 다음을 수행하십시오.

1. CA SSO 를 설치하고 구성합니다.

참고: CA SSO 정책 서버를 설치할 때 다음 정보를 수집하십시오.

- SSO 관리자 이름 및 암호. SiteMinder 정책 서버는 smauthetsso 인증 체계를 통해 CA SSO 정책 서버에 대해 인증할 때 관리자 이름과 암호를 사용합니다.
- SSO 티켓 암호화 키. SiteMinder 정책 서버의 smetssocookie 활성 응답에 이 값이 필요합니다.

2. SiteMinder 환경과 CA SSO 환경은 동일한 FIPS 작동 모드(AES 암호화)에서 작동 중인지 확인합니다.

중요! 두 환경이 모두 동일한 FIPS 작동 모드에서 실행되고 있지 않으면 통합에 실패합니다.

3. 다음 사항을 고려하십시오.

- 통합이 FIPS 전용 모드에서 작동하려면 SiteMinder 정책 서버가 r12.0 SP1 CR3 이상에서 작동해야 합니다. 필요한 경우 CA SSO 정책 서버와 통신할 SiteMinder 정책 서버를 업그레이드하십시오.
- 정책 서버가 설치된 운영 체제에서 smauthetsso 인증 체계를 지원하는지 확인합니다. 통합을 위해서는 smauthetsso 인증 체계를 구성해야 합니다. 자세한 내용은 "12.52 SP1 SiteMinder Platform Support Matrix"(12.52 SP1 SiteMinder 플랫폼 지원표)를 참조하십시오.

SiteMinder 에서 CA SSO 로의 싱글 사인온 구성

이 제품은 CA SSO 환경에 싱글 사인온 기능을 제공합니다.

SiteMinder 웹 에이전트 또는 CA SiteMinder® for Secure Proxy Server 를 사용하여 SiteMinder 에서 CA SSO 로의 싱글 사인온 기능이 사용되도록 설정하려면

에이전트 또는 CA SiteMinder for Secure Proxy Server 와 함께 설치된 SiteMinder SSO 플러그인이 사용되도록 설정합니다.

Apache 2.0 웹 에이전트의 경우

- WebAgent.conf 파일의 다음 줄 중 *하나*에서 주석(#) 문자를 제거합니다.
 - (Windows operating environments)
#LoadPlugin=Path_to_eTSSOPlugin.dll_file
 - (UNIX 또는 Linux 운영 환경)
#LoadPlugin=Path_to_libetssoplugin.so_file

참고: WebAgent.conf 파일을 수정한 후에는 새 구성 설정이 적용되도록 웹 서버를 다시 시작하십시오.

6.0 CA SiteMinder® for Secure Proxy Server 의 경우

- <SPS_install_dir>\proxy-engine\conf\defaultagent\WebAgent.conf 에 있는 WebAgent.conf 파일의 다음 줄에서 주석(#) 문자를 제거합니다.

#LoadPlugin=<Path to eTSSOPlugin.dll or libetssoplugin.so>

참고: WebAgent.conf 파일을 수정한 후에는 새 구성 설정이 적용되도록 웹 CA SiteMinder® for Secure Proxy Server 를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. WAC 웹 에이전트의 webagent.ini 파일에서 다음 매개 변수를 설정하여 도메인을 구성합니다.

DomainCookie=<domain>

여기서 <domain>은 CA SSO 및 SiteMinder 웹 에이전트의 도메인과 동일한 도메인(예: test.com)입니다.

이 파일은 WAC 웹 에이전트 컴퓨터의 다음 위치에 설치됩니다.

C:\Program Files\CA\WebAccessControl\WebAgent\webagent.ini

2. webagent.ini 파일에서 다음과 같은 웹 서버 및 인증 방법 설정을 확인합니다.
 - "인증 방법" 및 "기본 인증 방법"을 SSO 로 구성하십시오.
 - WebServerName, PrimaryWebServerName, AgentName, NTLMPath 및 Secure 가 CA SSO Web Access Control 이 설치된 컴퓨터를 가리킵니다.
 - ServerName 특성이 CA SSO 정책 서버가 설치된 컴퓨터의 IP 주소를 가리킵니다.

CA SSO 정책 관리자 확인 단계

1. SiteMinder 및 CA SSO 정책 서버가 동일한 사용자 저장소 또는 인증 저장소를 사용하는지 확인합니다.
2. 다음 설정을 확인합니다.
 - SSO 관리자 이름 및 암호. SiteMinder 정책 서버는 smauthetssso 인증 체계를 통해 CA SSO 정책 서버에 대해 인증할 때 관리자 이름과 암호를 사용합니다.
 - SSO 티켓 암호화 키. 정책 서버에서 smetssocookie 의 활성 응답은 키가 필요합니다.

SiteMinder 정책 서버 구성 단계

1. 관리 UI 를 사용하여 웹 에이전트, 에이전트 구성 개체 및 호스트 구성 개체를 생성합니다.
2. SiteMinder 및 CA SSO 정책 서버에서 동일한 사용자 또는 인증 저장소를 구성합니다.
3. smetssocookie(인증서) 사용자 지정 활성 응답을 구성합니다.
4. 관리 UI 를 사용하는 도메인, 영역, 규칙을 만듭니다. SiteMinder 웹 에이전트로 모든 리소스를 보호하십시오.

참고: 규칙을 생성할 때 규칙에 smetssocookie 사용자 지정 활성 응답을 연결하십시오.

전체 확인 단계

1. 자격 증명이 있는 사용자가 SiteMinder 웹 에이전트와 WAC 웹 에이전트로 보호된 리소스에 액세스할 수 있도록 구성합니다.
2. SiteMinder 정책 서버와 관리 UI 를 호스트하는 웹 서버를 다시 시작합니다.
3. SiteMinder 웹 에이전트로 보호된 리소스에 액세스하고 이 웹 에이전트에 적절한 사용자 자격 증명을 제공합니다.
4. 동일한 브라우저 세션에서 WAC 웹 에이전트로 보호된 리소스를 요청합니다.

자격 증명에 대한 메시지 없이 이 리소스에 대한 액세스 권한을 부여받아야 합니다.

CA SSO 클라이언트에서 SiteMinder 로의 싱글 사인온 구성

SiteMinder 는 CA SSO 클라이언트에서 SiteMinder 로의 싱글 사인온 기능을 제공합니다.

CA SSO 클라이언트에서 SiteMinder 로의 싱글 사인온 기능이 사용되도록 설정하려면

SiteMinder 정책 서버 구성 단계

1. 관리 UI 를 사용하여 smauthetssso 사용자 지정 인증 체계를 구성합니다.
2. 관리 UI 를 사용하는 도메인, 영역, 규칙을 만듭니다. SiteMinder 웹 에이전트로 모든 리소스를 보호하십시오.

3. 리소스를 위한 **smauthetsso** 사용자 지정 인증 체계를 구성합니다.
4. CA SSO 클라이언트를 보호하는 브라우저에 액세스할 수 있는 사용자에게 보호된 리소스에 대한 액세스 권한을 부여하는 정책을 생성합니다.

CA SSO 클라이언트 확인 단계

CA SSO 클라이언트 **SsoCInt.ini** 파일에서 다음 항목을 설정하십시오.

참고: **SsoCInt.ini** 파일은 CA SSO 클라이언트 컴퓨터의 **C:\Program Files\CA\CA SSO\Client** 에 설치됩니다.

DomainNameServer=<eSSO_WA_FQDN> <SM_WA_FQDN>

eSSO_WA_FQDN

(선택 사항) WAC 웹 에이전트의 정규화된 도메인 이름을 지정합니다.

SM_WA_FQDN

SiteMinder 웹 에이전트의 정규화된 이름을 지정합니다.

전체 확인 단계

1. CA SSO 클라이언트, SiteMinder 정책 서버, 그리고 관리 UI 를 호스트하는 웹 서버를 다시 시작합니다.
 2. SSO 클라이언트를 통해 보호되는 브라우저에 액세스하고 정책 서버가 보호하는 리소스의 URL 을 입력합니다.
- 리소스는 SiteMinder 가 다시 챌린지하지 않고 표시됩니다.

CA SSO 에서 SiteMinder 로의 싱글 사인온 구성

SiteMinder 는 CA SSO 에서 제품으로의 싱글 사인온 기능을 제공합니다.

다음 단계를 수행하십시오.

정책 서버 구성 단계

1. 관리 UI 를 사용하여 **smauthetsso** 사용자 지정 인증 체계를 구성합니다.
2. 도메인, 영역, 규칙을 만듭니다. 웹 에이전트로 모든 리소스를 보호하십시오.
3. 보호된 리소스를 위한 **smauthetsso** 사용자 지정 인증 체계를 구성합니다.

WAC 웹 에이전트 확인 단계

1. WAC 웹 에이전트의 webagent.ini 파일에서 DomainCookie=<domain>를 설정하여 도메인을 구성합니다.

참고: 도메인 값은 CA SSO 및 SiteMinder 웹 에이전트에 대해 동일해야 합니다. 이 파일은 WAC 웹 에이전트 컴퓨터의 C:\Program Files\CA\WebAccessControl\WebAgent\webagent.ini 에 설치됩니다.

2. webagent.ini 파일에서 다음과 같은 웹 서버 및 인증 방법 설정을 확인합니다.
 - "인증 방법" 및 "기본 인증 방법" 매개 변수를 SSO 로 구성하십시오.
 - WebServerName, PrimaryWebServerName, AgentName, NTLMPath 및 Secure 가 SSO Web Access Control 이 설치된 컴퓨터를 가리켜야 합니다.
 - ServerName 특성이 CA SSO 정책 서버가 설치된 컴퓨터의 IP 주소를 가리키도록 하십시오.
 - WAC 웹 에이전트 구성에 대한 자세한 내용은 CA SSO 설명서를 참조하십시오.

SiteMinder 웹 에이전트 또는 CA SiteMinder® for Secure Proxy Server 구성 단계

1. 웹 에이전트 또는 CA SiteMinder® for Secure Proxy Server 와 함께 설치된 SSO 플러그인을 활성화합니다. 이 플러그인은 SSO 클라이언트 쿠키를 인증합니다. WebAgent.conf 파일의 다음 줄에서 주석 문자(#)를 제거하십시오.

```
#LoadPlugin=path_to_eTSSOPlugin.dll | path_to_libetssoplugin.so
```

참고: WebAgent.conf 파일은 다음 위치에 있습니다.

Apache 2.0 웹 에이전트**6.0 CA SiteMinder® for Secure Proxy Server**

```
SPS_install_dir\proxy-engine\conf\defaultagent\
```

```
SPS_install_dir
```

CA SiteMinder® for Secure Proxy Server 설치 디렉터리

2. 정책 서버를 다시 시작합니다.

전체 확인 단계

1. WAC 웹 에이전트, 정책 서버, 그리고 관리 UI 를 호스트하는 웹 서버를 다시 시작합니다.
2. WAC 웹 에이전트가 보호하는 리소스에 액세스합니다. 유효한 자격 증명을 제공하십시오.
3. 동일한 브라우저를 사용하여 동일한 브라우저에서 웹 에이전트가 보호하는 리소스에 액세스합니다.
자격 증명 챌린지 없이 리소스가 표시됩니다.

smetssocookie 웹 에이전트 활성화 응답 특성 구성

smetssocookie 웹 에이전트 활성화 응답은 SSO 쿠키를 생성하고 웹 브라우저에 보냅니다. SSO 쿠키를 사용하면 SiteMinder 에서 인증된 사용자가 다시 인증할 필요 없이 WAC 또는 CA SSO 보호 콘텐츠에 액세스할 수 있습니다.

다음 단계를 수행하십시오.

1. "정책", "도메인"을 차례로 클릭합니다.
2. "응답"을 클릭합니다.
3. "응답 만들기"를 클릭합니다.
4. 목록에서 도메인을 선택한 후 "다음"을 클릭합니다.
5. 응답의 이름과 설명을 정의합니다.
6. SiteMinder 가 선택되어 있으며 "에이전트 유형" 목록에 "웹 에이전트"가 나타나는지 확인합니다.
7. "응답 특성 만들기"를 클릭합니다.
8. "Create a new object"(새 개체 만들기)가 선택되었는지 확인하고 "확인"을 클릭합니다.
9. "특성" 목록에서 WebAgent-HTTP-Cookie-Variable 을 선택합니다.
10. "특성 종류"에서 "활성 응답"을 선택합니다.
11. "쿠키 이름" 필드에 **SSOTK** 를 입력합니다.
12. "라이브러리 이름" 필드에 **smetssocookie** 를 입력합니다.
13. "함수 이름" 필드에 **GenEtssoCookie** 를 입력합니다.

참고: 함수 이름은 대/소문자를 구분합니다.

14. "매개 변수" 필드에서 다음 토큰을 정의합니다.

```
<CA_PS_Host_Name>;<SSO_Auth_Host>;<SSO_AuthMethod>;<EncryptionKey>
```

CA_PS_Host_Name

CA SSO 정책 서버의 호스트 이름을 지정합니다.

SSO_Auth_Host

CA Policy Manager 에서 SSO 인증 호스트 이름을 지정합니다. 이 호스트 이름은 "Web Access Control Resources"(Web Access Control 리소스), "Configuration Resources"(구성 리소스), "Authentication Host"(인증 호스트)로 이동하여 지정할 수 있습니다.

필요한 값: SSO_Authhost

SSO_AuthMethod

SSO 인증 방법을 정의합니다.

필요한 값: SSO

EncryptionKey

CA Policy Manager 에서 SSO 인증 호스트 이름에 대한 티켓 암호화 키를 정의합니다.

참고: 읽기 쉽도록 토큰 앞뒤에 공백을 입력할 수 있습니다.

15. 제출을 클릭합니다.

16. "마침"을 클릭합니다.

응답은 OnAuthAccept 규칙에 추가될 수 있습니다.

smauthetsso 사용자 지정 인증 체계 구성

CA SSO SiteMinder(smauthetsso) 인증 체계를 사용하면 CA SSO/WAC 환경에서 이미 인증된 사용자가 다시 인증할 필요 없이 정책 서버에서 CA SSO 인증 자격 증명을 확인할 수 있습니다. 이 사용자 지정 인증 체계는 CA SSO 쿠키를 로그인 자격 증명으로 허용합니다. 즉, 이 자격 증명을 CA SSO 정책 서버에서 확인을 받고 여기에서 사용자 이름을 추출한 다음 사용자 저장소에 이 이름이 있는지 확인합니다. 이 인증 체계는 cookie, cookieorbasic 또는 cookieorforms 모드에서 설정할 수 있습니다.

특정한 이유로 실패한 경우 하나의 CA SSO 정책 서버가 다른 CA SSO 정책 서버로 장애 조치되도록 구성할 수 있습니다. 장애 조치를 구성하려면 "인증 체계" 페이지의 "체계 설정"에서 쉽표로 구분된 CA SSO 정책 서버 목록을 매개 변수로 필드로 지정하십시오.

다음 단계를 수행하십시오.

1. "인프라", "인증"을 차례로 클릭합니다.
2. "인증 체계"를 클릭합니다.

3. "인증 체계 만들기"를 클릭합니다.
"인증 체계 유형의 새 개체 만들기"가 선택되어 있는지 확인합니다.
"확인"을 클릭합니다.
4. "인증 체계 유형" 목록에서 "사용자 지정 템플릿"을 선택합니다.
5. "라이브러리" 필드에 **smauthetssso** 를 입력합니다.
6. "암호" 및 "암호 확인" 필드에 CA SSO 정책 서버 관리자의 암호를 입력하고 확인합니다.
7. "매개 변수" 필드에서 정렬된 토큰 집합을 다음 형식으로 정의합니다.

Mode [*; <Target>*] ; *AdminID* ; *CAPS_Host* ; *FIPS_Mode* ; *Identity_File*

참고: 토큰은 세미콜론으로 구분합니다. 읽기 쉽도록 각 토큰 앞뒤에 공백을 입력할 수 있습니다.

예: cookie ; SMPS_sso ; myserver.myco.com ; 0 ; /certificates/def_root.pem

예: cookieorforms ; /siteminderagent/forms/login.fcc ; SMPS_sso ; myserver.myco.com ; 1 ; /certificates/def_root.pem

Mode

인증 체계가 허용하는 자격 증명 유형을 지정합니다. 허용되는 값으로는 cookie, cookieorbasic 또는 cookieorforms 가 있습니다.

쿠키

CA SSO 쿠키만 허용되도록 지정합니다.

cookieorbasic

CA SSO 쿠키가 제공되지 않는 경우 기본 인증 체계를 사용하여 로그인 이름과 암호를 확인하도록 지정합니다.

cookieorforms

CA SSO 쿠키가 제공되지 않는 경우 양식 인증 체계를 사용하여 로그인 이름과 암호를 확인하도록 지정합니다.

대상

HTML 양식 인증 체계에 사용되는 .fcc 파일의 경로 이름을 지정합니다.

참고: 이 값은 cookieorforms 모드에만 필요합니다.

AdminID

CA SSO 정책 서버에 대한 CA SSO 정책 서버 관리자의 사용자 이름을 지정합니다. SiteMinder에서는 CA SSO 정책 서버에 인증할 때 관리자의 사용자 이름과 암호를 사용하여 CA SSO 쿠키의 유효성 검사를 요청합니다.

CAPS_Host

CA SSO 정책 서버가 있는 호스트의 이름을 지정합니다.

FIPS_Mode

정책 서버가 작동 중인 작업의 FIPS 모드를 지정합니다. 0 은 비-FIPS 모드를 지정합니다. 1 은 FIPS 모드를 지정합니다.

Identity_File

CA SSO 아이덴티티 파일의 경로를 지정합니다. 정책 서버는 이 파일을 사용하여 CA SSO 정책 서버와 통신합니다.

8. 제출을 클릭합니다.

제 26 장: CA User Activity Reporting Module 통합

CA User Activity Reporting Module(UAR)은 SiteMinder 와 CA UAR 의 통합을 구성하는 방법을 자세히 설명하는 SiteMinder 커넥터 안내서를 제공합니다. 사용하는 안내서는 SiteMinder 가 감사 정보를 텍스트 파일(smaccess.log)에 저장하도록 구성되었는지 ODBC 데이터베이스에 저장하도록 구성되었는지에 따라 달라집니다.

CA UAR 커넥터 안내서를 찾으려면

1. [CA User Activity Reporting Module Integration Matrix](#) (CA User Activity Reporting Module 통합 표)로 이동합니다.
2. "Product Integrations"(제품 통합) 아래에 있는 "Authentication Service"(인증 서비스)를 클릭합니다.

SiteMinder 커넥터 안내서는 CA UAR 가 사용할 로그 센서의 유형을 기반으로 합니다.

3. 다음 작업 중 *하나*를 수행하십시오.

- SiteMinder 가 감사 정보를 텍스트 파일에 저장하는 경우 파일 로그 센서용 커넥터 안내서를 사용합니다.
- SiteMinder 가 감사 정보를 ODBC 데이터베이스에 저장하는 경우 ODBC 로그 센서용 커넥터 안내서를 사용합니다.

이러한 각 안내서는 **CA UAR** 관리 UI 에서 필요한 커넥터를 생성할 때도 사용할 수 있습니다. 커넥터를 생성할 때 이러한 안내서에 액세스하려면 "도움말"을 클릭하십시오.

부록 D: 정책 서버를 RADIUS 서버로 사용

이 섹션은 다음 항목을 포함하고 있습니다.

[정책 서버를 Radius 서버로 사용](#) (페이지 827)

[RADIUS 클라이언트/서버 아키텍처](#) (페이지 828)

[정책 서버에서 RADIUS 인증이 작동하는 방식](#) (페이지 828)

[RADIUS 환경의 정책](#) (페이지 830)

[RADIUS 정책 도메인의 응답](#) (페이지 835)

[RADIUS 환경에서 SiteMinder 배포](#) (페이지 844)

[RADIUS 장치를 보호하기 위한 지침](#) (페이지 845)

[동종 RADIUS 환경에서 사용자를 인증하는 방법](#) (페이지 845)

[사용자 디렉터리가 한 개인 이중 RADIUS 환경에서 사용자 인증](#) (페이지 848)

[사용자 디렉터리가 두 개인 이중 RADIUS 환경에서 사용자를 인증하는 방법](#) (페이지 852)

[RADIUS 에이전트 그룹 개요](#) (페이지 856)

[RADIUS 에이전트 그룹 설정](#) (페이지 857)

[RADIUS 응답 그룹화](#) (페이지 858)

[RADIUS 문제 해결 및 테스트](#) (페이지 859)

정책 서버를 Radius 서버로 사용

RADIUS(Remote Authentication Dial-In User Service)는 NAS(네트워크 액세스 서버) 장치와 RADIUS 인증 서버 간에 세션 인증 및 구성 정보를 교환할 수 있게 해 주는 프로토콜입니다. 정책 서버를 RADIUS 인증 서버로 사용할 수 있습니다.

RADIUS 프로토콜은 다음과 같은 역할을 하는 NAS 장치에서 종종 사용됩니다.

- ISP(인터넷 서비스 공급자)용 프록시 서비스
- 방화벽
- 회사 전화 접속 보안 서비스

RADIUS 클라이언트/서버 아키텍처

RADIUS 는 NAS 장치가 제공하는 통신 기술을 인증 서버가 제공하는 보안 기술과 구별하여 보안을 단순화하기 위해 설계되었습니다. RADIUS 보안은 분산 클라이언트/서버 아키텍처를 사용하여 네트워크 및 네트워크 서비스에 대한 원격 액세스를 보호합니다. 정책 서버는 RADIUS 서버이고, NAS 장치는 RADIUS 클라이언트입니다.

NAS 장치는 다음 중 하나를 수행합니다.

- SLIP 또는 PPP 등의 전화 접속 프로토콜을 지원하고, RADIUS 인증 서버를 사용하여 사용자를 인증하며, 사용자를 네트워크로 라우팅합니다.
- 방화벽을 통한 네트워크 직접 연결을 지원하고, RADIUS 인증 서버를 사용하여 사용자를 인증하며, 네트워크 액세스 권한을 부여합니다.

정책 서버는 이 장에서 설명한대로 구성된 경우 RADIUS 인증 서버의 역할을 할 수 있습니다. RADIUS 서버로 사용되는 정책 서버는 RADIUS 인증 체계와 미리 정의된 사용자 디렉터리를 사용하여 RADIUS 사용자를 인증합니다.

참고: RADIUS 계정을 사용하려면 별도의 RADIUS 계정 서버를 구성해야 합니다. 정책 서버는 계정 서버에 ACK 응답을 보내 NAS 장치를 지원합니다. 그러나 계정 정보는 파일에 로깅할 수 있습니다.

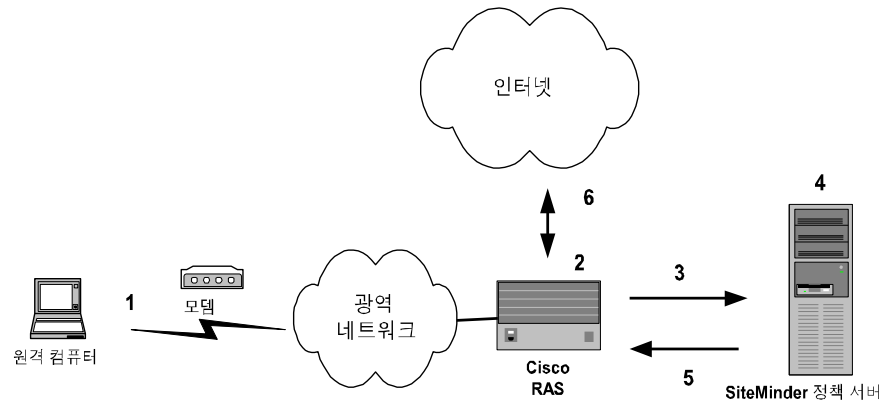
추가 정보:

[계정 설정 및 디버깅을 위한 RADIUS 로그 생성](#) (페이지 859)

정책 서버에서 RADIUS 인증이 작동하는 방식

정책 서버는 NAS 장치와 일련의 통신을 통해 사용자를 인증합니다. SiteMinder 가 사용자를 인증하면 NAS 는 해당 사용자에게 적절한 네트워크 서비스에 대한 액세스 권한을 제공합니다.

다음 그림에서는 이 인증 프로세스를 보여 줍니다.



1. 전화 접속 모뎀을 사용하는 사용자가 인터넷에 액세스할 수 있게 해 주는 Cisco RAS(NAS 장치)에 대한 연결을 열려고 합니다.
2. RAS가 RADIUS 사용자 프로필을 사용하여 사용자를 인증해야 하는지 확인합니다.
3. RAS가 정책 서버에 사용자 연결 요청을 보냅니다.
4. 정책 서버가 다음 방법 중 하나를 사용하여 사용자 이름과 암호를 가져옵니다.
 - PAP(암호 인증 프로토콜)를 사용하여 인증
PAP는 호스트가 양방향 핸드셰이크에서 아이덴티티를 설정하기 위한 간단한 방법을 제공하는 PPP 인증 프로토콜입니다. 인증은 초기 연결 설정 시에만 발생하며 이때 암호화는 사용되지 않습니다.
 - CHAP(Challenge-Handshake 인증 프로토콜)를 사용하여 인증
CHAP는 보안 PPP 인증 프로토콜이기도 합니다. CHAP를 사용하면 3방향 핸드셰이크 및 암호화를 사용하여 호스트의 아이덴티티를 정기적으로 확인할 수 있습니다. 인증은 초기 연결 설정 시에만 발생합니다. RAS는 연결이 이루어진 후 언제든지 인증 프로세스를 반복할 수 있습니다.
 - Security Dynamics ACE/서버 또는 Secure Computing SafeWord 서버를 사용하여 인증

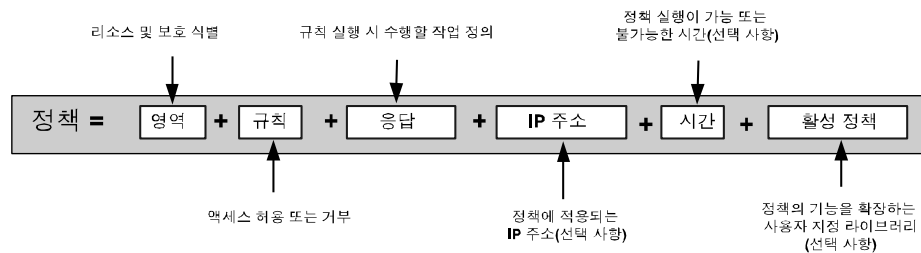
5. 정책 서버가 RAS 에 인증 응답을 보냅니다.
 6. 다음 중 하나가 발생합니다.
 - 인증에 실패한 경우 RAS 가 연결을 거부합니다.
 - 인증에 성공한 경우 RAS 가 사용자 인증 시 실행되는 SiteMinder 응답에서 특성 목록을 받습니다. 특성은 사용자의 네트워크 세션을 구성하는 사용자 프로파일로 사용됩니다.
- RAS 가 정책 서버에 세션이 시작되었다는 사실과 세션이 종료되는 시기를 알립니다.

RADIUS 환경의 정책

SiteMinder RADIUS 정책은 RADIUS 에이전트에 의해 적용되며, 다음 요소들을 바인딩함으로써 생성됩니다.

