SiteMinder Federation

레거시 페더레이션 안내서

12.52 SP1

ca technologies

CA Technologies 제품 참조

이 문서는 다음 CA Technologies 제품을 참조합니다 :

- SiteMinder
- CA SiteMinder® 웹 에이전트 옵션 팩
- CA SiteMinder for Secure Proxy Server

CA 에 문의

기술 지원팀에 문의

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

설명서 변경 사항

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

- 안내서 전체에서 SAML 가맹 에이전트에 대한 모든 참조가 제거되었습니다. 이 제품은 더 이상 지원되지 않습니다.
- smfedexport 에 대한 명령 옵션 (페이지 389) - smfedexport 유틸리티에서 -decryptionkeyalias 명령 옵션이 추가되었습니다.

목차

제 12 장: SAML 1.x 생산자 구성 129

제 1 장: 레거시 페더레이션 소개

이 섹션은 다음 항목을 포함하고 있습니다.

페더레이션의 파트너에 대한 용어

본 안내서에서는 *어설션 당사자*와 *신뢰 당사자*라는 용어를 사용하여 페더레이션된 관계의 양쪽 당사자를 식별합니다.

어설션을 생성하는 당사자를 어설션 당사자라고 합니다. 어설션 당사자는 다음과 같을 수 있습니다.

- SAML 1.x 생산자
- SAML 2.0 아이덴티티 공급자
- WS-페더레이션 계정 파트너

인증 목적으로 어설션을 소비하는 당사자를 신뢰 당사자라고 합니다. 신뢰 당사자는 다음과 같을 수 있습니다.

- SAML 1.x 소비자
- SAML 2.0 서비스 공급자
- WS-페더레이션 리소스 파트너

사이트는 어설션 당사자(생산자/IdP/AP)와 신뢰 당사자(소비자/SP/RP)로 작동할 수 있습니다.

레거시 페더레이션에 대한 구성 요소

레거시 페더레이션은 가맹 도메인, 가맹 파트너, 인증 체계, 페더레이션된 리소스를 보호하는 정책 등의 SiteMinder 개체 구성을 기반으로 합니다.

SiteMinder Federation 제공 기능, 레거시 페더레이션 사용 사례 및 프로세스 흐름도에 대한 자세한 내용은 *엔터프라이즈의 페더레이션*을 참조하십시오.

레거시 페더레이션은 다음과 같은 여러 구성 요소를 사용합니다.

SAML 어설션 생성자

어설션 당사자에서 SAML 어설션을 생성하는 정책 서버 구성 요소입니다.

SAML 어설션 생성자는 생산자/IdP 사이트에 세션이 있는 사용자에 대한 어설션을 생성합니다. 파트너가 SAML 어설션을 요청하면 웹 에이전트가 SAML 어설션 생성자를 호출합니다. 어설션 생성자가 사용자 세션과 정책 저장소에 있는 정보를 기반으로 어설션을 생성합니다.

어설션 생성자는 다음과 같이 구성된 인증 프로필이나 바인딩에 따라 어설션을 처리합니다.

- SAML 아티팩트 프로필/바인딩

  어설션 생성자가 SiteMinder 세션 저장소에 어설션을 저장합니다. 어설션에 대한 참조가 SAML 아티팩트 형식으로 웹 에이전트에 반환됩니다.

- SAML POST 프로필/바인딩

  SiteMinder 가 브라우저를 통해 HTTP 양식에 포함된 SAML 응답으로 어설션을 반환합니다.

웹 에이전트는 SAML 프로필에 따라 SAML 아티팩트, SAML 응답 또는 WS-페더레이션 보안 토큰 응답을 신뢰 당사자에게 보내는 작업을 담당합니다. 신뢰 당사자에서 클라이언트가 SAML 아티팩트 또는 응답 메시지를 처리할 수 있어야 합니다. SiteMinder 가 신뢰 당사자인 경우 클라이언트는 SAML 1.x 자격 증명 수집기 또는 SAML 2.0 어설션 소비자일 수 있습니다.

어설션 생성자 플러그인을 구성하여 SAML 어설션 콘텐츠를 사용자 지정할 수 있습니다. 이 플러그인을 사용하면 페더레이션된 환경에 맞게 콘텐츠를 사용자 지정할 수 있습니다.

WS-페더레이션 어설션 생성자

SAML 어설션이 포함된 WS-페더레이션 RequestSecurityTokenResponse 메시지를 생성하는 정책 서버 구성 요소입니다.

WS-페더레이션 어설션 생성자는 계정 파트너에 세션이 있는 사용자에 대한 SAML 1.1 어설션을 생성합니다. 사용자가 리소스를 요청하면 웹 에이전트가 정책 서버에서 WS-페더레이션 어설션 생성자를 호출합니다. 정책 서버가 사용자 세션과 정책 저장소에 구성된 정보를 기반으로 어설션을 생성합니다. 그런 다음 어설션 생성자가 WS-페더레이션 RequestSecurityTokenResponse 메시지에 어설션을 배치합니다.

웹 에이전트는 WS-페더레이션 피동 요청자 프로필에 따라 브라우저를 통해 보안 토큰 응답 메시지를 신뢰 당사자에게 보냅니다. 리소스 파트너에서 WS-페더레이션 어설션 소비자 등의 클라이언트가 어설션을 처리할 수 있어야 합니다.

어설션 생성자 플러그인을 구성하여 SAML 어설션 콘텐츠를 사용자 지정할 수 있습니다. 이 플러그인을 사용하면 페더레이션된 환경에 맞게 콘텐츠를 사용자 지정할 수 있습니다.

페더레이션 인증 체계

SAML 또는 WS-페더레이션 어설션의 유효성을 검사하고 어설션 데이터를 신뢰 당사자의 로컬 사용자에게 매핑하는 정책 서버 구성 요소입니다.

지원되는 인증 체계는 다음과 같습니다.

- SAML 1.x 아티팩트
- SAML 1.x POST
- SAML 2.0(아티팩트 및 POST 바인딩)
- WS-페더레이션

페더레이션 웹 서비스

어설션 당사자에서 어설션 검색, 세션 동기화 및 알림 경고를 지원하는 웹 에이전트 구성 요소입니다. 신뢰 당사자에서 이러한 서비스는 어설션을 수집합니다.

레거시 페더레이션 인증 체계

레거시 페더레이션은 다음 인증 체계를 지원합니다.

- SAML 1.x 아티팩트
- SAML 1.x POST
- SAML 2.0
- WS-페더레이션

각 인증 체계를 통해 신뢰 당사자의 SiteMinder 가 SAML 어설션을 처리할 수 있습니다. 어설션을 받는 경우 인증 체계는 다음을 수행합니다.

- SAML 어설션의 유효성을 검사합니다.
- 어설션 데이터를 로컬 사용자에게 매핑합니다.
- 어설션을 소비하는 사이트에서 SiteMinder 세션을 설정합니다.

SAML 인증 체계는 어설션 당사자의 원격 사용자를 신뢰 당사자의 로컬 사용자에게 매핑하는 위치입니다. 사용자 매핑을 통해 인증 체계에서 인증을 위한 올바른 사용자 레코드를 찾을 수 있습니다.

보안 영역이 있는 페더레이션된 싱글 사인온

웹 서비스 보호용 웹 응용 프로그램 환경과 페더레이션된 리소스 보호용 페더레이션 환경을 포함하도록 SiteMinder 환경을 설정할 수 있습니다. 이 방법을 통해 SiteMinder 배포의 효율성을 높일 수 있습니다.

특정 페더레이션 기능에는 영구 사용자 세션이 필요합니다. 즉, SAML 어설션이 정책 서버의 세션 저장소에 저장됩니다.

이러한 기능은 다음과 같습니다.

아티팩트 싱글 사인온

SAML 1.x 및 SAML 2.0 의 경우 SAML 어설션은 나중에 신뢰 당사자가 검색하는 영구 세션에 저장됩니다.

싱글 로그아웃

생산자 및 소비자 사이트의 (SAML 2.0 싱글 로그아웃 및 WS-페더레이션 사인아웃). 파트너 데이터는 페더레이션된 로그아웃 중에 파트너에게 쉽게 통지할 수 있도록 영구 사용자 세션에 저장됩니다.

어설션을 검색하거나 로그아웃 요청을 처리하려면 세션 저장소에 대한 호출이 필요하기 때문에 영구 사용자 세션을 사용하면 성능이 저하됩니다. 성능에 미치는 영향을 제한하려면 보안 영역을 사용하십시오.

보안 영역은 단일 쿠키 도메인의 세그먼트입니다. 보안 영역을 사용하면 응용 프로그램을 분할하여 리소스 액세스에 대한 다양한 보안 요구 사항을 허용할 수 있습니다. 단일 영역의 모든 응용 프로그램 간에 싱글 사인온이 허용됩니다. 응용 프로그램이 다른 영역에 있으면 구성하는 트러스트 관계에 따라 싱글 사인온이 결정됩니다.

어설션 당사자에서 페더레이션된 응용 프로그램의 경우 다음 설정을 구현하십시오.

- 전용 보안 영역을 생성합니다.
- 모든 페더레이션되지 않은 응용 프로그램에 사용할 다른 영역을 생성합니다.
- 페더레이션되지 않은 영역을 트러스트하도록 페더레이션된 영역을 구성합니다.

다양한 영역을 사용하면 세션 서버에 대한 호출이 페더레이션된 응용 프로그램 전용으로 국한됩니다.

참고: 페더레이션된 환경에서 웹 에이전트만 보안 영역을 사용하도록 구성할 수 있습니다. 보안 프록시 에이전트와 응용 프로그램 서버 에이전트는 이 기능을 지원하지 않습니다.

보안 영역을 구성하려면 다음 웹 에이전트 매개 변수에 대한 값을 입력하십시오.

SSOZoneName

싱글 사인온 보안 영역을 식별합니다. 영역 이름이 쿠키 도메인 이름에 추가되어 영역을 도메인과 연결합니다.

참고: 이 항목은 영어 문자만 지원합니다. 다른 언어의 문자는 지원되지 않습니다.

SSOTrustedZone

트러스트된 보안 영역의 정렬된 목록을 표시합니다. 영역과 트러스트된 영역 목록을 정의하면 웹 에이전트가 읽고 쓸 수 있는 쿠키가 결정됩니다.

이러한 매개 변수는 로컬 에이전트 구성 파일이나 에이전트 구성 개체의 일부입니다.

보안 영역에 대한 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.

보안 프록시 서버 페더레이션 게이트웨이

CA SiteMinder for Secure Proxy Server 페더레이션 게이트웨이는 페더레이션된 네트워크의 액세스 제어에 대한 프록시 기반 솔루션을 제공합니다. 기존 프록시는 대개 인터넷 리소스를 요청하는 사용자 그룹에 서비스를 제공합니다. SPS 페더레이션 게이트웨이는 역방향 프록시로, 사용자 대신 기업의 리소스를 요청하는 역할을 합니다.

SPS 페더레이션 게이트웨이는 자체 포함 시스템입니다. 게이트웨이는 자체 서블릿 엔진과 웹 서버를 기본 제공합니다. SPS 게이트웨이는 해당 프록시 엔진을 사용하여 페더레이션된 파트너의 보호된 리소스 요청을 처리합니다. 페더레이션 게이트웨이로 작동하도록 SPS 를 향상하면 빠르게 배포할 수 있습니다.

레거시 페더레이션의 구성 요소인 SPS 페더레이션 게이트웨이는 웹 에이전트 및 웹 에이전트 옵션 팩을 대체하여 페더레이션 웹 서비스 응용 프로그램 서비스를 제공할 수 있습니다. 단일 SPS 페더레이션 게이트웨이는 여러 웹 에이전트의 필요성을 제한하여 리소스 액세스에 필요한 구성의 양을 제한할 수 있습니다.

참고: CA SiteMinder for Secure Proxy Server 는 SiteMinder 와는 별개로 라이선스가 부여되는 제품입니다.

레거시 페더레이션의 국제화

레거시 페더레이션은 다음 I18N 국제화 기능을 지원합니다.

- 국제화를 위해 UTF-8 형식으로 인코딩된 레거시 페더레이션 구성 개체, Java 및 C++ 코드
- 멀티바이트 사용자 ID 와 특성 값이 있는 기본 어설션과 사용자 지정된 어설션 만들기 및 소비
- 인코딩된 대상 및 리디렉션 URL. 이러한 URL 은 HTTP 1.1 RFC 2616 에 따라 인코딩되므로 멀티바이트 경로 및 파일 이름이 올바로 처리됩니다.

어설션에 멀티바이트 문자가 포함되는 경우 운영 체제의 LANG 설정을 다음 UTF-8 형식으로 설정하십시오.

LANG=xx_xx.UTF-8

예를 들어 일본어에 대한 항목은 다음과 같습니다.

LANG=ja_JP.UTF-8

디버깅 기능

레거시 페더레이션 구성 요소는 페더레이션된 네트워크에서 발생하는 작업을 모니터링 및 디버깅하기 위해 특정 이벤트를 로깅합니다.

웹 에이전트 로그

생산자 사이트의 SAML 어설션 생성 요청에 대한 정보를 표시합니다.

페더레이션 웹 서비스 로그

SAML 어설션 검색 및 SAML 어설션 소비 요청에 대한 정보를 표시합니다.

정책 서버 로그

SAML 어설션 생성자 및 SAML 아티팩트 인증 체계의 호출 결과를 표시합니다. 정책 서버 관리 프로파일러를 사용하거나 제공된 프로파일러 템플릿 파일 중 하나를 사용하여 구성하는 정책 서버 추적 메시지도 표시합니다.

웹 에이전트 옵션 팩 로그

FWSTrace.conf 파일을 사용하거나 제공된 추적 템플릿 파일 중 하나를 사용하여 구성하는 FWS 추적 메시지를 표시합니다.

레거시 페더레이션에 대한 API

다음 API 는 레거시 페더레이션에 대한 지원을 제공합니다.

- 정책 관리 API
- Java 메시지 소비자 플러그인 API
- Java 어설션 생성기 플러그인 API

정책 관리 API

C 및 Perl 정책 관리 API 는 SiteMinder Federation 을 지원하는 새 언어 요소를 제공합니다. 이러한 새 언어 요소는 다음과 같습니다.

- 페더레이션 개체에 대한 C 구조 및 Perl 패키지. 개체에는 가맹 도메인, 가맹, 아이덴티티 및 서비스 공급자, 리소스 및 계정 파트너 등이 있습니다.
- SAML 1.x, SAML 2.0 및 WS-페더레이션 구성에 대한 C 함수 및 Perl 메서드
- SAML 2.0 메타데이터 상수
- WS-페더레이션 메타데이터 상수

정책 관리 API 에 대한 자세한 내용은 *SiteMinder Programming Guide for Perl*(SiteMinder Perl 프로그래밍 안내서) 또는 *SiteMinder Programming Guide for C*(SiteMinder C 프로그래밍 안내서)를 참조하십시오.

Java 메시지 소비자 플러그인 API

SiteMinder Java MessageConsumerPlugin API 는 SAML 1.x, SAML 2.0 및 WS-페더레이션 메시지 소비자 확장 인터페이스를 구현합니다. 이 API 를 통해 사용자 명확성과 인증을 위한 사용자 고유의 처리를 수행할 수 있습니다. 사용자 고유의 요구 사항에 맞게 코드를 사용자 지정한 후 사용자 지정 플러그인을 SiteMinder 에 통합하여 SAML 어설션 응답이나 WS-페더레이션 보안 토큰 응답을 추가로 처리하고 조작하십시오.

자세한 내용은 *SiteMinder Programming Guide for Java*(SiteMinder Java 프로그래밍 안내서)를 참조하십시오.

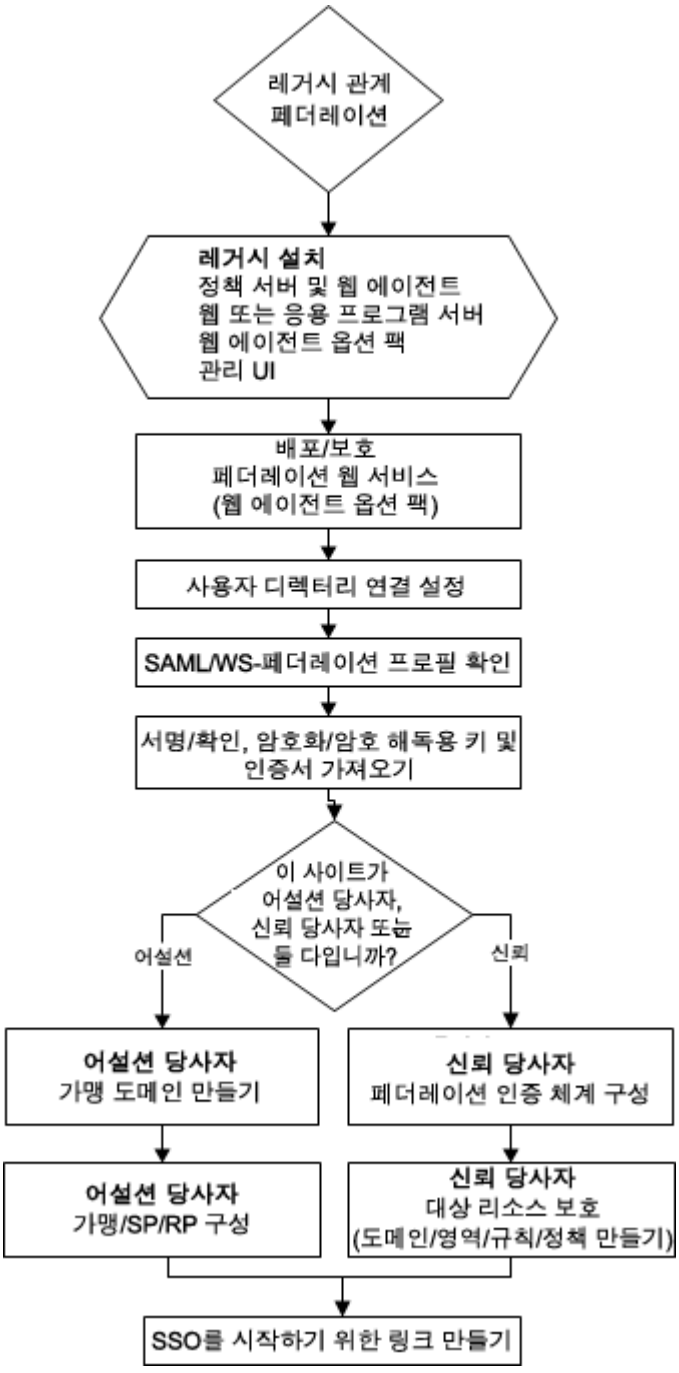
Java 어설션 생성기 플러그인 API

SiteMinder Java 어설션 생성기 플러그인 API 는 어설션 생성기 프레임워크를 구현합니다. 이 플러그인을 사용하여 파트너와 공급업체 간의 비즈니스 계약에 대한 어설션 콘텐츠를 수정할 수 있습니다.

자세한 내용은 *SiteMinder Programming Guide for Java*(SiteMinder Java 프로그래밍 안내서)를 참조하십시오.

레거시 페더레이션 구성 순서도

다음 흐름도는 레거시 페더레이션를 구성하는 일반적인 프로세스를 보여 줍니다.



제 2 장: 레거시 페더레이션에 대해 배우기 위해 샘플 구성 사용

이 섹션은 다음 항목을 포함하고 있습니다.

수동 SiteMinder-SiteMinder 배포 개요

수동으로 배포를 수행할 수 있습니다. 수동 배포 태스크는 간단한 구성, 즉 POST 바인딩이 있는 싱글 사인온으로 시작합니다. 기본 구성으로 시작하여 최소 개수의 단계를 완료하면 페더레이션의 작동 방식을 확인할 수 있습니다.

POST 싱글 사인온을 작동한 후 아티팩트 바인딩 구성, 디지털 서명, 암호화 등의 추가 태스크를 설명합니다. 이러한 기능을 추가하여 실제 프로덕션 환경을 반영할 수 있습니다.

중요! 배포 연습은 SAML 2.0 에만 적용됩니다. SAML 1.x 또는 WS-페더레이션 구성에는 이러한 절차가 적용되지 않습니다.

수동 배포 예는 다음과 같은 측면에서 샘플 응용 프로그램 배포와 다릅니다.

- 설명된 배포는 두 시스템에서 설정되고 각 시스템에는 정책 서버와 웹 에이전트가 있습니다. 두 시스템은 IdP 와 SP 를 나타냅니다.
- 수동 구성의 경우 다음을 포함하여 샘플 응용 프로그램에서 설정하지 않는 추가 기능을 설명합니다.
  - 아티팩트 백 채널에 대해 SSL 구성
  - 어설션에 특성 추가

- 디지털 서명 및 어설션 확인
- 어설션 암호화 및 암호 해독

수동 배포 절차 전반에 걸쳐 샘플 데이터가 사용됩니다. 사용자 환경의 데이터를 사용하려면 아이덴티티 공급자 및 서비스 공급자 구성에 대한 항목을 지정하십시오.

필수 구성 요소가 설치되었는지 확인

페더레이션을 사용하려면 다음 구성 요소를 설치해야 합니다.

- SiteMinder 정책 서버
- 관리 UI
- 웹 에이전트
- 웹 에이전트 옵션 팩

이 샘플 페더레이션 배포 예에서는 이러한 구성 요소가 설치되어 제대로 작동하고 있다고 가정합니다.

선택적으로 다음 기능을 설정하십시오.

- SSL 통신에 대해 웹 또는 응용 프로그램 서버가 사용되도록 설정합니다.

  SSL 은 백 채널을 통한 HTTP-아티팩트 싱글 사인온 통신의 보안을 유지하기 위한 선택 사항입니다.

- 세션 저장소로 사용되도록 데이터베이스를 설정합니다.

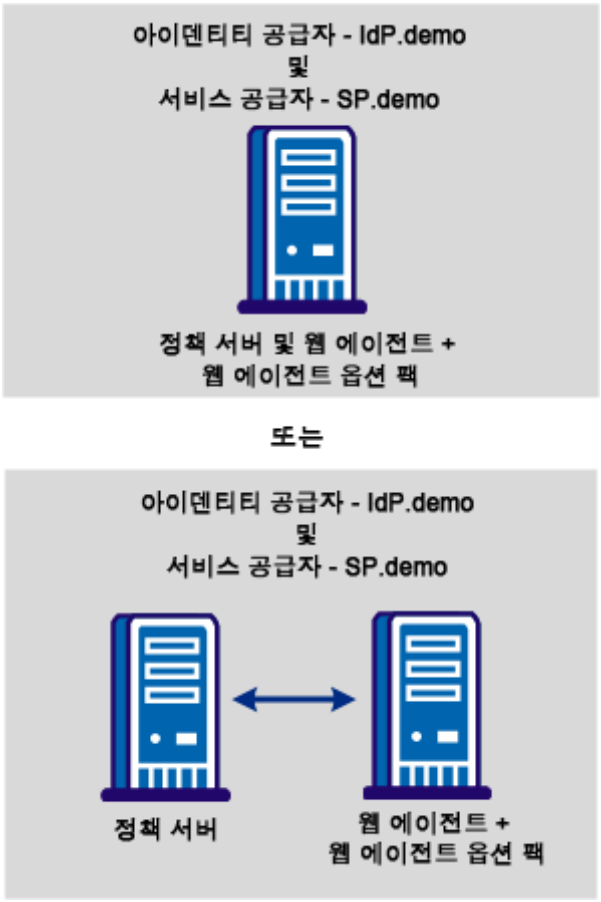
  HTTP-아티팩트 바인딩을 사용할 때 어설션 당사자에 어설션을 저장하려면 세션 저장소가 필요합니다. 세션 저장소는 두 당사자 모두의 싱글 로그아웃에도 필요합니다.

  세션 저장소 데이터베이스 설정에 대한 지침은 *정책 서버 설치 안내서*를 참조하십시오. 정책 서버 관리 콘솔을 사용하여 세션 저장소가 사용되도록 설정합니다. 지침은 *정책 서버 관리 안내서*를 참조하십시오.

샘플 페더레이션 네트워크

SiteMinder 페더레이션된 네트워크의 샘플 웹 사이트는 idp.demo 라는 아이덴티티 공급자와 sp.demo 라는 서비스 공급자입니다. 비즈니스 파트너 관계가 idp.demo 와 sp.demo 간에 설정됩니다.

다음 그림에서는 샘플 페더레이션된 네트워크를 보여 줍니다.



기본 구성에 대한 아이덴티티 공급자 데이터

IdP.demo 가 아이덴티티 공급자입니다. 다음 표에는 가장 기본적인 SAML 2.0 POST 싱글 사인온 구성에 대한 샘플 데이터가 나열되어 있습니다.

아이덴티티 공급자 구성 요소	샘플 네트워크
IdP 정책 서버	**서버**: www.idp.demo:80 **서버 유형**: IIS 웹 서버
IdP 정책 저장소	**IP 주소**: www.idp.demo:389 **저장소**: LDAP (Sun One Directory Server) **루트 DN**: o=idp.demo **관리자 사용자 이름**: cn=Directory Manager **암호**: federation
사용자 저장소	**디렉터리 이름:** IdP LDAP **서버**: www.idp.demo:42088 **서버 유형**: Sun One Directory Server (LDAP) **사용자 저장소**: LDAP 디렉터리에는 다음 사용자가 포함됩니다. ■ user1 ■ user2 **userpassword**: test **메일**: <*user_name*>@idp.demo **루트**: dc=idp,dc=demo **시작**: uid= **끝**: ,ou=People,dc=idp,dc=demo
웹 에이전트 옵션 팩이 있는 IdP 웹 에이전트	**서버**: www.idp.demo:80 **서버 유형**: IIS 웹 서버 **에이전트 이름**: idp-webagent

아이덴티티 공급자 구성 요소	샘플 네트워크
어설션 소비자 서비스 URL	**URL**: http://www.sp.demo:81/affwebservices/public/saml2assertionconsumer
어설션 검색 서비스 URL	**URL:** http://www.idp.demo:80/affwebservices/assertionretriever
인증 URL	**URL**: http://www.idp.demo/siteminderagent/redirectjsp/redirect.jsp

고급 구성에 대한 아이덴티티 공급자 데이터

다음 표에는 아티팩트 프로필, 어설션 서명 및 암호화 등의 고급 SAML 2.0 기능에 대한 샘플 데이터가 나열되어 있습니다.

아이덴티티 공급자 구성 요소	샘플 네트워크
세션 저장소	**서버:** www.idp.demo **데이터베이스 유형:** ODBC **데이터베이스 원본 정보:** SiteMinder 세션 데이터 원본 **사용자 이름:** admin **암호**: dbpassword
SSL-enabled 서버	**서버:** www.idp.demo:443 **서버 유형**: IIS 6.0 웹 웹 에이전트 옵션 팩이 있는 웹 서버가 아티팩트 바인딩에 대해 SSL 이 사용되도록 설정된 서버입니다.
CA(인증 기관) 인증서	**CA 인증서**: docCA.crt **DER 로 인코딩된 인증서:** docCA.der 이 CA 는 SSL 이 사용되도록 설정하기 위해 서버 측 인증서에 서명합니다.

아이덴티티 공급자 구성 요소	샘플 네트워크
SAML 응답에 서명하기 위한 개인 키/인증서 쌍	**인증서**: post-cert.crt **개인 키**: post-pkey.der **암호**: fedsvcs
암호화용 인증서(개인 키)	**공개 키**: sp-encrypt.crt
어설션에 포함할 특성	**특성**: 지정되지 않음(기본값) **특성 종류**: 사용자 DN **변수 이름**: firstname **변수 값**: givenname

기본 구성에 대한 서비스 공급자 데이터

서비스 공급자는 SP.demo 입니다. 다음 표에는 가장 기본적인 SAML 2.0 POST 싱글 사인온 구성에 대한 샘플 데이터가 나열되어 있습니다.

서비스 공급자 구성 요소	샘플 네트워크
SP 정책 서버	**서버**: www.sp.demo:80 **서버 유형**: IIS 웹 서버
SP 정책 저장소	**IP 주소**: www.sp.demo:389 **저장소**: LDAP (Sun One Directory Server) **루트 DN**: o=ca.com **관리자 사용자 이름**: cn=Directory Manager **암호**: federation

서비스 공급자 구성 요소	샘플 네트워크
사용자 저장소	**디렉터리 이름:** SP LDAP **서버**: www.sp.demo:32941 **서버 유형**: LDAP (Sun One Directory Server) **사용자 저장소**: LDAP 디렉터리에는 다음 사용자가 포함됩니다. ■ user1 ■ user2 **userpassword**: customer **메일**: <user_name>@sp.demo **루트**: dc=sp,dc=demo **시작**: uid= **끝**: ,ou=People,dc=sp,dc=demo
SP 웹 에이전트 및 웹 에이전트 옵션 팩	**서버**: www.sp.demo:81 **서버 유형**: Sun ONE 6.1 웹 서버 **에이전트 이름**: sp-webagent
싱글 사인온 서비스	**SSO 서비스**: http://www.idp.demo:80/affwebservices/public/saml2sso
대상 리소스	**대상 리소스**: http://www.sp.demo:81/ spsample/protected/target.jsp

고급 구성에 대한 서비스 공급자 데이터

다음 표에는 아티팩트 프로필 설정, 어설션 서명 및 암호화 등의 고급 SAML 2.0 기능에 대한 샘플 데이터가 나열되어 있습니다.

서비스 공급자 구성 요소	샘플 네트워크
아티팩트 레졸루션 서비스	**레졸루션 서비스**: https://www.idp.demo:443/ affwebservices/saml2artifactresolution

서비스 공급자 구성 요소	샘플 네트워크
인증 기관 인증서	**CA 인증서**: docCA.crt **DER 로 인코딩된 인증서**: docCA.der 이 CA 는 SSL 이 사용되도록 설정하기 위해 서버 측 인증서에 서명합니다.
인증서(공개 키) SAML 응답의 서명을 확인하는 데 사용됩니다.	**인증서**: post-cert.crt
개인 키/인증서 쌍 암호 해독과 디지털 서명에 사용됩니다.	**개인 키**: sp-encrypt.der **공개 키**: sp-encrypt.crt **암호**: fedsvcs **발급자 DN**: CN=Certificate Manager,OU=IAM,O=CA.COM **일련 번호**: 008D 8B6A D18C 46D8 5B

샘플 네트워크에 대한 아이덴티티 공급자 설정

다음 단원에서는 아이덴티티 공급자에서 레거시 페더레이션을 배포하기 위한 태스크를 자세히 설명합니다. 각 단원의 항목은 기본 구성에 대해 제공된 샘플 데이터를 반영합니다.

참고: 이러한 절차에서는 필수 구성 요소를 이미 설치했다고 가정합니다.

IdP 사용자 저장소 설정

아이덴티티 공급자에서 사용자가 정의되어 있는 사용자 저장소가 필요합니다. 아이덴티티 공급자가 이러한 사용자에 대한 어설션을 생성할 수 있습니다. 이 배포에서는 Sun ONE LDAP 사용자 디렉터리가 사용자 저장소입니다. Sun ONE 서버 콘솔이 이 사용자 저장소에 사용자를 추가하는 데 사용됩니다.

사용자 저장소를 구성하려면

1. 다음 사용자를 추가합니다.
   - user1
   - user2
2. 다음과 같이 user1 과 user2 에 대한 특성을 입력합니다.

   user1

   userpassword: test

   mail: user1@idp.demo

   user2

   userpassword: test

   mail: user2@idp.demo

   중요! 전자 메일 주소는 동일한 사용자의 서비스 공급자 사용자 저장소에 있는 것과 동일해야 합니다.
3. 추적 로깅이 사용되도록 설정합니다 (페이지 38).

정책 서버가 IdP LDAP 정책 저장소를 가리키도록 지정

이 배포에서는 LDAP 정책 저장소가 사용됩니다. 정책 서버가 LDAP 정책 저장소를 가리키고 있는지 확인하십시오.

참고: 이 절차에서는 배포의 사용자 저장소에 사용자를 추가하는 방법을 알고 있다고 가정합니다.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "데이터" 탭을 선택합니다.
3. 다음 필드를 작성하십시오.

   데이터베이스

   정책 저장소

   저장소

   LDAP

IP 주소(LDAP 디렉터리)

www.idp.demo:389

루트 DN

o=idp.demo

관리자 사용자 이름

cn=Directory Manager

암호

password

암호 확인

password

4. "확인"을 클릭하여 변경 내용을 저장하고 콘솔을 종료합니다.
5. IdP 사용자 저장소 설정 (페이지 36)으로 이동합니다.

IdP 에서 정책 서버 추적 로깅이 사용되도록 설정

아이덴티티 공급자에서 정책 서버에 대한 로깅이 사용되도록 설정하십시오. 로그 파일 smtracedefault.log 를 살펴보면 싱글 사인온과 싱글 로그아웃에 대한 추적 메시지를 검사할 수 있습니다. 이 로그 파일은 *policy_server_home*/siteminder/log 디렉터리에 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "프로파일러" 탭을 클릭하고 추적 로그 콘텐츠를 사용자 지정합니다.

   참고: 페더레이션 추적 메시지를 보려면 Fed_Server 구성 요소를 로그에 포함하십시오.

   정책 서버에서 정책 서버 관리 콘솔을 사용하여 추적 로깅을 구성할 수 있습니다.
3. IdP 웹 에이전트를 설치합니다.

웹 에이전트 옵션 팩이 있는 웹 서버 구성

샘플 배포용 FWS(페더레이션 웹 서비스) 응용 프로그램을 구성하십시오.

FWS 를 설정하려면

페더레이션 웹 서비스용 JDK 설치

웹 에이전트 옵션 팩을 사용하려면 페더레이션 웹 서비스 응용 프로그램을 실행할 JDK 가 필요합니다.

올바른 JDK 버전을 보려면 기술 지원 사이트로 이동하고 해당 릴리스에 대한 "SiteMinder Platform Support Matrix"(SiteMinder 플랫폼 지원표)를 검색하십시오.

ServletExec 를 설치하고 IdP 의 FWS 와 함께 작동하도록 구성

FWS 작동을 위해 ServletExec 또는 지원되는 모든 응용 프로그램 서버를 설치할 수 있습니다. 이 샘플 네트워크의 경우 IIS 6.0 웹 서버에서 ServletExec 를 사용합니다.

참고: SiteMinder 12.52 SP1 는 라이선스 키 파일 ServletExec_AS_6_license_key.txt 와 함께 제공됩니다. 이 라이선스 키가 없으면 CA 기술 지원 팀에 문의하십시오. 이 라이선스 파일에서 라이선스 키를 복사하여 ServletExec Administration(관리) 콘솔의 "ServletExec License"(ServletExec 라이선스) 대화 상자에 입력합니다. ServletExec 라이선스에 대한 자세한 내용은 New Atlanta Communication http://www.newatlanta.com 웹 사이트에 있는 ServletExec 설명서를 참조하십시오.

사용 중인 ServletExec 의 지원되는 버전에 대한 최신 핫픽스를 적용해야 합니다. 페더레이션 웹 서비스가 ServletExec 와 함께 작동하려면 핫픽스가 필요합니다. 핫픽스를 얻으려면 New Atlanta Communication 웹 사이트로 이동하십시오.

ServletExec 를 설정하려면

1. ServletExec 를 설치합니다. 자세한 내용은 New Atlanta 설명서를 참조하십시오.
2. ServletExec Administration(관리) 콘솔을 엽니다.
3. "Web Applications"(웹 응용 프로그램)에서 "manage"(관리)를 선택합니다.

   "Manage Web Applications"(웹 응용 프로그램 관리) 대화 상자가 열립니다.
4. "Add a Web Application"(웹 응용 프로그램 추가)을 클릭합니다.
5. 다음 정보를 입력합니다.

   Application Name(응용 프로그램 이름)

   affwebservices

   URL Context Path(URL 컨텍스트 경로)

   /affwebservices/

   위치

   C:\program files\ca\webagent\affwebservices

   참고: 설정 중인 affwebservices 의 위치가 다를 수 있습니다. 올바른 위치를 입력합니다.
6. "제출"을 클릭합니다.
7. ServletExec 콘솔을 종료합니다.
8. IIS 기본 사용자 계정에 대한 디렉터리 보안 설정을 수정합니다.

중요! IIS 사용자 계정에 적절한 권한이 있어야 IIS 에서 플러그인이 파일 시스템에 쓰도록 허용할 수 있습니다. 따라서 페더레이션 웹 서비스가 ServletExec 와 함께 작동하려면 IIS 기본 사용자 계정에 대한 디렉터리 보안 설정을 수정하십시오.

추가 정보:

ServletExec 가 IIS 파일 시스템에 쓸 수 있도록 설정 (페이지 41)
IdP 에서 FWS 속성 파일 구성 (페이지 42)

ServletExec 가 IIS 파일 시스템에 쓸 수 있도록 설정

플러그인이 IIS 파일 시스템에 쓸 수 있게 하려면 IIS 에 대한 적절한 권한이 IIS 서버 사용자 계정에 있어야 합니다. 예를 들어 ServletExec 가 페더레이션 로그 파일에 쓸 수 있게 하려면 ServletExec 와 연결된 익명 사용자 계정에 파일 시스템에 대한 쓰기 권한이 있어야 합니다.

다음 단계를 수행하십시오.

1. ServletExec 가 설치된 시스템에서 IIS 인터넷 정보 서비스 관리자를 엽니다.
2. "웹 사이트", "기본 웹 사이트"를 탐색합니다.

   오른쪽 창에 응용 프로그램 집합이 표시됩니다.
3. "ServletExec"를 선택하고 "속성"을 마우스 오른쪽 단추로 클릭합니다.
4. "속성" 대화 상자에서 "디렉터리 보안" 탭을 선택합니다.
5. "인증 및 액세스 제어" 섹션에서 "편집"을 클릭합니다.

   "인증 방법" 대화 상자가 열립니다.
6. 다음과 같이 컨트롤을 설정합니다.
   a. "익명 액세스 가능"을 선택합니다.

      익명 액세스의 경우 Windows 파일 시스템에 대한 권한이 있는 사용자 계정의 이름과 암호를 입력합니다. 사용자 계정에 이 권한을 부여하려면 Windows 설명서를 참조하십시오. 예를 들어 IUSR 인터넷 게스트 계정을 익명 액세스에 사용할 수 있습니다.
   b. "기본 인증"의 선택을 취소합니다.
   c. "Windows 통합 인증"의 선택을 취소합니다.
7. 메시지가 나타나면 웹 서버의 모든 자식 구성 요소에 보안 변경 내용을 적용합니다.
8. 웹 서버를 다시 시작합니다.

이제 ServletExec 와 연결된 사용자 계정으로 IIS 파일 시스템에 쓸 수 있습니다.

다음 단계를 수행하십시오.

1. "제어판", "관리 도구", "로컬 보안 정책", "로컬 정책", "사용자 권한 할당"을 엽니다.

   "로컬 보안 설정" 대화 상자가 나타납니다.

2. "운영 체제의 일부로 작동"을 두 번 클릭합니다.

   "운영 체제의 일부로 작동 속성" 대화 상자가 열립니다.

3. "로컬 보안 설정" 대화 상자에 익명 사용자 계정을 추가합니다.

4. "확인"을 클릭합니다.

5. 제어판을 종료합니다.

6. (선택 사항) IIS 웹 서버를 보호하는 웹 에이전트에 대한 에이전트 구성 개체를 검토하는 것이 좋습니다. 이 개체는 SetRemoteUser 매개 변수가 yes 로 설정되어 있는지 확인하여 익명 사용자가 파일 시스템에 쓸 수 없도록 합니다.

IdP 에서 FWS 속성 파일 구성

AffWebServices.properties 파일에는 페더레이션 웹 서비스에 대한 모든 초기화 매개 변수가 포함되어 있습니다. 이 파일의 설정을 하나 이상 수정하십시오.

affwebservices.properties 파일을 수정하려면

1. 웹 에이전트 옵션 팩이 있는 IdP 시스템에서 C:\Program Files\ca\webagent\affwebservices\WEB-INF\classes 디렉터리로 이동합니다.

2. AgentConfigLocation 매개 변수를 WebAgent.conf 파일의 위치로 설정합니다. 이 매개 변수에는 값이 있어야 합니다.

   이 배포의 경우 IIS 웹 서버가 FWS 응용 프로그램을 호스트합니다. 따라서 WebAgent.conf 파일의 경로는 다음과 같습니다.

   ```
   C:\\Program Files\\ca\\webagent\\bin\\IIS\\WebAgent.conf
   ```

   참고: 페더레이션 웹 서비스는 Java 구성 요소이므로 Windows 경로에 이중 백슬래시를 포함해야 합니다. 이 형식은 Windows 에만 적용됩니다.

   이 경로가 한 줄로 입력되었는지 확인합니다.

3. 파일을 저장한 후 닫습니다.

4. IdP 에서 페더레이션 웹 서비스를 테스트합니다 (페이지 43).

IdP 에서 페더레이션 웹 서비스 테스트

페더레이션 웹 서비스를 설정한 후 응용 프로그램이 올바로 작동하고 있는지 확인하십시오.

다음 단계를 수행하십시오.

1. 웹 브라우저를 열고 다음 링크를 입력합니다.

   http://<*fqhn*>:<*port_number*>/affwebservices/assertionretriever

   fqhn

   정규화된 호스트 이름을 정의합니다.

   port_number

   웹 에이전트와 웹 에이전트 옵션 팩이 설치된 서버의 포트 번호를 정의합니다.

   이 배포의 경우 다음과 같이 입력합니다.

   http://www.idp.demo:80/affwebservices/assertionretriever

   페더레이션 웹 서비스가 올바로 작동하고 있으면 다음 메시지가 표시됩니다.

   어설션 검색 서비스를 초기화했습니다.

   요청된 서블릿은 HTTP POST 요청만 수락합니다.

   이 메시지는 페더레이션 웹 서비스가 데이터 작업을 수신 대기하고 있음을 나타냅니다. 페더레이션 웹 서비스가 올바로 작동하고 있지 않으면 어설션 검색 서비스가 실패했다는 메시지가 표시됩니다. 어설션 검색 서비스가 실패하면 페더레이션 웹 서비스 로그를 검사합니다.

2. IdP 에서 웹 에이전트 옵션 팩 로깅이 사용되도록 설정 (페이지 43)합니다.

IdP 에서 웹 에이전트 옵션 팩 로깅이 사용되도록 설정

IdP 에서 웹 에이전트 옵션 팩이 있는 시스템에 대해 로깅이 사용되도록 설정하십시오. 다음 로그를 확인해야 하는 경우가 있습니다.

- affwebservices.log
- FWSTrace.log

다음 단계를 수행하십시오.

1. LoggerConfig.properties 파일을 설정하여 affwebservices.log 를 구성합니다.
2. FWS 추적 로깅을 구성합니다.
3. IdP 정책 서버에 대한 사용자 저장소를 지정합니다.

IdP 정책 서버에 대한 사용자 저장소 지정

IdP 사용자 디렉터리는 아이덴티티 공급자가 어설션을 생성하는 사용자 레코드로 구성됩니다.

다음 단계에서는 관리 UI 에서 사용자 디렉터리를 구성하는 방법을 지정합니다. IdP LDAP 디렉터리는 user1 및 user2 가 포함된 Sun ONE LDAP 디렉터리입니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "인프라", "디렉터리", "사용자 디렉터리"를 차례로 클릭합니다.
3. "사용자 디렉터리 만들기"를 클릭합니다.
4. 다음 필드를 완성합니다.

   이름

   IdP LDAP

   네임스페이스

   LDAP

   서버

   www.idp.demo:42088

5. "LDAP 설정" 섹션의 다음 필드에 데이터를 입력합니다.

   루트

   dc=idp,dc=demo

   다른 값의 경우 기본값을 적용합니다.

   "LDAP 사용자 DN 조회"의 다음 필드에 데이터를 입력합니다.

   시작

   uid=

   끝

   ,ou=People,dc=idp,dc=demo

6. "콘텐츠 보기"를 클릭하여 디렉터리 콘텐츠를 볼 수 있는지 확인합니다.
7. "제출"을 클릭합니다.
8. IdP 에서 가맹 도메인을 설정합니다.

IdP 에서 가맹 도메인 설정

아이덴티티 공급자에 대해 서비스 공급자를 식별하려면 가맹 도메인을 생성하고 sp.demo 에 대한 서비스 공급자 개체를 추가하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "페더레이션", "레거시 페더레이션", "가맹 도메인"을 차례로 클릭합니다.
3. "가맹 도메인 만들기"를 클릭합니다.
4. 다음 필드를 완성합니다.

   이름

   Federation Sample Partners(페더레이션 샘플 파트너)

   설명

   Domain for sp.demo(sp.demo 에 대한 도메인)

5. 이 대화 상자를 열고 IdP 의 가맹 도메인에 사용자 디렉터리를 추가합니다 (페이지 46).

IdP 의 가맹 도메인에 사용자 디렉터리 추가

사용자 디렉터리를 가맹 도메인과 연결하십시오.

다음 단계를 수행하십시오.

1. "가맹 도메인" 대화 상자의 "사용자 디렉터리" 섹션에 데이터를 입력합니다.
2. IdP LDAP 디렉터리를 추가합니다.

   사용 중인 네트워크의 경우 IdP 에서 설정한 사용자 저장소를 선택합니다.
3. "확인"을 클릭합니다.
4. IdP 의 가맹 도메인에 서비스 공급자 추가 (페이지 46)로 이동합니다.

IdP 의 가맹 도메인에 서비스 공급자 추가

sp.demo 라는 서비스 공급자를 가맹 도메인에 추가하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에서 "페더레이션", "레거시 페더레이션", "SAML 서비스 공급자"로 이동합니다.
2. "SAML 서비스 공급자 만들기"를 선택합니다.
3. 구성 마법사를 따릅니다.
4. "Federation Sample Partners"(페더레이션 샘플 파트너)를 도메인으로 선택하고 "다음"을 클릭합니다.
5. "일반" 단계의 다음 필드에 데이터를 입력합니다.

   이름

   sp.demo

설명

서비스 공급자

SP ID

sp.demo

IdP ID

idp.demo

차이 시간(초)

기본값을 적용합니다.

인증 URL

http://www.idp.demo/siteminderagent/redirectjsp/redirect.jsp

이 redirect.jsp 는 아이덴티티 공급자 사이트에 설치된 웹 에이전트 옵션 팩에 포함되어 있습니다. 이 배포에서 해당 서버는 www.idp.demo 입니다. 사용자에게 SiteMinder 세션이 없는 경우 IdP 의 SSO 서비스는 로그인을 위해 사용자를 인증 URL 로 리디렉션합니다.

성공적으로 인증한 후 redirect.jsp 응용 프로그램은 어설션 생성을 위해 사용자를 SSO 서비스로 다시 리디렉션합니다. SiteMinder 정책으로 이 URL 을 보호해야 합니다.

Enabled(사용)

이 옵션이 선택되어 있는지 확인합니다. 기본적으로 이 옵션은 선택되어 있습니다.

6. UI 를 열고 IdP 가 생성하는 어설션의 대상이 되는 사용자 선택으로 이동합니다.

인증 URL 보호(SAML 2.0)

SiteMinder 정책으로 인증 URL 을 보호해야 합니다. 인증 URL 을 보호하면 보호된 페더레이션된 리소스를 요청하는 사용자가 IdP 에서 SiteMinder 세션을 가지고 있지 않은 경우 해당 사용자에게 인증 챌린지가 표시됩니다.

다음 단계를 수행하십시오.

1. "도메인"에서 "Authentication URL Protection Domain"(인증 URL 보호 도메인)이라는 정책 도메인을 생성합니다.
2. "사용자 디렉터리" 페이지에서 IdP LDAP 사용자 디렉터리를 추가합니다.

3. "Authentication URL Protection domain"(인증 URL 보호 도메인)에서 다음 필드 항목을 사용하여 영구 영역을 생성합니다.

   이름

   Authentication URL Protection Realm(인증 URL 보호 영역)

   에이전트

   조회 단추를 사용하여 FSS 웹 에이전트 선택

   웹 에이전트 옵션 팩이 있는 서버를 보호하는 웹 에이전트입니다.

   리소스 필터

   /siteminderagent/redirectjsp/redirect.jsp

   다른 설정의 경우 기본값을 적용합니다.

   세션 탭

   영구 세션 선택

4. "IDP Authentication URL Protection Realm"(IDP 인증 URL 보호 영역)에서 다음 필드 항목을 사용하여 영역 아래에 규칙을 생성합니다.

   이름

   Authentication URL Protection Rule(인증 URL 보호 규칙)

   영역

   Authentication URL Protection Realm(인증 URL 보호 영역)

   리소스

   *

   웹 에이전트 작업

   Get

   다른 설정의 경우 기본값을 적용합니다.

5. "Authentication URL Protection domain"(인증 URL 보호 도메인)에서 다음 항목을 사용하여 정책을 생성합니다.

   이름

   Authentication URL Protection Policy(인증 URL 보호 정책)

   사용자 탭

   IdP LDAP 사용자 디렉터리에서 user1 추가

규칙 탭

Authentication URL Protection Rule(인증 URL 보호 규칙) 추가

이제 아이덴티티 공급자에서 인증 URL 을 보호하는 정책이 만들어졌습니다.

IdP 가 생성하는 어설션의 대상이 되는 사용자 선택

가맹 도메인에서 서비스 공급자를 지정하는 경우 어설션 생성기가 생성하는 SAML 어설션의 대상이 되는 사용자 및 그룹 목록을 포함하십시오. 가맹 도메인에 있는 디렉터리의 사용자 및 그룹만 추가하십시오.

어설션 생성을 위해 사용자를 선택하려면

1. "사용자" 단계로 이동합니다.
2. "사용자 디렉터리" 섹션에서 이전에 구성된 LDAP 사용자 디렉터리에 대해 "구성원 추가"를 선택합니다.

   "사용자/그룹" 대화 상자가 열립니다.
3. 다음 필드에 데이터를 입력하여 user1 및 user2 를 검색합니다.

   검색 유형

   특성-값

   특성

   uid

   값

   *

   해당 직원이 IdP LDAP 에 나열됩니다.
4. "확인"을 클릭합니다.
5. 마법사의 다음 단계로 이동하여 어설션에 대한 이름 ID 를 구성합니다.

어설션에 대한 이름 ID 구성

이름 ID 는 어설션에서 사용자를 식별하는 고유한 방법입니다. 관리 UI 에 입력하는 NameID 가 어설션에 포함됩니다.

이름 ID 를 구성하려면

1. "이름 ID" 단계로 이동합니다.

   "이름 ID" 대화 상자가 표시됩니다.

2. 다음 필드를 작성하십시오.

   이름 ID 형식

   전자 메일 주소

   전자 메일 주소 형식 값은 이름 ID 가 사용자 디렉터리의 전자 메일 주소를 사용하여 사용자를 식별해야 함을 의미합니다.

   이름 ID 유형 섹션

   사용자 특성

   이름 ID 필드 - 특성 이름

   메일

3. UI 를 열고 마법사의 다음 단계로 이동합니다.

IdP 에서 POST 싱글 사인온 구성

HTTP-POST 를 싱글 사인온에 대한 SAML 2.0 바인딩으로 지정하십시오.

다음 단계를 수행하십시오.

1. "SAML 프로필" 단계로 이동합니다.
2. 다음 필드를 작성하십시오.

   대상자

   sp.demo

   AuthnContext 클래스 참조

   urn:oasis:names:tc:SAML:2.0:ac:classes:Password(기본값)

어설션 소비자 서비스

```
http://www.sp.demo:81/affwebservices/public/
saml2assertionconsumer
```

어설션 소비자 서비스의 URL 을 지정합니다. 사용 중인 네트워크에 대해 지정하는 서버는 웹 에이전트 옵션 팩이 설치된 SP 웹 서버입니다.

인증 수준

5(기본값)

유효 기간 초

60(기본값)

테스트 환경에서 다음 메시지가 정책 서버 추적 로그에 나타나면 60 을 초과하도록 유효 기간 값을 높입니다.

```
Assertion rejected(_b6717b8c00a5c32838208078738c05ce6237) –current time
(Fri Sep 09 17:28:33 EDT 2005) is after SessionNotOnOrAfter time (Fri Sep 09
17:28:20 EDT 2005)
```

HTTP-POST

이 확인란을 선택합니다.

3. 나머지 필드는 무시합니다.
4. 마법사의 다음 단계로 이동합니다.

기본 샘플 배포에 대해 서명 처리가 사용되지 않도록 설정

프로덕션 환경에서는 어설션에 서명하기 위한 서명 처리가 필요합니다. 하지만 기본 샘플 배포의 경우 서명 처리가 사용되지 않도록 설정하십시오.

중요! SAML 2.0 프로덕션 환경에서는 서명 처리가 사용되지 않도록 설정하지 마십시오.

다음 단계를 수행하십시오.

1. "암호화 및 서명" 단계로 이동합니다.
2. 페이지의 "서명" 섹션에서 "서명 처리 사용 안 함"을 선택합니다.
3. "다음"을 클릭하여 마법사의 "특성" 단계로 이동합니다.

서비스 공급자 개체 구성 완료

특성은 서비스 공급자 구성의 마지막 단계입니다. 기본 구성의 경우 특성을 구성하지 마십시오. 대신 "마침"을 클릭하여 서비스 공급자 구성을 완료하십시오. 그러면 구성이 제출됩니다. 아이덴티티 공급자에 대한 서비스 공급자 개체를 식별했습니다.

서비스 공급자 구성

아이덴티티 공급자에서 구성을 마치면 서비스 공급자를 설정해야 합니다.

샘플 네트워크에 대한 서비스 공급자 설정

다음 단원에서는 서비스 공급자에서 레거시 페더레이션을 배포하기 위한 태스크를 자세히 설명합니다. 각 단원의 항목은 기본 구성에 대해 제공된 샘플 데이터를 반영합니다.

참고: 이러한 절차에서는 필수 구성 요소를 이미 설치했다고 가정합니다.

SP 사용자 저장소 설정

SP 에서 사용자 저장소를 구성하고 어설션이 필요한 사용자의 사용자 레코드를 추가하십시오. 그러면 인증하는 동안 어설션이 제공될 때 서비스 공급자가 사용자 저장소에서 사용자 레코드를 찾습니다.

이 배포에서는 Sun ONE LDAP 사용자 디렉터리가 사용자 저장소입니다. Sun ONE 서버 콘솔을 사용하여 디렉터리에 사용자를 추가하십시오.

사용자 저장소를 구성하려면

1. 다음 사용자를 추가합니다.
   - user1
   - user2
2. 다음과 같이 user1 과 user2 에 대한 특성을 입력합니다.

   user1

   userpassword: customer

   mail: user1@sp.demo

   user2

   userpassword: customer

   mail: user2@sp.demo

   중요! 전자 메일 주소는 동일한 사용자의 아이덴티티 공급자 사용자 저장소에 있는 것과 동일해야 합니다.
3. 추적 로깅이 사용되도록 설정합니다 (페이지 54).

정책 서버가 SP LDAP 정책 저장소를 가리키도록 지정

정책 서버와 LDAP 정책 저장소 간의 연결을 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "데이터" 탭을 선택합니다.

   다음 필드를 작성하십시오.

   데이터베이스

   정책 저장소

   저장소

   LDAP

   LDAP IP 주소

   sp.demo:389

   루트 DN

   o=sp.demo

관리자 사용자 이름

cn=Directory Manager

암호

federation

암호 확인

federation

3. "확인"을 클릭합니다.
4. SP 사용자 저장소를 설정합니다 (페이지 52).

SP 에서 페더레이션 구성 요소에 대한 추적 로깅 사용

SP 정책 서버에서 페더레이션 구성 요소를 추적 로그 smtracedefault.log 에 로깅하고 추적 메시지를 검사하도록 SiteMinder 프로파일러를 구성합니다.

로깅이 사용되도록 설정하려면

1. 정책 서버 관리 콘솔을 엽니다.
2. "프로파일러" 탭을 클릭하고 추적 로그 콘텐츠를 사용자 지정합니다. 페더레이션 추적 메시지를 보려면 Fed_Server 구성 요소를 로그에 포함하십시오.

   정책 서버에서 정책 서버 관리 콘솔을 사용하여 추적 로깅을 구성할 수 있습니다.
3. SP 웹 에이전트를 설치합니다.

웹 에이전트 옵션 팩이 있는 웹 서버 구성

웹 에이전트 옵션 팩이 FWS(페더레이션 웹 서비스) 응용 프로그램을 설치했습니다. 샘플 배포에 대해 FWS 응용 프로그램을 구성하십시오.

FWS 가 제대로 작동하도록 하려면 다음을 구성하십시오.

1. 페더레이션 웹 서비스용 JDK 설치 (페이지 55)
2. ServletExec 를 설치하고 SP 의 FWS 와 함께 작동하도록 구성 (페이지 55)

3. AffWebServices.properties 파일 구성 (페이지 56)
4. 웹 에이전트 옵션 팩 로깅이 사용되도록 설정 (페이지 57)
5. 페더레이션 웹 서비스 테스트 (페이지 57)

페더레이션 웹 서비스용 JDK 설치

웹 에이전트 옵션 팩을 사용하려면 페더레이션 웹 서비스 응용 프로그램을 실행할 JDK 가 필요합니다. 필요한 특정 버전을 확인하려면 기술 지원 사이트로 이동한 후 "SiteMinder Platform Support Matrix"(SiteMinder 플랫폼 지원표)에서 해당 릴리스를 검색합니다.

ServletExec 를 설치하고 SP 의 FWS 와 함께 작동하도록 구성

이 배포에서는 FWS 작동을 위해 ServletExec 가 Sun ONE 6.1 웹 서버에 설치되어 있습니다.

참고: SiteMinder 12.52 SP1 는 라이선스 키 파일 ServletExec_AS_6_license_key.txt 와 함께 제공됩니다. 이 라이선스 키가 없으면 CA 기술 지원 팀에 문의하십시오. 이 라이선스 파일에서 라이선스 키를 복사하여 ServletExec Administration(관리) 콘솔의 "ServletExec License"(ServletExec 라이선스) 대화 상자에 입력합니다. ServletExec 라이선스에 대한 자세한 내용은 New Atlanta Communication http://www.newatlanta.com 웹 사이트에 있는 ServletExec 설명서를 참조하십시오.

ServletExec 의 지원되는 버전에 대한 최신 핫픽스를 적용하십시오. 페더레이션 웹 서비스가 ServletExec 와 함께 작동하려면 핫픽스가 필요합니다. 핫픽스를 얻으려면 New Atlanta Communications http://www.newatlanta.com 웹 사이트로 이동하십시오.

ServletExec 를 설정하려면

1. ServletExec 를 설치합니다.

   지침은 New Atlanta Communications 설명서를 참조하십시오.

2. ServletExec Administration(관리) 콘솔을 엽니다.
3. "Web Applications"(웹 응용 프로그램)에서 "manage"(관리)를 선택합니다.

   "Manage Web Applications"(웹 응용 프로그램 관리) 대화 상자가 열립니다.

4. "Add a Web Application"(웹 응용 프로그램 추가)을 클릭합니다.
5. 다음 정보를 입력합니다.

   Application Name(응용 프로그램 이름)

   affwebservices

   URL Context Path(URL 컨텍스트 경로)

   /affwebservices/

   위치

   C:\program files\ca\webagent\affwebservices

   사용 중인 네트워크에 있는 affwebservices 의 위치가 다를 수 있습니다. 올바른 위치를 입력합니다.
6. "제출"을 클릭합니다.
7. ServletExec 콘솔을 종료합니다.
8. AffWebServices.properties 파일을 구성합니다 (페이지 56).

FWS 속성 파일 구성

AffWebServices.properties 파일에는 페더레이션 웹 서비스에 대한 모든 초기화 매개 변수가 포함되어 있습니다. 이 파일에서 WebAgent.conf 파일의 위치를 지정하십시오.

다음 단계를 수행하십시오.

1. 웹 에이전트 옵션 팩이 있는 SP 시스템에서 C:\Program Files\ca\webagent\affwebservices\WEB-INF\classes 디렉터리로 이동합니다.
2. AgentConfigLocation 매개 변수를 WebAgent.conf 파일의 위치로 설정합니다. 이 매개 변수에 대한 값 설정은 필수 사항입니다.

   이 배포의 경우 서비스 공급자에서 FWS 응용 프로그램을 호스트하는 웹 서버는 Sun ONE 웹 서버입니다. 따라서 WebAgent.conf 파일의 경로는 다음과 같습니다.

   ```
   C:\\Sun\\WebServer6.1\\https-sp.demo\\config\\WebAgent.conf
   ```

   참고: 페더레이션 웹 서비스는 Java 구성 요소이므로 Windows 경로에 이중 백슬래시를 포함해야 합니다. 한 줄로 이 항목을 지정하십시오.
3. 파일을 저장한 후 닫습니다.
4. 페더레이션 웹 서비스를 테스트합니다 (페이지 57).

페더레이션 웹 서비스 테스트

페더레이션 웹 서비스 응용 프로그램을 설정한 후 올바로 작동하고 있는지 확인하십시오.

다음 단계를 수행하십시오.

1. 웹 브라우저를 열고 다음 링크를 입력합니다.

   `http://fqhn:port_number/affwebservices/assertionretriever`

   fqhn

   정규화된 호스트 이름을 정의합니다.

   port_number

   웹 에이전트와 웹 에이전트 옵션 팩이 설치된 서버의 포트 번호를 정의합니다.

   이 배포의 경우 다음과 같이 입력합니다.

   `http://www.sp.demo:81/affwebservices/assertionretriever`

   페더레이션 웹 서비스가 올바로 작동하고 있으면 다음 메시지가 표시됩니다.

   ```
   어설션 검색 서비스를 초기화했습니다.
   요청된 서블릿은 HTTP POST 요청만 수락합니다.
   ```

   이 메시지는 페더레이션 웹 서비스가 데이터 작업을 수신 대기하고 있음을 나타냅니다. 페더레이션 웹 서비스가 올바로 작동하고 있지 않으면 어설션 검색 서비스가 실패했다는 메시지가 표시됩니다. 어설션 검색 서비스가 실패하면 페더레이션 웹 서비스 로그를 검사합니다.

2. 웹 에이전트 옵션 팩 로깅이 사용되도록 설정합니다. (페이지 57)

SP 에서 웹 에이전트 옵션 팩 로깅이 사용되도록 설정

SP 에서 웹 에이전트 옵션 팩이 있는 시스템에 대해 로깅이 사용되도록 설정하면 다음 로그를 볼 수 있습니다.

- affwebserv.log

  오류 로깅 메시지를 포함합니다.

- FWSTrace.log

오류 및 추적 로깅이 사용되도록 설정하려면

1. LoggerConfig.properties 파일을 엽니다. 이 파일은 *web_agent_home*/affwebservices/WEB-INF/classes 디렉터리에서 찾을 수 있습니다.
2. LoggingOn 매개 변수를 Y 로 설정합니다.
3. affwebserv.log 파일을 가리키는 LogFileName 설정의 기본 이름과 위치를 그대로 사용합니다.
4. TracingOn 설정을 Y 로 설정합니다.
5. FWSTrace.log 파일을 가리키는 TraceFileName 설정의 기본 이름과 위치를 그대로 사용합니다.

이제 로깅이 사용되도록 설정되었습니다.

SP 정책 서버에 대한 사용자 저장소 지정

SP 사용자 디렉터리는 서비스 공급자가 인증에 사용하는 사용자 레코드로 구성됩니다.

관리 UI 에서 사용자 디렉터리를 구성하십시오. SP LDAP 라는 디렉터리는 user1 및 user2 사용자가 포함된 Sun ONE LDAP 디렉터리입니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "인프라", "디렉터리", "사용자 디렉터리"를 차례로 클릭합니다.
3. "사용자 디렉터리 만들기"를 클릭합니다.
4. 다음 필드를 완료합니다.

   이름

   SP LDAP
5. "디렉터리 설정" 섹션의 다음 필드에 데이터를 입력합니다.

   네임스페이스

   LDAP

   서버

   www.sp.demo:32941

6. "LDAP 검색" 섹션의 다음 필드에 데이터를 입력합니다.

   루트

   dc=sp,dc=demo

   다른 값의 경우 기본값을 적용합니다.

7. "LDAP 사용자 DN 조회" 섹션의 다음 필드에 데이터를 입력합니다.

   시작

   uid=

   끝

   ,ou=People,dc=sp,dc=demo

8. "콘텐츠 보기"를 클릭하여 디렉터리 콘텐츠를 볼 수 있는지 확인합니다.
9. "제출"을 클릭합니다.

SP 에서 SAML 2.0 인증 체계 구성

서비스 공급자에서 사용자를 인증하려면 SAML 2.0 인증 체계를 구성하십시오. IdP 의 어설션이 인증에 대한 자격 증명을 제공합니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "인프라", "인증", "인증 체계"를 차례로 클릭합니다.
3. 다음 필드를 완성합니다.

   체계 일반 설정 섹션:

   이름

   파트너 IDP.demo 인증 체계

   인증 체계 유형

   SAML 2.0 템플릿

   보호 수준

   5(기본값)

4. "SAML 2.0 구성"을 클릭합니다.

   일반 및 사용자 명확성을 지정하는 대화 상자가 표시됩니다.

5. "일반" 섹션에서 다음 설정을 지정합니다.

   SP ID

   sp.demo

   IdP ID

   idp.demo

   SAML 버전

   2.0(기본값)

   차이 시간

   30(기본값)

   참고: "SP ID" 및 "IdP ID" 값이 IdP 의 값과 일치해야 합니다.

6. "사용자 명확성" 섹션에서 다음 설정을 구성합니다.

   LDAP

   Username=%s

7. "다음"을 클릭하여 싱글 사인온 설정으로 이동합니다.

추가 정보:

서비스 공급자에서 서명 유효성 검사가 사용되도록 설정 (페이지 77)

SP 에서 싱글 사인온에 대한 HTTP-POST 구성

인증 체계의 경우 사용할 싱글 사인온 바인딩을 지정해야 서비스 공급자가 아이덴티티 공급자와 통신하는 방법을 알게 됩니다.

다음 단계를 수행하십시오.

1. "SSO" 설정의 다음 필드에 데이터를 입력합니다.

   리디렉션 모드

   302 쿠키 데이터(기본값)

   HTTP 302 리디렉션을 통해 사용자를 리디렉션하며, 세션 쿠키는 포함하지만 다른 데이터는 제외됩니다.

   SSO 서비스

   `http://www.idp.demo:80/affwebservices/public/saml2sso`

대상자

sp.demo

이 값은 아이덴티티 공급자에 있는 값과 일치해야 합니다.

대상

`http://www.sp.demo:81/spsample/protected/target.jsp`

http 로 시작하는 대상의 경우 리소스의 전체 경로를 입력합니다. SAML 2.0 인증 체계를 사용하는 SiteMinder 정책이 대상을 보호합니다.

2. "바인딩" 섹션에서 "HTTP-POST"를 선택합니다.
3. "단일 사용 정책 적용" 확인란을 선택 취소합니다.

   이 옵션이 사용되지 않도록 설정하면 샘플 네트워크가 SAML 2.0 과 호환되지 않게 됩니다. 단일 사용 정책 기능이 사용되도록 설정하려면 서비스 공급자에서 세션 저장소를 설정합니다.
4. "암호화 및 서명" 단계에 도달할 때까지 "다음"을 클릭합니다.
5. "서명 처리 사용 안 함"을 선택합니다.

   중요! 서명이 사용되지 않도록 설정하는 *유일한* 목적은 초기 싱글 사인온 구성을 디버깅하기 위한 것입니다. 프로덕션 환경에서 서명 처리는 필수 보안 요구 사항입니다. SP 에서 서명 유효성 검사가 사용되도록 설정하고 서명의 유효성을 검사하도록 인증서 데이터 저장소를 설정하십시오.
6. 마지막 구성 단계에 도달할 때까지 "다음"을 클릭합니다.
7. "마침"을 클릭합니다.

   기본 인증 체계 구성이 완료되었습니다.
8. 관리 UI 를 열고 SAML 2.0 인증을 사용하여 대상 리소스 보호로 이동합니다.

SP 의 대상 리소스 보호

SAML 2.0 인증 체계를 구성한 후 서비스 공급자의 대상 리소스를 보호하는 정책에서 이 체계를 사용하십시오.

다음 단계를 수행하십시오.

1. "인프라", "에이전트", "에이전트"로 이동하고 sp-webagent 라는 웹 에이전트를 생성합니다. 이 에이전트는 웹 에이전트 옵션 팩이 설치된 서버를 보호합니다.
2. "정책", "도메인", "도메인"으로 이동합니다.
3. 다음 값이 포함된 정책 도메인을 생성합니다.

   이름

   Domain for IdP.demo Visitors(IdP.demo 방문자에 대한 도메인)

   "사용자 디렉터리" 섹션

   user1 과 user2 가 들어 있는 사용자 디렉터리를 추가합니다.
4. "영역" 페이지로 이동하고 다음 값이 포함된 영구 영역을 구성합니다.

   이름

   SP Target Page Protection Realm(SP 대상 페이지 보호 영역)

   에이전트

   sp-webagent

   리소스 필터

   /spsample/protected.jsp

   서비스 공급자 웹 서버에 있는 대상 리소스의 경로를 정의합니다.

   기본 리소스 보호

   보호됨

   인증 체계

   파트너 IdP.demo 인증 체계

5. 영역에 다음 값이 포함된 규칙을 추가합니다.

   이름

   SP Target Page Protection Rule(SP 대상 페이지 보호 규칙)

   영역

   SP Target Page Protection Realm(SP 대상 페이지 보호 영역)

   리소스

   *

   작업

   웹 에이전트 작업

   Get

   다른 모든 필드의 경우 기본값을 적용합니다.

6. "정책" 페이지로 이동하고 다음 값이 포함된 정책을 생성합니다.

   "일반" 페이지

   이름

   SP Target Page Protection Policy(SP 대상 페이지 보호 정책)

   "사용자" 페이지

   SP LDAP 디렉터리의 경우 "구성원 추가"를 클릭합니다. 이 사용자가 대상에 액세스할 수 있도록 user1 을 추가합니다.

   "규칙" 페이지

   "SP Target Page Protection Rule"(SP 대상 페이지 보호 규칙) 추가

7. "제출"을 클릭합니다.

   대상 리소스에 대한 보호 정책이 완료되었습니다.

8. 관리 UI 를 종료합니다.

9. HTML 페이지를 사용하여 페더레이션 설정을 테스트합니다 (페이지 64).

SAML 2.0 싱글 사인온 테스트

SiteMinder 에서 SiteMinder 로의 네트워크에서 싱글 사인온을 테스트하려면 자체 HTML 페이지를 사용하십시오. 이 HTML 페이지는 AuthnRequest 서비스에 대한 하드 코드된 링크를 포함해야 합니다. 이 배포의 경우 POST 바인딩용 샘플 링크는 다음과 같습니다.

```
http://www.sp.demo:81/affwebservices/public/saml2authnrequest?ProviderID=idp.demo
```

AuthnRequest 서비스는 사용자를 링크에 지정된 아이덴티티 공급자로 리디렉션하여 사용자의 인증 컨텍스트를 검색합니다. 아이덴티티 공급자는 사용자를 인증하고 세션을 설정한 후 사용자를 서비스 공급자의 대상 리소스에 다시 연결합니다.

참고: Authnrequest 링크의 ProviderID 는 SP 의 SAML 인증 체계에 지정된 "IdP ID" 필드 값과 일치해야 합니다. "IdP ID" 필드는 "인증 체계 속성" 대화 상자의 "체계 설정" 탭에 있습니다.

페더레이션된 싱글 사인온을 테스트하려면

1. 브라우저를 엽니다.
2. 싱글 사인온을 트리거하기 위한 링크가 있는 웹 페이지의 URL 을 입력합니다.

   로그인 챌린지가 표시됩니다.
3. 사용자 저장소에 있는 기존 사용자의 로그인을 사용하여 사용자 자격 증명을 입력합니다. 예를 들어 사용자 저장소에 있는 사용자가 user1 인 경우 이 사용자의 자격 증명을 입력합니다.

   싱글 사인온이 성공하면 대상 페이지가 표시됩니다.
4. 싱글 사인온을 테스트한 후 페더레이션 배포에 기능 추가 (페이지 65)를 수행할 수 있습니다.

페더레이션 배포에 기능 추가

POST 싱글 사인온 구성을 완료한 후 페더레이션된 네트워크에 기능을 추가할 수 있습니다.

이 배포 예에서 다루는 추가 태스크는 다음과 같습니다.

- 싱글 로그아웃 구성
- 아티팩트 싱글 사인온 구성
- 어설션에 특성 추가
- 어설션의 디지털 서명이 사용되도록 설정
- 어설션 암호화 및 암호 해독

이러한 추가 기능 중 일부는 POST 바인딩에 대한 디지털 서명과 같은 프로덕션 환경의 싱글 사인온에 필요합니다. 필요한 태스크가 나와 있습니다.

싱글 로그아웃 구성

SLO(싱글 로그아웃 프로토콜)를 사용하면 특정 사용자의 모든 세션이 동시에 종료되므로 보안을 유지하는 데 도움이 됩니다. 이러한 세션과 로그아웃을 시작한 브라우저를 연결하십시오. 싱글 로그아웃이 반드시 사용자의 모든 세션을 종료하는 것은 아닙니다.

싱글 로그아웃을 구성하면 아이덴티티 공급자와 서비스 공급자가 싱글 로그아웃 프로토콜을 지원할 수 있습니다. 구성에 따라 싱글 로그아웃 처리 방법도 결정됩니다.

IdP 에서 싱글 로그아웃이 사용되도록 설정

IdP 에서 싱글 로그아웃을 시작할 수 있습니다. IdP 인 idp.demo 에서 SP 별로 싱글 로그아웃이 사용되도록 설정하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인하고 sp.demo 에 대한 SAML 서비스 공급자 개체에 액세스합니다.
2. "SAML 프로필" 페이지로 이동합니다.

3. "HTTP-리디렉션"을 선택합니다.

   나머지 필드가 활성화됩니다.

4. 다음 필드에 대한 값을 입력합니다.

   SLO 위치 URL

   http://www.sp.demo:81/affwebservices/public/saml2slo

   SP 의 SLO 서블릿을 정의합니다.

   SLO 확인 URL

   http://www.idp.demo:80/idpsample/SLOConfirm.jsp

5. 다른 필드의 경우 기본값을 적용합니다.
6. "제출"을 클릭합니다.
7. 정책 서버 관리 콘솔에 로그인하고 세션 저장소가 사용되도록 설정합니다.

   지침은 *정책 서버 관리 안내서*를 참조하십시오.

SP 에서 싱글 로그아웃이 사용되도록 설정

서비스 공급자에서 싱글 로그아웃을 시작할 수 있습니다.

다음 단계를 수행하십시오.

1. 보호된 리소스가 있는 영역이 영구 세션에 대해 구성되었는지 확인합니다.
2. "파트너 IDP.demo 인증 체계"라는 인증 체계로 이동합니다.
3. 체계가 "SLO" 탭에 액세스하도록 "SAML 2.0 구성"을 수정합니다.
4. "SLO" 탭에서 "HTTP-리디렉션"을 선택합니다.

   나머지 필드가 활성화됩니다.

5. 다음과 같이 필드에 데이터를 입력합니다.

   SLO 위치 URL

   http://www.idp.demo:80/affwebservices/public/saml2slo

   SLO 확인 URL

   http://www.sp.demo:81/spsample/SLOConfirm.jsp

6. 다른 모든 필드의 경우 기본값을 적용합니다.
7. 정책 서버 관리 콘솔에 로그인하고 세션 저장소가 사용되도록 설정합니다.

   지침은 *정책 서버 관리 안내서*를 참조하십시오.

싱글 로그아웃 테스트

싱글 로그아웃을 테스트하려면 자체 웹 페이지를 사용하십시오. SP 에서 시작되는 싱글 사인온을 테스트하기 위한 HTML 페이지에 싱글 로그아웃 서비스에 대한 하드 코드된 링크가 포함되어 있는지 확인하십시오.

싱글 사인온을 성공적으로 테스트한 후에 싱글 로그아웃을 테스트할 수 있습니다. 만든 시작 페이지에서 HTTP 리디렉션 바인딩을 사용하여 싱글 로그아웃 URL 로 브라우저를 디렉션하는 링크를 클릭하십시오.

SAML 2.0 아티팩트 싱글 사인온 구성

아이덴티티 공급자와 서비스 공급자에서 아티팩트 싱글 사인온 구성 태스크를 완료하십시오.

아이덴티티 공급자에 필요한 태스크는 다음과 같습니다.

- IdP 세션 저장소 설정 (페이지 68)
- IdP 웹 서버에 대해 SSL 이 사용되도록 설정 (페이지 69)
- 아티팩트 레졸루션 서비스 정책에 대한 액세스 허용
- IdP 에서 어설션을 저장하기 위해 영구 세션이 사용되도록 설정 (페이지 70)
- IdP 에서 아티팩트 바인딩 선택

서비스 공급자에 필요한 태스크는 다음과 같습니다.

- SP 의 인증서 데이터 저장소에 CA 인증서 추가
- SP 에서 아티팩트 바인딩이 사용되도록 설정
- 아티팩트 싱글 사인온 테스트 (페이지 74)

아티팩트 싱글 사인온을 위한 IdP 세션 저장소 설정

아티팩트 바인딩의 경우 IdP 에서 세션 저장소를 설정하고 사용되도록 설정하십시오. 아티팩트 바인딩을 사용하는 경우 세션 저장소는 아티팩트와 함께 검색되기 전에 어설션을 저장하는 데 필요합니다.

세션 저장소가 사용되도록 설정하려면

1. 세션 저장소 역할을 할 ODBC 데이터베이스를 설치하고 구성합니다. 이 배포에서는 Microsoft SQL Server 를 사용합니다.

   지침은 *정책 서버 설치 안내서*를 참조하십시오.
2. 정책 서버 관리 콘솔을 엽니다.
3. "데이터" 탭을 선택합니다.
4. "데이터베이스" 드롭다운 목록에서 "세션 서버"를 선택합니다.
5. 다음 필드를 작성하십시오.

   데이터 원본 정보

   SiteMinder Session Data Source

   사용자 이름

   admin

   암호

   dbpassword

   암호 확인

   dbpassword

   최대 연결 수

   16(기본값)
6. "Enable Session Server"(세션 서버 사용) 확인란을 선택합니다.
7. "확인"을 클릭하여 설정을 저장합니다.
8. 아티팩트 싱글 사인온용 IdP 웹 서버에 대해 SSL 이 사용되도록 설정합니다 (페이지 69).

아티팩트 싱글 사인온용 IdP 웹 서버에 대해 SSL 이 사용되도록 설정

웹 에이전트 옵션 팩이 설치된 웹 서버에 대해 SSL 이 사용되도록 설정하십시오. SSL 이 사용되도록 설정하면 어설션이 전달되는 백 채널이 안전해집니다.

다음 단계를 수행하십시오.

1. 서버 측 인증서 요청을 생성합니다.
2. 인증 기관이 서버 측 인증서에 서명하도록 합니다.
3. 웹 서버 구성에서 서버 측 인증서를 지정합니다.

   샘플 네트워크에 사용된 IIS 웹 서버의 경우 IIS 인증서 마법사가 사용됩니다.
4. IdP 에서 어설션을 저장하기 위해 영구 세션이 사용되도록 설정합니다.

아티팩트 레졸루션 서비스의 FWS 정책에 대한 액세스 허용

웹 에이전트 옵션 팩은 FWS(페더레이션 웹 서비스) 응용 프로그램을 설치합니다. 정책 서버를 웹 에이전트와 동일한 IdP 용으로 설치하면 FWS 응용 프로그램 내 서비스에 대한 여러 정책이 자동으로 생성됩니다. 이러한 정책 중 하나가 HTTP-아티팩트 싱글 사인온에 대한 아티팩트 레졸루션 서비스를 보호합니다.

이 아티팩트 레졸루션 정책의 보호를 적용하여 아티팩트 레졸루션 서비스에 액세스할 수 있는 신뢰 파트너를 지정하십시오.

IdP 에서 다음 단계를 수행하십시오.

1. 관리 UI 에 로그온합니다.
2. "인프라", "에이전트", "에이전트"를 차례로 클릭합니다.
3. "에이전트 만들기"를 클릭합니다.
4. "이름" 필드에 이 샘플 배포의 에이전트 이름인 "idp-webagent"를 입력합니다. "제출"을 클릭합니다.
5. "인프라", "에이전트 그룹"을 차례로 선택합니다.
6. "FederationWebServicesAgentGroup" 항목을 선택합니다.

   "에이전트 그룹" 대화 상자가 열립니다.
7. "추가/제거"를 클릭합니다. 그러면 "에이전트 그룹 구성원" 대화 상자가 열립니다.

8. "사용 가능한 구성원" 목록에서 "선택한 구성원" 목록으로 "idp-webagent"를 이동합니다.
9. "확인"을 클릭하여 "에이전트 그룹" 대화 상자로 돌아갑니다.
10. "제출", "닫기"를 차례로 클릭하여 기본 페이지로 돌아갑니다.
11. 다음과 같이 가맹 도메인 "Federation Sample Partners"(페더레이션 샘플 파트너)의 모든 서비스 공급자가 아티팩트 레졸루션 서비스에 액세스할 수 있도록 지정합니다.
    a. "인프라", "정책", "도메인", "도메인"을 차례로 선택합니다.
    b. "FederationWebServicesDomain"을 선택합니다.
    c. "정책" 탭을 선택하고 "수정"을 클릭합니다.
    d. "정책" 목록에서 "SAML2FWSArtifactResolutionServicePolicy" 항목 오른쪽의 "편집" 화살표를 클릭합니다.

       "정책" 대화 상자가 열립니다.
    e. "사용자" 탭에서 "SAML2FederationCustomUserStore" 디렉터리에 대해 "구성원 추가"를 선택합니다.

       "사용자/그룹" 대화 상자가 열립니다.
    f. 목록에서 "affiliate:FederationSamplePartners"를 선택하고 "확인"을 클릭합니다.
    g. "제출"을 클릭하여 변경을 완료합니다.

이제 아티팩트 레졸루션 서비스를 보호하는 정책이 적용되고 있습니다.

IdP 에서 어설션을 저장하기 위해 영구 세션이 사용되도록 설정

보호된 인증 URL(인증 URL 보호)이 포함된 영역에 대해 영구 세션이 사용되도록 설정하십시오. 영구 세션은 SAML 아티팩트 바인딩에 대한 어설션을 저장하는 데 필요합니다.

인증 URL 을 보호할 때 영구 세션이 사용되도록 설정하지 않았으면 지금 사용되도록 설정하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "인프라", "도메인", "도메인"으로 이동합니다.
3. 인증 URL 영역에 대한 도메인에 액세스합니다.

4. "영역" 페이지에서 인증 URL 이 포함된 영역을 선택하고 수정합니다.
5. "세션" 섹션에서 "영구"를 선택합니다.
6. "확인"을 클릭합니다.
7. IdP 에서 아티팩트 바인딩을 선택합니다.

IdP 에서 아티팩트 바인딩 선택

아티팩트 싱글 사인온의 경우 아티팩트 바인딩이 사용되도록 설정하십시오.

다음 단계를 수행하십시오.

1. "페더레이션", "레거시 페더레이션", "SAML 서비스 공급자"를 차례로 클릭합니다.
2. "sp.demo"를 선택하여 이 파트너에 대한 설정에 액세스합니다.
3. "수정"을 클릭하고 "SAML 프로필" 페이지를 선택합니다.
4. 다음 필드를 완성합니다.

   대상자

   sp.demo

   이 값은 서비스 공급자에 있는 값과 일치해야 합니다.

   어설션 소비자 서비스

   ```
   http://www.sp.demo:81/affwebservices/public/
   saml2assertionconsumer
   ```

   인증 수준, 유효 기간, AuthnContext 클래스 참조

   기본값을 적용합니다.

   테스트 환경에서 다음 메시지가 정책 서버 추적 로그에 표시되는 경우 "유효 기간" 값을 60(기본값)보다 크게 늘릴 수 있습니다.

   ```
   Assertion rejected (_b6717b8c00a5c32838208078738c05ce6237) – current time
   (Fri Sep 09 17:28:33 EDT 2005) is after SessionNotOnOrAfter time (Fri Sep 09
   17:28:20 EDT 2005)
   ```

5. "아티팩트 바인딩" 섹션에서 "HTTP-아티팩트"를 선택합니다.

6. "아티팩트 인코딩" 필드에서 "URL"을 선택합니다.

   아티팩트가 URL 로 인코딩된 쿼리 문자열에 추가됩니다.

7. "특성" 페이지로 이동합니다.
8. "백 채널" 섹션의 다음 필드에 데이터를 입력합니다.

   암호

   smfederation

   암호 확인

   smfederation

   아이덴티티 공급자는 이 암호를 백 채널을 통한 보안 통신에 사용합니다.

9. "제출"을 클릭합니다.
10. SP 의 인증서 데이터 저장소에 CA 인증서를 추가합니다.

SP 에서 SSL 백 채널에 대한 CA 인증서 추가

아티팩트 싱글 사인온의 경우 "SSL 을 통한 기본 인증"이 아티팩트 레졸루션 서비스를 보호하는 인증 체계이면 서비스 공급자의 인증서 데이터 저장소에 인증서를 추가하십시오.

인증서 데이터 저장소에는 서비스 공급자와 아이덴티티 공급자 간의 SSL 연결을 설정하는 인증 기관 인증서가 저장됩니다. 인증서는 어설션이 전송될 때 통과하는 백 채널의 보안을 유지합니다. 트러스트된 기관이 SSL 연결을 보호하고 있음을 서비스 공급자가 알도록 아티팩트 레졸루션 서비스를 보호하고 백 채널의 보안을 유지하십시오.

일반 루트 및 중간 CA 집합이 SiteMinder 에 포함되어 있습니다. 인증서 데이터 저장소에 없는 CA 인증서를 사용하려면 해당 CA 인증서를 가져오십시오.

이 배포의 경우 별칭은 sampleAppCertCA 이고 CA 인증서는 docCA.crt 입니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "인프라", "X509 인증서 관리", "인증 기관"을 차례로 클릭합니다.

3. "새로 가져오기"를 클릭합니다.

   참고: "도움말"을 클릭하면 필드, 컨트롤 및 해당되는 각 요구 사항에 대한 설명을 볼 수 있습니다.

4. "파일 선택" 단계에서 "docCA.crt"를 선택합니다.

   마법사가 "암호" 단계를 건너뜁니다.

5. "항목 선택" 단계의 "별칭" 열에 "sampleAppCertCA"를 입력합니다.

6. "확인" 단계에서 인증서 정보를 검토하고 "마침"을 클릭합니다.

   CA 인증서를 인증서 데이터 저장소로 가져왔습니다. 변경 내용은 가져오기가 완료된 직후 적용됩니다.

7. SP 에서 SAML 인증에 대해 아티팩트 바인딩이 사용되도록 설정합니다.

중요! 시스템이 사용하는 다른 인증서의 트러스트 체인에 속한 CA 인증서는 삭제할 수 없습니다. 사용 중인 CA 인증서를 삭제하려고 하면 인증서를 삭제할 수 없다는 오류 메시지가 표시됩니다.

서비스 공급자에서 아티팩트 바인딩이 사용되도록 설정

서비스 공급자에서 SAML 인증 체계에 대한 싱글 사인온 바인딩을 구성하십시오. 이 구성은 서비스 공급자에게 아이덴티티 공급자와 통신하는 방법을 지시합니다.

다음 단계를 수행하십시오.

1. "인프라", "인증", "인증 체계"를 차례로 클릭합니다.
2. "파트너 IDP.demo 인증 체계"를 선택합니다. 이 인증 체계는 기본 구성에 대해 생성한 것입니다.
3. "수정", "SAML 2.0 구성", "SSO" 탭을 차례로 선택합니다.
4. "레졸루션 서비스" 필드에 다음 값을 입력합니다.

   https:/www.idp.demo:443/affwebservices/saml2artifactresolution

5. "암호화 및 서명" 페이지로 이동합니다.
6. "백 채널" 섹션의 다음 필드에 데이터를 입력합니다.

   인증

   기본

   SP 이름

   sp.demo

암호

smfederation

암호 확인

smfederation

암호는 아이덴티티 공급자의 암호와 일치해야 합니다. 이 암호를 사용하면 백 채널을 통해 아이덴티티 공급자의 아티팩트 레졸루션 서비스에 안전하게 액세스할 수 있습니다.

7. "확인"을 클릭합니다.
8. SP 에서 시작되는 아티팩트 싱글 사인온을 테스트합니다 (페이지 74).

아티팩트 싱글 사인온 테스트

자체 웹 페이지를 사용하여 SiteMinder 에서 SiteMinder 로의 네트워크에서 싱글 사인온을 테스트하십시오.

자체 HTML 페이지는 AuthnRequest 서비스에 대한 하드 코드된 링크를 포함해야 합니다. 이 배포의 경우 아티팩트 바인딩용 링크는 다음과 같습니다.

```
http://<server:port>/affwebservices/public/saml2authnrequest?ProviderID=
IdP_ID&ProtocolBinding=urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact
```

server:port

SP 에서 웹 에이전트 옵션 팩이 설치된 서버의 이름과 포트를 정의합니다.

IdP_ID

공급자 ID 를 정의합니다.

이 배포의 링크는 다음과 같습니다.

```
http://www.sp.demo:81/affwebservices/public/saml2authnrequest?ProviderID=
idp.demo&ProtocolBinding=urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact
```

링크가 포함된 HTML 원본 파일은 다음 예와 유사합니다.

```
<a
href="http://www.sp.demo:81/affwebservices/public/saml2authnrequest?ProviderI
D=
idp.demo&ProtocolBinding=urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact">
Link for ARTIFACT Single Sign-on</a>
```

AuthnRequest 서비스는 사용자를 링크에 지정된 아이덴티티 공급자로 리디렉션하여 사용자의 인증 컨텍스트를 검색합니다. 아이덴티티 공급자는 사용자를 인증하고 세션을 설정한 후 사용자를 서비스 공급자의 대상 리소스에 다시 연결합니다.

참고: Authnrequest 링크의 ProviderID 는 SP 의 SAML 인증 체계에 있는 "IdP ID" 필드 값과 일치해야 합니다. "IdP ID" 필드는 "인증 체계 속성" 대화 상자의 "체계 설정" 탭에 있습니다.

이제 SP 에서 시작되는 싱글 사인온 테스트 (페이지 64) 단계를 따릅니다.

어설션에 특성 포함

사용자 저장소 기록의 특성을 SAML 어설션에 추가하여 사용자를 식별할 수 있습니다. 특성이 대상 리소스에 대한 액세스를 요청하고 있는 특정 사용자에 대한 아이덴티티 공급자의 사용자 저장소에 있어야 합니다.

이 배포의 경우 사용자 레코드에 있는 givenname 을 나타내는 user1 에 대한 특성을 추가하십시오.

아이덴티티 공급자에서 다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "페더레이션", "레거시 페더레이션", "SAML 서비스 공급자"를 차례로 클릭합니다.
3. "sm.demo"를 선택합니다.
4. "수정"을 클릭하고 "특성" 페이지로 이동합니다.

5. "특성" 섹션에서 "추가"를 클릭합니다.
6. "특성 추가" 대화 상자의 다음 필드에 데이터를 입력합니다.

   특성 유형

   지정되지 않음(기본값)

   특성 종류

   사용자 특성

   변수 이름

   firstname

   특성 이름

   givenname

   givenname 은 user1 의 프로필에 있는 특성입니다.
7. "확인"을 클릭하여 변경 내용을 저장하고 "특성" 페이지로 돌아갑니다.
8. "제출"을 클릭합니다.

디지털 서명 및 확인 구성

SAML 2.0 POST 싱글 사인온의 경우 아이덴티티 공급자가 SAML 응답에 서명해야 합니다. 아이덴티티 공급자의 구성 태스크는 디지털 서명이 사용되도록 설정합니다. 서비스 공급자의 구성 태스크는 서명 확인이 사용되도록 설정합니다.

중요! 프로덕션 환경에서 서명 처리는 필수 보안 요구 사항입니다.

- 아이덴티티 공급자에서 서명이 사용되도록 설정 (페이지 76)
- 서비스 공급자에서 서명 확인이 사용되도록 설정 (페이지 77)

아이덴티티 공급자에서 서명이 사용되도록 설정

POST 바인딩에 대한 SAML 어설션에 서명하는 키와 인증서는 인증서 데이터 저장소에 저장됩니다. SAML 응답에 서명해야 하므로 적절한 키/인증서 쌍이 아이덴티티 공급자의 인증서 데이터 저장소에 포함되어 있어야 합니다.

자동으로 설치되는 키/인증서 쌍을 사용하여 샘플 응용 프로그램을 배포하십시오. 새 키/인증서 쌍을 가져오려면 다음 절차를 완료하십시오.

개인 키/인증서 쌍을 가져오려면

1. 관리 UI 에 로그인합니다.
2. "인프라", "X509 인증서 관리", "트러스트된 인증서 및 개인 키"로 이동합니다.
3. 개인 키/인증서 "idp.demo"를 인증서 데이터 저장소로 가져옵니다.

   idp.demo 는 SAML 응답에 서명합니다.
4. "페더레이션", "레거시 페더레이션", "SAML 서비스 공급자"를 차례로 선택합니다.
5. 서비스 공급자 "sp.demo"를 선택하고 "암호화 및 서명" 탭으로 이동합니다.
6. "서명 처리 사용 안 함" 확인란을 선택 취소합니다. 이 확인란을 선택 취소하면 서명 처리가 사용되도록 설정됩니다.
7. 다음 필드를 작성하십시오.

   서명 별칭

   개인 키/인증서 쌍을 가져올 때 지정한 별칭을 입력합니다.

   서명 알고리즘

   RSAwithSHA1(기본값)

   POST 서명 옵션

   서명 어설션(기본값)
8. "제출"을 클릭합니다.

서비스 공급자에서 서명 유효성 검사가 사용되도록 설정

POST 싱글 사인온의 경우 아이덴티티 공급자가 SAML 어설션에 디지털로 서명해야 합니다. 따라서 서비스 공급자가 서명의 유효성을 검사해야 합니다.

디지털 서명의 유효성을 검사하려면

- 인증서(공개 키)를 인증서 데이터 저장소로 가져옵니다.
- 발급자의 DN 과 인증서의 일련 번호를 지정합니다.

공개 키를 가져오려면

1. 관리 UI 에서 "인프라", "X509 인증서 관리", "트러스트된 인증서 및 개인 키"로 이동합니다.

2. 공개 키/인증서 쌍을 인증서 데이터 저장소에 추가합니다. 이 배포에서 인증서는 post-cert.crt 입니다.

   키/인증서 쌍이 데이터 저장소에 추가됩니다.

3. "제출"을 클릭합니다.
4. "인프라", "인증", "인증 체계"로 이동합니다.
5. SAML 2.0 인증 체계인 "파트너 IdP.demo 인증 체계"를 선택합니다.
6. "암호화 및 서명" 탭을 선택합니다.
7. "D-서명 정보" 섹션에서 "서명 처리 사용 안 함" 확인란을 선택 취소하여 서명 처리가 사용되도록 설정합니다.
8. 다음 필드 값을 지정합니다.

   발급자 DN

   CN=Certificate Manager,OU=IAM,O=CA.COM

   일련 번호

   008D 8B6A D18C 46D8 5B

   D-서명 정보를 사용하면 서비스 공급자가 SAML 응답 서명을 확인할 수 있습니다. "발급자 DN"과 "일련 번호"에 대한 값은 서비스 공급자의 인증서 데이터 저장소에 저장된 인증서에서 가져옵니다.

9. "확인"을 클릭합니다.

   이제 유효성 검사 구성이 완료되었습니다.

10. POST 싱글 사인온을 테스트합니다.

어설션 암호화 및 암호 해독

보안을 강화하기 위해 어설션을 암호화할 수 있습니다. 암호화는 기본 싱글 사인온 네트워크를 구성한 후에 수행할 수 있는 선택적 태스크입니다.

아이덴티티 공급자는 서비스 공급자가 어설션의 암호를 해독하는 데 사용하는 개인 키/인증서 쌍에 해당하는 인증서로 어설션을 암호화합니다.

아이덴티티 공급자와 서비스 공급자에서 구성 태스크를 수행할 수 있습니다.

- 아이덴티티 공급자에서 암호화가 사용되도록 설정 (페이지 79)
- 서비스 공급자에서 암호 해독이 사용되도록 설정 (페이지 80)

IdP 에서 어설션 암호화가 사용되도록 설정

이 배포에서 sp_encrypt.crt 는 암호화용 인증서입니다.

IdP 에서 암호화가 사용되도록 설정하려면

1. 관리 UI 에 로그인합니다.
2. "인프라", "X509 인증서 관리", "트러스트된 인증서 및 개인 키"로 이동합니다.
3. sp-encrypt.crt 인증서를 인증서 데이터 저장소로 가져옵니다.
4. "페더레이션", "레거시 페더레이션", "SAML 서비스 공급자"로 이동합니다.
5. "sp.demo"를 선택합니다.
6. "수정", "SAML 2.0 구성"을 차례로 선택합니다.
7. "암호화 및 서명" 탭으로 이동합니다.
8. "어설션 암호화"를 선택합니다.
9. "암호화 블록 알고리즘"과 "암호화 키 알고리즘"에서 기본값을 적용합니다.
10. "발급자 DN"에 인증서 발급자를 입력합니다. 이 배포에서 DN 은 다음과 같습니다.

    CN=Doc Certificate Authority, OU=Doc, O=CA.COM

    참고: "발급자 DN" 필드에 입력하는 값은 인증서 데이터 저장소에 있는 인증서의 발급자 DN 과 일치해야 합니다. DN 을 확인하여 입력하는 값이 일치하는 값인지 확인합니다.
11. "일련 번호" 필드에 인증서 데이터 저장소에 있는 인증서의 일련 번호를 입력합니다. 이 배포에서 값은 00EFF6AFB49925C3F4 입니다.

    이 숫자는 16 진수여야 합니다.
12. "확인"을 클릭하여 변경 내용을 저장합니다.
13. SP 에서 암호화된 어설션의 암호를 해독합니다.

SP 에서 어설션 암호 해독이 사용되도록 설정

어설션이 아이덴티티 공급자에서 암호화된 경우 서비스 공급자는 인증서 데이터 저장소에 개인 키와 해당 인증서를 가지고 있어야 합니다.

어설션의 암호를 해독하기 위한 개인 키/인증서 쌍을 가지고 있는 경우 서비스 공급자는 아이덴티티 공급자에서 암호화된 어설션을 수락합니다.

참고: "암호화된 어설션 필요" 기능이 사용되도록 설정하지 않아도 암호화된 어설션이 서비스 공급자에서 수락됩니다.

다음 단계를 수행하십시오.

1. 명령 창을 엽니다.
2. "인프라", "X509 인증서 관리", "트러스트된 인증서 및 개인 키"로 이동합니다.
3. 개인 키/인증서 쌍 "sp-encrypt.crt"를 인증서 데이터 저장소에 추가합니다. 이 쌍에 대한 별칭은 sp1privkey 입니다. 개인 키에 대한 암호는 fedsvcs 입니다.
4. 싱글 사인온을 테스트합니다. 다음 중 하나로 이동합니다.
   - SAML 2.0 POST 싱글 사인온 테스트
   - 아티팩트 싱글 사인온 테스트

제 3 장: SiteMinder Federation 설정 개요

이 섹션은 다음 항목을 포함하고 있습니다.

페더레이션 설정 개요

이 개요에서는 페더레이션된 네트워크 설정에 대해 간략하게 설명합니다.

각 절차의 단계는 어설션을 생성하는 당사자와 어설션을 소비하는 당사자의 태스크로 나뉘어집니다. 이 구성 내에서 절차는 각 사이트의 정책 서버 및 웹 에이전트 태스크로 추가로 나뉘어집니다.

일반적인 목적에 따라 본 안내서에서는 어설션 당사자와 신뢰 당사자라는 용어를 사용하여 페더레이션된 관계의 양쪽 당사자를 식별합니다.

어설션을 생성하는 당사자를 *어설션 당사자*라고 합니다. 어설션 당사자는 다음 파트너 중 하나일 수 있습니다.

- SAML 1.x 생산자
- SAML 2.0 아이덴티티 공급자
- WS-페더레이션 계정 파트너

인증 목적으로 어설션을 소비하는 당사자를 *신뢰 당사자*라고 합니다. 신뢰 당사자는 다음 파트너 중 하나일 수 있습니다.

- SAML 1.x 소비자
- SAML 2.0 서비스 공급자
- WS-Federation 리소스 파트너

참고: 모든 설치 태스크를 먼저 수행한 다음 관리 UI 를 통해 소프트웨어 구성을 완료할 수 있습니다.

이러한 절차에서는 최신 SiteMinder 릴리스를 참조합니다. 릴리스에 대한 버전 정보는 "Platform Matrix"(플랫폼 지원표)를 참조하십시오.

"Platform Support Matrix"(플랫폼 지원표)를 찾으려면

1. 기술 지원 사이트에 로그온합니다.
2. "Platform Support Matrix"(플랫폼 지원표)를 검색합니다.

다음 정보를 확인하십시오.

- 이 제품은 동일한 쿠키 도메인을 사용하는 두 시스템 간의 페더레이션을 지원하지 않습니다.
- 레거시 페더레이션은 핵심 SiteMinder 와는 별개로 라이선스가 부여됩니다.

설치 개요 절차의 명명 규칙

다음 변수가 설치 및 구성 절차에 사용됩니다.

web_agent_home

웹 에이전트가 설치된 위치를 지정합니다.

policy_server_home

정책 서버가 설치된 위치를 지정합니다.

web_server_home

웹 서버가 설치된 위치를 나타냅니다.

fqhn

정규화된 호스트 이름을 지정합니다.

port_number

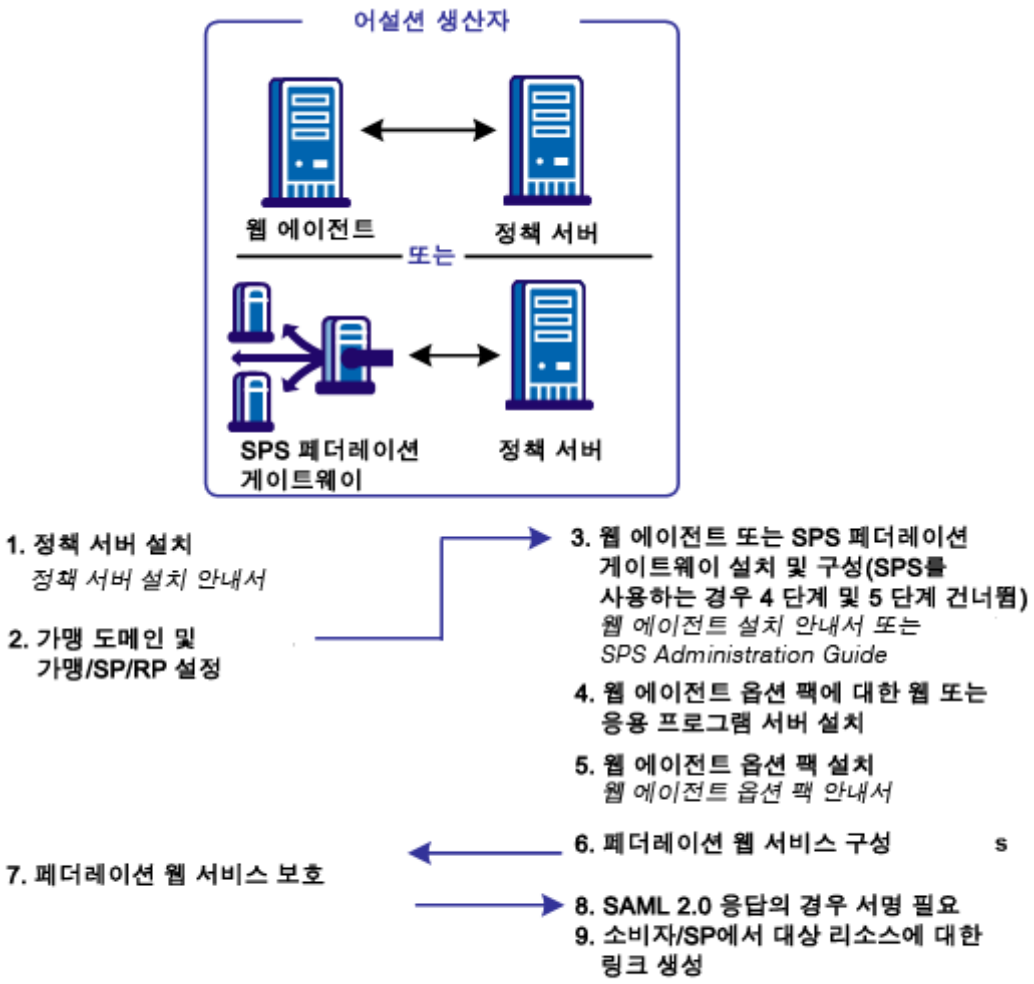
서버의 포트 번호를 지정합니다.

sps_home

CA SiteMinder for Secure Proxy Server 가 설치된 위치를 지정합니다.

어설션 당사자 구성 요소 설정

다음 그림에서는 SAML 1.x 생산자, SAML 2.0 아이덴티티 공급자 또는 WS-페더레이션 계정 파트너 설정을 보여 줍니다.



참고: SPS 페더레이션 게이트웨이가 페더레이션 웹 서비스 응용 프로그램 기능을 제공하기 위해 웹 에이전트 및 웹 에이전트 옵션 팩을 대체할 수 있습니다. SPS 페더레이션 게이트웨이 설치 및 구성에 대한 자세한 내용은 *Secure Proxy Server Administration Guide*(보안 프록시 서버 관리 안내서)를 참조하십시오.

어설션 당사자 정책 서버 설치

어설션 당사자 측에서의 설정은 다음과 같습니다.

1. 정책 서버를 설치합니다.

   *정책 서버 설치 안내서*를 참조하십시오.

2. 아티팩트 싱글 사인온에 대해서만 세션 저장소와 해당 데이터베이스를 설정합니다.

   세션 저장소에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

   세션 저장소는 세션 서버가 어설션을 저장한 후에 검색되므로 아티팩트 싱글 사인온에만 필요합니다.

3. 정책 서버에 사용할 정책 저장소를 설정합니다. 지침은 *정책 서버 설치 안내서*를 참조하십시오.

4. 사용자 디렉터리는 *정책 서버 구성 안내서*의 지침을 따라 설정하십시오.

   이 사용자 디렉터리에는 생성하는 어설션의 대상이 되는 사용자가 포함되어 있어야 합니다.

5. (선택 사항) 어설션 당사자와 신뢰 당사자 간의 통신을 보려면 정책 서버에 대해 오류 및 추적 로깅이 사용되도록 설정합니다.

가맹 도메인을 설정하고 해당 도메인에 사이트 추가

페더레이션 웹 서비스를 설정하기 전에 가맹 도메인을 설정하고 가맹 도메인에 어설션을 소비하는 사이트를 추가합니다. 가맹 도메인은 어설션을 생성하는 사이트에 대해 파트너를 식별합니다.

어설션 당사자 측에서 다음을 수행하십시오.

1. 관리 UI 에 액세스합니다.
2. 가맹 도메인을 생성합니다.
3. 어설션 당사자(생산자, IdP, AP)가 어설션을 생성하는 사용자에 대한 사용자 저장소를 추가합니다.
4. 가맹 도메인에 각 신뢰 당사자(소비자, SP, RP)에 대한 개체를 추가합니다.

   신뢰 당사자와 도메인에 추가된 각 개체 간에 일대일 대응 관계가 있어야 합니다.

5. 가맹 도메인에 사이트를 추가한 후 인증 URL 이 보호되는지 확인합니다. 이 확인에서는 페더레이션된 리소스에 대한 요청을 처리하기 전에 사용자 세션이 어설션 당사자에 있는지 확인합니다.

   이 태스크를 수행하려면

   a. 정책 도메인을 생성합니다.

   b. 웹 에이전트로 정책 도메인을 보호합니다. 웹 에이전트 옵션 팩이 있는 서버를 보호하고 있는 웹 에이전트를 사용합니다.

   c. 이 정책 도메인에 인증 URL 을 보호하는 영역, 규칙 및 정책을 추가합니다.

추가 정보:

SiteMinder 세션이 없는 사용자 인증(SAML 1.x) (페이지 133)

어설션 당사자에서 웹 에이전트 또는 SPS 페더레이션 게이트웨이 설치

웹 에이전트는 SiteMinder Federation 네트워크의 필수 구성 요소입니다. 웹 서버에 웹 에이전트를 설치하거나 포함된 웹 에이전트가 있는 SPS 페더레이션 게이트웨이를 설치하십시오.

어설션 당사자에서 다음 구성 요소를 설정하십시오.

1. 다음 구성 요소 중 하나를 설치합니다.
   - 웹 에이전트

     지침은 *웹 에이전트 설치 안내서*를 참조하십시오.
   - SPS 페더레이션 게이트웨이

     지침은 *Secure Proxy Server Administration Guide*(보안 프록시 서버 관리 안내서)를 참조하십시오.
2. 아티팩트 싱글 사인온의 경우 웹 에이전트가 설치된 웹 서버나 SPS 페더레이션 게이트웨이가 있는 시스템에서 SSL 이 사용되도록 설정합니다.

웹 에이전트 옵션 팩용 응용 프로그램 서버 설치(어설션 당사자)

웹 에이전트 및 웹 에이전트 옵션 팩이 있는 레거시 페더레이션을 구현하고 있는 경우 웹 에이전트 옵션 팩을 설치하십시오. 웹 또는 응용 프로그램 서버에 이 구성 요소를 설치하십시오.

어설션 당사자 측에서 다음을 수행하십시오.

1. 웹 에이전트 옵션 팩과 함께 설치된 응용 프로그램인 페더레이션 웹 서비스를 실행하려면 다음 서버 중 하나를 설치합니다.
   - ServletExec 를 실행하는 웹 서버
   - WebLogic 응용 프로그램 서버
   - WebSphere 응용 프로그램 서버
   - JBoss 응용 프로그램 서버
   - Tomcat 응용 프로그램 서버
2. 이러한 시스템에 페더레이션 웹 서비스를 배포합니다.
3. 아티팩트 싱글 사인온의 경우 웹 에이전트 옵션 팩이 설치된 웹 서버에서 SSL 이 사용되도록 설정합니다.

어설션 당사자 웹 에이전트 옵션 팩 설치

웹 에이전트 옵션 팩은 SiteMinder 레거시 페더레이션에 대한 필수 구성 요소인 페더레이션 웹 서비스 응용 프로그램을 제공합니다.

어설션 당사자 측에서 다음을 수행하십시오.

1. 웹 에이전트 옵션 팩을 설치합니다.

   지침은 *웹 에이전트 옵션 팩 안내서*를 참조하십시오.

2. JDK 를 설치했는지 확인합니다. 웹 에이전트 옵션 팩에는 JDK 가 필요합니다.

   지원되는 JDK 버전을 보려면 기술 지원 사이트에 로그온하고 릴리스에 대한 "SiteMinder Platform Support Matrix"(SiteMinder 플랫폼 지원표)를 검색하십시오.

참고: SPS 페더레이션 게이트웨이가 페더레이션 웹 서비스 응용 프로그램 기능을 제공하기 위해 웹 에이전트 및 웹 에이전트 옵션 팩을 대체할 수 있습니다. SPS 페더레이션 게이트웨이 설치 및 구성에 대한 자세한 내용은 *Secure Proxy Server Administration Guide*(보안 프록시 서버 관리 안내서)를 참조하십시오.

페더레이션 웹 서비스(어설션 당사자) 구성

페더레이션 웹 서비스 응용 프로그램은 웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이가 있는 서버에 설치됩니다.

어설션 당사자 측에서 페더레이션 웹 서비스를 구성하려면

1. 웹 에이전트 옵션 팩을 사용하도록 지원되는 응용 프로그램 서버 중 하나를 구성합니다. 웹 에이전트 옵션 팩 배포 지침을 참조하십시오.

   SPS 페더레이션 게이트웨이에는 페더레이션 웹 서비스가 이미 배포되어 있습니다.

2. AffWebServices.properties 파일에 있는 AgentConfigLocation 매개 변수가 WebAgent.conf 파일의 전체 경로로 설정되어 있는지 확인합니다. 구문이 올바르고 경로가 파일에 한 줄로 나타나는지 확인합니다.

   AffWebServices.properties 파일에는 페더레이션 웹 서비스에 대한 초기화 매개 변수가 포함되어 있습니다. 이 파일은 다음 디렉터리 중 하나에 있습니다.

   - *web_agent_home*/affwebservices/WEB-INF/classes
   - *sps_home*/secure-proxy/Tomcat/webapps/affwebservices/WEB-INF/classes

   web_agent_home

   웹 에이전트가 설치된 위치를 나타냅니다.

   sps_home

   SPS 페더레이션 게이트웨이가 설치된 위치를 나타냅니다.

3. 페더레이션 웹 서비스 응용 프로그램에 대해 오류 및 추적 로깅이 사용되도록 설정합니다. LoggerConfig.properties 파일에서 로깅이 사용되도록 설정합니다. 로그를 통해 어설션 당사자와 신뢰 당사자 간의 통신을 볼 수 있습니다.

   - 오류 로깅은 기본 오류 로그 파일인 affwebserv.log 파일에 기록됩니다.
   - 추적 로깅은 기본 추적 로그 파일인 FWSTrace.log 파일에 기록됩니다.

4. 웹 브라우저를 열고 다음 링크를 입력하여 페더레이션 웹 서비스를 테스트합니다.

   http://*fqhn*:*port_number*/affwebservices/assertionretriever

   fqhn

   정규화된 호스트 이름을 정의합니다.

   port_number

   페더레이션 웹 서비스 응용 프로그램이 설치된 서버의 포트 번호를 정의합니다.

예를 들면 다음과 같습니다.

http://myhost.ca.com:81/affwebservices/assertionretriever

페더레이션 웹 서비스가 올바로 작동하면 다음과 같은 메시지가 표시됩니다.

어설션 검색 서비스를 초기화했습니다.
요청된 서블릿은 HTTP POST 요청만 수락합니다.

이 메시지는 페더레이션 웹 서비스가 데이터 작업을 수신 대기하고 있음을 나타냅니다. 페더레이션 웹 서비스가 올바로 작동하고 있지 않으면 어설션 검색 서비스가 실패했다는 메시지가 표시됩니다. 테스트가 실패한 경우 페더레이션 웹 서비스 로그를 살펴보십시오.

페더레이션 웹 서비스에 대한 액세스 허용(어설션 당사자)

정책 서버를 설치하면 SiteMinder 가 FWS(페더레이션 웹 서비스) 응용 프로그램에 대한 정책을 생성합니다. FWS 응용 프로그램은 웹 에이전트 옵션 팩과 함께 설치됩니다. 일부 페더레이션 기능의 경우 신뢰 당사자에게 보호된 FWS 서비스에 액세스할 수 있는 권한이 있어야 합니다. 정책에 신뢰 파트너를 추가하는 태스크는 어설션 당사자 측에서만 수행됩니다.

예를 들어 싱글 사인온에 대한 HTTP-아티팩트 바인딩의 경우 SiteMinder 가 어설션을 검색하는 서비스가 정책으로 보호됩니다. SiteMinder 가 특정 신뢰 파트너에 대한 어설션을 검색하려면 해당 파트너가 서비스를 보호하는 정책에 사용자로 추가되어 있어야 합니다.

페더레이션 파트너 관계에 대해 구성된 기능에 적용되는 특정 FWS 정책에 대한 액세스 권한을 부여 (페이지 125)하십시오.

SAML POST 응답 서명이 사용되도록 설정

SAML POST 응답 서명은 SAML 사양 요구 사항입니다. SAML POST 응답에 서명하려면 어설션 당사자의 인증서 데이터 저장소에 개인 키와 인증서를 추가하십시오.

키와 인증서를 데이터 저장소로 가져오는 방법에 대한 지침은 *정책 서버 구성 안내서*를 참조하십시오.

대상 리소스에 대한 링크 생성(선택 사항)

다음 중 하나로 이동합니다.

- SAML 1.x 싱글 사인온을 위한 링크 (페이지 90)
- 아이덴티티 공급자에서 SAML 2.0 싱글 사인온을 위한 링크 (페이지 91)
- WS-페더레이션 싱글 사인온을 시작하기 위한 링크 (페이지 92)

생산자에서 SAML 1.x 싱글 사인온 시작

SAML 1.x 생산자에서 사용자를 소비자 사이트에 연결하는 링크가 포함된 페이지를 생성하십시오. 각 링크는 사이트 간 전송 URL 을 나타냅니다. 사용자가 생산자 측 웹 에이전트에 요청을 보내는 사이트 간 전송 URL 을 방문해야 합니다. 그러면 사용자가 소비자 사이트로 리디렉션됩니다.

사용자가 생산자에서 선택하는 링크에는 특정 쿼리 매개 변수가 포함되어 있어야 합니다. 이러한 매개 변수는 생산자 웹 에이전트에 대한 HTTP GET 요청의 일부입니다.

SAML 아티팩트 프로필의 경우 사이트 간 전송 URL 구문은 다음과 같습니다.

```
http://producer_site/affwebservices/public/intersitetransfer?SMASSERTIONREF=
QUERY&NAME=affiliate_name&TARGET=http://consumer_site/target_url?query_parame
ter_name%3Dquery_parameter_value%26query_parameter_name%3Dquery_parameter_val
ue&SMCONSUMERURL=http://consumer_site/affwebservices/public/samlcc&AUTHREQUIR
EMENT=2
```

producer_site

페더레이션 네트워크에 설치된 구성 요소에 따라 웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하는 시스템의 서버 및 포트 번호를 지정합니다.

consumer_site

페더레이션 네트워크에 설치된 구성 요소에 따라 웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하는 시스템의 서버 및 포트 번호를 지정합니다.

SAML POST 프로필의 경우 사이트 간 전송 URL 구문은 다음과 같습니다.

http://*producer_site*/affwebservices/public/intersitetransfer?SMASSERTIONREF=QUERY&NAME=*affiliate_name*&TARGET=http://*consumer_site/target_url*

producer_site

페더레이션 네트워크에 설치된 구성 요소에 따라 웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하는 시스템의 서버 및 포트 번호를 지정합니다.

consumer_site

페더레이션 네트워크에 설치된 구성 요소에 따라 웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하는 시스템의 서버 및 포트 번호를 지정합니다.

참고: SAML POST 프로필에서는 SMCONSUMERURL 및 AUTHREQUIREMENT 매개 변수를 사용하지 않습니다. 하지만 사이트 간 전송 URL 에 이러한 매개 변수 중 하나를 포함하는 경우에는 다른 매개 변수도 포함하십시오.

추가 정보:

소비자 리소스에 대한 링크 만들기(SAML 1.x) (페이지 161)

아이덴티티 공급자에서 SAML 2.0 싱글 사인온 시작

사용자가 서비스 공급자로 이동하기 전에 아이덴티티 공급자를 방문하는 경우(POST 또는 아티팩트 바인딩) 아이덴티티 공급자에서 원치 않는 응답을 시작하십시오. 원치 않는 응답을 시작하기 위해 페더레이션 웹 서비스 응용 프로그램과 어설션 생성기는 쿼리 매개 변수가 있는 HTTP Get 요청을 수락합니다. 이 쿼리 매개 변수는 IdP 가 응답을 생성하는 서비스 공급자 ID 를 나타냅니다.

SAML 2.0 아티팩트 또는 POST 프로필의 경우 링크 구문은 다음과 같습니다.

http://*IdP_server:port*/affwebservices/public/saml2sso?SPID=*SP_ID*

idp_server:port

웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하는 웹 서버와 포트를 식별합니다.

SP_ID

서비스 공급자 ID 값입니다. 엔터티 ID 는 대/소문자를 구분합니다. "관리 UI"에 표시되는 그대로 입력하십시오.

사용되도록 설정된 바인딩에 따라 이 링크에 ProtocolBinding 쿼리 매개 변수 (페이지 240)를 추가하십시오.

참고: 쿼리 매개 변수를 HTTP-인코딩할 필요는 없습니다.

서비스 공급자에서 싱글 사인온을 시작할 수도 있습니다.

추가 정보:

IdP 가 사용하는 원치 않는 응답 쿼리 매개 변수 (페이지 240)

계정 파트너에서 WS-페더레이션 싱글 사인온 시작

WS-페더레이션 싱글 사인온을 시작하려면 사용자가 하드 코드된 HTML 링크가 있는 페이지를 클릭합니다. 이 HTML 링크는 사용자의 브라우저를 계정 파트너의 싱글 사인온 서비스에 연결합니다. 그런 다음 계정 파트너가 사용자를 리소스 파트너로 리디렉션합니다.

싱글 사인온을 시작하는 링크는 모든 사이트에 포함될 수 있지만 항상 먼저 사용자를 계정 파트너에 연결해야 합니다.

링크 구문은 다음과 같습니다.

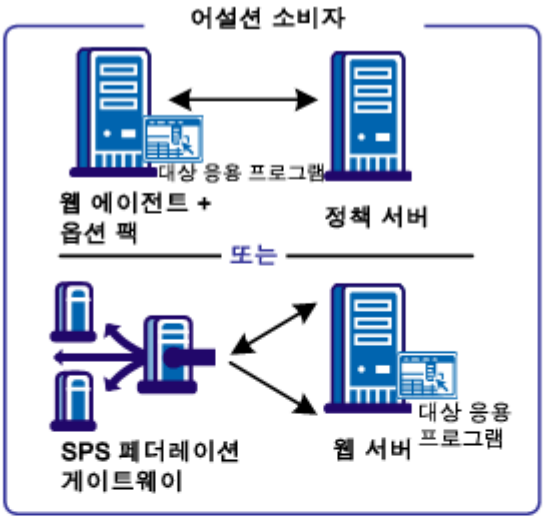
https://*AP:port*/affwebservices/public/wsfedsso?wa=wsignin1.0&wtrealm=*RP_ID*

ap_server:port

계정 파트너에 있는 시스템의 서버 및 포트 번호를 지정합니다. 시스템은 페더레이션 네트워크에 설치된 구성 요소에 따라 웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하고 있습니다.

참고: 쿼리 매개 변수를 HTTP-인코딩할 필요는 없습니다.

신뢰 당사자 구성 요소 설정



1. **정책 서버 설치**
   정책 서버 설치 안내서
2. **각 생산자/IdP/AP에 대한 SAML 인증 체계 구성**
3. **대상 리소스를 보호하는 영역, 규칙 및 정책 생성**
4. **웹 에이전트 또는 SPS 페더레이션 게이트웨이 설치 및 구성**
   웹 에이전트 설치 안내서 또는 SPS Administration Guide(SPS를 사용하는 경우 6 단계 및 7 단계 건너뜀)
5. **페더레이션 웹 서비스에 대한 웹 또는 응용 프로그램 서버 설치**
6. **웹 에이전트 옵션 팩 설치**
   웹 에이전트 옵션 팩 안내서
7. **페더레이션 웹 서비스 구성**
8. **페더레이션 웹 서비스 보호**
9. **아티팩트 SSO의 경우 인증서 데이터 저장소 설정**

별도로 명시되지 않은 경우 이 안내서의 구성 지침 참조

신뢰 당사자의 여러 정책 서버 및 웹 에이전트 설정 단계는 다음 예외를 제외하고 어설션 당사자의 경우와 유사합니다.

- 소비자, 서비스 공급자 또는 리소스 파트너를 구성하지 않습니다.
- 정책 서버에서 SAML 또는 WS-페더레이션 인증 체계를 구성합니다.

다음 그림에서는 SAML 1.x 소비자, SAML 2.0 서비스 공급자 또는 WS-페더레이션 리소스 파트너에 필요한 태스크를 보여 줍니다.

참고: 이 절차에서는 대상 리소스가 신뢰 당사자 웹 사이트에 있다고 가정합니다.

신뢰 당사자 정책 서버 설치

신뢰 당사자 사이트에 정책 서버를 설치하십시오. 정책 서버는 페더레이션 인증 체계, 어설션 생성기 등의 기능을 제공합니다.

자세한 내용은 *정책 서버 설치 안내서* 및 *정책 서버 구성 안내서*를 참조하십시오.

신뢰 당사자 측에서 다음을 수행하십시오.

1. 정책 서버를 설치합니다.
2. 정책 저장소를 설정합니다.

   중요! 새 정책 저장소를 초기화하면 정책 서버 설치 관리자가 ampolicy.smdif 파일에 있는 가맹 개체를 자동으로 가져옵니다. 이러한 개체는 페더레이션에 필요합니다. 기존 정책 저장소를 사용하는 경우 가맹 개체를 수동으로 가져오십시오. 가져오기가 성공했는지 확인하려면 관리 UI 에 로그인하고 "정책", "도메인", "도메인"으로 이동하십시오. 가져오기가 성공한 경우 목록에서 FederationWebServices 도메인 개체를 볼 수 있습니다.
3. 사용자 저장소를 설정하고 대상 리소스에 액세스하도록 허용된 사용자를 추가합니다.

SAML 또는 WS-페더레이션 인증 체계 구성

신뢰 당사자 정책 서버에서 각 어설션 당사자의 인증 체계(아티팩트, POST 프로필, SAML 2.0, WS-페더레이션)를 구성하십시오.

중요! 인증 체계에 대해 지정하는 파트너 이름은 어설션 당사자 측에서 지정하는 신뢰 당사자 이름과 일치해야 합니다.

구체적인 사항은 다음과 같습니다.

- SAML 1.x 인증 체계의 경우 체계 구성의 "가맹 이름" 필드는 생산자 사이트에 있는 가맹 개체의 가맹 이름과 일치해야 합니다.
- SAML 2.0 의 경우 해당 필드인 "SP ID"는 아이덴티티 공급자의 SP ID 와 일치해야 합니다.
- WS-페더레이션의 경우 체계 구성에 대한 리소스 파트너 ID 는 계정 파트너의 리소스 파트너 ID 와 일치해야 합니다.

추가 정보:

SAML 1.x 소비자로 구성 (페이지 165)
SAML 2.0 서비스 공급자 구성 (페이지 263)
SiteMinder 를 WS-페더레이션 리소스 파트너로 구성 (페이지 335)

신뢰 당사자 측에서 대상 리소스 보호

SAML 또는 WS-페더레이션 인증 체계를 생성한 후 해당 체계를 고유 영역이나 단일 사용자 지정 영역에 할당하십시오. 영역은 신뢰 당사자 측에서 사용자 액세스용 어설션이 필요한 대상 리소스를 수집한 것입니다. 신뢰 당사자는 다음 방법 중 하나로 대상 리소스를 식별합니다.

- 사이트 간 전송 URL 의 TARGET 변수(SAML 1.x)
- AuthnRequest URL(SAML 2.0 및 WS-페더레이션)
- 인증 체계 구성(SAML 2.0 및 WS-페더레이션)

영역을 생성하여 SAML 또는 WS-페더레이션 인증 체계를 할당한 후 영역에 대한 규칙을 생성하고 리소스를 보호하는 정책에 규칙을 추가하십시오.

웹 에이전트 또는 SPS 페더레이션 게이트웨이 설치(신뢰 당사자)

웹 에이전트는 SiteMinder 레거시 페더레이션 네트워크의 필수 구성 요소입니다. 웹 서버에 웹 에이전트를 설치하거나 포함된 웹 에이전트가 있는 SPS 페더레이션 게이트웨이를 설치할 수 있습니다.

신뢰 당사자 측에서 다음 구성 요소를 설정하십시오.

1. 다음 구성 요소 중 하나를 설치합니다.
   - 웹 에이전트

     지침은 *웹 에이전트 설치 안내서*를 참조하십시오.
   - SPS 페더레이션 게이트웨이

     지침은 *보안 프록시 서버 관리 안내서*를 참조하십시오.
2. 웹 에이전트 또는 SPS 페더레이션 게이트웨이를 구성합니다.

웹 에이전트 옵션 팩용 웹 또는 응용 프로그램 서버 설치(신뢰 당사자)

웹 에이전트 및 웹 에이전트 옵션 팩은 있고 SPS 페더레이션 게이트웨이는 없는 레거시 페더레이션을 구현하고 있는 경우 웹 에이전트 옵션 팩을 설치하십시오. 웹 또는 응용 프로그램 서버에 이 구성 요소를 설치하십시오.

신뢰 당사자 측에서 다음을 수행하십시오.

1. 웹 에이전트 옵션 팩과 함께 설치된 응용 프로그램인 페더레이션 웹 서비스를 실행하려면 다음 서버 중 하나를 설치합니다.
   - ServletExec 를 실행하는 웹 서버
   - WebLogic 응용 프로그램 서버
   - WebSphere 응용 프로그램 서버
   - JBoss 응용 프로그램 서버
   - Tomcat 응용 프로그램 서버
2. 이러한 시스템에 페더레이션 웹 서비스를 배포합니다.

신뢰 당사자 측에서 웹 에이전트 옵션 팩 설치

웹 에이전트 옵션 팩은 레거시 페더레이션에 대한 필수 구성 요소인 페더레이션 웹 서비스 응용 프로그램을 제공합니다.

신뢰 당사자 측에서 다음을 수행하십시오.

1. 웹 에이전트 옵션 팩을 설치합니다.

   지침은 *웹 에이전트 옵션 팩 안내서*를 참조하십시오.

2. JDK 를 설치하는지 확인합니다. 웹 에이전트 옵션 팩에는 이 JDK 가 필요합니다.

   필요한 JDK 버전을 확인하려면 기술 지원 사이트로 이동하고 "SiteMinder Platform Matrix"(SiteMinder 플랫폼 지원표)를 검색합니다.

참고: SPS 페더레이션 게이트웨이가 페더레이션 웹 서비스 응용 프로그램 기능을 제공하기 위해 웹 에이전트 및 웹 에이전트 옵션 팩을 대체할 수 있습니다. SPS 페더레이션 게이트웨이 설치 및 구성에 대한 자세한 내용은 *Secure Proxy Server Administration Guide*(보안 프록시 서버 관리 안내서)를 참조하십시오.

신뢰 당사자 측에서 페더레이션 웹 서비스 구성

이러한 단계를 수행하면 페더레이션 웹 서비스 응용 프로그램을 설정할 수 있습니다. 페더레이션 웹 서비스 응용 프로그램은 웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이가 있는 서버에 설치됩니다.

신뢰 당사자 측에서 페더레이션 웹 서비스를 구성하려면

1. 웹 에이전트 옵션 팩을 사용하도록 지원되는 응용 프로그램 서버 중 하나를 구성합니다. 웹 에이전트 옵션 팩 배포 지침을 참조하십시오.

   SPS 페더레이션 게이트웨이를 사용하고 있는 경우 페더레이션 웹 서비스 응용 프로그램이 이미 배포되어 있습니다.

2. AffWebServices.properties 파일에 있는 AgentConfigLocation 매개 변수를 WebAgent.conf 파일의 전체 경로로 설정합니다. 구문이 올바르고 경로가 파일에 한 줄로 나타나는지 확인합니다.

   AffWebServices.properties 파일에는 페더레이션 웹 서비스에 대한 초기화 매개 변수가 포함되어 있습니다. 이 파일은 다음 디렉터리 중 하나에 있습니다.

   - *web_agent_home*/affwebservices/WEB-INF/classes
   - *sps_home*/secure-proxy/Tomcat/webapps/affwebservices/WEB-INF/classes

   web_agent_home

   웹 에이전트가 설치된 위치를 나타냅니다.

   sps_home

   SPS 페더레이션 게이트웨이가 설치된 위치를 나타냅니다.

3. 페더레이션 웹 서비스 응용 프로그램에 대해 오류 및 추적 로깅이 사용되도록 설정합니다. 로깅은 LoggerConfig.properties 파일에서 사용되도록 설정됩니다. 로그를 통해 어설션 당사자와 신뢰 당사자 간의 통신을 볼 수 있습니다.

   - 오류 로깅은 기본 오류 로그 파일인 affwebserv.log 파일에 기록됩니다.
   - 추적 로깅은 기본 추적 로그 파일인 FWSTrace.log 파일에 기록됩니다.

4. 웹 브라우저를 열고 다음 링크를 입력하여 페더레이션 웹 서비스를 테스트합니다.

   http://*fqhn*:*port_number*/affwebservices/assertionretriever

   fqhn

   정규화된 호스트 이름을 정의합니다.

   port_number

   페더레이션 웹 서비스 응용 프로그램이 설치된 서버의 포트 번호를 정의합니다.

   예를 들면 다음과 같습니다.

   http://myhost.ca.com:81/affwebservices/assertionretriever

   페더레이션 웹 서비스가 올바로 작동하고 있으면 다음 메시지가 표시됩니다.

   어설션 검색 서비스를 초기화했습니다.
   요청된 서블릿은 HTTP POST 요청만 수락합니다.

   이 메시지는 페더레이션 웹 서비스가 데이터 작업을 수신 대기하고 있음을 나타냅니다. 페더레이션 웹 서비스가 올바로 작동하고 있지 않으면 어설션 검색 서비스가 실패했다는 메시지가 표시됩니다. 테스트가 실패한 경우 페더레이션 웹 서비스 로그를 살펴보십시오.

추가 정보:

페더레이션 웹 서비스(어설션 당사자) 구성 (페이지 87)

페더레이션 웹 서비스에 대한 액세스 허용(어설션 당사자)

정책 서버를 설치하면 SiteMinder 가 FWS(페더레이션 웹 서비스) 응용 프로그램에 대한 정책을 생성합니다. FWS 응용 프로그램은 웹 에이전트 옵션 팩과 함께 설치됩니다. 일부 페더레이션 기능의 경우 신뢰 당사자에게 보호된 FWS 서비스에 액세스할 수 있는 권한이 있어야 합니다. 정책에 신뢰 파트너를 추가하는 태스크는 어설션 당사자 측에서만 수행됩니다.

예를 들어 싱글 사인온에 대한 HTTP-아티팩트 바인딩의 경우 SiteMinder 가 어설션을 검색하는 서비스가 정책으로 보호됩니다. SiteMinder 가 특정 신뢰 파트너에 대한 어설션을 검색하려면 해당 파트너가 서비스를 보호하는 정책에 사용자로 추가되어 있어야 합니다.

페더레이션 파트너 관계에 대해 구성된 기능에 적용되는 특정 FWS 정책에 대한 액세스 권한을 부여 (페이지 125)하십시오.

아티팩트 싱글 사인온을 위한 인증서 데이터 저장소 수정(선택 사항)

인증서 데이터 저장소에는 암호화, 암호 해독, 서명, 확인, 클라이언트 인증 등의 PKI 작업을 위한 키와 인증서가 저장됩니다.

아티팩트 싱글 사인온을 구현하고 있는 경우 어설션 당사자의 인증서 데이터 저장소에는 SSL 연결 설정을 위한 인증 기관 인증서가 저장됩니다. 이 SSL 연결은 신뢰 당사자와 어설션 당사자 간에 설정됩니다. 이 SSL 연결은 아티팩트 싱글 사인온을 위해 어설션을 보내는 데 사용되는 백 채널을 안전하게 보호합니다.

일반 루트 CA 집합이 인증서 데이터 저장소에서 제공됩니다. 데이터 저장소에 *없는* 웹 서버에 대해 루트 CA 를 사용하려면 이러한 루트 CA 를 가져오십시오.

인증서 데이터 저장소에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

싱글 사인온을 시작하기 위한 링크 만들기(선택 사항)

SAML 2.0 및 WS-페더레이션의 경우 사용자가 어설션 당사자를 방문하기 전에 신뢰 당사자를 방문하면 하드 코드된 링크를 설정하십시오. 사용자가 하드 코드된 링크를 클릭하면 인증 컨텍스트를 가져오기 위해 어설션 당사자로 리디렉션됩니다. 이 인증 컨텍스트는 신뢰 당사자가 사용자 인증 방법을 이해하는 데 사용되는 특징으로 구성됩니다.

추가 정보:

SP 에서 SAML 2.0 싱글 사인온 시작(선택 사항) (페이지 100)
리소스 파트너에서 WS-페더레이션 싱글 사인온 시작 (페이지 101)

SP 에서 SAML 2.0 싱글 사인온 시작(선택 사항)

사용자가 아이덴티티 공급자를 방문하기 전에 서비스 공급자를 방문하는 경우 서비스 공급자는 사용자를 아이덴티티 공급자로 리디렉션해야 합니다. 서비스 공급자에서 AuthnRequest 서비스에 대한 하드 코드된 링크가 포함된 HTML 페이지를 생성하십시오. 그러면 AuthnRequest 서비스가 인증 컨텍스트를 가져오기 위해 사용자를 아이덴티티 공급자로 리디렉션합니다.

참고: HTML 페이지는 보호되지 않은 영역에 있어야 합니다.

사용자가 서비스 공급자에서 클릭하는 하드 코드된 링크에는 특정 쿼리 매개 변수가 포함되어 있어야 합니다. 이러한 매개 변수는 AuthnRequest 서비스에 대한 HTTP GET 요청의 일부가 됩니다. AuthnRequest 서비스는 서비스 공급자의 정책 서버에 있습니다.

SAML 2.0(아티팩트 또는 프로필)의 경우 링크 구문은 다음과 같습니다.

http://*sp_server:port*/affwebservices/public/saml2authnrequest?ProviderID=*IdP_ID*

sp_server:port

웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하는 서비스 공급자의 서버 및 포트 번호를 지정합니다.

IdP_ID

아이덴티티 공급자 ID 를 지정합니다.

사용되도록 설정된 바인딩에 따라 이 링크에 ProtocolBinding 쿼리 매개 변수를 추가할 수 있습니다. 서비스 공급자의 링크 구성에 대한 자세한 내용은 싱글 사인온을 시작하도록 IdP 또는 SP 의 링크 설정을 참조하십시오.

참고: 쿼리 매개 변수를 HTTP-인코딩할 필요는 없습니다.

아이덴티티 공급자에서 링크를 생성할 수도 있습니다.

리소스 파트너에서 WS-페더레이션 싱글 사인온 시작

사용자가 계정 파트너를 방문하기 전에 리소스 파트너를 방문하는 경우 리소스 파트너는 사용자를 계정 파트너로 리디렉션해야 합니다. 인증하는 데 사용할 계정 파트너에 대한 링크가 포함된 사이트 선택 페이지 등의 HTML 페이지를 생성하십시오. 사용자가 링크를 선택하면 계정 파트너의 싱글 사인온 서비스에 연결됩니다.

참고: 사이트 선택 페이지는 보호되지 않은 영역에 있어야 합니다.

사용자가 리소스 파트너에서 클릭하는 하드 코드된 링크에는 특정 쿼리 매개 변수가 포함되어 있어야 합니다. 이러한 매개 변수는 계정 파트너의 정책 서버에서 싱글 사인온 서비스에 대한 HTTP GET 요청의 일부입니다.

링크 구문은 다음과 같습니다.

https://*host:port*/affwebservices/public/wsfedsso?wa=wsignin1.0&wtrealm=*RP_ID*

host:port

싱글 사인온 서비스가 있는 서버 및 포트 번호를 나타냅니다.

RP_ID

리소스 파트너 아이덴티티를 지정합니다.

참고: 쿼리 매개 변수를 HTTP-인코딩할 필요는 없습니다.

제 4 장: SAML 1.x 어설션 생성기 파일 구성

생산자의 정책 서버에는 어설션 생성기라는 구성 요소가 포함되어 있습니다. SAML 1.x 의 경우에만 AMAssertionGenerator.properties 파일이 있어야 어설션 생성기가 어설션을 생성할 수 있습니다. 이 속성 파일에는 파일의 설정에 대한 자세한 내용을 얻을 수 있는 주석 처리된 지침도 포함되어 있습니다.

이 파일이 설치된 위치는 다음과 같습니다.

policy_server_home/config/properties

이 파일의 설정을 수정하지 않아도 어설션 생성기가 제대로 작동합니다. 하지만 어설션에 사용되는 기본값이 파일에 포함되어 있으므로 해당 네트워크에 맞게 이러한 값을 변경하십시오.

AmAssertionGenerator.properties 파일에 대한 업데이트는 정책 서버가 다시 시작된 후에 선택됩니다.

AMAssertionGenerator.properties 파일을 구성하려면

1. *policy_server_home*/config/properties 디렉터리로 이동합니다.
2. 텍스트 편집기에서 AMAssertionGenerator.properties 파일을 엽니다.
3. 다음 매개 변수를 수정합니다.

   AssertionIssuerID

   어설션을 발급하는 사이트를 식별하는 URL 을 지정합니다.

   이 URL 은 SAML 인증 체계에 대해 입력하는 "발급자" 필드와 동일한 값이어야 합니다.

SecurityDomain

생산자의 도메인(예: example.com)을 식별합니다.

SourceID

SAML 1.x 아티팩트 프로필의 경우에만 아티팩트에서 생산자를 식별하는 고유 ID 를 지정합니다. 자세한 내용은 OASIS 웹 사이트의 SAML 사양을 참조하십시오.

중요! 이 파일의 값은 소비자 사이트의 해당 설정에 대한 값과 일치해야 합니다.

제 5 장: JVM 에 대한 JVMOptions 파일 검토

JVMOptions.txt 파일에는 정책 서버가 페더레이션 웹 서비스를 지원하는 데 사용되는 Java Virtual Machine 을 생성할 때 사용하는 설정이 포함되어 있습니다. SAML 1.x, SAML 2.0 및 WS-페더레이션에서 이 파일을 사용합니다.

정책 서버 업그레이드 중에 기존 JVMOptions.txt 파일의 이름이 JVMOptions.txt.backup 으로 변경됩니다. 새 JVMOptions.txt 파일이 생성됩니다. 원본 파일에 사용자 지정된 매개 변수가 포함된 경우 이러한 사용자 지정된 매개 변수를 포함하도록 새로 생성된 파일을 수정하십시오.

이 파일이 설치된 위치는 다음과 같습니다.

policy_server_home/config/

중요! JVMOptions.txt 파일을 업데이트한 경우 정책 서버를 다시 시작해야 변경 내용이 적용됩니다.

참고:

- 일부 환경에서 정책 서버가 실행되는 동안 시스템에서 로그오프하면 정책 서버 서비스가 실패합니다. 이 오류는 JVM 문제로 인해 발생합니다. 이 오류를 방지하려면 JVMOptions.txt 파일에서 -Xrs 명령을 자체 명령줄에 추가하십시오. 이 Java 명령을 사용하면 Java Virtual Machine 의 운영 체제 신호 사용량이 줄어듭니다.

  이 명령은 대/소문자를 구분하므로 X 를 대문자로 입력해야 합니다.

- 누락된 클래스와 관련된 오류가 발생하면 이 파일에서 클래스 경로 지시문을 수정하십시오. JVMOptions.txt 파일에 포함된 설정에 대한 자세한 내용은 Java 설명서를 참조하십시오. Java 컴파일러 지시문 java.endorsed.dirs 는 JVMOptions.txt 파일에서 클래스 로드를 제어하는 데 사용됩니다.

제 6 장: 사용자 세션, 어설션 및 만료 데이터 저장

이 섹션은 다음 항목을 포함하고 있습니다.

세션 저장소에 저장되는 페더레이션 데이터

세션 저장소에는 다음 페더레이션 기능에 대한 데이터가 저장됩니다.

- HTTP-아티팩트 싱글 사인온(SAML 1.x 또는 2.x)

  SAML 어설션 및 연결된 아티팩트가 어설션 당사자 측에서 생성됩니다. 아티팩트가 생성된 어설션을 식별합니다. 어설션 당사자는 신뢰 당사자에 아티팩트를 반환합니다. 신뢰 당사자는 아티팩트를 사용하여 어설션 당사자가 세션 저장소에 저장한 어설션을 검색합니다.

  이 프로세스가 작동하려면 영구 세션이 필요합니다.

  SAML POST 프로필은 세션 저장소에 어설션을 저장하지 않습니다.

- HTTP-POST 단일 사용 정책(SAML 2.0 및 WS-페더레이션)

  단일 사용 정책 기능은 어설션(POST 바인딩)이 신뢰 당사자 측에서 두 번째 세션을 설정하는 데 재사용되지 않도록 합니다. 신뢰 당사자는 자체 세션 저장소에 만료 데이터라고 하는 어설션에 대한 시간 기반 데이터를 저장합니다. 만료 데이터는 어설션이 한 번만 사용되도록 합니다.

  신뢰 당사자에 세션 저장소가 필요하지만 영구 세션은 필요하지 않습니다.

- 인증 세션 변수 유지(SAML 1.x 및 SAML 2.0)

  신뢰 당사자 측에서 페더레이션을 구성할 때 "인증 세션 변수 유지" 옵션을 선택할 수 있습니다. 이 옵션은 정책 서버에 인증 컨텍스트 데이터를 세션 저장소에 세션 변수로 저장하도록 지시합니다. 정책 서버는 이러한 변수에 액세스하여 인증 결정에 사용할 수 있습니다.

- 어설션 특성 유지(모든 프로필)

  신뢰 당사자 측에서 "특성 유지"를 리디렉션 모드로 선택할 수 있습니다. 리디렉션 모드는 사용자를 대상 응용 프로그램으로 리디렉션하는 방법을 결정합니다. "특성 유지" 모드에서는 정책 서버가 어설션에서 추출된 특성을 세션 저장소에 저장하도록 합니다. 그러면 이 특성을 HTTP 헤더 변수로 제공할 수 있습니다.

- 싱글 로그아웃(SAML 2.0)

  싱글 로그아웃이 사용되도록 설정된 경우 어느 파트너든지 사용자 세션에 대한 정보를 저장할 수 있습니다. 세션 정보는 세션 저장소에 보관됩니다. 싱글 로그아웃 요청이 완료되면 사용자의 세션 정보가 제거되어 세션이 무효화됩니다.

  아이덴티티 공급자와 서비스 공급자에 영구 세션이 필요합니다.

- 사인아웃(WS-페더레이션)

  사인아웃이 사용되도록 설정된 경우 사용자 컨텍스트 정보가 세션 저장소에 저장됩니다. 이 정보를 통해 소프트웨어가 사인아웃 요청을 생성할 수 있습니다. 사인아웃 요청이 완료되면 사용자의 세션 정보가 제거되면서 사용자 세션이 무효화됩니다.

  영구 세션은 계정 파트너와 리소스 파트너에 필요합니다.

세션 저장소가 사용되도록 설정

SAML 아티팩트 싱글 사인온, 싱글 로그아웃, WS-페더레이션 사인아웃 및 단일 사용 정책을 사용할 때 데이터를 저장할 세션 저장소가 사용되도록 설정하십시오.

세션 서버 데이터베이스는 정책 서버 세션 서버가 영구 세션 데이터를 저장하는 위치입니다.

정책 서버 관리 콘솔에서 세션 저장소가 사용되도록 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔에 로그인합니다.
2. "데이터" 탭을 선택합니다.

3. "데이터베이스" 필드의 드롭다운 목록에서 "세션 저장소"를 선택합니다.
4. "저장소" 필드의 드롭다운 목록에서 사용 가능한 저장소 유형을 선택합니다.
5. "세션 저장소 사용" 확인란을 선택합니다.

   하나 이상의 영역에서 영구 세션을 사용하려면 세션 서버가 사용되도록 설정하십시오. 사용되도록 설정된 경우 세션 서버는 정책 서버 성능에 영향을 줍니다.

   참고: 성능상의 이유로 세션 서버는 정책 저장소와 동일한 데이터베이스에서 실행할 수 없습니다. 따라서 정책 저장소 데이터베이스를 사용하는 옵션이 사용되지 않도록 설정되어 있습니다.
6. 선택한 저장소 유형에 적절한 데이터 원본 정보를 지정합니다.
7. "확인"을 클릭하여 설정을 저장하고 콘솔을 종료합니다.
8. 정책 서버를 중지했다가 다시 시작합니다.

공유 세션 저장소가 필요한 환경

다음 SiteMinder 기능을 사용하려면 SAML 어설션과 사용자 세션 정보를 저장할 공유 세션 저장소가 필요합니다.

클러스터된 정책 서버 환경에서 이러한 기능을 구현하려면 환경을 다음과 같이 설정하십시오.

- HTTP-POST 단일 사용 정책을 *제외한* 모든 기능에 대해 영구 세션의 로그인 영역을 구성하십시오.

  영구 세션은 영역 구성의 일부입니다.
- HTTP-아티팩트 싱글 사인온의 경우 클러스터의 모든 정책 서버에서 생산자/아이덴티티 공급자 사이트의 세션 저장소를 공유하십시오.

  세션 저장소를 공유하면 모든 정책 서버가 각각 어설션에 대한 요청을 받을 때 어설션에 액세스할 수 있게 됩니다.

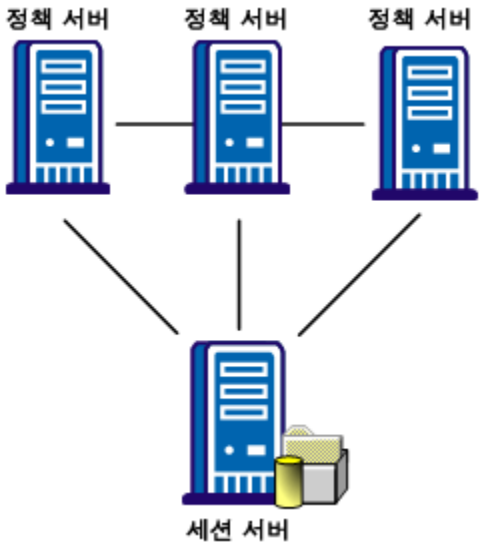
- SAML 2.0 싱글 로그아웃 및 WS-페더레이션 사인아웃의 경우 클러스터의 모든 정책 서버에서 어설션 당사자 및 신뢰 당사자의 세션 저장소를 공유합니다.

  세션 저장소를 공유하면 모든 정책 서버가 각각 세션 로그아웃에 대한 요청을 받을 때 사용자 세션 데이터에 액세스할 수 있게 됩니다.

- HTTP-POST 및 WS-페더레이션 단일 사용 정책 기능의 경우 클러스터에 있는 모든 정책 서버에서 신뢰 당사자의 세션 저장소를 공유합니다.

어설션을 생성 또는 소비하거나 영구 SMSESSION 쿠키를 처리하는 모든 정책 서버는 공용 세션 저장소에 연결할 수 있어야 합니다. 예를 들어 사용자가 example.com 에 로그인하고 해당 도메인에 대한 영구 세션 쿠키를 얻는다고 가정합니다. 이 경우 example.com 에 대한 요청을 처리하는 모든 정책 서버는 세션이 여전히 유효한지 확인할 수 있어야 합니다.

다음 그림에서는 세션 저장소 하나와 통신하는 정책 서버 클러스터를 보여 줍니다.



세션 저장소를 공유하려면 다음 방법 중 하나를 사용하십시오.

- 모든 정책 서버가 세션 저장소 하나를 가리키도록 지정

  정책 서버 관리 콘솔에서 지정된 세션 저장소가 사용되도록 정책 서버를 구성합니다.

- 세션 저장소를 여러 세션 저장소에 복제

  데이터베이스 복제에 대한 지침은 해당 데이터베이스 설명서를 참조하십시오.

제 7 장: 페더레이션된 환경의 보안

이 섹션은 다음 항목을 포함하고 있습니다.

페더레이션된 통신 보호

어설션 암호화 및 파트너 사이트 간에 SSL 연결 사용 등과 같이 페더레이션된 파트너 간의 트랜잭션에 보안을 적용하는 데 도움이 되는 몇 가지 메커니즘이 있습니다.

SiteMinder 를 사용하여 페더레이션 환경을 설정하는 경우 환경을 보호하기 위한 몇 가지 권장 사항은 다음과 같습니다.

- 어설션의 일회 사용을 적용합니다.
- 어설션 당사자와 신뢰 당사자 간의 연결에 보안을 설정합니다.
- 교차 사이트 스크립팅을 방지합니다.