- 인증 규칙
- 응답
- 사용자 또는 사용자 그룹
- IP 주소, 시간 및 활성 정책(선택 사항)

다음 다이어그램에서는 정책의 기본 구조를 보여 줍니다.

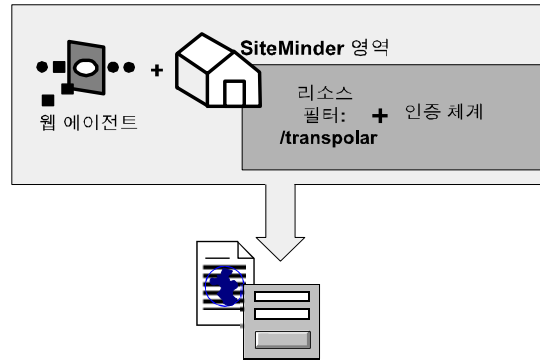


RADIUS 정책은 SiteMinder 에이전트가 사용하는 정책에 포함된 것과 동일한 요소로 구성되지만 RADIUS 에이전트가 이러한 구성 요소를 해석하는 방식에는 차이가 있습니다. 규칙, 영역 및 응답은 다음 표에서 보여 주는 것과 같이 각기 다른 기능을 수행합니다.

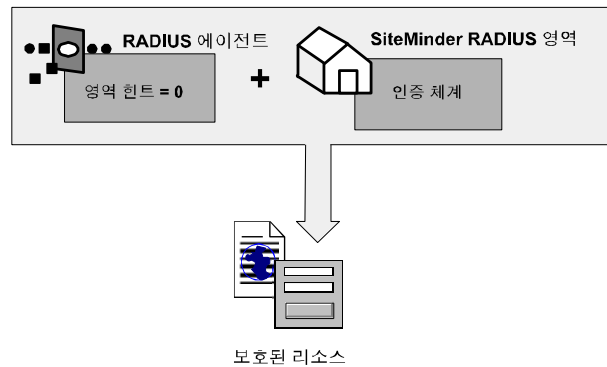
정책 구성 요소	RADIUS 정책에서의 기능	SiteMinder 에이전트 정책에서의 기능
영역	■ 에이전트를 식별합니다. ■ 인증 체계를 식별합니다. ■ 세션 만료 시간을 정의합니다.	■ 리소스 필터(SiteMinder 에이전트가 제어하는 도메인 내의 디렉터리)를 정의합니다. ■ 에이전트를 식별합니다. ■ 인증 체계를 식별합니다. ■ 리소스의 상태(보호됨 또는 보호 안 함)를 정의합니다. ■ 처리할 이벤트(인증 또는 권한 부여)를 식별합니다. ■ 세션 만료 시간을 정의합니다.
규칙	■ 인증만 수행합니다. ■ 액세스를 허용하거나 거부합니다. ■ 시간 또는 활성 규칙 제한을 정의합니다.	■ 리소스 필터를 정의합니다. ■ 작업(웹 에이전트 작업, 권한 부여 이벤트 또는 인증 이벤트)을 정의합니다. ■ 액세스를 허용하거나 거부합니다. ■ 권한 부여 및 인증을 수행합니다. ■ 시간 또는 활성 규칙 제한을 정의합니다.
응답	■ 인증 이벤트에 대해 반환할 값을 정의합니다.	■ 권한 부여 이벤트에 대해 반환할 값을 정의합니다. ■ 인증 이벤트에 대해 반환할 값을 정의합니다. ■ 권한 부여 거부 이벤트에 대해 반환할 값을 정의합니다. ■ 인증 거부 이벤트에 대해 반환할 값을 정의합니다.

RADIUS 및 비 RADIUS 리소스 비교

RADIUS 환경에서는 리소스 식별 방식으로 인해 RADIUS 정책의 요소가 부분적으로 다르게 처리됩니다. SiteMinder 에이전트 환경에서는 특정 리소스가 영역 정의의 리소스 필터를 사용하여 식별됩니다. 리소스 필터는 리소스의 디렉터리 위치를 식별합니다. 또한 영역 정의는 다음 다이어그램에 표시된 것과 같이 웹 에이전트와 인증 체계를 식별합니다.



다음 다이어그램에 표시된 것과 같이 RADIUS 환경에서는 보호된 리소스가 배치되는 방식이 다릅니다. 필터를 사용하여 리소스를 식별하는 영역 대신 RADIUS 에이전트는 *영역 힌트*를 사용하여 리소스를 식별합니다. 영역 힌트는 정책 서버가 사용자를 인증할 도메인을 설정할 수 있게 해 주는 특성입니다. 영역 힌트는 에이전트가 보호하는 특정 영역을 식별하거나 에이전트가 전체 NAS 장치를 보호해야 함을 나타냅니다.



영역 힌트 사용

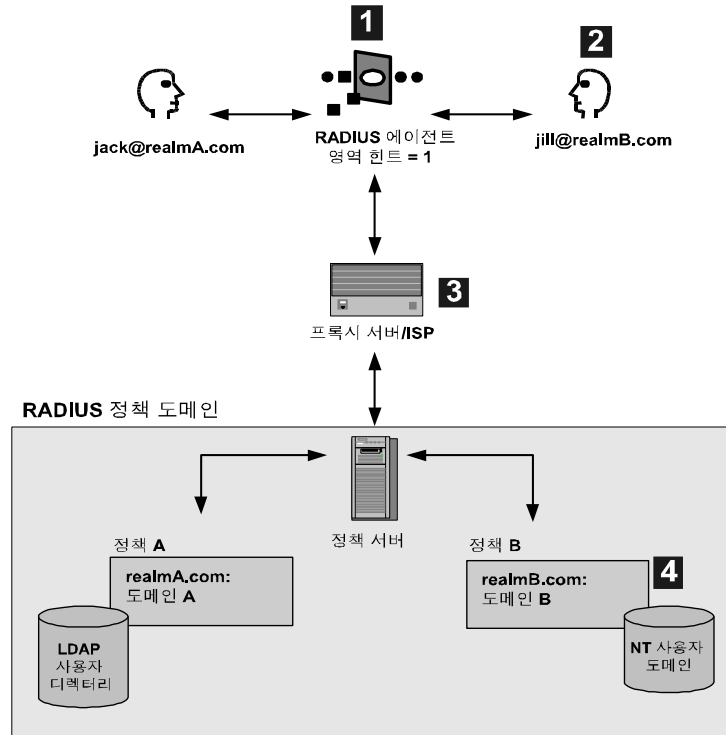
도메인 A 및 도메인 B 와 같이 서로 다른 도메인의 사용자를 인증해야 하는 NAS 장치를 RADIUS 에이전트에서는 어떤 방법으로 보호할까요? 영역 힌트는 SiteMinder 가 사용자를 인증할 올바른 도메인을 결정할 수 있게 해주는 RADIUS 특성입니다. RADIUS 에이전트에 다음과 같은 영역 힌트 값 중 하나를 제공해야 합니다.

- 0 - (기본값) 정책 도메인에 영역이 하나만 있으므로 힌트가 필요하지 않음을 나타냅니다. 영역은 NAS 장치에 직접 바인딩됩니다.
- 1 - (RADIUS User-Name 특성) 아래에 설명된 대로 SiteMinder 가 이 특성의 사용자 이름에서 영역 이름을 구문 분석하고 연결된 도메인을 찾습니다.
- 도메인의 실제 이름이 포함된 특성. 일부 NAS 장치에서는 이 특성을 사용할 수 없습니다. 자세한 내용은 사용 중인 NAS 장치의 제품 설명서를 참조하십시오.

영역 힌트가 1 로 설정된 경우 영역 이름은 사용자 이름 특성에서 구문 분석됩니다. 사용자 이름과 영역 이름의 구분 기호는 "@" 또는 "/"여야 합니다.

- 구분 기호가 "@"인 경우 "@" 뒤의 요소가 영역 이름입니다. 예를 들어 jack@realmA.com 에서 영역은 realmA.com 입니다.
- 구분 기호가 "/"인 경우 "/" 앞의 요소가 영역 이름입니다. 예를 들어 x5/jack 에서 영역은 x5 입니다.

다음 다이어그램 및 설명에서는 프록시 서버가 사용자를 인증할 올바른 SiteMinder 도메인을 결정하는 방법을 보여 줍니다.



1. RADIUS 에이전트 하나가 두 SiteMinder 도메인을 모두 보호합니다.
RADIUS 에이전트는 영역 힌트 값 1 로 구성되어 있습니다.
2. Jill 이 ISP 의 프록시 서버에 액세스하려고 하면 RADIUS 에이전트는 해당 요청을 가로채어 Jill 의 사용자 이름 특성 jill@realmB.com 을 정책 서버에 전달합니다.
3. 정책 서버가 사용자 이름 특성에서 사용자 이름과 영역 이름을 구문 분석합니다.
예: jill@realmB.com 의 경우, jill 은 사용자 이름이고 realmB.com 은 영역 이름입니다.
정책 서버가 영역 이름과 연결된 도메인을 식별합니다. realmB.com 과 연결된 도메인은 도메인 B 입니다.
4. 정책 서버가 적절한 디렉터리에서 사용자 이름을 인증합니다. 사용자 이름 jill 이 정책 B: realmB.com: 도메인 B 에 대해 정의된 NT 사용자 도메인에서 인증됩니다.

RADIUS 정책 도메인의 응답

SiteMinder 응답은 사용자가 인증된 경우 RADIUS 특성을 NAS 장치에 반환하는 데 사용될 수 있습니다. 특성은 사용자가 인증된 후 세션의 특성을 구성하고 인증된 사용자의 사용자 프로필을 정의합니다. 사용자 프로필은 NAS 장치에서 사용될 수 있습니다. 예를 들어 응답에 특성을 사용하면 RADIUS 사용자 세션에 대한 제한 시간을 정의할 수 있습니다.

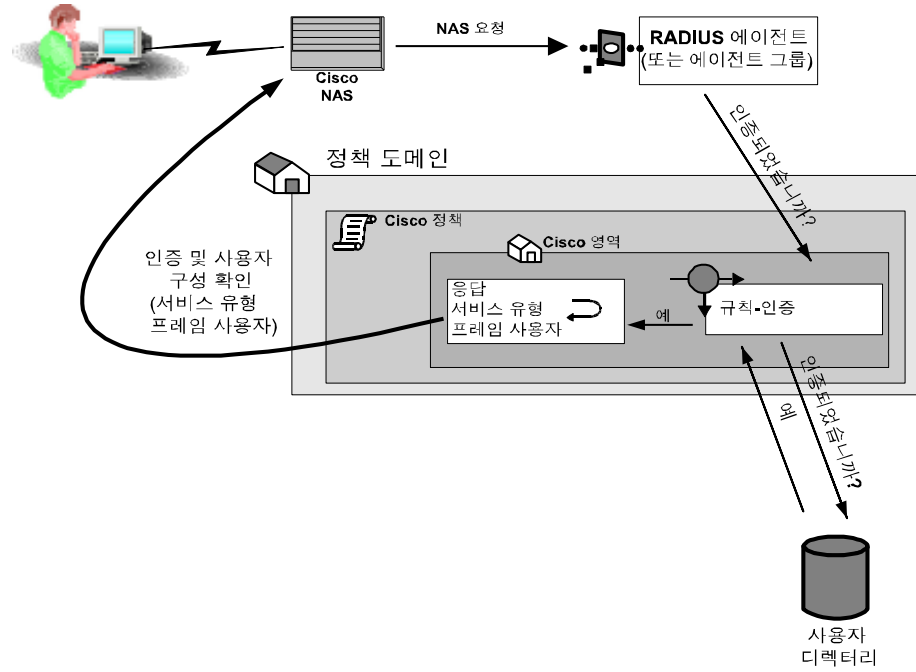
응답을 사용하여 사용자에게 권한을 할당하는 사용자 프로필 정보를 NAS 장치에 제공할 수 있습니다. 예를 들어 한 사용자에게 리소스에 대한 무제한 액세스를 허용하고 다른 사용자에게는 동일한 리소스에 대한 액세스를 제한할 수 있습니다. 이때 응답을 사용하면 주로 RADIUS가 유일한 인증 메커니즘인 경우에도 사용자에게 권한을 부여할 수 있습니다.

참고: NAS가 인증만 지정하는 경우에는 기본적으로 SiteMinder가 RADIUS 특성을 반환하지 않습니다. NAS가 인증만 지정하는 경우 RADIUS 특성을 반환하려면 [항상 RADIUS 특성을 반환하도록 SiteMinder 구성](#) (페이지 839)의 지침을 따르십시오.

응답 작동 방식

RADIUS 응답은 인증하는 규칙과 쌍으로 연결됩니다. 규칙이 사용자를 성공적으로 인증하면 RADIUS 응답이 트리거됩니다. 규칙이 사용자를 인증하지 않는 경우에는 응답이 트리거되지 않습니다.

응답이 트리거되면 정책 서버는 응답에 포함된 특성을 NAS 장치로 보냅니다. 이 정보는 다음 다이어그램과 같이 사용자의 세션을 사용자 지정하는 데 사용됩니다.



특성 유형

응답에는 다음 특성을 사용할 수 있습니다.

- 사용자 특성
- DN 특성
- 활성 응답 특성
- Radius 특성

사용자 특성

이 특성은 LDAP, WinNT 또는 ODBC 사용자 디렉터리의 사용자와 연결된 정보를 반환합니다. 사용자 특성은 사용자 디렉터리에서 검색되며 RADIUS 장치의 동작을 수정하는 데 사용될 수 있습니다.

DN 특성

이 특성은 사용자와 관련된 LDAP 디렉터리 개체에 연결된 프로필 정보를 반환합니다. 예를 들어 DN 특성은 사용자의 그룹 또는 OU(조직 단위)와 같은 LDAP 개체에 대한 정보를 반환할 수 있습니다.

활성 응답 특성

이 특성은 SiteMinder 권한 부여 API 를 사용하여 개발된 사용자 지정 라이브러리의 값을 반환합니다. 활성 응답은 SiteMinder 가 사용자 지정 라이브러리의 함수를 호출할 때 생성됩니다.

Radius 특성

이 특성은 다음과 같은 에이전트 유형 특성으로 정의된 값을 반환합니다.

RADIUS

RADIUS 프로토콜 사양인 *RFC(Request for Comment) 2138* 에 정의된 일반 Radius 특성입니다. 이러한 특성의 식별자에는 1-25 및 27-63 이 포함됩니다. 이러한 특성 중 일부는 동일한 응답에서 여러 번 사용될 수도 있습니다.

RADIUS 에이전트 유형은 일반 RADIUS 특성이 포함된 응답을 반환할 수 있습니다.

RADIUS 확장

NAS 장치의 사전 파일에 정의된 특성입니다. 이러한 특성은 일반 Radius 특성으로 정의되지 않는 값을 정의하며 사용 중인 NAS 장치 유형과 관련됩니다. 이러한 특성의 고유 식별자는 일반 Radius 특성에 예약된 범위를 벗어나 64 부터 시작합니다. 예를 들어 Lucent 는 식별자 195 를 사용하는 *Ascend-Disconnect-Cause* 라는 확장 RADIUS 특성을 제공합니다.

확장 RADIUS 특성의 공급업체 유형과 일치하는 에이전트 유형만 이 특성을 사용할 수 있습니다. 예를 들어 Shiva 에이전트 유형은 Shiva에 대해 정의된 확장 RADIUS 특성을 사용할 수 있지만 Cisco 에이전트 유형은 응답에 Shiva 확장 특성을 사용할 수 없습니다. 응답에 사용되는 확장 특성은 RADIUS 클라이언트의 사전 파일에 정의된 특성과 일치해야 합니다.

기본적으로 SiteMinder는 이러한 특성을 사용하는 Ascend(Lucent) 등의 일부 에이전트 유형에 대한 미리 정의된 RADIUS 확장 특성을 제공합니다. 필요한 경우 RADIUS 에이전트 유형에 대한 추가 RADIUS 확장 특성을 정의할 수도 있습니다.

공급업체 관련

NAS 장치의 사전 파일에 정의된 특성으로, 식별자로 26을 사용합니다. 공급업체 관련 특성을 사용하여 일반 Radius 특성이 제공하지 않는 값의 특성을 정의할 수 있습니다. 일부 공급업체에서는 RADIUS 확장 특성 대신 또는 RADIUS 확장 특성에 추가적으로 공급업체 관련 특성을 사용합니다. 예를 들어 Cisco는 RADIUS 확장 특성을 사용하지 않지만 이 NAS 장치는 Cisco AV-pair 및 Account-Info 같은 여러 공급업체 관련 특성을 지원합니다.

공급업체 관련 특성을 사용하여 다른 프로토콜에 정보를 전달할 수 있습니다. 예를 들어 Cisco AV-pair 특성에 대한 공급업체 관련 특성을 정의하여 TACACS+ 서버에 TACACS+ 정보를 전달할 수 있습니다.

공급업체 관련 특성은 RADIUS 클라이언트의 공급업체 유형과 일치하는 응답에서만 정의할 수 있습니다.

기본적으로 SiteMinder는 Network Associates의 Sniffer 에이전트 유형과 같이 이러한 특성을 사용하는 일부 에이전트 유형에 대한 미리 정의된 공급업체 관련 특성을 제공합니다. 필요한 경우 RADIUS 에이전트 유형에 대한 추가 RADIUS 확장 특성을 정의할 수도 있습니다.

참고: RADIUS 특성에 대한 자세한 내용은 *Request for Comment (RFC) RADIUS Protocol 2138*(RFC(Request for Comment) RADIUS 프로토콜 2138)을 참조하십시오.

추가 정보:

[에이전트 유형에 대한 특성 만들기](#) (페이지 839)

항상 RADIUS 특성을 반환하도록 SiteMinder 구성

일부 NAS 장치에는 NAS가 인증만 지정하는 경우에도 Access-Accept에 포함된 RADIUS 응답이 필요합니다. NAS가 인증만 지정하는 경우에는 기본적으로 SiteMinder가 RADIUS 특성을 반환하지 않습니다.

NAS 장치에 항상 RADIUS 특성을 반환하려면 다음 매개 변수로 새 레지스트리 값을 생성하십시오.

- 값 종류 - DWORD
- 값 이름 - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Authentication\AlwaysReturnRadiusAttrs
- 값 데이터 - 0보다 큰 숫자 값

참고: 설치 프로그램은 AlwaysReturnRadiusAttrs에 대한 레지스트리 항목을 생성하지 않습니다. 사용자가 이 항목을 생성하고 설정할 때까지 SiteMinder는 기본값 0을 사용합니다.

AlwaysReturnRadiusAttrs를 0보다 큰 값으로 설정한 후에는 인증 서버의 디버그 로그에 다음 메시지가 표시됩니다.

```
Radius Attributes will be returned regardless of
RA_SERVICE_TYPE_AUTHENTICATE_ONLY(RA_SERVICE_TYPE_AUTHENTICAT
E_ONLY에 관계없이 항상 Radius 특성이 반환됨)
```

에이전트 유형에 대한 특성 만들기

응답에 특성을 사용하려면 응답을 반환하는 에이전트 유형이 해당 특성을 사용할 수 있어야 합니다. 에이전트 유형에 특성을 정의하면 에이전트 유형에서 특성을 사용할 수 있도록 합니다. 대부분의 에이전트 유형에는 공급업체 관련 특성과 RADIUS 확장 특성이 미리 구성되어 있지만 추가적인 확장 RADIUS 특성, 일반 RADIUS 특성 및 공급업체 관련 특성을 필요한 대로 에이전트 유형에 추가할 수 있습니다.

특성의 여러 인스턴스 정의

동일한 에이전트 유형에 대해 공급업체 관련 특성의 인스턴스를 여러 개 정의할 수 있습니다. 공급업체 관련 특성의 인스턴스를 여러 개 정의하는 경우 각 특성 인스턴스마다 서로 다른 값을 NAS 장치로 전송할 수 있습니다. 예를 들어 Cisco 에이전트의 경우 모두 동일한 식별자(26)를 사용하여 다음의 공급업체 관련 특성을 정의할 수 있습니다.

- Cisco-AVpair
- Account-Info
- Command-Code

응답 내에서 특성을 사용할 수 있는 횟수를 정의하는 설정은 관리 UI의 "에이전트 유형 특성 수정" 페이지에 있습니다.

여러 번 사용할 특성을 구성하려면 "액세스 수락" 값을 "0 또는 많음"으로 설정해야 합니다.

정의하는 특성의 유형은 응답을 반환하는 에이전트의 공급업체 유형과 일치해야 합니다. 예를 들어 공급업체 관련 Cisco 특성은 Cisco 에이전트에서만 반환할 수 있습니다.

에이전트가 응답을 반환할 경우 응답의 패킷 구조는 응답을 전송한 RADIUS 에이전트의 유형을 반영합니다. 예를 들어 Cisco 에이전트가 반환한 응답의 패킷 구조에는 공급업체 ID와 문자열 길이가 포함됩니다.

에이전트 유형에 대한 특성을 정의하려면

1. "인프라", "에이전트"를 차례로 클릭합니다.
2. "에이전트 유형"을 클릭합니다.
"에이전트 유형" 페이지가 표시됩니다.
3. 검색 조건을 지정하고 "검색"을 클릭합니다.
검색 조건과 일치하는 에이전트 유형의 목록이 표시됩니다.
4. 에이전트 유형의 이름을 클릭합니다.
"에이전트 유형 보기" 페이지가 표시됩니다.
5. "수정"을 클릭합니다.
설정과 컨트롤이 활성화됩니다.

6. "에이전트 유형 특성 만들기"를 클릭합니다.
"Create a new object of type Agent Type Attribute"(에이전트 유형 특성 유형의 새 개체 만들기) 옵션이 선택되어 있는지 확인합니다.
7. "확인"을 클릭합니다.
"에이전트 유형 특성 만들기" 페이지가 표시됩니다.
8. 에이전트 유형의 이름과 설명을 입력합니다.
9. "RADIUS 유형" 목록에서 "RADIUS", "RADIUS 확장" 또는 "공급업체 관련"을 선택합니다.
10. "데이터 형식" 목록에서 특성에 포함된 데이터 형식을 선택합니다.
11. "식별자" 필드에 다음 특성 식별자 중 하나를 입력합니다.

■ 일반 Radius

이 특성의 식별자는 RADIUS 프로토콜 사양에 정의되어 있습니다. 일반 RADIUS 특성의 식별자를 덮어쓸 수는 있지만 일반적으로 RADIUS 사양(RFC 2138)과 일치하는 미리 정의된 일반 RADIUS 특성 정의를 유지해야 합니다.

예: Callback-Id 변수의 특성을 생성하려면 "식별자" 필드에 20 을 입력합니다.

■ RADIUS 확장

이 특성의 식별자는 공급업체 설명서에 정의되어 있습니다.

예: Ascend-Callback 특성의 특성을 생성하려면 "식별자" 필드에 246 을 입력합니다.

■ 공급업체 관련

이 특성의 식별자는 26 입니다.

예: 에이전트가 TACACS+를 사용할 수 있도록 Cisco 에이전트용 특성을 생성하려면 "식별자" 필드에 26 을 입력합니다.

참고: 특성 식별자에 대한 자세한 내용은 RADIUS 공급업체 설명서를 참조하십시오.

12. "RADIUS 동작"에서 각 필드에 대한 RADIUS 코드를 선택합니다. RADIUS 코드는 다음과 같습니다.

허용되지 않음

응답에 특성을 사용할 수 없습니다.

0 또는 1

같은 응답에서 특성의 인스턴스 한 개 또는 0 개가 반환될 수 있습니다. 이 값을 선택하고 응답에 특성을 사용하는 경우 응답에 특성을 사용하고 나면 "특성" 목록에서 특성이 제거됩니다.

0 또는 많음

같은 응답에서 특성의 인스턴스 여러 개 또는 0 개가 반환될 수 있습니다.

1 개만

특성의 인스턴스 1 개가 응답에서 반환되어야 합니다. 이 값을 선택하고 응답에 특성을 사용하는 경우 응답에 특성을 사용하고 나면 "특성" 목록에서 특성이 제거됩니다.

RADIUS 특정 필드는 다음과 같습니다.

액세스 요청

특정 NAS 에 대한 사용자의 액세스가 허용되는지 여부를 확인하는데 사용되는 정보를 제공합니다. "액세스 요청" 패킷은 해당 사용자에게 요청된 모든 특별한 서비스에 대한 정보도 제공합니다.

액세스 수락

사용자에게 서비스 제공을 시작하는 데 필요한 특정 구성 정보를 제공합니다.

참고: 응답에 특성을 사용하려면 "액세스 수락" 값을 "0 또는 1", "0 또는 많음" 또는 "1 개만"으로 설정해야 합니다.

액세스 거부

수신된 특성의 값 중 허용되지 않는 값이 있는 경우에 정보를 보냅니다. 이 코드는 주로 회신 메시지에 사용됩니다.

액세스 챌린지

NAS 장치가 챌린지/응답을 사용하도록 구성된 경우에 정보를 보냅니다.

계정 설정 요청

전송되는 서비스의 유형과 이를 전송 중인 사용자를 설명합니다.

계정 응답

"계정 설정 요청"이 성공적으로 기록된 경우에 정보를 보냅니다.
RADIUS Accounting-Response 에는 특성이 없어도 됩니다.

13. 데이터 형식이 숫자인 경우 "만들기"를 클릭합니다.

14. 특성의 심볼 이름과 숫자 값을 해당 필드에 입력하고 "확인"을 클릭합니다.

"에이전트 유형 특성 수정" 페이지가 다시 나타나고 특성 이름-값 쌍이 추가됩니다.

참고: 여러 개의 특성 이름-값 쌍을 생성하려면 11 단계와 12 단계를 반복합니다. 심볼 이름을 값에 매핑하면 이름만 기억하면 됩니다.

15. "제출"을 클릭합니다.

"에이전트 유형 수정" 페이지가 다시 나타나고 에이전트 유형 특성이 추가됩니다.

16. "제출"을 클릭합니다.

선택된 에이전트 유형에 대해 특성이 정의됩니다.

참고: 태스크가 완료되면 이 에이전트 유형에 대한 응답을 생성할 때 방금 에이전트 유형에 추가한 에이전트 유형 특성을 특성 목록에서 선택할 수 있습니다.

기존 특성 수정

생성한 특성 및 RADIUS 에이전트에 대해 미리 정의된 특성을 수정할 수 있습니다. 예를 들어 Ascend 에이전트 유형의 미리 정의된 Ascend-PPP-Address 특성을 수정할 수 있습니다.

참고: 기존 특성을 수정할 경우 특성을 이미 사용하는 응답에서 해당 특성은 동적으로 업데이트되지 않습니다. 응답에 특성이 사용되는 경우 업데이트된 특성을 사용하여 응답을 다시 생성해야 합니다.

모든 RADIUS 에이전트 유형은 **RFC 2138**에 정의된 대로 일반 RADIUS 특성을 사용하도록 미리 구성되어 있습니다. 이러한 특성은 각 RADIUS 에이전트 유형에서 사용할 수 있습니다.

중요! 일반 RADIUS 에이전트에서 새 특성을 정의하거나 일반 특성을 덮어쓰면 변경 내용은 모든 RADIUS 에이전트에 적용됩니다. 예를 들어 일반 RADIUS 에이전트에서 필터 ID 특성을 수정하면 Cisco, Shiva, Livingston, Ascend 및 Checkpoint 와 같은 다른 모든 RADIUS 에이전트 유형에도 수정 사항이 적용됩니다.