이어지는 단원에서 이러한 내용을 설명합니다.

어설션에 대한 일회 사용 조건 설정

SAML 1.x 및 2.0 사양에 따라 SiteMinder 가 어설션의 일회 사용을 적용할 수 있습니다. 즉, 일회 사용하도록 설계된 어설션을 생성하여 신뢰 당사자에게 향후 트랜잭션 용도로 어설션을 보관하지 않도록 지시합니다. 유효 기간이 지난 어설션을 다시 사용하면 오래된 아이덴티티 정보에 기반한 인증 결정이 내려집니다.

SiteMinder 가 어설션 당사자(생산자/IdP)로 작동하는 경우 어설션의 일회 사용을 구성할 수 있습니다. SAML 1.x 가맹의 경우 **DoNotCache 조건 설정** 설정을 선택할 수 있습니다. SAML 2.0 IdP 의 경우 **OneTimeUse 조건 설정** 설정을 선택할 수 있습니다. 이러한 구성 설정을 둘 다 사용하면 SiteMinder 가 일회 사용 조건을 나타내는 적절한 요소를 어설션에 삽입할 수 있습니다.

참고: 어설션의 일회 사용과 SAML 1.x 및 2.0 HTTP-POST 싱글 사인온에 대한 단일 사용 정책을 혼동하지 마십시오. 단일 사용 정책은 POST 트랜잭션에만 사용되지만 일회 사용 기능은 HTTP-아티팩트와 HTTP-POST 에 사용됩니다.

페더레이션 환경의 연결 보안

페더레이션된 파트너 간에 전송되거나 파트너와 응용 프로그램 간에 전송되는 아이덴티티 정보는 통신이 보안 연결을 통해 수행될 때 최적으로 보호됩니다.

신뢰 당사자와 대상 응용 프로그램 간의 연결 보안

신뢰 당사자 측에서 클라이언트 사이트의 대상 응용 프로그램으로 흐르는 데이터 전송을 보호하십시오. 보안 연결을 통신 채널로 사용하면 보안 공격에 대한 환경 취약점이 줄어듭니다.

예를 들어 신뢰 당사자가 추출하여 클라이언트 응용 프로그램에 보내는 특성이 어설션에 포함될 수 있습니다. 신뢰 당사자는 HTTP 헤더 변수나 쿠키를 사용하여 이러한 특성을 응용 프로그램에 전달할 수 있습니다. 헤더나 쿠키에 저장된 특성이 클라이언트 측에서 덮어쓰여질 수 있으므로 악의적인 사용자가 다른 사용자를 가장할 수 있습니다. SSL 연결을 사용하면 환경이 이러한 종류의 보안 위반으로부터 보호됩니다.

해당 ACO(에이전트 구성 개체)에서 UseSecureCookies 매개 변수를 설정하여 이 취약점을 방지하는 것이 가장 좋습니다. UseSecureCookies 매개 변수는 페더레이션 웹 서비스에 "secure" 플래그로 표시된 쿠키를 생성하도록 지시합니다. 이 플래그는 쿠키가 SSL 통신 채널을 통해서만 전송됨을 나타냅니다.

참고: 수정할 ACO 는 페더레이션 환경 설정에 따라 다릅니다. 웹 에이전트가 설치된 것과 같은 시스템에 페더레이션 웹 서비스를 배포하는 경우 웹 에이전트에 대한 ACO 를 편집하십시오. 웹 에이전트가 설치된 것과 다른 시스템에 페더레이션 웹 서비스를 배포하는 경우에는 페더레이션 웹 서비스에 대해 생성한 고유한 ACO 를 편집하십시오.

SiteMinder 어설션 당사자의 초기 인증 보안

SiteMinder 어설션 당사자의 초기 사용자 인증에는 잠재적인 취약점이 있습니다. 사용자가 어설션 당사자 측에서 사용자 세션을 설정하기 위해 맨 처음 인증할 때 세션 ID 쿠키가 브라우저에 기록됩니다. 쿠키가 비 SSL 연결을 통해 전송되면 공격자가 쿠키를 획득하고 중요한 사용자 정보를 도용할 수 있습니다. 그런 다음 공격자가 이 정보를 사용하여 사용자를 가장하거나 아이덴티티를 도용할 수 있습니다.

에이전트 구성 개체에서 수정할 수 있는 웹 에이전트 매개 변수 UseSecureCookies 를 설정하여 이 취약점을 방지하는 것이 가장 좋습니다. UseSecureCookies 매개 변수는 웹 에이전트에 "secure" 플래그로 표시된 쿠키를 생성하도록 지시합니다. 이 플래그는 브라우저가 SSL 연결을 통해서만 쿠키를 전달하여 보안이 강화됨을 나타냅니다. 일반적으로 모든 URL 에 대해 SSL 연결을 설정하는 것이 좋습니다.

교차 사이트 스크립팅 방지

응용 프로그램에서 실행 가능한 스크립트를 구성할 수 있는 문자를 필터링하지 않고 브라우저에서 입력된 텍스트를 표시할 때 XSS(교차 사이트 스크립팅) 공격이 발생할 수 있습니다. 입력된 텍스트는 일반적으로 게시물에 있는 데이터 또는 URL 의 쿼리 매개 변수에 있는 데이터입니다. 이러한 문자가 브라우저에 표시되면 원치 않는 스크립트가 브라우저에서 실행될 수 있습니다.

SiteMinder 는 SiteMinder Federation 기능에 사용할 여러 JSP 를 제공합니다. 이러한 JSP 는 요청에 있는 문자를 확인하여 출력 스트림의 안전하지 않은 정보가 브라우저에 표시되지 않도록 합니다.

SiteMinder 가 페더레이션 요청을 받으면 다음 JSP 가 디코딩된 값을 검사하여 교차 사이트 스크립팅 문자가 있는지 확인합니다.

- idpdiscovery.jsp

  신뢰 당사자 측에서 아이덴티티 공급자 검색에 사용합니다.

- linkaccount.jsp

  신뢰 당사자 측에서 동적 계정 연결에 사용합니다.

- sample_application.jsp

  IDP 측에서 싱글 사인온을 시작하는 데 사용합니다. 이 샘플 응용 프로그램을 사용하여 사용자를 SSO 서비스와 사용자 지정 웹 응용 프로그램에 차례로 연결할 수 있습니다. 일반적으로 사용자 고유의 응용 프로그램을 사용합니다.

- signoutconfirmurl.jsp

  계정 파트너에서 WS-페더레이션 사인아웃에 사용합니다.

- unsolicited_application.jsp

  사용자가 SSO 서비스에 먼저 전송되지 않고 웹 응용 프로그램에 직접 전송될 때 IdP 에서 시작되는 싱글 사인온에 사용됩니다.

해당 페이지에서는 요청을 검사하여 다음 문자가 있는지 확인합니다.

문자	설명
<	왼쪽 꺾쇠 괄호
>	오른쪽 꺾쇠 괄호
‘	작은따옴표
"	큰따옴표
%	백분율 기호
;	세미콜론
(	여는(왼쪽) 괄호
)	닫는(오른쪽) 괄호
&	앰퍼샌드
+	더하기 기호

SiteMinder 에서 제공된 JSP 각각에는 검사할 문자를 정의하는 변수가 포함되어 있습니다. 이러한 JSP 를 수정하여 문자 집합을 확장할 수 있습니다.

제 8 장: 페더레이션에 대한 키 및 인증서 관리

어설션에 보안을 적용하고 어설션 내의 데이터를 암호화하는 것은 파트너 관계 구성의 중요한 부분입니다. 페더레이션 환경에서는 키/인증서 쌍 및 독립 실행형 인증서가 다음과 같은 여러 기능을 수행합니다.

- 어설션의 서명/확인(3 개 프로필 모두)
- 인증 요청 서명/확인(SAML 2.0 만 해당)
- 싱글 로그아웃 요청 및 응답 서명/확인(SAML 2.0)
- HTTP-아티팩트 SSO 에 대한 채널 요청 및 응답 서명(SAML 1.1 및 2.0)
- 전체 어설션 또는 어설션의 일부 암호화/암호 해독(SAML 2.0)
- 아티팩트 SSO(Single Sign–On)를 위한 백 채널 전반의 클라이언트 자격 증명(SAML 1.1 및 2.0)

*정책 서버 구성 안내서*에는 키 및 인증서 관리에 대한 정보와 지침이 포함되어 있습니다.

SSL 서버 인증서를 사용하여 다음 태스크를 수행할 수 있습니다.

- SSL 연결을 통한 페더레이션 트래픽 관리
- 백 채널을 통한 아티팩트 싱글 사인온의 보안 통신

SiteMinder 웹 에이전트가 설치된 웹 서버에서 SSL 을 사용하도록 설정하는 지침을 참조하십시오.

참고: SSL 이 사용되도록 설정하는 경우 "기준 URL" 매개 변수를 포함한 모든 서비스의 모든 URL 이 영향을 받습니다. 즉, 모든 서비스 URL 이 https://로 시작해야 합니다.

SAML 2.0 서명 알고리즘

SAML 2.0 의 경우 서명 태스크에 대한 서명 알고리즘을 선택할 수 있습니다. 알고리즘을 선택할 수 있으므로 다음과 같은 사용 사례가 지원됩니다.

- IdP 가 RSAwithSHA1 을 사용하는 어설션, 응답 및 SLO-SOAP 메시지 또는 RSAwithSHA256 알고리즘에 서명하는 IdP-->SP 파트너 관계
- SP 가 RSAwithSHA1 을 사용하는 인증 요청과 SLO-SOAP 메시지 또는 RSAwithSHA256 알고리즘에 서명하는 SP-->IdP 파트너 관계

서명 확인은 서명된 문서에서 사용 중인 알고리즘을 자동으로 감지하고 이를 확인합니다. 따라서 서명 확인을 위한 구성은 필요하지 않습니다.

제 9 장: 페더레이션에 대한 사용자 디렉터리 구성

디렉터리 연결은 SiteMinder 가 사용자 ID 에 대한 컨텍스트를 설정하는 방식을 확인합니다. 소프트웨어는 이러한 연결을 사용하여 사용자 ID 를 확인하고 사용자 레코드에 속한 사용자 특성을 검색합니다.

어설션 당사자는 사용자 디렉터리에 대해 각 사용자를 인증하여 어설션을 생성할 수 있는 사용자를 결정합니다. 신뢰 당사자 측에서는 인증 중에 어설션이 제공될 때 신뢰 당사자가 사용자 디렉터리에서 사용자 레코드를 찾습니다.

페더레이션된 트랜잭션에 대한 사용자를 선택하기 전에 사용자 디렉터리를 구성하십시오. 사용자 디렉터리를 구성하려면 *정책 서버 구성 안내서*를 참조하십시오.

참고: 페더레이션된 구성에서 ODBC 데이터베이스를 사용하려면 사용자 디렉터리로 ODBC 데이터베이스를 선택하기 전에 SQL 쿼리 체계와 올바른 SQL 쿼리를 설정하십시오.

제 10 장: 가맹 도메인 생성

이 섹션은 다음 항목을 포함하고 있습니다.

가맹 도메인 개요

가맹 도메인은 하나 이상의 사용자 디렉터리와 연결된 페더레이션된 엔터티의 논리적 그룹입니다.

가맹 도메인은 페더레이션된 엔터티를 포함할 뿐 아니라 도메인과 연결된 사용자 디렉터리를 정의합니다. 어설션을 생성하려면 아이덴티티 공급자로 작동하는 SiteMinder 가 사용자 레코드가 정의된 사용자 디렉터리에 액세스할 수 있어야 합니다. 정책 서버는 가맹 도메인의 검색 순서에 지정된 사용자 디렉터리를 쿼리하여 사용자 레코드를 찾습니다.

검색 순서는 가맹 도메인에 대한 사용자 디렉터리 연결을 추가할 때 정의됩니다. 선택적으로 디렉터리 순서를 바꿀 수 있습니다.

가맹 도메인에는 도메인의 개체를 수정할 수 있는 관리자 계정이 하나 이상 필요합니다. 시스템 수준 관리자는 모든 도메인의 모든 개체를 관리할 수 있으며 "Manage Affiliates"(가맹 관리) 권한을 가집니다. 다른 관리자에게 정책 도메인에 대한 제어 권한을 부여할 수 있는 시스템 관리자는 "시스템 및 도메인 개체 관리" 권한을 가집니다.

가맹 도메인 구성

도메인 개체를 추가하고 소비자, 서비스 공급자 또는 리소스 파트너의 리소스에 액세스할 수 있는 사용자를 선택한 다음 연결된 엔터티를 추가할 수 있습니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "페더레이션", "레거시 페더레이션", "가맹 도메인"을 차례로 클릭합니다.
3. "가맹 도메인 만들기"를 클릭합니다.
4. "일반" 설정에 가맹 도메인에 대한 이름과 간단한 설명을 입력합니다.
5. "사용자 디렉터리" 섹션에서 "추가/제거"를 클릭합니다.
6. "사용 가능한 구성원"에서 "선택한 구성원"으로 도메인과 연결할 사용자 디렉터리를 이동합니다.

   가맹 리소스에 대한 액세스를 허용할 사용자의 기록을 저장할 디렉터리를 지정하십시오.
7. "확인"을 클릭합니다.

   선택한 디렉터리가 "사용자 디렉터리" 테이블에 나타납니다.

   기존 디렉터리가 없는 경우 "만들기"를 클릭하여 사용자 디렉터리를 만드십시오. 필수 정보를 입력하면 생성한 디렉터리가 "사용자 디렉터리" 테이블에 나타납니다.
8. 선택적으로 "사용자 디렉터리" 테이블에서 오른쪽의 화살표를 사용하여 디렉터리가 테이블에 나타나는 순서를 조정합니다. 디렉터리 상세 정보를 편집하려면 왼쪽의 화살표를 사용합니다.

   디렉터리가 나타나는 순서는 목록 맨 위에서 시작하여 SiteMinder 가 사용자 레코드를 찾기 위해 검색하는 순서입니다.
9. 제출을 클릭합니다.

   가맹 도메인이 생성되었습니다.

다음 단계는 파트너를 가맹 도메인에 추가하고 SiteMinder 를 페더레이션된 파트너 관계의 어설션 당사자로 구성하는 것입니다.

추가 정보:

SAML 1.x 생산자 구성 (페이지 129)
SAML 2.0 서비스 공급자 구성 (페이지 263)
SiteMinder 를 WS-페더레이션 리소스 파트너로 구성 (페이지 335)

가맹 도메인에 엔터티 추가

페더레이션된 파트너 관계에서 어설션 당사자의 역할을 수행하도록 SiteMinder 를 구성하십시오. SiteMinder 가 어설션 당사자로 작동하도록 하려면 파트너를 가맹 도메인에 추가하십시오. 파트너가 인증 요청을 보내면 SiteMinder 가 응답에 어설션을 생성할 수 있습니다.

가맹 도메인에 다음 엔터티를 추가할 수 있습니다.

- SAML 1.x 가맹
- SAML 2.0 서비스 공급자
- WS-페더레이션 리소스 파트너

참고: 이러한 엔터티는 어설션 당사자의 페더레이션 웹 서비스에 액세스할 수 있는 (페이지 145) 권한이 있어야 합니다.

가맹 도메인에 파트너를 추가하는 방법에 대한 지침은 다음 단원 중 하나를 참조하십시오.

- SiteMinder 를 SAML 1.x 생산자로 구성 (페이지 129)
- SiteMinder 를 SAML 2.0 아이덴티티 공급자로 구성 (페이지 197)
- SiteMinder 를 계정 파트너로 구성 (페이지 309)

추가 정보:

SAML 1.x 생산자 구성 (페이지 129)
SAML 2.0 아이덴티티 공급자 구성 (페이지 197)
WS-페더레이션 계정 파트너 구성 (페이지 309)

제 11 장: 페더레이션 웹 서비스에 대한 액세스 권한 부여

이 섹션은 다음 항목을 포함하고 있습니다.

페더레이션 웹 서비스를 보호하는 정책

정책 서버를 설치하면 SiteMinder 가 여러 서비스에 대한 정책을 생성합니다. 이러한 서비스는 FWS(페더레이션 웹 서비스) 응용 프로그램을 구성합니다. 일부 페더레이션 기능의 경우 신뢰 당사자에게 연결된 보호된 서비스에 액세스할 수 있는 권한이 있어야 합니다.

정책에 신뢰 파트너를 추가하는 태스크는 어설션 당사자 측에서만 수행됩니다.

예를 들어 HTTP-아티팩트 바인딩의 경우 SiteMinder 가 어설션을 검색하는 서비스가 정책으로 보호됩니다. SiteMinder 가 특정 신뢰 파트너에 대한 어설션을 검색하려면 해당 파트너가 서비스를 보호하는 정책에 사용자로 추가되어 있어야 합니다.

다음 표에는 FWS 서비스와 관련된 FWS 정책 개체가 나열되어 있습니다.

개체 유형	개체 이름
도메인	FederationWebServicesDomain
영역	FederationWebServicesRealm public
에이전트 그룹	FederationWebServicesAgentGroup

개체 유형	개체 이름
규칙	SAML2FWSAttributeServiceRule FederationWSSessionServiceRule SAML2FWSArtifactResolutionRule FederationWSAssertionRetrievalServiceRule FederationWSNotificationServiceRule
정책	SAML2FWSArtifactResolutionServicePolicy SAML2FWSAttributeServicePolicy FederationWSAssertionRetrievalServicePolicy FederationWSNotificationServicePolicy FederationWSSessionServicePolicy
변수	AllowNotification AllowSessionSync
사용자 디렉터리	FederationWSCustomUserStore SAML2FederationCustomUserStore

FWS 정책과 연결된 기능

SiteMinder 가 생성하는 정책은 다음 레거시 페더레이션 기능을 지원합니다.

FWS 정책		페더레이션 기능
	SAML2FWSArtifactResolutionServicePolicy	SAML 2.0 아티팩트 싱글 사인온에 대한 아티팩트 레졸루션 서비스 보호
	FederationWSAssertionRetrievalServicePolicy	SAML 1.x 아티팩트 싱글 사인온에 대한 어설션 검색 서비스 보호
	SAML2FWSAttributeServicePolicy	SAML 2.0 에 대한 특성 기관 서비스 보호
	FederationWSNotificationServicePolicy	알림 서비스 보호. 알림은 SAML 가맹 에이전트가 소비자인 경우에만 사용할 수 있습니다.
	FederationWSSessionServicePolicy	세션 관리에 대한 세션 서비스 보호. 세션 관리는 SAML 가맹 에이전트가 소비자인 경우에만 사용할 수 있습니다.

페더레이션 웹 서비스를 보호하는 정책 적용

FWS 정책이 포함된 페더레이션 기능을 구현하고 있는 경우 보호된 서비스에 액세스할 수 있는 권한이 신뢰 당사자에게 필요합니다.

액세스 권한 부여에는 다음과 같은 태스크가 포함됩니다.

- 에이전트 그룹 FederationWebServicesAgentGroup 에 FWS 응용 프로그램을 보호하는 웹 에이전트 추가
- 특정 서비스에 액세스하도록 허용된 사용자로 신뢰 파트너 추가

  지정된 정책에 사용자를 추가하는 것 외에는 다른 모든 정책 개체가 자동으로 설정됩니다.

HTTP-아티팩트 어설션 검색 및 특성 기관 정책을 적용하는 상세 절차는 해당 기능 관련 단원에 나와 있습니다.

추가 정보:

어설션 검색 서비스에 대한 액세스 권한 부여(아티팩트 SSO) (페이지 144)
신뢰 파트너에게 특성 기관 서비스에 대한 액세스 권한 부여 (페이지 376)

제 12 장: SAML 1.x 생산자 구성

이 섹션은 다음 항목을 포함하고 있습니다.

어설션 파트너(레거시)에 대한 사전 요구 사항

어설션 파트너를 구성하려면 다음 조건을 확인하십시오.

- 정책 서버가 설치되어 있어야 합니다.
- 다음 옵션 중 하나가 설치되어 있어야 합니다.
  - 웹 에이전트 및 웹 에이전트 옵션 팩. 웹 에이전트는 사용자를 인증하고 SiteMinder 세션을 설정합니다. 옵션 팩은 페더레이션 웹 서비스 응용 프로그램을 제공합니다. 적절한 네트워크 시스템에 FWS 응용 프로그램을 배포해야 합니다.
  - SPS 페더레이션 게이트웨이에 포함된 웹 에이전트가 있고 포함된 Tomcat 웹 서버에 페더레이션 웹 서비스 응용 프로그램이 있습니다.

  자세한 내용은 *웹 에이전트 옵션 팩 안내서*를 참조하십시오.
- 메시지 서명 및 암호 해독이 필요한 기능을 위해 개인 키와 인증서를 가져와야 합니다.
- 페더레이션된 네트워크 내에 신뢰 파트너가 설정되어 있어야 합니다.

생산자를 구성하는 방법

SiteMinder 는 SAML 생산자로 작동하는 경우 해당 비즈니스 파트너인 소비자에 대한 어설션을 생성합니다. 페더레이션된 파트너 관계를 설정하려면 각 파트너(관리 UI 에서는 가맹이라고 함)에 대한 정보가 생산자에게 필요합니다. 각 파트너에 대해 가맹 개체를 생성하고, 엔터티 두 개가 어설션을 전달하고 싱글 사인온 등의 프로필을 충족하기 위해 통신하는 방법을 정의하십시오.

생산자에 필요한 구성 태스크는 다음과 같습니다.

1. 가맹을 가맹 도메인과 연결합니다.
2. 가맹에 대한 일반 설정을 구성합니다 (페이지 132).
3. 생산자가 생성하는 어설션의 대상이 되는 사용자를 선택합니다 (페이지 136).
4. 어설션을 구성합니다 (페이지 140).
5. (HTTP-아티팩트 SSO 만 해당)
   a. 어설션을 저장할 세션 저장소가 사용되도록 설정합니다. 정책 서버 관리 콘솔을 사용하여 세션 저장소를 관리합니다.
   b. 해당하는 신뢰 당사자 각각에 대해 어설션 검색 서비스에 대한 액세스를 허용합니다 (페이지 145).
6. 싱글 사인온을 시작하기 위한 링크를 생성합니다 (페이지 161).
7. 선택적 구성 태스크를 완료합니다 (페이지 130).

팁:

- 생산자와 소비자의 특정 매개 변수 값이 일치해야 구성이 올바로 작동합니다. 이러한 매개 변수 목록은 동일한 값을 사용해야 하는 구성 설정 (페이지 411)에 있습니다.
- 페더레이션 웹 서비스 서블릿에 대해 올바른 URL 을 사용하고 있는지 확인하십시오. URL 은 SiteMinder 구성에 사용되는 페더레이션 웹 서비스 URL (페이지 417)에 나열되어 있습니다.

가맹을 식별하기 위한 선택적 구성 태스크

가맹을 식별하기 위한 선택적 태스크는 다음과 같습니다.

- 어설션에 포함할 특성을 구성합니다 (페이지 153).

- 가맹 작업에 대한 시간 제한을 구성합니다 (페이지 135).
- 가맹에 액세스하는 주소를 제한할 IP 주소 제한을 설정합니다 (페이지 135).
- 어설션 생성자 플러그인을 사용하여 어설션 콘텐츠를 사용자 지정합니다 (페이지 158).

레거시 페더레이션 대화 상자 탐색

관리 UI 에서는 레거시 페더레이션 구성 대화 상자로 이동하는 방법 두 가지를 제공합니다.

다음 두 방법 중 하나로 탐색할 수 있습니다.

- 마법사를 따라 새 레거시 페더레이션 개체 구성

  개체를 생성하는 경우 페이지가 표시되면서 구성 마법사가 나타납니다. 구성 마법사의 단계를 따라 개체를 생성하십시오.

- 탭을 선택하여 기존 레거시 페더레이션 개체 수정

  기존 개체를 수정하는 경우 페이지가 표시되면서 일련의 탭이 나타납니다. 이러한 탭에서 구성을 수정하십시오. 이러한 탭은 구성 마법사의 단계와 동일합니다.

SAML 1.x 가맹을 가맹 도메인과 연결

가맹 도메인은 페더레이션 파트너의 논리적 그룹입니다. SiteMinder 가 인식할 수 있도록 가맹을 가맹 도메인과 연결합니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "페더레이션", "레거시 페더레이션", "가맹"을 차례로 클릭합니다.
3. "가맹 만들기"를 클릭합니다.
4. 이 가맹이 속한 가맹 도메인을 선택합니다.
5. "다음"을 클릭합니다.

가맹이 가맹 도메인과 연결되었습니다. 다음 단계에서는 가맹에 대한 몇 가지 일반 정보 (페이지 132)를 제공합니다.

추가 정보:

SiteMinder 세션이 없는 사용자 인증(SAML 1.x) (페이지 133)

가맹에 대한 일반 설정 완료

가맹에 대한 일반 설정을 구성합니다.

가맹에 대한 일반 정보를 제공하려면

1. 구성 마법사의 "일반" 단계에서 시작합니다.
2. "일반" 섹션의 다음 필수 필드에 데이터를 입력합니다.
   - 이름
   - 암호 및 암호 확인
   - 인증 URL

     이 URL 은 redirect.jsp 파일을 가리켜야 합니다. 예를 들면 다음과 같습니다.

     파일(예: http://myserver.mysite.com/siteminderagent/redirectjsp/redirect.jsp)을 가리켜야 합니다.

     myserver 는 웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이가 있는 웹 서버를 식별합니다.

     인증 URL 을 보호하는 정책을 생성해야 합니다.
3. "사용"을 선택하여 가맹 개체를 활성화합니다.
4. (선택 사항) "보안 URL 사용"을 선택합니다.

   "보안 URL 사용" 기능은 SSO 서비스에 SiteMinder 세션을 설정하기 위해 사용자를 리디렉션하기 전에 인증 URL 에 추가하는 SMPORTALURL 쿼리 매개 변수를 암호화하도록 지시합니다. SMPORTALURL 을 암호화하면 악의적인 사용자가 수정하지 못하게 됩니다.

   참고: 이 확인란을 선택하는 경우 "인증 URL" 필드를 다음 URL 로 설정하십시오.

   http(s)://*idp_server:port*/affwebservices/secure/secureredirect

   이 필드에 대한 자세한 내용을 보려면 "도움말"을 클릭하십시오.

5. (선택 사항) "제한" 및 "고급" 섹션의 필드에 데이터를 입력합니다.
6. "다음"을 클릭합니다.

SiteMinder 세션이 없는 사용자 인증(SAML 1.x)

가맹 도메인에 소비자를 추가하는 경우 "인증 URL" 필드를 설정해야 합니다. 인증 URL 이 redirect.jsp 파일을 가리켜야 합니다. 이 URL 의 용도는 생산자에서 세션을 설정하는 것입니다.

redirect.jsp 파일은 웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 설치하는 생산자에 설치됩니다. 보호된 리소스를 요청하는 사용자에게 인증을 받으라는 메시지를 표시하도록 SiteMinder 정책으로 redirect.jsp 파일을 보호하십시오. 웹 에이전트가 챌린지를 표시하는 이유는 사용자에게 SiteMinder 세션이 없기 때문입니다.

사용자가 인증되어 redirect.jsp 파일에 성공적으로 액세스한 후 세션이 설정됩니다. redirect.jsp 파일이 사용자를 생산자 웹 에이전트로 다시 리디렉션합니다. 에이전트가 요청을 처리하고 SAML 어설션을 생성할 수 있습니다.

인증 URL 을 보호하는 절차는 다음 설정 모두에서 동일합니다.

- 웹 에이전트와 동일한 시스템에 설치된 웹 에이전트 옵션 팩
- 웹 서버 프록시에 웹 에이전트가 설치된 응용 프로그램 서버
- 응용 프로그램 서버 에이전트와 함께 설치된 응용 프로그램 서버
- 어설션 당사자에 설치된 SPS 페더레이션 게이트웨이

인증 URL 을 보호하도록 정책 구성

인증 URL 을 보호하려면

1. 관리 UI 에 로그인합니다.
2. 어설션 당사자 웹 서버에 대해 정의하는 영역에 바인드할 웹 에이전트를 생성합니다. 웹 서버와 FWS 응용 프로그램에 대해 고유한 에이전트 이름을 할당하거나 둘 다에 대해 동일한 에이전트 이름을 사용합니다.
3. 소비자 리소스에 액세스하려고 할 때 챌린지가 표시되는 사용자에 대한 정책 도메인을 생성합니다.
4. 정책 도메인에 속한 리소스에 액세스할 수 있어야 하는 사용자를 선택합니다.

5. 다음 값으로 정책 도메인에 대한 영역을 정의합니다.

   에이전트

   어설션 당사자 웹 서버에 대한 에이전트

   리소스 필터

   웹 에이전트 r6.x QMR 6, r12.0 SP2, r12.0 SP3 및 SPS 페더레이션 게이트웨이. 다음과 같이 입력합니다.

   /siteminderagent/redirectjsp/

   리소스 필터 /siteminderagent/redirectjsp/는 FWS 응용 프로그램이 자동으로 설정하는 별칭입니다. 별칭 참조는 다음과 같습니다.

   - 웹 에이전트:

     web_agent_home/affwebservices/redirectjsp

   - SPS 페더레이션 게이트웨이:

     sps_home/secure-proxy/Tomcat/webapps/affwebservices/redirectjsp

   영구 세션

   SAML 아티팩트 프로필의 경우에만 영역 대화 상자의 "세션" 섹션에 있는 "영구" 확인란을 선택합니다. 영구 세션을 구성하지 않으면 사용자가 소비자 리소스에 액세스할 수 없습니다.

   나머지 설정의 경우 기본값을 적용하거나 필요에 따라 수정합니다.

6. "확인"을 클릭하여 영역을 저장합니다.
7. 영역에 대한 규칙을 생성합니다. "리소스" 필드에서 기본값인 별표(*)를 적용하여 영역에 대한 리소스를 모두 보호합니다.
8. 이전 단계에서 만든 규칙이 포함된 어설션 당사자 웹 서버에 대한 정책을 생성합니다.
9. 생성하는 어설션의 대상이 되는 사용자 선택 (페이지 136) 태스크를 완료합니다.

SAML 1.x 소비자에 대한 시간 제한 구성(선택 사항)

소비자 리소스를 사용할 수 있는 시기를 제한하는 시간 제한을 지정할 수 있습니다. 시간 제한을 지정하면 소비자 리소스에 대한 액세스가 지정된 기간 동안에만 허용됩니다. 사용자가 허용된 기간을 벗어나 리소스에 액세스하려고 하면 생산자가 SAML 어설션을 생성하지 않습니다.

참고: 시간 제한은 정책 서버가 설치된 서버의 시스템 클록을 기준으로 합니다.

시간 제한을 지정하려면

1. "일반" 설정에서 시작합니다.

   페이지의 "제한" 섹션에 있는 "시간"에서 "설정"을 클릭합니다.

   "시간 제한" 페이지가 표시됩니다.

2. 일정을 완료합니다. 이 일정 표는 규칙 개체의 "시간 제한" 표와 같습니다. 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.
3. "확인"을 클릭합니다.

시간 제한 일정이 설정되었습니다.

SAML 1.x 소비자에 대한 IP 주소 제한 구성(선택 사항)

소비자에 액세스하기 위해 브라우저가 실행되고 있는 웹 서버의 IP 주소, 범위 주소 또는 서브넷 마스크를 지정할 수 있습니다. IP 주소를 지정하면 소비자가 적절한 IP 주소의 사용자만 허용합니다.

IP 주소를 지정하려면

1. 관리 UI 의 "일반" 설정에서 시작합니다.

   페이지의 "제한" 섹션에 있는 "IP 주소" 영역에서 "추가"를 클릭합니다.

   "IP 제한" 페이지가 표시됩니다.

2. 추가하고 있는 IP 주소 유형에 대한 옵션을 선택하고 연결된 필드에 해당 주소 유형에 대한 데이터를 입력합니다.

   IP 주소는 모르지만 도메인 이름은 알고 있는 경우 "DNS 조회" 단추를 클릭하십시오. 이 단추를 클릭하면 "DNS 조회" 페이지가 열립니다. "호스트 이름" 필드에 정규화된 호스트 이름을 입력하고 "확인"을 클릭합니다.

   옵션은 다음과 같습니다.

   - 단일 호스트--브라우저를 호스트하는 단일 IP 주소를 지정합니다. 단일 IP 주소를 지정하면 사용자가 지정된 IP 주소에서만 소비자에 액세스할 수 있습니다.
   - 호스트 이름--호스트 이름을 사용하여 웹 서버를 지정합니다. 호스트 이름을 지정하면 지정된 호스트의 사용자만 소비자에 액세스할 수 있습니다.
   - 서브넷 마스크--웹 서버에 대한 서브넷 마스크를 지정합니다. 서브넷 마스크를 지정하면 지정된 서브넷 마스크의 사용자만 서비스 공급자에 액세스할 수 있습니다. 이 단추를 선택하면 "주소 및 서브넷 마스크 추가" 대화 상자가 열립니다. 왼쪽 및 오른쪽 화살표 단추를 사용하거나 슬라이더 막대를 클릭한 상태로 끌어서 놓아 서브넷 마스크를 선택합니다.
   - 범위--IP 주소 범위를 지정합니다. IP 주소 범위를 지정하면 소비자가 주소 범위에 속한 IP 주소 중 하나의 사용자만 허용합니다. 시작 및 끝 주소를 입력하여 범위를 결정합니다.

3. "확인"을 클릭하여 구성을 저장합니다.

생성하는 어설션의 대상이 되는 사용자 선택

어설션 당사자 측에서 수행되는 구성의 일부로, 어설션 생성기가 생성하는 SAML 어설션의 대상이 되는 사용자 및 그룹 목록을 포함하십시오. 어설션 당사자는 SAML 1.x 생산자, SAML 2.0 아이덴티티 공급자 또는 WS 페더레이션 계정 파트너입니다.

가맹 도메인에 있는 디렉터리의 사용자 및 그룹만 추가할 수 있습니다.

페더레이션된 트랜잭션에 대한 사용자 및 그룹을 지정하려면

1. 구성하고 있는 파트너에 대한 "사용자" 설정으로 이동합니다.

   "사용자 디렉터리" 페이지가 열리면서 정책 도메인의 각 사용자 디렉터리에 대한 항목이 표시됩니다.

2. 사용자 디렉터리의 사용자 또는 그룹을 정책에 추가합니다.

   각 사용자 디렉터리 테이블에서 "구성원 추가", "항목 추가", "모두 추가"를 선택할 수 있습니다. 선택하는 방법에 따라 사용자를 추가할 수 있는 대화 상자가 열립니다.

   - "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.
   - "항목 추가"를 선택하는 경우 "User Directory Search Express Edit"(사용자 디렉터리 검색 빠른 편집) 대화 상자에서 수동 입력 (페이지 138)을 통해 사용자를 선택합니다.

   오른쪽 화살표(>)를 클릭하여 사용자 또는 그룹을 편집하거나 빼기 기호(-)를 클릭하여 사용자 또는 그룹을 삭제합니다.

3. 아무 방법이나 사용하여 개별 사용자, 사용자 그룹 또는 둘 다를 선택하고 "확인"을 클릭합니다.

   "사용자 디렉터리" 페이지가 다시 열리면서 새 사용자가 사용자 디렉터리 테이블에 나열됩니다.

추가 정보:

리소스에 액세스하지 못하도록 사용자 또는 그룹 제외 (페이지 137)
리소스에 대한 중첩된 그룹 액세스 허용 (페이지 138)
수동 입력으로 사용자 추가 (페이지 138)

리소스에 액세스하지 못하도록 사용자 또는 그룹 제외

어설션을 획득하지 못하도록 사용자 또는 사용자 그룹을 제외할 수 있습니다.

다음 단계를 수행하십시오.

1. "사용자" 설정으로 이동합니다.
2. 특정 사용자 디렉터리에 대한 목록에서 사용자 또는 그룹을 선택합니다.
3. "제외"를 클릭하여 선택한 사용자 또는 그룹을 제외합니다.

   선택 사항이 관리 UI 에 반영됩니다.
4. "확인"을 클릭하여 변경 내용을 저장합니다.

리소스에 대한 중첩된 그룹 액세스 허용

LDAP 사용자 디렉터리에는 하위 그룹이 있는 그룹이 포함될 수 있습니다. 복합 디렉터리에서는 다른 그룹의 계층 구조에 중첩된 그룹을 사용하여 많은 양의 사용자 정보를 구성할 수 있습니다.

중첩된 그룹에 있는 사용자를 검색하도록 설정하는 경우 요청된 사용자 레코드가 모든 중첩된 그룹에서 검색됩니다. 중첩된 그룹이 사용되도록 설정하지 않은 경우에는 지정하는 그룹만 검색됩니다.

중첩된 그룹에서 검색하도록 설정하려면

1. "사용자" 설정으로 이동합니다.

   연결된 가맹 도메인에 여러 사용자 디렉터리가 포함된 경우 각 사용자 디렉터리가 자체 섹션에 나타납니다.
2. "중첩된 그룹 허용" 확인란을 선택하여 중첩된 그룹에서 검색하도록 설정합니다.

수동 입력으로 사용자 추가

어설션 생성을 위해 사용자를 지정할 때 선택할 수 있는 옵션 중 하나는 수동 입력으로 사용자를 식별하는 것입니다.

다음 단계를 수행하십시오.

1. 구성하고 있는 파트너에 대한 "사용자" 설정으로 이동합니다.

   가맹 도메인에 여러 사용자 디렉터리가 포함된 경우 모든 디렉터리가 "사용자 디렉터리" 페이지에 나타납니다.

2. "항목 추가"를 클릭합니다.

   "User Directory Search Express Edit"(사용자 디렉터리 검색 빠른 편집) 페이지가 표시됩니다.

3. 검색 옵션을 선택하고 해당 검색 옵션에 대한 필드에 데이터를 입력합니다.

   검색 위치

   LDAP 디렉터리의 경우 드롭다운 목록에서 옵션을 선택합니다.

   DN 유효성 검사

   LDAP 검색이 디렉터리에서 이 DN 을 찾습니다.

   사용자 검색

   LDAP 검색이 일치하는 사용자 항목으로 제한됩니다.

   그룹 검색

   LDAP 검색이 일치하는 그룹 항목으로 제한됩니다.

   조직 검색

   LDAP 검색이 일치하는 조직 항목으로 제한됩니다.

   모든 항목 검색

   LDAP 검색이 일치하는 사용자, 그룹 및 조직 항목으로 제한됩니다.

   - Microsoft SQL Server, Oracle 및 WinNT 디렉터리의 경우 "수동 입력" 필드에 사용자 이름을 입력할 수 있습니다.
   - Microsoft SQL Server 또는 Oracle 의 경우 SQL 쿼리를 대신 입력할 수 있습니다. 예를 들면 다음과 같습니다.

     SELECT NAME FROM EMPLOYEE WHERE JOB ='MGR';

     정책 서버는 사용자 디렉터리에 대한 "연결 자격 증명" 탭의 "사용자 이름" 필드에 지정된 데이터베이스 사용자로 쿼리를 수행합니다. "수동 입력" 필드에 대한 SQL 문을 작성하는 경우 사용자 디렉터리에 대한 데이터베이스 스키마를 숙지해야 합니다. 예를 들어 SmSampleUsers 스키마를 사용하고 있는 경우 특정 사용자를 추가하려면 SmUser 테이블에서 사용자 항목을 선택합니다.
   - LDAP 디렉터리의 경우 모든 디렉터리 항목을 추가하려면 "수동 입력" 필드에 **all** 을 입력합니다.

4. "확인"을 클릭하여 변경 내용을 저장합니다.

SAML 1.x 어설션 구성

생산자 사이트에서 SAML 어설션을 소비자에게 전달하는 방법을 결정하십시오. 어설션은 소비자에서 사용자를 식별합니다.

어설션은 다음 정보가 포함된 XML 문서입니다.

- 소비자에 대한 정보
- 세션 정보
- 사용자 특성

SAML 어설션에 대한 자세한 내용은 OASIS 웹 사이트의 SAML 사양을 참조하십시오.

SAML 1.x 어설션을 구성하려면

1. "어설션" 설정으로 이동합니다.
2. "어설션" 페이지의 필드에 데이터를 입력합니다. 필드 설명을 보려면 "도움말"을 클릭하십시오.
   - 어설션 소비자 URL(SAML POST 의 경우 필수 사항, SAML 아티팩트의 경우 선택 사항)

     SAML 1.x 아티팩트 바인딩의 경우 어설션 소비자 URL 이 필수 사이트 간 전송 URL 매개 변수인 SMCONSUMERURL 쿼리 매개 변수보다 우선합니다. 사용자가 이 URL 을 선택하면 싱글 사인온이 시작됩니다. 악의적인 사용자가 쿼리 매개 변수를 수정하고 아티팩트 검색을 위해 사용자를 권한 없는 사이트로 보낼 수 있습니다. 사용자가 잘못 연결되지 않도록 하려면 어설션 소비자 URL 에 대한 값을 지정하십시오.
   - 차이 시간 초

     생산자의 시스템 클록과 소비자의 시스템 클록 간의 차이(초)를 지정합니다. 차이 시간은 싱글 사인온과 싱글 로그아웃에 사용됩니다.

     싱글 사인온의 경우 차이 시간 및 싱글 사인온 유효 기간 값에 따라 어설션 유효 기간이 결정됩니다. 어설션 유효 기간 계산 (페이지 141) 방법을 검토하면 차이 시간에 대해 자세히 이해할 수 있습니다.
3. "마침"을 클릭하여 선택한 항목을 저장합니다.

"어설션" 페이지에는 선택 사항인 특성 (페이지 153) 섹션도 있습니다. 이 섹션에서는 어설션에 특성을 포함시킬 수 있습니다.

추가 정보:

SAML 1.x 어설션 관련 보안 문제 (페이지 141)

SAML 1.x 어설션 관련 보안 문제

SAML 어설션 생성기는 임의의 인증 체계 보호 수준에서 인증된 사용자에 대한 세션을 기반으로 어설션을 생성합니다. 생산자가 어설션을 생성하는 사용자는 제어할 수 있습니다. 사용자가 인증되는 보호 수준은 제어할 수 없습니다.

특정 보호 수준이 필요한 리소스가 있을 수 있습니다. 다양한 보호 수준에서 리소스를 보호할 수 있습니다. 사용자가 인증될 때 원하는 보호 수준으로 인증되는지 확인하십시오.

싱글 사인온에 대한 어설션 유효 기간

싱글 사인온의 경우 차이 시간 및 유효 기간 값에 따라 SiteMinder 가 어설션의 총 유효 기간을 계산하는 방법이 결정됩니다. SiteMinder 는 어설션의 생성 및 소비에 차이 시간을 적용합니다.

참고: 이 설명에서 어설션 당사자는 SAML 1.x 생산자, SAML 2.0 아이덴티티 공급자 또는 WS-페더레이션 계정 파트너입니다. 신뢰 당사자는 SAML 1.x 소비자, SAML 2.0 서비스 공급자 또는 WS-페더레이션 리소스 파트너입니다.

어설션 문서에서 NotBefore 및 NotOnOrAfter 값은 유효 간격의 시작 및 끝을 나타냅니다.

어설션 당사자 측에서 SiteMinder 는 어설션 유효 기간을 설정합니다. 유효 간격은 어설션이 생성되는 시스템 시간입니다. SiteMinder 는 이 시간을 사용하여 어설션의 IssueInstant 값을 설정한 다음 IssueInstant 값에서 차이 시간 값을 뺍니다. 그 결과로 얻은 시간이 NotBefore 값입니다.

NotBefore = IssueInstant - 차이 시간

유효 간격의 끝을 결정하기 위해 SiteMinder 는 유효 기간 값과 차이 시간을 IssueInstant 값에 더합니다. 그 결과로 얻은 시간은 NotOnOrAfter 값이 됩니다.

NotOnOrAfter = 유효 기간 + 차이 시간 + IssueInstant

시간은 GMT 를 기준으로 합니다.

예를 들어 어설션 당사자 측에서 어설션이 1:00 GMT 에 생성된다고 가정합니다. 차이 시간은 30 초이고 유효 기간은 60 초이며 어설션 유효 간격은 12:59:30 GMT 에서 1:01:30 GMT 사이입니다. 이 간격은 어설션이 생성된 시간보다 30 초 전에 시작되고 90 초 후에 끝납니다.

신뢰 당사자 측에서 SiteMinder 는 어설션 당사자 측에서와 동일한 계산을 수행하여 수신된 어설션이 유효한지 확인합니다.

SiteMinder 가 파트너 관계의 양쪽 모두에 있는 경우의 어설션 유효 기간 계산

SiteMinder 가 파트너 관계의 양쪽 모두에 있는 경우 어설션 유효 기간은 유효 기간을 차이 시간의 두 배에 더한 합계입니다. 공식은 다음과 같습니다.

어설션 유효 기간 = 2 x 차이 시간(어설션 당사자) + 유효 기간 + 2 x 차이 시간(신뢰 당사자)

공식의 초기 부분(2 x 차이 시간 + 유효 기간)은 어설션 당사자의 유효 기간 시작 및 끝을 나타냅니다. 공식의 두 번째 부분(2 x 차이 시간)은 신뢰 당사자에 있는 시스템 클록의 차이 시간을 나타냅니다. 2 를 곱하는 이유는 유효 기간의 NotBefore 및 NotOnOrAfter 끝을 고려하기 때문입니다.

참고: 레거시 페더레이션의 경우 유효 기간은 어설션 당사자 측에서만 설정됩니다.

예

어설션 당사자

어설션 당사자 측에서의 값은 다음과 같습니다.

- IssueInstant = 5:00PM
- 유효 기간 = 60 초
- 차이 시간 = 60 초
- NotBefore = 4:59PM
- NotOnOrAfter = 5:02PM

신뢰 당사자

신뢰 당사자는 어설션의 NotBefore 및 NotOnOrAfter 값을 사용하고 해당 차이 시간을 이러한 값에 적용합니다. 이 공식은 신뢰 당사자가 새 NotBefore 및 NotOnOrAfter 값을 계산하는 방법입니다.

- 차이 시간 = 180 초(3 분)
- NotBefore = 4:56PM
- NotOnOrAfter = 5:05PM

어설션 유효 기간 창

이 예제의 값을 사용한 전체 어설션 유효 기간 창의 계산은 다음과 같습니다.

120 초(2 x 60) + 60 초 + 360 초(2 x 180) = 540 초(9 분)

일회 사용하기 위한 어설션 구성

SAML 1.x 사양에 따라 SiteMinder 가 어설션의 일회 사용을 적용할 수 있습니다. 일회 사용하기 위한 어설션을 생성하여 신뢰 당사자에게 향후 트랜잭션 용도로 어설션을 보관하지 않음을 알립니다. 유효 기간이 지난 어설션을 재사용하면 오래된 아이덴티티 정보를 사용하여 인증 결정이 내려집니다.

일회 사용하기 위한 어설션을 구성하려면

1. 가맹 개체에 대한 "일반" 설정으로 이동합니다.
2. "고급" 섹션에서 "DoNotCache 조건 설정"을 선택합니다.
3. "제출"을 클릭합니다.

어설션 검색 서비스에 대한 액세스 권한 부여(아티팩트 SSO)

HTTP-아티팩트 싱글 사인온의 경우 어설션을 얻기 위한 FWS 서비스를 보호하는 정책에 액세스할 수 있는 권한이 신뢰 당사자에게 필요합니다.

액세스 권한을 부여하려면

- 에이전트 그룹 FederationWebServicesAgentGroup 에 FWS 응용 프로그램을 보호하는 웹 에이전트를 추가하십시오.
- 특정 서비스에 액세스하도록 허용된 사용자로 신뢰 파트너를 추가하십시오 (페이지 145).

  지정된 정책에 사용자를 추가하는 것 외에는 다른 모든 정책 개체가 자동으로 설정됩니다.

페더레이션 에이전트 그룹에 웹 에이전트 추가

에이전트 그룹 FederationWebServicesAgentGroup 에 FWS 응용 프로그램을 보호하는 웹 에이전트를 추가하십시오.

- ServletExec 의 경우 이 에이전트는 웹 에이전트 옵션 팩이 설치된 웹 서버에 있습니다.
- WebLogic 이나 JBOSS 와 같은 응용 프로그램 서버의 경우 이 웹 에이전트는 응용 프로그램 서버 프록시가 설치된 위치에 설치됩니다. 웹 에이전트 옵션 팩은 다른 시스템에 있을 수 있습니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "인프라", "에이전트", "에이전트"를 차례로 클릭합니다.
3. "에이전트 만들기"를 클릭합니다.
4. 배포에 있는 웹 에이전트의 이름을 지정합니다. "제출"을 클릭합니다.
5. "인프라", "에이전트", "에이전트 그룹"을 차례로 클릭합니다.
6. "FederationWebServicesAgentGroup" 항목을 선택합니다.
7. "추가/제거"를 클릭합니다. 그러면 "에이전트 그룹 구성원" 대화 상자가 열립니다.
8. "사용 가능한 구성원" 목록에서 "선택한 구성원" 목록으로 웹 에이전트를 이동합니다.
9. "확인"을 클릭하여 "에이전트 그룹" 대화 상자로 돌아갑니다.
10. "제출", "닫기"를 차례로 클릭하여 기본 페이지로 돌아갑니다.

어설션을 획득하기 위한 FWS 정책에 신뢰 파트너 추가

싱글 사인온에 대해 HTTP-아티팩트 바인딩을 사용하고 있는 경우 파트너 관계의 신뢰 당사자에게 어설션 검색 서비스에 액세스할 수 있는 권한이 있어야 합니다. SiteMinder 는 정책으로 SAML 1.x 및 2.0 검색 서비스를 보호합니다.

정책 서버를 설치하면 FederationWebServicesDomain 이 기본적으로 설치됩니다. 이 도메인에는 SiteMinder 가 어설션을 검색하는 서비스에 대한 다음 정책이 포함되어 있습니다.

SAML 1.x

FederationWSAssertionRetrievalServicePolicy

SAML 2.0

SAML2FWSArtifactResolutionServicePolicy

참고: WS-페더레이션은 HTTP-아티팩트 프로필을 사용하지 않습니다. 따라서 이 절차는 리소스 공급자에게 적용되지 않습니다.

이러한 정책에 모든 관련 신뢰 파트너에 대한 액세스 권한을 부여하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에서 "정책", "도메인", "도메인 정책"으로 이동합니다.

   도메인 정책 목록이 표시됩니다.

2. SAML 프로필에 대한 정책을 선택합니다.

   SAML 1.x

   FederationWSAssertionRetrievalServicePolicy

   SAML 2.0

   SAML2FWSArtifactResolutionServicePolicy

   "도메인 정책" 페이지가 열립니다.

3. "수정"을 클릭하여 정책을 변경합니다.

4. "사용자" 탭을 선택합니다.

5. 적절한 사용자 디렉터리에 대한 대화 상자에서 "구성원 추가"를 클릭합니다.

   SAML 1.x

   FederationWSCustomUserStore

   SAML 2.0

   SAML2FederationCustomUserStore

   "사용자/그룹" 페이지가 열립니다.

   이전에 구성한 가맹 도메인이 "사용자/그룹" 대화 상자에 나열됩니다. 예를 들어 가맹 도메인의 이름이 fedpartners 인 경우 항목은 **affiliate:fedpartners** 입니다.

6. 서비스에 대한 액세스 권한이 필요한 파트너가 있는 가맹 도메인 옆의 확인란을 선택합니다. "확인"을 클릭합니다.

   "사용자 디렉터리" 목록으로 돌아갑니다.

7. "제출"을 클릭합니다.

   정책 목록으로 돌아갑니다.

어설션 검색 서비스의 기본 보호 확인

어설션 검색 서비스를 보호하도록 기본 인증을 구성하는 경우 보호를 확인하십시오.

다음 단계를 수행하십시오.

1. 웹 브라우저를 엽니다.

   페더레이션 웹 서비스 응용 프로그램이 설치된 서버에 대한 정규화된 호스트 이름 및 포트 번호를 입력하여 페더레이션 웹 서비스에 액세스합니다. 예를 들면 다음과 같습니다.

   SAML 1.x: http://idp-fws.ca.com:81/affwebservices/assertionretriever

   SAML 2.0: http://idp-fws.ca.com:81/affwebservices/saml2artifactresolution

   서비스가 보호된 경우 SiteMinder 가 자격 증명에 대한 챌린지를 표시합니다. 권한 있는 가맹만 페더레이션 웹 서비스에 액세스하도록 허용됩니다.

2. 정책 서버에서 구성된 신뢰 당사자에 대해 유효한 이름 및 암호를 입력합니다. 이름 및 암호는 인증 챌린지에 대한 자격 증명입니다.

인증 챌린지는 서비스가 보호됨을 나타냅니다. SiteMinder 가 챌린지를 표시하지 않으면 정책이 잘못 구성된 것입니다.

아티팩트 서비스를 보호하는 인증 체계 구성

HTTP-아티팩트 프로필의 경우 어설션 검색 서비스(SAML 1.x)와 아티팩트 레졸루션 서비스(SAML 2.0)는 어설션 당사자 측에서 어설션을 검색합니다. 이러한 서비스가 신뢰 당사자에게 어설션 응답을 보내는 경우 해당 어설션 응답은 보안 백 채널을 통해 전송됩니다. 권한 없는 액세스로부터 이러한 서비스와 백 채널을 통한 통신을 보호하는 것이 좋습니다.

참고: WS-페더레이션은 HTTP-아티팩트 프로필을 지원하지 않습니다.

이러한 서비스를 보호하려면 어설션 당사자 측에서 서비스가 포함된 영역에 대한 인증 체계를 지정하십시오. 인증 체계는 신뢰 당사자의 소비 서비스가 백 채널을 통해 관련 서비스에 액세스하기 위해 제공해야 하는 자격 증명 유형을 지정합니다.

다음 인증 체계 중 하나를 선택할 수 있습니다.

- 기본 (페이지 148)
- SSL 을 통한 기본 인증 (페이지 149)
- X.509 클라이언트 인증서 (페이지 149)

기본 인증으로 어설션 검색 서비스 보호

HTTP-아티팩트 싱글 사인온의 경우 어설션 당사자가 보안 백 채널을 통해 어설션을 신뢰 당사자에게 보냅니다. 기본 인증의 경우 아티팩트를 확인하고 어설션을 검색하는 서비스에 액세스하기 위한 암호를 구성하십시오. 그러면 서비스가 백 채널을 통해 신뢰 당사자에게 어설션을 보냅니다.

SSL 이 사용되도록 설정한 상태로 기본 인증을 사용할 수 있지만 SSL 이 반드시 필요한 것은 아닙니다.

참고: 암호는 "기본 인증" 또는 "SSL 을 통한 기본 인증"을 백 채널을 통한 인증 방법으로 사용하는 경우에만 관련됩니다.

SAML 1.x 어설션 검색 서비스의 경우 다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. 생산자에 대한 "일반" 설정으로 이동합니다.
3. 다음 필드에 대한 값을 입력합니다.
   - 암호
   - 암호 확인
4. "제출"을 클릭하여 변경 내용을 저장합니다.

SAML 2.0 아티팩트 레졸루션 서비스의 경우 다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. 아이덴티티 공급자에 대한 "특성" 설정으로 이동합니다.
3. "백 채널" 섹션에서 다음 필드에 대한 값을 입력합니다.
   - 암호
   - 암호 확인
4. "제출"을 클릭하여 변경 내용을 저장합니다.

SSL 을 통한 기본 인증으로 어설션 검색 서비스 보호

SSL 을 통한 기본 인증 체계로 어설션 검색 서비스(SAML 1.x)나 아티팩트 레졸루션 서비스(SAML 2.0)를 보호할 수 있습니다. 어설션 당사자 측에서는 정책 서버를 설치할 때 서비스를 보호하기 위한 기본 정책 집합이 이미 구성되어 있습니다.

필요한 구성은 각 파트너에서 SSL 이 사용되도록 설정하는 것뿐입니다. 어설션 당사자 또는 신뢰 당사자 측에서 다른 구성은 필요하지 않습니다. 신뢰 당사자 측에서 인증서 데이터 저장소의 기본 루트 CA(인증 기관) 중 하나를 사용하여 SSL 연결을 설정할 수 있습니다. 기본 CA 대신 사용자 고유의 루트 CA 를 사용하려면 CA 인증서를 데이터 저장소로 가져오십시오.

SSL 을 통한 기본 인증 체계를 사용하는 경우 모든 끝점 URL 은 SSL 통신을 사용해야 합니다. 즉, URL 이 **https://**로 시작해야 합니다. 끝점 URL 은 서버에서 싱글 사인온, 싱글 로그아웃, 어설션 소비자 서비스, 아티팩트 레졸루션 서비스(SAML 2.0), 어설션 검색 서비스(SAML 1.x) 등의 다양한 SAML 서비스를 찾습니다.

클라이언트 인증서 인증으로 어설션 검색 서비스 보호

클라이언트 인증서 인증 체계로 어설션 검색 서비스(SAML 1.x)나 아티팩트 레졸루션 서비스(SAML 2.0)를 보호할 수 있습니다. 어설션 당사자가 클라이언트 인증서 인증을 요구하도록 구성된 경우 신뢰 당사자는 어설션 당사자에 역방향으로 연결하고 클라이언트 인증서를 제공하려고 합니다.

클라이언트 인증서 인증 체계를 사용하려면

1. 어설션 당사자 측에서 관련 서비스를 보호할 정책을 생성합니다. 이 정책은 클라이언트 인증서 인증 체계를 사용합니다.
2. 신뢰 당사자 측에서 백 채널 구성에 대해 클라이언트 인증서 인증이 사용되도록 설정합니다.
3. 파트너 관계 양쪽에서 SSL 이 사용되도록 설정합니다.

클라이언트 인증서 인증을 사용하는 경우에는 모든 끝점 URL 이 SSL 통신을 사용해야 합니다. 따라서 URL 이 **https://**로 시작해야 합니다. 끝점 URL 은 서버에서 싱글 사인온, 싱글 로그아웃, 어설션 소비자 서비스, 아티팩트 레졸루션 서비스(SAML 2.0), 어설션 검색 서비스(SAML 1.x) 등의 다양한 SAML 서비스를 찾습니다.

ServletExec 를 실행 중인 다음 웹 서버에는 클라이언트 인증서 인증을 사용할 수 없습니다.

- SiteMinder 생산자/아이덴티티 공급자의 IIS 웹 서버 - IIS 의 제한 때문
- SiteMinder 생산자/아이덴티티 공급자의 SunOne/Sun Java Server 웹 서버 - ServletExec 에 설명된 제한 때문

검색 서비스를 보호하기 위한 정책 만들기

어설션 당사자 측에서 어설션 당사자의 어설션 검색 서비스를 보호하기 위한 정책을 생성하십시오.

다음 단계를 수행하십시오.

1. 어설션을 요청하는 가맹 각각에 대해 별개의 항목을 사용자 디렉터리에 추가합니다. 사용자 디렉터리를 생성하거나 기존 디렉터리를 사용합니다.

   사용자 레코드에 관리 UI 에 있는 가맹 일반 설정의 "이름" 필드에 지정된 것과 동일한 값을 입력합니다. 예를 들어 가맹에 대한 "이름" 필드 값이 Company A 인 경우 사용자 디렉터리 항목은 다음과 같습니다.

   uid=CompanyA, ou=Development,o=CA

   정책 서버가 가맹 클라이언트 인증서의 주체 DN 값을 이 디렉터리 항목에 매핑합니다.

2. 구성된 사용자 디렉터리를 FederationWebServicesDomain 에 추가합니다.

3. 인증서 매핑 항목을 생성합니다.

   특성 이름을 가맹에 대한 사용자 디렉터리 항목에 매핑합니다. 특성은 가맹에 대한 인증서의 주체 DN 항목을 나타냅니다. 예를 들어 특성 이름으로 CN 을 선택하는 경우 이 값은 cn=CompanyA,ou=Development,o=partner 라는 가맹을 나타냅니다.

   매핑 설정을 위해 "인프라", "디렉터리", "인증서 매핑"으로 이동합니다.

4. X509 클라이언트 인증서 인증 체계를 구성합니다.

5. FederationWebServicesDomain 아래에 다음 항목이 포함된 영역을 생성합니다.

   이름

   any_name

   예: cert assertion retrieval

   에이전트

   FederationWebServicesAgentGroup

   리소스 필터

   /affwebservices/certassertionretriever(SAML 1.x)

   /affwebservices/saml2certartifactresolution(SAML 2.0)

   인증 체계

   이전 단계에서 생성한 클라이언트 인증서 인증 체계입니다.

6. cert assertion retrieval 영역 아래에 다음 정보가 포함된 규칙을 생성합니다.

   이름

   any_name

   예: cert assertion retrieval rule

   Resource

   *

   웹 에이전트 작업

   GET, POST, PUT

7. FederationWebServicesDomain 아래에 웹 에이전트 응답 헤더를 생성합니다.

   어설션 검색 서비스가 이 HTTP 헤더를 사용하여 가맹이 어설션을 검색하는 사이트인지 확인합니다.

   다음 값이 포함된 응답을 생성합니다.

   이름

   any_name

   특성

   WebAgent-HTTP-Header-Variable

   특성 종류

   사용자 특성

   변수 이름

   consumer_name

   특성 이름

   가맹 이름 값이 포함된 사용자 디렉터리 특성을 입력합니다.

   예: uid=CompanyA

   다음 항목을 기반으로 웹 에이전트가 HTTP_CONSUMER_NAME 이라는 응답을 반환합니다.

8. FederationWebServicesDomain 아래에 다음 값이 포함된 정책을 생성합니다.

   이름

   any_name

   사용자

   이 절차에서 이전에 생성한 사용자 디렉터리의 사용자를 추가합니다.

   규칙

   rule_created_earlier_in_this_procedure

   응답

   response_created_earlier_in_this_procedure

아티팩트 레졸루션 서비스를 보호하기 위한 정책이 완료되었습니다.

신뢰 당사자 측에서 관리자가 관련 어설션 서비스에 연결하는 백 채널을 통해 클라이언트 인증서 인증이 사용되도록 설정해야 합니다.

SAML 1.x: 어설션 검색 서비스에 대해 클라이언트 인증서 인증이 사용되도록 설정 (페이지 188)

SAML 2.0: 아티팩트 레졸루션 서비스에 대해 클라이언트 인증서 인증이 사용되도록 설정 (페이지 300)

SAML 1.x 어설션에 포함할 특성 구성(선택 사항)

특성을 어설션에 포함할 수 있습니다. 그러면 서블릿이나 응용 프로그램에서 특성을 사용하여 사용자 지정된 콘텐츠를 표시할 수 있습니다. 생산자에서 어설션에 있는 소비자로 사용자 특성, DN 특성 또는 정적 데이터를 모두 전달할 수 있습니다. 웹 응용 프로그램에서 사용되는 경우 특성은 사용자가 소비자에서 수행하는 작업을 제한할 수 있습니다. 예를 들어 생산자가 "Authorized Amount"(권한 부여된 금액)라는 특성을 보낸다고 가정합니다. 이 경우 소비자는 이 특성을 사용자가 소비할 수 있는 최대 금액(달러)으로 설정합니다.

특성은 이름/값 쌍의 형태를 지니며 우편 주소, 직함, 트랜잭션에 대해 승인된 소비 제한 등의 정보를 포함합니다. 소비자가 어설션을 받으면 특성을 추출합니다. 그런 다음 소비자가 특성을 HTTP 헤더 변수나 HTTP 쿠키 변수로 응용 프로그램에 제공합니다.

특성을 전달하려면 응답을 구성하십시오. 이러한 용도로 사용할 수 있는 응답은 다음과 같습니다.

- Affiliate-HTTP-Header-Variable
- Affiliate-HTTP-Cookie-Variable

HTTP 헤더와 HTTP 쿠키에는 어설션 특성이 초과할 수 없는 크기 제한이 있습니다. 크기 제한은 다음과 같습니다.

- HTTP 헤더의 경우 SiteMinder 는 헤더에 대한 웹 서버 크기 제한까지 헤더에 있는 특성을 보낼 수 있습니다. 헤더당 허용되는 어설션 특성은 하나뿐입니다. 헤더 크기 제한을 확인하려면 해당 웹 서버 설명서를 참조하십시오.
- HTTP 쿠키의 경우 SiteMinder 는 쿠키에 대한 크기 제한까지 쿠키를 보낼 수 있습니다. 각 어설션 특성은 자체 쿠키로 전송됩니다. 쿠키 크기 제한은 브라우저별로 다르고, 해당 제한은 각 특성에만 적용되는 것이 아니라 응용 프로그램에 전달되고 있는 모든 특성에 적용됩니다. 쿠키 크기 제한을 확인하려면 해당 웹 브라우저 설명서를 참조하십시오.

추가 정보:

SAML 1.x 어설션에 대한 특성 구성 (페이지 154)
스크립트를 사용하여 새 응답 특성 만들기 (페이지 157)

SAML 1.x 어설션에 대한 특성 구성

SAML 어설션에서 소비자 사이트에 있는 대상 응용 프로그램으로 특성을 전달하도록 응답을 구성할 수 있습니다.

어설션에 대한 특성을 구성하려면

1. "어설션" 설정으로 이동합니다.
2. "특성" 섹션에서 "추가"를 클릭합니다.

   "특성 추가" 대화 상자가 열립니다.
3. "특성 유형" 드롭다운에서 헤더 변수를 구성할지 아니면 쿠키 변수를 구성할지 선택합니다.

4. "특성 설정" 섹션의 "특성 종류" 섹션에서 다음 옵션 중 하나를 선택합니다.
   - 정적
   - 사용자 특성
   - DN 특성

   필드 설명을 보려면 "도움말"을 클릭하십시오.

   선택 항목에 따라 "특성 필드" 섹션에서 사용 가능한 필드가 결정됩니다.
5. 선택한 특성 종류에 대한 필드에 데이터를 입력합니다. 선택한 특성 종류에 따라 구성해야 하는 추가 필드가 결정됩니다.

   정적

   다음 필드에 정보를 입력합니다.

   - 변수 이름

     SiteMinder 가 가맹에 반환하는 특성에 대한 이름을 입력합니다.
   - 변수 값

     정적 텍스트를 이름/값 쌍에 대한 값으로 입력합니다.

     예를 들어 이름/값 쌍 show_content=yes 를 반환하려면 show_content 를 변수 이름으로, yes 를 변수 값으로 입력합니다.

   사용자 특성

   다음 필드에 정보를 입력합니다.

   - 변수 이름

     SiteMinder 가 소비자에게 반환하는 특성에 대한 이름을 입력합니다.
   - 특성 이름

     이름/값 쌍에 대한 사용자 디렉터리의 특성을 입력합니다.

     예를 들어 사용자의 전자 메일 주소를 소비자에게 반환하려면 email_address 를 변수 이름으로, email 을 특성 이름으로 입력합니다.

DN 특성

다음 필드에 정보를 입력합니다.

- 변수 이름

  SiteMinder 가 소비자에게 반환하는 특성에 대한 이름을 입력합니다.

- DN 사양

  SiteMinder 가 사용자 특성을 검색하는 사용자 그룹의 고유 이름을 입력합니다. DN 값이 소비자에게 반환됩니다. DN 을 모르는 경우 "조회"를 클릭합니다. "SiteMinder 사용자 조회" 대화 상자를 사용하여 사용자 그룹을 찾고 DN 을 선택합니다.

- 특성 이름

  이 이름/값 쌍 특성에 대한 사용자 디렉터리의 특성을 입력합니다.

"특성" 메뉴에서 "Affiliate-HTTP-Cookie-Variable"을 선택한 경우 "변수 이름" 필드 레이블이 "쿠키 이름"으로 변경됩니다.

6. (선택 사항) 중첩된 그룹에서 DN 특성을 검색하려면 "특성 종류" 섹션에서 "중첩된 그룹 허용" 확인란을 선택합니다.
7. "확인"을 클릭하여 변경 내용을 저장합니다.

어설션 특성의 최대 길이 지정

사용자 어설션 특성의 최대 길이를 구성할 수 있습니다. 어설션 특성의 최대 길이를 수정하려면 EntitlementGenerator.properties 파일에서 해당 설정을 변경하십시오.

이 파일에 있는 속성 이름은 구성하고 있는 프로토콜에 따라 다릅니다.

다음 단계를 수행하십시오.

1. 정책 서버가 설치된 시스템에서 *policy_server_home*\config\properties\EntitlementGenerator.properties 로 이동합니다.
2. 텍스트 편집기에서 파일을 엽니다.

3. 사용자의 환경에서 사용하고 있는 프로토콜에 맞게 사용자 특성의 최대 길이를 조정합니다. 각 프로토콜에 대한 설정은 다음과 같습니다.

   WS-페더레이션

   속성 이름:
   com.netegrity.assertiongenerator.wsfed.MaxUserAttributeLength

   속성 유형: 양의 정수 값

   기본값: 1024

   설명: WS-FED 어설션 특성의 최대 특성 길이를 나타냅니다.

   SAML 1.x

   속성 이름:
   com.netegrity.assertiongenerator.saml1.MaxUserAttributeLength

   속성 유형: 양의 정수 값

   기본값: 1024

   설명: SAML1.1 어설션 특성의 최대 특성 길이를 나타냅니다.

   SAML 2.0

   속성 이름:
   com.netegrity.assertiongenerator.saml2.MaxUserAttributeLength

   속성 유형: 양의 정수 값

   기본값: 1024

   설명: SAML2.0 어설션 특성의 최대 특성 길이를 나타냅니다.

4. 이러한 매개 변수를 변경한 후 정책 서버를 다시 시작합니다.

스크립트를 사용하여 새 응답 특성 만들기

"특성 추가" 페이지의 "고급" 섹션에는 "스크립트" 필드가 포함되어 있습니다. 이 필드에는 "특성 설정" 섹션에 입력한 사항을 기반으로 SiteMinder 가 생성하는 스크립트가 표시됩니다. 이 필드의 내용을 복사하여 다른 응답 특성에 대한 "스크립트" 필드에 붙여 넣을 수 있습니다.

참고: "스크립트" 필드의 내용을 복사하여 다른 특성에 붙여 넣는 경우 "특성 종류" 그룹에서 적절한 옵션 단추를 선택하십시오.

SAML 어설션 응답 사용자 지정(선택 사항)

어설션 생성기 플러그인을 사용하여 어설션 콘텐츠를 수정할 수 있습니다. 플러그인을 통해 사용자와 파트너 및 공급업체 간의 비즈니스 계약을 사용하는 어설션 콘텐츠를 사용자 지정할 수 있습니다. 플러그인은 각 파트너에 대해 하나씩 허용됩니다.

어설션 생성기 플러그인을 구성하는 단계는 다음과 같습니다.

1. 아직 설치하지 않은 경우 SiteMinder SDK 를 설치합니다.
2. SDK 의 일부인 AssertionGeneratorPlugin.java 인터페이스를 구현합니다.
3. 어설션 생성기 플러그인 구현 클래스를 배포합니다.
4. 관리 UI 에서 어설션 생성기 플러그인 매개 변수가 사용되도록 설정합니다.

어설션 생성기 플러그인에 대한 추가 정보는 다음과 같이 찾을 수 있습니다.

- 참조 정보(메서드 서명, 매개 변수, 반환 값, 데이터 형식)와 UserContext 클래스에 대한 새 생성자는 *Javadoc 참조서*에서 확인할 수 있습니다. Javadoc 의 AssertionGeneratorPlugin 인터페이스를 참조하십시오.
- 인증 및 권한 부여 API 에 대한 개요와 개념 정보는 *SiteMinder Programming Guide for Java*(SiteMinder Java 프로그래밍 안내서)에 있습니다.

AssertionGeneratorPlugin 인터페이스 구현

사용자 지정 어설션 생성기 플러그인을 생성할 때의 첫 번째 단계는 AssertionGeneratorPlugin 인터페이스를 구현하는 것입니다.

다음 단계를 수행하십시오.

1. 매개 변수가 포함되지 않은 공개 기본 생성자 메서드를 제공합니다.
2. 상태 비저장 구현이 되도록 코드를 제공합니다. 여러 스레드가 단일 플러그인 클래스를 사용할 수 있어야 합니다.

3. 인터페이스에서 요구 사항을 충족할 메서드를 구현합니다.

   구현에 customizeAssertion 메서드 호출이 포함되어야 합니다. 기존 구현을 덮어쓸 수 있습니다. 이에 대한 예는 다음 샘플 클래스를 참조하십시오.

   SAML 1.x/WS-페더레이션

   AssertionSample.java

   SAML 2.0

   SAML2AssertionSample.java

   샘플 클래스는 /sdk/samples/assertiongeneratorplugin 디렉터리에 있습니다.

   구현이 customizeAssertion 메서드에 전달하는 매개 변수 문자열의 내용은 사용자 지정 개체의 책임입니다.

어설션 생성기 플러그인 배포

AssertionGeneratorPlugin 인터페이스에 대한 구현 클래스를 코드화했으면 해당 구현 클래스를 컴파일하고 SiteMinder 가 실행 파일을 찾을 수 있는지 확인하십시오.

어설션 생성기 플러그인을 배포하려면

1. 어설션 플러그인 Java 파일을 컴파일합니다.

   컴파일하려면 정책 서버와 함께 설치되는 다음 .jar 파일이 필요합니다.

   - *policy_server_home*/bin/jars/SmJavaApi.jar
   - *policy_server_home*/bin/thirdparty/xercesImpl.jar
   - *policy_server_home*/bin/endorsed/xalan.jar

2. JVMOptions.txt 파일에서 플러그인의 클래스 경로를 포함하도록 -Djava.class.path 값을 수정합니다. 이렇게 수정하면 수정된 클래스 경로를 사용하여 플러그인을 로드할 수 있습니다. *installation_home*\siteminder\config 디렉터리에서 JVMOptions.txt 파일을 찾습니다.

   참고: xercesImpl.jar, xalan.jar 또는 SMJavaApi.jar 의 클래스 경로를 수정하지 마십시오.

3. 플러그인이 사용되도록 설정합니다.

어설션 생성기 플러그인이 사용되도록 설정

어설션 생성기 플러그인을 작성하고 컴파일한 후 관리 UI 에서 설정을 구성하여 플러그인이 사용되도록 설정하십시오. UI 매개 변수는 SiteMinder 에게 플러그인을 찾을 수 있는 위치를 알려 줍니다.

플러그인을 배포 (페이지 159)할 때까지 플러그인 설정을 구성하지 마십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그온합니다.
2. "페더레이션", "레거시 페더레이션", "가맹"을 차례로 클릭합니다.
3. 기존 가맹 항목을 선택하거나 새로 생성합니다.
4. "일반" 설정으로 이동합니다.
5. "어설션 생성기 플러그인" 섹션의 다음 필드에 데이터를 입력합니다.

   Java 클래스 이름

   기존 플러그인에 대한 Java 클래스 이름을 지정합니다.

   플러그인 클래스는 어설션을 구문 분석하고 수정한 다음 최종 처리를 위해 결과를 어설션 생성기에게 반환할 수 있습니다.

   플러그인은 각 가맹에 대해 하나씩만 허용됩니다. 예를 들면 com.mycompany.assertiongenerator.AssertionSample 입니다.

   매개 변수

   (선택 사항) "Java 클래스 이름" 필드에서 지정한 플러그인에 전달되는 매개 변수 문자열을 지정합니다.

   참고: 관리 UI 에서 어설션 플러그인이 사용되도록 설정하는 대신 정책 관리 API(C 또는 Perl)를 사용하여 플러그인을 통합할 수 있습니다. 자세한 내용은 *SiteMinder Programming Guide for C*(SiteMinder C 프로그래밍 안내서) 또는 *SiteMinder Programming Guide for Java*(SiteMinder Java 프로그래밍 안내서)를 참조하십시오.

6. 정책 서버를 다시 시작합니다.

   정책 서버를 다시 시작하면 최신 버전의 어설션 플러그인이 다시 컴파일된 후 선택됩니다.