에이전트 유형 특성을 수정하려면

1. 관리 UI 에 로그인합니다.
2. "인프라" 탭에서 "에이전트"를 선택합니다.
3. "에이전트 유형 수정"을 클릭합니다.
4. "검색"을 클릭합니다.
5. 에이전트 유형을 선택하고 "선택"을 클릭합니다.
"에이전트 유형 수정" 창이 열립니다.
6. 특성 왼쪽의 "편집" 단추를 클릭하여 에이전트 유형 값을 수정합니다.
7. "제출"을 클릭하여 변경 내용을 저장합니다.

RADIUS 환경에서 SiteMinder 배포

SiteMinder 가 다음과 같은 다양한 RADIUS 환경에서 인증 서비스를 제공하도록 설정할 수 있습니다.

- Cisco RAS 같은 NAS 장치 하나와 사용자 디렉터리 하나만으로 구성된 동종 환경. 이 환경에 대한 자세한 내용은 동종 RADIUS 환경에서 사용자를 인증하는 방법에서 설명합니다.
- Checkpoint 방화벽 및 Cisco RAS 같은 여러 NAS 장치와 사용자 디렉터리 하나로 구성된 이종 환경. 이 환경에 대한 자세한 내용은 [사용자 디렉터리가 한 개인 이종 RADIUS 환경에서 사용자 인증](#) (페이지 848)에서 설명합니다.
- Checkpoint 방화벽 및 Cisco RAS 같은 여러 NAS 장치와 여러 사용자 디렉터리로 구성된 이종 환경. 이 환경에 대한 자세한 내용은 [사용자 디렉터리가 두 개인 이종 RADIUS 환경에서 사용자 인증](#) (페이지 852)에서 설명합니다.

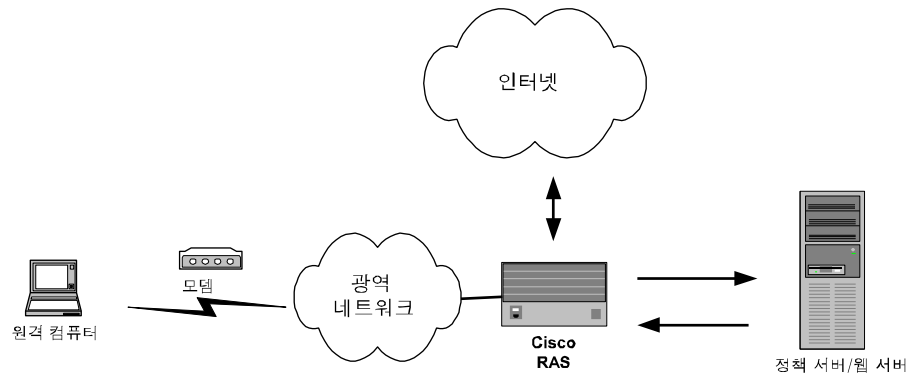
RADIUS 장치를 보호하기 위한 지침

RADIUS 환경에서 SiteMinder 를 배포하기 전에 다음 지침에 주의하십시오.

- 동일한 정책 도메인의 영역 이름은 고유해야 합니다.
- 한 정책 내에서 한 가지 유형의 **RAS** 장치만 보호할 수 있습니다.
공급업체마다 사용하는 사전 파일이 다르므로 단일 정책으로 여러 RADIUS 장치를 보호할 수는 없습니다. 단일 정책의 응답은 반환 특성을 동일하게 해석해야 합니다. 환경이 이중 환경이고 다양한 RAS 장치가 포함되어 있는 경우 RADIUS 장치의 각 유형에 대해 개별 정책을 정의하십시오.
- 한 정책 도메인 내에 여러 사용자 디렉토리를 정의할 수 없습니다. 여러 사용자 디렉토리를 정의할 경우에는 검색 순서를 지정하십시오.
- 서로 다른 NAS 공급업체의 RADIUS 에이전트를 단일 일반 RADIUS 에이전트 그룹으로 결합한 다음 각 RADIUS 에이전트 유형에 대한 개별 정책에서 동일한 에이전트 그룹을 사용할 수 있습니다. 예를 들어 에이전트 그룹에 Shiva 에이전트와 Cisco 에이전트가 포함되었으면 Shiva 정책과 Cisco 정책을 생성합니다. 그러면 각 정책에 동일한 규칙 및 영역이 추가되므로 시간이 절약됩니다. 그러나 동일한 규칙의 각 인스턴스에 연결된 응답은 서로 다릅니다. 즉, Cisco 정책은 일반 규칙에 Cisco 응답을 연결하고 Shiva 정책은 일반 규칙에 Shiva 응답을 연결합니다.

동종 RADIUS 환경에서 사용자를 인증하는 방법

동종 RADIUS 환경은 보호하기가 가장 간단합니다. 즉, 정책 하나만으로 RADIUS 장치를 보호할 수 있습니다. 이 유형의 환경에는 다음 그림과 같이 Cisco RAS 같은 RADIUS 장치 하나와 사용자 디렉토리 하나만 포함됩니다.



다음 단계를 수행하십시오.

1. 시스템을 구성합니다.
 - a. RADIUS 에이전트 구성에 설명된 대로 RADIUS 에이전트를 정의합니다.
 - b. 사용자 디렉터리 설정에 설명된 대로 RADIUS 사용자를 인증할 사용자 디렉터리를 설정합니다.
 - c. 필요한 경우 관리 사용자를 정의하고 인증 체계를 수정할 수도 있습니다.
2. 정책 도메인을 구성합니다.
 - a. 인증 체계 만들기에 설명된 대로 RADIUS 인증 체계(CHAP 또는 PAP)를 생성합니다.
 - b. RADIUS 에이전트로 보호되는 영역 구성에 설명된 대로 RADIUS 에이전트와 RADIUS 인증 체계를 식별하는 영역을 정의합니다.
 - c. 인증 이벤트 작업을 위한 규칙 구성에 설명된 대로 인증된 사용자가 RADIUS 에이전트로 보호되는 영역에 액세스할 수 있도록 하는 규칙을 정의합니다.
 - d. 응답 구성 및 [RADIUS 에이전트 응답 특성](#) (페이지 591)에 설명된 대로 NAS 장치에 사용자 프로필을 제공하고, 응답 특성을 사용하여 세션의 특성을 구성하는 응답을 정의합니다.
 - e. 정책을 구성하는 방법에 설명된 대로 규칙 및 응답을 사용자 디렉터리와 바인딩하는 정책을 생성합니다.

추가 정보:

[정책 서버에서 RADIUS 인증이 작동하는 방식](#) (페이지 828)

사용자 디렉터리 설정

사용 중인 NT 또는 UNIX 플랫폼에 대해 지원되는 사용자 디렉터리를 사용하여 RADIUS 사용자를 인증할 수 있습니다.

사용자 디렉터리에 사용자 권한에 대한 정보가 포함된 경우 사용자 특성을 사용하여 응답을 생성할 수 있습니다. 사용자 특성이 다시 RADIUS 장치로 보내지면 사용자 세션을 구성하는 데 해당 특성이 사용됩니다.

다음 디렉토리를 사용할 수 있습니다.

- ODBC-enabled 데이터베이스
- NT 도메인
- Netscape 또는 NDS LDAP

정책 도메인 설정

정책 도메인은 RADIUS 사용자의 이름, 도메인을 수정할 수 있는 관리자의 이름, 그리고 RADIUS 에이전트가 보호 중인 영역이 포함된 하나 이상의 사용자 디렉토리를 식별해야 합니다.

인증 체계 만들기

다음 인증 체계를 사용할 수 있습니다.

- PAP(암호 인증 프로토콜)

PAP 는 호스트가 양방향 핸드셰이크에서 아이덴티티를 설정하기 위한 간단한 방법을 제공하는 PPP 인증 프로토콜입니다. 인증은 초기 연결 설정 시에만 발생하며 이때 암호화는 사용되지 않습니다.

- CHAP(Challenge-Handshake 인증 프로토콜)

CHAP 는 보안 PPP 인증 프로토콜이기도 합니다. CHAP 를 사용하면 3 방향 핸드셰이크 및 암호화를 사용하여 호스트의 아이덴티티를 정기적으로 확인할 수 있습니다. 인증은 초기 연결 설정 시에만 발생합니다. RAS 는 연결이 이루어진 후 언제든지 인증 프로세스를 반복할 수 있습니다.

- Security Dynamics ACE/서버 또는 Secure Computing SafeWord 서버

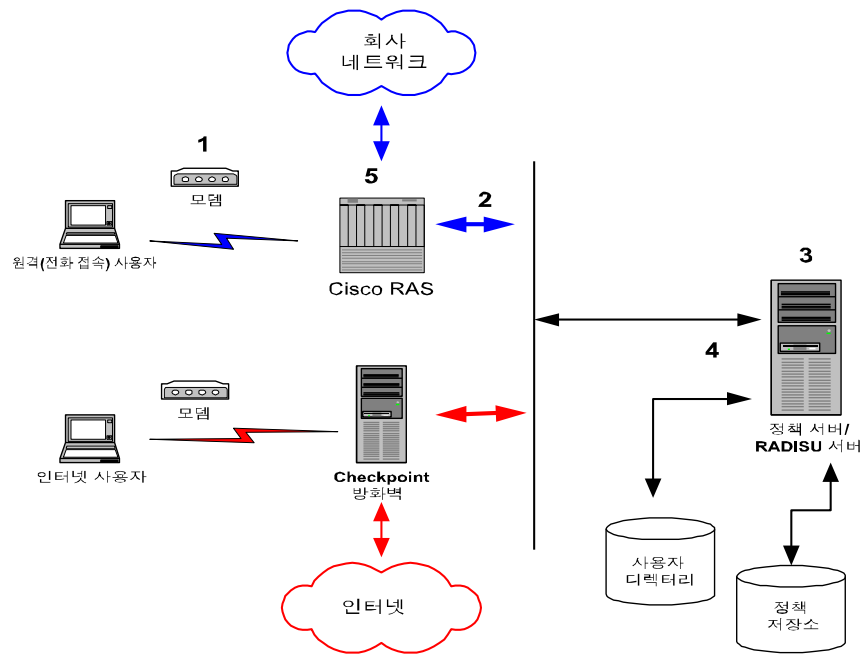
사용자 디렉터리가 한 개인 이중 RADIUS 환경에서 사용자 인증

RADIUS 환경에서 보다 강력하고 복잡한 정책 서버 배포는 여러 NAS 장치에서 관리되는 여러 영역을 포함하는 배포입니다. 이 시나리오에서는 정책 서버가 동시에 여러 RADIUS 클라이언트에 대해 RADIUS 인증 서버의 역할을 할 수 있습니다.

이중 구성을 사용하면 각 RADIUS 클라이언트에 대해 동일한 RADIUS 인증 서버(즉, 정책 서버)를 사용하여 시간을 절약할 수 있다는 장점이 있습니다.

단일 디렉터리를 사용하는 이중 환경에서 사용자가 인증되는 방식

다음 그림에서는 이중 구성의 예를 보여 줍니다.



위 다이어그램에 표시된 네트워크 토폴로지에서는 정책 서버가 두 NAS 장치(Cisco RAS 및 Checkpoint 방화벽)의 사용자를 인증합니다. 정책 서버는 사용자 디렉터리 하나를 사용하여 사용자를 인증합니다.

각 NAS 장치에는 영역 힌트로 구성된 고유한 RADIUS 에이전트가 있습니다. 정책 서버는 사용자 인증 요청을 받으면 RADIUS 에이전트의 영역 힌트를 사용하여 인증된 사용자가 액세스할 수 있는 리소스(도메인)를 확인합니다.

사용자 디렉터리가 한 개 사용될 때의 인증 프로세스는 다음과 같습니다.

1. 원격 사용자가 전화 접속 모뎀을 사용하여 연결하면 Cisco RAS 는 RADIUS 사용자 프로필을 사용하여 사용자를 인증해야 하는지 확인합니다.
2. RAS 가 정책 서버에 사용자 연결 요청을 보냅니다.
3. 정책 서버가 RAS 에 대해 정의된 정책을 규정하고 Cisco RAS 와 연결된 RADIUS 에이전트가 다음을 수행합니다.
 - a. 영역 힌트를 사용하여 사용자의 도메인을 확인합니다.
 - b. 에이전트에 대해 구성된 인증 체계를 사용하여 사용자의 이름과 암호를 가져옵니다.
4. 정책 서버가 사용자 디렉터리 및 정책 저장소를 기준으로 사용자 정보를 평가합니다.
5. 정책 서버가 Cisco RAS 에 인증 응답을 보내고 다음 중 하나가 발생합니다.
 - 인증에 실패한 경우 RAS 가 연결을 거부합니다.
 - 인증에 성공한 경우 RAS 가 RADIUS 서버의 데이터베이스에 있는 사용자 프로필에서 특성 목록을 받고 호출자에 대한 네트워크 액세스를 설정합니다.

RAS 가 정책 서버에 세션이 시작되었다는 사실과 세션이 종료되는 시기를 알립니다.

인터넷 사용자가 Checkpoint 방화벽을 통해 인터넷 서비스 공급자에 전화 접속을 시도할 경우에도 유사한 인증 프로세스가 발생합니다. Checkpoint 방화벽에 대해 정의된 RADIUS 에이전트는 영역 힌트를 사용하여 인터넷 사용자가 액세스할 수 있는 도메인을 확인합니다. 사용자가 인증된 경우 정책 서버는 방화벽에 올바른 특성을 전달하여 세션을 설정합니다.

두 NAS 장치에 대한 사용자 정보는 모두 동일한 사용자 디렉터리에 저장됩니다. 정책 서버는 인증 요청을 받을 때마다 동일한 데이터 디렉터리를 사용하여 사용자를 인증합니다.

시스템 및 정책 도메인 구성

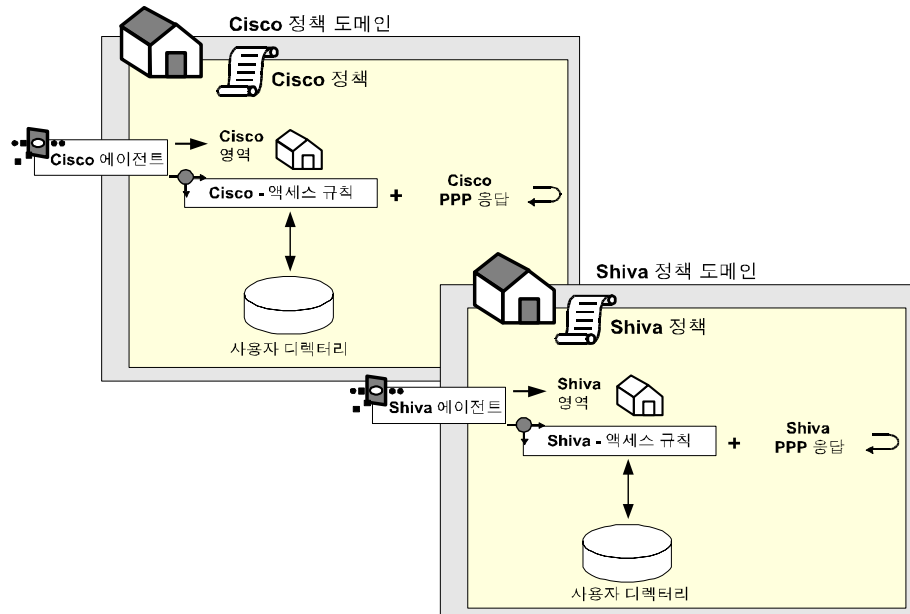
이 시스템 구성은 동종 환경과 다릅니다. 즉, 이제는 에이전트를 두 개 생성해야 합니다.

정책 도메인 내에는 Cisco 에이전트 및 Checkpoint 에이전트에 대한 규칙과 응답이 포함된 정책 하나가 있습니다.

위에서 설명한 단일 디렉터리를 사용하는 이중 환경에서 SiteMinder 를 설정하려면 다음을 수행해야 합니다.

1. 시스템을 구성합니다.
 - a. [단일 디렉터리를 사용하는 이중 환경에 대한 에이전트 정의](#) (페이지 851)에 설명된 대로 두 개의 RADIUS 에이전트를 정의합니다.
 - b. [사용자 디렉터리 구성](#) (페이지 851)에 설명된 대로 RADIUS 사용자를 인증할 사용자 디렉터리를 설정합니다.
 - c. 정책 도메인 만들기에 설명된 대로 정책 도메인을 하나 생성합니다.
 - d. 인증 체계 만들기에 설명된 대로 인증 체계를 생성합니다.
2. 정책 도메인을 구성합니다.
 - a. 영역을 두 개 정의합니다. 영역 하나는 Cisco RAS 용이고 다른 하나는 Checkpoint 방화벽용입니다. 각 영역은 RADIUS 에이전트를 RADIUS 인증 체계와 바인딩합니다.
 - b. 인증된 사용자가 적절한 영역에 액세스할 수 있도록 하는 규칙을 두 개 정의합니다. 각 규칙은 영역을 액세스 허용 또는 거부 이벤트와 바인딩합니다.
 - c. NAS 장치에 사용자 프로필을 제공하는 응답을 두 개 정의하고 응답 특성을 사용하여 세션의 특성을 구성합니다. 각 장치는 서로 다른 사전 파일을 사용하므로 각 NAS 장치에 대해 개별 응답을 정의해야 합니다.
 - d. Cisco 규칙을 Cisco 응답과 바인딩하고 Checkpoint 규칙을 Checkpoint 응답과 바인딩하는 정책을 하나 생성합니다. 또한 이 정책은 정책 도메인의 구성 요소(규칙 및 응답 그룹)를 RADIUS 사용자 디렉터리와 바인딩합니다.

다음 그림에서는 이 정책 도메인의 다이어그램을 보여 줍니다.



단일 디렉터를 사용하는 이중 환경에 대한 에이전트 정의

이 환경의 경우 RADIUS 에이전트를 두 개 구성해야 합니다.

- 에이전트 하나는 Cisco RAS 와 연결해야 합니다.
- 다른 하나는 Checkpoint 방화벽과 연결해야 합니다.
- 두 RADIUS 에이전트 모두 영역 힌트로 1 을 사용하여 각 에이전트가 보호할 올바른 도메인을 식별할 수 있도록 해야 합니다.

사용자 디렉터리 구성

정책 서버는 두 NAS 장치 모두에 대해 동일한 사용자 디렉터를 사용하여 사용자를 인증할 수 있습니다.

정책 도메인 만들기

정책 도메인은 RADIUS 사용자의 이름, 도메인을 수정할 수 있는 관리자의 이름, 그리고 RADIUS 에이전트가 보호 중인 영역이 포함된 사용자 디렉터를 식별해야 합니다. 사용자 디렉터를 하나만 사용하는 RADIUS 환경에는 정책 도메인도 하나만 필요합니다.

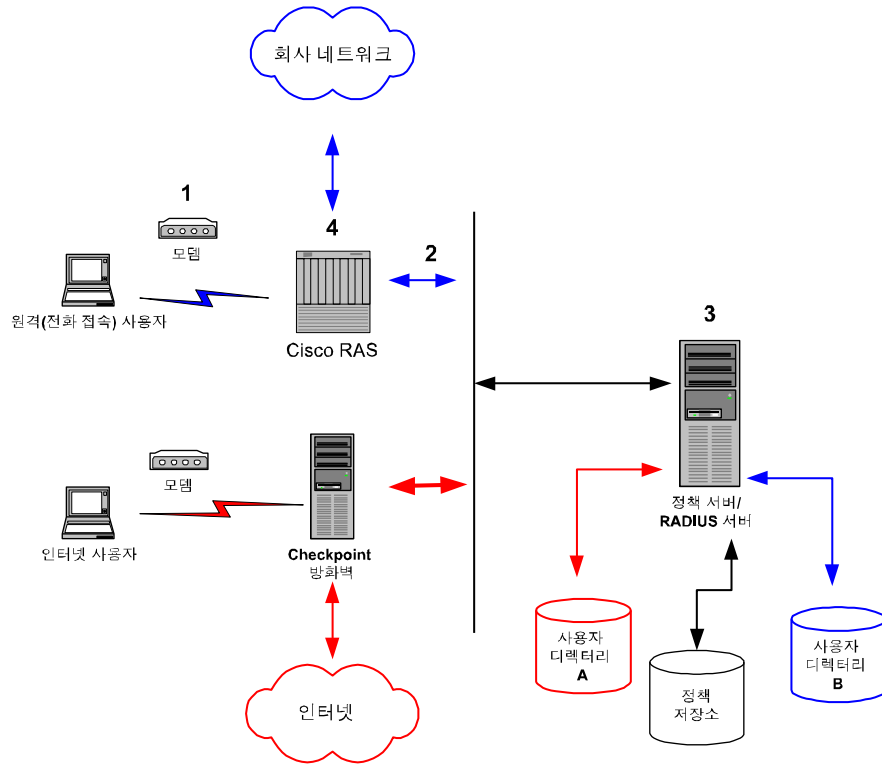
사용자 디렉터리가 두 개인 이중 RADIUS 환경에서 사용자를 인증하는 방법

각 NAS 장치의 사용자 정보가 개별 사용자 디렉터리에 있는 경우 여러 NAS 장치의 사용자를 인증하도록 정책 서버를 구성할 수도 있습니다. NAS 장치의 공급업체 유형은 서로 다를 수 있습니다.

이 구성을 사용하면 다음과 같은 몇 가지 장점이 있습니다.

- 단일 정책 도메인에 사용자 디렉터리를 두 개 사용하면 서로 다른 사용자에게 각 디렉터리의 관리를 위임할 수 있습니다.
- 여러 RADIUS 클라이언트의 사용자를 인증하도록 정책 서버를 구성하여 시간을 절약할 수 있습니다. RADIUS 클라이언트마다 개별 인증 서버를 설치하고 구성할 필요가 없습니다.
- 기존 사용자 디렉터리를 보다 효율적으로 사용할 수 있습니다. 사용자 정보를 단일 디렉터리에 병합할 필요가 없습니다.

다음 그림에서는 사용자 디렉터리를 두 개 사용하는 이중 구성의 예를 보여 줍니다.



이전 단원에서 설명한 토폴로지와 달리 이 정책 서버는 두 개의 사용자 디렉터리를 사용하여 사용자를 인증합니다. Cisco RAS 사용자에 대한 사용자 정보는 사용자 디렉터리 A에 저장됩니다. Checkpoint 방화벽의 사용자 정보는 사용자 디렉터리 B에 저장됩니다. 정책 서버는 이러한 두 디렉터리를 모두 사용하여 사용자를 인증할 수 있습니다.

구성을 두 개의 정책 도메인으로 나누면 영역 힌트가 필요하지 않게 됩니다. 각 RADIUS 에이전트는 개별 정책 도메인에 있으며 한 영역에만 바인딩됩니다.

사용자 디렉터리가 두 개 사용될 때의 인증 프로세스는 다음과 같습니다.

1. 원격 사용자가 전화 접속 모뎀을 사용하여 연결하면 Cisco RAS는 RADIUS 사용자 프로ファイルを 사용하여 사용자를 인증해야 하는지 확인합니다.
2. RAS가 정책 서버에 사용자 연결 요청을 보냅니다.
3. 정책 서버가 RAS에 대해 정의된 정책을 규정하고 RADIUS 에이전트가 에이전트에 대해 구성된 인증 체계를 사용하여 사용자의 이름과 암호를 가져옵니다.
4. 정책 서버가 정책의 도메인과 연결된 사용자 디렉터리 및 정책 저장소를 기준으로 사용자 정보를 평가합니다.
5. 정책 서버가 Cisco RAS에 인증 응답을 보내고 다음 중 하나가 발생합니다.
 - 인증에 실패한 경우 RAS가 연결을 거부합니다.
 - 인증에 성공한 경우 RAS가 RADIUS 서버의 데이터베이스에 있는 사용자 프로파일에서 특성 목록을 받고 호출자에 대한 네트워크 액세스를 설정합니다.

RAS가 정책 서버에 세션이 시작되었다는 사실과 세션이 종료되는 시기를 알립니다.

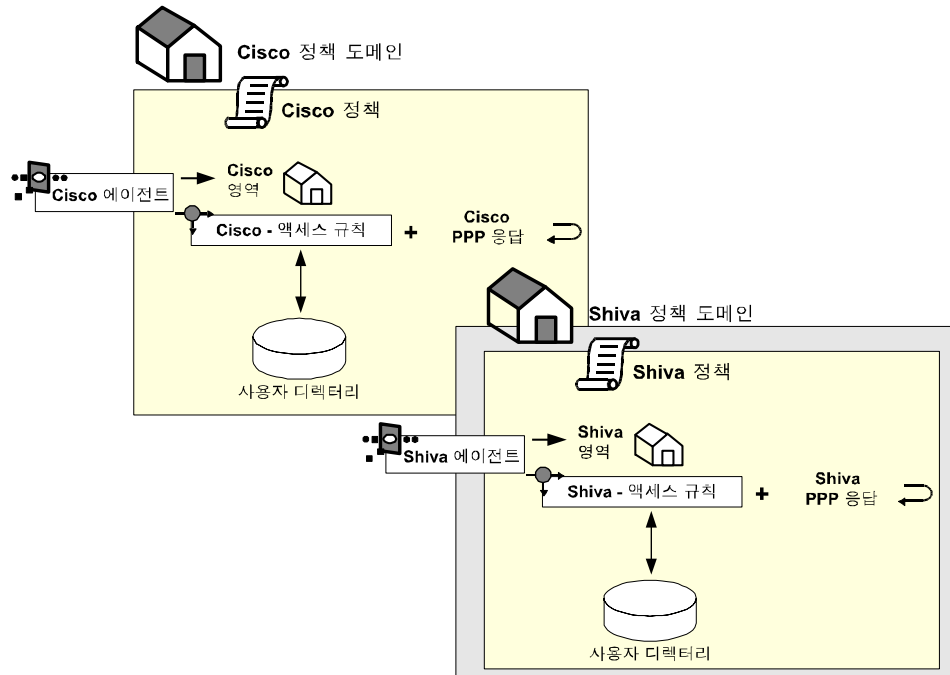
인터넷 사용자가 Checkpoint 방화벽을 사용하여 인터넷 서비스 공급자에 전화 접속을 시도할 경우에도 이와 동일한 인증 프로세스가 발생합니다. 그러나 정책 서버는 다른 사용자 디렉터리를 기준으로 인터넷 사용자의 인증 정보를 평가합니다.

시스템 및 정책 도메인을 구성하는 방법

위에서 설명한 사용자 디렉터리가 두 개 포함된 이중 환경을 구성하려면 다음을 수행해야 합니다.

1. 시스템을 구성합니다.
 - a. [두 개의 디렉터를 사용하는 이중 환경에 대한 에이전트 정의](#) (페이지 855)에 설명된 대로 두 개의 RADIUS 에이전트를 정의합니다.
 - b. [사용자 디렉터리 설정](#) (페이지 855)에 설명된 대로 사용자 디렉터를 설정합니다.
 - c. [두 개의 정책 도메인 만들기](#) (페이지 856)에 설명된 대로 정책 도메인을 두 개 생성합니다.
2. 정책 도메인을 구성합니다.
 - a. 영역 하나를 정의합니다. 이 영역은 RADIUS 에이전트를 RADIUS 인증 체계와 바인딩합니다.
 - b. 인증된 사용자가 영역에 액세스할 수 있도록 하는 규칙을 정의합니다. 각 규칙은 영역을 액세스 허용 또는 거부 이벤트와 바인딩합니다.
 - c. NAS 장치에 사용자 프로필을 제공하는 응답을 정의하고, 필요한 경우 응답 특성을 사용하여 세션의 특성을 구성합니다.
 - d. 규칙을 응답과 바인딩하는 정책을 생성합니다. 또한 이 정책은 규칙 및 응답을 RADIUS 사용자 디렉터리와 바인딩합니다.

다음 그림에서는 이 두 정책 도메인의 다이어그램을 보여 줍니다.



두 개의 디렉터리를 사용하는 이중 환경에 대한 에이전트 정의

이 환경의 경우 RADIUS 에이전트를 두 개 구성해야 합니다.

- 에이전트 하나는 Cisco RAS 와 연결해야 합니다.
- 다른 에이전트는 Checkpoint 방화벽과 연결해야 합니다.
- 두 RADIUS 에이전트 모두 영역 힌트가 필요하지 않습니다.

추가 정보:

[단일 디렉터리를 사용하는 이중 환경에 대한 에이전트 정의](#) (페이지 851)

사용자 디렉터리 설정

정책 서버에 RADIUS 사용자 정보를 포함하는 각 사용자 디렉터리를 구성해야 합니다. 각 정책 도메인에 대해 개별 관리자가 정의될 수 있도록 각 디렉터리는 개별 정책 도메인과 연결됩니다.

두 개의 정책 도메인 만들기

Cisco RAS 에 대한 정책 도메인 하나와 Checkpoint 방화벽에 대한 정책 도메인 하나를 생성해야 합니다. 정책 도메인을 정의할 때 각 도메인을 적절한 사용자 디렉터리와 연결하십시오.

RADIUS 에이전트 그룹 개요

RADIUS 에이전트 그룹을 생성하면 여러 RADIUS 에이전트를 동시에 관리할 수 있으며 각 RADIUS 에이전트에 대한 개별 영역을 생성하고 구성할 필요가 없게 됩니다. 단일 영역을 사용하면 모든 RADIUS 에이전트에 대해 동일한 세션 만료 시간과 동일한 인증 체계를 동시에 정의할 수 있으므로 시간이 절약됩니다.

RADIUS 에이전트 그룹에는 서로 다른 유형의 NAS 장치에 대한 에이전트가 포함될 수 있습니다. 예를 들어 Shiva LAN Rover RAS, Checkpoint 방화벽 및 Cisco RAS 를 에이전트 그룹에 포함할 수 있습니다. 이러한 모든 RADIUS 에이전트가 포함된 에이전트 그룹은 인증 체계 및 세션 시간 만료 요구 사항을 정의하는 단일 영역과 연결됩니다.

에이전트 그룹은 자주 변경되지 않는 정적 환경에 가장 적합합니다. 에이전트 그룹을 사용하여 여러 NAS 장치의 사용자를 인증하도록 SiteMinder 를 빠르게 구성할 수 있습니다. 새 NAS 장치가 추가되거나 제거됨에 따라 자주 변경되는 비정적 환경의 경우에는 에이전트 그룹을 사용하지 않는 것이 좋습니다. 일반적으로 RADIUS 에이전트가 그룹에 속하지 않는 편이 RADIUS 에이전트를 추가하고 제거하는 데는 더 편리합니다. 에이전트가 구분되고 그룹화되어 있지 않으면 일반적으로 특정 에이전트를 보다 빠르게 찾을 수 있으며 정책 수정 또는 제거도 보다 빠르게 수행할 수 있습니다.

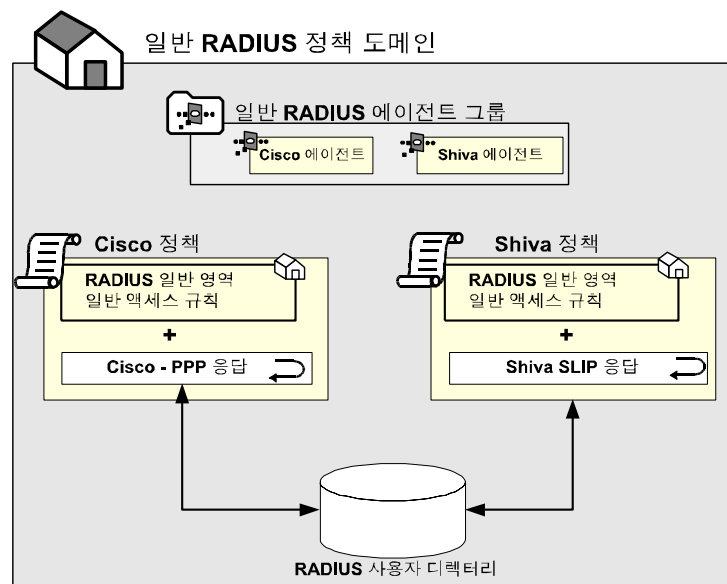
RADIUS 에이전트 그룹 설정

RADIUS 에이전트 그룹을 사용하는 경우에는 일반적으로 각 RADIUS 에이전트 유형에 대해 개별 정책을 설정합니다. 각 RADIUS 에이전트 유형마다 개별 정책을 사용하면 각 정책에서 영역 및 규칙과 같은 정책 도메인의 공통 요소를 공유할 수 있습니다. 이러한 공통 요소를 공유하면 시간이 절약됩니다.

규칙 및 영역과 달리 각 정책의 응답은 공유되지 않습니다. 각 정책에는 정책의 RADIUS 에이전트 장치 유형에 해당하는 고유한 응답이 있습니다. 응답의 특성은 NAS 장치의 사전 파일에서 제공되는 특성과 일치합니다. 예를 들어 Cisco RAS에 대한 응답은 Cisco RAS가 Cisco 사전 파일을 사용하여 해석할 수 있는 특성을 제공해야 합니다.

참고: RADIUS 에이전트 그룹에 표시되는 모든 NAS 장치는 동일한 사용자 디렉터리를 공유해야 합니다. 동일한 사용자 디렉터리를 공유하지 않을 경우에는 장치가 동일한 정책 도메인에 있을 수 없으므로 동일한 일반 영역이나 일반 규칙을 공유할 수 없습니다.

다음 예에서는 Cisco RAS용 에이전트와 Shiva RAS용 에이전트가 모두 포함된 RADIUS 에이전트 그룹 하나를 보여 줍니다. 이 에이전트 그룹은 Cisco 정책과 Shiva 정책 모두에서 공유됩니다. 이러한 두 정책은 모두 액세스를 허용하기 위한 동일한 일반 규칙과, 에이전트 그룹을 동일한 인증 체계에 바인딩하는 동일한 일반 영역을 공유합니다. 그러나 각 정책의 응답은 고유합니다.



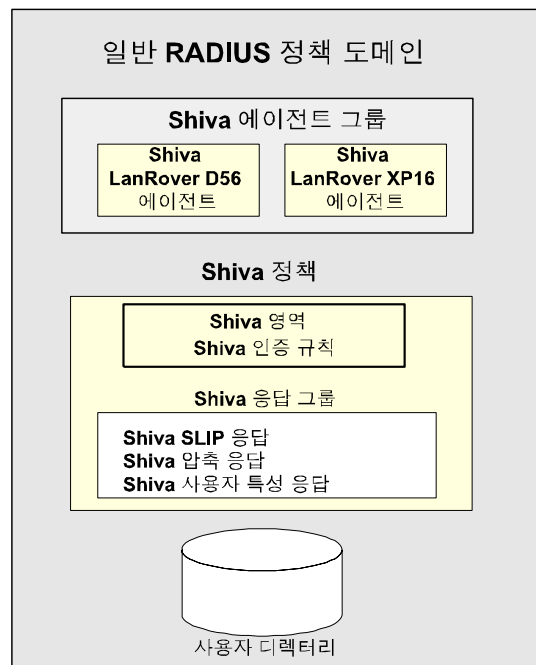
RADIUS 에이전트 그룹을 설정하는 절차는 에이전트 그룹 구성을 참조하십시오.

RADIUS 응답 그룹화

RADIUS 응답 그룹은 일반 Radius 와 같이 동일한 에이전트 유형에 대해 정의된 응답의 모음입니다. 규칙이 실행되면 응답 그룹에서 해당 규칙과 쌍으로 연결된 모든 RADIUS 응답이 트리거됩니다.

응답은 에이전트 유형이 동일해야 동일한 사전 파일을 사용할 수 있습니다. 예를 들어 두 개의 Cisco 응답을 동일한 그룹으로 묶거나 두 개의 일반 Radius 응답을 동일한 그룹으로 묶을 수 있습니다. 그러나 일반 Radius 응답과 Cisco 응답을 동일한 그룹으로 그룹화할 수는 없습니다.

RADIUS 응답 그룹을 사용하면 적은 수의 정책을 사용하여 정책 도메인을 구성할 수 있다는 장점이 있습니다. 각 RADIUS 에이전트에 대해 개별 영역과 개별 정책을 생성하는 대신 동일한 유형의 RADIUS 에이전트를 그룹화하고 인증을 위한 일반 규칙을 하나 생성한 다음 이 규칙에 대한 응답을 그룹화할 수 있습니다. 다음 다이어그램에서는 이러한 유형의 구성을 보여 줍니다.



또한 응답 그룹을 사용하면 환경에 RADIUS 장치를 보다 쉽게 추가할 수 있습니다. 예를 들어 위 그림에 표시된 것과 같은 환경에서는 RADIUS 에이전트 그룹에 또 다른 Shiva RAS 를 빠르게 추가할 수 있으며 이 새 RAS 에는 적절한 규칙과 응답이 자동으로 구성됩니다.

RADIUS 문제 해결 및 테스트

정책 서버가 RADIUS 인증 서버의 역할을 하도록 구성한 다음에는 이후 항목에서 설명하는 도구를 사용하여 정책을 테스트하고 문제를 해결할 수 있습니다.

계정 설정 및 디버깅을 위한 RADIUS 로그 생성

RADIUS 로그는 정책 서버가 생성한 디버깅 및 계정 정보를 추적합니다. 다음을 추적하려면 RADIUS 로그 파일을 사용하십시오.

- 정책 서버의 상태
- 연결 시도 및 세션 생성
- 각 정책 서버 작업에 대한 정보

정책 서버 관리 콘솔의 "디버그" 탭에서 로그 기능을 설정하거나 해제할 수 있습니다.

정책 서버는 로그 파일이 생성된 날짜 및 시간으로 로그 파일에 타임스탬프를 지정합니다. 예를 들어 파일 이름으로 "log.txt"를 지정할 경우, 정책 서버가 다시 시작되어 로그 파일을 생성할 때는 이름에 날짜 및 시간이 추가됩니다.

로깅 정보를 동일한 파일에 추가할 경우 파일의 날짜는 해당 정보가 생성된 날짜를 반영합니다. 타임스탬프는 정책 서버가 다시 시작되는 경우에만 업데이트됩니다.

Smreadclog 를 사용하여 RADIUS 로그 파일 읽기

이 도구는 정책 서버가 생성한 RADIUS 로그 파일을 읽는 데 사용됩니다. 이 도구는 정책 서버가 RADIUS 인증 서버로 사용될 때의 문제를 해결하는 데 유용합니다. NAS와 SiteMinder 간에 교환되는 개별 RADIUS 특성을 표시할 수 있는 옵션이 제공됩니다.

Smreadclog 는 다음 인수를 사용하여 RADIUS 로그 파일을 읽는 데 필요한 정보를 제공합니다.

-i<input-file>

로그 파일의 파일 이름을 지정합니다.

-o<output-file>

출력 파일의 파일 이름을 지정합니다.

-s<secret>

RADIUS 암호를 디코딩하는 데 사용할 수 있는 공유 암호를 지정합니다.

-r

전체 RADIUS 패킷의 16 진수 덤프를 표시하도록 지정합니다.

-a

RADIUS 특성을 개별적으로 표시하도록 지정합니다.

-d

RADIUS 특성을 정책 저장소에서의 정의에 따라 표시하도록 지정합니다. 이 옵션은 실제 특성 이름뿐 아니라 해당 특성 유형을 기반으로 형식이 지정된 특성 값도 표시합니다. 이 옵션을 사용하지 않으면 특성 이름과 값만 16 진수 문자열로 표시됩니다.

-p<radius-server>

RADIUS 서버에 대한 정책 서버 서비스의 RADIUS 작업을 기록하고 재생할 수 있도록 합니다.

-m<authentication port>

RADIUS 인증에 기본 포트 1645 가 아닌 다른 포트를 사용할 경우 해당 포트를 지정합니다.

-n<accounting port>

RADIUS 계정 설정에 기본 포트 1646 이 아닌 다른 포트를 사용할 경우 해당 포트를 지정합니다.

smreadclog 를 사용하려면

1. 다음 위치 중 하나로 이동합니다.

- NT: <sitefinder_installation>\Bin

여기서 <sitefinder_installation>은 SiteMinder 가 설치된 위치입니다.

- UNIX: <sitefinder_installation>/bin

여기서 <sitefinder_installation>은 SiteMinder 가 설치된 위치입니다.

2. 다음 명령을 입력합니다.

```
smreadclog -i<input-file> -o<output-file>
-s<secret> -r -a -d -p<radius-server> -m<portnumber>
-n<portnumber>
```

예를 들면 다음과 같습니다.

```
smreadclog -iradiuslog.txt -oradiuslog2.txt
-ssecret -r -a -d -p123.123.12.12
```

SiteMinder 테스트 도구를 사용하여 테스트하는 방법

SiteMinder 테스트 도구는 RADIUS 인증 서버의 동작을 시뮬레이트합니다. 테스트 도구를 사용하여 RADIUS 사용자를 인증하는 정책을 테스트하고 구성된 응답 특성이 적절한 데이터를 반환하는지 확인할 수 있습니다.

RADIUS 정책을 테스트하는 과정에는 다음 단계가 포함됩니다.

1. RADIUS 정책을 생성합니다.
2. [정책 서버 관리 콘솔 구성](#) (페이지 861)에 설명된 대로 정책 서버 관리 콘솔이 RADIUS 를 사용하도록 구성합니다.
3. [RADIUS 정책 테스트](#) (페이지 862)에 설명된 대로 SiteMinder 테스트 도구가 RADIUS 정책을 테스트하도록 구성합니다.

정책 서버 관리 콘솔 구성**정책 서버 관리 콘솔을 구성하려면**

1. 정책 서버 관리 콘솔을 시작합니다.

중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "설정" 탭을 선택합니다.
 3. "설정"에서 다음을 수행합니다.
 - a. "RADIUS UDP 포트" 그룹 상자에서 "사용" 확인란을 선택합니다.
 - b. "인증" 필드에 1645 를 입력합니다.
 - c. "계정" 필드에 1646 을 입력합니다.
 4. "상태" 탭에서 정책 서버를 다시 시작하여 정책 서버 구성 변경 내용을 적용합니다.
- 이제 테스트 도구를 사용하여 RADIUS 정책을 테스트할 수 있습니다.

RADIUS 정책 테스트

RADIUS 정책을 테스트하려면

1. 테스트 도구를 시작합니다.

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.
 2. "SiteMinder 에이전트" 그룹 상자에서 다음을 수행합니다.
 - a. "RADIUS" 라디오 단추를 선택합니다.
 - b. "암호" 필드에 SiteMinder 관리 사용자 인터페이스에서 RADIUS 에이전트에 대해 정의된 공유 암호를 입력합니다.
 3. "사용자 정보" 그룹 상자에서 다음을 수행합니다.
 - a. "사용자" 필드에 인증을 테스트할 RADIUS 사용자 디렉터리의 사용자 이름을 입력합니다.
 - b. "암호" 필드에 사용자의 암호를 입력합니다.
 - c. RADIUS CHAP 인증 체계를 사용하는 경우 "CHAP Password"(CHAP 암호) 확인란을 선택합니다.
 4. "명령" 그룹 상자에서 "IsAuthenticated"를 클릭합니다.
- 정책이 테스트되고 "특성" 그룹 상자에 응답 특성이 표시됩니다.

부록 E: 특성 및 식 참조

이 섹션은 다음 항목을 포함하고 있습니다.

[데이터 형식](#) (페이지 863)

[식 구문 개요](#) (페이지 866)

[붙여넣기](#) (페이지 868)

[연산자](#) (페이지 870)

[식에서 사용할 수 있는 함수](#) (페이지 887)

데이터 형식

모든 상수 데이터는 문자열, 숫자 또는 부울이라는 세 가지 기본 리터럴 데이터 형식 중 하나입니다. 문자열 데이터 형식에는 두 개의 하위 형식으로 집합과 LDAP 고유 이름이 포함됩니다. 숫자 데이터 형식에는 한 개의 하위 형식으로 날짜가 포함됩니다. 모든 함수 및 연산은 이러한 형식 또는 하위 형식 중 하나를 반환합니다.

- 문자열
 - 집합
 - LDAP 고유 이름
- 숫자
 - 날짜
- 부울

리터럴 데이터 형식 외에 다음과 같이 변수로 작동하는 데이터 형식도 있습니다.

- 사용자 특성
- 명명된 식

문자열

문자열은 문자 데이터를 0 개 이상의 문자가 작은따옴표나 큰따옴표 쌍으로 묶인 문자열로 나타냅니다. 문자열 값은 기본 제공 연산자 및 함수로 조작할 수 있는 상수입니다. 예를 들어 문자열은 연결되거나 다른 데이터 형식으로 변환될 수 있습니다.

선택적인 양수 또는 음수 부호로 시작하고 "0"에서 "9" 사이의 문자를 포함하는 문자열은 숫자 값으로 변환될 수 있습니다. 문자열 "TRUE" 및 "YES"(또는 "true" 및 "yes")는 부울 값 TRUE 로 변환될 수 있습니다. 다른 모든 문자열 값은 FALSE 로 변환됩니다. 또한 두 개의 문자열이 연결될 수 있습니다. 연결 시 두 번째 문자열의 시작 부분이 첫 번째 문자열의 끝에 결합됩니다.

집합과 LDAP DN(고유 이름)은 문자열 데이터 형식의 특수한 경우입니다. 집합은 'element1^element2'와 같이 각 요소가 캐럿 문자로 구분된 문자열입니다. 집합의 각 요소는 문자열입니다.

LDAP DN 은 LDAP 디렉터리의 항목을 고유하게 식별하는 간단한 문자열로, 해당 형식은 LDAP 사양에 의해 정의됩니다.

숫자

숫자는 앞에 선택적 양수 또는 음수 부호가 오는 정수여야 합니다. 4 바이트 정수나 -2^{31} 에서 2^{31} 사이의 정수가 지원됩니다. 소수점은 무시됩니다. 숫자 값은 기본 제공 연산자 및 함수로 조작할 수 있는 상수입니다. 예를 들어 숫자는 다른 데이터 형식으로 변환될 수 있습니다.

숫자는 선택적 음수 부호로 시작하고 "0"에서 "9" 사이의 문자를 포함하는 문자열로 변환될 수 있습니다. 또한 숫자는 부울 값으로 변환될 수도 있습니다. 0 이 아닌 숫자는 TRUE 로 변환되고 0 은 FALSE 로 변환됩니다.

날짜는 숫자 데이터 형식의 특수한 경우입니다. 날짜는 1970 년 1 월 1 일 이후 경과된 초 수로 표현됩니다.

날짜를 조작하는 함수는 매우 다양합니다. 예를 들어 DOW 함수는 날짜의 숫자 표현을 받아 요일에 해당하는 0~6 범위의 숫자를 반환합니다. 문자열 형식의 날짜를 숫자로 변환하고 숫자로 표현된 날짜를 문자열로 변환하는 함수도 있습니다.

부울

부울은 TRUE 또는 FALSE 라는 두 개의 값 중 하나입니다. 부울 값은 기본 제공 연산자 및 함수로 비교 및 조작할 수 있는 상수입니다. 예를 들어 부울은 다른 데이터 형식으로 변환될 수 있습니다.

부울 값이 숫자 값으로 변환될 경우 TRUE 는 1 로 변환되고 FALSE 는 0 으로 변환됩니다. 부울 값이 문자열 값으로 변환될 경우 TRUE 는 "TRUE"로 변환되고 FALSE 는 "FALSE"로 변환됩니다.

사용자 특성

사용자 특성에는 이름과 값이 있습니다. 사용자 특성 *이름*은 *따옴표*로 묶이지 않습니다. 사용자 특성 *값*은 문자열로, *따옴표*로 묶입니다. 사용자 특성 이름은 다음 규칙을 따라야 합니다.

- 대/소문자를 구분하지 않습니다.
- 첫 번째 문자는 문자여야 합니다.
- US-ASCII 영문자, 숫자 및 밑줄 문자만 포함합니다.

사용자 특성 이름은 리터럴이 아닌 변수 데이터 형식으로 작동합니다. 사용자 특성 이름이 있을 경우 해당하는 특성 값이 사용자 디렉터리에서 검색됩니다. 특성 값이 여러 개인 경우에는 집합으로 반환됩니다. 집합은 'value1^value2'와 같이 각 요소가 캐럿 문자로 구분된 문자열입니다. 집합의 각 요소는 문자열입니다.

명명된 식

명명된 식에는 가상 사용자 특성과 사용자 클래스라는 두 가지 유형이 있습니다.

가상 사용자 특성은 사용자 특성과는 다릅니다. 사용자 디렉터리에 문자열로 저장되는 사용자 특성과 달리 가상 사용자 특성은 런타임에 계산되고 문자열, 숫자 또는 부울 값을 반환하는 식을 명명합니다. 또한 사용자 특성과 달리 가상 사용자 특성은 읽기 전용입니다.

사용자 클래스는 가상 사용자 특성의 특수한 경우입니다. 사용자 클래스는 가상 사용자 특성과 마찬가지로 런타임에 식을 명명합니다. 또한 사용자 클래스는 가상 사용자 특성과 달리 사용자 그룹 또는 디렉터리의 구성원 자격을 테스트하고 부울 값만 반환하는 식을 명명합니다.

가상 사용자 특성 이름과 사용자 클래스 이름은 모두 다음 규칙을 따라야 합니다.

- 대/소문자를 구분하지 않습니다.
- 가상 사용자 특성의 경우 첫 번째 문자는 파운드 기호(#)여야 합니다.
- 사용자 클래스의 경우 첫 번째 문자는 at 기호(@)여야 합니다.
- 두 번째 문자는 문자나 밑줄이어야 합니다.
- 나머지 문자는 US-ASCII 영문자, 숫자 및 밑줄 문자여야 합니다.

참고: 활성 식과 명명된 식은 동일하지 않습니다. 두 유형의 식은 모두 런타임에 평가되지만 다음과 같은 차이점이 있습니다.

- 활성 식은 부울 식인 반면, 명명된 식은 문자열, 숫자 또는 부울 값을 반환할 수 있습니다.
- 활성 식은 있는 그대로 참조되고 사용할 때마다 다시 입력해야 하는 반면, 명명된 식은 이름으로 참조되며 어느 위치에서나 참조되고 재사용될 수 있습니다.

식 구문 개요

이 부록에 설명된 구문은 내부 SiteMinder 식 계산기에 속해 있습니다. 관리 UI에서 역할 또는 권한을 정의할 때 식에서 이 구문을 구성하는 데이터 형식, 연산자 및 기본 제공 함수를 사용할 수 있습니다. 명명되지 않은 식은 정의하는 특정 역할 및 권한에 로컬로 적용되며, 전역적으로 정의되는 명명된 식을 사용할 수도 있습니다.

명명된 식에는 이름이 #로 시작하는 가상 사용자 특성과 이름이 @로 시작하는 사용자 클래스가 포함됩니다.

가상 사용자 특성은 사용자 디렉터리 항목에서 필요한 정보를 읽을 수 없을 때 값을 계산합니다. 가상 사용자 특성은 문자열, 숫자 또는 부울 값을 반환합니다. 예를 들어 이름 정보를 정렬용으로 자주 사용할 수 있도록 이름 정보에 형식을 지정하려면 사용자 인터페이스에서 다음과 같이 **#SortName** 이라는 가상 사용자 특성을 정의합니다.

```
UCase(RTrim(LastName + "," + FirstName + " " + Initial))
```

이 예에서는 두 개의 기본 제공 함수 **UCASE** 및 **RTRIM** 을 사용합니다. 이러한 이름은 대/소문자를 구분하지 않습니다.

사용자 클래스는 관리자 등의 사용자 유형을 기반으로 사용자가 특정 범주에 속해 있는지 여부를 확인하는 식입니다. 사용자는 특정 사용자 클래스의 구성원이거나 구성원이 아니므로 사용자 클래스 식의 결과는 항상 부울입니다.

가상 사용자 특성 또는 사용자 클래스를 정의할 때 이를 전용으로 지정할 수 있습니다. 이는 다른 명명된 식에서만 호출할 수 있음을 의미합니다. 마찬가지로 일부 기본 제공 함수는 권한 있는 함수로 지정되며, 이는 다른 명명된 식 내에서만 호출할 수 있음을 의미합니다. 권한 있는 함수는 "설명" 단원에서 "권한 있음"으로 표시됩니다. 하나 이상의 LDAP 고유 이름을 매개 변수로 사용하는 함수는 "설명" 단원에서 "LDAP 전용"으로 표시됩니다.

붙여넣기

식은 정책 저장소에 개체로 저장될 수 있으며, 다른 식을 비롯한 다른 위치에서 이름으로 참조될 수 있습니다. 식은 자리 표시자 %1~%9 와 특수 자리 표시자 %0 을 통해 명명된 식에 값을 전달할 수 있습니다. 이를 붙여넣기라고 합니다.

명명된 식에는 가상 사용자 특성과 사용자 클래스라는 두 가지 유형이 있습니다. 가상 사용자 특성 이름은 파운드 기호로 시작하고 사용자 클래스 이름은 at 기호로 시작합니다. 두 유형의 명명된 식 뒤에는 최대 9 개의 매개 변수가 옵니다. 이 구문은 다음과 같이 함수 구문과 유사합니다.

```
#virtual_user_attribute(P1, P2, P3, P4, P5, P6, P7, P8, P9)
```

```
@user_class(P1, P2, P3, P4, P5, P6, P7, P8, P9)
```

정책 저장소에 명명된 식을 생성할 때 기본 제공되는 연산자와 함수, 리터럴 데이터 형식, 자리 표시자 및 다른 명명된 식을 사용할 수 있습니다. 변수 데이터를 명명된 식으로 전달하려면 자리 표시자를 사용하십시오. 다음 예에서 URL 은 각 반복 중에 업데이트되므로 자리 표시자 %1 로 나타내야 합니다.

예:

다음과 같이 URL 을 받아 파일 이름을 반환하는 #URLFile 이라는 가상 특성을 생성할 수 있습니다.

```
#URLFile := { FIND(%1, '/')=0 ? %1 : #URLFile(AFTER(%1, '/')) }
```

```
Return_value=#URLFile('C:\My Documents\expression_syntax.doc')
```

```
Return_value='expression_syntax.doc'
```

이 예에서 URL 은 자리 표시자 %1 을 통해 기본 제공 함수 FIND 에 전달됩니다. FIND 는 URL 에서 첫 번째로 나타나는 "/" 를 찾아 해당 위치를 반환합니다. "/" 를 찾을 수 없는 경우 FIND 는 0 을 반환하고 #URLFile 은 파일 이름을 반환합니다. 그렇지 않은 경우 URL 이 자리 표시자 %1 을 통해 기본 제공 함수 AFTER 에 전달됩니다. AFTER 는 URL 중 "/" 의 뒷부분을 반환합니다. 그런 다음 단축된 URL 이 #URLFile 에 전달됩니다. 재귀가 지원됩니다.