소비자 리소스에 대한 링크 만들기(SAML 1.x)

생산자에서 사용자를 소비자 사이트에 연결하는 링크가 포함된 페이지를 생성하십시오. 각 링크는 사이트 간 전송 URL 을 나타냅니다. 사용자가 사이트 간 전송 URL 을 방문하여 생산자 측 웹 에이전트에 대한 요청을 만들어야 합니다. 그러면 사용자가 소비자 사이트로 리디렉션됩니다.

SAML 아티팩트 프로필의 경우 사이트 간 전송 URL 구문은 다음과 같습니다.

http://*producer_site*/affwebservices/public/intersitetransfer?SMASSERTIONREF=QUERY&NAME=*affiliate_name*&TARGET=http://*consumer_site*/*target_url*?*query_parameter_name*%3D*query_parameter_value*%26*query_parameter_name*%3D*query_parameter_value*&SMCONSUMERURL=http://*consumer_site*/affwebservices/public/samlcc&AUTHREQUIREMENT=2

SAML POST 프로필의 경우 사이트 간 전송 URL 구문은 다음과 같습니다.

http://*producer_site*/affwebservices/public/intersitetransfer?SMASSERTIONREF=QUERY&NAME=*affiliate_name*&TARGET=http://*consumer_site*/*target_url*

사이트 간 전송 URL 의 변수는 다음과 같습니다.

producer_site

사용자가 인증되는 웹 사이트를 지정합니다.

affiliate_name

가맹 도메인에 구성된 가맹의 이름을 나타냅니다.

consumer_site

사용자가 생산자 사이트에서 방문하려는 사이트를 나타냅니다.

target_url

소비자 사이트의 대상 페이지입니다.

사용자가 선택하는 사이트 간 전송 URL 에는 다음 표에 나열된 쿼리 매개 변수가 포함되어 있어야 합니다.

참고: SAML 아티팩트 프로필에 대한 쿼리 매개 변수에서는 HTTP-인코딩을 사용해야 합니다.

쿼리 매개 변수	의미
SMASSERTIONREF(필수)	내부용입니다. 값은 항상 QUERY 입니다. 이 값을 변경하지 마십시오.
NAME (필수)	가맹 도메인에 구성된 가맹의 이름입니다.
TARGET (필수)	소비자 사이트의 대상 URL 입니다.
SMCONSUMERURL(아티팩트 프로필의 경우에만 필수)	소비자 사이트의 URL 은 어설션을 처리하고 사용자를 인증합니다. SAML 1.x 아티팩트 바인딩의 경우 어설션 소비자 URL 에 대해 지정된 값이 이 쿼리 매개 변수의 값보다 우선합니다.
AUTHREQUIREMENT=2(아티팩트 프로필의 경우에만 필수)	내부용입니다. 값은 항상 2 입니다. 이 값을 변경하지 마십시오.

참고: SAML POST 프로필에서는 SMCONSUMERURL 및 AUTHREQUIREMENT 매개 변수를 사용하지 않습니다. 하지만 사이트 간 전송 URL 에 이러한 매개 변수 중 하나를 포함하는 경우에는 다른 매개 변수도 포함해야 합니다.

예: 아티팩트 프로필에 대한 사이트 간 전송 URL

http://www.smartway.com/affwebservices/public/intersitetransfer?SMASSERTIONREF=QUERY&NAME=ahealthco&TARGET=http://www.ahealthco.com:85/smartway/index.jsp&SMCONSUMERURL=http://www.ahealthco.com:85/affwebservices/public/samlcc&AUTHREQUIREMENT=2

예: POST 프로필에 대한 사이트 간 전송 URL

http://www.smartway.com/affwebservices/public/intersitetransfer?SMASSERTIONREF
=QUERY&NAME=ahealthco&TARGET=http://www.ahealthco.com/index.html

사이트 간 전송 URL 보호 여부 선택

사이트 간 전송 URL 과 연결된 웹 페이지는 영구 세션에 대해 구성된 SiteMinder 로 보호된 영역에 포함될 수 있습니다. 사용자가 보호된 페이지의 링크 중 하나를 선택하면 SiteMinder 가 사용자에게 인증 챌린지를 표시합니다. 사용자가 로그인한 후 SAML 어설션을 저장하는 데 필요한 영구 세션을 설정할 수 있습니다.

이러한 페이지가 보호되지 않은 경우 생산자는 SiteMinder 세션이 없는 가맹 사용자를 인증 URL 에 연결합니다. 이 URL 은 사용자에게 SiteMinder 세션을 받으려면 로그인하라는 메시지를 표시합니다. 관리 UI 에서 가맹을 구성할 때 인증 URL 을 정의하십시오.

참고: 영구 세션을 설정하려면 세션 저장소를 구성하십시오. 정책 서버 관리 콘솔을 사용하여 세션 저장소를 설정하십시오.

제 13 장: SAML 1.x 소비자로 구성

신뢰 파트너에 대한 사전 요구 사항

SiteMinder 를 신뢰 파트너로 사용하려면 다음 태스크를 완료하십시오.

- 정책 서버를 설치합니다.
- 다음 구성 요소 중 하나를 설치합니다.
  - 웹 에이전트 및 웹 에이전트 옵션 팩. 웹 에이전트는 사용자를 인증하고 세션을 설정합니다. 옵션 팩은 페더레이션 웹 서비스 응용 프로그램을 제공합니다. 적절한 네트워크 시스템에 FWS 응용 프로그램을 배포해야 합니다.
  - 포함된 웹 에이전트가 있고 포함된 Tomcat 웹 서버에 페더레이션 웹 서비스 응용 프로그램이 있는 SPS 페더레이션 게이트웨이

  자세한 내용은 *웹 에이전트 옵션 팩 안내서*를 참조하십시오.
- 메시지 서명 및 암호화를 필요로 하는 기능을 위해 개인 키와 인증서를 가져옵니다.
- 어설션 파트너는 페더레이션된 네트워크 내에서 설정됩니다.

SAML 1.x 소비자를 구성하는 방법

SiteMinder 를 SAML 1.x 소비자로 구성하려면 다음 태스크를 수행해야 합니다.

1. SAML 1.x 인증 체계 필수 구성 요소를 완료합니다.
2. 인증 체계 유형을 선택하고 해당 이름을 할당합니다.
3. SAML 1.x 인증 체계로 인증되고 있는 사용자에 대한 네임스페이스를 지정합니다.

4. 이 소비자가 지원하는 싱글 사인온 프로필(아티팩트 또는 POST)을 선택합니다.
5. 페더레이션 파트너이면서 어설션을 생성하는 파트너 각각에 대해 SAML 인증 체계를 구성합니다. 각 체계를 영역에 바인드합니다. 영역에는 페더레이션된 리소스에 대한 대상 URL 이 포함되어 있어야 합니다. SiteMinder 정책으로 이러한 리소스를 보호합니다.

팁:

- 생산자와 소비자의 특정 매개 변수 값이 일치해야 구성이 올바로 작동합니다. 이러한 매개 변수 목록은 동일한 값을 사용해야 하는 구성 설정 (페이지 411)에서 제공됩니다.
- 페더레이션 웹 서비스 서블릿에 대해 올바른 URL 을 사용하고 있는지 확인하십시오. URL 은 SiteMinder 구성에 사용되는 페더레이션 웹 서비스 URL (페이지 417)에 나열되어 있습니다.

소비자에 대한 선택적 구성 태스크

소비자를 구성하기 위한 선택적 태스크는 다음과 같습니다.

- 메시지 소비자 플러그인을 사용하여 어설션을 사용자 지정합니다.
- 실패한 인증 시도를 리디렉션합니다.

레거시 페더레이션 대화 상자 탐색

관리 UI 에서는 레거시 페더레이션 구성 대화 상자로 이동하는 방법 두 가지를 제공합니다.

다음 두 방법 중 하나로 탐색할 수 있습니다.

- 마법사를 따라 새 레거시 페더레이션 개체 구성

  개체를 생성하는 경우 페이지가 표시되면서 구성 마법사가 나타납니다. 구성 마법사의 단계를 따라 개체를 생성하십시오.

- 탭을 선택하여 기존 레거시 페더레이션 개체 수정

  기존 개체를 수정하는 경우 페이지가 표시되면서 일련의 탭이 나타납니다. 이러한 탭에서 구성을 수정하십시오. 이러한 탭은 구성 마법사의 단계와 동일합니다.

SAML 1.x 인증 체계

소비자는 SAML 1.x 어설션을 사용하여 사용자를 인증하는 사이트입니다.

참고: 사이트는 SAML 생산자와 SAML 소비자일 수 있습니다.

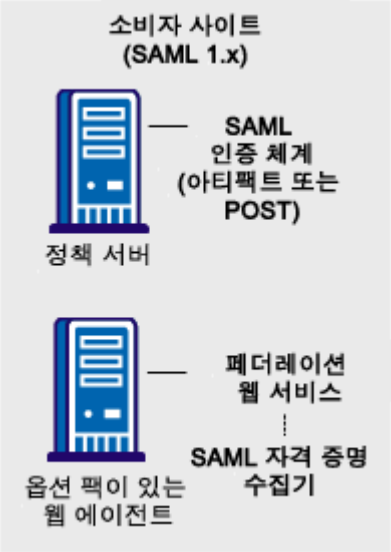
레거시 페더레이션 기능이 있는 모든 SiteMinder 사이트에서는 SAML 1.x 어설션을 소비할 수 있고 이러한 어설션을 사용하여 사용자를 인증할 수 있습니다. 어설션이 소비되는 경우 사이트에서 어설션의 정보를 사용자 디렉터리와 비교할 수 있어야 인증 프로세스가 완료됩니다.

SiteMinder 는 다음 SAML 1.x 인증 방법을 제공합니다.

- SAML 아티팩트 프로필
- SAML POST 프로필

SAML 기반 인증 체계를 통해 소비자 사이트에서 사용자를 인증할 수 있습니다. SAML 어설션을 소비하고 SiteMinder 세션을 설정하면 도메인 간 싱글 사인온이 사용되도록 설정됩니다. 사용자가 식별된 후 소비자 사이트에서 사용자에게 특정 리소스에 대한 권한을 부여할 수 있습니다.

다음 그림에서는 소비자 사이트의 주요 인증 구성 요소를 보여 줍니다.



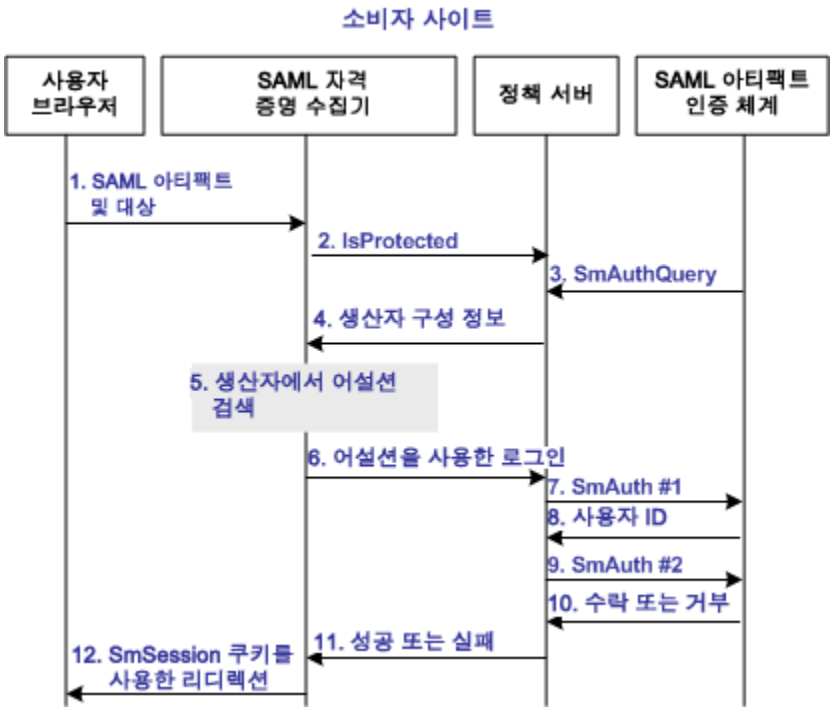
참고: SPS 페더레이션 게이트웨이가 페더레이션 웹 서비스 응용 프로그램 기능을 제공하기 위해 웹 에이전트 및 웹 에이전트 옵션 팩을 대체할 수 있습니다. SPS 페더레이션 게이트웨이 설치 및 구성에 대한 자세한 내용은 *Secure Proxy Server Administration Guide*(보안 프록시 서버 관리 안내서)를 참조하십시오.

SAML 1.x 인증 체계는 소비자 측 정책 서버에서 구성됩니다. SAML 자격 증명 수집기는 페더레이션 웹 서비스 응용 프로그램의 구성 요소입니다. 자격 증명 수집기는 소비자 측 웹 에이전트나 SPS 페더레이션 게이트웨이에 설치됩니다. 자격 증명 수집기는 정책 서버의 SAML 인증 체계에서 정보를 얻은 다음 해당 정보를 사용하여 SAML 어설션에 액세스합니다.

SAML 어설션은 소비자 사이트의 정책 서버에 대한 액세스 권한을 부여하는 자격 증명이 됩니다. 사용자가 인증되어 권한이 부여되고, 권한 부여가 성공한 경우 대상 리소스로 리디렉션됩니다.

SAML 1.x 아티팩트 인증 체계 개요

다음 그림에서는 SAML 1.x 아티팩트 인증 체계가 요청을 처리하는 방법을 보여 줍니다.



참고: SPS 페더레이션 게이트웨이나 웹 에이전트 및 웹 에이전트 옵션 팩이 에이전트 및 SAML 자격 증명 수집기 기능을 제공합니다.

달리 지정하지 않은 경우 이 프로세스의 모든 작업은 소비자 사이트에서 발생합니다.

1. 사용자가 SAML 아티팩트 및 대상 URL 을 사용하여 SAML 자격 증명 수집기로 리디렉션됩니다.

   아티팩트 및 대상 URL 은 원래 생산자 사이트의 웹 에이전트에서 생성됩니다.

2. SAML 자격 증명 수집기가 정책 서버를 호출하여 SAML 아티팩트 인증 체계가 요청된 리소스를 보호하는지 여부를 확인합니다.

3. 정책 서버가 필요한 데이터를 SAML 아티팩트 인증 체계에 전달하면 SAML 아티팩트 인증 체계가 생산자 구성 정보를 추출합니다.

4. 정책 서버가 생산자 구성 정보를 SAML 자격 증명 수집기에 반환합니다. 이 정보를 사용하여 자격 증명 수집기 서블릿이 생산자 사이트를 호출하고 SAML 어설션을 검색할 수 있습니다.

5. SAML 자격 증명 수집기가 정책 서버에서 데이터를 가져와 SAML 어설션을 검색하는 데 사용합니다.

6. 어설션이 반환된 후 자격 증명 수집기가 어설션을 자격 증명으로 사용하고 정책 서버에 로그인합니다.

7. 정책 서버가 SAML 인증 체계에 대한 초기 사용자 명확성 호출을 합니다.

8. 인증 체계 데이터와 어설션을 사용하여 인증 체계가 사용자를 찾고 해당 사용자의 고유 식별자를 자격 증명 수집기에 반환합니다.

9. 정책 서버가 인증 체계에 대한 두 번째 사용자 인증 호출을 합니다.

   참고: SiteMinder 인증 AP 는 2 단계로 구성된 인증 프로세스를 지정합니다. 자세한 내용은 *SiteMinder Programming Guide for C*(SiteMinder C 프로그래밍 안내서) 또는 *SiteMinder Programming Guide for Java*(SiteMinder Java 프로그래밍 안내서)를 참조하십시오.

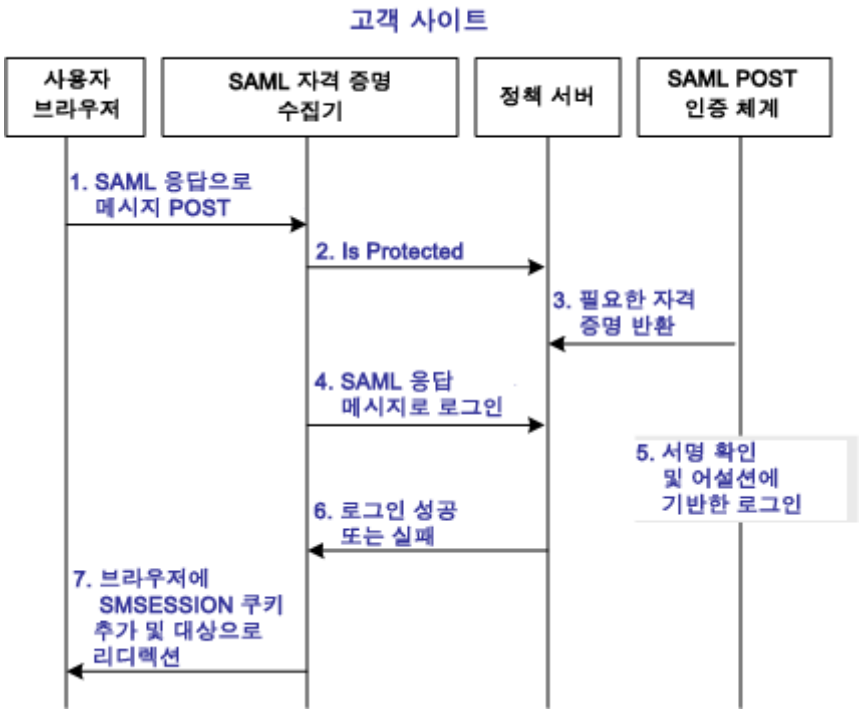
10. 인증 체계가 SAML 어설션의 유효성을 검사하고 수락 또는 거부 메시지를 정책 서버에 반환합니다.

11. 정책 서버가 수락 또는 거부 메시지를 자격 증명 수집기에 보냅니다.

12. SAML 자격 증명 수집기가 세션 쿠키를 생성하여 브라우저에 배치하고 사용자를 대상 리소스로 리디렉션합니다. 로그인이 실패하면 자격 증명 수집기가 사용자를 액세스 권한 없음 URL 로 리디렉션합니다.

SAML 1.x POST 프로필 인증 체계 개요

다음 그림에서는 SAML 1.x POST 프로필 인증 체계가 요청을 처리하는 방법을 보여 줍니다.



참고: SPS 페더레이션 게이트웨이나 웹 에이전트 옵션 팩은 SAML 자격 증명 수집기 기능을 제공합니다.

달리 지정하지 않은 경우 다음 프로세스가 소비자 사이트에서 수행됩니다.

1. 브라우저가 SAML 자격 증명 수집기 URL 에 HTML 양식을 포스트합니다. 이 양식에는 SAML 응답 메시지와 원래 생산자에서 생성된 대상 URL 의 주소가 포함되어 있습니다.
2. SAML 자격 증명 수집기가 정책 서버에 연결하여 대상 리소스 보호 여부를 확인합니다.
3. 정책 서버가 SAML POST 프로필 인증 체계로 대상 URL 을 보호한다고 회신합니다. 포스트된 양식에서 서명된 응답이 로그인 호출에 대해 예상된 자격 증명입니다.
4. SAML 자격 증명 수집기가 디지털로 서명된 SAML 응답을 자격 증명으로 전달하면서 정책 서버에 대한 로그인 호출을 수행합니다.

5. SAML POST 프로필 인증 체계가 서명과 응답 및 어설션의 기타 필드를 확인합니다.
6. 검사가 성공하고 사용자가 디렉터리에서 발견되면 인증이 성공합니다. 검사가 하나라도 실패하면 인증이 실패합니다.
7. SAML 자격 증명 수집기가 SMSESSION 쿠키를 생성합니다. 이 쿠키가 브라우저에 배치되고 사용자가 대상 리소스로 리디렉션됩니다. 로그인이 실패하면 자격 증명 수집기가 사용자를 구성된 액세스 권한 없음 URL 로 리디렉션합니다.

SAML 1.x 인증 체계 사전 요구 사항

SAML 인증 체계 구성에 대한 사전 요구 사항은 다음과 같습니다.

- 생산자와 소비자에서 SiteMinder 정책 서버를 설치합니다.
- 생산자와 소비자에서 페더레이션 웹 서비스를 설치합니다.
- SAML POST 응답에 서명하기 위한 인증서 데이터 저장소를 준비합니다.

SiteMinder 정책 서버 설치

SiteMinder 정책 서버에는 레거시 페더레이션 기능이 포함되어 있습니다.

정책 서버를 설치하려면 *정책 서버 설치 안내서*를 참조하십시오.

생산자와 소비자에 페더레이션 웹 서비스 설치

FWS(페더레이션 웹 서비스)는 웹 응용 프로그램입니다. FWS 는 어설션과 기타 페더레이션된 네트워크 구성 서비스를 소비하는 SAML 자격 증명 수집기 서블릿을 제공합니다.

FWS 응용 프로그램 기능을 사용하려면 웹 에이전트 및 웹 에이전트 옵션 팩을 설치하거나 생산자와 소비자 사이트에 FWS 가 포함되어 있는 SPS 페더레이션 게이트웨이를 설치하십시오.

설치 및 구성 지침은 다음 안내서를 참조하십시오.

- *웹 에이전트 옵션 팩 안내서*
- *보안 프록시 서버 관리 안내서*

DefaultAgentName 설정에 대한 값 지정

웹 에이전트를 설치하는 경우 모든 소비자 웹 에이전트에 대해 웹 에이전트 매개 변수 DefaultAgentName 의 값을 정의하십시오. 이 값은 웹 에이전트 아이덴티티를 지정합니다.

DefaultAgentName 을 식별하는 지정된 에이전트를 대상 리소스를 보호하는 영역의 리소스 필터에 포함하십시오. 에이전트 구성 개체 또는 로컬 에이전트 구성 파일에서 DefaultAgentName 매개 변수를 구성하십시오. DefaultAgentName 매개 변수를 생략하거나 영역 리소스 필터의 AgentName 매개 변수에 지정된 값을 사용하면 싱글 사인온 프로필과 관계없이 SAML 1.x 인증이 실패합니다.

POST 응답에 서명하고 확인하도록 인증서 데이터 저장소 설정

SAML POST 프로필을 사용하여 어설션을 전달하려면 생산자가 어설션이 포함된 SAML 응답에 서명해야 합니다. 소비자 사이트의 어설션 소비자가 해당 서명을 확인해야 합니다.

이러한 태스크를 수행하려면 서명, 확인 또는 둘 다에 사용할 개인 키/인증서 쌍을 인증서 데이터 저장소에 추가하십시오. 인증서 데이터 저장소를 사용하면 SAML 응답에 서명하고 유효성을 검사하는 데 필요한 키와 인증서를 관리 및 검색할 수 있습니다.

인증서 데이터 저장소에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

SAML 1.x 아티팩트 인증 구성

SAML 아티팩트 인증 체계를 영역에 할당하려면 먼저 체계를 구성하십시오.

다음 단계를 수행하십시오.

1. "인프라", "인증", "인증 체계"로 이동합니다.
2. "인증 체계 만들기"를 클릭합니다.

3. "Create a new object of type Authentication Scheme"(인증 체계 유형의 새 개체 만들기)를 선택합니다.

   "인증 체계" 페이지가 열립니다.

4. 인증 체계의 이름을 입력합니다.
5. "인증 체계 유형" 드롭다운 목록에서 "SAML 아티팩트 템플릿"을 선택합니다.

   SAML 아티팩트 체계를 지원하도록 "인증 체계" 대화 상자의 내용이 변경됩니다.

6. 체계 설정을 구성합니다.

   설정에 대한 설명을 보려면 "도움말"을 클릭하십시오.

   중요! "가맹 이름", "암호" 및 "암호 확인" 필드가 페더레이션 네트워크의 다른 값과 일치해야 합니다. 자세한 내용은 동일한 값을 사용해야 하는 구성 설정 (페이지 411)을 참조하십시오.

7. (선택 사항) "기본 대상 URL" 필드에서 대상 리소스를 지정합니다. 이 필드는 페이지의 "추가 구성" 섹션에 있습니다. 대상은 소비자에서 보호된 페더레이션된 리소스입니다.

   소비자가 기본 대상을 사용하지 않아도 됩니다. 싱글 사인온을 시작하는 링크에는 대상을 지정하는 쿼리 매개 변수가 포함됩니다.

   또는 인증 응답 URL 에 있는 TARGET 쿼리 매개 변수의 값을 사용하여 대상 리소스를 지정합니다. 이 옵션이 사용되도록 설정하려면 "쿼리 매개 변수 TARGET 은 기본 대상 URL 에 우선합니다." 확인란을 선택합니다.

8. (선택 사항) "추가 구성" 섹션에서 메시지 소비자 API, 인증 오류에 대한 리디렉션 URL 등의 기능을 구성합니다.
9. "확인"을 클릭하여 체계를 저장합니다.

이제 SAML 1.x 아티팩트 인증 체계가 구성되었습니다.

추가 정보:

HTTP-아티팩트 SSO 에 대한 백 채널 구성 (페이지 174)

HTTP-아티팩트 SSO 에 대한 백 채널 구성

SAML 아티팩트 프로필의 경우 어설션 당사자가 백 채널을 통해 어설션을 소비자에게 보냅니다. 인증 체계로 백 채널을 보호하십시오. 기본 또는 클라이언트 인증서 인증 체계를 사용하여 백 채널을 보호할 수 있습니다.

- 기본 인증

  기본 인증을 사용하는 경우 SiteMinder 가 두 파트너 모두에 있으면 각 사이트의 가맹 이름이 소비자의 이름입니다. 어설션 당사자가 SiteMinder 가 아닌 경우 어설션 당사자의 관리자는 사이트를 식별하는 데 사용하고 있는 이름을 제공해야 합니다. 인증 체계 구성에서 제공된 이름을 가맹 이름으로 지정하십시오.

- 클라이언트 인증서 인증

  클라이언트 인증서 인증을 백 채널에 사용하는 경우 관리 UI 에 있는 가맹 이름은 클라이언트 인증서의 별칭이어야 합니다. 또한 인증서 주체의 CN 도 가맹 이름과 일치해야 합니다. 가맹 이름, 별칭 및 CN 이 일치해야 합니다.

정책 서버는 비 FIPS 140 으로 암호화된 인증서를 사용하는 백 채널을 통해 클라이언트 인증서 인증을 지원하는데, 이는 정책 서버가 FIPS 전용 모드로 작동하고 있는 경우에도 마찬가지입니다. 하지만 엄격한 FIPS 전용 설치의 경우 FIPS 140 호환 알고리즘으로 암호화된 인증서만 사용하십시오.

클라이언트 인증서는 인증서 데이터 저장소에 저장됩니다.

SAML 1.x POST 프로필 인증 구성

SAML POST 프로필 인증 체계를 구성하려면

1. "인프라", "인증", "인증 체계"로 이동합니다.
2. "인증 체계 만들기"를 클릭합니다.
3. "Create a new object of type Authentication Scheme"(인증 체계 유형의 새 개체 만들기)를 선택합니다.

   "인증 체계" 페이지가 열립니다.
4. 인증 체계의 이름을 입력합니다.

5. "인증 체계 유형" 드롭다운 목록에서 "SAML POST 템플릿"을 선택합니다.

   SAML POST 체계를 지원하도록 "인증 체계" 대화 상자의 내용이 변경됩니다.

6. 체계 설정을 구성합니다.

   필드 설명을 보려면 "도움말"을 클릭하십시오.

   중요! "가맹 이름", "암호" 및 "암호 확인" 필드가 페더레이션 네트워크의 다른 값과 일치해야 합니다. 자세한 내용은 동일한 값을 사용해야 하는 구성 설정 (페이지 411)을 참조하십시오.

7. (선택 사항) "기본 대상 URL" 필드에서 대상 리소스를 지정합니다. 이 필드는 페이지의 "추가 구성" 섹션에 있습니다. 대상은 소비자에서 보호된 페더레이션된 리소스입니다.

   소비자가 기본 대상을 사용하지 않아도 됩니다. 싱글 사인온을 시작하는 링크에는 대상을 지정하는 쿼리 매개 변수가 포함됩니다.

   또는 인증 응답 URL 에 있는 TARGET 쿼리 매개 변수의 값을 사용하여 대상 리소스를 지정합니다. 이 옵션이 사용되도록 설정하려면 "쿼리 매개 변수 TARGET 은 기본 대상 URL 에 우선합니다." 확인란을 선택합니다.

8. (선택 사항) "추가 구성" 섹션에서 메시지 소비자 API, 인증 오류에 대한 리디렉션 URL 등의 기능을 구성합니다.

9. "확인"을 클릭하여 체계를 저장합니다.

이제 SAML 1.x POST 인증 체계가 구성되었습니다.

메시지 소비자 플러그인으로 어설션 처리 사용자 지정

메시지 소비자 플러그인은 메시지 소비자 플러그인을 구현하는 Java 프로그램입니다. 이 플러그인을 통해 어설션 거부, 상태 코드 반환 등의 어설션 처리를 위한 사용자 고유의 비즈니스 논리를 구현할 수 있습니다. 이 추가 처리는 어설션의 표준 처리와 함께 작동합니다.

참고: 인증 및 명확성의 상태 코드에 대한 자세한 내용은 *SiteMinder Programming Guide for Java*(SiteMinder Java 프로그래밍 안내서)를 참조하십시오.

인증 중에 SiteMinder 는 먼저 사용자를 해당 로컬 사용자 저장소에 매핑하여 어설션을 처리하려고 합니다. 사용자를 찾을 수 없는 경우 SiteMinder 는 메시지 소비자 플러그인의 postDisambiguateUser 메서드를 호출합니다.

플러그인이 사용자를 찾은 경우 SiteMinder 는 인증의 두 번째 단계로 진행합니다. 플러그인이 사용자를 로컬 사용자 저장소에 매핑할 수 없는 경우에는 UserNotFound 오류가 반환됩니다. 플러그인이 선택적으로 리디렉션 URL 기능을 사용할 수 있습니다. 소비자 플러그인이 없는 경우 리디렉션 URL 은 SAML 인증 체계가 생성하는 오류를 기반으로 합니다.

두 번째 인증 단계에서 SiteMinder 는 플러그인이 구성된 경우 메시지 소비자 플러그인의 postAuthenticateUser 메서드를 호출합니다. 메서드가 성공하는 경우 SiteMinder 는 사용자를 요청된 리소스로 리디렉션합니다. 메서드가 실패하는 경우 사용자를 실패 페이지에 보내도록 플러그인을 구성할 수 있습니다. 실패 페이지는 인증 체계 구성으로 지정할 수 있는 리디렉션 URL 중 하나일 수 있습니다.

메시지 소비자 플러그인에 대한 자세한 내용은 다음과 같이 찾을 수 있습니다.

- 참조 정보(메서드 서명, 매개 변수, 반환 값, 데이터 형식)와 UserContext 클래스에 대한 생성자는 *Java Developer Reference*(Java 개발자 참조서)에 나와 있습니다. MessageConsumerPlugin 인터페이스를 참조하십시오.
- 인증 및 권한 부여 API 에 대한 개요와 개념 정보는 *SiteMinder Programming Guide for Java*(SiteMinder Java 프로그래밍 안내서)를 참조하십시오.

플러그인을 구성하려면

1. 아직 설치하지 않은 경우 SiteMinder SDK 를 설치합니다.
2. SiteMinder SDK 의 일부인 MessageconsumerPlugin.java 인터페이스를 구현합니다.
3. 메시지 소비자 플러그인 구현 클래스를 배포합니다.
4. 관리 UI 에서 메시지 소비자 플러그인이 사용되도록 설정합니다.

MessageConsumerPlugin 인터페이스 구현

MessageConsumerPlugin.java 인터페이스를 구현하여 사용자 지정 메시지 소비자 플러그인을 생성하십시오. 다음 절차에는 구현 클래스에 대한 최소 요구 사항이 나열되어 있습니다.

다음 단계를 수행하십시오.

1. 매개 변수가 포함되지 않은 공개 기본 생성자 메서드를 제공합니다.
2. 상태 비저장 구현이 되도록 코드를 제공합니다. 여러 스레드가 단일 플러그인 클래스를 사용할 수 있어야 합니다.
3. 인터페이스에서 요구 사항을 충족할 메서드를 구현합니다.

   MessageConsumerPlugin 에는 다음 네 가지 메서드가 포함됩니다.

   init()

   플러그인에 필요한 초기화 절차를 모두 수행합니다. SiteMinder 는 플러그인이 로드될 때 각 플러그인 인스턴스에 대해 한 번씩 이 메서드를 호출합니다.

   release()

   플러그인에 필요한 런다운 절차를 모두 수행합니다. SiteMinder 는 SiteMinder 가 종료될 때 각 플러그인 인스턴스에 대해 한 번씩 이 메서드를 호출합니다.

   postDisambiguateUser()

   인증 체계가 사용자 명확성 처리를 수행할 수 없을 때 해당 처리를 제공합니다. 또는 이 메서드가 새 페더레이션 사용자에 대한 데이터를 사용자 저장소에 추가할 수 있습니다. 이 메서드는 암호 해독된 어설션을 수신합니다. 암호 해독된 어설션은 플러그인에 전달된 속성 맵의 "_DecryptedAssertion" 키 아래에 추가됩니다.

   postAuthenticateUser()

   정책 서버 처리 성공 여부와 관계없이 최종 어설션 처리 결과를 확인하기 위한 추가 코드를 제공합니다.

SiteMinder 는 다음과 같은 메시지 소비자 플러그인 클래스 샘플을 제공합니다.

installation_home\sdk\samples\messageconsumerplugin 의 MessageConsumerPluginSample.java

installation_home\sdk\samples\authextensionsaml20 의 MessageConsumerSAML20.java

메시지 소비자 플러그인 배포

MessageConsumerPlugin 인터페이스에 대한 구현 클래스를 코드화했으면 해당 구현 클래스를 컴파일하고 SiteMinder 가 실행 파일을 찾을 수 있는지 확인하십시오.

메시지 소비자 플러그인을 배포하려면

1. MessageConsumerPlugin Java 파일을 컴파일합니다. 이 파일을 컴파일하려면 정책 서버와 함께 설치되는 다음 종속 라이브러리가 필요합니다.

   installation_home\siteminder\bin\jars\SmJavaApi.jar

   SmJavaApi.jar 의 동일한 복사본이 SiteMinder SDK 와 함께 설치됩니다. 이 파일은 *installation_home*\sdk\java\SmJavaApi.jar 디렉터리에 있습니다.

   개발 시 두 파일 중 아무 파일이나 사용할 수 있습니다.

2. 폴더나 jar 파일에서 플러그인 클래스를 사용할 수 있는 경우 JVMOptions.txt 파일에서 -Djava.class.path 값을 수정합니다. 이 단계를 수행하면 수정된 클래스 경로를 사용하여 플러그인 클래스를 로드할 수 있습니다. *installation_home*\siteminder\config 디렉터리에서 JVMOptions.txt 파일을 찾습니다.

   참고: 기존 xerces.jar, xalan.jar 또는 SmJavaApi.jar 의 클래스 경로를 수정하지 마십시오.

3. 정책 서버를 다시 시작하여 최신 버전의 MessageConsumerPlugin 을 선택합니다. 이 단계는 플러그인 Java 파일이 다시 컴파일될 때마다 필요합니다.

4. 플러그인이 사용되도록 설정합니다.

SAML 1.x 에 대해 메시지 소비자 플러그인이 사용되도록 설정

메시지 소비자 플러그인을 작성하고 컴파일한 후 관리 UI 에서 설정을 구성하여 플러그인이 사용되도록 설정하십시오. UI 설정은 SiteMinder 에게 플러그인을 찾을 수 있는 위치를 알려 줍니다.

플러그인을 배포 (페이지 178)할 때까지 플러그인 설정을 구성하지 마십시오.

메시지 소비자 플러그인이 사용되도록 설정하려면

1. 관리 UI 에 로그온합니다.

2. 적절한 SAML 1.x 체계에 대한 "인증 체계" 대화 상자로 이동합니다. "추가 구성" 섹션의 다음 필드에 데이터를 입력합니다.

   전체 Java 클래스 이름

   플러그인에 대한 Java 클래스 이름을 지정합니다. 예를 들어 SiteMinder SDK 에 포함된 샘플 클래스는 다음과 같습니다.

   com.ca.messageconsumerplugin.MessageConsumerPluginSample

   매개 변수

   "전체 Java 클래스 이름" 필드에서 지정한 플러그인에 전달되는 매개 변수 문자열을 지정합니다.

   관리 UI 에서 플러그인을 구성하는 대신 정책 관리 API(C 또는 Perl)를 사용하여 IdpPluginClass 와 IdpPluginParameters 를 설정할 수 있습니다.

3. 정책 서버를 다시 시작합니다.

실패한 SAML 1.x 인증 시도 후 사용자 리디렉션

싱글 사인온 트랜잭션 중에 소비자가 사용자를 인증할 수 없는 경우 소비자는 추가 처리를 위해 해당 사용자를 사용자 지정된 URL 로 리디렉션할 수 있습니다.

실패한 인증에 대해 여러 선택적 리디렉션 URL 을 구성할 수 있습니다. 이러한 리디렉션 URL 을 통해 사용자가 리디렉션되는 위치를 세부적으로 제어할 수 있습니다. 예를 들어 사용자 저장소에서 사용자를 찾을 수 없는 경우 사용자를 찾을 수 없음 리디렉션 URL 을 입력할 수 있습니다.

"상태 리디렉션 URL 및 모드"는 인증 대화 상자의 "추가 구성" 섹션에 있습니다. 리디렉션 URL 은 다음과 같은 특정 상태 조건에 적용됩니다.

- 사용자를 찾을 수 없습니다.
- 싱글 사인온 메시지가 잘못되었습니다.
- 사용자 자격 증명이 수락되지 않았습니다.

이러한 조건이 하나라도 발생하는 경우 리디렉션 URL 은 추가 작업을 위해 사용자를 응용 프로그램이나 사용자 지정된 오류 페이지로 보낼 수 있습니다.

참고: 리디렉션 URL 구성은 필수 사항이 아닙니다.

리디렉션 URL 을 구성하지 않으면 표준 SiteMinder 처리가 수행됩니다. 실패한 인증을 처리하는 방법은 인증 체계 구성에 따라 달라집니다.

상태 리디렉션 URL 을 구성하려면

1. SAML 아티팩트 또는 SAML POST 인증 체계에 대한 페이지로 이동합니다.
2. "상태 리디렉션 URL 및 모드" 섹션의 필드 중 하나 이상에 대한 URL 을 입력합니다.

   설정에 대한 설명을 보려면 "도움말"을 클릭하십시오.

   페더레이션 웹 서비스는 인증 사유를 구성된 리디렉션 URL 중 하나에 매핑하여 오류를 처리합니다. 오류를 보고하기 위해 사용자가 해당 URL 로 리디렉션될 수 있습니다.
3. 다음 모드 중 하나를 선택합니다.
   - 302 데이터 없음
   - HTTP POST
4. "확인"을 클릭하여 변경 내용을 저장합니다.

참고: 이러한 리디렉션 URL 은 추가 어설션 처리를 위해 SiteMinder 메시지 소비자 플러그인과 함께 사용될 수 있습니다. 인증이 실패하면 플러그인이 사용자를 지정한 리디렉션 URL 중 하나에 보낼 수 있습니다.

추가 정보:

SAML 1.x 아티팩트 인증 구성 (페이지 172)
SAML 1.x POST 프로필 인증 구성 (페이지 174)

SAML 특성을 HTTP 헤더로 제공

어설션 응답이 특성을 어설션에 포함할 수 있습니다. 이러한 특성을 HTTP 헤더 변수로 제공하면 클라이언트 응용 프로그램에서 해당 특성을 사용하여 세부적인 액세스 제어를 구현할 수 있습니다.

특성을 HTTP 헤더에 포함하여 얻을 수 있는 이점은 다음과 같습니다.

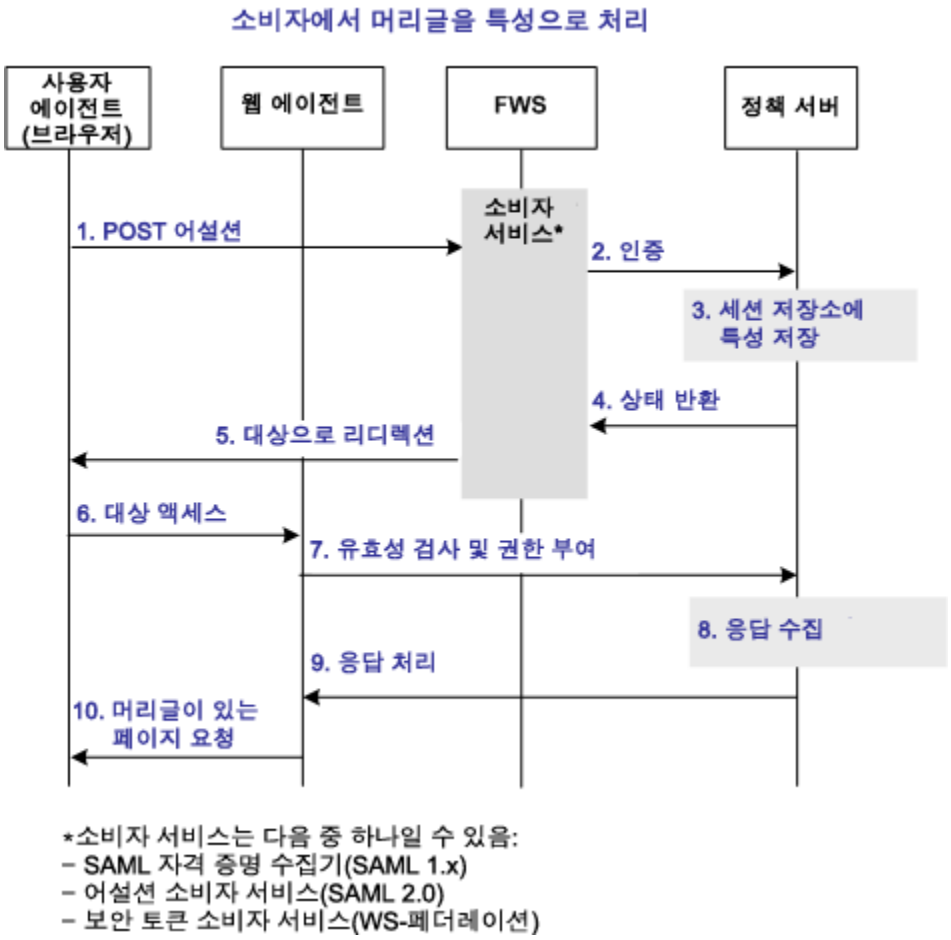
- HTTP 헤더가 영구적이지 않습니다. 즉, HTTP 헤더가 포함된 요청이나 응답 내에서만 표시됩니다.
- SiteMinder 웹 에이전트가 제공한 HTTP 헤더가 브라우저에 표시되지 않으므로 보안 문제가 줄어듭니다.

참고: HTTP 헤더에는 특성이 초과할 수 없는 크기 제한이 있습니다. SiteMinder 는 헤더에 대한 웹 서버 크기 제한까지 헤더에 있는 특성을 보낼 수 있습니다. 헤더당 허용되는 어설션 특성은 하나뿐입니다. 헤더 크기 제한을 확인하려면 해당 웹 서버 설명서를 참조하십시오.

SAML 특성을 HTTP 헤더로 처리하기 위한 사용 사례

인증 중에 일련의 SAML 특성이 어설션에서 추출되어 HTTP 헤더로 제공됩니다. 권한 부여 프로세스 중에 이러한 헤더가 고객 응용 프로그램에 반환됩니다.

다음 순서도에서는 런타임 시 이벤트 순서를 보여 줍니다.



참고: SPS 페더레이션 게이트웨이가 페더레이션 웹 서비스 응용 프로그램 기능을 제공하기 위해 웹 에이전트 및 웹 에이전트 옵션 팩을 대체할 수 있습니다. 흐름도에서 웹 에이전트 블록은 SPS 페더레이션 게이트웨이에 포함된 웹 에이전트입니다. SPS 페더레이션 게이트웨이 설치 및 구성에 대한 자세한 내용은 *Secure Proxy Server Administration Guide*(보안 프록시 서버 관리 안내서)를 참조하십시오.

특성을 HTTP 헤더로 처리하기 위한 이벤트 순서는 다음과 같습니다.

1. 어설션이 어설션 당사자 측에서 생성된 후 해당 어설션이 신뢰 당사자의 적절한 소비자 서비스에 전송됩니다. 전송 메커니즘(POST 또는 아티팩트 또는 WS-페더레이션)은 무관합니다.

   참고: 소비자 서비스는 SAML 자격 증명 수집기(SAML 1.x), 어설션 소비자 서비스(SAML 2.0) 또는 보안 토큰 소비자 서비스(WS-페더레이션)일 수 있습니다.
2. 소비자 서비스가 해당 로컬 정책 서버를 호출하여 구성된 인증 체계를 통해 어설션으로 사용자를 인증합니다.
3. 인증 체계 리디렉션 모드 매개 변수가 PersistAttributes 로 설정된 경우 정책 서버가 세션 저장소에 있는 특성을 세션 변수로 캐시합니다.
4. 인증 결과가 소비자 서비스에 반환됩니다.
5. 소비자 서비스가 브라우저를 보호된 대상 리소스로 리디렉션합니다.
6. 브라우저가 대상 리소스 액세스를 시도합니다.
7. 웹 에이전트가 정책 서버를 호출하여 사용자 세션의 유효성을 검사하고 사용자에게 대상 리소스에 대한 액세스 권한이 부여되었는지 확인합니다.
8. 정책 서버가 구성된 응답별로 특성을 검색합니다.
9. 정책 서버가 응답을 처리하고 특성을 웹 에이전트에 보냅니다.
10. 웹 에이전트가 필요에 따라 HTTP 헤더를 설정합니다.

특성을 HTTP 헤더로 제공하기 위한 구성 개요

세션 저장소에 캐시된 SAML 특성을 검색하여 HTTP 헤더로 제공하려면 여러 구성 단계가 필요합니다.

다음 단계를 수행하십시오.

1. SAML 인증 체계에 대한 리디렉션 모드로 "PersistAttributes"를 선택합니다. 그러면 SAML 특성이 HTTP 헤더로 반환될 수 있습니다.
2. 대상 리소스가 포함된 영역에 대해 권한 부여 규칙을 구성합니다.
3. 대상 리소스를 보호하는 영역에서 "PersistentRealm"을 설정합니다.

4. 헤더로 제공할 SAML 특성 각각에 대해 활성 응답 유형을 사용하는 응답을 구성합니다.
5. 권한 부여 규칙과 활성 응답을 바인딩하여 특성을 HTTP 헤더로 사용하도록 구현하는 정책을 생성합니다.

SAML 특성을 저장하도록 리디렉션 모드 설정

신뢰 당사자가 SAML 어설션으로 사용자를 인증한 후 SAML 특성이 세션 저장소에 기록됩니다. 그런 다음 브라우저가 대상 리소스로 리디렉션됩니다.

특성 데이터와 함께 브라우저를 리디렉션하려면

1. 관리 UI 에 로그인합니다.
2. SAML 인증 체계의 구성 페이지로 이동합니다.
3. "리디렉션 모드" 매개 변수를 "특성 유지"로 설정합니다. 다음과 같이 "리디렉션 모드" 필드를 찾습니다.

   SAML 1.x

   "리디렉션 모드"는 기본 구성 페이지의 "체계 설정" 섹션에 있습니다.

   SAML 2.0

   "SAML 2.0 구성", "SSO"를 차례로 클릭합니다. "리디렉션 모드"는 페이지의 "SSO" 섹션에 있습니다.

   WS-페더레이션

   "WS-페더레이션 구성", "SAML 프로필"을 차례로 클릭합니다. "리디렉션 모드"는 페이지의 "SSO" 섹션에 있습니다.
4. "제출"을 클릭하여 변경 내용을 저장합니다.

이제 리디렉션 모드가 특성 데이터를 전달하도록 설정되었습니다.

사용자의 유효성을 검사하기 위한 권한 부여 규칙 만들기

보호된 대상 리소스가 포함된 영역의 경우 세션 저장소에서 SAML 특성을 검색하기 위한 규칙을 생성하십시오.

규칙은 권한 부여 이벤트(onAccessAccept)를 기반으로 합니다. 사용자는 FWS 응용 프로그램에서 이미 인증되었습니다. 웹 에이전트는 사용자를 다시 인증하고 HTTP 헤더를 전달할 수 없습니다. 특성 검색은 권한 부여 단계에서 발생합니다.

영역에 대한 OnAccessAccept 규칙을 생성하려면

1. 관리 UI 에 로그온합니다.
2. "정책", "도메인", "영역"으로 이동합니다.
3. 대상 리소스가 포함된 영역을 선택합니다.
4. "규칙" 섹션에서 "만들기"를 클릭합니다.

   "규칙 만들기" 페이지가 표시됩니다.
5. 이름과 설명(선택 사항)을 입력합니다.
6. "리소스" 필드에 별표(*)를 입력합니다.
7. "작업" 섹션에서 "권한 부여 이벤트"와 "OnAccessAccept"를 선택합니다.
8. "허용/거부 및 사용/사용 안 함" 섹션에서 "사용"을 선택합니다.
9. "확인"을 클릭하여 규칙을 저장합니다.

이제 보호된 리소스가 포함된 영역에 대한 권한 부여 규칙이 정의되었습니다.

특성을 HTTP 헤더로 보내기 위한 응답 구성

SAML 특성을 웹 에이전트에 HTTP 헤더로 보내는 응답을 구성하십시오. 그러면 웹 에이전트가 응답을 처리하고 헤더 변수를 클라이언트 응용 프로그램에 제공합니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그온합니다.
2. "정책", "도메인", "도메인"으로 이동합니다.
3. 대상 리소스에 대한 도메인을 선택하고 "수정"을 클릭합니다.

4. "응답" 탭을 선택합니다.
5. "만들기"를 클릭합니다.

   "응답" 대화 상자가 열립니다.
6. 이름을 입력합니다.
7. 에이전트 유형이 SiteMinder 웹 에이전트인지 확인합니다.
8. "응답 특성 만들기"를 클릭합니다.

   "응답 특성" 대화 상자가 열립니다.
9. "특성" 필드에서 "WebAgent-HTTP-Header-Variable"을 선택합니다.
10. "특성 종류"에서 "활성 응답"을 선택합니다.
11. 다음과 같이 필드에 데이터를 입력합니다.

    변수 이름

    원하는 헤더 변수 이름을 지정합니다. 사용자가 이 이름을 할당합니다.

    라이브러리 이름

    smfedattrresponse

    이 값은 이 필드에 대한 항목이어야 합니다.

    함수 이름

    getAttributeValue

    이 값은 이 필드에 대한 항목이어야 합니다.

    매개 변수

    어설션에 나타나는 대로 특성 이름을 지정합니다.

    사용자와 페더레이션된 파트너 간의 계약에 따라 어설션에 있는 특성이 결정됩니다.
12. "확인"을 클릭하여 특성을 저장합니다.
13. HTTP 헤더 변수가 될 특성 각각에 대해 절차를 반복합니다. 단일 응답에 대해 여러 특성을 구성할 수 있습니다.

    "응답" 탭으로 돌아갑니다. 생성한 특성이 "특성 목록" 섹션에 나열됩니다.

14. "확인"을 클릭하여 응답을 저장합니다.

    "응답" 탭으로 돌아갑니다.

15. "제출"을 클릭하여 도메인을 저장합니다.

응답이 HTTP 헤더가 될 특성을 웹 에이전트에 보냅니다.

특성을 HTTP 헤더로 구현하기 위한 정책 만들기

SAML 특성을 HTTP 헤더로 사용하도록 구현하려면 정책에서 권한 부여 이벤트 규칙과 활성 응답을 함께 그룹화하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그온합니다.
2. "정책", "도메인", "도메인"으로 이동합니다.
3. 대상 리소스가 포함된 도메인을 선택하고 "수정"을 클릭합니다.
4. "정책" 탭을 선택하고 "정책" 섹션에서 "만들기"를 클릭합니다.

   "정책 만들기" 대화 상자가 열립니다.

5. "이름" 필드에 설명이 포함된 이름을 입력합니다.
6. "사용자" 탭에서 보호된 리소스에 액세스할 수 있는 사용자를 선택합니다.
7. "규칙" 탭에서 이전에 생성한 권한 부여 규칙을 추가합니다.
8. 권한 부여 규칙을 선택하고 "응답 추가"를 클릭합니다.

   "사용 가능한 응답" 대화 상자가 열립니다.

9. 이전에 생성한 활성 응답을 선택하고 "확인"을 클릭합니다.

   "규칙" 탭으로 돌아갑니다. 권한 부여 규칙과 함께 응답이 나타납니다.

10. "제출"을 클릭하여 정책을 저장합니다.

SAML 특성이 HTTP 헤더로 사용되도록 설정하는 정책이 완성되었습니다.

백 채널에 대해 클라이언트 인증서 인증이 사용되도록 설정(선택 사항)

HTTP-아티팩트 싱글 사인온을 사용하고 있는 경우 클라이언트 인증서 인증을 선택하여 생산자의 어설션 검색 서비스를 보호할 수 있습니다. 이 서비스는 어설션을 검색하여 소비자에게 보냅니다.

참고: 클라이언트 인증서 인증은 선택 사항입니다. 기본 인증을 사용할 수도 있습니다.

SAML 자격 증명 수집기가 SAML 아티팩트 인증 체계를 호출합니다. SAML 자격 증명 수집기가 생산자에서 SAML 어설션을 검색하기 위해 체계에서 정보를 수집합니다. 어설션 검색 서비스가 포함된 영역에 대한 인증 방법을 지정해야 합니다. SAML 자격 증명 수집기가 어설션을 검색하기 위해 제공할 자격 증명 유형을 확인합니다.

어설션 검색 서비스가 클라이언트 인증서 인증 체계로 보호되는 경우 다음 구성 태스크를 수행하십시오.

1. 인증서 데이터 저장소에 클라이언트 인증서를 추가합니다 (페이지 188).
2. 백 채널 인증에 대한 클라이언트 인증서 옵션을 선택합니다 (페이지 189). 인증서는 필수 자격 증명입니다.

참고: 어설션 측 정책 서버의 관리자가 어설션 검색 서비스를 보호하도록 정책을 구성해야 합니다. 이 정책에 대한 영역이 X.509 클라이언트 인증서 인증 체계를 사용해야 합니다.

인증서 데이터 저장소에 클라이언트 인증서 추가

인증 기관으로부터 받은 개인 키/인증서 쌍이 있어야 합니다. 관리 UI 를 사용하여 개인 키/인증서 쌍을 인증서 데이터 저장소에 추가하십시오. 키/인증서 쌍이 데이터 저장소에 이미 있는 경우 이 단계를 건너뛰십시오. 지침은 *정책 서버 구성 안내서*를 참조하십시오.

키/인증서 쌍을 가져오는 경우 할당하는 별칭은 인증 체계 설정에 있는 "가맹 이름" 필드와 동일한 값이어야 합니다. 또한 인증서에 있는 "주체"의 CN 특성도 "가맹 이름" 필드와 일치해야 합니다. 예를 들어 "가맹 이름"이 CompanyA 인 경우를 가정합니다. 이 경우 별칭은 Company A 이고 "주체"에 대한 CN 값은 CN=CompanyA, OU=Development, O=CA, L=Islandia, ST=NY, C=US 여야 합니다.

중요! 인증 체계에 있는 "가맹 이름" 필드는 생산자의 가맹 개체에 할당된 이름과 일치해야 합니다. SiteMinder 가 생산자인 경우 인증 체계에 있는 "가맹 이름"은 가맹 개체의 "일반" 설정에 있는 "이름" 필드와 일치해야 합니다.

백 채널 인증에 대한 클라이언트 인증서 옵션 선택

소비자가 생산자의 어설션 검색 서비스에 액세스하려고 할 때 인증서를 자격 증명으로 제공하도록 하려면 클라이언트 인증서 옵션을 선택하십시오.

클라이언트 인증서 옵션을 선택하려면

1. SAML 아티팩트 인증 체계 대화 상자의 "체계 설정" 섹션으로 이동합니다.
2. "Client Cert for the Authentication"(인증용 클라이언트 인증서) 필드를 선택합니다.

SAML 1.x 인증 체계로 리소스를 보호하는 방법

SAML 1.x 인증 체계를 사용하는 SiteMinder 정책을 구성하여 대상 페더레이션 리소스를 보호하십시오.

다음 단계를 수행하십시오.

1. SAML 인증 체계를 사용하는 영역을 생성합니다. 영역은 대상 리소스를 수집한 것입니다.

   다음과 같은 방법으로 영역을 생성할 수 있습니다.

   - 이미 구성된 인증 체계 각각에 대해 고유한 영역을 생성합니다 (페이지 190).
   - 사용자 지정 인증 체계를 사용하여 요청을 해당 SAML 인증 체계로 발송하는 단일 대상 영역을 구성합니다 (페이지 191). 모든 생산자에 대해 단일 대상이 있는 영역 하나를 구성하면 SAML 인증을 위한 영역 구성이 단순화됩니다.

2. 연결된 규칙과 응답(선택 사항)을 구성합니다.
3. 대상 리소스를 보호하는 정책으로 영역, 규칙 및 응답을 그룹화합니다.

중요! 영역의 각 대상 URL 은 사이트 간 전송 URL 에서도 식별됩니다. 사이트 간 전송 URL 은 생산자에서 소비자로 사용자를 리디렉션합니다. URL TARGET 변수에서 이 URL 을 지정합니다. 생산자 사이트에서 관리자가 사용자를 소비자로 리디렉션하는 링크에 이 URL 을 포함합니다.

각 인증 체계에 대해 고유 영역 구성

각 SAML 또는 WS-페더레이션 인증 체계에 대해 고유 영역을 구성하는 절차는 영역을 생성하는 표준 지침을 따릅니다.

다음 단계를 수행하십시오.

1. "정책", "도메인", "도메인"으로 이동합니다.

   도메인을 생성하는 페이지가 표시됩니다.

2. "도메인 만들기"를 클릭합니다.
3. 도메인 이름을 입력합니다.
4. 도메인에 사용자 디렉터리를 추가합니다. 이 디렉터리는 페더레이션된 리소스에 대한 액세스를 요청하는 사용자가 포함된 디렉터리입니다.

5. "영역" 탭을 선택하고 영역을 생성합니다.
   - "에이전트" 필드에서 대상 리소스가 있는 웹 서버를 보호하는 웹 에이전트를 선택합니다.
   - "인증 체계" 필드에서 적절한 인증 체계를 선택합니다.
6. 영역에 대한 규칙을 생성합니다.

   규칙의 일부로 사용자 인증 시 처리를 제어하는 데 사용되는 작업(Get, Post, or Put)을 선택합니다.
7. "정책" 탭을 선택하고 대상 페더레이션 리소스를 보호하는 정책을 구성합니다. 이전에 생성한 영역을 이 정책과 연결합니다.

이제 고유 영역이 있는 정책이 페더레이션된 리소스를 보호합니다.

모든 인증 체계에 대해 단일 대상 영역 구성

인증 체계에 대한 영역 구성을 단순화하려면 어설션을 생성하는 사이트 여러 개에 대해 단일 대상 영역을 생성하십시오.

이 태스크를 수행하려면 다음 구성 요소를 설정하십시오.

- 단일 사용자 지정 인증 체계

  이 사용자 지정 체계는 이미 각 어설션 당사자에 대해 구성한 해당 SAML 또는 WS-페더레이션 인증 체계에 요청을 전달합니다.
- 대상 URL 이 하나 있는 단일 영역

단일 대상 영역에 대한 인증 체계 만들기

단일 대상 영역에 대한 사용자 지정 인증 체계를 정의하려면

- 인증 체계를 구성해야 합니다.
- 사용자 지정 체계에서 정책 서버에 리소스 요청에 적용할 인증 체계를 알려 주는 매개 변수를 정의해야 합니다.

먼저 구성된 SAML 또는 WS-페더레이션 인증 체계가 있는지 확인하십시오. 없는 경우 사용자 지정 체계가 참조할 수 있는 이러한 체계를 구성하십시오.

인증 체계를 생성하려면

1. "인프라", "인증", "인증 체계"로 이동합니다.

   "인증 체계 만들기" 페이지가 표시됩니다.
2. 사용 중인 프로토콜의 절차에 따라 인증 체계를 하나 이상 생성합니다.
3. "확인"을 클릭하여 종료합니다.

추가 정보:

SAML 1.x 인증 체계 (페이지 167)
WS-페더레이션 인증 체계 개요 (페이지 337)
SAML 2.0 인증 체계를 구성하는 방법 (페이지 267)

사용자 지정 인증 체계 만들기

단일 대상 영역이 특정 사용자 지정 인증 체계를 통해 제대로 작동합니다.

단일 대상 영역에 대한 사용자 지정 인증 체계를 구성하려면

1. "인프라", "인증", "인증 체계"로 이동합니다.

   "인증 체계 만들기" 페이지가 표시됩니다.
2. 다음과 같이 필드에 데이터를 입력합니다.

   이름

   사용자 지정 인증 체계의 설명이 포함된 이름(예: SAML Custom Auth Scheme)을 입력합니다.
3. "체계 일반 설정" 섹션의 다음 필드에 데이터를 입력합니다.

   인증 체계 유형

   사용자 지정 템플릿

   보호 수준

   새 수준 설정의 기본값을 적용합니다.
4. 체계 설정 섹션의 다음 필드에 데이터를 입력합니다.

   라이브러리

   smauthsinglefed

암호

이 필드는 비워 둡니다.

암호 확인

이 필드는 비워 둡니다.

매개 변수

다음 매개 변수 중 하나를 지정합니다.

- SCHEMESET=LIST; <*saml-scheme1*>;<*saml_scheme2*>

  사용할 SAML 인증 체계 이름 목록을 지정합니다. artifact_producer1 이라는 아티팩트 체계와 samlpost_producer2 라는 POST 프로필 체계를 구성한 경우 이러한 체계를 입력합니다. 예를 들면 다음과 같습니다.

  SCHEMESET=LIST;artifact_producer1;samlpost_producer2

- SCHEMESET=SAML_ALL;

  구성된 체계를 모두 지정합니다. 그러면 사용자 지정 인증 체계가 모든 SAML 인증 체계를 열거하고 요청에 대해 올바른 공급자 원본 ID 가 있는 체계를 찾습니다.

- SCHEMESET=SAML_POST;

  구성한 SAML POST 프로필 체계를 모두 지정합니다. 그러면 사용자 지정 인증 체계가 POST 프로필 체계를 열거하고 요청에 대해 올바른 공급자 원본 ID 가 있는 체계를 찾습니다.

- SCHEMESET=SAML_ART;

  구성한 SAML 아티팩트 체계를 모두 지정합니다. 그러면 사용자 지정 인증 체계가 아티팩트 체계를 열거하고 요청에 대해 올바른 공급자 원본 ID 가 있는 체계를 찾습니다.

- SCHEMESET=WSFED_PASSIVE;

  올바른 계정 파트너 ID 가 있는 체계를 찾기 위해 모든 WS-페더레이션 인증 체계를 지정합니다.

SiteMinder 관리자에 대해 이 체계 사용

선택 취소된 상태로 둡니다.

5. 제출을 클릭합니다.

사용자 지정 인증 체계가 완료되었습니다.

단일 대상 영역 구성

인증 체계를 구성하여 사용자 지정 체계와 연결한 후 페더레이션 리소스에 대한 단일 대상 영역을 구성하십시오.

다음 단계를 수행하십시오.

1. "정책", "도메인", "도메인"으로 이동합니다.
2. 단일 대상 영역에 대한 정책 도메인을 수정합니다.
3. "영역" 탭을 선택하고 "만들기"를 클릭합니다.

   "영역 만들기" 대화 상자가 열립니다.
4. 다음 값을 입력하여 단일 대상 영역을 생성합니다.

   이름

   이 단일 대상 영역에 대한 이름을 입력합니다.
5. "리소스" 옵션의 다음 필드에 데이터를 입력합니다.

   에이전트

   대상 리소스가 있는 웹 서버를 보호하는 웹 에이전트를 선택합니다.

   리소스 필터

   대상 리소스의 위치를 지정합니다. 이 위치는 페더레이션된 리소스를 요청하는 사용자가 리디렉션되는 위치입니다.

   예를 들면 /FederatedResources 입니다.
6. "기본 리소스 보호" 섹션에서 "보호됨" 옵션을 선택합니다.
7. "인증 체계" 필드에서 이전에 구성된 사용자 지정 인증 체계를 선택합니다.

   예를 들어 사용자 지정 체계의 이름이 "Fed Custom Scheme"(페더레이션 사용자 지정 체계)인 경우 이 체계를 선택합니다.
8. "확인"을 클릭합니다.

단일 대상 영역 태스크가 완료되었습니다.

단일 대상 영역에 대한 규칙 구성

단일 대상 영역을 구성한 후 리소스를 보호하기 위한 규칙을 구성하십시오.

1. 단일 대상 영역에 대한 "수정" 페이지로 이동합니다.
2. "규칙" 섹션에서 "만들기"를 클릭합니다.

   "규칙 만들기" 페이지가 표시됩니다.
3. 규칙 페이지의 필드에 대한 값을 입력합니다.
4. "확인"을 클릭합니다.

단일 대상 영역 구성에 새 규칙이 포함됩니다.

단일 대상 영역을 사용하여 정책 만들기

단일 대상 영역을 참조하는 정책을 생성하십시오. 단일 대상 영역에서는 요청을 적절한 SAML 인증 체계로 보내는 사용자 지정 인증 체계를 사용합니다.

참고: 이 절차에서는 도메인, 사용자 지정 인증 체계, 단일 대상 영역 및 연결된 규칙을 이미 구성했다고 가정합니다.

다음 단계를 수행하십시오.

1. 이전에 구성한 도메인으로 이동합니다.
2. "정책" 탭을 선택하고 "만들기"를 클릭합니다.

   "정책 만들기" 페이지가 열립니다.
3. "일반" 섹션에 정책의 이름과 설명을 입력합니다.
4. "사용자" 섹션에서 사용자를 정책에 추가합니다.
5. "규칙" 탭에서 단일 대상 영역에 대해 생성한 규칙을 추가합니다.

   나머지 탭은 선택 사항입니다.
6. "확인"을 클릭합니다.
7. "제출"을 클릭합니다.

정책 태스크가 완료되었습니다. 요청으로 인해 이 정책이 트리거되는 경우 단일 영역 및 연결된 인증 체계에 따라 사용자가 인증됩니다.

제 14 장: SAML 2.0 아이덴티티 공급자 구성

어설션 파트너(레거시)에 대한 사전 요구 사항

어설션 파트너를 구성하려면 다음 조건을 확인하십시오.

- 정책 서버가 설치되어 있어야 합니다.
- 다음 옵션 중 하나가 설치되어 있어야 합니다.
  - 웹 에이전트 및 웹 에이전트 옵션 팩. 웹 에이전트는 사용자를 인증하고 SiteMinder 세션을 설정합니다. 옵션 팩은 페더레이션 웹 서비스 응용 프로그램을 제공합니다. 적절한 네트워크 시스템에 FWS 응용 프로그램을 배포해야 합니다.
  - SPS 페더레이션 게이트웨이에 포함된 웹 에이전트가 있고 포함된 Tomcat 웹 서버에 페더레이션 웹 서비스 응용 프로그램이 있습니다.

  자세한 내용은 *웹 에이전트 옵션 팩 안내서*를 참조하십시오.
- 메시지 서명 및 암호 해독이 필요한 기능을 위해 개인 키와 인증서를 가져와야 합니다.
- 페더레이션된 네트워크 내에 신뢰 파트너가 설정되어 있어야 합니다.

아이덴티티 공급자를 구성하는 방법

SiteMinder 는 아이덴티티 공급자로 작동하는 경우 해당 비즈니스 파트너인 서비스 공급자에 대한 어설션을 생성합니다. 페더레이션된 파트너 관계를 설정하려면 아이덴티티 공급자에게 각 파트너에 대한 정보가 필요합니다. 각 파트너에 대해 서비스 공급자 개체를 생성하고, 엔터티 두 개가 어설션을 전달하고 싱글 사인온 등의 프로필을 충족하기 위해 통신하는 방법을 정의하십시오.

아이덴티티 공급자를 구성하려면

1. 서비스 공급자 개체를 생성합니다.
2. 서비스 공급자를 가맹 도메인에 추가합니다.

3. 서비스 공급자에 대한 일반 식별 정보를 지정합니다.
4. 사용자 저장소에서 사용자를 선택합니다. 아이덴티티 공급자가 이러한 사용자에 대한 어설션을 생성합니다.
5. 이름 ID 를 지정합니다.
6. SSO(싱글 사인온) 프로필을 구성합니다.

   전체 SSO 프로필을 구성하지 않은 상태로 서비스 공급자 엔터티를 저장할 수 있습니다. 하지만 SSO 구성을 완료하지 않고는 어설션을 서비스 공급자에게 전달할 수 없습니다.
7. 요청과 응답에 대해 서명 및 암호화를 구성합니다.
8. 선택적 구성 태스크를 완료합니다.

팁:

- 아이덴티티 공급자와 서비스 공급자의 특정 매개 변수 값이 일치해야 구성이 올바로 작동합니다. 이러한 매개 변수 목록은 동일한 값을 사용해야 하는 구성 설정 (페이지 411)에서 찾을 수 있습니다.
- 페더레이션 웹 서비스 서블릿에 대해 올바른 URL 을 사용하십시오. URL 목록은 SiteMinder 구성에 사용되는 페더레이션 웹 서비스 URL (페이지 417)에서 찾을 수 있습니다.

서비스 공급자를 식별하기 위한 선택적 구성 태스크

서비스 공급자를 식별하기 위한 선택적 태스크는 다음과 같습니다.

- 서비스 공급자에 액세스하는 데 사용되는 주소를 제한할 IP 주소 제한을 구성합니다 (페이지 204).
- 서비스 공급자 작업에 대한 시간 제한을 구성합니다 (페이지 203).
- 향상된 클라이언트 또는 프록시 프로필이 사용되도록 설정합니다 (페이지 214).
- 어설션에 포함할 특성을 구성합니다.
- SLO(싱글 로그아웃)를 구성합니다 (페이지 253).
- 아이덴티티 공급자 검색 프로필을 구성합니다 (페이지 256).
- 어설션 및/또는 전체 어설션의 이름 ID 를 암호화합니다 (페이지 260).
- 어설션 및/또는 전체 어설션 응답에 서명합니다 (페이지 222).

- 아티팩트 확인 메시지 및/또는 아티팩트 응답에 서명합니다 (페이지 222).
- 어설션 생성기 플러그인을 사용하여 SAML 어설션 응답을 사용자 지정합니다 (페이지 158).

레거시 페더레이션 대화 상자 탐색

관리 UI 에서는 레거시 페더레이션 구성 대화 상자로 이동하는 방법 두 가지를 제공합니다.

다음 두 방법 중 하나로 탐색할 수 있습니다.

- 마법사를 따라 새 레거시 페더레이션 개체 구성

  개체를 생성하는 경우 페이지가 표시되면서 구성 마법사가 나타납니다. 구성 마법사의 단계를 따라 개체를 생성하십시오.

- 탭을 선택하여 기존 레거시 페더레이션 개체 수정

  기존 개체를 수정하는 경우 페이지가 표시되면서 일련의 탭이 나타납니다. 이러한 탭에서 구성을 수정하십시오. 이러한 탭은 구성 마법사의 단계와 동일합니다.

가맹 도메인에 SAML 2.0 서비스 공급자 추가

서비스 공급자를 SiteMinder 에서 생성된 어설션의 사용 가능한 소비자로 식별하려면 아이덴티티 공급자의 가맹 도메인에 서비스 공급자를 추가하십시오. 그런 다음 서비스 공급자 구성을 정의하면 아이덴티티 공급자가 해당 어설션을 발급할 수 있습니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "페더레이션", "레거시 페더레이션", "SAML 서비스 공급자"를 차례로 클릭합니다.
3. "SAML 서비스 공급자 만들기"를 클릭합니다.
4. "가맹 도메인"을 선택하고 "다음"을 클릭합니다.

일반 설정을 구성합니다.

서비스 공급자 개체에 대한 일반 정보 구성

"일반" 페이지를 선택하여 서비스 공급자를 명명하고 SP ID, IDP ID 등의 상세 정보를 제공하십시오. 또한 서비스 공급자에 액세스하기 위한 IP 주소 및 시간 제한을 구성할 수 있습니다.

일반 설정을 구성하려면

1. "일반" 설정으로 이동합니다.
2. 필수 필드에 주의하면서 필드에 대한 값을 입력합니다.

   필드 설명을 보려면 "도움말"을 클릭하십시오. 특히 다음 필드에 유의하십시오.

   인증 URL

   이 URL 은 redirect.jsp 파일을 가리킵니다. SiteMinder 정책으로 redirect.jsp 파일을 보호하십시오. 정책은 보호된 서비스 공급자 리소스를 요청하지만 SiteMinder 세션이 없는 사용자에 대한 인증 챌린지를 트리거합니다.

   차이 시간

   아이덴티티 공급자의 시스템 클록과 서비스 공급자의 시스템 클록 간의 차이(초)를 지정합니다. 차이 시간은 싱글 사인온과 싱글 로그아웃에 사용됩니다.

   싱글 사인온의 경우 차이 시간 및 싱글 사인온 유효 기간("SSO" 탭의 "유효 기간" 필드) 값에 따라 어설션 유효 기간이 결정됩니다. 어설션 유효 기간 계산 (페이지 141) 방법을 검토하면 차이 시간에 대해 자세히 이해할 수 있습니다.

   싱글 로그아웃의 경우 SLO 유효 기간("SLO" 탭의 "유효 기간" 필드) 및 차이 시간 값에 따라 싱글 로그아웃 요청의 총 유효 시간이 결정됩니다. 싱글 로그아웃 요청 유효 기간 (페이지 254) 계산 방법을 검토하면 차이 시간에 대해 자세히 이해할 수 있습니다.

추가 정보:

서비스 공급자에 대한 IP 주소 제한 구성(선택 사항) (페이지 204)
서비스 공급자 가용성에 대한 시간 제한 구성(선택 사항) (페이지 203)

SiteMinder 세션이 없는 사용자 인증

가맹 도메인에 서비스 공급자를 추가하는 경우 설정해야 하는 매개 변수 중 하나는 인증 URL 매개 변수입니다.

인증 URL 은 redirect.jsp 파일을 가리킵니다. 이 파일은 웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 설치하는 아이덴티티 공급자 사이트에 설치됩니다. SiteMinder 정책으로 redirect.jsp 파일을 보호하십시오. 정책은 보호된 서비스 공급자 리소스를 요청하지만 SiteMinder 세션이 없는 사용자에 대한 인증 챌린지를 트리거합니다.

다음 바인딩에는 SiteMinder 세션이 필요합니다.

- 보호된 서비스 공급자 리소스를 요청하는 사용자의 경우

  HTTP 아티팩트 바인딩을 사용하여 싱글 사인온을 구성하는 경우 영구 세션을 설정하여 SAML 어설션을 세션 저장소에 저장하십시오.

- HTTP POST 바인딩을 사용하는 싱글 사인온의 경우

  사용자에게 세션이 있어야 하지만 영구 세션이 아니어도 됩니다. 어설션은 브라우저를 통해 서비스 공급자에게 직접 전달됩니다. 어설션이 세션 저장소에 저장되지 않아도 됩니다.

- 싱글 로그아웃의 경우

  싱글 로그아웃이 사용되도록 설정하는 경우에는 영구 세션이 필요합니다. 사용자가 먼저 서비스 공급자 리소스를 요청하면 세션이 세션 저장소에 저장됩니다. 세션 정보는 나중에 싱글 로그아웃이 실행될 때 필요합니다.

사용자가 인증되어 redirect.jsp 파일에 성공적으로 액세스한 후 세션이 설정됩니다. redirect.jsp 파일이 사용자를 아이덴티티 공급자 웹 에이전트나 SPS 페더레이션 게이트웨이로 다시 리디렉션합니다. 그런 다음 SiteMinder 가 요청을 처리합니다.

인증 URL 을 보호하는 절차는 다음 배포와 관계없이 동일합니다.