다음 표에서는 이 예의 각 반복이 완료될 때의 위치 값과 URL 을 보여 줍니다.

반복	위치	URL
1	3	'My Documents\expression_syntax.doc'
2	16	'expression_syntax.doc'

ENUMERATE 또는 LOOP 와 같은 일부 기본 제공 함수가 명명된 식을 여러 번, 즉 집합의 각 요소에 대해 한 번씩 호출할 경우 특수 자리 표시자 %0 을 사용하여 명명된 식이 생성되어야 합니다. 예를 들어 다음과 같이 임의 개수의 집합 요소에서 후행 공백을 제거하는 #RTrimset 이라는 식을 생성할 수 있습니다.

```
#RTrimset := RTrim(%0)
```

그런 후 다음과 같이 기본 제공 함수 ENUMERATE 를 통해 집합을 #RTrimset 에 전달할 수 있습니다.

```
Return_value=ENUMERATE('First_name ^Middle_name ^Last_name ',#RTrimset)
Return_value='First_name^Middle_name^Last_name'
```

이 예에서 집합은 세 개의 요소(이름, 중간 이름 및 성)로 구성되어 있습니다. ENUMERATE 는 각 요소를 #RTrimset 에 전달합니다. #RTrimset 은 후행 공백을 제거하고 ENUMERATE 에 단축된 이름을 반환합니다. ENUMERATE 는 반환된 각 이름을 결과 문자열에 포함하고 캐럿 문자를 사용하여 각 이름을 구분합니다.

연산자

이 항목에는 지원되는 모든 연산자가 범주별로 나와 있습니다.

비교 연산자

- 같음(= 및 ~=)
- 같지 않음(!= 및 ~=)
- 보다 큼(> 및 ~>)
- 보다 작음(< 및 ~<)
- 크거나 같음(>= 및 ~>=)
- 작거나 같음(<= 및 ~<=)

문자열 연산자

- BEGINS_WITH 및 ~BEGINS_WITH
- ENDS_WITH 및 ~ENDS_WITH
- CONTAINS 및 ~CONTAINS
- 패턴 일치(LIKE)
- 연결(+)

집합 연산자

- 집합 포함(IN 및 ~IN)
- INTERSECT 및 ~INTERSECT
- UNION 및 ~UNION
- 인덱싱([..])

논리 연산자

- AND, & 및 &&
- NOT
- OR, | 및 ||
- XOR

산술 연산자

- 더하기(+)
- 빼기(-)
- 곱하기(*)
- 나누기(/)

기타 연산자

- 조건부 결정(? 및 :)

같음 연산자

같음 연산자 `=`는 두 값을 비교합니다. 두 값이 같은 경우 이 연산의 결과는 **TRUE** 입니다. 그렇지 않은 경우 이 연산의 결과는 **FALSE** 입니다. 두 값이 문자열인 경우 연산은 대/소문자를 구분합니다.

같음 연산자 `~=`는 문자열 값만 비교하고 대/소문자를 구분하지 않습니다.

예:

```
1 = 1  
Result = TRUE
```

```
1 = 2  
Result = FALSE
```

```
"sparrow" = "SPARROW"  
Result = FALSE
```

```
"sparrow" ~= "SPARROW"  
Result = TRUE
```

추가 정보:

[같지 않음 연산자](#) (페이지 872)

같지 않음 연산자

같지 않음 연산자 `!=`는 두 값을 비교합니다. 두 값이 같지 않은 경우 이 연산의 결과는 **TRUE** 입니다. 그렇지 않은 경우 이 연산의 결과는 **FALSE** 입니다. 두 값이 문자열인 경우 연산은 대/소문자를 구분합니다.

같지 않음 연산자 `~!=`는 문자열 값만 비교하고 대/소문자를 구분하지 않습니다.

예:

```
1 != 1  
Result = FALSE
```

```
1 != 2  
Result = TRUE
```

```
"sparrow" != "SPARROW"  
Result = TRUE
```

```
"sparrow" ~!= "SPARROW"  
Result = FALSE
```

추가 정보:

[같은 연산자](#) (페이지 871)

보다 작음 연산자

보다 작음 연산자 `<`는 두 값을 비교합니다. 첫 번째 값이 두 번째 값보다 작은 경우 이 연산의 결과는 **TRUE** 입니다. 그렇지 않은 경우 이 연산의 결과는 **FALSE** 입니다. 두 값이 부울인 경우 **TRUE** 가 **FALSE** 보다 큼니다. 두 값이 문자열인 경우 연산은 대/소문자를 구분합니다.

보다 작음 연산자 `~<`는 문자열 값만 비교하고 대/소문자를 구분하지 않습니다.

예:

```
1 < 2  
Result = TRUE
```

```
2 < 1  
Result = FALSE
```

```
'crow' < 'CROW'  
Result = FALSE
```

```
'crow' ~< 'CROW'  
Result = FALSE
```

추가 정보:

[보다 큼 연산자](#) (페이지 873)

보다 큼 연산자

보다 큼 연산자 >는 두 값을 비교합니다. 첫 번째 값이 두 번째 값보다 큰 경우 이 연산의 결과는 **TRUE** 입니다. 그렇지 않은 경우 이 연산의 결과는 **FALSE** 입니다. 두 값이 부울인 경우 **TRUE** 가 **FALSE** 보다 큼니다. 두 값이 문자열인 경우 연산은 대/소문자를 구분합니다.

보다 큼 연산자 ~>는 문자열 값만 비교하고 대/소문자를 구분하지 않습니다.

예:

```
1 > 2  
Result = FALSE
```

```
2 > 1  
Result = TRUE
```

```
'crow' > 'CROW'  
Result = TRUE
```

```
'crow' ~> 'CROW'  
Result = FALSE
```

추가 정보:

[보다 작음 연산자](#) (페이지 872)

작거나 같음 연산자

작거나 같음 연산자 `<=`는 두 값을 비교합니다. 첫 번째 값이 두 번째 값보다 작거나 같은 경우 이 연산의 결과는 **TRUE** 입니다. 그렇지 않은 경우 이 연산의 결과는 **FALSE** 입니다. 두 값이 부울인 경우 **TRUE**가 **FALSE**보다 큼니다. 두 값이 문자열인 경우 연산은 대/소문자를 구분합니다.

작거나 같음 연산자 `~<=`는 문자열 값만 비교하고 대/소문자를 구분하지 않습니다.

예:

```
1 <= 2  
Result = TRUE
```

```
2 <= 1  
Result = FALSE
```

```
'junco' <= 'JUNCO'  
Result = FALSE
```

```
'junco' ~<= 'JUNCO'  
Result = TRUE
```

추가 정보:

[크거나 같음 연산자](#) (페이지 875)

크거나 같음 연산자

크거나 같음 연산자 `>=`는 두 값을 비교합니다. 첫 번째 값이 두 번째 값보다 크거나 같은 경우 이 연산의 결과는 **TRUE** 입니다. 그렇지 않은 경우 이 연산의 결과는 **FALSE** 입니다. 두 값이 부울인 경우 **TRUE**가 **FALSE**보다 큼니다. 두 값이 문자열인 경우 연산은 대/소문자를 구분합니다.

크거나 같음 연산자 `~>=`는 문자열 값만 비교하고 대/소문자를 구분하지 않습니다.

예:

```
1 >= 2  
Result = FALSE
```

```
2 >= 1  
Result = TRUE
```

```
'junco' >= 'JUNCO'  
Result = TRUE
```

```
'junco' ~>= 'JUNCO'  
Result = TRUE
```

추가 정보:

[작거나 같음 연산자](#) (페이지 874)

시작 문자 연산자

두 시작 문자 연산자(`BEGINS_WITH` 및 `~BEGINS_WITH`)는 문자열 값과 함께 사용할 수 있습니다. 첫 번째 문자열이 두 번째 문자열로 시작하는 경우 이 연산의 결과는 **TRUE** 입니다. 그렇지 않은 경우 이 연산의 결과는 **FALSE** 입니다.

"`BEGINS_WITH`" 연산자는 대/소문자를 구분합니다. "`~BEGINS_WITH`" 연산자는 대/소문자를 구분하지 않습니다.

예:

```
'SiteMinder' BEGINS_WITH 'site'  
Result = FALSE
```

```
'SiteMinder' ~BEGINS_WITH 'site'  
Result = TRUE
```

추가 정보:

[끝 문자 연산자](#) (페이지 876)

[포함 연산자](#) (페이지 876)

끝 문자 연산자

두 끝 문자 연산자(ENDS_WITH 및 ~ENDS_WITH)는 문자열 값과 함께 사용할 수 있습니다. 첫 번째 문자열이 두 번째 문자열로 끝나는 경우 이 연산의 결과는 TRUE 입니다. 그렇지 않은 경우 이 연산의 결과는 FALSE 입니다.

"ENDS_WITH" 연산자는 대/소문자를 구분합니다. "~ENDS_WITH" 연산자는 대/소문자를 구분하지 않습니다.

예:

```
'SiteMinder' ENDS_WITH 'DER'  
Result = FALSE
```

```
'SiteMinder' ~ENDS_WITH 'DER'  
Result = TRUE
```

포함 연산자

두 포함 연산자(CONTAINS 및 ~CONTAINS)는 문자열 값과 함께 사용할 수 있습니다. 첫 번째 문자열에 두 번째 문자열이 포함된 경우 이 연산의 결과는 TRUE 입니다. 그렇지 않은 경우 이 연산의 결과는 FALSE 입니다.

"CONTAINS" 연산자는 대/소문자를 구분합니다. "~CONTAINS" 연산자는 대/소문자를 구분하지 않습니다.

예:

'SiteMinder' CONTAINS 'EMI'
Result = FALSE

'SiteMinder' ~CONTAINS 'EMI'
Result = TRUE

추가 정보:

[시작 문자 연산자](#) (페이지 875)

[끝 문자 연산자](#) (페이지 876)

집합 포함 연산자

집합 포함 연산자(IN 및 ~IN)는 첫 번째 피연산자인 문자열이 두 번째 피연산자인 집합의 요소인지 여부를 테스트합니다. 문자열이 집합의 요소인 경우 이 연산의 결과는 TRUE 입니다. 그렇지 않은 경우 이 연산의 결과는 FALSE 입니다.

"IN" 연산자는 대/소문자를 구분합니다. "~IN" 연산자는 대/소문자를 구분하지 않습니다.

예:

'MON' IN 'Sun^Mon^Tue^Wed^Thu^Fri^Sat'
Result = FALSE

'MON' ~IN 'Sun^Mon^Tue^Wed^Thu^Fri^Sat'
Result = TRUE

패턴 일치 연산자

패턴 일치 연산자 LIKE 는 'abc' LIKE '???'와 같이 문자열 값을 문자 패턴(역시 문자열임)과 비교합니다. 문자열 값이 패턴과 일치하는 경우 이 연산의 결과는 TRUE 입니다. 그렇지 않은 경우 이 연산의 결과는 FALSE 입니다. 패턴 일치 연산은 대/소문자를 구분합니다.

패턴은 단일 문자, 문자 범위 또는 둘 모두를 조합하여 생성합니다. 문자 범위는 0-9 와 같이 범위의 첫 번째 문자, 하이픈 및 범위의 마지막 문자를 연결하여 지정합니다. 유효한 문자에는 숫자, 대문자, 소문자, 특별한 의미를 갖는 예약된 문자가 포함됩니다. 문자 집합은 하나 이상의 문자, 문자 범위 또는 둘 모두를 포함하며 대괄호로 묶입니다. 예를 들어 [0-9A-Za-z], [0-2ABC] 및 [789x-z]는 모두 유효한 문자 집합입니다.

참고: 문자 범위는 항상 문자 집합의 일부입니다.

다음 표에서는 예약된 문자와 해당 의미에 대해 설명합니다.

문자	의미
' 또는 "	'abc' 또는 "abc"와 같이 문자열을 지정합니다.
-	0-9 와 같이 문자 범위를 지정합니다.
?	임의의 단일 문자와 일치합니다.
*	문자가 하나 있거나 없는 경우를 포함하여 임의의 문자 시퀀스와 일치합니다.
[set]	지정된 집합에 있는 임의의 단일 문자와 일치합니다.
[!set] 또는 [^set]	지정된 집합에 <u>없는</u> 임의의 단일 문자와 일치합니다.
[set]?	지정된 집합에 있는 임의의 단일 문자나 빈 문자열과 일치합니다.
[set]*	문자가 하나 있거나 없는 경우를 포함하여 지정된 집합에 있는 문자 시퀀스와 일치합니다.
\	*와 같이 예약된 문자를 일반 문자로 처리합니다.

'?' 사용 예

" LIKE '?'
Result = FALSE

'a' LIKE '?'
Result = TRUE

'ab' LIKE '?'
Result = FALSE

'abc' LIKE '???'
Result = TRUE

'191' LIKE '1??'
Result = TRUE

'201' LIKE '1??'
Result = FALSE

'*' 사용 예

" LIKE '*'
Result = TRUE

'a' LIKE '*'
Result = TRUE

'a1b2c3' LIKE '*'
Result = TRUE

'robin' LIKE 'r*n'
Result = TRUE

'room' LIKE 'r*n'
Result = FALSE

'[set]' 사용 예

" LIKE '[abcde]'
Result = FALSE

'f' LIKE '[abcde]'
Result = FALSE

'c' LIKE '[abcde]'
Result = TRUE

'abc' LIKE '[abcde]' 비교: 'abc' LIKE '[abcde]*'
Result = FALSE

'[!set]' 또는 '[^set]' 사용 예

" LIKE '[!abcde]'
Result = FALSE

'f' LIKE '[^abcde]'
Result = TRUE

'c' LIKE '[!abcde]'
Result = FALSE

'xyz' LIKE '[^abcde]'
Result = FALSE

'[set]?' 사용 예

" LIKE '[abcde]?'
Result = TRUE

'a' LIKE '[abcde]?'
Result = TRUE

'ab' LIKE '[abcde]?'
Result = FALSE

'z' LIKE '[abcde]?'
Result = FALSE

'[set]*' 사용 예

" LIKE '[abcde]*'
Result = TRUE

'a' LIKE '[abcde]*'
Result = TRUE

'aabbccdde' LIKE '[abcde]*'
Result = TRUE

'abcdef' LIKE '[abcde]*'
Result = FALSE

'abc' LIKE '[abcde]*' 비교: 'abc' LIKE '[abcde]'
Result = TRUE

'\' 사용 예

'123-456-7890' LIKE '[0-9][0-9][0-9]\-[0-9][0-9][0-9]\-[0-9][0-9][0-9]'
Result = TRUE

'_!^*_?_' LIKE '_!_^_*_?_'
Result = TRUE

대/소문자 구분 테스트 예

'a' LIKE '[a-z]'
Result = TRUE

'A' LIKE '[a-z]'
Result = FALSE

'A' LIKE '[A-Za-z]'
Result = TRUE

'Robin' LIKE '[A-Za-z]*'
Result = TRUE

'Robin' LIKE '[A-Z][a-z]*'
Result = TRUE

'robin' LIKE '[A-Z][a-z]*'
Result = FALSE

교집합 연산자

교집합 연산자(**INTERSECT** 및 **~INTERSECT**)는 두 집합을 비교합니다. 집합은 각 요소가 캐럿 문자로 구분된 문자열입니다. 결과 집합은 두 집합 모두에 있는 요소만 포함하는 문자열입니다. "**INTERSECT**" 연산자는 대/소문자를 구분합니다. "**~INTERSECT**" 연산자는 대/소문자를 구분하지 않습니다.

중요! 결과 집합의 요소 순서는 예측할 수 없습니다. 연산이 대/소문자를 구분하지 않는 경우에는 결과 집합 요소의 대/소문자도 예측할 수 없습니다.

예:

```
'BLUE JAY^ORIOLE^WREN' INTERSECT 'BLUE JAY^wren'  
Result = 'BLUE JAY'
```

```
'BLUE JAY^ORIOLE^WREN' ~INTERSECT 'BLUE JAY^wren'  
Result = 'BLUE JAY^WREN'
```

합집합 연산자

합집합 연산자(**UNION**)는 두 피연산자 집합의 고유 요소를 모두 포함하는 집합(두 집합의 합집합)을 반환합니다. 중복 요소는 제거됩니다.

~UNION 과 같이 **UNION** 연산자 앞에 물결표 문자(~)가 있는 경우 대/소문자만 다른 두 요소는 동일한 것으로 간주됩니다.

중요! 결과 집합의 요소 순서는 예측할 수 없습니다. 또한 **~UNION** 연산자가 지정된 경우에는 결과 교집합 요소의 대/소문자도 예측할 수 없습니다.

예:

```
"JUAN^BART^CHUCK" UNION "CHUCK^Bart"  
Result = "JUAN^BART^CHUCK^Bart"
```

```
"JUAN^BART^CHUCK" ~UNION "CHUCK^Bart"  
Result = "JUAN^BART^CHUCK"
```

```
"JUAN^BART^JUAN^CHUCK" UNION "JUAN^BART^JUAN^CHUCK"  
Result = "JUAN^BART^CHUCK"
```

NOT 연산자

NOT 연산자는 단일 부울 피연산자를 사용하며, 해당 값을 반대 값으로 바꿉니다. 즉, FALSE 를 TRUE 로, TRUE 를 FALSE 로 바꿉니다. 이 연산자는 대개 비교 연산자의 결과를 반대로 바꾸는 데 사용됩니다.

예:

```
NOT ("SiteMinder" ENDS_WITH "R")  
Result = TRUE
```

```
NOT ("SiteMinder " ~ENDS_WITH "R")  
Result = FALSE
```

AND 연산자

AND 연산자(& 및 &&로 쓰기도 함)는 두 개의 부울 피연산자를 사용하며, 두 피연산자가 모두 TRUE 일 경우에 TRUE 를 반환합니다. 이 연산자는 대개 두 비교를 연결하는 데 사용됩니다.

첫 번째 부울 피연산자가 FALSE 이면 결과가 틀림없이 FALSE 이므로 두 번째 부울 피연산자는 평가되지 않습니다.

예:

```
(1 > 2) AND ("JUAN" ~= "JUAN")  
Result = FALSE
```

```
(1 < 2) AND ("JUAN" ~= "JUAN")  
Result = TRUE
```

OR 연산자

OR 연산자(| 또는 ||로 쓰기도 함)는 두 개의 부울 피연산자를 사용하며, 두 피연산자 중 어느 하나가 TRUE 일 경우에 TRUE 를 반환합니다. 이 연산자는 대개 두 비교를 연결하는 데 사용됩니다.

첫 번째 부울 피연산자가 TRUE 이면 결과가 틀림없이 TRUE 이므로 두 번째 부울 피연산자는 평가되지 않습니다.

예:

```
(1 > 2) OR ("JUAN" ~= "JUAN")  
Result = TRUE
```

```
(1 < 2) OR ("JUAN" ~= "JUAN")  
Result = TRUE
```

배타적 OR 연산자

배타적 OR(XOR) 연산자는 부울 피연산자를 두 개 사용하며, 두 피연산자 중 하나만 TRUE 일 경우에 TRUE 를 반환합니다. 이 연산자는 대개 두 비교를 연결하는 데 사용됩니다.

예:

```
(1 > 2) XOR ("JUAN" ~= "JUAN")  
Result = TRUE
```

```
(1 < 2) XOR ("JUAN" ~= "JUAN")  
Result = FALSE
```

문자열 연결 연산자

문자열 연결 연산자(+)는 두 문자열 피연산자의 조합을 포함하는 문자열을 반환합니다.

첫 번째 피연산자가 문자열이지만 두 번째 피연산자는 숫자나 부울인 경우 두 번째 피연산자가 문자열로 변환됩니다. 첫 번째 피연산자가 숫자인 경우 + 연산자는 연결이 아니라 산술 더하기를 나타냅니다.

예:

```
"JUAN" + " " + "Jones"  
Result = "JUAN Jones"
```

```
"JUAN" + 2  
Result = "JUAN2"
```


산술 더하기 연산자

산술 더하기(+) 연산자는 두 숫자 피연산자의 합을 반환합니다.

첫 번째 피연산자가 숫자이지만 두 번째 피연산자는 문자열이나 부울인 경우 두 번째 피연산자가 숫자로 변환됩니다.

예:

```
1 + 2  
Result = 3
```

```
1 + "JUAN"  
Result = 1
```

```
1 + "32JUAN"  
Result = 33
```

산술 빼기 연산자

산술 빼기(-) 연산자는 두 숫자 피연산자의 차를 반환합니다.

첫 번째 피연산자가 숫자이지만 두 번째 피연산자는 문자열이나 부울인 경우 두 번째 피연산자가 숫자로 변환됩니다.

예:

```
1 - 2  
Result = -1
```

```
1 - "JUAN"  
Result = 1
```

```
100 - "32JUAN"  
Result = 68
```

산술 곱하기 연산자

산술 곱하기(*) 연산자는 두 피연산자의 곱을 반환합니다.

첫 번째 피연산자가 숫자이지만 두 번째 피연산자는 문자열이나 부울인 경우 두 번째 피연산자가 숫자로 변환됩니다.

예:

```
1 * 2  
Result = 2
```

```
1 * "JUAN"  
Result = 0
```

```
100 * "32JUAN"  
Result = 3200
```

산술 나누기 연산자

산술 나누기 연산자(/)는 두 피연산자를 나눈 몫을 반환합니다.

첫 번째 피연산자가 숫자이지만 두 번째 피연산자는 문자열이나 부울인 경우 두 번째 피연산자가 숫자로 변환됩니다.

모든 나누기는 정수 나누기입니다.

참고: 산술적으로 정의되지 않는 0 으로 나누기는 이 환경에서 항상 오류를 반환합니다.

예:

```
1 / 2  
Result = 0
```

```
1 / "JUAN"  
Result = 0
```

```
100 / "32JUAN"  
Result = 3
```

조건부 연산자

조건부 연산자는 부울 식(첫 번째 피연산자)을 평가한 후 그 결과에 따라 다른 두 피연산자 중 하나를 반환합니다.

부울 피연산자가 **TRUE** 인 경우 이 연산자의 결과는 두 번째 피연산자(**THEN** 절)이고, 그렇지 않은 경우 세 번째 피연산자(**ELSE** 절)가 반환됩니다. 두 번째와 세 번째 피연산자는 동일한 형식이어야 합니다.

이 연산자의 절은 항상 하나만 평가됩니다. 즉, **THEN** 절(피연산자)이 평가된 경우 **ELSE** 절(피연산자)은 평가되지 않습니다. 그 반대의 경우도 마찬가지입니다.

예:

```
"JUAN" = "juan" ? "YES" : "NO"
Result = "NO"
```

```
"JUAN" ~= "juan" ? "YES" : "NO"
Result = "YES"
```

인덱싱 연산자

인덱싱 연산자는 두 개의 인수(집합과 인덱스를 나타내는 숫자)를 사용합니다. 집합은 구성 요소로 분할되고 지정된 인덱스에 해당하는 구성 요소가 반환됩니다(일반적인 배열의 경우와 같음). 인덱스가 범위를 벗어나면 빈 문자열이 반환됩니다.

집합의 첫 번째 요소는 인덱스가 0입니다.

예:

```
"Sun^Mon^Tue^Wed^Thu^Fri^Sat"[2]
Result = "Tue"
```

```
"Sun^Mon^Tue^Wed^Thu^Fri^Sat"[0]
Result = "Sun"
```

식에서 사용할 수 있는 함수

이 항목에는 모든 함수가 이용 영역별로 나와 있습니다.

숫자 함수

- ABS
- ALL
- ANDBITS
- ANY
- HEX

- MAX
- MIN
- MOD
- NOTBITS
- ORBITS
- SIGN
- XORBITS

문자열 함수

- AFTER
- BEFORE
- CENTER
- CHAR
- FIND
- LCASE
- LEFT
- LEN
- LPAD
- LTRIM
- MID
- PCASE
- RIGHT
- RPAD
- RPT
- RTRIM
- SPACE

- TRANSLATE
- UCASE

집합 함수

- COUNT
- ENUMERATE
- FILTER
- LOOP
- SORT

날짜 함수

- DATE(형식 1)
- DATE(형식 2)
- DATEFROMSTRING
- DATETOSTRING
- DAY
- DOW
- DOY
- HOUR
- HOUR24
- MINUTE
- MONTH
- NOW
- NOWGMT
- SECOND
- YEAR
- YEAR4

변환 함수

- BOOLEAN
- NUMBER
- STRING

일반 사용자 디렉터리 I/O 함수

- GET
- SET

LDAP 함수

- ABOVE
- AT
- BELOW
- COMMONDN
- EXPLODEDN
- PARENTDN
- RDN
- RELATIONDN

URL/경로 처리 함수

- QS
- URL
- URLDECODE
- URLENCODE

로깅 함수

- ERROR
- INFO
- TRACE
- WARNING

파일 I/O 함수

- EXISTS
- KEY
- LOG

오류 처리 함수

- MAYBE
- THROW
- VEXIST

기타 함수

- EVALUATE

ABOVE 함수 - 사용자가 지정된 LDAP DN 위에 있는지 여부

ABOVE 함수는 지정된 사용자(`user_DN`)가 지정된 컨테이너(`root_DN`)의 *상위* 컨테이너 내에 있는 경우 TRUE 를 반환합니다.

구문

ABOVE 함수의 형식은 다음과 같습니다.

`ABOVE(root_DN, user_DN)`

매개 변수

ABOVE 함수는 다음 매개 변수를 사용합니다.

root_DN(문자열)

user_DN(문자열)

반환 값

ABOVE 함수는 부울 값을 반환합니다.

설명

LDAP 전용: 예

ABS 함수 - 절대값 찾기

ABS 함수는 숫자의 절대값을 찾습니다.

구문

ABS 함수의 형식은 다음과 같습니다.

`ABS(number)`

매개 변수

ABS 함수는 다음 매개 변수를 사용합니다.

number(숫자)

반환 값

ABS 함수는 숫자를 반환합니다.

예

```
Return_value=ABS(3)  
Return_value=3
```

```
Return_value=ABS(-2)  
Return_value=2
```

AFTER 함수 - 문자열 찾기

AFTER 함수는 원본 문자열에서 지정된 검색 문자열을 찾고 원본 문자열 중 검색 문자열의 뒷부분을 반환합니다. 검색 문자열을 찾을 수 없는 경우 AFTER 함수는 빈 문자열을 반환합니다.

구문

AFTER 함수의 형식은 다음과 같습니다.

`AFTER(source_string, search_string[, not_case_sensitive][, n])`

매개 변수

AFTER 함수는 다음 매개 변수를 사용합니다.

source_string(문자열)

search_string(문자열)

not_case_sensitive(부울)

(선택 사항) 대/소문자 구분 여부를 지정합니다. *not_case_sensitive* 플래그가 생략되거나 FALSE 로 설정된 경우 이 함수는 원본 문자열에서 정확히 일치하는 문자열을 검색합니다. *not_case_sensitive* 플래그가 TRUE 로 설정된 경우 이 함수는 대/소문자를 무시합니다.

n(숫자)

(선택 사항) 원본 문자열에 포함된 검색 문자열의 인스턴스를 지정합니다. *n* 이 0 또는 1 로 설정되거나 생략된 경우 이 함수는 검색 문자열의 첫 번째 인스턴스를 찾습니다. 그렇지 않은 경우 이 함수는 검색 문자열의 *n* 번째 인스턴스를 찾습니다. *n* 이 음수이면 이 함수는 원본 문자열의 끝에서부터 검색을 시작합니다.

반환 값

AFTER 함수는 문자열을 반환합니다.

예

```
Return_value=AFTER('EricEric', 'r')
Return_value='icEric'
```

```
Return_value=AFTER('EricEric', 'R')
Return_value=''
```

```
Return_value=AFTER('EricEric', 'R', TRUE)
Return_value='icEric'
```

```
Return_value=AFTER('EricEric', 'r', -1)
Return_value='ic'
```

```
Return_value=AFTER('EricEric', 'R', -1)
Return_value=''
```

```
Return_value=AFTER('EricEric', 'R', TRUE, -1)
Return_value='ic'
```

```
Return_value=AFTER('EricEric', 'r', 2)  
Return_value='ic'
```

```
Return_value=AFTER('EricEric', 'R', 2)  
Return_value=""
```

```
Return_value=AFTER('EricEric', 'R', TRUE, 2)  
Return_value='ic'
```

ALL 함수 - 설정된 모든 비트

ALL 함수는 두 개의 숫자를 매개 변수로 사용하며, 두 번째 숫자에 설정된 모든 비트가 첫 번째 숫자에도 설정된 경우 TRUE 를 반환합니다.

구문

ALL 함수의 형식은 다음과 같습니다.

```
ALL(number1, number2)
```

매개 변수

ALL 함수는 다음 매개 변수를 사용합니다.

number1(숫자)

number2(숫자)

반환 값

ALL 함수는 부울 값을 반환합니다.

예

```
Return_value=ALL(7, 2)  
Return_value=TRUE
```

```
Return_value=ALL(7, 15)  
Return_value=FALSE
```

ANDBITS 함수 - bitwise AND 연산 수행

ANDBITS 함수는 두 숫자에 대해 bitwise AND 연산을 수행합니다.

구문

ANDBITS 함수의 형식은 다음과 같습니다.

```
ANDBITS(number1,number2)
```

매개 변수

ANDBITS 함수는 다음 매개 변수를 사용합니다.

number1(숫자)

number2(숫자)

반환 값

ANDBITS 함수는 숫자를 반환합니다.

예

```
Return_value=ANDBITS(7,2)
```

```
Return_value=2
```

```
Return_value=ANDBITS(7,15)
```

```
Return_value=7
```

ANY 함수 - 설정된 임의 비트

ANY 함수는 두 개의 숫자를 매개 변수로 사용하며, 두 번째 숫자에 설정된 임의 비트가 첫 번째 숫자에도 설정된 경우 TRUE 를 반환합니다.

구문

ANY 함수의 형식은 다음과 같습니다.

```
ANY(number1, number2)
```

매개 변수

ANY 함수는 다음 매개 변수를 사용합니다.

number1(숫자)

number2(숫자)

반환 값

ANY 함수는 부울 값을 반환합니다.

예

```
Return_value=ANY(7, 2)
```

```
Return_value=TRUE
```

```
Return_value=ANY(7, 15)
```

```
Return_value=TRUE
```

AT 함수 - 사용자가 지정된 LDAP DN 에 있는지 여부

AT 함수는 지정된 사용자(*user_DN*)가 지정된 컨테이너(*root_DN*) 내에 있는 경우 TRUE 를 반환합니다.

구문

AT 함수의 형식은 다음과 같습니다.

```
AT(root_DN, user_DN)
```

매개 변수

AT 함수는 다음 매개 변수를 사용합니다.

root_DN(문자열)

user_DN(문자열)

반환 값

AT 함수는 부울 값을 반환합니다.

설명

LDAP 전용: 예

BEFORE 함수 - 문자열 찾기

BEFORE 함수는 원본 문자열에서 지정된 검색 문자열을 찾고 원본 문자열 중 검색 문자열의 앞부분을 반환합니다. 검색 문자열을 찾을 수 없는 경우 BEFORE 함수는 전체 원본 문자열을 반환합니다.

구문

BEFORE 함수의 형식은 다음과 같습니다.

```
BEFORE(source_string, search_string[, not_case_sensitive][, n])
```

매개 변수

BEFORE 함수는 다음 매개 변수를 사용합니다.

source_string(문자열)

search_string(문자열)

not_case_sensitive(부울)

대/소문자 구분 여부를 지정합니다. *not_case_sensitive* 플래그가 FALSE 로 설정되거나 생략된 경우 BEFORE 함수는 원본 문자열에서 정확히 일치하는 문자열을 검색합니다. *not_case_sensitive* 플래그가 TRUE 로 설정된 경우 이 함수는 대/소문자를 무시합니다.

n(숫자)

원본 문자열에 포함된 검색 문자열의 인스턴스를 지정합니다. *n* 이 0 또는 1 로 설정되거나 생략된 경우 BEFORE 함수는 검색 문자열의 첫 번째 인스턴스를 찾습니다. 그렇지 않은 경우 이 함수는 검색 문자열의 *n* 번째 인스턴스를 찾습니다. *n* 이 음수이면 이 함수는 원본 문자열의 끝에서부터 검색을 시작합니다.

반환 값

BEFORE 함수는 문자열을 반환합니다.

예

```
Return_value=BEFORE('EricEric', 'r')  
Return_value='E'
```

```
Return_value=BEFORE('EricEric', 'R')  
Return_value='EricEric'
```

```
Return_value=BEFORE('EricEric', 'R', TRUE)  
Return_value='E'
```

```
Return_value=BEFORE('EricEric', 'r', -1)  
Return_value='EricE'
```

```
Return_value=BEFORE('EricEric', 'R', -1)  
Return_value='EricEric'
```

```
Return_value=BEFORE('EricEric', 'R', TRUE, -1)  
Return_value='EricE'
```

```
Return_value=BEFORE('EricEric', 'r', 2)  
Return_value='EricE'
```

```
Return_value=BEFORE('EricEric', 'R', 2)  
Return_value='EricEric'
```

```
Return_value=BEFORE('EricEric', 'R', TRUE, 2)  
Return_value='EricE'
```

BELOW 함수 - 사용자가 지정된 LDAP DN 아래에 있는지 여부

BELOW 함수는 지정된 사용자(user_DN)가 지정된 컨테이너(root_DN)의 하위 컨테이너 내에 있는 경우 TRUE 를 반환합니다.

구문

BELOW 함수의 형식은 다음과 같습니다.

```
BELOW(root_DN, user_DN)
```

매개 변수

BELOW 함수는 다음 매개 변수를 사용합니다.

root_DN(문자열)

user_DN(문자열)

반환 값

BELOW 함수는 부울 값을 반환합니다.

설명

LDAP 전용: 예

BOOLEAN 함수 - "TRUE" 또는 "FALSE"로 변환

BOOLEAN 함수는 숫자 또는 문자열 값을 "TRUE" 또는 "FALSE" 문자열 값으로 변환합니다. 숫자 값 0 은 "FALSE"로 변환됩니다. 다른 모든 숫자 값은 "TRUE"로 변환됩니다. 문자열 값 "true" 또는 "yes"는 "TRUE"로 변환됩니다. 다른 모든 문자열 값은 "FALSE"로 변환됩니다. BOOLEAN 함수는 대/소문자를 구분하지 않습니다.

구문

BOOLEAN 함수의 형식은 다음과 같습니다.

`BOOLean(number | string)`

매개 변수

BOOLEAN 함수는 다음 두 매개 변수 중 하나를 사용합니다.

number(숫자)

string(문자열)

반환 값

BOOLEAN 함수는 다음 문자열 값 중 하나를 반환합니다.

- "TRUE"
- "FALSE"

예

```
Return_value=BOOLEAN('Phoebe')  
Return_value="FALSE"
```

```
Return_value=BOOLEAN('Yes')  
Return_value="TRUE"
```

```
Return_value=BOOLEAN(123)  
Return_value="TRUE"
```

```
Return_value=BOOLEAN(0)  
Return_value="FALSE"
```

CHAR 함수 - ASCII 값 변환

CHAR 함수는 지정된 ASCII 값을 단일 문자 문자열로 변환합니다.

구문

CHAR 함수의 형식은 다음과 같습니다.

```
CHAR(ASCII_value)
```

매개 변수

CHAR 함수는 다음 매개 변수를 사용합니다.

ASCII_value(숫자)

ASCII 값을 지정합니다. *ASCII_value* 가 0 인 경우 이 함수는 빈 문자열을 반환합니다. *ASCII_value* 가 255 보다 큰 경우 이 함수는 *ASCII_value* 를 256 으로 나눈 나머지를 단일 문자 문자열로 변환합니다.

참고: 값을 256 으로 나눈 나머지를 구하는 것은 255 와의 bitwise AND 를 수행하는 것과 같습니다.

반환 값

CHAR 함수는 단일 문자 문자열을 반환합니다.

예

```
Return_value=CHAR(0)
Return_value=""

Return_value=CHAR(36)
Return_value='$'

Return_value=CHAR(299)
Return_value='+'

```

CENTER 함수 - 원본 문자열 채우기

CENTER 함수는 결과 문자열이 지정된 길이가 될 때까지 원본 문자열의 양쪽 끝을 지정된 문자로 채웁니다. 양쪽을 고르게 채울 수 없는 경우 이 함수는 문자열의 끝에 한 문자를 더 추가합니다.

구문

CENTER 함수의 형식은 다음과 같습니다.

```
CENTER(source, length[, padding])
```

매개 변수

CENTER 함수는 다음 매개 변수를 사용합니다.

source(문자열 또는 숫자)

원본 문자열을 지정합니다. 이 함수는 자동으로 숫자를 문자열로 변환합니다.

length(숫자)

결과 문자열의 길이를 지정합니다.

padding(문자열)

(선택 사항) 이 함수가 원본 문자열을 채우는 데 사용할 문자를 지정합니다.

- *padding* 의 길이가 1 자를 초과할 경우 이 함수는 첫 번째 문자를 사용합니다.
- *padding* 이 빈 문자열일 경우 이 함수는 원본을 채우지 않습니다.
- *padding* 이 생략되고 원본이 문자열일 경우 이 함수는 채우기에 공백을 사용합니다.
- *padding* 이 생략되고 원본이 숫자일 경우 이 함수는 채우기에 0 을 사용합니다.

반환 값

CENTER 함수는 문자열을 반환합니다.

예

```
Return_value=CENTER('Robin', 9, '*')  
Return_value='**Robin**'
```

```
Return_value=CENTER('Robin', 7, 'ooo')  
Return_value='oRobino'
```

```
Return_value=CENTER('Robin', 7, '')  
Return_value='Robin'
```

```
Return_value=CENTER('Robin', 11)  
Return_value=' Robin'
```

```
Return_value=CENTER(123, 9)  
Return_value='000123000'
```

COMMONDN 함수 - 공통 루트 찾기

COMMONDN 함수는 LDAP 서버를 호출하지 않고 두 LDAP DN(고유 이름)의 공통 루트를 반환합니다.

구문

COMMONDN 함수의 형식은 다음과 같습니다.

```
COMMONDN(ldapdn1, ldapdn2)
```

매개 변수

COMMONDN 함수는 다음 매개 변수를 사용합니다.

ldapdn1(문자열)

LDAP DN(고유 이름)을 지정합니다.

ldapdn2(문자열)

LDAP DN(고유 이름)을 지정합니다.

참고: *ldapdn1* 또는 *ldapdn2* 가 유효한 LDAP DN 이 아니거나 두 DN 이 공통 루트를 공유하지 않는 경우 이 함수는 빈 문자열을 반환합니다. LDAP DN 은 대/소문자를 구분하지 않습니다.

반환 값

COMMONDN 함수는 문자열을 반환합니다.

설명

LDAP 전용: 예

예

```
Return_value=COMMONDN('uid=Vincent,o=NDS.com', 'ou=People,o=nds.com')
Return_value='o=NDS.com'
```

COUNT 함수 - 집합의 요소 수 계산

COUNT 함수는 집합에 있는 요소의 수를 계산합니다.

구문

COUNT 함수의 형식은 다음과 같습니다.

```
COUNT(set[, case_sensitive])
```

매개 변수

COUNT 함수는 다음 매개 변수를 사용합니다.

set(문자열)

'element1^element2'와 같이 각 요소가 캐럿 문자로 구분된 문자열을 지정합니다. 각 요소는 문자열입니다.

case_sensitive(부울)

(선택 사항) 대/소문자 구분 여부를 지정합니다.

- **case_sensitive** 플래그가 생략된 경우 이 함수는 모든 요소 수를 계산합니다.
- **case_sensitive** 플래그가 제공된 경우 이 함수는 고유 요소 수만 계산합니다.
- **case_sensitive** 플래그가 TRUE 인 경우 이 함수는 대/소문자를 구분합니다.
- **case_sensitive** 플래그가 FALSE 인 경우 이 함수는 대/소문자를 구분하지 않습니다.

반환 값

COUNT 함수는 숫자를 반환합니다.

예

```
Return_value=COUNT('phoebe^PHOEBE^robin^robin')
Return_value=4
```

```
Return_value=COUNT('phoebe^PHOEBE^robin^robin', FALSE)
Return_value=2
```

```
Return_value=COUNT('phoebe^PHOEBE^robin^robin', TRUE)
Return_value=3
```

DATE 함수 - 자정으로 설정(형식 1)

DATE 함수(형식 1)는 날짜 및 시간의 숫자 표현을 받아 시간을 지정된 날짜의 자정으로 설정합니다.

구문

DATE 함수(형식 1)의 형식은 다음과 같습니다.

```
DATE(date_time)
```

매개 변수

DATE 함수(형식 1)는 다음 매개 변수를 사용합니다.

date_time(숫자)

날짜 및 시간을 1970 년 1 월 1 일 이후 경과된 초 수로 지정합니다.
date_time 이 올바른 날짜 및 시간 표현이 아닌 경우 이 함수는 -1 을 반환합니다.

반환 값

DATE 함수(형식 1)는 숫자를 반환합니다.

DATE 함수 - 년, 월, 일, 시, 분 및 초 변환(형식 2)

DATE 함수(형식 2)는 년, 월, 일, 시, 분 및 초를 나타내는 여섯 개의 숫자를 받아 이를 날짜 및 시간의 숫자 표현으로 변환합니다. 날짜 및 시간은 숫자로는 1970 년 1 월 1 일 이후 경과된 초 수로 표현됩니다. 시간 매개 변수 세 개가 생략된 경우 이 함수는 시간을 지정된 날짜의 자정으로 설정합니다.

구문

DATE 함수(형식 2)의 형식은 다음과 같습니다.

DATE(year, month, day[, hours, minutes, seconds])

매개 변수

DATE 함수(형식 2)는 다음 매개 변수를 사용합니다.

year(숫자)

4 자리 연도 표현을 지정합니다.

예: 2007

month(숫자)

월을 지정합니다.

범위: 1~12

day(숫자)

일을 지정합니다.

범위: 1~31

hours(숫자)

(선택 사항) 시간을 지정합니다.

범위: 0~23

minutes(숫자)

(선택 사항) 분을 지정합니다.

범위: 0~59

seconds(숫자)

(선택 사항) 초를 지정합니다.

범위: 0~59

반환 값

DATE 함수(형식 2)는 숫자를 반환합니다.

DATEFROMSTRING 함수 - 문자열을 숫자로 변환

DATEFROMSTRING 함수는 날짜, 시간 또는 둘 모두의 문자열 표현을 받아 문자열을 숫자 표현으로 변환합니다. 날짜 및 시간은 숫자로는 1970 년 1 월 1 일 이후 경과된 초 수로 표현됩니다.

구문

DATEFROMSTRING 함수의 형식은 다음과 같습니다.

DATEFROMSTRING(*date_time*[, *format_string*])

매개 변수

DATEFROMSTRING 함수는 다음 매개 변수를 사용합니다.

date_time(문자열)

format_string(문자열)

(선택 사항) *date_time*의 형식을 지정합니다. 예를 들어 *format_string* "YYYYMMDD"는 "20020223"의 형식을 지정합니다. *format_string*이 생략된 경우 이 함수는 기본 형식인 "YYYYMMDDhhmmss"를 사용합니다. *date_time*이 유효하지 않은 경우 이 함수는 -1을 반환합니다.

반환 값

DATEFROMSTRING 함수는 숫자를 반환합니다.

예

```
Return_value=DATEFROMSTRING('20020223')
Return_value=1024804800
```

DATETOSTRING 함수 - 숫자를 문자열로 변환

DATETOSTRING 함수는 날짜, 시간 또는 둘 모두의 숫자 표현을 받아 숫자를 문자열 표현으로 변환합니다.

구문

DATETOSTRING 함수의 형식은 다음과 같습니다.

```
DATETOSTRING(date_time[, format_string])
```

매개 변수

DATETOSTRING 함수는 다음 매개 변수를 사용합니다.

date_time(숫자)

날짜, 시간 또는 둘 모두를 1970 년 1 월 1 일 이후 경과된 초 수로 지정합니다. *date_time* 이 유효하지 않은 경우 이 함수는 "INVALID DATE" 값을 반환합니다.

format_string(문자열)

(선택 사항) 아래 표에 나열된 형식 코드를 사용하여 결과 문자열의 날짜, 시간 또는 둘 모두의 형식을 지정합니다. 표에 나열되지 않은 문자 또는 문자 조합은 결과 문자열에 그대로 삽입됩니다. *format_string* 이 생략된 경우 이 함수는 정책 서버에 현재 저장된 로캘에 적절한 날짜 및 시간 표현을 사용하여 결과 문자열의 형식을 지정합니다. 형식 코드 및 결과 형식은 다음과 같습니다.

코드	결과 형식
%a	약식 요일 이름(영어)
%A	전체 요일 이름(영어)

코드	결과 형식
%b	약식 월 이름(영어)
%B	전체 월 이름(영어)
%c	현재 로캘에 적절한 날짜 및 시간 표현
%#c	현재 로캘에 적절한 긴 날짜 및 시간 표현
%d	10 진수 형식의 날짜(01~31)
%H	24 시간 형식의 시간(00~23)
%I	12 시간 형식의 시간(01~12)
%j	10 진수 형식의 연간 일자(001~366)
%m	10 진수 형식의 월(01~12)
%M	10 진수 형식의 분(00~59)
%P	12 시간제에 사용되는 현지 AM 및 PM 표시기
%S	10 진수 형식의 초(00~59)
%U	일요일을 첫 번째 요일로 하는 10 진수 형식의 연간 주(00~53)
%w	10 진수 형식의 요일(0~6. 일요일이 0)
%W	월요일을 첫 번째 요일로 하는 10 진수 형식의 연간 주(00~53)
%x	현재 로캘에 적절한 날짜 표현
%#x	현재 로캘에 적절한 긴 날짜 표현
%X	현재 로캘에 적절한 시간 표현
%y	세기 부분을 제외한 10 진수 형식의 연도(00~99)
%Y	세기 부분을 포함한 10 진수 형식의 연도
%z, %Z	표준 시간대 이름 또는 약어(알려진 경우)
%%	백분율 기호

참고: 파운드 기호는 형식 코드의 의미를 다음과 같이 수정합니다.

- 형식 코드 **%#c** 는 현재 로캘에 적절한 긴 날짜 및 시간 표현을 지정합니다.
- 형식 코드 **%#x** 는 현재 로캘에 적절한 긴 날짜 표현을 지정합니다.
- 다른 모든 경우 형식 코드에서 백분율 기호 다음에 파운드 기호가 삽입되면 선행 0(있는 경우)이 제거됩니다.
- 파운드 기호는 영어 월 이름과 같은 영문자의 형식을 지정하는 코드에는 아무 영향도 주지 않습니다.

반환 값

DATEToString 함수는 문자열을 반환합니다.

예

```
Return_value=DATEToString(1024804800, '%Y%m%d')  
Return_value='20020223'
```

```
Return_value=DATEToString(1024804800, '%Y%#m%#d')  
Return_value='2002223'
```

DAY 함수 - 월간 일자 반환

DAY 함수는 날짜 및 시간의 숫자 표현을 받아 월간 일자에 해당하는 숫자를 반환합니다.

구문

DAY 함수의 형식은 다음과 같습니다.

```
DAY(date_time)
```

매개 변수

DAY 함수는 다음 매개 변수를 사용합니다.

date_time(숫자)

날짜 및 시간을 1970 년 1 월 1 일 이후 경과된 초 수로 지정합니다.
날짜가 유효하지 않은 경우 이 함수는 -1 을 반환합니다.

반환 값

DAY 함수는 1 에서 31 사이의 숫자를 반환합니다.

예

```
Return_value=DAY(1024804800)  
Return_value=23
```

추가 정보:

[DOW 함수 - 요일 반환](#) (페이지 911)

[DOY 함수 - 연간 일자 반환](#) (페이지 912)

DOW 함수 - 요일 반환

DOW 함수는 날짜 및 시간의 숫자 표현을 받아 요일에 해당하는 숫자를 반환합니다.

구문

DOW 함수의 형식은 다음과 같습니다.

```
DOW(date_time)
```

매개 변수

DOW 함수는 다음 매개 변수를 사용합니다.

date_time(숫자)

날짜 및 시간을 1970 년 1 월 1 일 이후 경과된 초 수로 지정합니다.

날짜가 유효하지 않은 경우 이 함수는 -1 을 반환합니다.

반환 값

DOW 함수는 0(일요일)에서 6(토요일) 사이의 숫자를 반환합니다.

예

```
Return_value=DOW(1024804800)  
Return_value=0
```

DOY 함수 - 연간 일자 반환

DOY 함수는 날짜 및 시간의 숫자 표현을 받아 연간 일자에 해당하는 숫자를 반환합니다.

구문

DOY 함수의 형식은 다음과 같습니다.

`DOY(date_time)`

매개 변수

DOY 함수는 다음 매개 변수를 사용합니다.

`date_time`(숫자)

날짜 및 시간을 1970 년 1 월 1 일 이후 경과된 초 수로 지정합니다.
날짜가 유효하지 않은 경우 이 함수는 -1 을 반환합니다.

반환 값

DOY 함수는 1 에서 366 사이의 숫자를 반환합니다.

예

```
Return_value=DOY(1024804800)  
Return_value=173
```

추가 정보:

[DAY 함수 - 월간 일자 반환](#) (페이지 910)

[DOW 함수 - 요일 반환](#) (페이지 911)

ENUMERATE 함수 - 집합 요소 테스트

ENUMERATE 함수는 붙여넣기를 사용하여 `#virtual_user_attribute` 또는 `@user_class` 매개 변수로 지정된 명명된 식에 지정된 집합의 각 요소를 전달합니다. 명명된 식이 값을 반환하면 해당 요소가 결과 문자열에 포함됩니다.

구문

ENUMERATE 함수의 형식은 다음과 같습니다.

```
ENUMERATE(set, #virtual_user_attribute | @user_class)
```

매개 변수

ENUMERATE 함수는 다음 매개 변수를 사용합니다.

`set`(문자열)

'element1^element2'와 같이 각 요소가 캐럿 문자로 구분된 문자열을 지정합니다. 각 요소는 문자열입니다.

`#virtual_user_attribute`(명명된 식)

사용자 특성을 계산하는 명명된 식을 지정합니다.

`@user_class`(명명된 식)

사용자 디렉터리 또는 그룹의 구성원 자격을 테스트하는 명명된 식을 지정합니다.

반환 값

ENUMERATE 함수는 함수에 필요한 특성 유형에 따라 문자열이나 정수를 반환합니다.

예 1

가상 사용자 특성 #GetCN 을 RDN(String(%0),FALSE)으로 설정

```
ENUMERATE(SM_USERGROUPS, #GetCN)
```

예 2

```
ENUMERATE(SM_USERGROUPS, STRING(RDN(%0, FALSE)))
```

ERROR 함수 - 콘솔 로그에 오류 메시지 기록

ERROR 함수는 SiteMinder 의 콘솔 로그에 지정된 오류 메시지를 기록합니다.

구문

ERROR 함수의 형식은 다음과 같습니다.

```
ERROR(error_message)
```

매개 변수

ERROR 함수는 다음 매개 변수를 사용합니다.

error_message(문자열)

반환 값

ERROR 함수는 빈 문자열을 반환합니다. 부울 컨텍스트에 사용될 경우 ERROR 함수는 TRUE 값을 반환합니다.

설명

권한 있음: 예

예

```
Return_value=ERROR('Invalid Access')
Return_value=""
```

EVALUATE 함수 - 식 평가

EVALUATE 함수는 현재 사용자의 컨텍스트에서 식을 평가하고 결과를 문자열로 반환합니다. 선택적 사용자 경로가 제공된 경우 이 함수는 지정된 사용자의 컨텍스트에서 식을 평가합니다.

구문

EVALUATE 함수의 형식은 다음과 같습니다.

EVALUATE(식)

매개 변수

EVALUATE 함수는 다음 매개 변수를 사용합니다.

expression(문자열)

평가할 식을 지정합니다.

반환 값

EVALUATE 함수는 문자열을 반환합니다.

설명

권한 있음: 예

예

```
Return_value=EVALUATE("sn + ',' + givenname")  
Return_value="Hood, Robin"
```

EXISTS 함수 - 파일 이름 조회

EXISTS 함수는 지정된 파일을 조회하여 파일이 있으면 TRUE 를 반환합니다.
그렇지 않으면 이 함수는 FALSE 를 반환합니다.

구문

EXISTS 함수의 형식은 다음과 같습니다.

```
EXISTS(filename)
```

매개 변수

EXISTS 함수는 파일 이름을 매개 변수로 사용합니다.

filename(문자열)

반환 값

EXISTS 함수는 부울 값을 반환합니다.

설명

권한 있음: 예

예

```
Return_value=EXISTS('SmUtilities.dll')  
Return_value=TRUE
```

추가 정보:

[KEY 함수 - 키 조회](#) (페이지 924)

EXPLODEDN 함수 - LDAP DN 을 집합으로 변환

EXPLODEDN 함수는 LDAP 서버를 호출하지 않고 LDAP DN(고유 이름)을 집합으로 변환합니다.

구문

EXPLODEDN 함수의 형식은 다음과 같습니다.

```
EXPLODED(ldapdn[, remove_attribute_names])
```

매개 변수

EXPLODEDN 함수는 다음 매개 변수를 사용합니다.

ldapdn(문자열)

LDAP DN(고유 이름)을 지정합니다.

remove_attribute_names(부울)

(선택 사항) *remove_attribute_names* 플래그를 지정합니다. 이 플래그가 TRUE 인 경우 이 함수는 LDAP DN(고유 이름)에서 특정 이름을 제거합니다.

반환 값

EXPLODEDN 함수는 'element1^element2'와 같이 각 요소가 캐럿 문자로 구분된 문자열을 반환합니다. 각 요소는 문자열입니다.