- 웹 에이전트와 동일한 시스템에 설치된 웹 에이전트 옵션 팩
- 웹 서버 프록시에 웹 에이전트가 설치된 응용 프로그램 서버
- 응용 프로그램 서버 에이전트와 함께 설치된 응용 프로그램 서버
- 아이덴티티 공급자에 설치된 SPS 페더레이션 게이트웨이

인증 URL 을 보호하도록 정책 구성

인증 URL 을 보호하려면

1. 관리 UI 에 로그인합니다.
2. 어설션 당사자 웹 서버에 대해 정의하는 영역에 바인드할 웹 에이전트를 생성합니다. 웹 서버와 FWS 응용 프로그램에 대해 고유한 에이전트 이름을 할당하거나 둘 다에 대해 동일한 에이전트 이름을 사용합니다.
3. 소비자 리소스에 액세스하려고 할 때 챌린지가 표시되는 사용자에 대한 정책 도메인을 생성합니다.
4. 정책 도메인에 속한 리소스에 액세스할 수 있어야 하는 사용자를 선택합니다.
5. 다음 값으로 정책 도메인에 대한 영역을 정의합니다.

   에이전트

   어설션 당사자 웹 서버에 대한 에이전트

   리소스 필터

   웹 에이전트 r6.x QMR 6, r12.0 SP2, r12.0 SP3 및 SPS 페더레이션 게이트웨이. 다음과 같이 입력합니다.

   /siteminderagent/redirectjsp/

   리소스 필터 /siteminderagent/redirectjsp/는 FWS 응용 프로그램이 자동으로 설정하는 별칭입니다. 별칭 참조는 다음과 같습니다.

   - 웹 에이전트:

     web_agent_home/affwebservices/redirectjsp

   - SPS 페더레이션 게이트웨이:

     sps_home/secure-proxy/Tomcat/webapps/affwebservices/redirectjsp

   영구 세션

   SAML 아티팩트 프로필의 경우에만 영역 대화 상자의 "세션" 섹션에 있는 "영구" 확인란을 선택합니다. 영구 세션을 구성하지 않으면 사용자가 소비자 리소스에 액세스할 수 없습니다.

   나머지 설정의 경우 기본값을 적용하거나 필요에 따라 수정합니다.
6. "확인"을 클릭하여 영역을 저장합니다.
7. 영역에 대한 규칙을 생성합니다. "리소스" 필드에서 기본값인 별표(*)를 적용하여 영역에 대한 리소스를 모두 보호합니다.

8. 이전 단계에서 만든 규칙이 포함된 어설션 당사자 웹 서버에 대한 정책을 생성합니다.
9. 생성하는 어설션의 대상이 되는 사용자 선택 (페이지 136) 태스크를 완료합니다.

서비스 공급자 가용성에 대한 시간 제한 구성(선택 사항)

서비스 공급자 리소스를 사용할 수 있는 시기에 대한 시간 제한을 지정할 수 있습니다. 시간 제한을 지정하면 리소스에 대한 액세스가 지정된 기간 동안에만 허용됩니다. 사용자가 지정된 기간을 벗어나 리소스에 액세스하려고 하면 아이덴티티 공급자가 SAML 어설션을 생성하지 않습니다.

참고: 시간 제한은 정책 서버가 설치된 서버의 시스템 클록을 기준으로 합니다.

시간 제한을 지정하려면

1. "일반" 설정에서 시작합니다.

   페이지의 "제한" 섹션에 있는 "시간" 섹션에서 "설정"을 클릭합니다.

   "시간 제한" 페이지가 표시됩니다.
2. 일정을 완료합니다. 이 일정 표는 규칙 개체의 "시간 제한" 표와 같습니다. 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.
3. "확인"을 클릭합니다.

시간 제한 일정이 설정되었습니다.

서비스 공급자에 대한 IP 주소 제한 구성(선택 사항)

서비스 공급자에 액세스하기 위해 브라우저가 실행되고 있는 웹 서버의 IP 주소, 범위 주소 또는 서브넷 마스크를 지정할 수 있습니다. 서비스 공급자에 대해 IP 주소를 지정하면 서비스 공급자가 적절한 IP 주소의 사용자만 허용합니다.

IP 주소를 지정하려면

1. "일반" 설정에서 시작합니다.

   페이지의 "제한" 섹션에 있는 "IP 주소" 영역에서 "추가"를 클릭합니다.

   "IP 제한" 페이지가 표시됩니다.

2. 추가하고 있는 IP 주소 유형에 대한 옵션을 선택하고 연결된 필드에 해당 주소 유형에 대한 데이터를 입력합니다.

   참고: IP 주소는 모르지만 주소에 대한 도메인 이름은 알고 있는 경우 "DNS 조회" 단추를 클릭합니다. 이 단추를 클릭하면 "DNS 조회" 페이지가 열립니다. "호스트 이름" 필드에 정규화된 호스트 이름을 입력하고 "확인"을 클릭합니다.

   - 단일 호스트--브라우저를 호스트하는 단일 IP 주소를 지정합니다. 단일 IP 주소를 지정하면 사용자가 지정된 IP 주소에서만 서비스 공급자에 액세스할 수 있습니다.
   - 호스트 이름--호스트 이름을 사용하여 웹 서버를 지정합니다. 호스트 이름을 지정하면 지정된 호스트의 사용자만 서비스 공급자에 액세스할 수 있습니다.
   - 서브넷 마스크--웹 서버에 대한 서브넷 마스크를 지정합니다. 서브넷 마스크를 지정하면 지정된 서브넷 마스크의 사용자만 서비스 공급자에 액세스할 수 있습니다. 이 단추를 선택하면 "주소 및 서브넷 마스크 추가" 대화 상자가 열립니다. 왼쪽 및 오른쪽 화살표 단추를 사용하거나 슬라이더 막대를 클릭한 상태로 끌어서 놓아 서브넷 마스크를 선택합니다.
   - 범위--IP 주소 범위를 지정합니다. IP 주소 범위를 지정하면 서비스 공급자가 주소 범위에 속한 IP 주소 중 하나의 사용자만 허용합니다. 시작 및 끝 주소를 입력하여 범위를 결정합니다.

3. "확인"을 클릭하여 구성을 저장합니다.

프록시 서버 식별(선택 사항)

사용 중인 네트워크의 클라이언트와 페더레이션 웹 서비스가 있는 시스템 간에 프록시 서버가 있는 경우 URL 의 프로토콜 및 기관 부분을 지정하십시오. 구문은 *protocol*:*authority* 입니다.

protocol

http: 또는 https:

authority

//*host.domain.com* 또는 //*host.domain.com:port*

예: http://example.ca.com

프록시 서버를 식별하려면

1. 구성 마법사의 "일반" 단계에서 시작합니다.

   페이지의 "고급" 섹션에 있는 "서버" 필드에 URL 을 입력합니다.

2. "제출"을 클릭합니다.

생성하는 어설션의 대상이 되는 사용자 선택

어설션 당사자 측에서 수행되는 구성의 일부로, 어설션 생성기가 생성하는 SAML 어설션의 대상이 되는 사용자 및 그룹 목록을 포함하십시오. 어설션 당사자는 SAML 1.x 생산자, SAML 2.0 아이덴티티 공급자 또는 WS 페더레이션 계정 파트너입니다.

가맹 도메인에 있는 디렉터리의 사용자 및 그룹만 추가할 수 있습니다.

페더레이션된 트랜잭션에 대한 사용자 및 그룹을 지정하려면

1. 구성하고 있는 파트너에 대한 "사용자" 설정으로 이동합니다.

   "사용자 디렉터리" 페이지가 열리면서 정책 도메인의 각 사용자 디렉터리에 대한 항목이 표시됩니다.

2. 사용자 디렉터리의 사용자 또는 그룹을 정책에 추가합니다.

   각 사용자 디렉터리 테이블에서 "구성원 추가", "항목 추가", "모두 추가"를 선택할 수 있습니다. 선택하는 방법에 따라 사용자를 추가할 수 있는 대화 상자가 열립니다.

   - "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.
   - "항목 추가"를 선택하는 경우 "User Directory Search Express Edit"(사용자 디렉터리 검색 빠른 편집) 대화 상자에서 수동 입력 (페이지 138)을 통해 사용자를 선택합니다.

   오른쪽 화살표(>)를 클릭하여 사용자 또는 그룹을 편집하거나 빼기 기호(-)를 클릭하여 사용자 또는 그룹을 삭제합니다.

3. 아무 방법이나 사용하여 개별 사용자, 사용자 그룹 또는 둘 다를 선택하고 "확인"을 클릭합니다.

   "사용자 디렉터리" 페이지가 다시 열리면서 새 사용자가 사용자 디렉터리 테이블에 나열됩니다.

추가 정보:

리소스에 액세스하지 못하도록 사용자 또는 그룹 제외 (페이지 137)
리소스에 대한 중첩된 그룹 액세스 허용 (페이지 138)
수동 입력으로 사용자 추가 (페이지 138)

리소스에 액세스하지 못하도록 사용자 또는 그룹 제외

어설션을 획득하지 못하도록 사용자 또는 사용자 그룹을 제외할 수 있습니다.

다음 단계를 수행하십시오.

1. "사용자" 설정으로 이동합니다.
2. 특정 사용자 디렉터리에 대한 목록에서 사용자 또는 그룹을 선택합니다.
3. "제외"를 클릭하여 선택한 사용자 또는 그룹을 제외합니다.

   선택 사항이 관리 UI 에 반영됩니다.
4. "확인"을 클릭하여 변경 내용을 저장합니다.

리소스에 대한 중첩된 그룹 액세스 허용

LDAP 사용자 디렉터리에는 하위 그룹이 있는 그룹이 포함될 수 있습니다. 복합 디렉터리에서는 다른 그룹의 계층 구조에 중첩된 그룹을 사용하여 많은 양의 사용자 정보를 구성할 수 있습니다.

중첩된 그룹에 있는 사용자를 검색하도록 설정하는 경우 요청된 사용자 레코드가 모든 중첩된 그룹에서 검색됩니다. 중첩된 그룹이 사용되도록 설정하지 않은 경우에는 지정하는 그룹만 검색됩니다.

중첩된 그룹에서 검색하도록 설정하려면

1. "사용자" 설정으로 이동합니다.

   연결된 가맹 도메인에 여러 사용자 디렉터리가 포함된 경우 각 사용자 디렉터리가 자체 섹션에 나타납니다.
2. "중첩된 그룹 허용" 확인란을 선택하여 중첩된 그룹에서 검색하도록 설정합니다.

수동 입력으로 사용자 추가

어설션 생성을 위해 사용자를 지정할 때 선택할 수 있는 옵션 중 하나는 수동 입력으로 사용자를 식별하는 것입니다.

다음 단계를 수행하십시오.

1. 구성하고 있는 파트너에 대한 "사용자" 설정으로 이동합니다.

   가맹 도메인에 여러 사용자 디렉터리가 포함된 경우 모든 디렉터리가 "사용자 디렉터리" 페이지에 나타납니다.

2. "항목 추가"를 클릭합니다.

   "User Directory Search Express Edit"(사용자 디렉터리 검색 빠른 편집) 페이지가 표시됩니다.

3. 검색 옵션을 선택하고 해당 검색 옵션에 대한 필드에 데이터를 입력합니다.

   검색 위치

   LDAP 디렉터리의 경우 드롭다운 목록에서 옵션을 선택합니다.

   DN 유효성 검사

   LDAP 검색이 디렉터리에서 이 DN 을 찾습니다.

   사용자 검색

   LDAP 검색이 일치하는 사용자 항목으로 제한됩니다.

   그룹 검색

   LDAP 검색이 일치하는 그룹 항목으로 제한됩니다.

   조직 검색

   LDAP 검색이 일치하는 조직 항목으로 제한됩니다.

   모든 항목 검색

   LDAP 검색이 일치하는 사용자, 그룹 및 조직 항목으로 제한됩니다.

   - Microsoft SQL Server, Oracle 및 WinNT 디렉터리의 경우 "수동 입력" 필드에 사용자 이름을 입력할 수 있습니다.
   - Microsoft SQL Server 또는 Oracle 의 경우 SQL 쿼리를 대신 입력할 수 있습니다. 예를 들면 다음과 같습니다.

     SELECT NAME FROM EMPLOYEE WHERE JOB ='MGR';

     정책 서버는 사용자 디렉터리에 대한 "연결 자격 증명" 탭의 "사용자 이름" 필드에 지정된 데이터베이스 사용자로 쿼리를 수행합니다. "수동 입력" 필드에 대한 SQL 문을 작성하는 경우 사용자 디렉터리에 대한 데이터베이스 스키마를 숙지해야 합니다. 예를 들어 SmSampleUsers 스키마를 사용하고 있는 경우 특정 사용자를 추가하려면 SmUser 테이블에서 사용자 항목을 선택합니다.
   - LDAP 디렉터리의 경우 모든 디렉터리 항목을 추가하려면 "수동 입력" 필드에 **all** 을 입력합니다.

4. "확인"을 클릭하여 변경 내용을 저장합니다.

SAML 2.0 어설션에 대한 이름 ID 지정

이름 ID 는 어설션에서 고유한 방법으로 사용자를 명명합니다. 이름 ID 는 서비스 공급자에게 전송되는 어설션에 추가됩니다.

이름 ID 형식에 따라 ID 에 사용되는 콘텐츠 유형이 설정됩니다. 예를 들어 형식이 "사용자 DN"인 경우 콘텐츠는 uid 입니다.

이름 ID 를 암호화할 수 있습니다. 하지만 아티팩트 바인딩을 사용하는 싱글 사인온의 경우 어설션의 다른 데이터와 함께 이름 ID 를 암호화하면 어설션 크기가 증가합니다.

참고: 이름 ID 는 어설션의 필수 사항입니다.

이름 ID 를 구성하려면

1. 구성 마법사의 "이름 ID" 단계에서 시작합니다.
2. 이름 ID 형식을 선택합니다.

   각 형식에 대한 설명은 *OASIS SAML(Security Assertion Markup Language) V2.0* 사양을 참조하십시오.
3. 다음 옵션 중에서 이름 ID 유형을 선택합니다.
   - 정적 값
   - 사용자 특성
   - DN 특성(중첩된 그룹 포함 또는 제외)

   선택한 이름 ID 유형에 따라 "이름 ID 필드" 섹션의 내용이 변경됩니다.
4. 필드에 선택한 이름 ID 유형에 대한 데이터를 입력합니다.

참고: 이름 ID 를 구성하는 경우 "SAML 가맹" 필드에서 가맹을 선택하지 마십시오. 이름 ID 와 가맹은 동시에 사용할 수 없습니다.

추가 정보:

NameID 및 어설션 암호화 (페이지 260)

SAML 어설션 응답 사용자 지정(선택 사항)

어설션 생성기 플러그인을 사용하여 어설션 콘텐츠를 수정할 수 있습니다. 플러그인을 통해 사용자와 파트너 및 공급업체 간의 비즈니스 계약을 사용하는 어설션 콘텐츠를 사용자 지정할 수 있습니다. 플러그인은 각 파트너에 대해 하나씩 허용됩니다.

어설션 생성기 플러그인을 구성하는 단계는 다음과 같습니다.

1. 아직 설치하지 않은 경우 SiteMinder SDK 를 설치합니다.
2. SDK 의 일부인 AssertionGeneratorPlugin.java 인터페이스를 구현합니다.
3. 어설션 생성기 플러그인 구현 클래스를 배포합니다.
4. 관리 UI 에서 어설션 생성기 플러그인 매개 변수가 사용되도록 설정합니다.

어설션 생성기 플러그인에 대한 추가 정보는 다음과 같이 찾을 수 있습니다.

- 참조 정보(메서드 서명, 매개 변수, 반환 값, 데이터 형식)와 UserContext 클래스에 대한 새 생성자는 *Javadoc 참조서*에서 확인할 수 있습니다. Javadoc 의 AssertionGeneratorPlugin 인터페이스를 참조하십시오.
- 인증 및 권한 부여 API 에 대한 개요와 개념 정보는 *SiteMinder Programming Guide for Java*(SiteMinder Java 프로그래밍 안내서)에 있습니다.

AssertionGeneratorPlugin 인터페이스 구현

사용자 지정 어설션 생성기 플러그인을 생성할 때의 첫 번째 단계는 AssertionGeneratorPlugin 인터페이스를 구현하는 것입니다.

다음 단계를 수행하십시오.

1. 매개 변수가 포함되지 않은 공개 기본 생성자 메서드를 제공합니다.
2. 상태 비저장 구현이 되도록 코드를 제공합니다. 여러 스레드가 단일 플러그인 클래스를 사용할 수 있어야 합니다.

3. 인터페이스에서 요구 사항을 충족할 메서드를 구현합니다.

   구현에 customizeAssertion 메서드 호출이 포함되어야 합니다. 기존 구현을 덮어쓸 수 있습니다. 이에 대한 예는 다음 샘플 클래스를 참조하십시오.

   SAML 1.x/WS-페더레이션

   AssertionSample.java

   SAML 2.0

   SAML2AssertionSample.java

   샘플 클래스는 /sdk/samples/assertiongeneratorplugin 디렉터리에 있습니다.

   구현이 customizeAssertion 메서드에 전달하는 매개 변수 문자열의 내용은 사용자 지정 개체의 책임입니다.

어설션 생성기 플러그인 배포

AssertionGeneratorPlugin 인터페이스에 대한 구현 클래스를 코드화했으면 해당 구현 클래스를 컴파일하고 SiteMinder 가 실행 파일을 찾을 수 있는지 확인하십시오.

어설션 생성기 플러그인을 배포하려면

1. 어설션 플러그인 Java 파일을 컴파일합니다.

   컴파일하려면 정책 서버와 함께 설치되는 다음 .jar 파일이 필요합니다.

   - *policy_server_home*/bin/jars/SmJavaApi.jar
   - *policy_server_home*/bin/thirdparty/xercesImpl.jar
   - *policy_server_home*/bin/endorsed/xalan.jar

2. JVMOptions.txt 파일에서 플러그인의 클래스 경로를 포함하도록 -Djava.class.path 값을 수정합니다. 이렇게 수정하면 수정된 클래스 경로를 사용하여 플러그인을 로드할 수 있습니다. *installation_home*\siteminder\config 디렉터리에서 JVMOptions.txt 파일을 찾습니다.

   참고: xercesImpl.jar, xalan.jar 또는 SMJavaApi.jar 의 클래스 경로를 수정하지 마십시오.

3. 플러그인이 사용되도록 설정합니다.

어설션 생성기 플러그인이 사용되도록 설정

어설션 생성기 플러그인을 작성하고 컴파일한 후 관리 UI 에서 설정을 구성하여 플러그인이 사용되도록 설정하십시오. UI 매개 변수는 SiteMinder 에게 플러그인을 찾을 수 있는 위치를 알려 줍니다.

플러그인을 배포 (페이지 159)할 때까지 플러그인 설정을 구성하지 마십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그온합니다.
2. "페더레이션", "레거시 페더레이션", "SAML 서비스 공급자"를 차례로 클릭합니다.
3. 기존 서비스 공급자 항목을 선택하거나 새로 생성합니다.
4. "일반" 설정으로 이동합니다.
5. "어설션 생성기 플러그인" 섹션의 다음 필드에 데이터를 입력합니다.

   Java 클래스 이름

   기존 플러그인에 대한 Java 클래스 이름을 지정합니다.

   플러그인 클래스는 어설션을 구문 분석하고 수정한 다음 최종 처리를 위해 결과를 어설션 생성기에게 반환할 수 있습니다.

   플러그인은 각 서비스 공급자에 대해 하나씩만 허용됩니다. 예를 들면 com.mycompany.assertiongenerator.AssertionSample 입니다.

   매개 변수

   (선택 사항) "Java 클래스 이름" 필드에서 지정한 플러그인에 전달되는 매개 변수 문자열을 지정합니다.

   참고: 관리 UI 를 통해 어설션 플러그인이 사용되도록 설정하는 대신 정책 관리 API(C 또는 Perl)를 사용하여 플러그인을 통합할 수 있습니다. 자세한 내용은 *SiteMinder Programming Guide for C*(SiteMinder C 프로그래밍 안내서) 또는 *SiteMinder Programming Guide for Java*(SiteMinder Java 프로그래밍 안내서)를 참조하십시오.
6. 정책 서버를 다시 시작합니다.

   정책 서버를 다시 시작하면 최신 버전의 어설션 플러그인이 다시 컴파일된 후 선택됩니다.

웹 응용 프로그램 특성으로 어설션 사용자 지정

어설션 생성기 플러그인을 사용하여 어설션에 웹 응용 프로그램 특성을 추가할 수 있습니다. 이것은 어설션을 사용자 지정하는 또 다른 방법입니다.

어설션에 웹 응용 프로그램 특성을 포함하려면

1. 어설션 플러그인 Java 파일을 컴파일합니다.

   컴파일하려면 정책 서버와 함께 설치되는 다음 .jar 파일이 필요합니다.

   - *policy_server_home*/bin/jars/SmJavaApi.jar
   - *policy_server_home*/bin/thirdparty/xercesImpl.jar
   - *policy_server_home*/bin/endorsed/xalan.jar

2. JVMOptions.txt 파일에서 플러그인의 클래스 경로를 포함하도록 -Djava.class.path 값을 수정합니다. 이렇게 수정하면 수정된 클래스 경로를 사용하여 플러그인을 로드할 수 있습니다. *installation_home*\siteminder\config 디렉터리에서 JVMOptions.txt 파일을 찾습니다.

   참고: xercesImpl.jar, xalan.jar 또는 SMJavaApi.jar 의 클래스 경로를 수정하지 마십시오.

3. 샘플 플러그인을 구성합니다.

   SMJavaAPI 의 APIContext 클래스에는 어설션에 포함된 웹 응용 프로그램의 특성을 포함하는 맵 개체를 반환하는 새 메서드인 getAttrMap()이 있습니다. SiteMinder SDK 에는 이 맵 개체를 사용하는 방법을 보여 주는 샘플 어설션 생성기 플러그인 두 개가 있습니다.

   - SAML2AppAttrPlugin.java(SAML 2.0)
   - WSFedAppAttrPlugin.java(WS-페더레이션)

   이러한 샘플은 sdk/samples/assertiongeneratorplugin 디렉터리에 있습니다. 이러한 샘플을 통해 어설션 생성기가 어설션에 웹 응용 프로그램 특성을 추가할 수 있습니다.

4. 관리 UI 에 로그인합니다.
5. "페더레이션", "레거시 페더레이션", "SAML 서비스 공급자" 또는 "리소스 파트너"를 차례로 선택합니다.
6. 기존 항목을 선택하거나 새로 생성합니다.
7. "일반" 설정으로 이동합니다.

8. "어설션 생성기 플러그인" 섹션의 다음 필드에 데이터를 입력합니다.

   Java 클래스 이름

   플러그인에 대한 Java 클래스의 이름을 지정합니다. 예를 들어 SiteMinder SDK 에 포함된 샘플 클래스는 다음과 같습니다.

   - com.ca.assertiongenerator.SAML2AppAttrPlugin

     (SAML 2.0)

   - com.ca.assertiongenerator.WSFedAppAttrPlugin

     (WS-페더레이션)

   매개 변수

   "Java 클래스 이름" 필드에서 지정한 플러그인에 전달되는 매개 변수 문자열을 지정합니다. 이러한 매개 변수는 어설션에 포함할 특성입니다.

   참고: 관리 UI 를 통해 설정을 구성하는 대신 정책 관리 API(C 또는 Perl)를 사용하여 플러그인을 통합할 수 있습니다. 지침은 *SiteMinder Programming Guide for C*(SiteMinder C 프로그래밍 안내서) 또는 *SiteMinder Programming Guide for Java*(SiteMinder Java 프로그래밍 안내서)를 참조하십시오.

9. 정책 서버를 다시 시작합니다.

   정책 서버를 다시 시작하면 최신 버전의 어설션 플러그인이 다시 컴파일된 후 선택됩니다.

SAML 2.0 에 대한 싱글 사인온 구성

싱글 사인온 구성에는 아이덴티티 공급자가 어설션을 서비스 공급자에게 전달하는 방법을 결정하는 작업이 포함됩니다.

다음 단계를 수행하십시오.

1. 관리 UI 에서 서비스 공급자 개체에 대한 "SAML 프로필" 설정으로 이동합니다.

2. 페이지의 "SSO" 섹션에 있는 필드에 데이터를 입력합니다. 통신에 사용할 SAML 바인딩을 선택합니다.

   HTTP-아티팩트 바인딩의 경우 사용자가 보호된 아티팩트 레졸루션 서비스에 액세스할 수 있도록 백 채널 설정을 구성합니다. 백 채널 설정은 구성 마법사의 "특성" 단계에 있습니다.

3. "제출"을 클릭하여 변경 내용을 저장합니다.

추가 정보:

아티팩트 서비스를 보호하는 인증 체계 구성 (페이지 147)

싱글 사인온에 대한 어설션 유효 기간

싱글 사인온의 경우 차이 시간 및 유효 기간 값에 따라 SiteMinder 가 어설션의 총 유효 기간을 계산하는 방법이 결정됩니다. SiteMinder 는 어설션의 생성 및 소비에 차이 시간을 적용합니다.

참고: 이 설명에서 어설션 당사자는 SAML 1.x 생산자, SAML 2.0 아이덴티티 공급자 또는 WS-페더레이션 계정 파트너입니다. 신뢰 당사자는 SAML 1.x 소비자, SAML 2.0 서비스 공급자 또는 WS-페더레이션 리소스 파트너입니다.

어설션 문서에서 NotBefore 및 NotOnOrAfter 값은 유효 간격의 시작 및 끝을 나타냅니다.

어설션 당사자 측에서 SiteMinder 는 어설션 유효 기간을 설정합니다. 유효 간격은 어설션이 생성되는 시스템 시간입니다. SiteMinder 는 이 시간을 사용하여 어설션의 IssueInstant 값을 설정한 다음 IssueInstant 값에서 차이 시간 값을 뺍니다. 그 결과로 얻은 시간이 NotBefore 값입니다.

NotBefore = IssueInstant - 차이 시간

유효 간격의 끝을 결정하기 위해 SiteMinder 는 유효 기간 값과 차이 시간을 IssueInstant 값에 더합니다. 그 결과로 얻은 시간은 NotOnOrAfter 값이 됩니다.

NotOnOrAfter = 유효 기간 + 차이 시간 + IssueInstant

시간은 GMT 를 기준으로 합니다.

예를 들어 어설션 당사자 측에서 어설션이 1:00 GMT 에 생성된다고 가정합니다. 차이 시간은 30 초이고 유효 기간은 60 초이며 어설션 유효 간격은 12:59:30 GMT 에서 1:01:30 GMT 사이입니다. 이 간격은 어설션이 생성된 시간보다 30 초 전에 시작되고 90 초 후에 끝납니다.

신뢰 당사자 측에서 SiteMinder 는 어설션 당사자 측에서와 동일한 계산을 수행하여 수신된 어설션이 유효한지 확인합니다.

SiteMinder 가 파트너 관계의 양쪽 모두에 있는 경우의 어설션 유효 기간 계산

SiteMinder 가 파트너 관계의 양쪽 모두에 있는 경우 어설션 유효 기간은 유효 기간을 차이 시간의 두 배에 더한 합계입니다. 공식은 다음과 같습니다.

어설션 유효 기간 = 2 x 차이 시간(어설션 당사자) + 유효 기간 + 2 x 차이 시간(신뢰 당사자)

공식의 초기 부분(2 x 차이 시간 + 유효 기간)은 어설션 당사자의 유효 기간 시작 및 끝을 나타냅니다. 공식의 두 번째 부분(2 x 차이 시간)은 신뢰 당사자에 있는 시스템 클록의 차이 시간을 나타냅니다. 2 를 곱하는 이유는 유효 기간의 NotBefore 및 NotOnOrAfter 끝을 고려하기 때문입니다.

참고: 레거시 페더레이션의 경우 유효 기간은 어설션 당사자 측에서만 설정됩니다.

예

어설션 당사자

어설션 당사자 측에서의 값은 다음과 같습니다.

- IssueInstant = 5:00PM
- 유효 기간 = 60 초
- 차이 시간 = 60 초
- NotBefore = 4:59PM
- NotOnOrAfter = 5:02PM

신뢰 당사자

신뢰 당사자는 어설션의 NotBefore 및 NotOnOrAfter 값을 사용하고 해당 차이 시간을 이러한 값에 적용합니다. 이 공식은 신뢰 당사자가 새 NotBefore 및 NotOnOrAfter 값을 계산하는 방법입니다.

- 차이 시간 = 180 초(3 분)
- NotBefore = 4:56PM
- NotOnOrAfter = 5:05PM

어설션 유효 기간 창

이 예제의 값을 사용한 전체 어설션 유효 기간 창의 계산은 다음과 같습니다.

120 초(2 x 60) + 60 초 + 360 초(2 x 180) = 540 초(9 분)

다른 싱글 사인온 바인딩에 대해 인덱싱된 끝점 정의

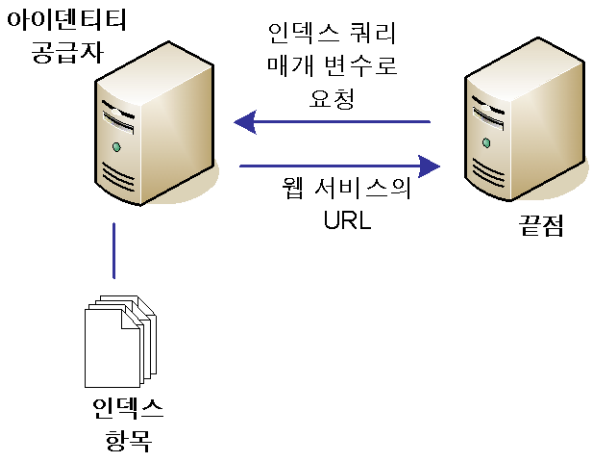
페더레이션 통신에 대해 인덱싱된 끝점을 구성할 수 있습니다. 인덱싱된 끝점은 어설션이 소비되는 사이트입니다. SiteMinder 의 컨텍스트에서 이 끝점은 어설션 소비자 서비스가 있는 서비스 공급자입니다.

구성하는 끝점 각각에는 어설션 소비자 서비스 URL 에 대한 단일 명시적 참조 대신 고유 인덱스 값이 할당됩니다. 할당된 인덱스는 서비스 공급자가 아이덴티티 공급자에게 보내는 어설션 요청에 추가됩니다.

인덱싱된 끝점을 지원하는 타사 아이덴티티 공급자와의 페더레이션된 관계가 있는 SiteMinder 서비스 공급자에 대해 인덱싱된 끝점을 구성할 수 있습니다. 여러 끝점을 서비스에 할당하여 어설션 소비자 서비스에 대해 다양한 프로토콜 바인딩(아티팩트, POST)을 구성할 수도 있습니다.

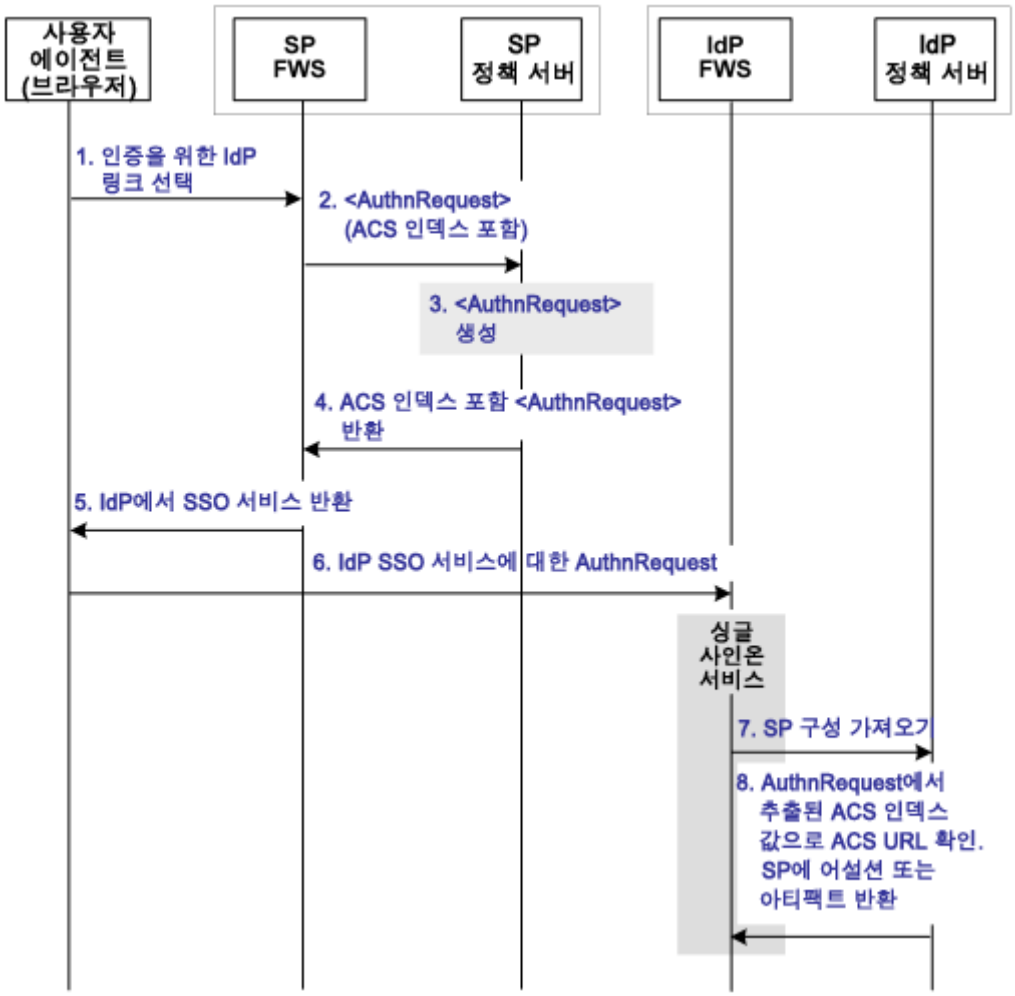
참고: 사용 중인 네트워크에 다양한 SiteMinder 버전이 포함된 경우 인덱싱된 끝점을 구성할 수 없습니다. 예를 들어 서비스 공급자는 r12.0 SP 2 이고 아이덴티티 공급자는 r12.0 SP3 인 경우 인덱싱된 끝점을 구성할 수 없습니다. 두 HTTP 바인딩 모두에 대해 어설션 소비자 서비스를 하나만 구성하십시오.

다음 그림에서는 인덱싱된 끝점의 이점을 활용하는 네트워크를 보여 줍니다.



인덱싱된 끝점 순서도

다음 그림에서는 인덱싱된 끝점을 사용하여 싱글 사인온이 작동하는 방식을 보여 줍니다.



참고: 웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이가 FWS 기능을 제공할 수 있습니다.

인덱싱된 끝점을 사용하는 경우 이벤트 순서는 다음과 같습니다.

1. 사용자가 특정 IdP 의 인증을 받기 위해 링크를 선택합니다. 인덱스 기능이 사용되도록 설정되어 있으므로 링크에는 IdP ID 및 AssertionConsumerServiceIndex 쿼리 매개 변수 인덱스가 쿼리 매개 변수로 포함됩니다.

2. SP FWS(페더레이션 웹 서비스) 응용 프로그램이 해당 로컬 정책 서버에서 AuthnRequest 를 요청합니다. 이 응용 프로그램이 보내는 요청에는 IdP ID 와 선택적으로 AssertionConsumerServiceIndex 및 ForceAuthn 쿼리 매개 변수가 포함됩니다.

   ACS 인덱스 및 프로토콜 바인딩 매개 변수는 동시에 사용할 수 없으므로 프로토콜 바인딩이 요청에 포함되지 않습니다. AssertionConsumerServiceIndex 가 바인딩과 이미 연결되어 있으므로 프로토콜 바인딩 값을 지정할 필요가 없습니다. 프로토콜 바인딩과 AssertionConsumerServiceIndex 가 쿼리 매개 변수로 전달되면 로컬 정책 서버가 요청을 거부하는 오류로 응답합니다.

3. AuthnRequest 서비스가 SP 정책 서버에서 IdP 정보를 추출하고 AssertionConsumerServiceIndex 가 포함된 AuthnRequest 메시지를 생성합니다. AssertionConsumerServiceIndex 가 쿼리 매개 변수 중 하나이므로 해당 값이 IdP 설명자 문서의 IdP 와 비교하여 확인됩니다. 이 문서는 이전에 IdP 에서 SP 로 전송됩니다.

   AuthnRequest 서비스는 다음과 같이 반응합니다.

   - 아티팩트 바인딩에 대한 인덱스가 IdP 메타데이터에 설정된 경우 이 인덱스가 AssertionConsumerServiceIndex 값과 비교됩니다. 값이 일치하는 경우 인덱스 값이 AuthnRequest 의 일부로 유지됩니다. 인덱스 값이 일치하지 않는 경우에는 IdP 메타데이터가 확인됩니다. AssertionConsumerServiceIndex 는 POST 바인딩에 해당해야 합니다.
   - 인덱스가 HTTP-POST 바인딩에 해당하는 경우 이 인덱스 값이 AuthnRequest 의 AssertionConsumerServiceIndex 와 다시 비교됩니다. AssertionConsumerServiceIndex 매개 변수의 값이 POST 바인딩과 일치하지 않는 경우에는 AuthnRequest 서비스가 오류를 생성합니다. 오류에서는 AssertionConsumerServiceIndex 가 IdP 메타데이터의 인덱스와 일치하지 않음을 나타냅니다.

4. IdP 메타데이터 인덱스 및 AssertionConsumerServiceIndex 값이 일치한다고 가정하여 SP 정책 서버가 AuthnRequest 를 생성합니다.

5. SP 정책 서버가 HTTP-리디렉션 바인딩에서 AuthnRequest 를 반환합니다.

6. SP FWS 응용 프로그램이 AuthnRequest 를 IdP 의 싱글 사인온 서비스로 리디렉션합니다. URL 이 AuthnRequest 에 있는 구성 정보의 일부이므로 SP 는 싱글 사인온 서비스의 URL 을 알고 있습니다.
7. 브라우저가 싱글 사인온 서비스를 요청합니다.
8. 싱글 사인온 서비스가 AuthnRequest 에서 AssertionConsumerServiceIndex 값을 추출합니다. 서비스는 AssertionConsumerServiceIndex 를 사용하여 어설션 소비자 서비스 URL 을 확인합니다. 인덱스가 메타데이터에 없으면 서비스가 오류를 생성합니다. 오류 메시지에서는 잘못된 AssertionConsumerServiceIndex 가 AuthnRequest 메시지에 있음을 나타냅니다.

   어설션이나 아티팩트를 SP 에 보내는 어설션 소비자 URL 은 사용 중인 싱글 사인온 프로필에 따라 다릅니다.

   참고: AssertionConsumerServiceIndex 매개 변수가 AuthnRequest 에 없으면 어설션 소비자 서비스의 값과 해당 바인딩이 기본적으로 사용됩니다.

어설션 소비자 서비스에 대해 인덱싱된 끝점 구성

싱글 사인온 서비스는 AuthnRequest 에서 ACS 인덱스 값을 추출합니다. 서비스가 인덱스 값을 인덱스 항목 목록과 비교하고 해당 인덱스 값과 연결된 어설션 소비자 서비스 URL 을 확인합니다. 그런 다음 싱글 사인온 서비스가 인덱스 값과 연결된 바인딩에 따라 어설션이나 아티팩트를 보낼 위치를 알게 됩니다.

아이덴티티 공급자에서 인덱스 항목을 구성하려면

1. 관리 UI 에 로그인합니다.
2. 수정할 서비스 공급자 항목을 선택하거나 새로 생성합니다.
3. "SAML 프로필" 페이지로 이동합니다.
4. 페이지의 "SSO" 섹션에서 "어설션 소비자 서비스" 필드 끝의 줄임표 단추를 클릭합니다.

   "어설션 소비자 서비스" 페이지가 열립니다.
5. "추가"를 클릭합니다.

   "어설션 소비자 서비스 추가" 페이지가 열립니다.

6. 페이지의 필드에 데이터를 입력합니다.

   동일한 어설션 소비자 서비스 URL 에 다양한 인덱스 값을 할당할 수 있습니다.

7. "확인"을 클릭하여 변경 내용을 저장합니다.

참고: 서비스 공급자의 SAML 2.0 인증 체계에서 인덱스 항목을 구성해야 합니다.

SSO 에 대한 인증 체계 보호 수준 적용

사용자가 페더레이션된 리소스를 요청하는 경우 사용자에게 SiteMinder 세션이 있어야 합니다. 세션이 없으면 세션을 설정하기 위해 사용자가 인증 URL 로 리디렉션됩니다. 인증 URL 을 보호하는 인증 체계는 특정 보호 수준으로 구성됩니다. 이 보호 수준은 SAML 서비스 공급자 구성에 대해 구성하는 인증 수준보다 크거나 같아야 합니다.

인증 URL 에 대한 보호 수준이 관리 UI 에 설정된 인증 수준보다 낮으면 정책 서버가 어설션을 생성하지 않습니다.

디지털 서명 옵션 결정

페더레이션은 개인 키/인증서 쌍을 사용하여 페더레이션 통신의 다양한 디지털 서명 태스크를 수행할 수 있습니다. 개인 키/인증서 쌍으로 서명할 수 있는 메시지는 다음과 같습니다.

- 어설션
- SAML 응답
- 아티팩트 응답
- 싱글 로그아웃 요청 및 응답

  싱글 로그아웃의 경우 로그아웃을 시작하는 측에서 요청에 서명합니다. 요청을 수신하는 측에서 서명의 유효성을 검사합니다. 반대로 수신하는 측에서 SLO 응답에 서명하고 시작하는 측에서 응답 서명의 유효성을 검사해야 합니다.

- 특성 응답(사용자 특성에 기반한 권한 부여의 경우)

서명을 담당하는 파트너는 서명을 확인하는 파트너에게 개인 키와 연결된 인증서(공개 키)를 제공합니다. 이 교환은 트랜잭션이 발생하기 전에 독립된 통신으로 수행됩니다.

IdP 가 어설션을 SP 에 보내는 경우 기본적으로 인증서가 어설션에 포함되어 있습니다. 하지만 SP 는 자신의 사이트에 저장하는 인증서를 사용하여 서명을 확인합니다.

디지털 서명에 대한 구성 옵션은 다음과 같습니다.

- 서명 별칭
- 서명 알고리즘(RSAwithSHA1 또는 RSAwithSHA256)
- HTTP-아티팩트 어설션, SAML 응답 및 아티팩트 응답 옵션
- HTTP-POST 어설션 및 SAML 응답 옵션

"일반" 또는 "SSO" 탭에서 서명 옵션을 지정하려면

1. 기존 SAML 서비스 공급자 개체를 수정하거나 새로 생성합니다.
2. "SAML 프로필"로 이동합니다.
3. 대화 상자의 "서명 옵션" 섹션에 있는 필드에 데이터를 입력합니다.
4. 제출을 클릭합니다.

ECP(향상된 클라이언트 또는 프록시) 프로필 개요

ECP(향상된 클라이언트 또는 프록시) 프로필은 싱글 사인온을 위한 응용 프로그램입니다. 향상된 클라이언트는 ECP 기능을 지원하는 브라우저 또는 일부 다른 사용자 에이전트입니다. 향상된 프록시는 무선 장치용 무선 액세스 프로토콜 프록시와 같은 HTTP 프록시입니다.

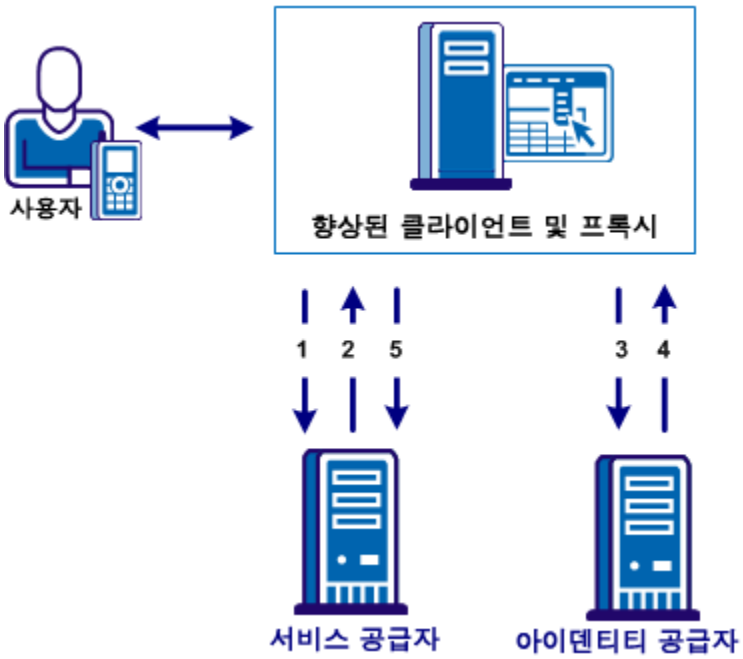
ECP 프로필은 아이덴티티 공급자와 서비스 공급자가 직접 통신할 수 없을 때 싱글 사인온을 가능하게 합니다. ECP 는 서비스 공급자와 아이덴티티 공급자 사이에서 중재자 역할을 합니다.

중재자 역할을 하는 것 외에도 ECP 프로필은 다음과 같은 경우에 유용합니다.

- 이 프로필이 필요한 향상된 클라이언트 또는 프록시에 서비스를 제공할 것으로 예상되는 서비스 공급자의 경우
- 기능이 제한된 모바일 장치 앞의 WAP(무선 액세스 프로토콜) 게이트웨이와 같은 프록시 서버가 사용되고 있는 경우

ECP 응용 프로그램은 사용자가 직접 얻거나 개발해야 합니다. 정책 서버는 SAML 요구 사항에 맞는 ECP 응용 프로그램에 대한 ECP 요청 및 응답만 처리합니다.

다음 그림에서는 ECP 프로필의 흐름을 보여 줍니다.



ECP 통신에서 사용자는 휴대폰 등에서 응용 프로그램에 대한 액세스를 요청합니다. 응용 프로그램은 서비스 공급자에 있으며 사용자에 대한 아이덴티티 정보는 아이덴티티 공급자에 있습니다. 서비스 공급자와 아이덴티티 공급자는 직접 통신하지 않습니다.

ECP 호출의 흐름은 다음과 같습니다.

1. ECP 응용 프로그램이 리버스 SOAP(PAOS) 요청을 서비스 공급자에 전달합니다. 서비스 공급자는 아이덴티티 공급자에 직접 액세스할 수 없습니다.

   아이덴티티 공급자와 달리 ECP 엔터티에는 항상 직접 액세스할 수 있습니다.
2. 서비스 공급자는 ECP 응용 프로그램에 AuthnRequest 를 되보냅니다.
3. ECP 응용 프로그램은 AuthnRequest 를 처리 및 수정하여 아이덴티티 공급자에 보냅니다.

4. 아이덴티티 공급자는 요청을 처리한 후 ECP 응용 프로그램에 SOAP 응답을 반환합니다. 이 응답에는 어설션이 포함됩니다.
5. ECP 응용 프로그램은 서명된 PAOS 응답을 서비스 공급자에 되보냅니다.

싱글 사인온이 진행되고 사용자가 응용 프로그램에 대한 액세스 권한을 얻습니다.

아이덴티티 공급자에서 ECP 구성

ECP 를 구성하려면 아이덴티티 공급자와 서비스 공급자에서 해당 기능을 사용하도록 설정하십시오. 다음 절차는 SiteMinder 아이덴티티 공급자에 해당됩니다.

다음 단계를 수행하십시오.

1. 아이덴티티 공급자에서 관리 UI 에 로그인합니다.
2. 수정할 SAML 서비스 공급자에 대한 "SAML 프로필" 탭으로 이동합니다.
3. 대화 상자에서 필요한 싱글 사인온 구성 설정을 완료합니다.
4. SSO 섹션에서 "향상된 클라이언트 및 프록시 프로필" 확인란을 선택합니다.
5. "제출"을 클릭합니다.

이제 아이덴티티 공급자가 ECP 호출을 처리할 수 있습니다.

페더레이션된 파트너도 ECP 를 사용하도록 설정해야 합니다. SiteMinder 의 경우 SAML 2.0 인증 체계에서 ECP 를 사용하도록 설정 (페이지 278)합니다.

참고: 단일 SAML 서비스 공급자 개체가 싱글 사인온 요청에 대한 아티팩트, POST, SOAP 및 PAOS 바인딩을 처리할 수 있습니다. SOAP 및 PAOS 는 ECP 프로필에 대한 바인딩입니다. 아이덴티티 공급자와 서비스 공급자는 요청의 매개 변수를 기준으로 사용되는 바인딩을 확인합니다.

"허용/만들기"가 사용되도록 설정하여 사용자 식별자 만들기

SAML 2.0 "허용/만들기" 기능을 통해 아이덴티티 공급자가 서비스 공급자 요청 시 사용자 식별자를 생성할 수 있습니다. 이 기능이 올바로 작동하려면 서비스 공급자 요청에 "허용/만들기" 특성이 포함되어 있어야 합니다. 또한 관리자가 식별자를 생성하도록 아이덴티티 공급자를 구성해야 합니다. 아이덴티티 공급자는 서비스 공급자에게 반환되는 어설션에 있는 NameID 의 일부가 되는 고유한 값을 생성합니다.

서비스 공급자가 어설션을 받으면 SAML 2.0 인증 체계가 응답을 처리합니다. 그런 다음 인증 체계가 해당 로컬 사용자 저장소에서 사용자를 조회합니다. 사용자 레코드가 있는 경우 사용자에게 액세스 권한이 부여됩니다.

새 사용자 식별자 만들기가 사용되도록 설정하려면

1. 관리 UI 에 로그인합니다.
2. "서비스 공급자" 개체에 대한 "SAML 프로필" 설정으로 이동합니다.
3. 페이지의 "SSO" 섹션에서 "새 식별자의 생성 허용" 선택합니다.
4. 제출을 클릭합니다.

SP 의 인증 컨텍스트 무시

사용자 인증 컨텍스트에 대한 정보 교환은 페더레이션된 파트너 관계 양쪽에 인증 프로세스에 대해 통신할 수 있는 방법을 제공합니다.

서비스 공급자가 아이덴티티 공급자에 대한 요청에서 인증 컨텍스트를 요청하는 경우 컨텍스트를 무시하도록 아이덴티티 공급자를 구성할 수 있습니다.

인증 컨텍스트를 무시하려면

1. 서비스 공급자 개체에 대한 "일반" 설정으로 이동합니다.
2. "고급 SSO 구성" 섹션에서 "요청된 AuthnContext 무시"를 선택합니다.
3. "제출"을 클릭합니다.

일회 사용하기 위한 어설션 구성

SAML 2.0 사양에 따라 정책 서버가 어설션의 일회 사용을 적용할 수 있습니다. 일회 사용하기 위한 어설션을 생성하여 신뢰 당사자에게 향후 트랜잭션 용도로 어설션을 보관하지 않음을 알립니다. 유효 기간이 지난 어설션을 재사용하면 오래된 아이덴티티 정보에 기반한 인증 결정이 내려집니다.

일회 사용하기 위한 어설션을 구성하려면

1. 서비스 공급자 개체에 대한 "일반" 설정으로 이동합니다.
2. "고급 SSO 구성" 섹션에서 "OneTimeUse 조건 설정"을 선택합니다.
3. 제출을 클릭합니다.

IdP 의 HTTP 오류 처리

다양한 이유로 아이덴티티 공급자에서 어설션 기반 싱글 사인온이 실패할 수 있습니다. HTTP 오류가 발생하면 추가 처리를 위해 사용자가 다른 응용 프로그램(URL)으로 리디렉션될 수 있습니다. 사용자 지정된 오류 페이지로의 리디렉션은 필요한 서비스 공급자 정보가 아이덴티티 공급자에게 있는 경우에만 발생할 수 있습니다. 정보를 사용할 수 없는 경우에는 HTTP 오류 코드가 브라우저에 반환될 뿐입니다. 리디렉션은 발생하지 않습니다.

HTTP 처리에 대한 리디렉션 URL 을 구성할 수 있지만 이는 필수 사항이 아닙니다.

오류 처리에 대한 선택적 리디렉션 URL 을 구성하려면

1. "일반" 설정으로 이동합니다.
2. "고급 SSO 구성" 섹션에서 사용되도록 설정할 URL 을 선택하고 URL 을 입력합니다. 다음 오류 중 하나 이상에 대한 URL 을 지정할 수 있습니다.
   - 서버 오류 URL 사용
   - 잘못된 요청 URL 사용
   - 권한 없는 액세스 URL 사용
3. "모드"의 경우 다음 옵션 중 하나를 선택합니다.
   - 302 데이터 없음
   - HTTP POST
4. 제출을 클릭합니다.

참고: 이러한 리디렉션 URL 은 추가 어설션 처리를 위해 SiteMinder 어설션 소비자 플러그인과 함께 사용될 수 있습니다. 어설션 요청이 실패하면 플러그인이 사용자를 지정한 리디렉션 URL 중 하나에 보낼 수 있습니다.

어설션의 세션 기간 사용자 지정

정책 서버 IdP 가 어설션을 보내는 경우 기본적으로 SessionNotOnOrAfter 매개 변수가 어설션의 인증 문에 포함됩니다. 타사 SP 가 SessionNotOnOrAfter 값을 사용하여 자체 시간 만료 값을 설정할 수 있습니다. 시간 만료 값은 사용자 세션이 무효화되어 IdP 에서 다시 인증하기 위해 사용자를 보내는 시기를 결정합니다.

중요! 정책 서버가 SP 로 작동하고 있는 경우 SessionNotOnOrAfter 값이 무시됩니다. 대신에 SP 는 대상 리소스를 보호하도록 구성된 SAML 인증 체계에 해당하는 영역 시간 만료를 기반으로 세션 시간 만료를 설정합니다.

SessionNotOnOrAfter 매개 변수는 어설션 유효 기간과 차이 시간을 결정하는 데 사용되는 NotOnOrAfter 매개 변수와 다릅니다.

SessionNotOnOrAfter 매개 변수를 사용자 지정하려면

1. UI 에 로그온합니다.
2. 수정할 서비스 공급자 항목을 선택합니다.
3. "고급" 탭으로 이동합니다.
4. 대화 상자의 "고급 SSO 구성" 섹션에서 "유효 기간 사용자 지정"을 선택합니다.

   "유효 기간 사용자 지정" 대화 상자가 표시됩니다.
5. "SP 세션 유효 기간"에 대한 값을 선택합니다. 입력하는 값은 어설션의 SessionNotOnOrAfter 매개 변수 값입니다.

   옵션은 다음과 같습니다.

   어설션 유효성 사용

   어설션 유효 기간에 기반하여 SessionNotOnOrAfter 값을 계산합니다.

   생략

   IdP 에게 SessionNotOnOrAfter 매개 변수를 어설션에 포함하지 않도록 지시합니다.

IDP 세션

IdP 세션 시간 만료에 기반한 SessionNotOnOrAfter 값을 계산합니다. 시간 만료는 인증 URL 에 대한 IdP 영역에서 구성됩니다. 이 옵션을 사용하면 IdP 및 SP 세션 시간 만료 값을 동기화할 수 있습니다.

사용자 지정

어설션의 SessionNotOnOrAfter 매개 변수에 대한 사용자 지정 값을 지정할 수 있습니다. 이 옵션을 선택하는 경우 "어설션 세션 기간 사용자 지정" 필드에 시간을 입력합니다.

6. "확인"을 클릭하여 변경 내용을 저장합니다.

어설션 검색 서비스에 대한 액세스 권한 부여(아티팩트 SSO)

HTTP-아티팩트 싱글 사인온의 경우 어설션을 얻기 위한 FWS 서비스를 보호하는 정책에 액세스할 수 있는 권한이 신뢰 당사자에게 필요합니다.

액세스 권한을 부여하려면

- 에이전트 그룹 FederationWebServicesAgentGroup 에 FWS 응용 프로그램을 보호하는 웹 에이전트를 추가하십시오.
- 특정 서비스에 액세스하도록 허용된 사용자로 신뢰 파트너를 추가하십시오 (페이지 145).

  지정된 정책에 사용자를 추가하는 것 외에는 다른 모든 정책 개체가 자동으로 설정됩니다.

페더레이션 에이전트 그룹에 웹 에이전트 추가

에이전트 그룹 FederationWebServicesAgentGroup 에 FWS 응용 프로그램을 보호하는 웹 에이전트를 추가하십시오.

- ServletExec 의 경우 이 에이전트는 웹 에이전트 옵션 팩이 설치된 웹 서버에 있습니다.
- WebLogic 이나 JBOSS 와 같은 응용 프로그램 서버의 경우 이 웹 에이전트는 응용 프로그램 서버 프록시가 설치된 위치에 설치됩니다. 웹 에이전트 옵션 팩은 다른 시스템에 있을 수 있습니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "인프라", "에이전트", "에이전트"를 차례로 클릭합니다.
3. "에이전트 만들기"를 클릭합니다.
4. 배포에 있는 웹 에이전트의 이름을 지정합니다. "제출"을 클릭합니다.
5. "인프라", "에이전트", "에이전트 그룹"을 차례로 클릭합니다.
6. "FederationWebServicesAgentGroup" 항목을 선택합니다.
7. "추가/제거"를 클릭합니다. 그러면 "에이전트 그룹 구성원" 대화 상자가 열립니다.
8. "사용 가능한 구성원" 목록에서 "선택한 구성원" 목록으로 웹 에이전트를 이동합니다.
9. "확인"을 클릭하여 "에이전트 그룹" 대화 상자로 돌아갑니다.
10. "제출", "닫기"를 차례로 클릭하여 기본 페이지로 돌아갑니다.

어설션을 획득하기 위한 FWS 정책에 신뢰 파트너 추가

싱글 사인온에 대해 HTTP-아티팩트 바인딩을 사용하고 있는 경우 파트너 관계의 신뢰 당사자에게 어설션 검색 서비스에 액세스할 수 있는 권한이 있어야 합니다. SiteMinder 는 정책으로 SAML 1.x 및 2.0 검색 서비스를 보호합니다.

정책 서버를 설치하면 FederationWebServicesDomain 이 기본적으로 설치됩니다. 이 도메인에는 SiteMinder 가 어설션을 검색하는 서비스에 대한 다음 정책이 포함되어 있습니다.

SAML 1.x

FederationWSAssertionRetrievalServicePolicy

SAML 2.0

SAML2FWSArtifactResolutionServicePolicy

참고: WS-페더레이션은 HTTP-아티팩트 프로필을 사용하지 않습니다. 따라서 이 절차는 리소스 공급자에게 적용되지 않습니다.

이러한 정책에 모든 관련 신뢰 파트너에 대한 액세스 권한을 부여하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에서 "정책", "도메인", "도메인 정책"으로 이동합니다.

   도메인 정책 목록이 표시됩니다.

2. SAML 프로필에 대한 정책을 선택합니다.

   SAML 1.x

   FederationWSAssertionRetrievalServicePolicy

   SAML 2.0

   SAML2FWSArtifactResolutionServicePolicy

   "도메인 정책" 페이지가 열립니다.

3. "수정"을 클릭하여 정책을 변경합니다.

4. "사용자" 탭을 선택합니다.

5. 적절한 사용자 디렉터리에 대한 대화 상자에서 "구성원 추가"를 클릭합니다.

   SAML 1.x

   FederationWSCustomUserStore

   SAML 2.0

   SAML2FederationCustomUserStore

   "사용자/그룹" 페이지가 열립니다.

   이전에 구성한 가맹 도메인이 "사용자/그룹" 대화 상자에 나열됩니다. 예를 들어 가맹 도메인의 이름이 fedpartners 인 경우 항목은 **affiliate:fedpartners** 입니다.

6. 서비스에 대한 액세스 권한이 필요한 파트너가 있는 가맹 도메인 옆의 확인란을 선택합니다. "확인"을 클릭합니다.

   "사용자 디렉터리" 목록으로 돌아갑니다.

7. "제출"을 클릭합니다.

   정책 목록으로 돌아갑니다.

아티팩트 서비스를 보호하는 인증 체계 구성

HTTP-아티팩트 프로필의 경우 어설션 검색 서비스(SAML 1.x)와 아티팩트 레졸루션 서비스(SAML 2.0)는 어설션 당사자 측에서 어설션을 검색합니다. 이러한 서비스가 신뢰 당사자에게 어설션 응답을 보내는 경우 해당 어설션 응답은 보안 백 채널을 통해 전송됩니다. 권한 없는 액세스로부터 이러한 서비스와 백 채널을 통한 통신을 보호하는 것이 좋습니다.

참고: WS-페더레이션은 HTTP-아티팩트 프로필을 지원하지 않습니다.

이러한 서비스를 보호하려면 어설션 당사자 측에서 서비스가 포함된 영역에 대한 인증 체계를 지정하십시오. 인증 체계는 신뢰 당사자의 소비 서비스가 백 채널을 통해 관련 서비스에 액세스하기 위해 제공해야 하는 자격 증명 유형을 지정합니다.

다음 인증 체계 중 하나를 선택할 수 있습니다.

- 기본 (페이지 148)
- SSL 을 통한 기본 인증 (페이지 149)
- X.509 클라이언트 인증서 (페이지 149)

기본 인증으로 어설션 검색 서비스 보호

HTTP-아티팩트 싱글 사인온의 경우 어설션 당사자가 보안 백 채널을 통해 어설션을 신뢰 당사자에게 보냅니다. 기본 인증의 경우 아티팩트를 확인하고 어설션을 검색하는 서비스에 액세스하기 위한 암호를 구성하십시오. 그러면 서비스가 백 채널을 통해 신뢰 당사자에게 어설션을 보냅니다.

SSL 이 사용되도록 설정한 상태로 기본 인증을 사용할 수 있지만 SSL 이 반드시 필요한 것은 아닙니다.

참고: 암호는 "기본 인증" 또는 "SSL 을 통한 기본 인증"을 백 채널을 통한 인증 방법으로 사용하는 경우에만 관련됩니다.

SAML 1.x 어설션 검색 서비스의 경우 다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. 생산자에 대한 "일반" 설정으로 이동합니다.
3. 다음 필드에 대한 값을 입력합니다.
   - 암호
   - 암호 확인
4. "제출"을 클릭하여 변경 내용을 저장합니다.

SAML 2.0 아티팩트 레졸루션 서비스의 경우 다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. 아이덴티티 공급자에 대한 "특성" 설정으로 이동합니다.
3. "백 채널" 섹션에서 다음 필드에 대한 값을 입력합니다.
   - 암호
   - 암호 확인
4. "제출"을 클릭하여 변경 내용을 저장합니다.

SSL 을 통한 기본 인증으로 어설션 검색 서비스 보호

SSL 을 통한 기본 인증 체계로 어설션 검색 서비스(SAML 1.x)나 아티팩트 레졸루션 서비스(SAML 2.0)를 보호할 수 있습니다. 어설션 당사자 측에서는 정책 서버를 설치할 때 서비스를 보호하기 위한 기본 정책 집합이 이미 구성되어 있습니다.

필요한 구성은 각 파트너에서 SSL 이 사용되도록 설정하는 것뿐입니다. 어설션 당사자 또는 신뢰 당사자 측에서 다른 구성은 필요하지 않습니다. 신뢰 당사자 측에서 인증서 데이터 저장소의 기본 루트 CA(인증 기관) 중 하나를 사용하여 SSL 연결을 설정할 수 있습니다. 기본 CA 대신 사용자 고유의 루트 CA 를 사용하려면 CA 인증서를 데이터 저장소로 가져오십시오.

SSL 을 통한 기본 인증 체계를 사용하는 경우 모든 끝점 URL 은 SSL 통신을 사용해야 합니다. 즉, URL 이 **https://**로 시작해야 합니다. 끝점 URL 은 서버에서 싱글 사인온, 싱글 로그아웃, 어설션 소비자 서비스, 아티팩트 레졸루션 서비스(SAML 2.0), 어설션 검색 서비스(SAML 1.x) 등의 다양한 SAML 서비스를 찾습니다.

클라이언트 인증서 인증으로 어설션 검색 서비스 보호

클라이언트 인증서 인증 체계로 어설션 검색 서비스(SAML 1.x)나 아티팩트 레졸루션 서비스(SAML 2.0)를 보호할 수 있습니다. 어설션 당사자가 클라이언트 인증서 인증을 요구하도록 구성된 경우 신뢰 당사자는 어설션 당사자에 역방향으로 연결하고 클라이언트 인증서를 제공하려고 합니다.

클라이언트 인증서 인증 체계를 사용하려면

1. 어설션 당사자 측에서 관련 서비스를 보호할 정책을 생성합니다. 이 정책은 클라이언트 인증서 인증 체계를 사용합니다.
2. 신뢰 당사자 측에서 백 채널 구성에 대해 클라이언트 인증서 인증이 사용되도록 설정합니다.
3. 파트너 관계 양쪽에서 SSL 이 사용되도록 설정합니다.

클라이언트 인증서 인증을 사용하는 경우에는 모든 끝점 URL 이 SSL 통신을 사용해야 합니다. 따라서 URL 이 **https://**로 시작해야 합니다. 끝점 URL 은 서버에서 싱글 사인온, 싱글 로그아웃, 어설션 소비자 서비스, 아티팩트 레졸루션 서비스(SAML 2.0), 어설션 검색 서비스(SAML 1.x) 등의 다양한 SAML 서비스를 찾습니다.

ServletExec 를 실행 중인 다음 웹 서버에는 클라이언트 인증서 인증을 사용할 수 없습니다.

- SiteMinder 생산자/아이덴티티 공급자의 IIS 웹 서버 - IIS 의 제한 때문
- SiteMinder 생산자/아이덴티티 공급자의 SunOne/Sun Java Server 웹 서버 - ServletExec 에 설명된 제한 때문

검색 서비스를 보호하기 위한 정책 만들기

어설션 당사자 측에서 어설션 당사자의 어설션 검색 서비스를 보호하기 위한 정책을 생성하십시오.

다음 단계를 수행하십시오.

1. 어설션을 요청하는 가맹 각각에 대해 별개의 항목을 사용자 디렉터리에 추가합니다. 사용자 디렉터리를 생성하거나 기존 디렉터리를 사용합니다.

   사용자 레코드에 관리 UI 에 있는 가맹 일반 설정의 "이름" 필드에 지정된 것과 동일한 값을 입력합니다. 예를 들어 가맹에 대한 "이름" 필드 값이 Company A 인 경우 사용자 디렉터리 항목은 다음과 같습니다.

   uid=CompanyA, ou=Development,o=CA

   정책 서버가 가맹 클라이언트 인증서의 주체 DN 값을 이 디렉터리 항목에 매핑합니다.

2. 구성된 사용자 디렉터리를 FederationWebServicesDomain 에 추가합니다.

3. 인증서 매핑 항목을 생성합니다.

   특성 이름을 가맹에 대한 사용자 디렉터리 항목에 매핑합니다. 특성은 가맹에 대한 인증서의 주체 DN 항목을 나타냅니다. 예를 들어 특성 이름으로 CN 을 선택하는 경우 이 값은 cn=CompanyA,ou=Development,o=partner 라는 가맹을 나타냅니다.

   매핑 설정을 위해 "인프라", "디렉터리", "인증서 매핑"으로 이동합니다.

4. X509 클라이언트 인증서 인증 체계를 구성합니다.

5. FederationWebServicesDomain 아래에 다음 항목이 포함된 영역을 생성합니다.

   이름

   any_name

   예: cert assertion retrieval

   에이전트

   FederationWebServicesAgentGroup

   리소스 필터

   /affwebservices/certassertionretriever(SAML 1.x)

   /affwebservices/saml2certartifactresolution(SAML 2.0)

   인증 체계

   이전 단계에서 생성한 클라이언트 인증서 인증 체계입니다.

6. cert assertion retrieval 영역 아래에 다음 정보가 포함된 규칙을 생성합니다.

   이름

   any_name

   예: cert assertion retrieval rule

   Resource

   *

   웹 에이전트 작업

   GET, POST, PUT

7. FederationWebServicesDomain 아래에 웹 에이전트 응답 헤더를 생성합니다.

   어설션 검색 서비스가 이 HTTP 헤더를 사용하여 가맹이 어설션을 검색하는 사이트인지 확인합니다.

   다음 값이 포함된 응답을 생성합니다.

   이름

   any_name

   특성

   WebAgent-HTTP-Header-Variable

   특성 종류

   사용자 특성

   변수 이름

   consumer_name

   특성 이름

   가맹 이름 값이 포함된 사용자 디렉터리 특성을 입력합니다.

   예: uid=CompanyA

   다음 항목을 기반으로 웹 에이전트가 HTTP_CONSUMER_NAME 이라는 응답을 반환합니다.

8. FederationWebServicesDomain 아래에 다음 값이 포함된 정책을 생성합니다.

   이름

   any_name

   사용자

   이 절차에서 이전에 생성한 사용자 디렉터리의 사용자를 추가합니다.

   규칙

   rule_created_earlier_in_this_procedure

   응답

   response_created_earlier_in_this_procedure

아티팩트 레졸루션 서비스를 보호하기 위한 정책이 완료되었습니다.

신뢰 당사자 측에서 관리자가 관련 어설션 서비스에 연결하는 백 채널을 통해 클라이언트 인증서 인증이 사용되도록 설정해야 합니다.

SAML 1.x: 어설션 검색 서비스에 대해 클라이언트 인증서 인증이 사용되도록 설정 (페이지 188)

SAML 2.0: 아티팩트 레졸루션 서비스에 대해 클라이언트 인증서 인증이 사용되도록 설정 (페이지 300)

백 채널 인증에 필요한 WebLogic 구성

아이덴티티 공급자에서 WebLogic 9.2.*x* 응용 프로그램 서버에 웹 에이전트 옵션 팩을 설치할 수 있습니다. 백 채널을 통한 기본 인증이 이 서버에서 올바로 작동하도록 하려면 WebLogic config.xml 파일을 수정하십시오.

응용 프로그램 도메인에 대한 WebLogic config.xml 파일에서 다음과 같이 <security-configuration> 요소 내의 <enforce-valid-basic-auth-credentials>를 설정하십시오.

```
<enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>
```

IdP 또는 SP 에서 싱글 사인온 초기화

사용자는 아이덴티티 공급자나 서비스 공급자에서 시작하여 싱글 사인온을 시작할 수 있습니다. 각 사이트에서 링크를 구성하거나 싱글 사인온 작업을 트리거하는 응용 프로그램의 일부로 링크를 구성하십시오.

추가 정보:

아이덴티티 공급자에서 시작되는 SSO(POST 또는 아티팩트 바인딩) (페이지 239)
서비스 공급자에서 시작되는 SSO(POST 또는 아티팩트 바인딩) (페이지 242)

아이덴티티 공급자에서 시작되는 SSO(POST 또는 아티팩트 바인딩)

사용자가 서비스 공급자로 이동하기 전에 아이덴티티 공급자를 방문하는 경우 아이덴티티 공급자는 원치 않는 응답을 생성해야 합니다. 원치 않는 응답을 시작하려면 서비스 공급자 ID 와 함께 쿼리 매개 변수가 포함된 HTTP Get 요청을 생성하는 하드 코드된 링크를 생성하십시오. 그러면 아이덴티티 공급자가 이 ID 에 대한 어설션 응답을 생성합니다. 페더레이션 웹 서비스 응용 프로그램과 어설션 생성기가 GET 요청을 수락해야 합니다.

사용자가 설정된 링크를 클릭하면 원치 않는 응답이 시작됩니다.

원치 않는 응답에서 아티팩트 또는 POST 프로필이 사용되도록 지정하려는 경우 원치 않는 응답 링크의 구문은 다음과 같습니다.

```
http://idp_server:port/affwebservices/public/saml2sso?SPID=SP_ID&
ProtocolBinding=URI_for_binding
```

idp_server:port

웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하는 웹 서버와 포트를 식별합니다.

SP_ID

서비스 공급자 ID 값입니다. 엔터티 ID 는 대/소문자를 구분합니다. "관리 UI"에 표시되는 그대로 입력하십시오.

URI_for_binding

ProtocolBinding 요소에 대한 POST 또는 아티팩트 바인딩의 URI 를 식별합니다. 이 URI 는 SAML 2.0 사양에 의해 정의됩니다.

또한 SAML 서비스 공급자 속성에서 바인딩을 지정해야 원치 않는 응답이 올바로 작동합니다.

다음 정보에 주의하십시오.

- 링크에 ProtocolBinding 매개 변수가 없고 서비스 공급자 속성에 바인딩이 하나만 있는 경우 서비스 공급자는 바인딩 하나를 사용합니다.
- 아티팩트 바인딩과 POST 바인딩이 서비스 공급자 속성에서 사용되도록 설정된 경우에는 POST 가 기본값입니다. 따라서 아티팩트 바인딩 *만* 사용하려면 링크에 ProtocolBinding 쿼리 매개 변수를 포함하십시오.
- 어설션 소비자 서비스에 대해 인덱싱된 끝점을 구성하면 ProtocolBinding 쿼리 매개 변수가 어설션 소비자 서비스에 대한 바인딩을 재정의합니다.

추가 정보:

IdP 가 사용하는 원치 않는 응답 쿼리 매개 변수 (페이지 240)

IdP 가 사용하는 원치 않는 응답 쿼리 매개 변수

정책 서버 IdP 에서 싱글 사인온을 시작하는 원치 않는 응답에는 다음 쿼리 매개 변수가 포함될 수 있습니다.

- SPID
- ProtocolBinding
- RelayState

SPID

(필수) 아이덴티티 공급자가 원치 않는 응답을 보내는 서비스 공급자의 ID 를 지정합니다. 엔터티 ID 는 대/소문자를 구분합니다. "관리 UI"에 표시되는 그대로 입력하십시오.

ProtocolBinding

원치 않는 응답의 ProtocolBinding 요소를 지정합니다. 이 요소는 서비스 공급자에게 어설션 응답을 보낼 때 사용되는 프로토콜을 지정합니다. 서비스 공급자가 지정된 프로토콜 바인딩을 지원하도록 구성되어 있지 않으면 요청이 실패합니다.

ProtocolBinding 쿼리 매개 변수의 필수 사용

서비스 공급자 속성에서 아티팩트 및 POST 바인딩이 사용되도록 설정한 *경우에만* ProtocolBinding 매개 변수를 사용해야 합니다. 두 프로필이 모두 사용되도록 설정된 경우에는 쿼리 매개 변수를 사용하여 아티팩트 바인딩만 사용하십시오.

- SAML 2.0 사양의 아티팩트 바인딩 URI 는 다음과 같습니다.

  urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact

- SAML 2.0 사양의 POST 바인딩 URI 는 다음과 같습니다.

  urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST

  HTTP-POST 싱글 사인온에 대해서는 이 매개 변수를 설정할 필요가 없습니다.

참고: 쿼리 매개 변수를 HTTP-인코딩하지 마십시오.

예: ProtocolBinding 이 있는 원치 않는 응답

이 링크는 사용자를 싱글 사인온 서비스로 리디렉션합니다. 이 링크에는 서비스 공급자 아이덴티티가 있습니다. SPID 쿼리 매개 변수는 아이덴티티를 지정합니다. 또한 bindings 쿼리 매개 변수는 아티팩트 바인딩이 사용되고 있음을 나타냅니다. 사용자가 이 하드 코드된 링크를 클릭하면 로컬 싱글 사인온 서비스로 리디렉션됩니다.

```
http://idp-ca:82/affwebservices/public/saml2sso?SPID=http%3A%2F%2Ffedsrv.
acme.com
%2Fsmidp2for90&ProtocolBinding=urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Artifact
```

ProtocolBinding 쿼리 매개 변수의 선택적 사용

ProtocolBinding 쿼리 매개 변수를 사용하지 *않는* 경우 다음 조건이 적용됩니다.

- ProtocolBinding 이 원치 않는 응답에 지정되지 않은 경우 서비스 공급자에 대한 프로필이 사용됩니다.
- 서비스 공급자에 대해 두 프로필이 모두 사용되도록 설정할 수 있습니다. ProtocolBinding 이 원치 않는 응답에 없는 경우 서비스 공급자는 기본적으로 POST 프로필을 사용합니다.