설명

LDAP 전용: 예

예

```
Return_value=EXPLODEDN('uid=hawk,o=NDS.com', FALSE)
Return_value='uid=hawk^o=NDS.com'
```

```
Return_value=EXPLODEDN('uid=hawk,o=NDS.com', TRUE)
Return_value='hawk^NDS.com'
```

FILTER 함수 - 집합 요소 테스트

FILTER 함수는 지정된 집합의 각 요소를 지정된 패턴과 비교하고 패턴과 일치하는 요소만 포함된 새 집합을 반환합니다. 선택적 **NOT** 연산자가 포함된 경우 **FILTER** 함수는 패턴과 일치하지 않는 요소만 포함된 새 집합을 반환합니다.

구문

FILTER 함수의 형식은 다음과 같습니다.

FILTER(set, [NOT]pattern)

매개 변수

FILTER 함수는 다음 매개 변수를 사용합니다.

set(문자열)

'element1^element2'와 같이 각 요소가 캐럿 문자로 구분된 문자열을 지정합니다. 각 요소는 문자열입니다.

pattern(문자열)

문자의 패턴을 지정합니다. **pattern**에는 단일 문자, 문자 범위 또는 둘 모두를 포함할 수 있습니다. 문자 범위는 하이픈으로 구분된 두 문자로 나타냅니다. 예를 들어 0-9, a-z 및 A-Z는 유효한 문자 범위입니다. **pattern** 매개 변수에 특별한 의미가 있는 예약된 문자를 포함할 수도 있습니다. 예약된 문자는 다음과 같습니다.

문자	의미
?	임의의 단일 문자와 일치합니다.
*	문자가 하나 있거나 없는 경우를 포함하여 임의의 문자 시퀀스와 일치합니다.
[set]	지정된 집합에 있는 임의의 단일 문자와 일치합니다.
[!set] 또는 [^set]	지정된 집합에 없는 임의의 단일 문자와 일치합니다.
\	*와 같이 예약된 문자를 일반 문자로 처리합니다.

NOT(연산자)

(선택 사항) **NOT** 연산자가 포함된 경우 이 함수는 패턴과 일치하지 않는 요소만 포함된 새 집합을 반환합니다.

반환 값

FILTER 함수는 'element1^element2'와 같이 각 요소가 캐럿 문자로 구분된 문자열을 반환합니다. 각 요소는 문자열입니다.

예

```
Return_value=FILTER('Faith^Earl^Emilie^Fred', 'E*')
```

```
Return_value='Earl^Emilie'
```

```
Return_value=FILTER('Faith^Earl^Emilie^Fred', NOT 'E*')
```

```
Return_value='Faith^Fred'
```

FIND 함수 - 문자열 내 위치 반환

FIND 함수는 원본 문자열에서 지정된 검색 문자열을 찾고 해당 위치를 반환합니다. 검색 문자열을 찾을 수 없는 경우 이 함수는 0 을 반환합니다.

구문

FIND 함수의 형식은 다음과 같습니다.

```
FIND(source_string, search_string[, not_case_sensitive][, n])
```

매개 변수

FIND 함수는 다음 매개 변수를 사용합니다.

source_string(문자열)

search_string(문자열)

not_case_sensitive(부울)

(선택 사항) 대/소문자 구분 여부를 지정합니다. *not_case_sensitive* 플래그가 생략되거나 FALSE 로 설정된 경우 이 함수는 원본 문자열에서 정확히 일치하는 문자열을 검색합니다. *not_case_sensitive* 플래그가 TRUE 로 설정된 경우 FIND 함수는 대/소문자를 무시합니다.

n (숫자)

(선택 사항) 원본 문자열에 포함된 검색 문자열의 인스턴스를 지정합니다. n 이 0 또는 1로 설정되거나 생략된 경우 이 함수는 검색 문자열의 첫 번째 인스턴스를 찾습니다. 그렇지 않은 경우 이 함수는 검색 문자열의 n 번째 인스턴스를 찾습니다. n 이 음수이면 이 함수는 원본 문자열의 끝에서부터 검색을 시작합니다.

반환 값

FIND 함수는 숫자를 반환합니다.

예

```
Return_value=FIND('PhoebePhoebe', 'oe', FALSE, 1)  
Return_value=3
```

```
Return_value=FIND('PhoebePhoebe', 'OE', FALSE, 1)  
Return_value=0
```

```
Return_value=FIND('PhoebePhoebe', 'OE', TRUE, 1)  
Return_value=3
```

```
Return_value=FIND('PhoebePhoebe', 'oe', FALSE, -1)  
Return_value=9
```

```
Return_value=FIND('PhoebePhoebe', 'OE', FALSE, -1)  
Return_value=0
```

```
Return_value=FIND('PhoebePhoebe', 'OE', TRUE, -1)  
Return_value=9
```

```
Return_value=FIND('PhoebePhoebe', 'oe', FALSE, 2)  
Return_value=9
```

```
Return_value=FIND('PhoebePhoebe', 'OE', FALSE, 2)  
Return_value=0
```

```
Return_value=FIND('PhoebePhoebe', 'OE', TRUE, 2)  
Return_value=9
```

GET 함수 - 사용자 디렉터리의 특성 찾기

GET 함수는 사용자 디렉터리에서 지정된 특성을 찾고 특성 값을 반환합니다. 특성 값이 여러 개인 경우 각 값은 캐럿 문자로 구분됩니다. 특성을 찾을 수 없는 경우 이 함수는 빈 문자열을 반환합니다.

구문

GET 함수의 형식은 다음과 같습니다.

```
GET(user_attribute_name | user_attributes_string)
```

매개 변수

GET 함수는 다음 매개 변수 중 하나를 사용합니다.

user_attribute_name(따옴표 없는 문자열)

단일 사용자 특성을 지정합니다.

user_attributes_string(문자열)

각 사용자 특성 이름이 문자로 구분된 문자열을 지정합니다. 이 함수는 이 문자를 사용하여 결과 문자열의 각 특성 값을 구분합니다.

반환 값

GET 함수는 문자열을 반환합니다.

설명

권한 있음: 예

LDAP 전용: 예

예

```
Return_value=GET('sn,givenname')
```

```
Return_value='Finch,Robin'
```

HEX 함수 - 16 진수로 변환

HEX 함수는 10 진수를 16 진수로 변환한 다음 문자열로 반환합니다.

구문

HEX 함수의 형식은 다음과 같습니다.

HEX(decimal_number)

매개 변수

HEX 함수는 다음 매개 변수를 사용합니다.

decimal_number(숫자)

반환 값

HEX 함수는 문자열을 반환합니다.

예

```
Return_value=HEX(16)  
Return_value='10'
```

HOUR 함수 - 시간으로 변환

HOUR 함수는 지정된 날짜 및 시간을 1 에서 12 사이의 시간으로 변환합니다.

구문

HOUR 함수의 형식은 다음과 같습니다.

HOUR(date_time)

매개 변수

HOUR 함수는 다음 매개 변수를 사용합니다.

date_time(숫자)

날짜 및 시간을 1970 년 1 월 1 일 이후 경과된 초 수로 지정합니다.
date_time 이 올바른 날짜 및 시간 표현이 아닌 경우 이 함수는 -1 을 반환합니다.

반환 값

HOUR 함수는 1 에서 12 사이의 숫자를 반환합니다.

추가 정보:

[HOUR24 함수 - 시간으로 변환](#) (페이지 923)

HOUR24 함수 - 시간으로 변환

HOUR24 함수는 지정된 날짜 및 시간을 0 에서 23 사이의 시간으로 변환합니다.

구문

HOUR24 함수의 형식은 다음과 같습니다.

HOUR24(*date_time*)

매개 변수

HOUR24 함수는 다음 매개 변수를 사용합니다.

date_time(숫자)

날짜 및 시간을 1970 년 1 월 1 일 이후 경과된 초 수로 지정합니다.
date_time 이 올바른 날짜 및 시간 표현이 아닌 경우 이 함수는 -1 을 반환합니다.

반환 값

HOUR24 함수는 0 에서 23 사이의 숫자를 반환합니다.

추가 정보:

[HOUR 함수 - 시간으로 변환](#) (페이지 922)

INFO 함수 - 콘솔 로그에 정보 메시지 기록

INFO 함수는 문자열 인수를 SiteMinder 콘솔 로그에 정보 메시지로 기록합니다.

구문

INFO 함수의 형식은 다음과 같습니다.

```
INFO(source_string)
```

매개 변수

INFO 함수는 다음 매개 변수를 사용합니다.

source_string(문자열)

반환 값

INFO 함수는 부울(항상 TRUE)을 반환합니다.

예

```
Return_value=INFO("86% Complete")  
Return_value=TRUE
```

KEY 함수 - 키 조회

KEY 함수는 지정된 파일의 지정된 응용 프로그램 섹션에서 지정된 키 이름을 조회하고 키 값을 반환합니다. 키, 응용 프로그램 또는 파일을 찾을 수 없는 경우 KEY 함수는 빈 문자열을 반환합니다.

구문

KEY 함수의 형식은 다음과 같습니다.

```
KEY(filename, [application_name, ]key_name)
```


매개 변수

KEY 함수는 다음 매개 변수를 사용합니다.

filename(문자열)

파일을 지정합니다. 지정된 파일에서 주석 행은 세미콜론, 파운드 기호 또는 두 개의 슬래시로 시작합니다. 주석 줄, 빈 줄, 선행 및 후행 공백은 무시됩니다.

application_name(문자열)

(선택 사항) 응용 프로그램 섹션의 이름을 지정합니다. 지정된 파일에서 응용 프로그램 이름은 대괄호로 묶여 있으며 응용 프로그램 섹션의 시작 부분을 지정합니다(예: *[application_name]*). 응용 프로그램 이름은 대/소문자를 구분합니다.

key_name(문자열)

키의 이름을 지정합니다. 지정된 파일에서 키 이름 및 값은 꺾쇠 괄호로 묶이고 등호(=)로 연결되어 있으며 한 줄에 한 쌍씩 표시되어 있습니다(예: *<key_name>=<key_value>*). 키 이름은 대/소문자를 구분합니다.

반환 값

KEY 함수는 문자열을 반환합니다.

설명

권한 있음: 예

LDAP 전용: 아니요

예

```
Return_value=KEY('application.dat', 'login user')
Return_value='key_value'
```

추가 정보:

[EXISTS 함수 - 파일 이름 조회](#) (페이지 916)

LCASE 함수 - 소문자로 변환

LCASE 함수는 지정된 문자열의 대문자를 소문자로 변환합니다.

구문

LCASE 함수의 형식은 다음과 같습니다.

LCASE(*specified_string*)

매개 변수

LCASE 함수는 다음 매개 변수를 사용합니다.

specified_string(문자열)

반환 값

LCASE 함수는 문자열을 반환합니다.

예

```
Return_value=LCASE('BARRED OWL')  
Return_value='barred owl'
```

LEFT 함수 - 문자열의 일부 반환

LEFT 함수는 문자열에서 지정된 수의 문자를 반환합니다. 문자열이 지정된 문자 수보다 짧으면 전체 문자열이 반환됩니다.

구문

LEFT 함수의 형식은 다음과 같습니다.

LEFT(*source_string*, *length*)

매개 변수

LEFT 함수는 다음 매개 변수를 사용합니다.

source_string(문자열)

length(숫자)

반환 값

LEFT 함수는 문자열을 반환합니다.

예

```
Return_value=LEFT('JuanJuan', 2)  
Return_value='Ju'
```

```
Return_value=LEFT('JuanJuan', 10)  
Return_value=('JuanJuan')
```

```
Return_value=LEFT('JuanJuan', 0)  
Return_value=""
```

LEN 함수 - 문자열 길이 반환

LEN 함수는 문자열의 길이를 반환합니다.

구문

LEN 함수의 형식은 다음과 같습니다.

```
LEN(source_string)
```

매개 변수

LEN 함수는 다음 매개 변수를 사용합니다.

source_string(문자열)

반환 값

이 함수는 숫자를 반환합니다.

예

```
Return_value=LEN("JuanJuan")  
Return_value=8
```

LOG 함수 - 파일에 문자열 기록

LOG 함수는 문자열 인수를 지정된 파일에 기록합니다.

구문

LOG 함수의 형식은 다음과 같습니다.

```
LOG(filename, source_string)
```

매개 변수

LOG 함수는 다음 매개 변수를 사용합니다.

filename(문자열)

source_string(문자열)

반환 값

LOG 함수는 부울(항상 TRUE)을 반환합니다.

설명

권한 있음: 예

예

```
Return_value=LOG("auditlog.txt", "Accessing Realm XXX")  
Return_value=TRUE
```

LOOP 함수 - 루프에서 가상 특성 호출

LOOP 함수는 루프에서 지정된 값으로 시작하고 끝나는 가능한 각 숫자에 대해 가상 특성을 한 번씩 호출합니다. **step** 값이 지정된 경우 숫자가 **step** 값만큼씩 증가합니다. 가상 특성이 비어 있지 않은 값을 반환하면 해당 값이 결과 집합에 포함됩니다.

구문

LOOP 함수의 형식은 다음과 같습니다.

```
LOOP(#virtual_user_attribute, start_value, end_value, [step,] )
```

매개 변수

LOOP 함수는 다음 매개 변수를 사용합니다.

`#virtual_user_attribute`(명명된 식)

정의된 가상 특성의 이름입니다. 가상 특성은 %0 에 대한 참조를 사용하여 현재 루프 카운터에 액세스할 수 있습니다.

`start_value`(숫자)

`end_value`(숫자)

`step`(숫자)

(선택 사항) 기본값은 1 입니다. 음수 값이 허용됩니다.

반환 값

LOOP 함수는 집합을 반환합니다.

예

이 예제에서는 가상 사용자 특성이 `#Padset := LPAD(%0, 2)`라고 가정합니다.

```
Return_set=LOOP(#Padset ,1, 5)
Return_set="001^002^003^004^005"
Return_set=LOOP(#Padset ,1, 5, 2)
Return_set="001^003^005"
Return_set=LOOP(#Padset ,5, 1, -1)
Return_set="005^004^003^002^001"
```

LPAD 함수 - 왼쪽에 원본 문자열 채우기

LPAD 함수는 결과 문자열이 지정된 길이가 될 때까지 지정된 padding 의 첫 번째 문자로 원본 문자열의 왼쪽을 채웁니다.

구문

LPAD 함수의 형식은 다음과 같습니다.

`LPAD(source_string, length[, padding])`

매개 변수

LPAD 함수는 다음 매개 변수를 사용합니다.

source_string(문자열)

이 매개 변수는 숫자일 수도 있으며 이 경우 자동으로 문자열로 변환됩니다.

length(숫자)

최종 문자열의 문자 수입니다.

padding(문자열)

(선택 사항) *padding* 의 길이가 1 자를 초과할 경우 첫 번째 문자만 사용됩니다. *padding* 길이가 0 이면 채우기가 수행되지 않습니다. 원본이 문자열이고 *padding* 이 생략된 경우에는 채우기에 공백이 사용됩니다. 원본이 숫자이고 *padding* 이 생략된 경우에는 채우기에 0 이 사용됩니다.

반환 값

LPAD 함수는 문자열을 반환합니다.

예

```
Result_value=LPAD('Juan', 5)
Result_value=' Juan'
```

```
Result_value=LPAD('Juan', 5, 'X')
Result_value='XJuan'
```

```
Result_value=LPAD('Juan', 6, 'XY')
Result_value='XXJuan'
```

```
Result_value=LPAD(5, 2)
Result_value='05'
```

```
Result_value=LPAD(5, 2, ' ')
Result_value=' 5'
```

LTRIM 함수 - 문자열의 선행 공백 제거

LTRIM 함수는 선행 공백이 제거된 *source_string* 을 나타내는 문자열을 반환합니다.

구문

LTRIM 함수의 형식은 다음과 같습니다.

LTRIM(*source_string*)

매개 변수

LTRIM 함수는 다음 매개 변수를 사용합니다.

source_string(문자열)

반환 값

LTRIM 함수는 문자열을 반환합니다.

예

```
Return_value=LTRIM(' Juan ')  
Return_value='Juan '
```

추가 정보:

[RTRIM 함수 - 문자열의 후행 공백 제거](#) (페이지 950)

MAX 함수 - 두 값 중 더 큰 값 확인

MAX 함수는 두 숫자 인수 중 더 큰 인수를 반환합니다.

구문

MAX 함수의 형식은 다음과 같습니다.

MAX(*int_1*, *int_2*)

매개 변수

MAX 함수는 다음 매개 변수를 사용합니다.

int_1(숫자)

int_2(숫자)

반환 값

MAX 함수는 숫자를 반환합니다.

예

Return_value=MAX(-2, 4)

Return_value=4

추가 정보:

[MIN 함수 - 두 숫자 중 더 작은 숫자 확인](#) (페이지 935)

MAYBE 함수 - 미확정 결과 보고

조건을 테스트하고 테스트에 필요한 정보가 누락되거나 불완전한 경우 MAYBE 함수를 호출하는 식을 작성할 수 있습니다. MAYBE 가 사용된 경우 식 계산기는 필요한 정보 없이 식을 확인하려고 시도합니다. 이는 MAYBE 가 복합 식의 일부인 경우에만 가능합니다.

예를 들어 연산자가 AND 이고 피연산자 하나가 FALSE 인 경우 계산기는 연산의 결과가 FALSE 인 것으로 결정할 수 있습니다. 피연산자 하나가 TRUE 이고 다른 피연산자가 정의되지 않았거나, 두 피연산자가 모두 정의되지 않은 경우 계산기는 연산의 결과를 결정할 수 없습니다. 두 피연산자가 모두 TRUE 인 경우 AND 연산의 결과는 TRUE 입니다.

AND 연산자	True	False	정의되지 않음
True	True	False	미확정
False	False	False	False
정의되지 않음	미확정	False	미확정

마찬가지로 연산자가 OR 이고 피연산자 하나가 TRUE 인 경우 계산기는 연산의 결과가 TRUE 인 것으로 결정할 수 있습니다. 피연산자 하나가 FALSE 이고 다른 피연산자가 정의되지 않았거나, 두 피연산자가 모두 정의되지 않은 경우 계산기는 연산의 결과를 결정할 수 없습니다. 두 피연산자가 모두 FALSE 인 경우 OR 연산의 결과는 FALSE 입니다.

OR 연산자	True	False	정의되지 않음
True	True	True	True
False	True	False	미확정
정의되지 않음	True	미확정	미확정

식을 확인할 수 없는 경우 계산기가 처리를 중지하며 컨텍스트에 따라 콘솔 로그나 보고서에 지정된 메시지가 출력됩니다. MAYBE 는 일반적으로 정책 또는 보고서 생성 컨텍스트에서 역할 평가 중에 호출됩니다.

일반적으로 조건은 가상 사용자 특성(# 기호로 지정), 사용자 클래스(@ 기호로 지정), 컨텍스트 변수(% 기호로 지정) 또는 사용자 특성의 값, IP 주소 또는 시간에 따라 달라집니다.

참고: LDAP 사용자 디렉터리의 경우 계산기는 사용자 특성이 정의되었는지 여부를 확인할 수 없습니다.

구문

MAYBE 함수의 형식은 다음과 같습니다.

MAYBE(message)

매개 변수

MAYBE 함수는 다음 매개 변수를 사용합니다.

message(문자열)

식의 조건을 평가하는 데 필요한 누락된 정보를 지정합니다.

반환 값

MAYBE 함수는 결과를 반환하지 않습니다.

예

VEXIST(%ClientIP) ? #CheckIP : MAYBE('Client IP address is not defined.')
콘솔 로그 또는 보고서에 출력되는 메시지: 'Client IP address is not defined.'

MID 함수 - 문자열의 일부 반환

MID 함수는 *source_string* 중 *start* 위치(1 부터 시작하는 번호)부터 지정된 *length* 까지의 문자를 반환합니다. *length* 가 지정되지 않은 경우 *start* 위치 다음부터 나머지 *source_string* 이 반환됩니다.

구문

MID 함수의 형식은 다음과 같습니다.

MID(*source_string*, *start*[,*length*])

매개 변수

MID 함수는 다음 매개 변수를 사용합니다.

source_string(문자열)

start(숫자)

length(숫자)(선택 사항)

반환 값

MID 함수는 문자열을 반환합니다.

예

```
Return_value=MID('JuanJuan', 2, 3)  
Return_value='uan'
```

```
Return_value=MID('JuanJuan', 2)  
Return_value='uanJuan'
```

MIN 함수 - 두 숫자 중 더 작은 숫자 확인

MIN 함수는 두 숫자 인수 중 더 작은 인수를 반환합니다.

구문

MIN 함수의 형식은 다음과 같습니다.

```
MIN(int_1, int_2)
```

매개 변수

MIN 함수는 다음 매개 변수를 사용합니다.

int_1(숫자)

int_2(숫자)

반환 값

MIN 함수는 숫자를 반환합니다.

예

```
Return_value=MIN(-2, 4)  
Return_value=-2
```

추가 정보:

[MAX 함수 - 두 값 중 더 큰 값 확인](#) (페이지 931)

MINUTE 함수 - 날짜의 분 구성 요소 반환

MINUTE 함수는 1970 년 1 월 1 일 이후 경과된 초 수로 표현된 지정된 *date_time* 의 분 구성 요소를 나타내는 숫자를 반환합니다.

구문

MINUTE 함수의 형식은 다음과 같습니다.

MINUTE(*date_time*)

매개 변수

MINUTE 함수는 다음 매개 변수를 사용합니다.

date_time(숫자)

초 수로 표현된 날짜입니다.

반환 값

MINUTE 함수는 0 에서 59 사이의 숫자를 반환합니다. *date_time* 이 유효하지 않은 경우 MINUTE 는 -1 을 반환합니다.

MOD 함수 - 나누기 나머지 반환

MOD 함수는 첫 번째 숫자를 두 번째 숫자로 나눈 나머지를 반환합니다. 두 번째 숫자가 0 이면 0 이 반환됩니다.

구문

MOD 함수의 형식은 다음과 같습니다.

MOD(*int_1*, *int_2*)

매개 변수

MOD 함수는 다음 매개 변수를 사용합니다.

int_1(숫자)

나누기 연산의 피제수입니다.

int_2(숫자)

나누기 연산의 제수입니다.

반환 값

MOD 함수는 숫자를 반환합니다.

예

```
Return_value=MOD(3, 2)
```

```
Return_value=1
```

```
Return_value=MOD(6, 3)
```

```
Return_value =0
```

MONTH 함수 - 날짜의 월 구성 요소 반환

MONTH 함수는 1970 년 1 월 1 일 이후 경과된 초 수로 표현된 지정된 *date_time* 의 월 구성 요소를 나타내는 숫자를 반환합니다.

구문

MONTH 함수의 형식은 다음과 같습니다.

```
MONTH(date_time)
```

매개 변수

MONTH 함수는 다음 매개 변수를 사용합니다.

date_time(숫자)

초 수로 표현된 날짜입니다.

반환 값

MONTH 함수는 1 에서 12 사이의 숫자를 반환합니다. *date_number* 가 유효하지 않은 경우 MONTH 는 -1 을 반환합니다.

NOTBITS 함수 - bitwise NOT 수행

NOTBITS 함수는 숫자에 대해 bitwise NOT 연산을 수행합니다.

구문

NOTBITS 함수의 형식은 다음과 같습니다.

NOTBITS(*number*)

매개 변수

NOTBITS 함수는 다음 매개 변수를 사용합니다.

number(숫자)

반환 값

NOTBITS 함수는 숫자를 반환합니다.

예

```
Return_value=NOTBITS(0)  
Return_value=-1
```

```
Return_value=NOTBITS(1)  
Return_value=-2
```

NOW 함수 - 현재 시간을 초 단위로 반환

NOW 함수는 1970 년 1 월 1 일 이후부터 함수 호출 시점까지 경과된 초 수를 나타내는 숫자 값을 반환합니다. 시간은 현재 서버 시스템의 현지 시간입니다.

이 값은 특정 식에서 연산의 시작 부분에 계산됩니다. 따라서 동일한 식 내에서 NOW 함수를 여러 번 참조하더라도 결과는 항상 동일합니다.

구문

NOW 함수의 형식은 다음과 같습니다.

NOW()

매개 변수

NOW 함수는 매개 변수를 사용하지 않습니다.

반환 값

NOW 함수는 숫자를 반환합니다.

예

```
Return_value=NOW()  
Return_value=1024804800
```

추가 정보:

[NOWGMT 함수 - 현재 시간을 초 단위로 반환](#) (페이지 939)

NOWGMT 함수 - 현재 시간을 초 단위로 반환

NOWGMT 함수는 1970 년 1 월 1 일 이후부터 함수 호출 시점까지 경과된 초 수를 나타내는 숫자 값을 반환합니다. 이 시간은 그리니치(ZULU) 표준 시간대의 시간입니다.

이 값은 특정 식에서 연산의 시작 부분에 계산됩니다. 따라서 동일한 식 내에서 NOWGMT 함수를 여러 번 참조하더라도 결과는 항상 동일합니다.

구문

NOWGMT 함수의 형식은 다음과 같습니다.

```
NOWGMT ( )
```

매개 변수

NOWGMT 함수는 매개 변수를 사용하지 않습니다.

반환 값

NOWGMT 함수는 숫자를 반환합니다.

추가 정보:

[NOW 함수 - 현재 시간을 초 단위로 반환](#) (페이지 938)

NUMBER 함수 - 숫자 값으로 변환

NUMBER 함수는 인수를 숫자 값으로 변환합니다. 문자열은 숫자가 아닌 첫 번째 문자까지 변환됩니다. 부울의 경우 값이 TRUE 이면 1 로 변환되고, 그렇지 않으면 0 으로 변환됩니다.

구문

NUMBER 함수의 형식은 다음과 같습니다.

```
NUMBER(source_string | bool_val)
```

매개 변수

NUMBER 함수는 다음 매개 변수 중 하나를 사용합니다.

source_string(문자열)

bool_val(부울)

반환 값

NUMBER 함수는 숫자를 반환합니다.

예

```
Return_value=NUMBER('juan')
```

```
Return_value=0
```

```
Return_value=NUMBER('45juan')
```

```
Return_value=45
```

```
Return_value=NUMBER(TRUE)
```

```
Return_value=1
```


ORBITS 함수 - bitwise OR 연산 수행

ORBITS 함수는 두 인수에 대해 bitwise OR 연산을 수행합니다.

구문

ORBITS 함수의 형식은 다음과 같습니다.

```
ORBITS(int_1, int_2)
```

매개 변수

ORBITS 함수는 다음 매개 변수를 사용합니다.

int_1(숫자)

int_2(숫자)

반환 값

ORBITS 함수는 숫자를 반환합니다.

예

```
Result_value=ORBITS(6, 1)
```

```
Result_value=7
```

```
Result_value=ORBITS(7, 8)
```

```
Result_value=15
```

PARENTDN 함수 - LDAP 트리에서 부모 검색

PARENTDN 함수는 LDAP 디렉터리 정보 트리에서 지정된 DN(고유 이름)의 바로 위 수준을 반환합니다. 지정된 DN 이 유효하지 않거나 이미 트리의 맨 위에 있는 경우에는 빈 문자열이 반환됩니다.

구문

PARENTDN 함수의 형식은 다음과 같습니다.

```
PARENTDN(source_string)
```

매개 변수

PARENTDN 함수는 다음 매개 변수를 사용합니다.

source_string(문자열)

LDAP DN(고유 이름)입니다.

반환 값

PARENTDN 함수는 문자열을 반환합니다.