예: ProtocolBinding 이 없는 원치 않는 응답

이 링크는 사용자를 싱글 사인온 서비스로 리디렉션합니다. 이 링크에는 서비스 공급자 아이덴티티가 포함되어 있습니다. SPID 쿼리 매개 변수는 아이덴티티를 지정합니다. ProtocolBinding 쿼리 매개 변수가 없습니다. 사용자가 이 하드 코드된 링크를 클릭하면 로컬 싱글 사인온 서비스로 리디렉션됩니다.

```
http://fedsrv.fedsite.com:82/affwebservices/public/saml2sso?SPID=
http%3A%2F%2Ffedsrv.acme.com%2Fsmidp2for90
```

RelayState

서비스 공급자에 있는 대상을 지정합니다. RelayState 쿼리 매개 변수를 사용하여 대상을 나타내십시오. 하지만 이 방법은 선택 사항입니다. 대상을 나타내기 위한 구성 메커니즘이 서비스 공급자에 있을 수 있습니다.

RelayState 값을 URL-인코딩하십시오.

예

```
http://ca.sp.com:90/affwebservices/public/saml2authnrequest?ProviderID=
http%3A%2F%2Ffedsrv.acme.com%2Fsmidp2for90&
RelayState=http%3A%2F%2Fwww.spdemo.com%2Fapps%2Fapp.jsp
```

서비스 공급자에서 시작되는 SSO(POST 또는 아티팩트 바인딩)

사용자가 먼저 서비스 공급자를 방문한 다음 아이덴티티 공급자로 이동할 수 있습니다. 따라서 해당 AuthnRequest 서비스에 대한 하드 코드된 링크가 포함된 HTML 페이지를 서비스 공급자에 생성하십시오. HTML 페이지에 있는 링크는 인증을 위해 사용자를 아이덴티티 공급자로 리디렉션합니다. 링크는 AuthnRequest 에 포함된 사항도 나타냅니다.

사용자가 선택하는 하드 코드된 링크에는 특정 쿼리 매개 변수가 포함되어 있어야 합니다. 이러한 매개 변수는 서비스 공급자의 AuthnRequest 서비스에 대한 HTTP GET 요청의 일부입니다.

참고: 이러한 하드 코드된 링크가 포함된 페이지는 보호되지 않은 영역에 있어야 합니다.

트랜잭션에 대해 아티팩트 또는 프로필 바인딩이 사용되도록 지정하기 위한 링크 구문은 다음과 같습니다.

```
http://SP_server:port/affwebservices/public/saml2authnrequest?
ProviderID=IdP_ID&ProtocolBinding=URI_of_binding
```

sp_server:port

웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하는 서비스 공급자의 서버 및 포트 번호를 지정합니다.

IdP_ID

아이덴티티 공급자에게 할당된 아이덴티티를 지정합니다. 엔터티 ID 는 대/소문자를 구분합니다. "관리 UI"에 표시되는 그대로 입력하십시오.

URI_of_binding

ProtocolBinding 요소에 대한 POST 또는 아티팩트 바인딩의 URI 를 식별합니다. 이 URI 는 SAML 2.0 사양에 의해 정의됩니다.

요청이 올바로 작동하도록 하려면 SAML 인증 체계에 대해 바인딩이 사용되도록 설정하십시오.

다음 정보에 주의하십시오.

- AuthnRequest 에 ProtocolBinding 쿼리 매개 변수를 포함하지 않는 경우 기본 바인딩은 인증 체계에 대해 정의된 바인딩입니다. 두 바인딩이 모두 인증 체계에 정의되어 있는 경우에는 AuthnRequest 에서 바인딩이 전달되지 않습니다. 따라서 아이덴티티 공급자의 기본 바인딩이 사용됩니다.
- SAML 인증 체계에 대해 아티팩트와 POST 가 사용되도록 설정할 수 있습니다. 아티팩트 바인딩을 사용하려면 링크에 ProtocolBinding 쿼리 매개 변수를 포함하십시오.

SiteMinder SP 에서 사용되는 AuthnRequest 쿼리 매개 변수

SiteMinder 서비스 공급자가 AuthnRequest 서비스에 대한 링크에서 쿼리 매개 변수를 사용할 수 있습니다. 허용되는 쿼리 매개 변수는 다음과 같습니다.

ProviderID(필수)

AuthnRequest 서비스가 AuthnRequest 메시지를 보내는 아이덴티티 공급자의 ID 입니다. 엔터티 ID 는 대/소문자를 구분합니다. "관리 UI"에 표시되는 그대로 입력하십시오.

ProtocolBinding

AuthnRequest 메시지의 ProtocolBinding 요소를 지정합니다. 이 요소는 아이덴티티 공급자가 SAML 응답을 반환하는 데 사용하는 프로토콜을 지정합니다. 지정된 아이덴티티 공급자가 지정된 프로토콜 바인딩을 지원하도록 구성되어 있지 않으면 요청이 실패합니다.

AuthnRequest 에서 이 매개 변수를 사용하는 경우에는 AssertionConsumerServiceIndex 매개 변수를 포함할 수 없습니다. 두 매개 변수는 동시에 사용할 수 없습니다.

ProtocolBinding 쿼리 매개 변수의 필수 사용

인증 체계에 대해 아티팩트 및 POST 바인딩이 사용되도록 설정할 수 있습니다. 아티팩트 바인딩만 사용하려면 ProtocolBinding 매개 변수가 필요합니다.

- SAML 2.0 사양의 아티팩트 바인딩 URI 는 다음과 같습니다.

  urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact

- SAML 2.0 사양의 POST 바인딩 URI 는 다음과 같습니다.

  urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST

  HTTP-POST 싱글 사인온에 대해서는 이 매개 변수를 설정할 필요가 없습니다.

  예: ProtocolBinding 이 있는 AuthnRequest 링크

  ```
  http://ca.sp.com:90/affwebservices/public/saml2authnrequest?ProviderID=
  http%3A%2F%2Ffedsrv.acme.com%2Fsmidp2for90&ProtocolBinding=urn:oasis:
  names:tc:SAML:2.0:bindings:HTTP-Artifact
  ```

  사용자가 서비스 공급자의 링크를 클릭합니다. 그러면 페더레이션 웹 서비스 응용 프로그램이 로컬 정책 서버에서 AuthnRequest 메시지를 요청합니다.

ProtocolBinding 의 선택적 사용

ProtocolBinding 쿼리 매개 변수를 사용하지 *않는* 경우 다음 조건이 적용됩니다.

- 하나의 바인딩만 인증 체계에 대해 사용되도록 설정된 경우 ProtocolBinding 쿼리 매개 변수를 지정하지 않으면 인증 체계가 사용되도록 설정된 바인딩을 사용합니다.
- 두 바인딩이 모두 사용되도록 설정된 경우 ProtocolBinding 쿼리 매개 변수를 지정하지 않으면 POST 바인딩이 기본값으로 사용됩니다.

참고: 쿼리 매개 변수를 HTTP-인코딩하지 마십시오.

예: ProtocolBinding 이 없는 AuthnRequest 링크

이 샘플 링크는 AuthnRequest 서비스로 이동합니다. 이 링크는 ProviderID 쿼리 매개 변수에 있는 아이덴티티 공급자를 지정합니다.

```
http://ca.sp.com:90/affwebservices/public/saml2authnrequest?ProviderID=
http%3A%2F%2Ffedsrv.acme.com%2Fsmidp2for90
```

사용자가 서비스 공급자의 링크를 클릭합니다. 그러면 페더레이션 웹 서비스 응용 프로그램이 로컬 정책 서버에서 AuthnRequest 메시지를 요청합니다.

ForceAuthn

SP 가 해당 사용자에 대한 기존 보안 컨텍스트가 있는 경우에도 사용자를 인증하도록 아이덴티티 공급자를 강제하는지 여부를 나타냅니다.

- ForceAuthn=True 가 AuthnRequest 메시지에 설정된 경우 특정 사용자에 대한 SiteMinder 세션이 있으면 IdP 가 사용자에게 자격 증명에 대한 챌린지를 다시 표시합니다. 사용자가 성공적으로 인증되면 IdP 가 기존 세션의 ID 정보를 어설션에 포함합니다. IdP 가 재인증용으로 생성한 세션은 무시됩니다.

  참고: 사용자가 기존 세션과 다른 자격 증명으로 재인증을 시도할 수 있습니다. 그러면 IdP 가 현재 세션과 기존 세션의 userDN 및 사용자 디렉터리 OID 를 비교합니다. 동일한 사용자에 대한 세션이 아니면 IdP 가 SAML 2.0 응답을 반환합니다. 응답은 인증이 실패했음을 나타냅니다.

- SP 가 AuthnRequest 메시지에 ForceAuthn=True 를 설정한 경우 SiteMinder 세션이 없으면 SiteMinder IdP 가 사용자에게 자격 증명에 대한 챌린지를 표시합니다. 사용자가 성공적으로 인증되면 세션이 설정됩니다.

예

http://www.sp.demo:81/affwebservices/public/saml2authnrequest?ProviderID=idp.demo&ForceAuthn=yes

RelayState

서비스 공급자에 있는 대상을 지정합니다. RelayState 쿼리 매개 변수를 사용하여 대상을 나타낼 수 있습니다. 하지만 이 방법은 선택 사항입니다. 대신 SAML 2.0 인증 체계에 구성된 대상을 지정할 수 있습니다. 인증 체계에는 RelayState 쿼리 매개 변수로 대상을 재정의하는 옵션도 있습니다.

RelayState 값을 URL-인코딩하십시오.

예

```
http://www.spdemo.com:81/affwebservices/public/saml2authnrequest?
ProviderID=idp.demo&RelayState=http%3A%2F%2Fwww.spdemo.com%2Fapps%2Fapp.jsp
```

IsPassive

아이덴티티 공급자가 사용자와 상호 작용할 수 있는지 여부를 결정합니다. 이 쿼리 매개 변수를 true 로 설정한 경우 아이덴티티 공급자가 사용자와 상호 작용하면 안 됩니다. 또한 IsPassive 매개 변수가 아이덴티티 공급자에게 전송되는 AuthnRequest 에 포함됩니다. 이 쿼리 매개 변수를 false 로 설정한 경우에는 아이덴티티 공급자가 사용자와 상호 작용할 수 있습니다.

예

```
http://www.spdemo.com:81/affwebservices/public/saml2authnrequest?
ProviderID=idp.demo&RelayState=http%3A%2F%2Fwww.spdemo.com%
2Fapps%2Fapp.jsp&IsPassive=true
```

AssertionConsumerServiceIndex

어설션 소비자로 작동하고 있는 끝점의 인덱스를 지정합니다. 인덱스는 아이덴티티 공급자에게 어설션 응답을 보낼 위치를 알려 줍니다.

AuthnRequest 에서 이 매개 변수를 사용하는 경우에는 ProtocolBinding 매개 변수를 포함할 수 없습니다. 두 매개 변수는 동시에 사용할 수 없습니다.

SiteMinder IdP 를 사용한 쿼리 매개 변수 처리

서비스 공급자가 싱글 사인온을 시작하는 경우 해당 서비스 공급자는 ForceAuthn 또는 IsPassive 쿼리 매개 변수를 AuthnRequest 메시지에 포함할 수 있습니다. 서비스 공급자가 이러한 쿼리 매개 변수 두 개를 AuthnRequest 메시지에 포함하면 SiteMinder 아이덴티티 공급자가 다음과 같이 해당 쿼리 매개 변수를 처리합니다.

ForceAuthn 처리

서비스 공급자가 ForceAuthn=True 를 AuthnRequest 에 포함하면 SiteMinder 아이덴티티 공급자가 다음 작업을 수행합니다.

- ForceAuthn=True 가 AuthnRequest 메시지에 포함되어 있고 특정 사용자에 대한 SiteMinder 세션이 있는 경우. SiteMinder IdP 가 사용자에게 자격 증명에 대한 챌린지를 다시 표시합니다. 사용자가 성공적으로 인증되면 IdP 가 기존 세션의 아이덴티티 정보를 어설션에 넣어 보냅니다. IdP 가 재인증용으로 생성한 세션은 무시됩니다.

  사용자가 원래 세션과 다른 자격 증명으로 재인증을 시도할 수 있습니다. 그러면 SiteMinder IdP 가 현재 세션과 기존 세션의 userDN 및 사용자 디렉터리 OID 를 비교합니다. 동일한 사용자에 대한 세션이 아니면 IdP 가 SAML 2.0 응답을 반환합니다. 응답은 인증이 실패했음을 나타냅니다.

- ForceAuthn=True 가 AuthnRequest 메시지에 포함되어 있고 SiteMinder 세션이 없는 경우. SiteMinder IdP 가 사용자에게 자격 증명에 대한 챌린지를 표시합니다. 사용자가 성공적으로 인증되면 세션이 설정됩니다.

IsPassive 처리

서비스 공급자가 IsPassive 를 AuthnRequest 에 포함하는 경우 IdP 가 이를 준수할 수 없으면 다음 SAML 응답 중 하나가 서비스 공급자에게 다시 전송됩니다.

- IsPassive=True 가 AuthnRequest 메시지에 포함되어 있고 SiteMinder 세션이 없는 경우. SiteMinder 아이덴티티 공급자가 SAML 응답을 반환합니다. SiteMinder 에 세션이 필요하므로 이 응답에 오류 메시지가 포함됩니다.

- IsPassive=True 가 AuthnRequest 메시지에 포함되어 있고 SiteMinder 세션이 있는 경우. SiteMinder 아이덴티티 공급자가 어설션을 반환합니다.
- IsPassive 와 ForceAuthn 이 AuthnRequest 메시지에 포함되어 있고 둘 다 True 로 설정되어 있는 경우. 요청이 잘못되었으므로 SiteMinder 아이덴티티 공급자가 오류를 반환합니다. IsPassive 와 ForceAuthn 은 동시에 사용할 수 없습니다.

어설션에 대한 특성 구성(선택 사항)

특성은 서비스 공급자 리소스에 대한 액세스를 요청하는 사용자에 대한 추가 정보를 제공할 수 있습니다. 특성 명령문은 아이덴티티 공급자에서 SAML 어설션에 있는 서비스 공급자로 사용자 특성, DN 특성 또는 정적 데이터를 전달합니다. 모든 구성된 특성은 <AttributeStatement> 요소 하나의 어설션에 포함되거나 어설션의 <EncryptedAttribute> 요소에 포함됩니다.

참고: 어설션에는 특성 명령문이 필요하지 않습니다.

서블릿, 웹 응용 프로그램 또는 기타 사용자 지정 응용 프로그램에서는 특성을 사용하여 사용자 지정된 콘텐츠를 표시하거나 다른 사용자 지정 기능이 사용되도록 설정합니다. 웹 응용 프로그램에서 사용되는 경우 특성은 사용자가 서비스 공급자에서 수행하는 작업을 제한할 수 있습니다. 예를 들어 최대 금액(달러)으로 설정된 "Authorized Amount"(권한 부여된 금액)라는 특성 변수를 보낼 수 있습니다. 이 금액은 사용자가 서비스 공급자에서 소비할 수 있는 한도입니다.

참고: SiteMinder 가 어설션 쿼리/요청 프로필의 일부로 SAML 2.0 특성 기관 역할을 하는 경우 특성은 권한 부여 프로세스의 일부입니다. 특성 기관을 사용하여 사용자에게 권한 부여 (페이지 369) 항목에서는 이러한 구현에 대해 설명합니다.

특성은 이름/값 쌍의 형식을 사용합니다. 서비스 공급자가 어설션을 받으면 응용 프로그램에 특성 값을 제공합니다.

특성을 HTTP 헤더나 HTTP 쿠키로 제공할 수 있습니다.

HTTP 헤더와 HTTP 쿠키에는 어설션 특성이 초과할 수 없는 크기 제한이 있습니다. 크기 제한은 다음과 같습니다.

- HTTP 헤더의 경우 SiteMinder 는 헤더에 대한 웹 서버 크기 제한까지 헤더에 있는 특성을 보낼 수 있습니다. 헤더당 허용되는 어설션 특성은 하나뿐입니다. 헤더 크기 제한을 확인하려면 해당 웹 서버 설명서를 참조하십시오.
- HTTP 쿠키의 경우 SiteMinder 는 쿠키에 대한 크기 제한까지 쿠키를 보낼 수 있습니다. 각 어설션 특성은 자체 쿠키로 전송됩니다. 쿠키 크기 제한은 브라우저별로 다르고, 해당 제한은 각 특성에만 적용되는 것이 아니라 응용 프로그램에 전달되고 있는 모든 특성에 적용됩니다. 쿠키 크기 제한을 확인하려면 해당 웹 브라우저 설명서를 참조하십시오.

SSO 어설션에 대한 특성 지정

특성은 서비스 공급자 리소스에 대한 액세스를 요청하는 사용자에 대한 정보를 제공할 수 있습니다. 특성 명령문은 아이덴티티 공급자에서 SAML 어설션에 있는 서비스 공급자로 사용자 특성, DN 특성 또는 정적 데이터를 전달합니다.

특성을 구성하려면

1. 편집하고 있는 엔터티에 대한 "특성" 설정으로 이동합니다.
2. "추가"를 클릭합니다.

   "특성 추가" 페이지가 열립니다.

3. "특성 유형" 드롭다운 목록에서 이름 형식 유형을 선택합니다. 이 항목은 어설션 특성 명령문에 있는 <Attribute> 요소의 <NameFormat> 특성과 일치해야 합니다. 유형은 서비스 공급자가 이름을 해석할 수 있도록 특성 이름을 분류합니다.

   옵션은 다음과 같습니다.

   지정되지 않음

   구현에 이름 해석을 맡기는 방법을 결정합니다.

   기본

   이름 형식이 허용 가능한 값을 사용해야 함을 나타냅니다. 허용 가능한 값은 기본 유형 xs:Name 에 속한 값에서 가져옵니다.

   URI

   이름 형식이 URI 참조에 대한 표준을 따라야 함을 나타냅니다. URI 를 해석하는 방법은 특성 값을 사용하는 응용 프로그램에 따라 달라집니다.

4. "특성 설정" 섹션의 "특성 종류" 섹션에서 다음 옵션 중 하나를 선택합니다.

   - 정적
   - 사용자 특성
   - DN 특성

   "특성 종류" 선택 항목에 따라 "특성 필드" 섹션에서 사용 가능한 필드가 결정됩니다.

5. 페이지의 "특성 필드" 섹션을 구성합니다. 설정은 "특성 종류" 선택 항목에 따라 달라집니다. 옵션은 다음과 같습니다.

   - 변수 이름
   - 변수 값
   - 특성 이름
   - DN 사양

6. (선택 사항) 특성이 중첩된 그룹이 있는 LDAP 사용자 디렉터리에서 검색되는 경우 정책 서버는 중첩된 그룹에서 DN 특성을 검색할 수 있습니다. 중첩된 그룹을 사용하려면 "특성 종류" 섹션에서 "중첩된 그룹 허용" 확인란을 선택합니다.

7. (선택 사항) 특성 값을 암호화하려면 "암호화됨" 확인란을 선택합니다.

8. "검색 방법"의 경우 기본값인 "SSO"를 적용하여 싱글 사인온 어설션에 대한 특성만 검색되는지 확인합니다.
9. "확인"을 클릭하여 변경 내용을 저장합니다.

스크립트를 사용하여 새 특성 만들기

"특성" 대화 상자의 "고급" 섹션에는 "스크립트" 필드가 포함되어 있습니다. 이 필드에는 "특성 설정" 섹션에 입력한 사항을 기반으로 SiteMinder 가 생성하는 스크립트가 표시됩니다. 이 필드의 내용을 복사하여 다른 응답 특성에 대한 "스크립트" 필드에 붙여 넣을 수 있습니다.

참고: 다른 특성에 대한 "스크립트" 필드의 내용을 복사하여 붙여 넣는 경우 "특성 종류" 섹션에서 적절한 옵션을 선택하십시오.

어설션 특성의 최대 길이 지정

사용자 어설션 특성의 최대 길이를 구성할 수 있습니다. 어설션 특성의 최대 길이를 수정하려면 EntitlementGenerator.properties 파일에서 해당 설정을 변경하십시오.

이 파일에 있는 속성 이름은 구성하고 있는 프로토콜에 따라 다릅니다.

다음 단계를 수행하십시오.

1. 정책 서버가 설치된 시스템에서 *policy_server_home*\config\properties\EntitlementGenerator.properties 로 이동합니다.
2. 텍스트 편집기에서 파일을 엽니다.

3. 사용자의 환경에서 사용하고 있는 프로토콜에 맞게 사용자 특성의 최대 길이를 조정합니다. 각 프로토콜에 대한 설정은 다음과 같습니다.

   WS-페더레이션

   속성 이름:
   com.netegrity.assertiongenerator.wsfed.MaxUserAttributeLength

   속성 유형: 양의 정수 값

   기본값: 1024

   설명: WS-FED 어설션 특성의 최대 특성 길이를 나타냅니다.

   SAML 1.x

   속성 이름:
   com.netegrity.assertiongenerator.saml1.MaxUserAttributeLength

   속성 유형: 양의 정수 값

   기본값: 1024

   설명: SAML1.1 어설션 특성의 최대 특성 길이를 나타냅니다.

   SAML 2.0

   속성 이름:
   com.netegrity.assertiongenerator.saml2.MaxUserAttributeLength

   속성 유형: 양의 정수 값

   기본값: 1024

   설명: SAML2.0 어설션 특성의 최대 특성 길이를 나타냅니다.

4. 이러한 매개 변수를 변경한 후 정책 서버를 다시 시작합니다.

SSO 및 특성 쿼리 요청에 대한 특성

구성하는 특성이 싱글 사인온 요청에 대한 것인지 아니면 특성 쿼리 요청에 대한 것인지 여부를 나타내십시오. 구성하는 검색 방법에 따라 특성 기능이 결정됩니다.

동일한 특성을 두 서비스 모두에 사용하려면 동일한 특성 이름과 변수를 사용하는 특성 명령문을 두 개 생성하십시오. 하지만 한 특성은 SSO 를 검색 방법으로 사용하고 다른 특성은 특성 서비스를 검색 방법으로 사용합니다.

싱글 로그아웃 구성(선택 사항)

SLO(싱글 로그아웃 프로토콜)를 사용하면 특정 사용자의 모든 세션이 동시에 종료되므로 보안을 유지하는 데 도움이 됩니다. 이러한 세션은 로그아웃을 시작한 브라우저 세션의 일부여야 합니다.

싱글 로그아웃이 반드시 사용자의 모든 세션을 종료하는 것은 아닙니다. 예를 들어 사용자가 브라우저 두 개를 연 경우 해당 사용자는 독립 세션 두 개를 설정할 수 있습니다. 싱글 로그아웃을 시작하는 브라우저에 대한 세션만 해당 세션에 대한 모든 페더레이션된 사이트에서 종료됩니다. 다른 브라우저의 세션은 여전히 활성 상태입니다. 사용자가 로그아웃을 시작하면 싱글 로그아웃이 트리거됩니다.

참고: SiteMinder 는 싱글 로그아웃 프로토콜에 대해 HTTP-리디렉션 바인딩만 지원합니다.

SLO 를 구성하면 서비스 공급자가 싱글 로그아웃 프로토콜을 지원하는지 여부와 지원하는 경우 서비스 공급자가 싱글 로그아웃을 처리하는 방법이 아이덴티티 공급자에게 알려집니다.

싱글 로그아웃이 사용되도록 설정하는 경우에는 다음 작업도 수행해야 합니다.

- 정책 서버 관리 콘솔을 사용하여 아이덴티티 공급자에서 세션 저장소가 사용되도록 설정합니다.

  세션 저장소에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

- 서비스 공급자에서 보호된 리소스가 포함된 영역에 대해 영구 세션을 구성하십시오. 관리 UI 에서 영구 세션을 구성하십시오.

  영역에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

싱글 로그아웃을 구성하려면

1. 관리 UI 에 로그온합니다.
2. 구성할 SAML 서비스 공급자에 대한 "SAML 프로필" 페이지로 이동합니다.
3. 페이지의 "SLO" 섹션에서 "HTTP-리디렉션" 확인란을 선택합니다. 이 설정은 싱글 로그아웃이 사용되도록 설정합니다.

4. 다음 필드에 주의하면서 나머지 필드에 대한 값을 입력합니다.

   유효 기간

   싱글 로그아웃 요청의 유효 시간(초)을 지정합니다. 이 속성은 어설션에 대한 싱글 사인온 유효 기간과 다릅니다. 유효 기간이 만료되면 IdP 가 로그아웃을 시작한 엔터티에 싱글 로그아웃 응답을 보냅니다. 유효 기간은 싱글 로그아웃 메시지 기간을 계산하기 위한 차이 시간("일반" 탭에서 설정됨)에 따라서도 달라집니다.

   "SLO 위치 URL", "SLO 응답 위치 URL" 및 "SLO 확인 URL"

   이러한 필드에 대한 항목은 https:// 또는 http://로 시작해야 합니다.

5. (선택 사항) 하나의 브라우저 세션 중에 동일한 파트너에게 전송되는 어설션에 동일한 세션 인덱스를 사용하려면 "세션 인덱스 재사용" 필드를 선택합니다. 이 옵션을 선택하면 모든 타사 파트너와의 싱글 로그아웃이 성공하게 됩니다.

사용자 세션이 아이덴티티 공급자와 모든 서비스 공급자 사이트에서 제거된 후 페더레이션 웹 서비스가 사용자를 로그아웃 확인 페이지로 리디렉션합니다.

추가 정보:

싱글 로그아웃 요청 유효 기간 (페이지 254)
싱글 로그아웃 확인 페이지에 대한 지침 (페이지 255)

싱글 로그아웃 요청 유효 기간

SLO 유효 기간과 차이 시간은 정책 서버에 싱글 로그아웃 요청이 유효한 총 시간을 계산하는 방법을 지시합니다.

참고: SLO 유효 기간은 SSO 유효 기간과는 다른 값입니다.

로그아웃 요청 기간 계산과 관련된 값 두 개를 IssueInstant 값과 NotOnOrAfter 값이라고 합니다. SLO 응답에서 싱글 로그아웃 요청은 NotOnOrAfter 값에 도달할 때까지 유효합니다.

싱글 로그아웃 요청이 생성되는 경우 정책 서버의 시스템 시간이 사용됩니다. 그 결과로 얻은 시간은 요청 메시지에 설정되는 IssueInstant 값이 됩니다.

정책 서버는 로그아웃 요청이 더 이상 유효하지 않은 시기를 결정합니다. 정책 서버의 현재 시스템 시간이 사용되고 차이 시간에 SLO 유효 기간이 더해집니다. 그 결과로 얻은 시간은 NotOnOrAfter 값이 됩니다. 시간은 GMT 를 기준으로 합니다.

예를 들어 아이덴티티 공급자에서 로그아웃 요청이 1:00 GMT 에 생성된다고 가정합니다. 차이 시간은 30 초이고 SLO 유효 기간은 60 초입니다. 따라서 요청은 1:00 GMT 에서 1:01:30 GMT 까지 유효합니다. IssueInstant 값은 1:00 GMT 이고 싱글 로그아웃 요청 메시지는 90 초 뒤에 더 이상 유효하지 않습니다.

싱글 로그아웃 확인 페이지에 대한 지침

싱글 로그아웃을 지원하려면 로그아웃 확인 페이지가 사이트에 있도록 하십시오. 이 페이지를 통해 사용자는 자신이 로그아웃되었음을 알 수 있습니다.

로그아웃 확인 페이지는 다음 조건을 충족해야 합니다.

- 싱글 로그아웃이 서비스 공급자에서 시작되는 경우 로그아웃 확인 페이지는 서비스 공급자 사이트의 보호되지 않은 로컬 리소스여야 합니다.
- 싱글 로그아웃이 아이덴티티 공급자 사이트에서 시작되는 경우 로그아웃 확인 페이지는 아이덴티티 공급자 사이트의 보호되지 않은 로컬 리소스여야 합니다.
- 페이지는 페더레이션 파트너 도메인에 있는 리소스일 수 없습니다. 예를 들어 로컬 도메인이 ca.com 인 경우 SLO 확인 페이지는 example.com 도메인에 있을 수 없습니다.

로그아웃 실패에 대한 피드백을 받으려면 로그아웃 확인 페이지가 다음 요구 사항도 충족해야 합니다.

- Base 64 로 인코딩된 데이터를 처리하고 쿠키를 읽을 수 있어야 합니다.
- SIGNOUTFAILURE 쿠키를 찾는 코드를 포함해야 합니다. IdP 와 SP 의 로그아웃 페이지가 이 조건을 충족해야 합니다. 싱글 로그아웃이 실패하면 브라우저에서 쿠키가 설정됩니다. 쿠키에는 로그아웃이 실패한 페더레이션 사이트의 파트너 ID 가 포함됩니다. 이러한 ID 는 Base 64 로 인코딩됩니다. 여러 ID 가 나열되는 경우 공백 문자로 구분됩니다.

  이 쿠키를 찾도록 로그아웃 확인 페이지를 구성하여 사용자에게 로그아웃이 실패한 위치를 알릴 수 있습니다. 이 정보는 사용자가 여러 파트너 사이트에서 로그아웃하고 있는 네트워크에서 유용합니다.

  또한 SIGNOUTFAILURE 쿠키가 발견된 경우 로그아웃 확인 페이지를 통해 사용자에게 웹 브라우저를 닫아서 모든 세션 데이터를 제거하도록 알려야 합니다.

IdP 에서 아이덴티티 공급자 검색 구성

IPD(아이덴티티 공급자 검색) 프로필이 제공하는 공통 검색 서비스를 사용하면 서비스 공급자가 인증을 위해 고유 IdP 를 선택할 수 있습니다. 네트워크에 있는 모든 사이트가 아이덴티티 공급자 검색 서비스와 상호 작용하도록 파트너 간의 사전 비즈니스 계약이 설정되어 있습니다.

이 프로필은 어설션을 제공하는 파트너가 둘 이상 있는 페더레이션된 네트워크에 유용합니다. 서비스 공급자는 자신이 특정 사용자에 대한 인증 요청을 보내는 아이덴티티 공급자를 결정할 수 있습니다.

IdP 검색 프로필은 두 페더레이션된 파트너에 공통적인 쿠키 도메인을 사용하여 구현됩니다. 약정된 도메인의 쿠키에는 사용자가 방문한 IdP 목록이 포함되어 있습니다.

IDP 검색 프로필의 경우 SP 는 자신이 인증 요청을 보내는 IdP 를 확인할 수 있어야 합니다. SP 가 인증하려는 사용자는 이전에 아이덴티티 공급자를 방문하여 인증을 받은 상태여야 합니다.

IdP 에서 아이덴티티 공급자 검색 기능만 사용되도록 설정합니다. 다른 구성은 필요하지 않습니다. 이 기능이 사용되도록 설정하면 IDP 검색 서비스의 일반 도메인에서 쿠키가 설정됩니다. 이 프로세스는 사용자에게 투명하게 처리됩니다.

아이덴티티 공급자 검색 프로필이 사용되도록 설정(선택 사항)

페더레이션된 네트워크에는 어설션을 생성하는 아이덴티티 공급자가 둘 이상 있을 수 있습니다. 아이덴티티 공급자 검색 프로필을 사용하면 사용자가 인증에 사용할 특정 아이덴티티 공급자를 선택할 수 있습니다.

아이덴티티 공급자 검색 프로필이 사용되도록 설정하려면

1. 관리 UI 에 로그온합니다.
2. 수정할 SP 에 대한 "SAML 프로필" 페이지로 이동합니다.
3. "IPD" 섹션에서 "사용" 확인란을 선택합니다.
4. 필요한 필드에 데이터를 입력하고 필요한 설정을 선택합니다.

   참고: "서비스 URL" 필드를 다음과 같은 아이덴티티 공급자 검색 프로필 서블릿으로 설정합니다.

   https://*host:port*/affwebservices/public/saml2ipd
5. "제출"을 클릭하여 변경 내용을 저장합니다.

공격으로부터 IdP 검색 대상 보안

SiteMinder 아이덴티티 공급자 검색 서비스가 일반 도메인 쿠키에 대한 요청을 받는 경우 요청에는 IPDTarget 이라는 쿼리 매개 변수가 포함되어 있습니다. 이 쿼리 매개 변수는 검색 서비스가 요청을 처리한 후 리디렉션해야 하는 URL 을 나열합니다.

IdP 의 경우 IPDTarget 은 SAML 2.0 싱글 사인온 서비스입니다. SP 의 경우 대상은 일반 도메인 쿠키를 사용하려고 요청하는 응용 프로그램입니다.

보안 공격으로부터 IPDTarget 쿼리 매개 변수를 보호하는 것이 좋습니다. 권한 없는 사용자가 이 쿼리 매개 변수에 임의의 URL 을 넣을 수 있습니다. 그러면 URL 로 인해 악의적인 사이트로 리디렉션될 수 있습니다.

공격으로부터 쿼리 매개 변수를 보호하려면 "에이전트 구성 개체" 설정 **ValidFedTargetDomain** 을 구성하십시오. ValidFedTargetDomain 매개 변수는 페더레이션 환경에 대해 유효한 도메인을 모두 나열합니다.

참고: ValidFedTargetDomain 설정은 웹 에이전트가 사용하는 ValidTargetDomain 설정과 유사하지만 이 설정은 구체적으로 페더레이션에 대해 정의됩니다.

IPD 서비스가 IPDTarget 쿼리 매개 변수를 검사합니다. 그런 다음 서비스는 쿼리 매개 변수가 지정하는 URL 의 도메인을 획득합니다. IPD 서비스가 이 도메인과 ValidFedTargetDomain 매개 변수에 지정된 도메인 목록을 비교합니다. URL 도메인이 ValidFedTargetDomain 에 구성된 도메인 중 하나와 일치하면 IPD 서비스가 사용자를 지정된 URL 로 리디렉션합니다.

일치하는 도메인이 없으면 IPD 서비스가 사용자 요청을 거부하고 브라우저를 통해 "403 사용 권한 없음" 오류가 수신됩니다. 또한 FWS 추적 로그와 affwebservices 로그에서 오류가 보고됩니다. 이러한 메시지는 IPDTarget 의 도메인이 유효한 페더레이션 대상 도메인으로 정의되지 않았음을 나타냅니다.

ValidFedTargetDomain 설정을 구성하지 않으면 서비스가 유효성 검사를 수행하지 않은 상태로 사용자를 대상 URL 로 리디렉션합니다.

서명된 요청 및 응답 유효성 검사

정책 서버는 다음과 같은 서명된 메시지를 확인할 수 있습니다.

- SSO 인증 요청
- 싱글 로그아웃 요청 및 응답

기본적으로 서명 처리는 사용되도록 설정되어 있는데, 이는 SAML 2.0 사양에 따라 필요하기 때문입니다. 프로덕션 환경에서 항상 서명 처리가 사용되도록 설정하십시오.

정책 서버는 항상 SAML 2.0 POST 응답과 싱글 로그아웃 요청에 서명합니다. 서명에는 관리 UI 를 통한 구성이 필요하지 않습니다. 서명에 필요한 설정은 인증서 데이터 저장소에 서명 기관의 개인 키/인증서 쌍을 추가하는 것뿐입니다.

중요! 디버깅에만 사용할 경우 일시적으로 모든 서명 처리(서명 및 서명 확인 모두)가 사용되지 않도록 설정할 수 있습니다. "암호화 및 서명" 설정의 "서명" 섹션에서 "서명 처리 사용 안 함"을 선택하십시오.

서비스 공급자로부터 받은 AuthnRequest 의 서명이나 싱글 로그아웃 요청 및 응답의 유효성을 검사하려면 관리 UI 에서 구성 단계를 완료하십시오.

유효성 검사를 설정하려면

1. 아이덴티티 공급자의 인증서 데이터 저장소에 공개 키를 추가합니다.

   공개 키는 서비스 공급자가 서명을 수행하는 데 사용한 개인 키 및 인증서에 해당해야 합니다.

2. 관리 UI 에서 다음 확인란 중 하나 또는 둘 모두를 선택합니다.

   - 서명된 AuthnRequest 필요("암호화 및 서명" 설정)

     이 확인란을 선택하면 아이덴티티 공급자가 서명된 authnrequest 를 요구한 다음 IdP 가 요청 서명의 유효성을 검사합니다. authnrequest 가 서명되지 않은 경우 아이덴티티 공급자가 해당 요청을 거부합니다.

     중요: AuthnRequest 에 서명하면 원치 않는 응답이 아이덴티티 공급자로부터 전송될 수 없습니다.

   - HTTP-리디렉션("SAML 프로필" 설정)

     이 확인란을 선택하면 아이덴티티 공급자가 SLO 요청 및 응답 서명의 유효성을 검사합니다.

3. "발급자 DN" 및 "일련 번호" 필드("암호화 및 서명" 설정)에 데이터를 입력합니다.

   필드 값이 인증서 데이터 저장소에 있는 인증서와 일치해야 합니다. 인증서는 요청에 서명하는 기관의 개인 키/인증서 쌍에 해당하는 것입니다. 입력하는 값이 일치하는 값인지 확인하려면 인증서의 DN 을 봅니다.

NameID 및 어설션 암호화

어설션에 있는 이름 ID 나 어설션 자체를 암호화할 수 있습니다. 암호화를 수행하면 어설션을 전송할 때 보호 수준이 강화됩니다.

암호화를 구성하는 경우 파트너 인증서를 지정하십시오. 인증서는 어설션에 있습니다. 어설션이 서비스 공급자에 도달하면 서비스 공급자가 연결된 개인 키를 사용하여 암호화된 데이터의 암호를 해독합니다.

참고: 암호화가 사용되도록 설정하는 경우 첫 번째 페더레이션 호출로 인해 암호화 라이브러리를 로드하고 추가 메모리를 할당하기 위해 정책 서버 메모리가 증가할 수 있습니다.

암호화가 사용되도록 설정

암호화를 구현하려면

1. 관리 UI 에 로그인합니다.
2. 구성할 서비스 공급자에 대한 "암호화 및 서명" 설정으로 이동합니다.
3. 어설션 암호화에 대한 설정을 구성합니다.

   다음 조건을 확인합니다.

   - rsa-oaep 를 암호화 키 알고리즘으로 선택하는 경우 필요한 최소 키 크기는 1024 비트입니다.
   - aes-256 비트 암호화 블록 알고리즘을 사용하려면 Sun JCE(Java Cryptography Extension) Unlimited Strength Jurisdiction Policy Files 를 설치합니다. 이러한 파일은 http://java.sun.com/javase/downloads/index.jsp 에서 다운로드할 수 있습니다.
   - "IssuerDN" 및 "일련 번호" 필드의 경우 IssuerDN 은 인증서 발급자의 DN 및 연결된 일련 번호입니다. 이 정보를 사용하여 인증서 데이터 저장소에 있는 서비스 공급자의 인증서를 찾을 수 있습니다. 서비스 공급자가 이 데이터를 제공합니다.

     입력하는 IssuerDN 및 일련 번호는 아이덴티티 공급자의 인증서 데이터 저장소에 저장된 키/인증서 쌍의 IssuerDN 및 일련 번호와 일치해야 합니다.
4. "제출"을 클릭하여 변경 내용을 저장합니다.

IdP 에서 프록시 서버로 요청 처리

IdP 로서 정책 서버가 요청을 처리하기 전에 정책 서버는 페더레이션 웹 서비스 응용 프로그램의 로컬 URL 을 사용하여 메시지 특성의 유효성을 검사합니다.

예를 들어 SP 의 AuthnRequest 메시지에 다음 특성이 포함될 수 있습니다.

```
Destination="http://idp.domain.com:8080/affwebservices/public/saml2sso"
```

이 예에서는 AuthnRequest 의 Destination 특성과 페더레이션 웹 서비스 응용 프로그램의 주소가 동일합니다. 정책 서버는 Destination 특성이 FWS 응용 프로그램의 로컬 URL 과 일치하는지 확인합니다.

정책 서버가 프록시 서버 뒤에 있는 경우 로컬 URL 과 Destination 특성 URL 은 동일하지 않습니다. Destination 특성은 프록시 서버의 URL 입니다. 예를 들어 AuthnRequest 에 다음 Destination 특성이 포함될 수 있습니다.

```
Destination="http://proxy.domain.com:9090/affwebservices/public/saml2sso"
```

페더레이션 웹 서비스에 대한 로컬 URL(http://idp.domain.com:8080/affwebservices/public/saml2sso)이 Destination 특성과 일치하지 않으므로 정책 서버가 요청을 거부합니다.

정책 서버가 메시지 특성을 확인하기 위해 로컬 URL 을 결정하는 방법을 변경하도록 프록시 구성을 지정할 수 있습니다. 프록시를 지정하는 경우 시스템은 로컬 URL 의 *protocol*://*authority* 부분을 프록시 서버 URL 로 대체합니다. 그 결과로 두 URL 간에 일치 항목이 발생합니다.

프록시 서버로 요청 처리 구성

정책 서버는 프록시 서버 내에 위치할 수 있습니다. 이 배포의 경우 시스템이 요청 메시지 특성에 있는 URL 과 로컬 프록시 URL 간의 일치 항목을 찾도록 프록시를 구성하십시오. 일치 항목이 있어야 요청을 처리할 수 있습니다. 정책 서버는 로컬 URL 의 *protocol*://*authority* 부분을 프록시 서버 URL 로 대체합니다. 그 결과로 두 URL 간에 일치 항목이 발생합니다.

IdP 에서 프록시 서버를 사용하려면

1. 관리 UI 에 로그인합니다.
2. 구성할 서비스 공급자에 대한 "일반" 설정으로 이동합니다.

3. *protocol*://*authority* 형식으로 프록시 서버에 대한 부분 URL 을 입력합니다.

   예를 들어 프록시 서버 구성은 다음과 같습니다.

   ```
   http://proxy.domain.com:9090
   ```

   네트워크에 SPS 페더레이션 게이트웨이가 포함되어 있으면 "서버" 필드에서 SPS 페더레이션 게이트웨이 호스트 및 포트를 지정해야 합니다. 예를 들면 다음과 같습니다.

   ```
   http://sps_gateway_server.ca.com:9090
   ```

4. "제출"을 클릭하여 변경 내용을 저장합니다.

"서버" 필드에 입력하는 값은 다음 IdP 서비스에 대한 URL 에 영향을 줍니다.

- 싱글 사인온 서비스
- 싱글 로그아웃 서비스
- 아티팩트 레졸루션 서비스
- 특성 서비스
- 인증 URL - 프록시 서버 URL 을 사용하십시오. 정책 서버가 사용자를 인증한 후 싱글 사인온 서비스를 얻기 위해 사용자가 프록시 서버로 리디렉션됩니다.

"서버" 값은 Destination 특성 같은 SAML 특성을 확인하는 데 사용되는 URL 의 일부가 됩니다. URL 하나에 대해 프록시 서버를 사용하고 있는 경우 이 모든 URL 에 대해 해당 프록시 서버를 사용하십시오.

제 15 장: SAML 2.0 서비스 공급자 구성

이 섹션은 다음 항목을 포함하고 있습니다.

서비스 공급자 설정

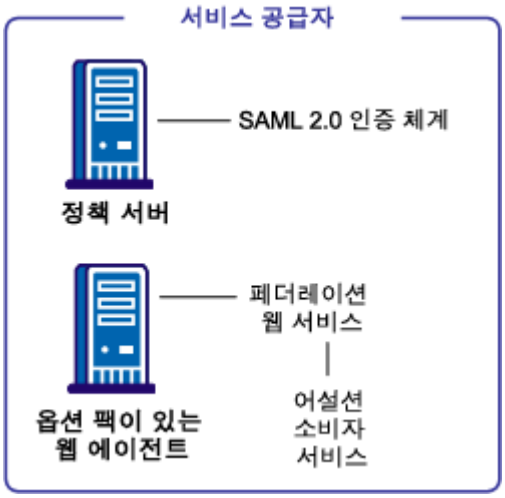
SiteMinder 또는 SPS 페더레이션 게이트웨이는 SAML 2.0 서비스 공급자로 작동할 수 있습니다. 서비스 공급자는 아이덴티티 공급자로부터 받은 어설션을 사용하여 사용자를 인증한 다음 요청된 페더레이션 리소스에 대한 액세스 권한을 제공합니다. SiteMinder 서비스 공급자가 해당 사이트의 사용자 저장소에 액세스할 수 있는 경우 서비스 공급자는 SiteMinder SAML 2.0 인증 체계를 사용하여 사용자를 인증합니다.

SAML 2.0 인증 체계를 사용하면 도메인 간 싱글 사인온이 사용되도록 설정됩니다. 서비스 공급자는 아이덴티티 공급자로부터 받은 어설션을 소비하고 사용자를 식별하며 SiteMinder 세션을 설정할 수 있습니다. 세션이 설정된 후 서비스 공급자가 사용자에게 특정 리소스에 대한 권한을 부여할 수 있습니다.

다음 그림에서는 서비스 공급자의 인증 구성 요소를 보여 줍니다.

참고: 사이트는 아이덴티티 공급자와 서비스 공급자 둘 다일 수 있습니다.

SAML 2.0 인증에 대한 주요 구성 요소가 다음 그림에 나와 있습니다.



참고: SPS 페더레이션 게이트웨이가 페더레이션 웹 서비스 응용 프로그램 기능을 제공하기 위해 웹 에이전트 및 웹 에이전트 옵션 팩을 대체할 수 있습니다. SPS 페더레이션 게이트웨이 설치 및 구성에 대한 자세한 내용은 *Secure Proxy Server Administration Guide*(보안 프록시 서버 관리 안내서)를 참조하십시오.

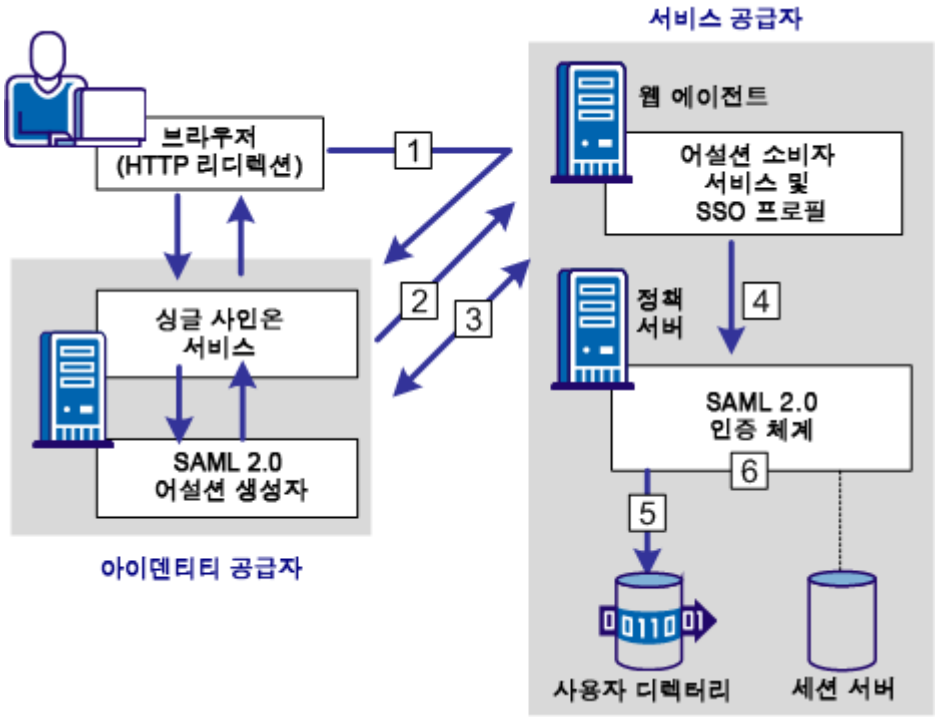
SAML 2.0 인증 체계는 서비스 공급자 사이트에 있는 정책 서버에서 구성됩니다. 인증 체계는 서비스 공급자 사이트의 웹 에이전트 또는 SPS 페더레이션 게이트웨이에 설치되는 페더레이션 웹 서비스 응용 프로그램의 구성 요소인 어설션 소비자 서비스를 호출합니다. 서비스는 SAML 인증 체계에서 정보를 얻은 다음 해당 정보를 사용하여 SAML 어설션에서 필요한 정보를 추출합니다.

SAML 어설션은 서비스 공급자 정책 서버에 로그인하기 위한 사용자 자격 증명이 됩니다. 사용자가 인증되어 권한이 부여되고, 권한 부여가 성공한 경우 대상 리소스로 리디렉션됩니다.

어설션 소비자 서비스는 AssertionConsumerServiceIndex 값인 0 을 포함하는 AuthnRequest 를 허용합니다. 이 설정에 대한 다른 값은 모두 거부됩니다.

SAML 인증 요청 프로세스

다음 그림에서는 SAML 2.0 인증 체계가 요청을 처리하는 방법을 보여 줍니다.



참고: SPS 페더레이션 게이트웨이가 페더레이션 웹 서비스 응용 프로그램 기능을 제공하기 위해 웹 에이전트 및 웹 에이전트 옵션 팩을 대체할 수 있습니다. SPS 페더레이션 게이트웨이 설치 및 구성에 대한 자세한 내용은 *Secure Proxy Server Administration Guide*(보안 프록시 서버 관리 안내서)를 참조하십시오.

인증에 대한 기능 흐름은 다음과 같습니다.

1. 사용자가 서비스 공급자 리소스를 요청합니다. 이 요청은 서비스 공급자의 AuthnRequest 서비스로 이동합니다. 그런 다음 SAML 어설션을 획득하기 위해 요청이 아이덴티티 공급자로 리디렉션됩니다.
2. 아이덴티티 공급자가 응답을 서비스 공급자에게 반환합니다.

   HTTP-POST 바인딩의 경우 응답에 어설션이 포함됩니다. HTTP-아티팩트 바인딩의 경우 응답에 SAML 아티팩트가 포함됩니다.

3. 서비스 공급자의 어설션 소비자 서비스가 응답 메시지를 수신하고 POST 바인딩이 사용되고 있는지 아니면 아티팩트 바인딩이 사용되고 있는지 확인합니다.

   HTTP-아티팩트 바인딩의 경우 어설션 소비자 서비스가 아티팩트를 아이덴티티 공급자에게 보내 어설션을 검색합니다. 아이덴티티 공급자가 어설션이 포함된 응답을 반환합니다. 어설션 소비자 서비스는 어설션이 포함된 응답을 정책 서버에 대한 자격 증명으로 사용합니다.

4. 정책 서버가 사용자 자격 증명이 포함된 응답 메시지를 인증될 체계에 전달하여 SAML 2.0 인증 체계를 호출합니다.

5. 사용자 명확성 프로세스가 시작됩니다.

6. 명확성 단계가 완료된 후 SAML 2.0 인증 체계가 어설션에 있는 자격 증명의 유효성을 검사합니다. 또한 체계는 어설션의 시간 유효성을 검사하고, 해당하는 경우 트러스트된 아이덴티티 공급자가 어설션에 서명했는지 확인합니다.

   참고: POST 바인딩의 경우 서명은 필수 사항입니다. 서명이 없으면 인증이 실패합니다. 아티팩트 바인딩의 경우 서비스 공급자와 아이덴티티 공급자 간의 보안 채널을 통해 어설션이 확보되므로 서명된 어설션은 선택 사항입니다.

   싱글 로그아웃이 사용되도록 설정된 경우 SLO 서블릿이 사용자를 액세스 권한 없음 URL 로 리디렉션합니다.

신뢰 파트너에 대한 사전 요구 사항

SiteMinder 를 신뢰 파트너로 사용하려면 다음 태스크를 완료하십시오.

- 정책 서버를 설치합니다.
- 다음 구성 요소 중 하나를 설치합니다.
  - 웹 에이전트 및 웹 에이전트 옵션 팩. 웹 에이전트는 사용자를 인증하고 세션을 설정합니다. 옵션 팩은 페더레이션 웹 서비스 응용 프로그램을 제공합니다. 적절한 네트워크 시스템에 FWS 응용 프로그램을 배포해야 합니다.
  - 포함된 웹 에이전트가 있고 포함된 Tomcat 웹 서버에 페더레이션 웹 서비스 응용 프로그램이 있는 SPS 페더레이션 게이트웨이

  자세한 내용은 *웹 에이전트 옵션 팩 안내서*를 참조하십시오.
- 메시지 서명 및 암호화를 필요로 하는 기능을 위해 개인 키와 인증서를 가져옵니다.

- 어설션 파트너는 페더레이션된 네트워크 내에서 설정됩니다.

SAML 2.0 인증 체계를 구성하는 방법

서비스 공급자를 구성하려면 다음 태스크를 수행해야 합니다.

1. SAML 2.0 인증 체계 필수 구성 요소를 완료합니다.
2. 인증 체계 유형을 선택합니다 (페이지 268).
3. 사용자를 인증하기 위한 명확성을 구성합니다.
4. 싱글 사인온을 구성합니다 (페이지 272).

페더레이션 파트너이면서 어설션을 생성하는 아이덴티티 공급자 각각에 대해 SAML 인증 체계를 구성합니다. 각 체계를 영역에 바인드합니다. 영역은 사용자가 요청한 대상 리소스의 모든 URL 로 구성됩니다. 이러한 리소스는 정책을 사용하여 보호하십시오.

팁:

- 아이덴티티 공급자와 서비스 공급자의 특정 매개 변수 값이 일치해야 구성이 올바로 작동합니다. 이러한 매개 변수 목록은 동일한 값을 사용해야 하는 구성 설정 (페이지 411)에서 제공됩니다.
- 페더레이션 웹 서비스 서블릿에 대해 올바른 URL 을 사용하고 있는지 확인하십시오. URL 은 SiteMinder 구성에 사용되는 페더레이션 웹 서비스 URL (페이지 417)에 나열되어 있습니다.

서비스 공급자에 대한 선택적 구성 태스크

SiteMinder 를 서비스 공급자로 구성하기 위한 선택적 태스크는 다음과 같습니다.

- 싱글 로그아웃이 사용되도록 설정합니다 (페이지 278).
- 이름 ID 및/또는 어설션에 대한 암호화가 사용되도록 설정합니다 (페이지 281).
- 아티팩트 확인 메시지에 서명합니다 (페이지 281).
- 서명된 아티팩트 응답을 요구합니다 (페이지 281).
- 메시지 소비자 플러그인을 사용하여 어설션을 사용자 지정합니다 (페이지 175).

레거시 페더레이션 대화 상자 탐색

관리 UI 에서는 레거시 페더레이션 구성 대화 상자로 이동하는 방법 두 가지를 제공합니다.

다음 두 방법 중 하나로 탐색할 수 있습니다.

- 마법사를 따라 새 레거시 페더레이션 개체 구성

  개체를 생성하는 경우 페이지가 표시되면서 구성 마법사가 나타납니다. 구성 마법사의 단계를 따라 개체를 생성하십시오.

- 탭을 선택하여 기존 레거시 페더레이션 개체 수정

  기존 개체를 수정하는 경우 페이지가 표시되면서 일련의 탭이 나타납니다. 이러한 탭에서 구성을 수정하십시오. 이러한 탭은 구성 마법사의 단계와 동일합니다.

인증 체계 유형 선택

서비스 공급자는 어설션의 아이덴티티 정보를 사용하여 보호된 페더레이션된 리소스에 대한 액세스 권한을 부여합니다. 이 프로세스에는 SAML 인증 체계가 사용됩니다.

리소스를 보호할 SAML 2.0 인증 체계를 할당하려면 먼저 체계를 구성하십시오.

다음 단계를 수행하십시오.

1. SAML 2.0 인증 체계 사전 요구 사항을 검토합니다.
2. 관리 UI 에 로그인합니다.
3. "인프라", "인증", "인증 체계"로 이동합니다.

   "인증 체계" 페이지가 열리면서 "일반" 설정이 표시됩니다.
4. 인증 체계를 명명합니다.

5. "인증 체계 유형" 드롭다운 목록에서 "SAML 2.0 템플릿"을 선택합니다. 이 체계에 대한 보호 수준을 선택할 수도 있습니다.

   SAML 2.0 체계를 지원하도록 "인증 체계" 대화 상자의 내용이 변경됩니다.

6. "체계 설정" 섹션에서 "SAML 2.0 구성"을 클릭하여 인증 체계의 상세 정보를 정의합니다.

   체계를 처음 구성하고 있는 경우 구성 마법사를 따라 인증 체계를 설정합니다.

SAML 2.0 인증 체계에 대한 일반 정보 지정

SAML 2.0 인증 체계에 대한 "일반" 설정에서 서비스 공급자와 아이덴티티 공급자를 식별하십시오.

다음 단계를 수행하십시오.

1. 기본 인증 체계 페이지에서 "SAML 2.0 구성"을 클릭합니다.

   기존 체계를 수정하고 있는 경우 "수정", "SAML 2.0 구성"을 차례로 클릭합니다.

   체계에 대한 상세 설정이 표시됩니다.

2. "일반" 설정의 필수 필드에 데이터를 입력합니다.
3. "사용자 명확성" 섹션으로 이동합니다.

SAML 2.0 인증에 대한 사용자 레코드 찾기

인증 체계를 구성할 때 인증 체계가 로컬 사용자 저장소에서 사용자를 조회하는 방법을 정의합니다. 올바른 사용자를 찾은 후 해당 사용자에 대한 세션이 시스템에서 생성됩니다. 사용자 저장소에서 사용자를 찾는 과정이 바로 명확성 프로세스입니다. 정책 서버가 사용자를 명확히 하는 방법은 인증 체계의 구성에 기초합니다.

성공적인 명확성을 위해 인증 체계는 먼저 어설션에서 LoginID 를 확인합니다. LoginID 는 사용자를 식별하는 SiteMinder 특정 용어입니다. 기본적으로 LoginID 는 어설션의 이름 ID 에서 추출됩니다. Xpath 쿼리를 사용하여 LoginID 를 얻을 수도 있습니다.

인증 체계가 LoginID 를 확인한 후 정책 서버는 인증 체계에 대한 검색 사양이 구성되어 있는지 확인합니다. 인증 체계에 대해 정의된 검색 사양이 없으면 LoginID 가 정책 서버에 전달됩니다. 정책 서버는 LoginID 와 사용자 저장소 검색 사양을 함께 사용하여 사용자를 찾습니다. 예를 들어 LoginID 값은 Username 이고 LDAP 검색 사양은 uid 특성으로 설정되어 있다고 가정합니다. 이 경우 정책 서버는 uid 값(Username=uid)을 사용하여 사용자를 찾습니다.

인증 체계에 대한 검색 사양을 구성하면 LoginID 가 정책 서버에 전달되지 않습니다. 대신에 검색 사양이 사용자를 찾는 데 사용됩니다.

다음 두 방법 중 하나로 사용자 명확성을 구성할 수 있습니다.

- 로컬에서 인증 체계의 일부로 구성
- 구성된 SAML 가맹을 선택하여 구성

인증 체계의 일부로 로컬 명확성 구성

로컬 명확성을 사용하도록 선택하는 경우 다음 두 가지 단계를 수행해야 합니다.

1. 기본 동작을 통해 또는 Xpath 쿼리를 사용하여 LoginID 를 얻습니다.
2. 기본 동작을 통해 또는 사용자 조회를 정의하여 사용자 저장소에서 사용자를 찾습니다.

참고: Xpath 및 검색 사양 사용은 선택 사항입니다.

LoginID 얻기

다음 두 가지 방법으로 LoginID 를 찾을 수 있습니다.

- LoginID 가 어설션의 NameID 에서 추출되는 기본 동작 사용. 이 옵션에는 구성이 필요하지 않습니다.
- 기본 동작 대신 Xpath 쿼리를 사용하여 LoginID 찾기

Xpath 쿼리를 사용하여 LoginID 를 확인하려면

1. SAML 2.0 인증 체계로 이동합니다.
2. "SAML 2.0 구성"을 클릭합니다.

3. "SAML 2.0 속성" 페이지에 인증 체계가 LoginID 를 얻는 데 사용하는 Xpath 쿼리를 입력합니다. "확인"을 클릭하여 변경 내용을 저장합니다.

   Xpath 쿼리에는 네임스페이스 접두사를 포함할 수 없습니다. 다음은 잘못된 Xpath 쿼리의 예입니다.

   ```
   /saml:Response/saml:Assertion/saml:AuthenticationStatement/
   saml:Subject/saml:NameIdentifier/text()
   ```

   유효한 Xpath 쿼리는 다음과 같습니다.

   ```
   //Response/Assertion/AuthenticationStatement/Subject/
   NameIdentifier/text()
   ```

사용자를 찾도록 사용자 조회 구성

LoginID 를 얻은 후에는 LoginID 를 정책 서버에 전달하는 기본 동작 대신 사용자를 찾도록 사용자 조회를 구성할 수 있습니다.

검색 사양으로 사용자를 찾으려면

1. SAML 2.0 인증 체계로 이동합니다.
2. "SAML 2.0 구성"을 클릭합니다.
3. "사용자 조회" 섹션의 적절한 네임스페이스 필드에 검색 사양을 입력합니다. 검색 사양은 인증 체계가 네임스페이스를 검색하는 데 사용하는 특성을 정의합니다. LoginID 를 나타내는 항목으로 %s 를 사용합니다.

   예를 들어 LoginID 의 값이 user1 이라고 가정합니다. "검색 사양" 필드에서 "Username=%s"를 지정하는 경우 결과 문자열은 Username=user1 입니다. 올바른 인증 기록을 찾기 위해 이 문자열이 사용자 저장소와 비교하여 확인됩니다.
4. "확인"을 클릭하여 구성 변경 내용을 저장합니다.

SAML 가맹을 사용하여 사용자 레코드 찾기(선택 사항)

서비스 공급자 그룹이 가맹을 구성할 수 있습니다. 서비스 공급자를 그룹화하면 페더레이션된 네트워크에서 가맹의 한 구성원과의 관계가 가맹의 모든 구성원과의 관계를 설정하도록 연결이 설정됩니다.

가맹의 모든 서비스 공급자는 단일 프린서펄에 대한 이름 식별자를 공유합니다. 한 아이덴티티 공급자가 사용자를 인증하고 해당 사용자에게 ID 를 할당하면 가맹의 모든 구성원이 동일한 이름 ID 를 사용합니다. 단일 이름 ID 를 사용하면 각 서비스 공급자에 필요한 구성이 줄어듭니다. 또한 프린서펄에 대한 이름 ID 를 하나만 사용하면 아이덴티티 공급자에서 저장소 공간이 절약됩니다.

사용자 명확성을 위해 선택적 Xpath 쿼리 및 검색 사양을 사용할 수 있습니다. 이러한 옵션은 인증 체계의 일부가 아닌 가맹 자체의 일부로 정의됩니다.

참고: 인증 체계 구성에 사용하기 전에 먼저 가맹을 정의하십시오.

가맹을 선택하려면

1. "SAML 2.0 인증 체계" 페이지로 이동합니다.
2. "SAML 2.0 구성"을 클릭합니다.
3. "일반" 설정으로 이동합니다.
4. "사용자 명확성" 섹션의 "SAML 가맹" 드롭다운 필드에서 미리 정의된 가맹을 선택합니다. 이러한 가맹은 아이덴티티 공급자에서 구성됩니다.

SP 에서 싱글 사인온 구성

아이덴티티 공급자와 서비스 공급자 간의 싱글 사인온을 설정하려면 SSO 바인딩을 지정하십시오.

"SSO" 설정을 사용하면 아티팩트 또는 POST 바인딩을 사용하는 싱글 사인온을 구성할 수 있습니다.

싱글 사인온 구성에는 "리디렉션 모드" 설정을 정의하는 단계가 포함됩니다. 리디렉션 모드는 사용 가능한 경우 SiteMinder 가 어설션 특성을 대상 응용 프로그램에 보내는 방법을 지정합니다. 어설션 특성을 HTTP 헤더나 HTTP 쿠키로 보낼 수 있습니다.

HTTP 헤더와 HTTP 쿠키에는 어설션 특성이 초과할 수 없는 크기 제한이 있습니다. 크기 제한은 다음과 같습니다.

- HTTP 헤더의 경우 SiteMinder 는 헤더에 대한 웹 서버 크기 제한까지 헤더에 있는 특성을 보낼 수 있습니다. 헤더당 허용되는 어설션 특성은 하나뿐입니다. 헤더 크기 제한을 확인하려면 해당 웹 서버 설명서를 참조하십시오.
- HTTP 쿠키의 경우 SiteMinder 는 쿠키에 대한 크기 제한까지 쿠키를 보낼 수 있습니다. 각 어설션 특성은 자체 쿠키로 전송됩니다. 쿠키 크기 제한은 브라우저별로 다르고, 해당 제한은 각 특성에만 적용되는 것이 아니라 응용 프로그램에 전달되고 있는 모든 특성에 적용됩니다. 쿠키 크기 제한을 확인하려면 해당 웹 브라우저 설명서를 참조하십시오.

싱글 사인온을 구성하려면

1. SAML 2.0 인증 체계로 이동합니다.
2. "SAML 2.0 구성", "SSO"를 차례로 클릭합니다.
3. "SSO" 필드에 대한 항목을 입력합니다.
4. (선택 사항) 싱글 사인온 작동을 위한 대상 리소스를 지정합니다. 대상은 대상 서비스 공급자 사이트의 요청된 리소스를 지정합니다.

   서비스 공급자는 기본 대상을 사용하지 않아도 됩니다. 싱글 사인온을 시작하는 링크에는 대상을 지정하는 쿼리 매개 변수가 포함될 수 있습니다.

5. "바인딩" 섹션에서 "HTTP-아티팩트"와 "HTTP-POST"를 선택할 수 있습니다.

   "HTTP-POST"는 선택하고 아티팩트는 선택하지 않은 경우 POST 바인딩만 아이덴티티 공급자에서 허용됩니다. 바인딩을 지정하지 않은 경우 기본값은 HTTP-artifact 입니다.

   "HTTP-아티팩트" 바인딩을 선택하는 경우

   - 검색되기 전에 어설션을 저장하도록 세션 서버를 설정합니다 (페이지 107).
   - 백 채널을 구성합니다 (페이지 277). 아티팩트 레졸루션 서비스와의 통신을 보호하는 인증 체계 유형을 선택합니다. 이 서비스는 아이덴티티 공급자에서 어설션을 검색합니다.
   - 선택적으로 각 바인딩에 대해 정수를 인덱스 항목으로 지정합니다.

     여러 끝점이 있는 경우 인덱싱된 끝점을 구성할 수 있습니다. 서비스 공급자가 지정된 끝점 항목을 AuthnRequest 에 쿼리 매개 변수로 포함합니다. AuthnRequest 가 아이덴티티 공급자의 싱글 사인온 서비스에 전송됩니다.

추가 정보:

아티팩트 서비스를 보호하는 인증 체계 구성 (페이지 147)

단일 사용 정책을 적용하여 보안 강화

단일 사용 정책은 SAML 2.0 어설션이 서비스 공급자에서 두 번째 세션을 설정하는 데 재사용되지 않도록 합니다. 이 기능은 POST 바인딩을 통해 도달하는 어설션에 적용됩니다.

참고: 단일 사용 정책 기능은 HTTP-POST 바인딩을 선택할 때 기본적으로 사용되도록 설정되어 있습니다.

어설션을 일회 사용 대상으로 지정하면 싱글 사인온 환경에서 인증 보안을 강화할 수 있습니다. 브라우저에서 공격자는 SiteMinder 세션을 설정하는 데 사용된 SAML 어설션을 획득할 수 있습니다. 그런 다음 공격자가 서비스 공급자의 어설션 소비자 서비스에 어설션을 포스트하여 두 번째 세션을 설정할 수 있습니다. 하지만 어설션이 일회 사용 대상으로 지정된 경우에는 이러한 유형의 위험이 완화됩니다.

SiteMinder 는 만료 데이터를 사용하여 단일 사용 정책을 적용합니다. 만료 데이터는 어설션에 대한 시간 기반 데이터입니다. SAML 2.0 인증 체계는 세션 저장소에 만료 데이터를 저장합니다. 만료 데이터는 SAML 2.0 POST 어설션이 한 번만 사용되는지 확인합니다.

단일 사용 정책의 적용 방식

SAML 2.0 어설션의 유효성 검사가 성공하면 인증 체계가 만료 데이터 테이블에 어설션 데이터를 씁니다. 데이터에는 어설션 ID 키와 만료 시간이 포함됩니다. 정책 서버의 어설션 저장소 관리 스레드가 만료 데이터 테이블에서 만료된 데이터를 삭제합니다.

체계가 어설션 데이터의 유효성을 검사하려고 하는 경우 만료 데이터 항목에 동일한 어설션 ID 키가 있으면 어설션 데이터 쓰기가 실패합니다. 체계가 만료 테이블에 쓸 수 없는 경우 SAML 2.0 인증 체계는 잘못된 어설션과 동일한 방식으로 인증을 거부합니다.

데이터베이스를 사용할 수 없으면 어설션의 단일 사용을 적용할 수 없습니다. 따라서 인증 체계가 요청을 거부하고 어설션이 재사용되지 않습니다.

단일 사용 정책 구성

단일 사용 정책을 구성하려면

1. SAML 2.0 인증 체계로 이동합니다.

   "수정", "SAML 2.0 구성"을 차례로 클릭합니다.

2. "SSO" 탭을 선택합니다.

3. "HTTP-POST" 섹션에서 "단일 사용 정책 적용" 확인란이 기본적으로 선택되어 있습니다.

4. 세션 저장소가 사용되도록 설정합니다.

   세션 저장소 사용에 대한 지침은 *정책 서버 관리 안내서*를 참조하십시오.

추가 정보:

사용자 세션, 어설션 및 만료 데이터 저장 (페이지 107)
단일 사용 정책을 적용하여 보안 강화 (페이지 274)

SSO 에 대한 이름 식별자 만들기 허용

싱글 사인온 요청의 일부로 서비스 공급자는 true 로 설정된 AllowCreate 라는 특성이 포함된 AuthnRequest 를 생성할 수 있습니다. 서비스 공급자는 사용자의 아이덴티티를 가져오려고 합니다. AuthnRequest 를 받으면 아이덴티티 공급자가 어설션을 생성합니다. 아이덴티티 공급자가 적절한 사용자 레코드에서 이름 ID 역할을 하는 어설션 특성을 검색합니다. 아이덴티티 공급자가 NameID 특성에 대한 값을 찾을 수 없으면 영구 식별자가 생성됩니다. "허용/만들기" 기능을 사용하여 식별자를 생성할 수 있습니다.

영구 식별자는 무작위로 생성된 ID 입니다. 아이덴티티 공급자는 이 식별자를 NameID 특성의 값으로 사용하고 어설션에 넣습니다. 그런 다음 아이덴티티 공급자가 어설션을 서비스 공급자에게 반환합니다. 예를 들어 NameID 특성이 telephone 으로 설정된 경우 telephone 에 대한 값이 사용자 레코드에 없으면 NameID 가 무작위로 생성된 식별자로 설정됩니다.

서비스 공급자가 어설션을 받으면 SAML 2.0 인증 체계가 응답을 처리합니다. 그런 다음 체계가 해당 로컬 사용자 저장소에서 사용자 조회를 수행합니다. 서비스 공급자가 사용자 레코드를 찾으면 사용자에게 액세스 권한이 부여됩니다.

아이덴티티 공급자가 고유 식별자를 생성하도록 아이덴티티 공급자에서 "허용/만들기" 기능이 사용되도록 설정하십시오. 아이덴티티 공급자는 이 기능이 사용되도록 설정된 경우에만 식별자를 생성합니다. 고유 식별자가 생성되지 않았다는 항목이 아이덴티티 공급자 로그 파일에 입력된 후 일반적인 어설션 생성 흐름이 계속됩니다.

인증 요청에 "허용/만들기" 특성 포함

아이덴티티 공급자가 이름 ID 에 대한 식별자를 생성하도록 허용하려면 AuthnRequest 메시지에 "허용/만들기" 특성을 포함하십시오.

참고: 아이덴티티 공급자의 관리자가 "허용/만들기" 기능이 사용되도록 설정해야 식별자가 생성됩니다.

다음 단계를 수행하십시오.

1. SAML 2.0 인증 체계로 이동합니다.
2. "SAML 2.0 구성", "SSO"를 차례로 클릭합니다.

3. "IDP 가 새 식별자를 만들도록 허용" 확인란을 선택합니다.
4. "확인"을 클릭합니다.

HTTP-아티팩트 SSO 에 대한 백 채널 구성

싱글 사인온에 대해 HTTP-아티팩트 바인딩을 선택하는 경우 아티팩트 레졸루션 서비스에 대한 백 채널을 보호할 인증 체계를 선택하십시오. 이 서비스는 아이덴티티 공급자에서 어설션을 검색합니다.

백 채널을 구성하려면

1. SAML 2.0 인증 체계로 이동합니다.
2. "SAML 2.0 구성", "암호화 및 서명"을 차례로 클릭합니다.
3. "백 채널" 섹션의 모든 필드에 데이터를 입력합니다.

   중요! 백 채널 인증 체계에 대해 기본 인증을 사용하고 있는 경우 "SP 이름" 필드의 값은 서비스 공급자의 이름입니다. 추가 구성이 필요하지 않습니다. 클라이언트 인증서 인증을 사용하고 있는 경우 "SP 이름" 필드는 인증서 데이터 저장소에 저장된 클라이언트 인증서의 별칭이어야 합니다. SP 는 인증서를 자격 증명으로 사용하여 아티팩트 레졸루션 서비스에 대한 액세스 권한을 얻습니다.
4. "확인"을 클릭하여 구성을 저장합니다.

추가 정보:

백 채널에 대해 클라이언트 인증서 인증이 사용되도록 설정(선택 사항) (페이지 300)

서비스 공급자의 ECP 구성

ECP 를 구성하려면 아이덴티티 공급자와 서비스 공급자에서 해당 기능을 사용하도록 설정하십시오. 다음 절차는 SiteMinder 서비스 공급자에게 해당됩니다.

ECP 에 대한 자세한 내용은 개요 (페이지 223)를 참조하십시오.

다음 단계를 수행하십시오.

1. 서비스 공급자에서 보호된 리소스에 대한 요청을 AuthnRequest 서비스에 전달합니다. URL 의 예는 다음과 같습니다.

   https://*host*:*port*/affwebservices/public/saml2authnrequest

2. 서비스 공급자 측에서 관리 UI 에 로그인합니다.
3. 관련 SAML 2.0 인증 체계 개체를 수정합니다.
4. "체계 설정" 섹션에서 "SAML 2.0 구성"을 클릭합니다.

   해당 체계에 대한 구성 탭이 표시됩니다.

5. "SSO" 탭을 선택합니다.
6. "향상된 클라이언트 및 프록시 프로필" 확인란을 선택하고 "확인"을 클릭합니다.
7. "제출"을 클릭하여 변경 내용을 저장합니다.

이제 SiteMinder 서비스 공급자가 ECP 호출을 처리할 수 있습니다.

참고: 단일 SAML 서비스 공급자 개체가 싱글 사인온 요청에 대한 아티팩트, POST, SOAP 및 PAOS 바인딩을 처리할 수 있습니다. SOAP 및 PAOS 는 ECP 프로필에 대한 바인딩입니다. 아이덴티티 공급자와 서비스 공급자는 요청의 매개 변수를 기준으로 사용되는 바인딩을 확인합니다.

싱글 로그아웃이 사용되도록 설정

SLO(싱글 로그아웃) 프로필을 사용하면 특정 세션 기관이 제공하는 세션 중에서 특정 사용자와 연결된 모든 세션에서 거의 동시에 로그아웃할 수 있습니다. 사용자가 로그아웃을 직접 시작합니다. 세션 기관은 초기에 사용자를 인증한 인증 엔터티입니다. 대부분의 경우 세션 기관은 아이덴티티 공급자입니다.

싱글 로그아웃을 사용하면 권한 없는 사용자가 서비스 공급자의 리소스에 액세스할 수 있도록 열려 있는 세션이 남지 않게 됩니다.

사용자는 서비스 공급자나 아이덴티티 공급자의 링크를 클릭하여 브라우저에서 싱글 로그아웃 서비스를 시작할 수 있습니다. 사용자가 SLO 서블릿을 가리키는 로그아웃 링크를 클릭합니다. 이 서블릿은 페더레이션 웹 서비스의 구성 요소로, 서비스 공급자나 아이덴티티 공급자에서 들어오는 로그아웃 요청과 응답을 처리합니다. 서블릿이 요청이나 응답의 보낸 사람을 몰라도 됩니다. 서블릿은 SiteMinder 세션 쿠키를 사용하여 로그아웃할 세션을 결정합니다.

싱글 로그아웃을 위한 바인딩

싱글 로그아웃 기능은 HTTP-리디렉션 바인딩을 사용하여 메시지를 전송합니다. 이 바인딩은 SAML 프로토콜 메시지가 302 상태 코드 응답인 HTTP 리디렉션 메시지를 사용하여 전송되는 방식을 결정합니다.

싱글 로그아웃 구성

서비스 공급자에서 싱글 로그아웃이 사용되도록 설정하는 경우 서비스 공급자에서 보호된 리소스가 포함된 영역에 대해 영구 세션을 구성하십시오. 관리 UI 에서 영구 세션을 구성하십시오.

싱글 로그아웃을 구성하려면

1. SAML 2.0 인증 체계로 이동합니다.
2. "SAML 2.0 구성", "SLO"를 차례로 클릭합니다.
3. 페이지의 "SLO" 섹션에서 "HTTP-리디렉션" 확인란을 선택합니다. 다른 싱글 로그아웃 설정이 활성화됩니다.
4. 다음 정보에 주의하면서 나머지 필드에 대한 값을 입력합니다.

   유효 기간

   싱글 로그아웃 요청의 유효 시간(초)을 지정합니다. 유효 기간이 만료되면 싱글 로그아웃 응답이 생성됩니다. 응답은 로그아웃을 시작한 엔터티에 전송됩니다. 유효 기간은 싱글 로그아웃 메시지 기간을 계산하기 위한 차이 시간에 따라서도 달라집니다.

"SLO 위치 URL", "SLO 응답 위치 URL" 및 "SLO 확인 URL"

이러한 필드에 대한 항목은 https:// 또는 http://로 시작해야 합니다.

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

싱글 로그아웃이 시작된 후 사용자 세션이 아이덴티티 공급자와 모든 서비스 공급자 사이트에서 제거됩니다. 그런 다음 페더레이션 웹 서비스가 사용자를 로그아웃 확인 페이지로 리디렉션합니다.

추가 정보:

사용자 세션, 어설션 및 만료 데이터 저장 (페이지 107)

서비스 공급자의 디지털 서명 옵션

SAML 2.0 인증 체계 구성에는 다음 트랜잭션에 대한 디지털 서명 옵션이 포함됩니다.

- 인증 요청
- 싱글 로그아웃 요청 및 응답
- 아티팩트 확인 메시지 - 어설션을 검색하기 위한 SAML 아티팩트 확인의 경우
- 특성 쿼리 - 특성 기관(IdP)과 SAML 요청자(SP) 간에 발생하는 권한 부여의 경우

기본적으로 서명 처리는 사용되도록 설정되어 있는데, 이는 SAML 2.0 사양에 따라 서명이 필요하기 때문입니다. 초기 페더레이션 설정을 디버깅하는 *경우에만* "서명 처리 사용 안 함" 옵션을 선택하여 서비스 공급자에 대한 모든 서명 처리(서명 및 서명 확인)가 일시적으로 사용되지 않도록 설정할 수 있습니다. 디버깅이 완료된 후 서명 처리가 다시 사용되도록 설정하십시오.

중요! 프로덕션 환경에서 서명 처리가 사용되지 않도록 설정하면 필수 보안 기능이 사용되지 않도록 설정됩니다.

서명 옵션을 지정하려면

1. SAML 2.0 인증 체계로 이동합니다.
2. "SAML 2.0 구성", "암호화 및 서명"을 차례로 클릭합니다.
3. "D-서명 정보" 섹션의 필드에 데이터를 입력합니다. 다음 정보에 주의하십시오.
   - HTTP-POST(싱글 사인온)의 경우 포스트되는 어설션의 서명 유효성을 검사하는 인증서에 대한 정보를 입력합니다. "발급자 DN"과 "일련 번호"는 IdP 가 어설션에 서명하는 데 사용한 개인 키에 해당하는 인증서를 식별합니다.

     "발급자 DN" 필드에 입력하는 값은 인증서 데이터 저장소에 있는 인증서의 발급자 DN 과 일치해야 합니다.
   - HTTP-리디렉션(싱글 로그아웃)의 경우 SLO 요청의 서명 유효성을 검사하는 인증서에 대한 정보를 입력합니다.
4. 대화 상자의 "서명 처리" 섹션에 있는 설정을 완료합니다.
5. HTTP-아티팩트 싱글 사인온의 경우에만 백 채널 설정을 구성합니다.
6. "확인"을 클릭합니다.

싱글 사인온에 대한 어설션 암호화 요구 사항 적용

암호화 기능은 인증 체계가 암호화된 어설션이나 어설션에 있는 이름 ID 만 처리하도록 지정합니다.

보안을 강화하기 위해 아이덴티티 공급자가 이름 ID, 사용자 특성 또는 전체 어설션을 암호화할 수 있습니다. 암호화를 수행하면 어설션을 전송할 때 보호 수준이 강화됩니다. 아이덴티티 공급자에서 암호화가 사용되도록 설정한 경우 인증서(공개 키)가 데이터를 암호화하는 데 사용됩니다. 어설션이 서비스 공급자에 도달하면 연결된 개인 키를 사용하여 암호화된 데이터의 암호가 해독됩니다.

세션 공급자에서 암호화를 구성하는 경우 어설션에는 암호화된 이름 ID 나 어설션이 포함되어야 합니다. 그렇지 않으면 서비스 공급자가 어설션을 거부합니다.

SSO 에 대한 암호화 설정

어설션에 대한 암호화 요구 사항을 적용할 수 있습니다.

암호화 요구 사항을 적용하려면

1. SAML 2.0 인증 체계로 이동합니다.
2. "SAML 2.0 구성", "암호화 및 서명"을 차례로 클릭합니다.

   암호화 및 서명 설정 페이지가 표시됩니다.
3. 암호화된 이름 ID 를 요구하려면 "암호화된 이름 ID 필요" 확인란을 선택합니다.
4. 암호화된 어설션을 요구하려면 "암호화된 어설션 필요" 확인란을 선택합니다.

   이름 ID 와 어설션을 선택할 수 있습니다.
5. (선택 사항) 아이덴티티 공급자로부터 받은 어설션에 있는 모든 암호화된 데이터의 암호를 해독하는 개인 키에 대한 별칭을 지정합니다.
6. "확인"을 클릭하여 변경 내용을 저장합니다.

암호화 요구 사항이 없는 경우 서비스 공급자는 암호화되었거나 ClearText 로 된 이름 ID 와 어설션을 수락합니다.

사용자 지정 SAML 2.0 인증 체계 만들기(선택 사항)

기존 SAML 2.0 인증 템플릿 대신 SiteMinder 인증 API 로 작성된 사용자 지정 SAML 2.0 체계를 사용할 수 있습니다.

기본 인증 체계 페이지의 "체계 설정" 섹션에는 "라이브러리" 필드가 있습니다. 이 필드에는 SAML 아티팩트 인증을 처리하는 공유 라이브러리의 이름이 있습니다. 사용자 지정 인증 체계가 없으면 이 값을 변경하지 마십시오.

HTML 양식 인증에 대한 기본 공유 라이브러리는 smauthhtml 입니다.

서비스 공급자의 IDP 검색 구성

IPD(아이덴티티 공급자 검색) 프로필이 제공하는 공통 검색 서비스를 사용하면 서비스 공급자가 인증을 위해 고유 IdP 를 선택할 수 있습니다. 네트워크에 있는 모든 사이트가 아이덴티티 공급자 검색 서비스와 상호 작용하도록 파트너 간의 사전 비즈니스 계약이 설정되어 있습니다.

이 프로필은 어설션을 제공하는 파트너가 둘 이상 있는 페더레이션된 네트워크에 유용합니다. 서비스 공급자는 자신이 특정 사용자에 대한 인증 요청을 보내는 아이덴티티 공급자를 결정할 수 있습니다.

IdP 검색 프로필은 두 페더레이션된 파트너에 공통적인 쿠키 도메인을 사용하여 구현됩니다. 약정된 도메인의 쿠키에는 사용자가 방문한 IdP 목록이 포함되어 있습니다.일반 도메인 쿠키를 검색하려면 SP 가 사용자를 IdP 검색 서비스로 리디렉션해야 합니다. 쿠키에는 사용자가 이미 방문한 IdP 목록이 포함됩니다. 이 목록에서 SP 는 올바른 아이덴티티 공급자를 선택하고 AuthnRequest 를 보냅니다.

참고: 인증을 요구하는 사용자는 이전에 아이덴티티 공급자를 방문하여 인증을 받은 상태여야 합니다.

IDP 검색은 다음과 같이 발생합니다.

1. 브라우저가 SP 의 사이트 선택 페이지를 요청합니다.

   이 사이트 선택 페이지는 IDP 검색 서비스 URL 을 인식하고 있습니다.

2. 사이트 선택 페이지가 사용자를 일반 도메인의 IDP 검색 서비스 URL 로 리디렉션합니다. 리디렉션 URL 에는 일반 도메인 쿠키를 원한다는 쿼리 매개 변수가 포함됩니다.

3. IDP 검색 서비스가 일반 도메인 쿠키의 값을 검색하여 쿼리 매개 변수로 설정합니다. 그런 다음 서비스가 사용자를 SP 의 사이트 선택 페이지로 다시 리디렉션합니다.

4. SP 가 IdP ID(사용자가 이전에 인증을 받은 URI)로 사이트 선택 페이지를 채웁니다.

5. 사용자가 IdP 를 선택하여 사용자 인증을 수행합니다.

추가 정보:

IdP 에서 아이덴티티 공급자 검색 구성 (페이지 256)

SP 에서 아이덴티티 공급자 검색 구성

서비스 공급자에서 아이덴티티 공급자 검색 프로필을 구성하는 과정에는 관리 UI 가 포함되지 않습니다. 프로필은 아이덴티티 공급자의 관리 UI 에서 사용되도록 설정됩니다.

이 프로세스의 첫 번째 단계는 사이트 선택 페이지를 만드는 것입니다. 정책 서버는 SP 가 사용할 수 있는 IdPDiscovery.jsp 라는 샘플 사이트 선택 페이지와 함께 제공됩니다.

사이트 선택 페이지의 첫 번째 링크는 한 도메인에서 일반 도메인의 IdP 검색 서비스로 브라우저를 리디렉션합니다. 서비스가 **_saml_idp** 라는 일반 도메인 쿠키를 가져옵니다. 요청을 받는 경우 SP 의 IdP 검색 서비스가 일반 도메인 쿠키를 가져옵니다. 서비스가 링크에 일반 도메인 쿠키를 쿼리 매개 변수로 추가합니다. 그런 다음 서비스가 사용자를 일반 도메인의 IdPDiscovery.jsp 사이트 선택 페이지로 다시 리디렉션합니다.

기본적으로 IdPDiscovery.jsp 페이지에는 공용 쿠키에서 추출하는 IdP 에 대한 ID 목록만 표시됩니다. 목록은 정적이고, 연결된 IdP 와의 통신을 시작하는 목록과 연결된 HTML 링크가 없습니다.

SP 에서 IdP 검색을 구성하려면

1. SP 의 IdP 검색 서비스에서 일반 도메인 쿠키를 요청하는 사이트 선택 페이지를 생성합니다.

   정책 서버는 SP 가 IdP 검색을 구현하는 데 사용할 수 있는 IdPDiscovery.jsp 라는 샘플 사이트 선택 페이지와 함께 제공됩니다. 이 페이지는 다음 디렉터리에서 찾을 수 있습니다.

   web_agent_home/affwebservices/public

2. SP 사이트에 대한 샘플 페이지에서 다음 링크를 편집합니다. 링크의 첫 번째 부분에서는 saml2idp 쿠키가 있는 일반 도메인을 지정합니다. 링크의 두 번째 부분에서는 IdPDiscovery.jsp 가 있는 일반 도메인을 지정합니다.

   예를 들면 다음과 같습니다.

   Retrieve idp discovery cookie from IPD Service

   사용자가 대상 사이트 선택 페이지가 있는 일반 도메인으로 다시 리디렉션되면 이제 해당 사용자가 공용 쿠키를 갖게 됩니다.

3. (선택 사항) 각 IdP 에 대해 HTML 링크를 표시하도록 IdPDiscovery.jsp 사이트 선택 페이지를 편집합니다. 각 링크는 싱글 사인온을 시작하도록 IdP 에 대한 AuthnRequest 를 트리거합니다. 기본적으로 IdPDiscovery.jsp 페이지에는 공용 쿠키에서 추출하는 IdP 에 대한 ID 목록만 표시됩니다.
4. 편집된 사이트 선택 페이지를 사용하여 IdP 검색을 테스트합니다.

IdP 검색이 제대로 작동하는 경우 사이트 선택 페이지에는 선택할 IdP 목록이 표시됩니다.

공격으로부터 IdP 검색 대상 보안

SiteMinder 아이덴티티 공급자 검색 서비스가 일반 도메인 쿠키에 대한 요청을 받는 경우 요청에는 IPDTarget 이라는 쿼리 매개 변수가 포함되어 있습니다. 이 쿼리 매개 변수는 검색 서비스가 요청을 처리한 후 리디렉션해야 하는 URL 을 나열합니다.

IdP 의 경우 IPDTarget 은 SAML 2.0 싱글 사인온 서비스입니다. SP 의 경우 대상은 일반 도메인 쿠키를 사용하려고 요청하는 응용 프로그램입니다.

보안 공격으로부터 IPDTarget 쿼리 매개 변수를 보호하는 것이 좋습니다. 권한 없는 사용자가 이 쿼리 매개 변수에 임의의 URL 을 넣을 수 있습니다. 그러면 URL 로 인해 악의적인 사이트로 리디렉션될 수 있습니다.

공격으로부터 쿼리 매개 변수를 보호하려면 "에이전트 구성 개체" 설정 **ValidFedTargetDomain** 을 구성하십시오. ValidFedTargetDomain 매개 변수는 페더레이션 환경에 대해 유효한 도메인을 모두 나열합니다.

참고: ValidFedTargetDomain 설정은 웹 에이전트가 사용하는 ValidTargetDomain 설정과 유사하지만 이 설정은 구체적으로 페더레이션에 대해 정의됩니다.

IPD 서비스가 IPDTarget 쿼리 매개 변수를 검사합니다. 그런 다음 서비스는 쿼리 매개 변수가 지정하는 URL 의 도메인을 획득합니다. IPD 서비스가 이 도메인과 ValidFedTargetDomain 매개 변수에 지정된 도메인 목록을 비교합니다. URL 도메인이 ValidFedTargetDomain 에 구성된 도메인 중 하나와 일치하면 IPD 서비스가 사용자를 지정된 URL 로 리디렉션합니다.

일치하는 도메인이 없으면 IPD 서비스가 사용자 요청을 거부하고 브라우저를 통해 "403 사용 권한 없음" 오류가 수신됩니다. 또한 FWS 추적 로그와 affwebservices 로그에서 오류가 보고됩니다. 이러한 메시지는 IPDTarget 의 도메인이 유효한 페더레이션 대상 도메인으로 정의되지 않았음을 나타냅니다.

ValidFedTargetDomain 설정을 구성하지 않으면 서비스가 유효성 검사를 수행하지 않은 상태로 사용자를 대상 URL 로 리디렉션합니다.

메시지 소비자 플러그인으로 어설션 처리 사용자 지정

메시지 소비자 플러그인은 메시지 소비자 플러그인을 구현하는 Java 프로그램입니다. 이 플러그인을 통해 어설션 거부, 상태 코드 반환 등의 어설션 처리를 위한 사용자 고유의 비즈니스 논리를 구현할 수 있습니다. 이 추가 처리는 어설션의 표준 처리와 함께 작동합니다.

참고: 인증 및 명확성의 상태 코드에 대한 자세한 내용은 *SiteMinder Programming Guide for Java*(SiteMinder Java 프로그래밍 안내서)를 참조하십시오.

인증 중에 SiteMinder 는 먼저 사용자를 해당 로컬 사용자 저장소에 매핑하여 어설션을 처리하려고 합니다. 사용자를 찾을 수 없는 경우 SiteMinder 는 메시지 소비자 플러그인의 postDisambiguateUser 메서드를 호출합니다.

플러그인이 사용자를 찾은 경우 SiteMinder 는 인증의 두 번째 단계로 진행합니다. 플러그인이 사용자를 로컬 사용자 저장소에 매핑할 수 없는 경우에는 UserNotFound 오류가 반환됩니다. 플러그인이 선택적으로 리디렉션 URL 기능을 사용할 수 있습니다. 소비자 플러그인이 없는 경우 리디렉션 URL 은 SAML 인증 체계가 생성하는 오류를 기반으로 합니다.

두 번째 인증 단계에서 SiteMinder 는 플러그인이 구성된 경우 메시지 소비자 플러그인의 postAuthenticateUser 메서드를 호출합니다. 메서드가 성공하는 경우 SiteMinder 는 사용자를 요청된 리소스로 리디렉션합니다. 메서드가 실패하는 경우 사용자를 실패 페이지에 보내도록 플러그인을 구성할 수 있습니다. 실패 페이지는 인증 체계 구성으로 지정할 수 있는 리디렉션 URL 중 하나일 수 있습니다.

메시지 소비자 플러그인에 대한 자세한 내용은 다음과 같이 찾을 수 있습니다.

- 참조 정보(메서드 서명, 매개 변수, 반환 값, 데이터 형식)와 UserContext 클래스에 대한 생성자는 *Java Developer Reference*(Java 개발자 참조서)에 나와 있습니다. MessageConsumerPlugin 인터페이스를 참조하십시오.
- 인증 및 권한 부여 API 에 대한 개요와 개념 정보는 *SiteMinder Programming Guide for Java*(SiteMinder Java 프로그래밍 안내서)를 참조하십시오.

플러그인을 구성하려면

1. 아직 설치하지 않은 경우 SiteMinder SDK 를 설치합니다.
2. SiteMinder SDK 의 일부인 MessageconsumerPlugin.java 인터페이스를 구현합니다.
3. 메시지 소비자 플러그인 구현 클래스를 배포합니다.
4. 관리 UI 에서 메시지 소비자 플러그인이 사용되도록 설정합니다.

MessageConsumerPlugin 인터페이스 구현

MessageConsumerPlugin.java 인터페이스를 구현하여 사용자 지정 메시지 소비자 플러그인을 생성하십시오. 다음 절차에는 구현 클래스에 대한 최소 요구 사항이 나열되어 있습니다.

다음 단계를 수행하십시오.

1. 매개 변수가 포함되지 않은 공개 기본 생성자 메서드를 제공합니다.
2. 상태 비저장 구현이 되도록 코드를 제공합니다. 여러 스레드가 단일 플러그인 클래스를 사용할 수 있어야 합니다.

3. 인터페이스에서 요구 사항을 충족할 메서드를 구현합니다.

   MessageConsumerPlugin 에는 다음 네 가지 메서드가 포함됩니다.

   init()

   플러그인에 필요한 초기화 절차를 모두 수행합니다. SiteMinder 는 플러그인이 로드될 때 각 플러그인 인스턴스에 대해 한 번씩 이 메서드를 호출합니다.

   release()

   플러그인에 필요한 런다운 절차를 모두 수행합니다. SiteMinder 는 SiteMinder 가 종료될 때 각 플러그인 인스턴스에 대해 한 번씩 이 메서드를 호출합니다.

   postDisambiguateUser()

   인증 체계가 사용자 명확성 처리를 수행할 수 없을 때 해당 처리를 제공합니다. 또는 이 메서드가 새 페더레이션 사용자에 대한 데이터를 사용자 저장소에 추가할 수 있습니다. 이 메서드는 암호 해독된 어설션을 수신합니다. 암호 해독된 어설션은 플러그인에 전달된 속성 맵의 "_DecryptedAssertion" 키 아래에 추가됩니다.

   postAuthenticateUser()

   정책 서버 처리 성공 여부와 관계없이 최종 어설션 처리 결과를 확인하기 위한 추가 코드를 제공합니다.

SiteMinder 는 다음과 같은 메시지 소비자 플러그인 클래스 샘플을 제공합니다.

installation_home\sdk\samples\messageconsumerplugin 의 MessageConsumerPluginSample.java

installation_home\sdk\samples\authextensionsaml20 의 MessageConsumerSAML20.java

메시지 소비자 플러그인 배포

MessageConsumerPlugin 인터페이스에 대한 구현 클래스를 코드화했으면 해당 구현 클래스를 컴파일하고 SiteMinder 가 실행 파일을 찾을 수 있는지 확인하십시오.

메시지 소비자 플러그인을 배포하려면

1. MessageConsumerPlugin Java 파일을 컴파일합니다. 이 파일을 컴파일하려면 정책 서버와 함께 설치되는 다음 종속 라이브러리가 필요합니다.

   installation_home\siteminder\bin\jars\SmJavaApi.jar

   SmJavaApi.jar 의 동일한 복사본이 SiteMinder SDK 와 함께 설치됩니다. 이 파일은 *installation_home*\sdk\java\SmJavaApi.jar 디렉터리에 있습니다.

   개발 시 두 파일 중 아무 파일이나 사용할 수 있습니다.

2. 폴더나 jar 파일에서 플러그인 클래스를 사용할 수 있는 경우 JVMOptions.txt 파일에서 -Djava.class.path 값을 수정합니다. 이 단계를 수행하면 수정된 클래스 경로를 사용하여 플러그인 클래스를 로드할 수 있습니다. *installation_home*\siteminder\config 디렉터리에서 JVMOptions.txt 파일을 찾습니다.

   참고: 기존 xerces.jar, xalan.jar 또는 SmJavaApi.jar 의 클래스 경로를 수정하지 마십시오.

3. 정책 서버를 다시 시작하여 최신 버전의 MessageConsumerPlugin 을 선택합니다. 이 단계는 플러그인 Java 파일이 다시 컴파일될 때마다 필요합니다.

4. 플러그인이 사용되도록 설정합니다.

SAML 2.0 에 대해 메시지 소비자 플러그인이 사용되도록 설정

메시지 소비자 플러그인을 작성하고 컴파일한 후 관리 UI 에서 설정을 구성하여 플러그인이 사용되도록 설정하십시오. UI 설정은 SiteMinder 에게 플러그인을 찾을 수 있는 위치를 알려 줍니다.

플러그인을 배포 (페이지 178)할 때까지 플러그인 설정을 구성하지 마십시오.

메시지 소비자 플러그인이 사용되도록 설정하려면

1. 관리 UI 에 로그온합니다.
2. "SAML 2.0 인증 체계" 대화 상자로 이동합니다.
3. "고급"을 클릭합니다.
4. "메시지 소비자 플러그인" 섹션의 다음 필드에 데이터를 입력합니다.

   전체 Java 클래스 이름

   플러그인에 대한 Java 클래스 이름을 지정합니다. 예를 들어 SiteMinder SDK 에 포함된 샘플 클래스는 다음과 같습니다.

   com.ca.messageconsumerplugin.MessageConsumerPluginSample

   매개 변수

   "전체 Java 클래스 이름" 필드에서 지정한 플러그인에 전달되는 매개 변수 문자열을 지정합니다.

   관리 UI 에서 플러그인을 구성하는 대신 정책 관리 API(C 또는 Perl)를 사용하여 IdpPluginClass 와 IdpPluginParameters 를 설정할 수 있습니다.
5. 정책 서버를 다시 시작합니다.

SAML 특성을 HTTP 헤더로 제공

어설션 응답이 특성을 어설션에 포함할 수 있습니다. 이러한 특성을 HTTP 헤더 변수로 제공하면 클라이언트 응용 프로그램에서 해당 특성을 사용하여 세부적인 액세스 제어를 구현할 수 있습니다.

특성을 HTTP 헤더에 포함하여 얻을 수 있는 이점은 다음과 같습니다.

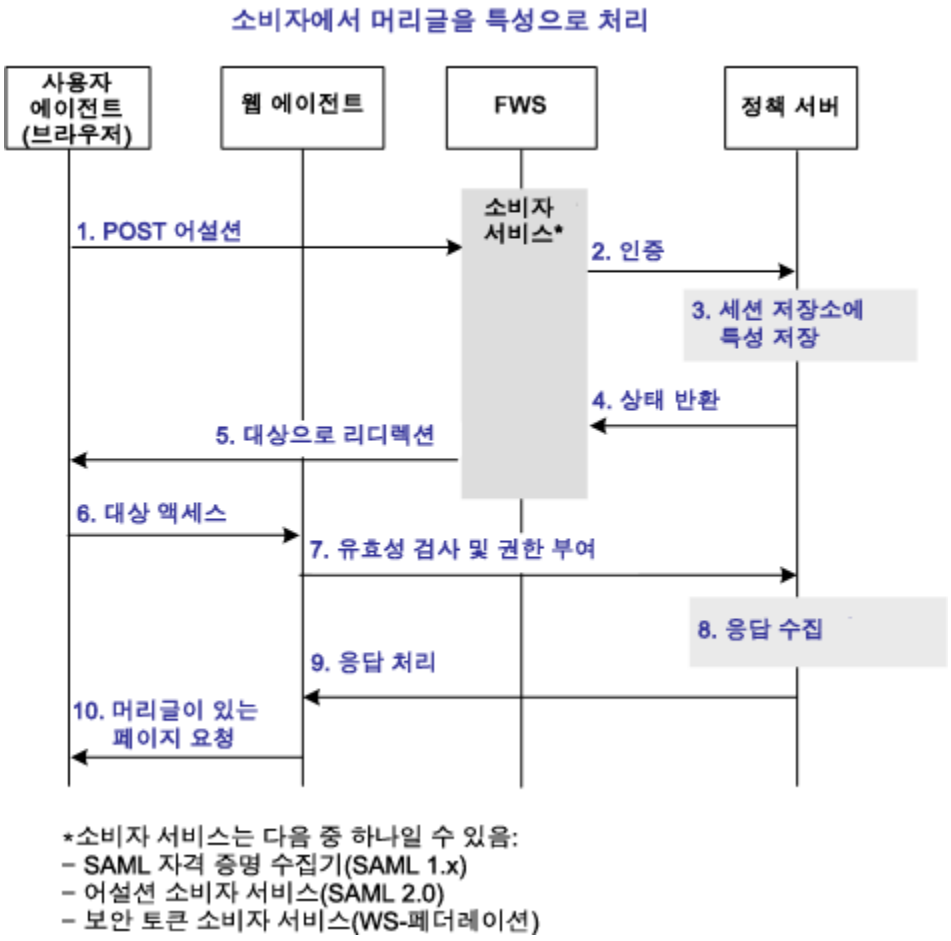
- HTTP 헤더가 영구적이지 않습니다. 즉, HTTP 헤더가 포함된 요청이나 응답 내에서만 표시됩니다.
- SiteMinder 웹 에이전트가 제공한 HTTP 헤더가 브라우저에 표시되지 않으므로 보안 문제가 줄어듭니다.

참고: HTTP 헤더에는 특성이 초과할 수 없는 크기 제한이 있습니다. SiteMinder 는 헤더에 대한 웹 서버 크기 제한까지 헤더에 있는 특성을 보낼 수 있습니다. 헤더당 허용되는 어설션 특성은 하나뿐입니다. 헤더 크기 제한을 확인하려면 해당 웹 서버 설명서를 참조하십시오.

SAML 특성을 HTTP 헤더로 처리하기 위한 사용 사례

인증 중에 일련의 SAML 특성이 어설션에서 추출되어 HTTP 헤더로 제공됩니다. 권한 부여 프로세스 중에 이러한 헤더가 고객 응용 프로그램에 반환됩니다.

다음 순서도에서는 런타임 시 이벤트 순서를 보여 줍니다.



참고: SPS 페더레이션 게이트웨이가 페더레이션 웹 서비스 응용 프로그램 기능을 제공하기 위해 웹 에이전트 및 웹 에이전트 옵션 팩을 대체할 수 있습니다. 흐름도에서 웹 에이전트 블록은 SPS 페더레이션 게이트웨이에 포함된 웹 에이전트입니다. SPS 페더레이션 게이트웨이 설치 및 구성에 대한 자세한 내용은 *Secure Proxy Server Administration Guide*(보안 프록시 서버 관리 안내서)를 참조하십시오.

특성을 HTTP 헤더로 처리하기 위한 이벤트 순서는 다음과 같습니다.

1. 어설션이 어설션 당사자 측에서 생성된 후 해당 어설션이 신뢰 당사자의 적절한 소비자 서비스에 전송됩니다. 전송 메커니즘(POST 또는 아티팩트 또는 WS-페더레이션)은 무관합니다.

   참고: 소비자 서비스는 SAML 자격 증명 수집기(SAML 1.x), 어설션 소비자 서비스(SAML 2.0) 또는 보안 토큰 소비자 서비스(WS-페더레이션)일 수 있습니다.
2. 소비자 서비스가 해당 로컬 정책 서버를 호출하여 구성된 인증 체계를 통해 어설션으로 사용자를 인증합니다.
3. 인증 체계 리디렉션 모드 매개 변수가 PersistAttributes 로 설정된 경우 정책 서버가 세션 저장소에 있는 특성을 세션 변수로 캐시합니다.
4. 인증 결과가 소비자 서비스에 반환됩니다.
5. 소비자 서비스가 브라우저를 보호된 대상 리소스로 리디렉션합니다.
6. 브라우저가 대상 리소스 액세스를 시도합니다.
7. 웹 에이전트가 정책 서버를 호출하여 사용자 세션의 유효성을 검사하고 사용자에게 대상 리소스에 대한 액세스 권한이 부여되었는지 확인합니다.
8. 정책 서버가 구성된 응답별로 특성을 검색합니다.
9. 정책 서버가 응답을 처리하고 특성을 웹 에이전트에 보냅니다.
10. 웹 에이전트가 필요에 따라 HTTP 헤더를 설정합니다.

특성을 HTTP 헤더로 제공하기 위한 구성 개요

세션 저장소에 캐시된 SAML 특성을 검색하여 HTTP 헤더로 제공하려면 여러 구성 단계가 필요합니다.

다음 단계를 수행하십시오.

1. SAML 인증 체계에 대한 리디렉션 모드로 "PersistAttributes"를 선택합니다. 그러면 SAML 특성이 HTTP 헤더로 반환될 수 있습니다.
2. 대상 리소스가 포함된 영역에 대해 권한 부여 규칙을 구성합니다.
3. 대상 리소스를 보호하는 영역에서 "PersistentRealm"을 설정합니다.

4. 헤더로 제공할 SAML 특성 각각에 대해 활성 응답 유형을 사용하는 응답을 구성합니다.
5. 권한 부여 규칙과 활성 응답을 바인딩하여 특성을 HTTP 헤더로 사용하도록 구현하는 정책을 생성합니다.

SAML 특성을 저장하도록 리디렉션 모드 설정

신뢰 당사자가 SAML 어설션으로 사용자를 인증한 후 SAML 특성이 세션 저장소에 기록됩니다. 그런 다음 브라우저가 대상 리소스로 리디렉션됩니다.

특성 데이터와 함께 브라우저를 리디렉션하려면

1. 관리 UI 에 로그인합니다.
2. SAML 인증 체계의 구성 페이지로 이동합니다.
3. "리디렉션 모드" 매개 변수를 "특성 유지"로 설정합니다. 다음과 같이 "리디렉션 모드" 필드를 찾습니다.

   SAML 1.x

   "리디렉션 모드"는 기본 구성 페이지의 "체계 설정" 섹션에 있습니다.

   SAML 2.0

   "SAML 2.0 구성", "SSO"를 차례로 클릭합니다. "리디렉션 모드"는 페이지의 "SSO" 섹션에 있습니다.

   WS-페더레이션

   "WS-페더레이션 구성", "SAML 프로필"을 차례로 클릭합니다. "리디렉션 모드"는 페이지의 "SSO" 섹션에 있습니다.
4. "제출"을 클릭하여 변경 내용을 저장합니다.

이제 리디렉션 모드가 특성 데이터를 전달하도록 설정되었습니다.

사용자의 유효성을 검사하기 위한 권한 부여 규칙 만들기

보호된 대상 리소스가 포함된 영역의 경우 세션 저장소에서 SAML 특성을 검색하기 위한 규칙을 생성하십시오.

규칙은 권한 부여 이벤트(onAccessAccept)를 기반으로 합니다. 사용자는 FWS 응용 프로그램에서 이미 인증되었습니다. 웹 에이전트는 사용자를 다시 인증하고 HTTP 헤더를 전달할 수 없습니다. 특성 검색은 권한 부여 단계에서 발생합니다.

영역에 대한 OnAccessAccept 규칙을 생성하려면

1. 관리 UI 에 로그온합니다.
2. "정책", "도메인", "영역"으로 이동합니다.
3. 대상 리소스가 포함된 영역을 선택합니다.
4. "규칙" 섹션에서 "만들기"를 클릭합니다.

   "규칙 만들기" 페이지가 표시됩니다.
5. 이름과 설명(선택 사항)을 입력합니다.
6. "리소스" 필드에 별표(*)를 입력합니다.
7. "작업" 섹션에서 "권한 부여 이벤트"와 "OnAccessAccept"를 선택합니다.
8. "허용/거부 및 사용/사용 안 함" 섹션에서 "사용"을 선택합니다.
9. "확인"을 클릭하여 규칙을 저장합니다.

이제 보호된 리소스가 포함된 영역에 대한 권한 부여 규칙이 정의되었습니다.

특성을 HTTP 헤더로 보내기 위한 응답 구성

SAML 특성을 웹 에이전트에 HTTP 헤더로 보내는 응답을 구성하십시오. 그러면 웹 에이전트가 응답을 처리하고 헤더 변수를 클라이언트 응용 프로그램에 제공합니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그온합니다.
2. "정책", "도메인", "도메인"으로 이동합니다.
3. 대상 리소스에 대한 도메인을 선택하고 "수정"을 클릭합니다.

4. "응답" 탭을 선택합니다.
5. "만들기"를 클릭합니다.

   "응답" 대화 상자가 열립니다.
6. 이름을 입력합니다.
7. 에이전트 유형이 SiteMinder 웹 에이전트인지 확인합니다.
8. "응답 특성 만들기"를 클릭합니다.

   "응답 특성" 대화 상자가 열립니다.
9. "특성" 필드에서 "WebAgent-HTTP-Header-Variable"을 선택합니다.
10. "특성 종류"에서 "활성 응답"을 선택합니다.
11. 다음과 같이 필드에 데이터를 입력합니다.

    변수 이름

    원하는 헤더 변수 이름을 지정합니다. 사용자가 이 이름을 할당합니다.

    라이브러리 이름

    smfedattrresponse

    이 값은 이 필드에 대한 항목이어야 합니다.

    함수 이름

    getAttributeValue

    이 값은 이 필드에 대한 항목이어야 합니다.

    매개 변수

    어설션에 나타나는 대로 특성 이름을 지정합니다.

    사용자와 페더레이션된 파트너 간의 계약에 따라 어설션에 있는 특성이 결정됩니다.
12. "확인"을 클릭하여 특성을 저장합니다.
13. HTTP 헤더 변수가 될 특성 각각에 대해 절차를 반복합니다. 단일 응답에 대해 여러 특성을 구성할 수 있습니다.

    "응답" 탭으로 돌아갑니다. 생성한 특성이 "특성 목록" 섹션에 나열됩니다.

14. "확인"을 클릭하여 응답을 저장합니다.

    "응답" 탭으로 돌아갑니다.

15. "제출"을 클릭하여 도메인을 저장합니다.

응답이 HTTP 헤더가 될 특성을 웹 에이전트에 보냅니다.

특성을 HTTP 헤더로 구현하기 위한 정책 만들기

SAML 특성을 HTTP 헤더로 사용하도록 구현하려면 정책에서 권한 부여 이벤트 규칙과 활성 응답을 함께 그룹화하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그온합니다.
2. "정책", "도메인", "도메인"으로 이동합니다.
3. 대상 리소스가 포함된 도메인을 선택하고 "수정"을 클릭합니다.
4. "정책" 탭을 선택하고 "정책" 섹션에서 "만들기"를 클릭합니다.

   "정책 만들기" 대화 상자가 열립니다.

5. "이름" 필드에 설명이 포함된 이름을 입력합니다.
6. "사용자" 탭에서 보호된 리소스에 액세스할 수 있는 사용자를 선택합니다.
7. "규칙" 탭에서 이전에 생성한 권한 부여 규칙을 추가합니다.
8. 권한 부여 규칙을 선택하고 "응답 추가"를 클릭합니다.

   "사용 가능한 응답" 대화 상자가 열립니다.

9. 이전에 생성한 활성 응답을 선택하고 "확인"을 클릭합니다.

   "규칙" 탭으로 돌아갑니다. 권한 부여 규칙과 함께 응답이 나타납니다.

10. "제출"을 클릭하여 정책을 저장합니다.

SAML 특성이 HTTP 헤더로 사용되도록 설정하는 정책이 완성되었습니다.

실패한 SAML 2.0 인증에 대한 리디렉션 URL 지정

싱글 사인온 트랜잭션 중에 서비스 공급자가 사용자를 인증할 수 없으면 해당 사용자가 추가 처리를 위해 사용자 지정된 URL 로 리디렉션될 수 있습니다.

실패한 인증에 대해 여러 선택적 리디렉션 URL 을 구성할 수 있습니다. 어설션이 잘못된 경우 리디렉션 URL 을 통해 사용자 리디렉션을 세부적으로 제어할 수 있습니다. 예를 들어 사용자 디렉터리에서 사용자를 찾을 수 없는 경우 사용자를 찾을 수 없음 리디렉션 URL 을 지정하십시오. 이 URL 은 사용자를 등록 페이지로 보낼 수 있습니다.

다음 URL 을 구성할 수 있습니다.

- 상태 리디렉션 URL
- HTTP 오류 리디렉션 URL

참고: 리디렉션 URL 구성은 필수 사항이 아닙니다.

일부 리디렉션 URL 은 다음과 같은 특정 상태 조건에 적용됩니다. 이러한 조건에는 사용자를 찾을 수 없음, 싱글 사인온 메시지가 잘못됨, 사용자 자격 증명이 수락되지 않음 등이 포함됩니다. 기타 리디렉션 URL 은 HTTP 500, 400, 405 및 403 오류 조건을 처리합니다. 이러한 조건이 하나라도 발생하는 경우 리디렉션 URL 은 추가 작업을 위해 사용자를 응용 프로그램이나 사용자 지정된 오류 페이지로 보낼 수 있습니다.

이러한 사용자 지정된 URL 로의 리디렉션은 아이덴티티 공급자에 대한 충분한 정보가 서비스 공급자에게 제공되는 경우에만 발생할 수 있습니다. 예를 들어 요청 중에 인증서 정보를 검색할 때 문제가 있는 경우 사용자가 지정된 서버 오류 URL 로 리디렉션됩니다. 하지만 요청에 잘못된 IdP ID 가 포함된 경우에는 리디렉션이 발생하지 않고 HTTP 오류 코드 400 이 브라우저에 반환됩니다.

선택적 리디렉션 URL 을 구성하려면

1. 수정할 SAML 2.0 인증 체계로 이동합니다.
2. "SAML 2.0 구성", "고급"을 차례로 선택합니다.

3. "상태 리디렉션 URL 및 모드" 섹션의 필드 중 하나 이상에 대한 URL 을 입력합니다.

   필드 설명을 보려면 "도움말"을 클릭하십시오.

   페더레이션 웹 서비스는 인증 사유를 구성된 리디렉션 URL 중 하나에 매핑하여 오류를 처리합니다. 오류를 보고하기 위해 사용자가 해당 리디렉션 URL 로 리디렉션될 수 있습니다.

4. 다음 모드 중 하나를 선택합니다.
   - 302 데이터 없음
   - HTTP POST
5. "확인"을 클릭하여 변경 내용을 저장합니다.

참고: 이러한 리디렉션 URL 은 추가 어설션 처리를 위해 메시지 소비자 플러그인과 함께 사용될 수 있습니다. 인증이 실패하면 플러그인이 사용자를 지정한 리디렉션 URL 중 하나에 보낼 수 있습니다.

SP 에서 프록시 서버로 요청 처리

SiteMinder 가 SP 에서 특정 요청을 받으면 메시지 특성의 유효성을 검사합니다. SiteMinder 는 페더레이션 웹 서비스 응용 프로그램에 대한 로컬 URL 을 사용하여 특성을 확인합니다. 확인 후 SiteMinder 가 요청을 처리합니다.

예를 들어 로그아웃 요청 메시지에 다음 특성이 포함될 수 있습니다.

```
Destination="http://sp.domain.com:8080/affwebservices/public/saml2slo"
```

이 예에서는 로그아웃 메시지의 Destination 특성과 페더레이션 웹 서비스 응용 프로그램의 주소가 동일합니다. SiteMinder 는 Destination 특성이 FWS 응용 프로그램의 로컬 URL 과 일치하는지 확인합니다.

SiteMinder 가 프록시 서버 뒤에 있는 경우 로컬 URL 과 Destination 특성 URL 은 동일하지 않습니다. Destination 특성은 프록시 서버의 URL 입니다. 예를 들어 로그아웃 메시지에 다음 Destination 특성이 포함될 수 있습니다.

```
Destination="http://proxy.domain.com:9090/affwebservices/public/saml2slo"
```

페더레이션 웹 서비스에 대한 로컬 URL(http://sp.domain.com:8080/affwebservices/public/saml2slo)이 Destination 특성과 일치하지 않으므로 요청이 거부됩니다.

SiteMinder 가 요청의 메시지 특성을 확인하는 데 사용되는 로컬 URL 을 결정하는 방법을 변경하도록 프록시 구성을 지정할 수 있습니다. 프록시 구성에서 SiteMinder 는 로컬 URL 의 *<protocol>://<authority>* 부분을 프록시 서버 URL 로 대체합니다. 그 결과로 두 URL 간에 일치 항목이 발생합니다.

SP 에서 프록시 서버로 요청 처리 구성

SiteMinder 가 요청의 메시지 특성을 확인하는 데 사용되는 로컬 URL 을 결정하는 방법을 변경하도록 프록시 구성을 지정할 수 있습니다.

서비스 공급자에서 프록시 서버를 사용하려면

1. 수정할 SAML 2.0 인증 체계로 이동합니다.
2. "SAML 2.0 구성", "고급"을 차례로 선택합니다.
3. "프록시" 섹션의 "서버" 필드에 부분 URL 을 입력합니다. 형식은 *<protocol>://<authority>*입니다.

   예를 들어 프록시 서버 구성은 다음과 같습니다.
   `http://proxy.domain.com:9090`

   네트워크에 SPS 페더레이션 게이트웨이가 포함되어 있으면 "서버" 필드에서 SPS 페더레이션 게이트웨이 호스트 및 포트를 지정해야 합니다. 예를 들면 다음과 같습니다.

   `http://sps_federation_gateway.domain.com:9090`
4. "확인"을 클릭하여 변경 내용을 저장합니다.

"서버" 구성은 SP 의 다음 서비스에 대한 URL 에 영향을 줍니다.

- 어설션 소비자 서비스
- 싱글 로그아웃 서비스

"서버" 값은 SiteMinder 가 Destination 특성 같은 SAML 특성을 확인하는 데 사용하는 URL 의 일부가 됩니다.

참고: URL 하나에 대해 프록시 서버를 사용하고 있는 경우 이 모든 URL 에 대해 해당 프록시 서버를 사용하십시오.

백 채널에 대해 클라이언트 인증서 인증이 사용되도록 설정(선택 사항)

이 절차는 아티팩트 바인딩을 사용하는 싱글 사인온에만 적용됩니다.

어설션 소비자 서비스가 아이덴티티 공급자에서 어설션을 검색하기 위해 인증 체계에서 인증 정보를 수집합니다. 인증 체계가 어설션 소비자 서비스에 어설션을 검색하기 위해 아이덴티티 공급자에게 제공할 자격 증명 유형을 알려 줍니다. 어설션이 검색된 후 아이덴티티 공급자가 보안 백 채널을 통해 어설션을 서비스 공급자에게 보냅니다. 클라이언트 인증서 인증을 사용하여 백 채널의 보안을 유지할 수 있습니다.

백 채널에 대한 인증서 인증은 선택 사항입니다. 대신 기본 인증을 사용할 수 있습니다.

백 채널에 대한 클라이언트 인증서 인증을 사용하려면

1. 인증서 데이터 저장소에 클라이언트 인증서를 추가합니다 (페이지 301).
2. 백 채널에 대한 클라이언트 인증서 인증을 선택합니다 (페이지 301). 이 체계는 인증서가 서비스 공급자에 대한 자격 증명 역할을 함을 나타냅니다.

   정책 서버가 FIPS 전용 모드로 작동하고 있는 경우에도 비 FIPS 140 으로 암호화된 인증서를 사용하여 백 채널의 보안을 유지할 수 있습니다. 하지만 엄격한 FIPS 전용 설치의 경우 FIPS 140 호환 알고리즘으로 암호화된 인증서만 사용하십시오.

어설션 측 정책 서버의 관리자가 어설션 검색 서비스를 보호하도록 정책을 구성해야 합니다. 이 정책에 대한 영역이 X.509 클라이언트 인증서 인증 체계를 사용해야 합니다.

추가 정보:

아티팩트 서비스를 보호하는 인증 체계 구성 (페이지 147)

인증서 데이터 저장소에 클라이언트 인증서 추가

인증 기관으로부터 받은 개인 키/인증서 쌍이 있어야 합니다. 관리 UI 를 사용하여 개인 키/인증서 쌍을 인증서 데이터 저장소에 추가하십시오. 키/인증서 쌍이 데이터 저장소에 이미 있는 경우 이 단계를 건너뛰십시오. 지침은 *정책 서버 구성 안내서*를 참조하십시오.

키/인증서 쌍을 가져오는 경우 할당하는 별칭은 인증 체계 설정에 있는 "이름" 필드와 동일한 값이어야 합니다. 또한 인증서에 있는 "주체"의 CN 특성도 "이름" 필드와 일치해야 합니다. 예를 들어 "이름"이 CompanyA 인 경우를 가정합니다. 이 경우 별칭은 Company A 이고 "주체"에 대한 CN 값은 CN=CompanyA, OU=Development, O=CA, L=Islandia, ST=NY, C=US 여야 합니다.

중요! 인증 체계에 있는 "이름" 필드는 아이덴티티 공급자의 서비스 공급자 개체에 할당된 이름과 일치해야 합니다. SiteMinder 가 아이덴티티 공급자인 경우 인증 체계에 있는 "이름"은 개체의 "일반" 설정에 있는 "이름" 필드와 일치해야 합니다.

백 채널에 대한 클라이언트 인증서 옵션 구성

백 채널에 대해 클라이언트 인증서 인증이 사용되도록 설정하면 인증서가 자격 증명 역할을 합니다.

클라이언트 인증서를 자격 증명으로 제공하려면

1. SAML 2.0 인증 체계로 이동합니다.
2. "SAML 2.0 구성", "SSO"를 차례로 선택합니다.

   "SSO" 페이지가 표시됩니다.
3. "바인딩" 섹션에서 "HTTP-아티팩트"를 선택합니다.
4. "확인"을 클릭합니다.
5. "암호화 및 서명" 페이지로 이동합니다.
6. "백 채널" 섹션에서 "Client Cert for the Authentication"(인증용 클라이언트 인증서) 필드를 선택합니다.
7. "SP 이름"에 대한 값을 입력합니다.
8. "확인"을 클릭합니다.

SAML 2.0 인증 체계로 리소스를 보호하는 방법

SAML 2.0 인증 체계를 사용하는 SiteMinder 정책을 구성하여 대상 페더레이션 리소스를 보호하십시오.

SAML 인증 체계로 페더레이션 리소스를 보호하려면

1. SAML 인증 체계를 사용하는 영역을 생성합니다. 영역은 사용자가 요청하는 대상 리소스를 수집한 것입니다.

   다음 방법 중 하나로 영역을 생성합니다.

   - 이미 구성된 인증 체계 각각에 대해 고유한 영역을 생성합니다 (페이지 190).
   - 사용자 지정 인증 체계를 사용하여 요청을 해당 SAML 인증 체계로 발송하는 단일 대상 영역을 구성합니다 (페이지 191). 모든 아이덴티티 공급자에 대해 단일 대상이 있는 영역 하나를 구성하면 SAML 인증을 위한 영역 구성이 단순화됩니다.

2. 영역을 구성한 후 연결된 규칙과 응답(선택 사항)을 설정합니다.
3. 대상 리소스를 보호하는 정책으로 영역, 규칙 및 응답을 그룹화합니다.

중요! 영역의 각 대상 URL 은 원치 않는 응답 URL 에서도 식별됩니다. 원치 않는 응답이 서비스 공급자의 초기 요청 없이 아이덴티티 공급자에서 서비스 공급자로 전송됩니다. 원치 않는 응답에는 대상이 포함되어 있습니다. 아이덴티티 공급자에서 관리자가 이 응답을 링크에 포함해야 아이덴티티 공급자가 사용자를 서비스 공급자로 리디렉션할 수 있습니다.

각 인증 체계에 대해 고유 영역 구성

각 SAML 또는 WS-페더레이션 인증 체계에 대해 고유 영역을 구성하는 절차는 영역을 생성하는 표준 지침을 따릅니다.

다음 단계를 수행하십시오.

1. "정책", "도메인", "도메인"으로 이동합니다.

   도메인을 생성하는 페이지가 표시됩니다.

2. "도메인 만들기"를 클릭합니다.
3. 도메인 이름을 입력합니다.
4. 도메인에 사용자 디렉터리를 추가합니다. 이 디렉터리는 페더레이션된 리소스에 대한 액세스를 요청하는 사용자가 포함된 디렉터리입니다.

5. "영역" 탭을 선택하고 영역을 생성합니다.
   - "에이전트" 필드에서 대상 리소스가 있는 웹 서버를 보호하는 웹 에이전트를 선택합니다.
   - "인증 체계" 필드에서 적절한 인증 체계를 선택합니다.
6. 영역에 대한 규칙을 생성합니다.

   규칙의 일부로 사용자 인증 시 처리를 제어하는 데 사용되는 작업(Get, Post, or Put)을 선택합니다.
7. "정책" 탭을 선택하고 대상 페더레이션 리소스를 보호하는 정책을 구성합니다. 이전에 생성한 영역을 이 정책과 연결합니다.

이제 고유 영역이 있는 정책이 페더레이션된 리소스를 보호합니다.

모든 인증 체계에 대해 단일 대상 영역 구성

인증 체계에 대한 영역 구성을 단순화하려면 어설션을 생성하는 사이트 여러 개에 대해 단일 대상 영역을 생성하십시오.

이 태스크를 수행하려면 다음 구성 요소를 설정하십시오.

- 단일 사용자 지정 인증 체계

  이 사용자 지정 체계는 이미 각 어설션 당사자에 대해 구성한 해당 SAML 또는 WS-페더레이션 인증 체계에 요청을 전달합니다.
- 대상 URL 이 하나 있는 단일 영역

단일 대상 영역에 대한 인증 체계 만들기

단일 대상 영역에 대한 사용자 지정 인증 체계를 정의하려면

- 인증 체계를 구성해야 합니다.
- 사용자 지정 체계에서 정책 서버에 리소스 요청에 적용할 인증 체계를 알려 주는 매개 변수를 정의해야 합니다.

먼저 구성된 SAML 또는 WS-페더레이션 인증 체계가 있는지 확인하십시오. 없는 경우 사용자 지정 체계가 참조할 수 있는 이러한 체계를 구성하십시오.

인증 체계를 생성하려면

1. "인프라", "인증", "인증 체계"로 이동합니다.

   "인증 체계 만들기" 페이지가 표시됩니다.
2. 사용 중인 프로토콜의 절차에 따라 인증 체계를 하나 이상 생성합니다.
3. "확인"을 클릭하여 종료합니다.

추가 정보:

SAML 1.x 인증 체계 (페이지 167)
WS-페더레이션 인증 체계 개요 (페이지 337)
SAML 2.0 인증 체계를 구성하는 방법 (페이지 267)

사용자 지정 인증 체계 만들기

단일 대상 영역이 특정 사용자 지정 인증 체계를 통해 제대로 작동합니다.

단일 대상 영역에 대한 사용자 지정 인증 체계를 구성하려면

1. "인프라", "인증", "인증 체계"로 이동합니다.

   "인증 체계 만들기" 페이지가 표시됩니다.
2. 다음과 같이 필드에 데이터를 입력합니다.

   이름

   사용자 지정 인증 체계의 설명이 포함된 이름(예: SAML Custom Auth Scheme)을 입력합니다.
3. "체계 일반 설정" 섹션의 다음 필드에 데이터를 입력합니다.

   인증 체계 유형

   사용자 지정 템플릿

   보호 수준

   새 수준 설정의 기본값을 적용합니다.
4. 체계 설정 섹션의 다음 필드에 데이터를 입력합니다.

   라이브러리

   smauthsinglefed

암호

이 필드는 비워 둡니다.

암호 확인

이 필드는 비워 둡니다.

매개 변수

다음 매개 변수 중 하나를 지정합니다.

- SCHEMESET=LIST; <*saml-scheme1*>;<*saml_scheme2*>

  사용할 SAML 인증 체계 이름 목록을 지정합니다. artifact_producer1 이라는 아티팩트 체계와 samlpost_producer2 라는 POST 프로필 체계를 구성한 경우 이러한 체계를 입력합니다. 예를 들면 다음과 같습니다.

  SCHEMESET=LIST;artifact_producer1;samlpost_producer2

- SCHEMESET=SAML_ALL;

  구성된 체계를 모두 지정합니다. 그러면 사용자 지정 인증 체계가 모든 SAML 인증 체계를 열거하고 요청에 대해 올바른 공급자 원본 ID 가 있는 체계를 찾습니다.

- SCHEMESET=SAML_POST;

  구성한 SAML POST 프로필 체계를 모두 지정합니다. 그러면 사용자 지정 인증 체계가 POST 프로필 체계를 열거하고 요청에 대해 올바른 공급자 원본 ID 가 있는 체계를 찾습니다.

- SCHEMESET=SAML_ART;

  구성한 SAML 아티팩트 체계를 모두 지정합니다. 그러면 사용자 지정 인증 체계가 아티팩트 체계를 열거하고 요청에 대해 올바른 공급자 원본 ID 가 있는 체계를 찾습니다.

- SCHEMESET=WSFED_PASSIVE;

  올바른 계정 파트너 ID 가 있는 체계를 찾기 위해 모든 WS-페더레이션 인증 체계를 지정합니다.

SiteMinder 관리자에 대해 이 체계 사용

선택 취소된 상태로 둡니다.

5. 제출을 클릭합니다.

사용자 지정 인증 체계가 완료되었습니다.

단일 대상 영역 구성

인증 체계를 구성하여 사용자 지정 체계와 연결한 후 페더레이션 리소스에 대한 단일 대상 영역을 구성하십시오.

다음 단계를 수행하십시오.

1. "정책", "도메인", "도메인"으로 이동합니다.
2. 단일 대상 영역에 대한 정책 도메인을 수정합니다.
3. "영역" 탭을 선택하고 "만들기"를 클릭합니다.

   "영역 만들기" 대화 상자가 열립니다.
4. 다음 값을 입력하여 단일 대상 영역을 생성합니다.

   이름

   이 단일 대상 영역에 대한 이름을 입력합니다.
5. "리소스" 옵션의 다음 필드에 데이터를 입력합니다.

   에이전트

   대상 리소스가 있는 웹 서버를 보호하는 웹 에이전트를 선택합니다.

   리소스 필터

   대상 리소스의 위치를 지정합니다. 이 위치는 페더레이션된 리소스를 요청하는 사용자가 리디렉션되는 위치입니다.

   예를 들면 /FederatedResources 입니다.
6. "기본 리소스 보호" 섹션에서 "보호됨" 옵션을 선택합니다.
7. "인증 체계" 필드에서 이전에 구성된 사용자 지정 인증 체계를 선택합니다.

   예를 들어 사용자 지정 체계의 이름이 "Fed Custom Scheme"(페더레이션 사용자 지정 체계)인 경우 이 체계를 선택합니다.
8. "확인"을 클릭합니다.

단일 대상 영역 태스크가 완료되었습니다.

단일 대상 영역에 대한 규칙 구성

단일 대상 영역을 구성한 후 리소스를 보호하기 위한 규칙을 구성하십시오.

1. 단일 대상 영역에 대한 "수정" 페이지로 이동합니다.
2. "규칙" 섹션에서 "만들기"를 클릭합니다.

   "규칙 만들기" 페이지가 표시됩니다.
3. 규칙 페이지의 필드에 대한 값을 입력합니다.
4. "확인"을 클릭합니다.

단일 대상 영역 구성에 새 규칙이 포함됩니다.

단일 대상 영역을 사용하여 정책 만들기

단일 대상 영역을 참조하는 정책을 생성하십시오. 단일 대상 영역에서는 요청을 적절한 SAML 인증 체계로 보내는 사용자 지정 인증 체계를 사용합니다.

참고: 이 절차에서는 도메인, 사용자 지정 인증 체계, 단일 대상 영역 및 연결된 규칙을 이미 구성했다고 가정합니다.

다음 단계를 수행하십시오.

1. 이전에 구성한 도메인으로 이동합니다.
2. "정책" 탭을 선택하고 "만들기"를 클릭합니다.

   "정책 만들기" 페이지가 열립니다.
3. "일반" 섹션에 정책의 이름과 설명을 입력합니다.
4. "사용자" 섹션에서 사용자를 정책에 추가합니다.
5. "규칙" 탭에서 단일 대상 영역에 대해 생성한 규칙을 추가합니다.

   나머지 탭은 선택 사항입니다.
6. "확인"을 클릭합니다.
7. "제출"을 클릭합니다.

정책 태스크가 완료되었습니다. 요청으로 인해 이 정책이 트리거되는 경우 단일 영역 및 연결된 인증 체계에 따라 사용자가 인증됩니다.

제 16 장: WS-페더레이션 계정 파트너 구성

어설션 파트너(레거시)에 대한 사전 요구 사항

어설션 파트너를 구성하려면 다음 조건을 확인하십시오.

- 정책 서버가 설치되어 있어야 합니다.
- 다음 옵션 중 하나가 설치되어 있어야 합니다.
  - 웹 에이전트 및 웹 에이전트 옵션 팩. 웹 에이전트는 사용자를 인증하고 SiteMinder 세션을 설정합니다. 옵션 팩은 페더레이션 웹 서비스 응용 프로그램을 제공합니다. 적절한 네트워크 시스템에 FWS 응용 프로그램을 배포해야 합니다.
  - SPS 페더레이션 게이트웨이에 포함된 웹 에이전트가 있고 포함된 Tomcat 웹 서버에 페더레이션 웹 서비스 응용 프로그램이 있습니다.

  자세한 내용은 *웹 에이전트 옵션 팩 안내서*를 참조하십시오.
- 메시지 서명 및 암호 해독이 필요한 기능을 위해 개인 키와 인증서를 가져와야 합니다.
- 페더레이션된 네트워크 내에 신뢰 파트너가 설정되어 있어야 합니다.

계정 파트너를 구성하는 방법

SiteMinder 는 계정 파트너로 작동하는 경우 해당 비즈니스 파트너인 리소스 파트너에 대한 어설션을 생성합니다. 페더레이션된 파트너 관계를 설정하려면 계정 파트너에게 각 리소스 파트너에 대한 정보가 필요합니다. 각 파트너에 대해 리소스 파트너 개체를 생성하십시오. 엔터티 두 개가 어설션을 전달하고 싱글 사인온 등의 프로필을 충족하기 위해 통신하는 방법을 정의하십시오.

다음 단계를 수행하십시오.

1. 리소스 파트너 개체를 생성합니다.
2. 리소스 파트너를 가맹 도메인에 추가합니다.

3. 리소스 파트너에 대한 일반 식별 정보를 지정합니다.
4. 사용자 저장소에서 사용자를 선택합니다. 계정 파트너가 선택한 사용자에 대한 어설션을 생성합니다.
5. 어설션에 포함할 이름 ID 를 지정합니다.
6. 싱글 사인온 프로필을 구성합니다.

   전체 SSO 프로필을 구성하지 않은 상태로 리소스 파트너 엔터티를 저장할 수 있습니다. 하지만 SSO 를 구성하지 않고는 어설션을 리소스 파트너에게 전달할 수 없습니다.
7. 선택적 구성 태스크 (페이지 310)를 완료합니다.

팁:

- 계정 파트너와 리소스 파트너의 특정 매개 변수 값이 일치해야 구성이 올바로 작동합니다. 이러한 매개 변수 목록은 동일한 값을 사용해야 하는 구성 설정 (페이지 411)에서 찾을 수 있습니다.
- 페더레이션 웹 서비스 서블릿에 대해 올바른 URL 을 사용하십시오. URL 목록은 SiteMinder 구성에 사용되는 페더레이션 웹 서비스 URL (페이지 417)에서 찾을 수 있습니다.

계정 파트너에 대한 선택적 구성 태스크

계정 파트너를 구성하기 위한 선택적 태스크는 다음과 같습니다.

- 싱글 사인온 제한을 구성합니다.
  - 리소스 파트너에 대한 시간 제한을 구성합니다 (페이지 317).
  - 리소스 파트너에 액세스하는 데 사용되는 주소를 제한할 IP 주소 제한을 설정합니다 (페이지 318).
- 어설션에 포함할 특성을 구성합니다 (페이지 330).
- 사인아웃을 구성합니다 (페이지 329).
- 어설션 생성기 플러그인을 사용하여 SAML 응답을 사용자 지정합니다 (페이지 158).

레거시 페더레이션 대화 상자 탐색

관리 UI 에서는 레거시 페더레이션 구성 대화 상자로 이동하는 방법 두 가지를 제공합니다.

다음 두 방법 중 하나로 탐색할 수 있습니다.

- 마법사를 따라 새 레거시 페더레이션 개체 구성

  개체를 생성하는 경우 페이지가 표시되면서 구성 마법사가 나타납니다. 구성 마법사의 단계를 따라 개체를 생성하십시오.

- 탭을 선택하여 기존 레거시 페더레이션 개체 수정

  기존 개체를 수정하는 경우 페이지가 표시되면서 일련의 탭이 나타납니다. 이러한 탭에서 구성을 수정하십시오. 이러한 탭은 구성 마법사의 단계와 동일합니다.

가맹 도메인에 리소스 파트너 추가

리소스 파트너를 어설션의 사용 가능한 소비자로 식별하려면 계정 파트너의 가맹 도메인에 리소스 파트너를 추가하십시오. 그런 다음 리소스 파트너를 구성하면 계정 파트너가 어설션이 포함된 보안 토큰 응답 메시지를 발급할 수 있습니다.

다음 단계를 수행하십시오.

1. "페더레이션", "레거시 페더레이션", "리소스 파트너"로 이동합니다.
2. "리소스 파트너 만들기"를 클릭합니다.

   "리소스 파트너 만들기" 페이지가 표시됩니다.

3. 가맹 도메인을 선택하고 "다음"을 클릭합니다.

   "일반" 페이지가 표시됩니다.

4. 대화 상자 맨 위의 필드에 데이터를 입력합니다.

   필드 설명을 보려면 "도움말"을 클릭하십시오.

5. "사용"을 선택하여 계정 파트너가 구성된 리소스 파트너를 인식할 수 있도록 합니다.

리소스 파트너 개체에 대한 일반 정보 구성

"일반" 페이지를 선택하여 리소스 파트너를 명명하고 리소스 파트너 및 계정 파트너 ID 등의 상세 정보를 제공하십시오. 또한 서비스 공급자에 액세스하기 위한 IP 주소 및 시간 제한을 구성할 수 있습니다.

일반 설정을 구성하려면

1. "일반" 설정으로 이동합니다.
2. 필수 필드에 주의하면서 필드에 대한 값을 입력합니다.

   참고: "도움말"을 클릭하면 필드, 컨트롤 및 해당되는 각 요구 사항에 대한 설명을 볼 수 있습니다.

   "차이 시간" 필드에 대한 다음 정보에 주의합니다.

   차이 시간

   현재 시스템 시간에서 차감되는 시간(초)을 지정합니다. 이 계산은 계정 파트너와 동기화되지 않은 클록이 있는 리소스 파트너에 해당합니다.

   싱글 사인온의 경우 차이 시간 및 싱글 사인온 유효 기간 값에 따라 어설션 유효 기간이 결정됩니다. 어설션 유효 기간 (페이지 141) 계산 방법을 검토하면 차이 시간에 대해 자세히 이해할 수 있습니다.
3. 디버깅에만 사용할 경우 "서명 처리 사용 안 함" 확인란을 선택하여 일시적으로 모든 서명 처리(서명 및 서명 확인 모두)가 사용되지 않도록 설정할 수 있습니다.

   중요! 서명 처리는 싱글 사인온에 대한 WS-페더레이션 피동 요청자 프로필에 필요하기 때문에 기본적으로 사용되도록 설정되어 있습니다.

SiteMinder 세션이 없는 사용자 인증

가맹 도메인에 리소스 파트너를 추가하는 경우 설정해야 하는 매개 변수 중 하나는 인증 URL 매개 변수입니다.

인증 URL 은 redirect.jsp 파일을 가리킵니다. 이 파일은 웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 설치하는 계정 파트너 사이트에 설치됩니다. SiteMinder 정책으로 redirect.jsp 파일을 보호하십시오. 정책은 보호된 리소스 파트너 리소스를 요청하지만 SiteMinder 세션이 없는 사용자에 대한 인증 챌린지를 트리거합니다.

다음 바인딩에는 SiteMinder 세션이 필요합니다.

- HTTP POST 바인딩을 사용하는 싱글 사인온의 경우

  사용자에게 세션이 있어야 하지만 영구 세션이 아니어도 됩니다. 어설션은 브라우저를 통해 리소스 파트너에게 직접 전달됩니다. 어설션이 세션 저장소에 저장되지 않아도 됩니다.

- 사인아웃의 경우

  싱글 로그아웃이 사용되도록 설정하는 경우에는 영구 세션이 필요합니다. 사용자가 먼저 리소스를 요청하면 계정 파트너가 세션을 세션 저장소에 저장합니다. 세션 정보는 나중에 싱글 로그아웃이 실행될 때 필요합니다.

사용자가 인증되어 redirect.jsp 파일에 성공적으로 액세스한 후 세션이 설정됩니다. redirect.jsp 파일이 사용자를 계정 파트너 웹 에이전트나 SPS 페더레이션 게이트웨이로 다시 리디렉션합니다. 그런 다음 SiteMinder 가 요청을 처리합니다.

인증 URL 을 보호하는 절차는 다음 배포와 관계없이 동일합니다.

- 웹 에이전트와 동일한 시스템에 설치된 웹 에이전트 옵션 팩
- 웹 서버 프록시에 웹 에이전트가 설치된 응용 프로그램 서버
- 응용 프로그램 서버 에이전트와 함께 설치된 응용 프로그램 서버
- 아이덴티티 공급자에 설치된 SPS 페더레이션 게이트웨이

인증 URL 을 보호하도록 정책 구성

인증 URL 을 보호하려면

1. 관리 UI 에 로그인합니다.
2. 어설션 당사자 웹 서버에 대해 정의하는 영역에 바인드할 웹 에이전트를 생성합니다. 웹 서버와 FWS 응용 프로그램에 대해 고유한 에이전트 이름을 할당하거나 둘 다에 대해 동일한 에이전트 이름을 사용합니다.
3. 소비자 리소스에 액세스하려고 할 때 챌린지가 표시되는 사용자에 대한 정책 도메인을 생성합니다.
4. 정책 도메인에 속한 리소스에 액세스할 수 있어야 하는 사용자를 선택합니다.

5. 다음 값으로 정책 도메인에 대한 영역을 정의합니다.

   에이전트

   어설션 당사자 웹 서버에 대한 에이전트

   리소스 필터

   웹 에이전트 r6.x QMR 6, r12.0 SP2, r12.0 SP3 및 SPS 페더레이션 게이트웨이. 다음과 같이 입력합니다.

   /siteminderagent/redirectjsp/

   리소스 필터 /siteminderagent/redirectjsp/는 FWS 응용 프로그램이 자동으로 설정하는 별칭입니다. 별칭 참조는 다음과 같습니다.

   - 웹 에이전트:

     web_agent_home/affwebservices/redirectjsp

   - SPS 페더레이션 게이트웨이:

     sps_home/secure-proxy/Tomcat/webapps/affwebservices/redirectjsp

   영구 세션

   SAML 아티팩트 프로필의 경우에만 영역 대화 상자의 "세션" 섹션에 있는 "영구" 확인란을 선택합니다. 영구 세션을 구성하지 않으면 사용자가 소비자 리소스에 액세스할 수 없습니다.

   나머지 설정의 경우 기본값을 적용하거나 필요에 따라 수정합니다.

6. "확인"을 클릭하여 영역을 저장합니다.
7. 영역에 대한 규칙을 생성합니다. "리소스" 필드에서 기본값인 별표(*)를 적용하여 영역에 대한 리소스를 모두 보호합니다.
8. 이전 단계에서 만든 규칙이 포함된 어설션 당사자 웹 서버에 대한 정책을 생성합니다.
9. 생성하는 어설션의 대상이 되는 사용자 선택 (페이지 136) 태스크를 완료합니다.

싱글 사인온에 대한 어설션 유효 기간

싱글 사인온의 경우 차이 시간 및 유효 기간 값에 따라 SiteMinder 가 어설션의 총 유효 기간을 계산하는 방법이 결정됩니다. SiteMinder 는 어설션의 생성 및 소비에 차이 시간을 적용합니다.

참고: 이 설명에서 어설션 당사자는 SAML 1.x 생산자, SAML 2.0 아이덴티티 공급자 또는 WS-페더레이션 계정 파트너입니다. 신뢰 당사자는 SAML 1.x 소비자, SAML 2.0 서비스 공급자 또는 WS-페더레이션 리소스 파트너입니다.

어설션 문서에서 NotBefore 및 NotOnOrAfter 값은 유효 간격의 시작 및 끝을 나타냅니다.

어설션 당사자 측에서 SiteMinder 는 어설션 유효 기간을 설정합니다. 유효 간격은 어설션이 생성되는 시스템 시간입니다. SiteMinder 는 이 시간을 사용하여 어설션의 IssueInstant 값을 설정한 다음 IssueInstant 값에서 차이 시간 값을 뺍니다. 그 결과로 얻은 시간이 NotBefore 값입니다.

NotBefore = IssueInstant - 차이 시간

유효 간격의 끝을 결정하기 위해 SiteMinder 는 유효 기간 값과 차이 시간을 IssueInstant 값에 더합니다. 그 결과로 얻은 시간은 NotOnOrAfter 값이 됩니다.

NotOnOrAfter = 유효 기간 + 차이 시간 + IssueInstant

시간은 GMT 를 기준으로 합니다.

예를 들어 어설션 당사자 측에서 어설션이 1:00 GMT 에 생성된다고 가정합니다. 차이 시간은 30 초이고 유효 기간은 60 초이며 어설션 유효 간격은 12:59:30 GMT 에서 1:01:30 GMT 사이입니다. 이 간격은 어설션이 생성된 시간보다 30 초 전에 시작되고 90 초 후에 끝납니다.

신뢰 당사자 측에서 SiteMinder 는 어설션 당사자 측에서와 동일한 계산을 수행하여 수신된 어설션이 유효한지 확인합니다.

SiteMinder 가 파트너 관계의 양쪽 모두에 있는 경우의 어설션 유효 기간 계산

SiteMinder 가 파트너 관계의 양쪽 모두에 있는 경우 어설션 유효 기간은 유효 기간을 차이 시간의 두 배에 더한 합계입니다. 공식은 다음과 같습니다.

어설션 유효 기간 = 2 x 차이 시간(어설션 당사자) + 유효 기간 + 2 x 차이 시간(신뢰 당사자)

공식의 초기 부분(2 x 차이 시간 + 유효 기간)은 어설션 당사자의 유효 기간 시작 및 끝을 나타냅니다. 공식의 두 번째 부분(2 x 차이 시간)은 신뢰 당사자에 있는 시스템 클록의 차이 시간을 나타냅니다. 2 를 곱하는 이유는 유효 기간의 NotBefore 및 NotOnOrAfter 끝을 고려하기 때문입니다.

참고: 레거시 페더레이션의 경우 유효 기간은 어설션 당사자 측에서만 설정됩니다.

예

어설션 당사자

어설션 당사자 측에서의 값은 다음과 같습니다.

- IssueInstant = 5:00PM
- 유효 기간 = 60 초
- 차이 시간 = 60 초
- NotBefore = 4:59PM
- NotOnOrAfter = 5:02PM

신뢰 당사자

신뢰 당사자는 어설션의 NotBefore 및 NotOnOrAfter 값을 사용하고 해당 차이 시간을 이러한 값에 적용합니다. 이 공식은 신뢰 당사자가 새 NotBefore 및 NotOnOrAfter 값을 계산하는 방법입니다.

- 차이 시간 = 180 초(3 분)
- NotBefore = 4:56PM
- NotOnOrAfter = 5:05PM

어설션 유효 기간 창

이 예제의 값을 사용한 전체 어설션 유효 기간 창의 계산은 다음과 같습니다.

120 초(2 x 60) + 60 초 + 360 초(2 x 180) = 540 초(9 분)

리소스 파트너 가용성에 대한 시간 제한 구성(선택 사항)

리소스 파트너 리소스 가용성에 대한 시간 제한을 지정할 수 있습니다. 시간 제한을 지정하면 리소스 파트너 리소스에 대한 액세스가 지정된 기간 동안에만 허용됩니다. 사용자가 지정된 기간을 벗어나 리소스에 액세스하려고 하면 계정 파트너가 SAML 어설션을 생성하지 않습니다.

참고: 시간 제한은 정책 서버가 설치된 서버의 시스템 클록을 기준으로 합니다.

시간 제한을 지정하려면

1. "일반" 설정에서 시작합니다.

   페이지의 "제한" 섹션에 있는 "시간" 섹션에서 "설정"을 클릭합니다.

   "시간 제한" 페이지가 표시됩니다.

2. 일정을 완료합니다. 이 일정 표는 규칙 개체의 "시간 제한" 표와 같습니다. 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.
3. "확인"을 클릭합니다.

시간 제한 일정이 설정되었습니다.

리소스 파트너에 대한 IP 주소 제한 구성(선택 사항)

리소스 파트너에 액세스할 웹 서버의 IP 주소, 범위 주소 또는 서브넷 마스크를 지정할 수 있습니다. 리소스 파트너에 대해 IP 주소를 지정하면 리소스 파트너가 적절한 IP 주소의 사용자만 허용합니다.

IP 주소를 지정하려면

1. "일반" 설정에서 시작합니다.

   페이지의 "제한" 섹션에 있는 "IP 주소" 영역에서 "추가"를 클릭합니다.

   "IP 제한" 페이지가 표시됩니다.

2. 추가하고 있는 IP 주소 유형에 대한 옵션을 선택하고 연결된 필드에 해당 주소 유형에 대한 데이터를 입력합니다.

   참고: IP 주소는 모르지만 주소에 대한 도메인 이름은 알고 있는 경우 "DNS 조회" 단추를 클릭합니다. 이 단추를 클릭하면 "DNS 조회" 페이지가 열립니다. "호스트 이름" 필드에 정규화된 호스트 이름을 입력하고 "확인"을 클릭합니다.

   - 단일 호스트--브라우저를 호스트하는 단일 IP 주소를 지정합니다. 단일 IP 주소를 지정하면 사용자가 지정된 IP 주소에서만 리소스 파트너에 액세스할 수 있습니다.
   - 호스트 이름--호스트 이름을 사용하여 웹 서버를 지정합니다. 호스트 이름을 지정하면 지정된 호스트의 사용자만 리소스 파트너에 액세스할 수 있습니다.