설명

LDAP 전용: 예

예

```
Return_value=PARENTDN("uid=juan,o=NDS.com")
```

```
Return_value="o=NDS.com"
```

```
Return_value=PARENTDN("o=NDS.com")
```

```
Return_value=""
```

PCASE 함수 - 문자열을 고유 명사 스타일 대/소문자로 변환

PCASE 함수는 지정된 문자열을 고유 명사 스타일 대/소문자(첫 자가 대문자)로 변환합니다.

구문

PCASE 함수의 형식은 다음과 같습니다.

```
PCASE(source_string)
```

매개 변수

PCASE 함수는 다음 매개 변수를 사용합니다.

source_string(문자열)

반환 값

PCASE 함수는 문자열을 반환합니다.

예

```
Return_value=PCASE("framingham, mass")
Return_value="Framingham, Mass")
```

QS 함수 - 쿼리 문자열에서 항목 검색

QS 함수는 식이 평가될 때 사용자가 액세스하는 리소스와 연결된 쿼리 문자열에서 항목을 검색합니다.

이 함수에 인수가 제공되지 않을 경우 전체 쿼리 문자열만 반환됩니다. 즉, 쿼리 문자열이 변경되지 않고 그대로 반환됩니다.

문자열 인수가 빈 문자열("")로 제공된 경우에는 명명되지 않은 쿼리 문자열의 모든 인수가 반환됩니다. 값이 여러 개이면 집합으로 반환됩니다.

문자열 인수가 비어 있지 않은 문자열로 제공된 경우에는 쿼리 문자열 중 일치 이름으로 명명된 모든 인수가 반환됩니다. 대/소문자 구분 여부는 선택적 부울 플래그에 의해 제어됩니다. 값이 여러 개이면 집합으로 반환됩니다.

구문

QS 함수의 형식은 다음과 같습니다.

```
QS([input_string],[ not_case_sensitive])
```

매개 변수

QS 함수는 다음과 같은 선택적 매개 변수를 사용합니다.

input_string(문자열)

(선택 사항) 쿼리 문자열의 인수 이름입니다.

not_case_sensitive(부울)

(선택 사항) *not_case_sensitive* 플래그가 FALSE 로 설정되거나 생략된 경우 이 함수는 쿼리 문자열에서 정확히 일치하는 항목을 검색합니다.

not_case_sensitive 플래그가 TRUE 로 설정된 경우 이 함수는 대/소문자를 무시합니다.

반환 값

QS 함수는 문자열을 반환합니다.

예

http://myserver.com/index.jsp?Test=A&X&TEST=D&c&Dbg 라는 리소스가 있다고 가정합니다.

```
Return_value=QS()
```

```
Return_value='Test=A&X&TEST=D&c&Dbg'
```

```
Return_value=QS("")
```

```
Return_value='X^c'
```

```
Return_value=QS("Test")
```

```
Return_value='A^D'
```

```
Return_value=QS("Test", false)
```

```
Return_value='A'
```

```
"Dbg" IN QS("")
```

```
Return_value=TRUE
```

추가 정보:

[URL 함수 - URL 문자열의 구성 요소 반환](#) (페이지 958)

RDN 함수 - LDAP DN 의 첫 번째 구성 요소 검색

RDN 함수는 지정된 LDAP DN(고유 이름)의 첫 번째 구성 요소를 반환합니다. 선택적 부울 인수가 TRUE(기본값)인 경우 특성 이름이 제거되고 값만 반환됩니다.

지정된 DN 이 유효하지 않으면 빈 문자열이 반환됩니다. 이 함수는 LDAP 서버를 호출하지 않습니다.

구문

RDN 함수의 형식은 다음과 같습니다.

```
RDN(DN_string[, remove_name])
```

매개 변수

RDN 함수는 다음 매개 변수를 사용합니다.

DN_string(문자열)

LDAP 고유 이름

remove_name

(선택 사항) TRUE(기본값)로 설정된 경우 반환되는 문자열에서 특성 이름이 제거됩니다. FALSE 로 설정된 경우 반환되는 문자열에 특성이 포함됩니다.

반환 값

RDN 함수는 문자열을 반환합니다.

설명

LDAP 전용: 예

예

```
Return_value=RDN("uid=juan,o=NDS.com")
Return_value="juan"

Return_value=RDN("uid=juan,o=NDS.com", TRUE)
Return_value="juan"

Return_value=RDN("uid=juan,o=NDS.com", FALSE)
Return_value="uid=juan"
```

RELATIONDN 함수 - 두 개의 고유 이름 비교

RELATIONDN 함수는 지정된 두 LDAP DN(고유 이름)을 비교하고 두 DN 간의 관계를 나타내는 문자열을 반환합니다.

두 DN 중 하나가 유효하지 않거나 두 DN 이 전혀 관련이 없으면 빈 문자열이 반환됩니다.

두 DN 이 관련되어 있으면 디렉터리 정보 트리에서의 수준 차이가 문자열로 반환됩니다. 첫 번째 DN 이 두 번째 DN 의 상위 DN 이면 양수가 반환되고, 첫 번째 DN 이 두 번째 DN 의 하위 DN 이면 음수가 반환됩니다. 두 DN 이 같거나 형제이면 수준 차이가 없음을 나타내는 0 이 반환됩니다.

참고: 이 함수는 LDAP 서버 함수를 호출하지 않습니다.

구문

RELATIONDN 함수의 형식은 다음과 같습니다.

```
RELATIONDN(dn_1, dn_2)
```

매개 변수

RELATIONDN 함수는 다음 매개 변수를 사용합니다.

dn_1(문자열)

dn_2(문자열)

반환 값

RELATIONDN 함수는 문자열을 반환합니다.

설명

LDAP 전용: 예

예

```
Return_value=RELATIONDN("uid=eric,o=NDS.com", "o=NDS.com")
```

```
Return_value="-1"
```

```
Return_value=RELATIONDN("o=NDS.com", "uid=eric,o=NDS.com")
```

```
Return_value="1"
```

```
Return_value=RELATIONDN("uid=dave,o=NDS.com", "uid=eric,o=NDS.com")
```

```
Return_value="0"
```

```
Return_value=RELATIONDN("uid=dave,o=XYZ.com", "uid=eric,o=NDS.com")
```

```
Return_value=""
```

RIGHT 함수 - 문자열에서 문자 검색

RIGHT 함수는 문자열의 끝에서부터 지정된 개수의 문자를 반환합니다.
문자열이 지정된 개수보다 짧으면 전체 문자열이 반환됩니다.

구문

RIGHT 함수의 형식은 다음과 같습니다.

```
RIGHT(source_string, length)
```

매개 변수

RIGHT 함수는 다음 매개 변수를 사용합니다.

source_string(문자열)

length(숫자)

문자열의 끝에서부터 추출할 문자 수입니다.

반환 값

RIGHT 함수는 문자열을 반환합니다.

예

```
Return_value=RIGHT('JuanJuan', 2)
Return_value='an'

Return_value=RIGHT('JuanJuan', 10)
Return_value='JuanJuan'

Return_value=RIGHT('JuanJuan', 0)
Return_value=''
```

RPAD 함수 - 오른쪽에 문자열 채우기

RPAD 함수는 원본 문자열이 지정된 길이가 될 때까지 지정된 **padding** 의 첫 번째 문자를 문자열의 끝에 추가합니다.

padding 의 길이가 1 자를 초과할 경우 첫 번째 문자만 사용됩니다. **padding** 길이가 0 이면 문자가 채워지지 않습니다.

원본이 문자열이고 **padding** 이 지정되지 않은 경우에는 채우기에 공백이 사용됩니다. 원본이 숫자이고 **padding** 이 지정되지 않은 경우 채우기에 0 이 사용됩니다.

구문

RPAD 함수의 형식은 다음과 같습니다.

```
RPAD(source_string|number, length[, padding])
```

매개 변수

RPAD 함수는 다음 매개 변수를 사용합니다.

source_string(문자열)

이 매개 변수는 숫자일 수도 있으며 이 경우 문자열로 변환됩니다.

length(숫자)

padding(문자열)

(선택 사항)

반환 값

RPAD 함수는 문자열을 반환합니다.

예

```
Return_value=RPAD('Juan', 5)
Return_value='Juan '
```

```
Return_value=RPAD('Juan', 5, 'X')
Return_value='JuanX'
```

```
Return_value=RPAD('Juan', 6, 'XY')
Return_value='JuanXX'
```

```
Return_value=RPAD(5, 2)
Return_value='50'
```

```
Return_value=RPAD(5, 2, ' ')
Return_value='5 '
```

RPT 함수 - 문자열 반복

RPT 함수는 원본 문자열을 지정된 횟수만큼 반복한 문자열을 반환합니다.

구문

RPT 함수의 형식은 다음과 같습니다.

```
RPT(source_string|number, repeat_count)
```

매개 변수

RPT 함수는 다음 매개 변수를 사용합니다.

source_string(문자열)

이 매개 변수는 숫자일 수도 있으며 이 경우 단일 문자로 변환됩니다.

repeat_count(문자열)

반환 값

RPT 함수는 문자열을 반환합니다.

예

```
Return_value=RPT('Juan', 3)
Return_value='JuanJuanJuan')

Return_value=RPT('*', 10)
Return_value="*****")
```

RTRIM 함수 - 문자열의 후행 공백 제거

RTRIM 함수는 원본 문자열에서 후행 공백을 제거하고 그 결과를 반환합니다.

구문

RTRIM 함수의 형식은 다음과 같습니다.

```
RTRIM(source_string)
```

매개 변수

RTRIM 함수는 다음 매개 변수를 사용합니다.

source_string(문자열)

반환 값

RTRIM 함수는 문자열을 반환합니다.

예

```
Return_value=RTRIM(' JuanJuan ')
Return_value=' JuanJuan'
```

추가 정보:

[LTRIM 함수 - 문자열의 선행 공백 제거](#) (페이지 931)

SECOND 함수 - 날짜의 초 수 반환

SECOND 함수는 1970 년 1 월 1 일 이후 경과된 초 수로 표현된 날짜의 초 구성 요소를 나타내는 값을 반환합니다.

구문

SECOND 함수의 형식은 다음과 같습니다.

SECOND(date_time)

매개 변수

SECOND 함수는 다음 매개 변수를 사용합니다.

date_time(숫자)

초 수입니다.

반환 값

SECOND 함수는 0 에서 59 사이의 숫자를 반환합니다.

추가 정보:

[MINUTE 함수 - 날짜의 분 구성 요소 반환](#) (페이지 936)

SET 함수 - 특성 값 설정

SET 함수는 지정된 특성에 지정된 값을 할당합니다. 다중값 특성의 경우 여러 값이 집합으로 지정됩니다. 이 함수는 SiteMinder 가 지원하는 모든 사용자 디렉터리에 사용할 수 있습니다.

SiteMinder 가 수정에 성공할 경우 SET 함수는 TRUE 를 반환합니다.

특성이 SiteMinder 에 표시되지 않는 경우 이 함수는 실패합니다. 특성은 보안(사용자 디렉터리의 보안)을 위해 표시되지 않을 수도 있고, ODBC 디렉터리의 경우 해당 특성이 구성된 쿼리에 없거나 SiteMinder 쿼리 체계의 "Set Properties"(속성 설정) 설정에 나열되지 않은 특성일 경우에도 표시되지 않을 수 있습니다.

구문

SET 함수의 형식은 다음과 같습니다.

SET(attr_name, value)

매개 변수

SET 함수는 다음 매개 변수를 사용합니다.

attr_name(문자열)

value(문자열)

하나 이상의 값을 지정합니다. 값이 여러 개인 경우 각 값은 캐럿 문자로 구분됩니다.

반환 값

SET 함수는 부울을 반환합니다.

설명

권한 있음: 예

예

Return_value=SET("Retries", STRING(NUMBER(Retries) + 1))

추가 정보:

[GET 함수 - 사용자 디렉터리의 특성 찾기](#) (페이지 921)

SIGN 함수 - 숫자의 부호 반환

SIGN 함수는 숫자를 매개 변수로 사용합니다. 숫자가 음수이면 -1 을 반환하고, 숫자가 0 이면 0 을 반환하며, 숫자가 양수이면 +1 을 반환합니다.

구문

SIGN 함수의 형식은 다음과 같습니다.

SIGN(number)

매개 변수

SIGN 함수는 다음 매개 변수를 사용합니다.

number(숫자)

반환 값

SIGN 함수는 숫자(-1, 0 또는 +1)를 반환합니다.

예

```
Return_value=SIGN(-40)
Return_value=-1
```

```
Return_value=SIGN(0)
Return_value=0
```

```
Return_value=SIGN(999)
Return_value=1
```

SORT 함수 - 집합 정렬

SORT 함수는 지정된 집합을 정렬합니다. 대/소문자 구분 여부는 선택적 부울 매개 변수로 지정됩니다. 중복 항목은 결과 집합에서 제거됩니다.

구문

SORT 함수의 형식은 다음과 같습니다.

```
SORT(source_set[, not_case_sensitive])
```

매개 변수

SORT 함수는 다음 매개 변수를 사용합니다.

source_set(문자열)

정렬할 집합입니다.

not_case_sensitive(부울)

(선택 사항) 이 매개 변수가 생략되거나 FALSE 로 설정된 경우 정렬 시 대/소문자까지 같은 항목만 동일한 것으로 처리됩니다. 이 매개 변수가 TRUE 로 설정된 경우에는 정렬 시 대/소문자가 무시됩니다.

반환 값

SORT 함수는 집합을 반환합니다.

예

```
Return_value= SORT("Eric^Bart^Chuck^BART^Chuck")
Return_value="BART^Bart^Chuck^Eric"

Return_value= SORT("Eric^Bart^Chuck^BART^Chuck", FALSE)
Return_value="BART^Bart^Chuck^Eric"

Return_value= SORT("Eric^Bart^Chuck^BART^Chuck", TRUE)
Return_value="Bart^Chuck^Eric"
```

SPACE 함수 - 공백 문자열 반환

SPACE 함수는 지정된 개수의 공백으로 구성된 문자열을 반환합니다.

구문

SPACE 함수의 형식은 다음과 같습니다.

```
SPACE(repeat_count)
```

매개 변수

SPACE 함수는 다음 매개 변수를 사용합니다.

repeat_count(숫자)

문자열에 포함할 공백 수입니다.

반환 값

SPACE 함수는 문자열을 반환합니다.

예

```
Return_value=SPACE(3) Return_value='   '

Return_value=SPACE(10) Return_value="          "
```

STRING 함수 - 문자열로 변환

STRING 함수는 숫자 또는 부울을 문자열 값으로 변환합니다.

구문

STRING 함수의 형식은 다음과 같습니다.

```
STRING(num_value|bool_value)
```

매개 변수

STRING 함수는 다음 매개 변수 중 하나를 사용합니다.

num_value(숫자)

bool_value(부울)

반환 값

STRING 함수는 문자열을 반환합니다.

예

```
Return_value=STRING(TRUEVAL)
```

```
Return_value="TRUE"
```

```
Return_value=STRING(123)
```

```
Return_value='123'
```

THROW 함수 - 처리 중지 및 사용자 지정 오류 보고

사용자 지정 오류 메시지를 매개 변수로 전달하여 오류가 발생하는지 테스트하고 오류가 발생한 경우 **THROW** 를 호출하는 식을 작성할 수 있습니다. **THROW** 가 사용된 경우 식 계산기는 식 처리를 중지하고 콘솔 로그에 사용자 지정 오류 메시지를 출력합니다.

구문

THROW 함수의 형식은 다음과 같습니다.

```
THROW(error_message)
```

매개 변수

THROW 함수는 다음 매개 변수를 사용합니다.

error_message(문자열)

콘솔 로그에 출력되는 사용자 지정 오류 메시지를 지정합니다.

반환 값

THROW 함수는 결과를 반환하지 않습니다.

예

```
EXISTS('MyFile') ? #Process('MyFile') : THROW('File does not exist.')
```

콘솔 로그에 출력되는 메시지: 'File does not exist.'

```
VEXIST(#Sortname) ? #Sortname : THROW('Sortname is not defined.')
```

콘솔 로그에 출력되는 메시지: 'Sortname is not defined.'

WARNING 함수 - 콘솔 로그에 경고 메시지 기록

TRACE 함수는 문자열 인수를 SiteMinder 콘솔 로그에 추적 항목으로 기록합니다.

구문

TRACE 함수의 형식은 다음과 같습니다.

TRACE(*source_string*)

매개 변수

TRACE 함수는 다음 매개 변수를 사용합니다.

source_string(문자열)

반환 값

TRACE 함수는 부울(항상 TRUE)을 반환합니다.

설명

권한 있음: 예

예

```
Return_value=TRACE("Executing Code")
Return_value=TRUE
```

TRANSLATE 함수 - 문자열 값 바꾸기

TRANSLATE 함수는 첫 번째 문자열을 두 번째 문자열 내에서 찾아 모두 세 번째 문자열로 바꿉니다. 선택적 부울이 TRUE 로 설정되지 않은 경우 검색 시 대/소문자가 구분됩니다.

구문

TRANSLATE 함수의 형식은 다음과 같습니다.

```
TRANSLATE(source_string, search_string, replace_string[, not_case_sensitive])
```

매개 변수

TRANSLATE 함수는 다음 매개 변수를 사용합니다.

source_string(문자열)

search_string(문자열)

replace_string(문자열)

not_case_sensitive(부울)

(선택 사항) 이 매개 변수가 설정되지 않거나 FALSE 로 설정된 경우 검색 시 대/소문자가 구분됩니다. TRUE 로 설정된 경우에는 대/소문자가 무시됩니다.

반환 값

TRANSLATE 함수는 문자열을 반환합니다.

예

```
Return_value=TRANSLATE('Eric','r','x')
Return_value='Exic'
```

```
Return_value=TRANSLATE('Eric','ri','x')
Return_value='Exc'
```

```
Return_value=TRANSLATE('Eric','r','xy')  
Return_value='Exyc'
```

```
Return_value=TRANSLATE('Eric','R','x')  
Return_value='Eric'
```

```
Return_value=TRANSLATE('Eric','R','x',TRUE)  
Return_value='Exic'
```

UCASE 함수 - 대문자로 변환

UCASE 함수는 원본 문자열을 대문자로 변환합니다.

구문

UCASE 함수의 형식은 다음과 같습니다.

```
UCASE(source_string)
```

매개 변수

UCASE 함수는 다음 매개 변수를 사용합니다.

source_string(문자열)

반환 값

UCASE 함수는 문자열을 반환합니다.

예

```
Return_value=UCASE('framingham, mass')  
Return_value='FRAMINGHAM, MASS'
```

URL 함수 - URL 문자열의 구성 요소 반환

URL 함수는 제공된 URL(또는 경로)을 구문 분석하고 지정된 구성 요소를 반환합니다. 이 함수는 URL 로 인코딩된 문자를 무시합니다.

참고: URL 함수는 백슬래시가 아니라 슬래시를 사용하는 문자열만 구문 분석합니다. Windows 를 실행하는 시스템을 사용하는 경우 백슬래시를 슬래시로 변환하려면 TRANSLATE 함수를 사용하십시오.

구문

URL 함수의 형식은 다음과 같습니다.

`URL(url_string, component)`

매개 변수

URL 함수는 다음 매개 변수를 사용합니다.

url_string(문자열)

URL 또는 경로는 다음과 같은 형식으로 지정해야 합니다.

```
[<protocol>:][//][<user>[:<password>]@]<server>[:<port>#]  
[/<directory>]/<file>][?<querystring>]
```

component(문자열)

구성 요소 이름은 대/소문자를 구분하지 않습니다. 다음과 같은 구성 요소를 지정할 수 있습니다.

- PROTOCOL, DRIVE 또는 NAMESPACE
- USER
- PASSWORD
- SERVER
- PORT
- DOMAIN
- URI
- PATH
- DIRECTORY
- FILENAME
- BASENAME
- EXTENSION
- QUERYSTRING

반환 값

URL 함수는 문자열을 반환합니다.

예

```
Return_value=URL("http://www.myserver.com:8080/app1/xyzzy.jsp?id=12",
"PROTOCOL")
Return_value="http:"

Return_value=URL("ftp://joe:dog@ftp.myserver.com/dir1/xyzzy.zip", "USER")
Return_value="joe"

Return_value=URL("ftp://joe:dog@ftp.myserver.com/dir1/xyzzy.zip",
"PASSWORD")
Return_value="dog"

Return_value=URL("http://www.myserver.com:8080/app1/xyzzy.jsp?id=12",
"SERVER")
Return_value="www.myserver.com"

Return_value=URL("http://www.myserver.com:8080/app1/xyzzy.jsp?id=12",
"PORT")
Return_value="8080"

Return_value=URL("http://www.myserver.com:8080/app1/xyzzy.jsp?id=12",
"DOMAIN")
Return_value="myserver.com"

Return_value=URL("ftp://joe:dog@ftp.myserver.com/dir1/xyzzy.zip", "URI")
Return_value="/dir1/xyzzy.zip"

Return_value=URL("ftp://joe:dog@ftp.myserver.com/dir1/xyzzy.zip", "PATH")
Return_value="/dir1/xyzzy.zip"

Return_value=URL("ftp://joe:dog@ftp.myserver.com/dir1/xyzzy.zip",
"DIRECTORY")
Return_value="/dir1"

Return_value=URL("ftp://joe:dog@ftp.myserver.com/dir1/xyzzy.zip",
"FILENAME")
Return_value="xyzzy.zip"

Return_value=URL("ftp://joe:dog@ftp.myserver.com/dir1/xyzzy.zip",
"BASENAME")
Return_value="xyzzy"
```

```
Return_value=URL("ftp://joe:dog@ftp.myserver.com/dir1/xyzzy.zip",  
"EXTENSION")  
Return_value="zip"  
  
Return_value=URL("ftp://joe:dog@ftp.myserver.com/dir1/xyzzy.zip",  
"QUERYSTRING")  
Return_value=""  
  
Return_value=URL("http://www.myserver.com:8080/app1/xyzzy.jsp?id=12",  
"QUERYSTRING")  
Return_value="id=12"
```

URLDECODE 함수 - URL 문자열 디코딩

URLDECODE 함수는 지정된 URL 문자열을 디코딩합니다.

구문

URLDECODE 함수의 형식은 다음과 같습니다.

```
URLDECODE(url)
```

매개 변수

이 함수는 다음 매개 변수를 사용합니다.

url(문자열)

반환 값

URLDECODE 함수는 문자열을 반환합니다.

예

```
Return_value=URLDECODE("Framingham%2C+Mass")  
Return_value="Framingham, Mass"
```

추가 정보:

[URLENCODE 함수 - 문자열 인코딩](#) (페이지 962)

URLENCODE 함수 - 문자열 인코딩

URLENCODE 함수는 전달된 문자열을 URL 형식으로 인코딩합니다.

구문

URLENCODE 함수의 형식은 다음과 같습니다.

```
URLENCODE(source_string)
```

매개 변수

URLENCODE 함수는 다음 매개 변수를 사용합니다.

source_string(문자열)

반환 값

URLENCODE 함수는 문자열을 반환합니다.

예

```
Return_value=URLENCODE('Framingham, Mass')  
Return_value='Waltham%2C+Mass'
```

추가 정보:

[URLDECODE 함수 - URL 문자열 디코딩](#) (페이지 961)

VEXIST 함수 - 매개 변수 정의 여부 확인

VEXIST 함수는 명명된 식, 컨텍스트 변수 또는 사용자 특성을 매개 변수로 받아 이러한 매개 변수가 정의되어 있는지 여부를 확인합니다. 매개 변수가 정의되어 있으면 VEXIST 는 TRUE 를 반환합니다. 그렇지 않으면 VEXIST 는 FALSE 를 반환합니다.

참고: LDAP 사용자 디렉터리의 경우 SiteMinder 는 사용자 특성이 정의되었는지 여부를 확인할 수 없으므로 FALSE 를 반환합니다.

구문

VEXIST 함수의 형식은 다음과 같습니다.

```
VEXIST(#virtual_user_attribute | @user_class | %context_variable |
user_attribute_name | user_attribute_string)
```

매개 변수

VEXIST 함수는 다음 매개 변수 중 하나를 사용합니다.

#virtual_user_attribute(명명된 식)

사용자 특성을 계산하는 명명된 식을 지정합니다.

@user_class(명명된 식)

사용자 디렉터리 또는 그룹의 구성원 자격을 테스트하는 명명된 식을 지정합니다.

%context_variable(컨텍스트 변수)

컨텍스트 변수를 지정합니다.

user_attribute_name(따옴표 없는 문자열)

단일 사용자 특성을 지정합니다.

user_attributes_string(문자열)

각 사용자 특성 이름이 문자로 구분된 문자열을 지정합니다.

반환 값

VEXIST 함수는 부울을 반환합니다.

예

```
Return_value=VEXIST(#Age)
Return_value=TRUE

Return_value=VEXIST(@IsDolphin)
Return_value=FALSE

Return_value=VEXIST(%ClientIP)
Return_value=TRUE

Return_value=VEXIST(givenname)
Return_value=FALSE

Return_value=VEXIST('last,first')
Return_value=TRUE
```

WARNING 함수 - 콘솔 로그에 경고 메시지 기록

WARNING 함수는 문자열 인수를 SiteMinder 콘솔 로그에 경고 메시지로 기록합니다.

구문

WARNING 함수의 형식은 다음과 같습니다.

```
WARNING(source_string)
```

매개 변수

WARNING 함수는 다음 매개 변수를 사용합니다.

source_string(문자열)

반환 값

WARNING 함수는 부울(항상 TRUE)을 반환합니다.

예

```
Return_value=WARNING("Buffer Full")
Return_value=TRUE
```


XORBITS 함수 - bitwise XOR 연산 수행

XORBITS 함수는 두 인수에 대해 bitwise XOR 연산을 수행합니다.

구문

XORBITS 함수의 형식은 다음과 같습니다.

```
XORBITS(num_1,num_2)
```

매개 변수

XORBITS 함수는 다음 매개 변수를 사용합니다.

num_1(숫자)

num_2(숫자)

반환 값

XORBITS 함수는 숫자를 반환합니다.

예

```
Return_value=XORBITS(7, 2)
```

```
Return_value=5
```

```
Return_value=XORBITS(7, 15)
```

```
Return_value=8
```

YEAR 함수 - 숫자 형식 날짜의 연도 구성 요소 반환

YEAR 함수는 1970 년 1 월 1 일 이후 경과된 초 수로 표현된 날짜의 연도 구성 요소를 나타내는 숫자를 반환합니다.

구문

YEAR 함수의 형식은 다음과 같습니다.

```
YEAR(date_time)
```

매개 변수

YEAR 함수는 다음 매개 변수를 사용합니다.

date_time(숫자)

초 수로 표현된 날짜입니다.

반환 값

YEAR 함수는 70 에서 138 사이의 숫자를 반환합니다.

YEAR4 함수 - 날짜의 연도 구성 요소(4 자리) 반환

YEAR4 함수는 1970 년 1 월 1 일 이후 경과된 초 수로 표현된 날짜의 4 자리 연도 구성 요소를 반환합니다.

구문

YEAR4 함수의 형식은 다음과 같습니다.

YEAR4(*date_time*)

매개 변수

YEAR4 함수는 다음 매개 변수를 사용합니다.

date_time(숫자)

반환 값

YEAR4 함수는 1970 에서 2038 사이의 숫자를 반환합니다.