- 서브넷 마스크--웹 서버에 대한 서브넷 마스크를 지정합니다. 서브넷 마스크를 지정하면 지정된 서브넷 마스크의 사용자만 리소스 파트너에 액세스할 수 있습니다. 이 단추를 선택하면 "주소 및 서브넷 마스크 추가" 대화 상자가 열립니다. 왼쪽 및 오른쪽 화살표 단추를 사용하거나 슬라이더 막대를 클릭한 상태로 끌어서 놓아 서브넷 마스크를 선택합니다.
- 범위--IP 주소 범위를 지정합니다. IP 주소 범위를 지정하면 리소스 파트너가 주소 범위에 속한 IP 주소 중 하나의 사용자만 허용합니다. 시작 및 끝 주소를 입력하여 범위를 결정합니다.

3. "확인"을 클릭하여 구성을 저장합니다.

생성하는 어설션의 대상이 되는 사용자 선택

어설션 당사자 측에서 수행되는 구성의 일부로, 어설션 생성기가 생성하는 SAML 어설션의 대상이 되는 사용자 및 그룹 목록을 포함하십시오. 어설션 당사자는 SAML 1.x 생산자, SAML 2.0 아이덴티티 공급자 또는 WS 페더레이션 계정 파트너입니다.

가맹 도메인에 있는 디렉터리의 사용자 및 그룹만 추가할 수 있습니다.

페더레이션된 트랜잭션에 대한 사용자 및 그룹을 지정하려면

1. 구성하고 있는 파트너에 대한 "사용자" 설정으로 이동합니다.

   "사용자 디렉터리" 페이지가 열리면서 정책 도메인의 각 사용자 디렉터리에 대한 항목이 표시됩니다.

2. 사용자 디렉터리의 사용자 또는 그룹을 정책에 추가합니다.

   각 사용자 디렉터리 테이블에서 "구성원 추가", "항목 추가", "모두 추가"를 선택할 수 있습니다. 선택하는 방법에 따라 사용자를 추가할 수 있는 대화 상자가 열립니다.

   - "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.
   - "항목 추가"를 선택하는 경우 "User Directory Search Express Edit"(사용자 디렉터리 검색 빠른 편집) 대화 상자에서 수동 입력 (페이지 138)을 통해 사용자를 선택합니다.

   오른쪽 화살표(>)를 클릭하여 사용자 또는 그룹을 편집하거나 빼기 기호(-)를 클릭하여 사용자 또는 그룹을 삭제합니다.

3. 아무 방법이나 사용하여 개별 사용자, 사용자 그룹 또는 둘 다를 선택하고 "확인"을 클릭합니다.

   "사용자 디렉터리" 페이지가 다시 열리면서 새 사용자가 사용자 디렉터리 테이블에 나열됩니다.

추가 정보:

리소스에 액세스하지 못하도록 사용자 또는 그룹 제외 (페이지 137)
리소스에 대한 중첩된 그룹 액세스 허용 (페이지 138)
수동 입력으로 사용자 추가 (페이지 138)

리소스에 액세스하지 못하도록 사용자 또는 그룹 제외

어설션을 획득하지 못하도록 사용자 또는 사용자 그룹을 제외할 수 있습니다.

다음 단계를 수행하십시오.

1. "사용자" 설정으로 이동합니다.
2. 특정 사용자 디렉터리에 대한 목록에서 사용자 또는 그룹을 선택합니다.
3. "제외"를 클릭하여 선택한 사용자 또는 그룹을 제외합니다.

   선택 사항이 관리 UI 에 반영됩니다.
4. "확인"을 클릭하여 변경 내용을 저장합니다.

리소스에 대한 중첩된 그룹 액세스 허용

LDAP 사용자 디렉터리에는 하위 그룹이 있는 그룹이 포함될 수 있습니다. 복합 디렉터리에서는 다른 그룹의 계층 구조에 중첩된 그룹을 사용하여 많은 양의 사용자 정보를 구성할 수 있습니다.

중첩된 그룹에 있는 사용자를 검색하도록 설정하는 경우 요청된 사용자 레코드가 모든 중첩된 그룹에서 검색됩니다. 중첩된 그룹이 사용되도록 설정하지 않은 경우에는 지정하는 그룹만 검색됩니다.

중첩된 그룹에서 검색하도록 설정하려면

1. "사용자" 설정으로 이동합니다.

   연결된 가맹 도메인에 여러 사용자 디렉터리가 포함된 경우 각 사용자 디렉터리가 자체 섹션에 나타납니다.

2. "중첩된 그룹 허용" 확인란을 선택하여 중첩된 그룹에서 검색하도록 설정합니다.

수동 입력으로 사용자 추가

어설션 생성을 위해 사용자를 지정할 때 선택할 수 있는 옵션 중 하나는 수동 입력으로 사용자를 식별하는 것입니다.

다음 단계를 수행하십시오.

1. 구성하고 있는 파트너에 대한 "사용자" 설정으로 이동합니다.

   가맹 도메인에 여러 사용자 디렉터리가 포함된 경우 모든 디렉터리가 "사용자 디렉터리" 페이지에 나타납니다.

2. "항목 추가"를 클릭합니다.

   "User Directory Search Express Edit"(사용자 디렉터리 검색 빠른 편집) 페이지가 표시됩니다.

3. 검색 옵션을 선택하고 해당 검색 옵션에 대한 필드에 데이터를 입력합니다.

   검색 위치

   LDAP 디렉터리의 경우 드롭다운 목록에서 옵션을 선택합니다.

   DN 유효성 검사

   LDAP 검색이 디렉터리에서 이 DN 을 찾습니다.

   사용자 검색

   LDAP 검색이 일치하는 사용자 항목으로 제한됩니다.

   그룹 검색

   LDAP 검색이 일치하는 그룹 항목으로 제한됩니다.

   조직 검색

   LDAP 검색이 일치하는 조직 항목으로 제한됩니다.

모든 항목 검색

LDAP 검색이 일치하는 사용자, 그룹 및 조직 항목으로 제한됩니다.

- Microsoft SQL Server, Oracle 및 WinNT 디렉터리의 경우 "수동 입력" 필드에 사용자 이름을 입력할 수 있습니다.
- Microsoft SQL Server 또는 Oracle 의 경우 SQL 쿼리를 대신 입력할 수 있습니다. 예를 들면 다음과 같습니다.

  SELECT NAME FROM EMPLOYEE WHERE JOB ='MGR';

  정책 서버는 사용자 디렉터리에 대한 "연결 자격 증명" 탭의 "사용자 이름" 필드에 지정된 데이터베이스 사용자로 쿼리를 수행합니다. "수동 입력" 필드에 대한 SQL 문을 작성하는 경우 사용자 디렉터리에 대한 데이터베이스 스키마를 숙지해야 합니다. 예를 들어 SmSampleUsers 스키마를 사용하고 있는 경우 특정 사용자를 추가하려면 SmUser 테이블에서 사용자 항목을 선택합니다.
- LDAP 디렉터리의 경우 모든 디렉터리 항목을 추가하려면 "수동 입력" 필드에 **all** 을 입력합니다.

4. "확인"을 클릭하여 변경 내용을 저장합니다.

WS-페더레이션 어설션에 대한 이름 ID 구성

이름 ID 는 어설션에서 고유한 방법으로 사용자를 지정합니다. 관리 UI 에서 구성하는 값이 리소스 파트너에게 전송되는 어설션에 포함됩니다.

이름 ID 형식에 따라 ID 에 사용되는 콘텐츠 유형이 설정됩니다. 예를 들어 형식이 "사용자 DN"인 경우 콘텐츠는 UID 입니다.

이름 ID 를 구성하려면

1. 구성할 리소스 파트너 개체로 이동합니다.
2. "이름 ID" 설정을 선택합니다.
3. 이름 ID 형식을 선택합니다.

   각 형식에 대한 설명은 *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*(OASIS SAML(Security Assertion Markup Language) V2.0 에 대한 어설션 및 프로토콜) 사양을 참조하십시오.

4. 다음 옵션 중에서 이름 ID 유형을 선택합니다.
   - 정적 값
   - 사용자 특성
   - DN 특성(중첩된 그룹 포함 또는 제외)

   이름 ID 유형에 따라 "이름 ID 필드"의 내용이 변경됩니다.
5. "이름 ID 필드"에 선택한 이름 ID 유형에 대한 데이터를 입력합니다.

WS-페더레이션에 대한 싱글 사인온 구성

어설션은 리소스 파트너에서 싱글 사인온을 쉽게 수행하는 데 필요한 아이덴티티 정보를 제공합니다. 계정 파트너는 설정된 세션이 있는 사용자에 대한 SAML 1.1 어설션을 생성합니다. 그런 다음 계정 파트너가 어설션을 WS-페더레이션 RequestSecurityTokenResponse 메시지에 배치하고 토큰을 리소스 파트너에 전달합니다. 리소스 파트너는 보안 토큰을 소비하고 WS-페더레이션 보안 토큰 콘텐츠에 기반한 세션을 설정합니다.

싱글 사인온 구성의 일부로 계정 파트너가 어설션을 리소스 파트너에 전달하는 방법을 결정하십시오.

계정 파트너에서 싱글 사인온을 구성하려면

1. 리소스 파트너 개체에 대한 "SAML 프로필" 설정으로 이동합니다.
2. 페이지의 "SSO" 섹션에 있는 필드에 데이터를 입력합니다.

   필드 설명을 보려면 "도움말"을 클릭하십시오.
3. "제출"을 클릭하여 변경 내용을 저장합니다.

계정 파트너에서 싱글 사인온 시작

사용자가 리소스 파트너로 이동하기 전에 계정 파트너를 방문할 수 있습니다. 사용자가 먼저 계정 파트너로 이동하면 링크가 HTTP Get 요청을 생성해야 합니다. 하드 코드된 링크는 계정 파트너의 싱글 사인온 서비스를 가리킵니다. 요청에는 RP 공급자 ID 와 선택적으로 기타 매개 변수가 포함됩니다.

싱글 사인온 서비스에 대한 링크 구문은 다음과 같습니다.

https://*ap_server:port*/affwebservices/public/wsfedsso?wa=wsignin1.0&wtrealm=*RP_ID*

ap_server:port

계정 파트너에 있는 시스템의 서버 및 포트 번호를 지정합니다. 시스템은 페더레이션 네트워크에 설치된 구성 요소에 따라 웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하고 있습니다.

RP_ID

리소스 파트너 아이덴티티입니다. 엔터티 ID 는 대/소문자를 구분합니다. "관리 UI"에 표시되는 그대로 입력하십시오.

리소스 파트너에서 싱글 사인온 시작

사용자가 리소스 파트너에서 싱글 사인온을 시작하는 경우 일반적으로 사용자는 목록에서 계정 파트너를 선택합니다. 사이트 선택 페이지는 보호되지 않은 영역에 있습니다.

사이트 선택 페이지에 있는 링크는 계정 파트너의 싱글 사인온 서비스를 가리킵니다. 링크가 선택된 후 리소스 파트너는 어설션을 가져오기 위해 사용자를 계정 파트너로 리디렉션합니다.

SAML 어설션 응답 사용자 지정(선택 사항)

어설션 생성기 플러그인을 사용하여 어설션 콘텐츠를 수정할 수 있습니다. 플러그인을 통해 사용자와 파트너 및 공급업체 간의 비즈니스 계약을 사용하는 어설션 콘텐츠를 사용자 지정할 수 있습니다. 플러그인은 각 파트너에 대해 하나씩 허용됩니다.

어설션 생성기 플러그인을 구성하는 단계는 다음과 같습니다.

1. 아직 설치하지 않은 경우 SiteMinder SDK 를 설치합니다.
2. SDK 의 일부인 AssertionGeneratorPlugin.java 인터페이스를 구현합니다.
3. 어설션 생성기 플러그인 구현 클래스를 배포합니다.
4. 관리 UI 에서 어설션 생성기 플러그인 매개 변수가 사용되도록 설정합니다.

어설션 생성기 플러그인에 대한 추가 정보는 다음과 같이 찾을 수 있습니다.

- 참조 정보(메서드 서명, 매개 변수, 반환 값, 데이터 형식)와 UserContext 클래스에 대한 새 생성자는 *Javadoc 참조서*에서 확인할 수 있습니다. Javadoc 의 AssertionGeneratorPlugin 인터페이스를 참조하십시오.
- 인증 및 권한 부여 API 에 대한 개요와 개념 정보는 *SiteMinder Programming Guide for Java*(SiteMinder Java 프로그래밍 안내서)에 있습니다.

AssertionGeneratorPlugin 인터페이스 구현

사용자 지정 어설션 생성기 플러그인을 생성할 때의 첫 번째 단계는 AssertionGeneratorPlugin 인터페이스를 구현하는 것입니다.

다음 단계를 수행하십시오.

1. 매개 변수가 포함되지 않은 공개 기본 생성자 메서드를 제공합니다.
2. 상태 비저장 구현이 되도록 코드를 제공합니다. 여러 스레드가 단일 플러그인 클래스를 사용할 수 있어야 합니다.
3. 인터페이스에서 요구 사항을 충족할 메서드를 구현합니다.

   구현에 customizeAssertion 메서드 호출이 포함되어야 합니다. 기존 구현을 덮어쓸 수 있습니다. 이에 대한 예는 다음 샘플 클래스를 참조하십시오.

   SAML 1.x/WS-페더레이션

   AssertionSample.java

   SAML 2.0

   SAML2AssertionSample.java

   샘플 클래스는 /sdk/samples/assertiongeneratorplugin 디렉터리에 있습니다.

   구현이 customizeAssertion 메서드에 전달하는 매개 변수 문자열의 내용은 사용자 지정 개체의 책임입니다.

어설션 생성기 플러그인 배포

AssertionGeneratorPlugin 인터페이스에 대한 구현 클래스를 코드화했으면 해당 구현 클래스를 컴파일하고 SiteMinder 가 실행 파일을 찾을 수 있는지 확인하십시오.

어설션 생성기 플러그인을 배포하려면

1. 어설션 플러그인 Java 파일을 컴파일합니다.

   컴파일하려면 정책 서버와 함께 설치되는 다음 .jar 파일이 필요합니다.

   - *policy_server_home*/bin/jars/SmJavaApi.jar
   - *policy_server_home*/bin/thirdparty/xercesImpl.jar
   - *policy_server_home*/bin/endorsed/xalan.jar

2. JVMOptions.txt 파일에서 플러그인의 클래스 경로를 포함하도록 -Djava.class.path 값을 수정합니다. 이렇게 수정하면 수정된 클래스 경로를 사용하여 플러그인을 로드할 수 있습니다. *installation_home*\siteminder\config 디렉터리에서 JVMOptions.txt 파일을 찾습니다.

   참고: xercesImpl.jar, xalan.jar 또는 SMJavaApi.jar 의 클래스 경로를 수정하지 마십시오.

3. 플러그인이 사용되도록 설정합니다.

어설션 생성기 플러그인이 사용되도록 설정

어설션 생성기 플러그인을 작성하고 컴파일한 후 관리 UI 에서 설정을 구성하여 플러그인이 사용되도록 설정하십시오. UI 매개 변수는 SiteMinder 에게 플러그인을 찾을 수 있는 위치를 알려 줍니다.

플러그인을 배포 (페이지 159)할 때까지 플러그인 설정을 구성하지 마십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그온합니다.
2. "페더레이션", "레거시 페더레이션", "리소스 파트너"를 차례로 클릭합니다.
3. 기존 리소스 파트너 항목을 선택하거나 새로 생성합니다.
4. "일반" 설정으로 이동합니다.

5. "고급" 섹션의 다음 필드에 데이터를 입력합니다.

   Java 클래스 이름

   기존 플러그인에 대한 Java 클래스 이름을 지정합니다.

   플러그인 클래스는 어설션을 구문 분석하고 수정한 다음 최종 처리를 위해 결과를 어설션 생성기에게 반환할 수 있습니다.

   플러그인은 각 파트너에 대해 하나씩만 허용됩니다. 예를 들면 com.mycompany.assertiongenerator.AssertionSample 입니다.

   매개 변수

   (선택 사항) "Java 클래스 이름" 필드에서 지정한 플러그인에 전달되는 매개 변수 문자열을 지정합니다.

   참고: 관리 UI 를 통해 어설션 플러그인이 사용되도록 설정하는 대신 정책 관리 API(C 또는 Perl)를 사용하여 플러그인을 통합할 수 있습니다. 자세한 내용은 *SiteMinder Programming Guide for C*(SiteMinder C 프로그래밍 안내서) 또는 *SiteMinder Programming Guide for Java*(SiteMinder Java 프로그래밍 안내서)를 참조하십시오.

6. 정책 서버를 다시 시작합니다.

   정책 서버를 다시 시작하면 최신 버전의 어설션 플러그인이 다시 컴파일된 후 선택됩니다.

웹 응용 프로그램 특성으로 어설션 사용자 지정

어설션 생성기 플러그인을 사용하여 어설션에 웹 응용 프로그램 특성을 추가할 수 있습니다. 이것은 어설션을 사용자 지정하는 또 다른 방법입니다.

어설션에 웹 응용 프로그램 특성을 포함하려면

1. 어설션 플러그인 Java 파일을 컴파일합니다.

   컴파일하려면 정책 서버와 함께 설치되는 다음 .jar 파일이 필요합니다.

   - *policy_server_home*/bin/jars/SmJavaApi.jar
   - *policy_server_home*/bin/thirdparty/xercesImpl.jar
   - *policy_server_home*/bin/endorsed/xalan.jar

2. JVMOptions.txt 파일에서 플러그인의 클래스 경로를 포함하도록 -Djava.class.path 값을 수정합니다. 이렇게 수정하면 수정된 클래스 경로를 사용하여 플러그인을 로드할 수 있습니다. *installation_home*\siteminder\config 디렉터리에서 JVMOptions.txt 파일을 찾습니다.

   참고: xercesImpl.jar, xalan.jar 또는 SMJavaApi.jar 의 클래스 경로를 수정하지 마십시오.

3. 샘플 플러그인을 구성합니다.

   SMJavaAPI 의 APIContext 클래스에는 어설션에 포함된 웹 응용 프로그램의 특성을 포함하는 맵 개체를 반환하는 새 메서드인 getAttrMap()이 있습니다. SiteMinder SDK 에는 이 맵 개체를 사용하는 방법을 보여 주는 샘플 어설션 생성기 플러그인 두 개가 있습니다.

   - SAML2AppAttrPlugin.java(SAML 2.0)
   - WSFedAppAttrPlugin.java(WS-페더레이션)

   이러한 샘플은 sdk/samples/assertiongeneratorplugin 디렉터리에 있습니다. 이러한 샘플을 통해 어설션 생성기가 어설션에 웹 응용 프로그램 특성을 추가할 수 있습니다.

4. 관리 UI 에 로그인합니다.
5. "페더레이션", "레거시 페더레이션", "SAML 서비스 공급자" 또는 "리소스 파트너"를 차례로 선택합니다.
6. 기존 항목을 선택하거나 새로 생성합니다.
7. "일반" 설정으로 이동합니다.
8. "어설션 생성기 플러그인" 섹션의 다음 필드에 데이터를 입력합니다.

   Java 클래스 이름

   플러그인에 대한 Java 클래스의 이름을 지정합니다. 예를 들어 SiteMinder SDK 에 포함된 샘플 클래스는 다음과 같습니다.

   - com.ca.assertiongenerator.SAML2AppAttrPlugin

     (SAML 2.0)
   - com.ca.assertiongenerator.WSFedAppAttrPlugin

     (WS-페더레이션)

매개 변수

"Java 클래스 이름" 필드에서 지정한 플러그인에 전달되는 매개 변수 문자열을 지정합니다. 이러한 매개 변수는 어설션에 포함할 특성입니다.

참고: 관리 UI 를 통해 설정을 구성하는 대신 정책 관리 API(C 또는 Perl)를 사용하여 플러그인을 통합할 수 있습니다. 지침은 *SiteMinder Programming Guide for C*(SiteMinder C 프로그래밍 안내서) 또는 *SiteMinder Programming Guide for Java*(SiteMinder Java 프로그래밍 안내서)를 참조하십시오.

9. 정책 서버를 다시 시작합니다.

   정책 서버를 다시 시작하면 최신 버전의 어설션 플러그인이 다시 컴파일된 후 선택됩니다.

WS-페더레이션에 대한 사인아웃 구성

사인아웃은 사용자가 로그아웃을 시작한 브라우저에 대한 모든 세션에서 로그아웃되는 프로세스입니다. 사인아웃이 반드시 사용자의 모든 세션을 종료하는 것은 아닙니다. 예를 들어 사용자가 브라우저 두 개를 연 경우 해당 사용자는 독립 세션 두 개를 설정할 수 있습니다. 사인아웃을 시작하는 브라우저에 대한 세션만 해당 세션에 대한 모든 페더레이션된 사이트에서 종료됩니다. 다른 브라우저의 세션은 여전히 활성 상태입니다.

사용자는 계정 파트너나 리소스 파트너에서 사인아웃 요청을 시작할 수 있습니다. 요청은 적절한 서블릿을 가리키는 링크를 클릭하여 트리거합니다.

참고: 시스템은 사인아웃에 대해 WS-페더레이션 피동 요청만 지원합니다.

"사인아웃" 섹션의 설정을 구성하여 계정 파트너에게 리소스 파트너가 사인아웃을 지원하는 방법을 알릴 수 있습니다.

사인아웃이 사용되도록 설정하는 경우에는 다음 작업도 수행해야 합니다.

- 정책 서버 관리 콘솔을 사용하여 계정 파트너에서 세션 저장소가 사용되도록 설정합니다.

  세션 저장소에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.
- 사인아웃은 싱글 사인온 중 구성된 유효한 SiteMinder 영구 세션이 필요합니다. 리소스 파트너에서 인증 URL 을 포함하여 보호된 리소스가 포함된 영역에 대해 영구 세션을 구성하십시오.

  영역에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

사인아웃을 구성하려면

1. 구성할 리소스 파트너에 대한 "SAML 프로필" 페이지로 이동합니다.
2. "사인아웃" 섹션에서 "사인아웃 사용"을 선택합니다.
3. 다음 URL 필드에 대한 값을 입력합니다.
   - 사인아웃 삭제 URL
   - 사인아웃 확인 URL

   이러한 필드 각각에는 https:// 또는 http://로 시작하는 항목이 있어야 합니다.

   필드 설명을 보려면 "도움말"을 클릭하십시오.
4. "확인"을 클릭합니다.

WS-페더레이션 어설션에 대한 특성 구성(선택 사항)

특성은 리소스 파트너 리소스에 대한 액세스를 요청하는 사용자에 대한 정보를 제공할 수 있습니다. 특성 명령문은 계정 파트너에서 SAML 어설션에 있는 리소스 파트너로 사용자 특성, DN 특성 또는 정적 데이터를 전달합니다. 모든 구성된 특성은 <AttributeStatement> 요소 하나의 어설션에 포함되거나 어설션의 <EncryptedAttribute> 요소에 포함됩니다.

참고: 어설션에는 특성 명령문이 필요하지 않습니다.

서블릿, 웹 응용 프로그램 또는 기타 사용자 지정 응용 프로그램에서는 특성을 사용하여 사용자 지정된 콘텐츠를 표시하거나 다른 사용자 지정 기능이 사용되도록 설정합니다. 웹 응용 프로그램에서 사용되는 경우 특성은 사용자가 리소스 파트너에서 수행하는 작업을 제한하여 세부적인 액세스 제어를 구현할 수 있습니다. 예를 들어 최대 금액(달러)으로 설정된 "Authorized Amount"(권한 부여된 금액)라는 특성 변수를 보낼 수 있습니다. 이 금액은 사용자가 리소스 파트너에서 소비할 수 있는 한도입니다.

특성은 이름/값 쌍의 형식을 사용합니다. 리소스 파트너가 어설션을 받으면 응용 프로그램에 특성 값을 제공합니다.

특성을 HTTP 헤더나 HTTP 쿠키로 제공할 수 있습니다.

HTTP 헤더와 HTTP 쿠키에는 어설션 특성이 초과할 수 없는 크기 제한이 있습니다. 크기 제한은 다음과 같습니다.

- HTTP 헤더의 경우 SiteMinder 는 헤더에 대한 웹 서버 크기 제한까지 헤더에 있는 특성을 보낼 수 있습니다. 헤더당 허용되는 어설션 특성은 하나뿐입니다. 헤더 크기 제한을 확인하려면 해당 웹 서버 설명서를 참조하십시오.
- HTTP 쿠키의 경우 SiteMinder 는 쿠키에 대한 크기 제한까지 쿠키를 보낼 수 있습니다. 각 어설션 특성은 자체 쿠키로 전송됩니다. 쿠키 크기 제한은 브라우저별로 다르고, 해당 제한은 각 특성에만 적용되는 것이 아니라 응용 프로그램에 전달되고 있는 모든 특성에 적용됩니다. 쿠키 크기 제한을 확인하려면 해당 웹 브라우저 설명서를 참조하십시오.

WS-페더레이션에 대한 어설션 특성 구성

어설션 특성을 구성하려면

1. 구성하고 있는 리소스 파트너 개체에 대한 "특성" 페이지로 이동합니다.
2. "특성" 섹션에서 "추가"를 클릭합니다.

   "특성 추가" 대화 상자가 나타납니다.

3. "특성" 드롭다운에서 이름 형식 식별자를 선택합니다. 어설션의 <Attribute> 요소에 있는 <NameFormat> 특성이 식별자를 지정합니다. 이 값은 리소스 파트너가 이름을 해석할 수 있도록 특성 이름을 분류합니다.

   옵션은 다음과 같습니다.

   - EmailAddress
   - UPN
   - CommonName
   - Group
   - NameValue

   이러한 옵션에 대한 자세한 내용은 WS-페더레이션 사양을 참조하십시오.

4. "특성 설정" 섹션에서 다음 옵션 중 하나를 선택합니다.

   - 정적
   - 사용자 특성
   - DN 특성

   다음 중에서 선택하는 옵션에 따라 "특성 필드" 섹션에서 사용할 수 있는 필드가 결정됩니다.

   필드 설명을 보려면 "도움말"을 클릭하십시오.

5. 선택 사항입니다. 중첩된 그룹이 있는 LDAP 사용자 디렉터리에서 특성을 검색할 수 있습니다. 정책 서버가 중첩된 그룹에서 DN 특성을 검색하도록 하려면 "특성 종류" 섹션에서 "중첩된 그룹 허용" 확인란을 선택합니다.

6. 필요한 필드에 특성 종류에 대한 데이터를 입력하고 변경 내용을 저장합니다.

어설션 특성의 최대 길이 지정

사용자 어설션 특성의 최대 길이를 구성할 수 있습니다. 어설션 특성의 최대 길이를 수정하려면 EntitlementGenerator.properties 파일에서 해당 설정을 변경하십시오.

이 파일에 있는 속성 이름은 구성하고 있는 프로토콜에 따라 다릅니다.

다음 단계를 수행하십시오.

1. 정책 서버가 설치된 시스템에서 *policy_server_home*\config\properties\EntitlementGenerator.properties 로 이동합니다.
2. 텍스트 편집기에서 파일을 엽니다.
3. 사용자의 환경에서 사용하고 있는 프로토콜에 맞게 사용자 특성의 최대 길이를 조정합니다. 각 프로토콜에 대한 설정은 다음과 같습니다.

   WS-페더레이션

   속성 이름:
   com.netegrity.assertiongenerator.wsfed.MaxUserAttributeLength

   속성 유형: 양의 정수 값

   기본값: 1024

   설명: WS-FED 어설션 특성의 최대 특성 길이를 나타냅니다.

   SAML 1.x

   속성 이름:
   com.netegrity.assertiongenerator.saml1.MaxUserAttributeLength

   속성 유형: 양의 정수 값

   기본값: 1024

   설명: SAML1.1 어설션 특성의 최대 특성 길이를 나타냅니다.

   SAML 2.0

   속성 이름:
   com.netegrity.assertiongenerator.saml2.MaxUserAttributeLength

   속성 유형: 양의 정수 값

   기본값: 1024

   설명: SAML2.0 어설션 특성의 최대 특성 길이를 나타냅니다.
4. 이러한 매개 변수를 변경한 후 정책 서버를 다시 시작합니다.

스크립트를 사용하여 새 특성 만들기

"특성" 대화 상자의 "고급" 섹션에는 "스크립트" 필드가 포함되어 있습니다. 이 필드에는 "특성 설정" 섹션에 입력한 사항을 기반으로 SiteMinder 가 생성하는 스크립트가 표시됩니다. 이 필드의 내용을 복사하여 다른 응답 특성에 대한 "스크립트" 필드에 붙여 넣을 수 있습니다.

참고: 다른 특성에 대한 "스크립트" 필드의 내용을 복사하여 붙여 넣는 경우 "특성 종류" 섹션에서 적절한 옵션을 선택하십시오.

제 17 장: SiteMinder 를 WS-페더레이션 리소스 파트너로 구성

이 섹션은 다음 항목을 포함하고 있습니다.

신뢰 파트너에 대한 사전 요구 사항

SiteMinder 를 신뢰 파트너로 사용하려면 다음 태스크를 완료하십시오.

- 정책 서버를 설치합니다.
- 다음 구성 요소 중 하나를 설치합니다.
  - 웹 에이전트 및 웹 에이전트 옵션 팩. 웹 에이전트는 사용자를 인증하고 세션을 설정합니다. 옵션 팩은 페더레이션 웹 서비스 응용 프로그램을 제공합니다. 적절한 네트워크 시스템에 FWS 응용 프로그램을 배포해야 합니다.
  - 포함된 웹 에이전트가 있고 포함된 Tomcat 웹 서버에 페더레이션 웹 서비스 응용 프로그램이 있는 SPS 페더레이션 게이트웨이

  자세한 내용은 *웹 에이전트 옵션 팩 안내서*를 참조하십시오.
- 메시지 서명 및 암호화를 필요로 하는 기능을 위해 개인 키와 인증서를 가져옵니다.
- 어설션 파트너는 페더레이션된 네트워크 내에서 설정됩니다.

리소스 파트너를 구성하는 방법

WS-페더레이션 리소스 파트너를 구성하려면 다음 태스크를 수행해야 합니다.

1. SAML 1.x 인증 체계 필수 구성 요소를 완료합니다.
2. 인증 체계 유형을 선택하고 해당 이름을 할당합니다.
3. SAML 1.x 인증 체계로 인증되고 있는 사용자에 대한 네임스페이스를 지정합니다.
4. 이 소비자가 지원하는 싱글 사인온 프로필(아티팩트 또는 POST)을 선택합니다.

페더레이션 파트너이면서 어설션을 생성하는 계정 파트너 각각에 대해 SAML 인증 체계를 구성합니다. 각 체계를 영역에 바인드합니다. 영역에는 사용자가 요청하는 대상 리소스의 URL 이 포함되어 있습니다. 계정 파트너별로 이 태스크를 수행할 수도 있고 단일 사용자 지정 인증 체계와 단일 영역을 생성할 수도 있습니다. SiteMinder 정책으로 이러한 리소스를 보호합니다.

팁:

- 계정 파트너와 리소스 파트너의 특정 매개 변수 값이 일치해야 구성이 올바로 작동합니다. 이러한 매개 변수 목록은 동일한 값을 사용해야 하는 구성 설정 (페이지 411)에서 제공됩니다.
- 페더레이션 웹 서비스 서블릿에 대해 올바른 URL 을 사용하고 있는지 확인하십시오. URL 은 SiteMinder 구성에 사용되는 페더레이션 웹 서비스 URL (페이지 417)에 나열되어 있습니다.

리소스 파트너에 대한 선택적 구성 태스크

리소스 파트너를 구성하기 위한 선택적 태스크는 다음과 같습니다.

- 메시지 소비자 플러그인을 사용하여 어설션을 사용자 지정합니다.
- 실패한 인증 시도를 리디렉션합니다.

레거시 페더레이션 대화 상자 탐색

관리 UI 에서는 레거시 페더레이션 구성 대화 상자로 이동하는 방법 두 가지를 제공합니다.

다음 두 방법 중 하나로 탐색할 수 있습니다.

- 마법사를 따라 새 레거시 페더레이션 개체 구성

  개체를 생성하는 경우 페이지가 표시되면서 구성 마법사가 나타납니다. 구성 마법사의 단계를 따라 개체를 생성하십시오.

- 탭을 선택하여 기존 레거시 페더레이션 개체 수정

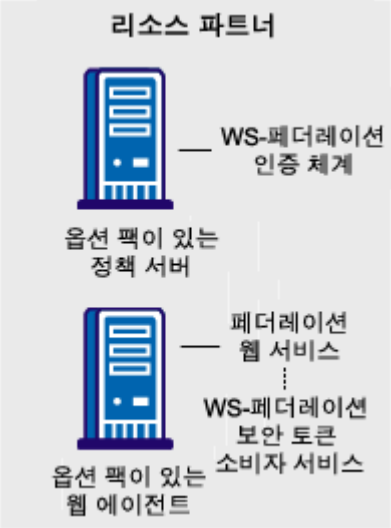
  기존 개체를 수정하는 경우 페이지가 표시되면서 일련의 탭이 나타납니다. 이러한 탭에서 구성을 수정하십시오. 이러한 탭은 구성 마법사의 단계와 동일합니다.

WS-페더레이션 인증 체계 개요

모든 SiteMinder 사이트나 SPS 페더레이션 게이트웨이가 <RequestSecurityTokenResponse> 메시지를 소비할 수 있으며 사용자를 인증하고 권한을 부여하기 위해 응답에서 어설션을 사용할 수 있습니다. 페더레이션된 네트워크의 사이트에 사용자 저장소가 있는 경우 WS-페더레이션 인증을 사용할 수 있습니다.

WS-페더레이션 인증 체계를 통해 리소스 파트너가 사용자를 인증할 수 있습니다. 인증 체계를 사용하면 SAML 어설션을 소비하고 SiteMinder 세션을 설정하여 도메인 간 싱글 사인온이 사용되도록 설정됩니다. 사용자가 식별된 후 리소스 파트너 사이트에서 사용자에게 특정 리소스에 대한 권한을 부여할 수 있습니다.

사이트는 WS-페더레이션 리소스 파트너와 계정 파트너 둘 다일 수 있습니다.



참고: SPS 페더레이션 게이트웨이가 페더레이션 웹 서비스 응용 프로그램 기능을 제공하기 위해 웹 에이전트 및 웹 에이전트 옵션 팩을 대체할 수 있습니다. SPS 페더레이션 게이트웨이 설치 및 구성에 대한 자세한 내용은 *Secure Proxy Server Administration Guide*(보안 프록시 서버 관리 안내서)를 참조하십시오.

WS-페더레이션 인증 체계는 리소스 파트너 측 정책 서버에서 구성됩니다. WS-페더레이션 보안 토큰 소비자 서비스가 인증 체계를 호출합니다. 보안 토큰 소비자 서비스는 페더레이션 웹 서비스 응용 프로그램의 구성 요소이며 리소스 파트너 측 웹 에이전트에 설치됩니다. 이 서비스는 정책 서버의 WS-페더레이션 인증 체계에서 정보를 가져옵니다. FWS 가 해당 정보를 사용하여 어설션에서 사용자를 인증하는 데 필요한 정보를 추출합니다.

SAML 어설션은 리소스 파트너 사이트의 정책 서버에 로그인하기 위한 사용자 자격 증명이 됩니다. 사용자가 인증되어 권한이 부여되고, 권한 부여가 성공한 경우 대상 리소스로 리디렉션됩니다.

WS-페더레이션 인증 체계 유형 선택

WS-페더레이션 인증 체계는 리소스 파트너에 대한 어설션을 생성하는 계정 파트너에 대한 정보를 제공합니다. 인증 체계는 리소스 파트너가 인증 프로세스를 지원하는 방식을 지정합니다.

인증 체계를 구성한 후 해당 체계와 보호할 리소스가 포함된 영역을 연결하십시오.

WS-페더레이션 인증 체계를 구성하려면

1. "인프라", "인증", "인증 체계"로 이동합니다.

   "인증 체계 만들기" 대화 상자가 열립니다.

2. "인증 체계 유형" 드롭다운 목록에서 "WS-페더레이션 템플릿"을 선택합니다.

   체계를 지원하도록 "인증 체계" 대화 상자의 내용이 변경됩니다.

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

인증 체계 템플릿을 선택한 후 인증 체계의 상세 정보를 구성할 수 있습니다. "WS-페더레이션 구성"을 클릭하여 구성 대화 상자의 나머지에 액세스합니다.

추가 정보:

WS-페더레이션 인증 체계로 대상 리소스를 보호하는 방법 (페이지 359)

WS-페더레이션 인증 체계에 대한 일반 정보 지정

WS-페더레이션 인증 체계에 대한 "일반" 설정에서 리소스 파트너와 계정 파트너를 식별하십시오.

다음 단계를 수행하십시오.

1. 기본 인증 체계 페이지에서 "WS-페더레이션 구성"을 클릭합니다.

   기존 체계를 수정하고 있는 경우에는 "수정", "WS-페더레이션 구성"을 차례로 클릭합니다.

   체계에 대한 상세 설정이 표시됩니다.
2. "일반" 설정의 필수 필드에 데이터를 입력합니다.
3. "서명 처리 사용 안 함" 옵션이 싱글 사인온에 맞게 적절히 설정되어 있는지 확인합니다.

   중요! 디버깅에만 사용할 경우 "서명 처리 사용 안 함" 옵션이 사용되도록 설정하여 일시적으로 모든 서명 처리(서명 및 서명 확인 모두)가 사용되지 않도록 설정할 수 있습니다.

일반 구성이 완료되었습니다.

인증에 대한 사용자 레코드 찾기

인증 체계를 구성할 때 인증 체계가 로컬 사용자 저장소에서 사용자를 조회하는 방법을 정의합니다. 올바른 사용자를 찾은 후 해당 사용자에 대한 세션이 시스템에서 생성됩니다. 사용자 저장소에서 사용자를 찾는 과정이 바로 명확성 프로세스입니다. SiteMinder 가 사용자를 명확히 하는 방법은 인증 체계 구성에 따라 다릅니다.

성공적인 명확성을 위해 인증 체계는 먼저 어설션에서 LoginID 를 확인합니다. 기본적으로 LoginID 는 어설션의 이름 ID 값에서 추출됩니다. Xpath 쿼리를 지정하여 LoginID 를 얻을 수도 있습니다.

인증 체계가 LoginID 를 확인한 후 SiteMinder 는 인증 체계에 대한 검색 사양이 구성되어 있는지 확인합니다. 인증 체계에 대해 정의된 검색 사양이 없으면 LoginID 가 정책 서버에 전달됩니다. 정책 서버는 LoginID 와 사용자 저장소 검색 사양을 함께 사용하여 사용자를 찾습니다. 예를 들어 LoginID 값은 Username 이고 LDAP 검색 사양은 uid 특성으로 설정되어 있다고 가정합니다. 이 경우 정책 서버는 uid 값(Username=uid)을 사용하여 사용자를 검색합니다.

인증 체계에 대한 검색 사양을 구성하면 LoginID 가 정책 서버에 전달되지 않습니다. 대신에 검색 사양이 사용자를 찾는 데 사용됩니다.

명확성 프로세스에는 다음 두 가지 단계가 포함됩니다.

1. 기본 동작을 통해 또는 Xpath 쿼리를 사용하여 LoginID 를 얻습니다.
2. 기본 동작을 통해 또는 검색 사양을 사용하여 사용자 저장소에서 사용자를 찾습니다.

참고: Xpath 및 검색 사양 사용은 선택 사항입니다.

WS-페더레이션 사용자에 대한 LoginID 얻기

다음 두 가지 방법으로 LoginID 를 찾을 수 있습니다.

- LoginID 가 어설션의 NameID 에서 추출되는 기본 동작 사용. 이 옵션에는 구성이 필요하지 않습니다.
- 기본 동작 대신 Xpath 쿼리를 사용하여 LoginID 찾기

Xpath 쿼리를 지정하려면

1. 구성하고 있는 리소스 파트너에 대한 인증 체계로 이동합니다.
2. "WS-페더레이션 구성", "SAML 프로필"을 차례로 선택합니다. 기존 체계를 수정하고 있으면 먼저 "수정"을 클릭합니다.

   "SAML 프로필" 대화 상자가 열립니다.
3. "사용자 명확성" 섹션에 인증 체계가 LoginID 를 얻는 데 사용하는 Xpath 쿼리를 입력하고 "확인"을 클릭합니다.

   Xpath 쿼리에는 네임스페이스 접두사를 포함할 수 없습니다. 다음은 잘못된 Xpath 쿼리의 예입니다.

   ```
   /saml:Response/saml:Assertion/saml:AuthenticationStatement/
   saml:Subject/saml:NameIdentifier/text()
   ```

   유효한 Xpath 쿼리는 다음과 같습니다.

   ```
   //Response/Assertion/AuthenticationStatement/Subject/
   ```

   NameIdentifier/text()

검색 사양을 사용하여 WS-페더레이션 사용자 찾기

LoginID 가 정책 서버에 전달되는 기본 동작 대신 검색 사양을 사용하여 사용자를 찾을 수 있습니다.

검색 사양으로 사용자를 찾으려면

1. 구성하고 있는 리소스 파트너에 대한 인증 체계로 이동합니다.
2. "WS-페더레이션 구성", "SAML 프로필"을 차례로 선택합니다. 기존 체계를 수정하고 있으면 먼저 "수정"을 클릭합니다.

   "SAML 프로필" 대화 상자가 열립니다.
3. "사용자 명확성" 섹션의 적절한 네임스페이스 필드에 검색 사양을 입력합니다. 검색 사양은 인증 체계가 네임스페이스를 검색하는 데 사용하는 특성을 정의합니다. 입력 시 %s 를 LoginID 를 나타내는 변수로 사용합니다.

   예를 들어 LoginID 의 값이 user1 이라고 가정합니다. "검색 사양" 필드에서 "Username=%s"를 지정하는 경우 결과 문자열은 Username=user1 입니다. 올바른 인증 기록을 찾기 위해 이 문자열이 사용자 저장소와 비교하여 확인됩니다.
4. "확인"을 클릭합니다.

리소스 파트너의 WS-페더레이션 싱글 사인온 구성

"SAML 프로필" 페이지의 "SSO" 섹션에서 인증을 위한 WS-페더레이션 싱글 사인온 바인딩을 구성합니다. 이 섹션에서 단일 사용 어설션 정책을 적용하여 유효한 어설션이 재생되지 않도록 할 수도 있습니다.

싱글 사인온 구성에는 "리디렉션 모드" 설정을 정의하는 단계가 포함됩니다. "리디렉션 모드"는 정책 서버가 (가능한 경우) 대상 응용 프로그램으로 어설션 특성을 보내는 방법을 지정합니다. 어설션 특성을 HTTP 헤더나 HTTP 쿠키로 보낼 수 있습니다.

HTTP 헤더와 HTTP 쿠키에는 어설션 특성이 초과할 수 없는 크기 제한이 있습니다. 크기 제한은 다음과 같습니다.

- HTTP 헤더의 경우 SiteMinder 는 헤더에 대한 웹 서버 크기 제한까지 헤더에 있는 특성을 보낼 수 있습니다. 헤더당 허용되는 어설션 특성은 하나뿐입니다. 헤더 크기 제한을 확인하려면 해당 웹 서버 설명서를 참조하십시오.
- HTTP 쿠키의 경우 SiteMinder 는 쿠키에 대한 크기 제한까지 쿠키를 보낼 수 있습니다. 각 어설션 특성은 자체 쿠키로 전송됩니다. 쿠키 크기 제한은 브라우저별로 다르고, 해당 제한은 각 특성에만 적용되는 것이 아니라 응용 프로그램에 전달되고 있는 모든 특성에 적용됩니다. 쿠키 크기 제한을 확인하려면 해당 웹 브라우저 설명서를 참조하십시오.

WS-페더레이션 싱글 사인온을 구성하려면

1. 구성하고 있는 리소스 파트너에 대한 인증 체계로 이동합니다.
2. "WS-페더레이션 구성", "SAML 프로필"을 차례로 선택합니다. 기존 체계를 수정하고 있으면 먼저 "수정"을 클릭합니다.

   "SAML 프로필" 대화 상자가 열립니다.
3. "SSO" 섹션의 필드에 데이터를 입력합니다.

   필드 설명을 보려면 "도움말"을 클릭하십시오.
4. 제출을 클릭합니다.

WS-페더레이션 사인아웃 구현

사인아웃은 사인아웃을 시작한 브라우저에 대해 모든 사용자 세션을 동시에 종료하는 것입니다. 모든 사용자 세션을 닫으면 권한 없는 사용자가 리소스 파트너의 리소스에 액세스하지 못하게 됩니다.

사인아웃이 반드시 사용자의 모든 세션을 종료하는 것은 아닙니다. 예를 들어 브라우저를 두 개 열어 둔 사용자에게는 두 개의 독립적 세션이 있을 수 있습니다. 이 경우 사인아웃을 시작하는 브라우저에 대한 세션만 해당 세션에 대한 모든 페더레이션된 사이트에서 종료됩니다. 다른 브라우저의 세션은 여전히 활성 상태입니다.

정책 서버는 signoutconfirmurl.jsp 를 사용하여 사인아웃을 수행합니다. 이 페이지는 아이덴티티 공급자 시스템에 있습니다. 아이덴티티 공급자는 사용자 대신 사인아웃 요청을 시작합니다. JSP 는 사용자가 특정 브라우저 세션 중에 사인온한 각 사이트에 사인아웃 요청을 보냅니다. 그러면 사용자가 사인아웃됩니다.

사용자는 아이덴티티 공급자에서만 사인아웃 요청을 시작할 수 있습니다. 적절한 서블릿을 가리키는 링크를 클릭하면 요청이 트리거됩니다. 아이덴티티 공급자 사이트에서 사인아웃 확인 페이지는 보호되지 않는 리소스여야 합니다.

참고: 정책 서버는 사인아웃에 대해 WS-페더레이션 피동 요청 프로필만 지원합니다.

사인아웃 사용

WS-페더레이션 사인아웃을 구성하려면

1. 수정할 인증 체계로 이동합니다.
2. "WS-페더레이션 구성", "SAML 프로필"을 차례로 선택합니다. 기존 체계를 수정하고 있으면 먼저 "수정"을 클릭합니다.

   "SAML 프로필" 대화 상자가 열립니다.
3. "사인아웃" 섹션에서 "사인아웃 사용" 확인란을 선택합니다.
4. 사인아웃 URL 에 대한 값을 입력합니다. URL 은 https:// 또는 http://로 시작해야 합니다.
5. "확인"을 클릭합니다.

추가 정보:

사용자 세션, 어설션 및 만료 데이터 저장 (페이지 107)

사용자 지정 WS-페더레이션 인증 체계 만들기

기존 WS-페더레이션 인증 템플릿 대신 SiteMinder 인증 API 로 작성된 사용자 지정 WS-페더레이션 인증 체계를 사용할 수 있습니다.

기본 인증 체계 페이지의 "체계 설정" 섹션에는 "라이브러리" 필드가 있습니다. 이 필드에는 SAML 아티팩트 인증을 처리하는 공유 라이브러리의 이름이 있습니다. 사용자 지정 인증 체계가 없으면 이 값을 변경하지 마십시오.

HTML 양식 인증에 대한 기본 공유 라이브러리는 smauthhtml 입니다.

메시지 소비자 플러그인으로 어설션 처리 사용자 지정

메시지 소비자 플러그인은 메시지 소비자 플러그인을 구현하는 Java 프로그램입니다. 이 플러그인을 통해 어설션 거부, 상태 코드 반환 등의 어설션 처리를 위한 사용자 고유의 비즈니스 논리를 구현할 수 있습니다. 이 추가 처리는 어설션의 표준 처리와 함께 작동합니다.

참고: 인증 및 명확성의 상태 코드에 대한 자세한 내용은 *SiteMinder Programming Guide for Java*(SiteMinder Java 프로그래밍 안내서)를 참조하십시오.

인증 중에 SiteMinder 는 먼저 사용자를 해당 로컬 사용자 저장소에 매핑하여 어설션을 처리하려고 합니다. 사용자를 찾을 수 없는 경우 SiteMinder 는 메시지 소비자 플러그인의 postDisambiguateUser 메서드를 호출합니다.

플러그인이 사용자를 찾은 경우 SiteMinder 는 인증의 두 번째 단계로 진행합니다. 플러그인이 사용자를 로컬 사용자 저장소에 매핑할 수 없는 경우에는 UserNotFound 오류가 반환됩니다. 플러그인이 선택적으로 리디렉션 URL 기능을 사용할 수 있습니다. 소비자 플러그인이 없는 경우 리디렉션 URL 은 SAML 인증 체계가 생성하는 오류를 기반으로 합니다.

두 번째 인증 단계에서 SiteMinder 는 플러그인이 구성된 경우 메시지 소비자 플러그인의 postAuthenticateUser 메서드를 호출합니다. 메서드가 성공하는 경우 SiteMinder 는 사용자를 요청된 리소스로 리디렉션합니다. 메서드가 실패하는 경우 사용자를 실패 페이지에 보내도록 플러그인을 구성할 수 있습니다. 실패 페이지는 인증 체계 구성으로 지정할 수 있는 리디렉션 URL 중 하나일 수 있습니다.

메시지 소비자 플러그인에 대한 자세한 내용은 다음과 같이 찾을 수 있습니다.

- 참조 정보(메서드 서명, 매개 변수, 반환 값, 데이터 형식)와 UserContext 클래스에 대한 생성자는 *Java Developer Reference*(Java 개발자 참조서)에 나와 있습니다. MessageConsumerPlugin 인터페이스를 참조하십시오.
- 인증 및 권한 부여 API 에 대한 개요와 개념 정보는 *SiteMinder Programming Guide for Java*(SiteMinder Java 프로그래밍 안내서)를 참조하십시오.

플러그인을 구성하려면

1. 아직 설치하지 않은 경우 SiteMinder SDK 를 설치합니다.
2. SiteMinder SDK 의 일부인 MessageconsumerPlugin.java 인터페이스를 구현합니다.
3. 메시지 소비자 플러그인 구현 클래스를 배포합니다.
4. 관리 UI 에서 메시지 소비자 플러그인이 사용되도록 설정합니다.

MessageConsumerPlugin 인터페이스 구현

MessageConsumerPlugin.java 인터페이스를 구현하여 사용자 지정 메시지 소비자 플러그인을 생성하십시오. 다음 절차에는 구현 클래스에 대한 최소 요구 사항이 나열되어 있습니다.

다음 단계를 수행하십시오.

1. 매개 변수가 포함되지 않은 공개 기본 생성자 메서드를 제공합니다.
2. 상태 비저장 구현이 되도록 코드를 제공합니다. 여러 스레드가 단일 플러그인 클래스를 사용할 수 있어야 합니다.

3. 인터페이스에서 요구 사항을 충족할 메서드를 구현합니다.

   MessageConsumerPlugin 에는 다음 네 가지 메서드가 포함됩니다.

   init()

   플러그인에 필요한 초기화 절차를 모두 수행합니다. SiteMinder 는 플러그인이 로드될 때 각 플러그인 인스턴스에 대해 한 번씩 이 메서드를 호출합니다.

   release()

   플러그인에 필요한 런다운 절차를 모두 수행합니다. SiteMinder 는 SiteMinder 가 종료될 때 각 플러그인 인스턴스에 대해 한 번씩 이 메서드를 호출합니다.

   postDisambiguateUser()

   인증 체계가 사용자 명확성 처리를 수행할 수 없을 때 해당 처리를 제공합니다. 또는 이 메서드가 새 페더레이션 사용자에 대한 데이터를 사용자 저장소에 추가할 수 있습니다. 이 메서드는 암호 해독된 어설션을 수신합니다. 암호 해독된 어설션은 플러그인에 전달된 속성 맵의 "_DecryptedAssertion" 키 아래에 추가됩니다.

   postAuthenticateUser()

   정책 서버 처리 성공 여부와 관계없이 최종 어설션 처리 결과를 확인하기 위한 추가 코드를 제공합니다.

SiteMinder 는 다음과 같은 메시지 소비자 플러그인 클래스 샘플을 제공합니다.

installation_home\sdk\samples\messageconsumerplugin 의 MessageConsumerPluginSample.java

installation_home\sdk\samples\authextensionsaml20 의 MessageConsumerSAML20.java

메시지 소비자 플러그인 배포

MessageConsumerPlugin 인터페이스에 대한 구현 클래스를 코드화했으면 해당 구현 클래스를 컴파일하고 SiteMinder 가 실행 파일을 찾을 수 있는지 확인하십시오.

메시지 소비자 플러그인을 배포하려면

1. MessageConsumerPlugin Java 파일을 컴파일합니다. 이 파일을 컴파일하려면 정책 서버와 함께 설치되는 다음 종속 라이브러리가 필요합니다.

   installation_home\siteminder\bin\jars\SmJavaApi.jar

   SmJavaApi.jar 의 동일한 복사본이 SiteMinder SDK 와 함께 설치됩니다. 이 파일은 *installation_home*\sdk\java\SmJavaApi.jar 디렉터리에 있습니다.

   개발 시 두 파일 중 아무 파일이나 사용할 수 있습니다.

2. 폴더나 jar 파일에서 플러그인 클래스를 사용할 수 있는 경우 JVMOptions.txt 파일에서 -Djava.class.path 값을 수정합니다. 이 단계를 수행하면 수정된 클래스 경로를 사용하여 플러그인 클래스를 로드할 수 있습니다. *installation_home*\siteminder\config 디렉터리에서 JVMOptions.txt 파일을 찾습니다.

   참고: 기존 xerces.jar, xalan.jar 또는 SmJavaApi.jar 의 클래스 경로를 수정하지 마십시오.

3. 정책 서버를 다시 시작하여 최신 버전의 MessageConsumerPlugin 을 선택합니다. 이 단계는 플러그인 Java 파일이 다시 컴파일될 때마다 필요합니다.

4. 플러그인이 사용되도록 설정합니다.

WS-페더레이션에 대해 메시지 소비자 플러그인이 사용되도록 설정

메시지 소비자 플러그인을 작성하고 컴파일한 후 관리 UI 에서 설정을 구성하여 플러그인이 사용되도록 설정하십시오. UI 설정은 SiteMinder 에게 플러그인을 찾을 수 있는 위치를 알려 줍니다.

플러그인을 배포 (페이지 178)할 때까지 플러그인 설정을 구성하지 마십시오.

메시지 소비자 플러그인이 사용되도록 설정하려면

1. 관리 UI 에 로그온합니다.

2. 적절한 WS-페더레이션 체계에 대한 "인증 체계" 대화 상자로 이동합니다. "일반" 설정에서 "고급" 섹션으로 이동하고 다음 필드에 데이터를 입력합니다.

   전체 Java 클래스 이름

   플러그인에 대한 Java 클래스 이름을 지정합니다. 예를 들어 SiteMinder SDK 에 포함된 샘플 클래스는 다음과 같습니다.

   com.ca.messageconsumerplugin.MessageConsumerPluginSample

   매개 변수

   "전체 Java 클래스 이름" 필드에서 지정한 플러그인에 전달되는 매개 변수 문자열을 지정합니다.

   관리 UI 에서 플러그인을 구성하는 대신 정책 관리 API(C 또는 Perl)를 사용하여 IdpPluginClass 와 IdpPluginParameters 를 설정할 수 있습니다.

3. 정책 서버를 다시 시작합니다.

실패한 WS-페더레이션 인증 시도 후 사용자 리디렉션

싱글 사인온 처리의 경우 리소스 파트너에서 사용자를 인증할 수 없으면 여러 선택적 리디렉션 URL 을 구성할 수 있습니다. 리디렉션 URL 을 통해 사용자가 리디렉션되는 위치를 세부적으로 제어할 수 있습니다. 예를 들어 사용자 저장소에서 사용자를 찾을 수 없는 경우 사용자를 찾을 수 없음 리디렉션 URL 을 지정하여 사용자를 적절한 위치로 리디렉션할 수 있습니다.

참고: 이러한 URL 은 필수 사항이 아닙니다.

리디렉션 URL 을 구성하지 않으면 표준 SiteMinder 처리가 수행됩니다. SiteMinder 가 실패한 인증을 처리하는 방법은 구성에 따라 달라집니다.

싱글 사인온 트랜잭션 중에 리소스 파트너가 사용자를 인증할 수 없는 경우 리소스 파트너는 추가 처리를 위해 해당 사용자를 사용자 지정된 URL 로 리디렉션할 수 있습니다.

실패한 인증에 대해 여러 선택적 리디렉션 URL 을 구성할 수 있습니다. 어설션이 올바르지 않은 경우 리디렉션 URL 을 통해 사용자가 리디렉션되는 위치를 세부적으로 제어할 수 있습니다. 예를 들어 사용자 저장소에서 사용자를 찾을 수 없는 경우 사용자를 찾을 수 없음 리디렉션 URL 을 입력할 수 있습니다.

"상태 리디렉션 URL 및 모드"는 인증 대화 상자의 "추가 구성" 섹션에 있습니다. 리디렉션 URL 은 다음과 같은 특정 상태 조건에 적용됩니다.

- 사용자를 찾을 수 없습니다.
- 싱글 사인온 메시지가 잘못되었습니다.
- 사용자 자격 증명이 수락되지 않았습니다.

이러한 조건이 하나라도 발생하는 경우 리디렉션 URL 은 추가 작업을 위해 사용자를 응용 프로그램이나 사용자 지정된 오류 페이지로 보낼 수 있습니다.

참고: 리디렉션 URL 구성은 필수 사항이 아닙니다.

선택적 리디렉션 URL 을 구성하려면

1. 수정할 WS-페더레이션 인증 체계로 이동합니다.
2. "WS-페더레이션 구성"을 선택합니다.
3. "고급" 섹션에서 다음 필드 중 하나 이상에 대한 URL 을 입력합니다.
   - Redirect URL for the User Not Found status(사용자를 찾을 수 없음 상태에 대한 리디렉션 URL)
   - Redirect URL for the invalid SSO Message status(잘못된 SSO 메시지 상태에 대한 리디렉션 URL)
   - Redirect URL for the Unaccepted User Credential (SSO Message) status(수락되지 않은 사용자 자격 증명(SSO 메시지)에 대한 리디렉션 URL)

   Redirect URL for the invalid SSO Message status(잘못된 SSO 메시지 상태에 대한 리디렉션 URL)에 대한 값을 입력하는 경우 모드를 선택합니다.

   페더레이션 웹 서비스는 인증 사유를 구성된 리디렉션 URL 중 하나에 매핑하여 오류를 처리합니다. 오류를 보고하기 위해 사용자가 해당 URL 로 리디렉션될 수 있습니다.

참고: 이러한 리디렉션 URL 은 추가 어설션 처리를 위해 SiteMinder 메시지 소비자 플러그인과 함께 사용될 수 있습니다. 인증이 실패하면 플러그인이 사용자를 지정한 리디렉션 URL 중 하나에 보낼 수 있습니다.

SAML 특성을 HTTP 헤더로 제공

어설션 응답이 특성을 어설션에 포함할 수 있습니다. 이러한 특성을 HTTP 헤더 변수로 제공하면 클라이언트 응용 프로그램에서 해당 특성을 사용하여 세부적인 액세스 제어를 구현할 수 있습니다.

특성을 HTTP 헤더에 포함하여 얻을 수 있는 이점은 다음과 같습니다.

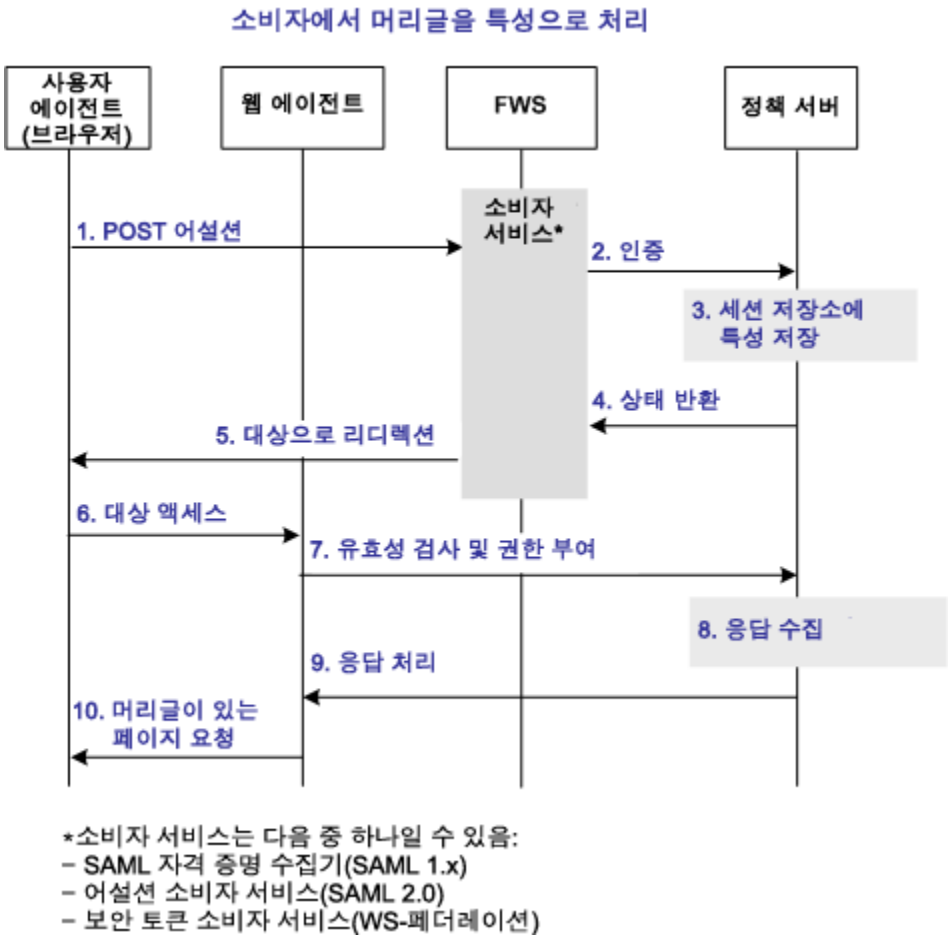
- HTTP 헤더가 영구적이지 않습니다. 즉, HTTP 헤더가 포함된 요청이나 응답 내에서만 표시됩니다.
- SiteMinder 웹 에이전트가 제공한 HTTP 헤더가 브라우저에 표시되지 않으므로 보안 문제가 줄어듭니다.

참고: HTTP 헤더에는 특성이 초과할 수 없는 크기 제한이 있습니다. SiteMinder 는 헤더에 대한 웹 서버 크기 제한까지 헤더에 있는 특성을 보낼 수 있습니다. 헤더당 허용되는 어설션 특성은 하나뿐입니다. 헤더 크기 제한을 확인하려면 해당 웹 서버 설명서를 참조하십시오.

SAML 특성을 HTTP 헤더로 처리하기 위한 사용 사례

인증 중에 일련의 SAML 특성이 어설션에서 추출되어 HTTP 헤더로 제공됩니다. 권한 부여 프로세스 중에 이러한 헤더가 고객 응용 프로그램에 반환됩니다.

다음 순서도에서는 런타임 시 이벤트 순서를 보여 줍니다.



참고: SPS 페더레이션 게이트웨이가 페더레이션 웹 서비스 응용 프로그램 기능을 제공하기 위해 웹 에이전트 및 웹 에이전트 옵션 팩을 대체할 수 있습니다. 흐름도에서 웹 에이전트 블록은 SPS 페더레이션 게이트웨이에 포함된 웹 에이전트입니다. SPS 페더레이션 게이트웨이 설치 및 구성에 대한 자세한 내용은 *Secure Proxy Server Administration Guide*(보안 프록시 서버 관리 안내서)를 참조하십시오.

특성을 HTTP 헤더로 처리하기 위한 이벤트 순서는 다음과 같습니다.

1. 어설션이 어설션 당사자 측에서 생성된 후 해당 어설션이 신뢰 당사자의 적절한 소비자 서비스에 전송됩니다. 전송 메커니즘(POST 또는 아티팩트 또는 WS-페더레이션)은 무관합니다.

   참고: 소비자 서비스는 SAML 자격 증명 수집기(SAML 1.x), 어설션 소비자 서비스(SAML 2.0) 또는 보안 토큰 소비자 서비스(WS-페더레이션)일 수 있습니다.
2. 소비자 서비스가 해당 로컬 정책 서버를 호출하여 구성된 인증 체계를 통해 어설션으로 사용자를 인증합니다.
3. 인증 체계 리디렉션 모드 매개 변수가 PersistAttributes 로 설정된 경우 정책 서버가 세션 저장소에 있는 특성을 세션 변수로 캐시합니다.
4. 인증 결과가 소비자 서비스에 반환됩니다.
5. 소비자 서비스가 브라우저를 보호된 대상 리소스로 리디렉션합니다.
6. 브라우저가 대상 리소스 액세스를 시도합니다.
7. 웹 에이전트가 정책 서버를 호출하여 사용자 세션의 유효성을 검사하고 사용자에게 대상 리소스에 대한 액세스 권한이 부여되었는지 확인합니다.
8. 정책 서버가 구성된 응답별로 특성을 검색합니다.
9. 정책 서버가 응답을 처리하고 특성을 웹 에이전트에 보냅니다.
10. 웹 에이전트가 필요에 따라 HTTP 헤더를 설정합니다.

특성을 HTTP 헤더로 제공하기 위한 구성 개요

세션 저장소에 캐시된 SAML 특성을 검색하여 HTTP 헤더로 제공하려면 여러 구성 단계가 필요합니다.

다음 단계를 수행하십시오.

1. SAML 인증 체계에 대한 리디렉션 모드로 "PersistAttributes"를 선택합니다. 그러면 SAML 특성이 HTTP 헤더로 반환될 수 있습니다.
2. 대상 리소스가 포함된 영역에 대해 권한 부여 규칙을 구성합니다.
3. 대상 리소스를 보호하는 영역에서 "PersistentRealm"을 설정합니다.

4. 헤더로 제공할 SAML 특성 각각에 대해 활성 응답 유형을 사용하는 응답을 구성합니다.
5. 권한 부여 규칙과 활성 응답을 바인딩하여 특성을 HTTP 헤더로 사용하도록 구현하는 정책을 생성합니다.

SAML 특성을 저장하도록 리디렉션 모드 설정

신뢰 당사자가 SAML 어설션으로 사용자를 인증한 후 SAML 특성이 세션 저장소에 기록됩니다. 그런 다음 브라우저가 대상 리소스로 리디렉션됩니다.

특성 데이터와 함께 브라우저를 리디렉션하려면

1. 관리 UI 에 로그인합니다.
2. SAML 인증 체계의 구성 페이지로 이동합니다.
3. "리디렉션 모드" 매개 변수를 "특성 유지"로 설정합니다. 다음과 같이 "리디렉션 모드" 필드를 찾습니다.

   SAML 1.x

   "리디렉션 모드"는 기본 구성 페이지의 "체계 설정" 섹션에 있습니다.

   SAML 2.0

   "SAML 2.0 구성", "SSO"를 차례로 클릭합니다. "리디렉션 모드"는 페이지의 "SSO" 섹션에 있습니다.

   WS-페더레이션

   "WS-페더레이션 구성", "SAML 프로필"을 차례로 클릭합니다. "리디렉션 모드"는 페이지의 "SSO" 섹션에 있습니다.
4. "제출"을 클릭하여 변경 내용을 저장합니다.

이제 리디렉션 모드가 특성 데이터를 전달하도록 설정되었습니다.

사용자의 유효성을 검사하기 위한 권한 부여 규칙 만들기

보호된 대상 리소스가 포함된 영역의 경우 세션 저장소에서 SAML 특성을 검색하기 위한 규칙을 생성하십시오.

규칙은 권한 부여 이벤트(onAccessAccept)를 기반으로 합니다. 사용자는 FWS 응용 프로그램에서 이미 인증되었습니다. 웹 에이전트는 사용자를 다시 인증하고 HTTP 헤더를 전달할 수 없습니다. 특성 검색은 권한 부여 단계에서 발생합니다.

영역에 대한 OnAccessAccept 규칙을 생성하려면

1. 관리 UI 에 로그온합니다.
2. "정책", "도메인", "영역"으로 이동합니다.
3. 대상 리소스가 포함된 영역을 선택합니다.
4. "규칙" 섹션에서 "만들기"를 클릭합니다.

   "규칙 만들기" 페이지가 표시됩니다.
5. 이름과 설명(선택 사항)을 입력합니다.
6. "리소스" 필드에 별표(*)를 입력합니다.
7. "작업" 섹션에서 "권한 부여 이벤트"와 "OnAccessAccept"를 선택합니다.
8. "허용/거부 및 사용/사용 안 함" 섹션에서 "사용"을 선택합니다.
9. "확인"을 클릭하여 규칙을 저장합니다.

이제 보호된 리소스가 포함된 영역에 대한 권한 부여 규칙이 정의되었습니다.

특성을 HTTP 헤더로 보내기 위한 응답 구성

SAML 특성을 웹 에이전트에 HTTP 헤더로 보내는 응답을 구성하십시오. 그러면 웹 에이전트가 응답을 처리하고 헤더 변수를 클라이언트 응용 프로그램에 제공합니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그온합니다.
2. "정책", "도메인", "도메인"으로 이동합니다.
3. 대상 리소스에 대한 도메인을 선택하고 "수정"을 클릭합니다.

4. "응답" 탭을 선택합니다.
5. "만들기"를 클릭합니다.

   "응답" 대화 상자가 열립니다.
6. 이름을 입력합니다.
7. 에이전트 유형이 SiteMinder 웹 에이전트인지 확인합니다.
8. "응답 특성 만들기"를 클릭합니다.

   "응답 특성" 대화 상자가 열립니다.
9. "특성" 필드에서 "WebAgent-HTTP-Header-Variable"을 선택합니다.
10. "특성 종류"에서 "활성 응답"을 선택합니다.
11. 다음과 같이 필드에 데이터를 입력합니다.

    변수 이름

    원하는 헤더 변수 이름을 지정합니다. 사용자가 이 이름을 할당합니다.

    라이브러리 이름

    smfedattrresponse

    이 값은 이 필드에 대한 항목이어야 합니다.

    함수 이름

    getAttributeValue

    이 값은 이 필드에 대한 항목이어야 합니다.

    매개 변수

    어설션에 나타나는 대로 특성 이름을 지정합니다.

    사용자와 페더레이션된 파트너 간의 계약에 따라 어설션에 있는 특성이 결정됩니다.
12. "확인"을 클릭하여 특성을 저장합니다.
13. HTTP 헤더 변수가 될 특성 각각에 대해 절차를 반복합니다. 단일 응답에 대해 여러 특성을 구성할 수 있습니다.

    "응답" 탭으로 돌아갑니다. 생성한 특성이 "특성 목록" 섹션에 나열됩니다.

14. "확인"을 클릭하여 응답을 저장합니다.

    "응답" 탭으로 돌아갑니다.

15. "제출"을 클릭하여 도메인을 저장합니다.

응답이 HTTP 헤더가 될 특성을 웹 에이전트에 보냅니다.

특성을 HTTP 헤더로 구현하기 위한 정책 만들기

SAML 특성을 HTTP 헤더로 사용하도록 구현하려면 정책에서 권한 부여 이벤트 규칙과 활성 응답을 함께 그룹화하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그온합니다.
2. "정책", "도메인", "도메인"으로 이동합니다.
3. 대상 리소스가 포함된 도메인을 선택하고 "수정"을 클릭합니다.
4. "정책" 탭을 선택하고 "정책" 섹션에서 "만들기"를 클릭합니다.

   "정책 만들기" 대화 상자가 열립니다.

5. "이름" 필드에 설명이 포함된 이름을 입력합니다.
6. "사용자" 탭에서 보호된 리소스에 액세스할 수 있는 사용자를 선택합니다.
7. "규칙" 탭에서 이전에 생성한 권한 부여 규칙을 추가합니다.
8. 권한 부여 규칙을 선택하고 "응답 추가"를 클릭합니다.

   "사용 가능한 응답" 대화 상자가 열립니다.

9. 이전에 생성한 활성 응답을 선택하고 "확인"을 클릭합니다.

   "규칙" 탭으로 돌아갑니다. 권한 부여 규칙과 함께 응답이 나타납니다.

10. "제출"을 클릭하여 정책을 저장합니다.

SAML 특성이 HTTP 헤더로 사용되도록 설정하는 정책이 완성되었습니다.

WS-페더레이션 인증 체계로 대상 리소스를 보호하는 방법

WS-페더레이션 인증 체계를 사용하는 SiteMinder 정책을 구성하여 대상 페더레이션 리소스를 보호하십시오.

다음 단계를 수행하십시오.

1. WS-Federation 인증 체계를 사용하는 영역을 생성합니다. 영역은 대상 리소스를 수집한 것입니다.

   다음과 같은 방법으로 영역을 생성할 수 있습니다.

   - 이미 구성된 인증 체계 각각에 대해 고유한 영역을 생성합니다 (페이지 190).
   - 사용자 지정 인증 체계를 사용하여 요청을 해당 WS-Federation 인증 체계로 발송하는 단일 대상 영역을 구성합니다 (페이지 191). 모든 생산자에 대해 단일 대상이 있는 영역 하나를 구성하면 인증을 위한 영역 구성이 단순화됩니다.

2. 연결된 규칙과 응답(선택 사항)을 구성합니다.
3. 대상 리소스를 보호하는 정책으로 영역, 규칙 및 응답을 그룹화합니다.

중요! 영역의 각 대상 URL 은 원치 않는 응답 URL 에서도 식별됩니다. 원치 않는 응답이 리소스 파트너의 초기 요청 없이 계정 파트너에서 리소스 파트너로 전송됩니다. 이 응답에는 대상이 포함되어 있습니다. 계정 파트너에서 관리자가 이 응답을 링크에 포함합니다. 사용자가 링크를 클릭하면 리소스 파트너로 리디렉션됩니다.

각 인증 체계에 대해 고유 영역 구성

각 SAML 또는 WS-페더레이션 인증 체계에 대해 고유 영역을 구성하는 절차는 영역을 생성하는 표준 지침을 따릅니다.

다음 단계를 수행하십시오.

1. "정책", "도메인", "도메인"으로 이동합니다.

   도메인을 생성하는 페이지가 표시됩니다.

2. "도메인 만들기"를 클릭합니다.
3. 도메인 이름을 입력합니다.
4. 도메인에 사용자 디렉터리를 추가합니다. 이 디렉터리는 페더레이션된 리소스에 대한 액세스를 요청하는 사용자가 포함된 디렉터리입니다.

5. "영역" 탭을 선택하고 영역을 생성합니다.
   - "에이전트" 필드에서 대상 리소스가 있는 웹 서버를 보호하는 웹 에이전트를 선택합니다.
   - "인증 체계" 필드에서 적절한 인증 체계를 선택합니다.
6. 영역에 대한 규칙을 생성합니다.

   규칙의 일부로 사용자 인증 시 처리를 제어하는 데 사용되는 작업(Get, Post, or Put)을 선택합니다.
7. "정책" 탭을 선택하고 대상 페더레이션 리소스를 보호하는 정책을 구성합니다. 이전에 생성한 영역을 이 정책과 연결합니다.

이제 고유 영역이 있는 정책이 페더레이션된 리소스를 보호합니다.

모든 인증 체계에 대해 단일 대상 영역 구성

인증 체계에 대한 영역 구성을 단순화하려면 어설션을 생성하는 사이트 여러 개에 대해 단일 대상 영역을 생성하십시오.

이 태스크를 수행하려면 다음 구성 요소를 설정하십시오.

- 단일 사용자 지정 인증 체계

  이 사용자 지정 체계는 이미 각 어설션 당사자에 대해 구성한 해당 SAML 또는 WS-페더레이션 인증 체계에 요청을 전달합니다.
- 대상 URL 이 하나 있는 단일 영역

단일 대상 영역에 대한 인증 체계 만들기

단일 대상 영역에 대한 사용자 지정 인증 체계를 정의하려면

- 인증 체계를 구성해야 합니다.
- 사용자 지정 체계에서 정책 서버에 리소스 요청에 적용할 인증 체계를 알려 주는 매개 변수를 정의해야 합니다.

먼저 구성된 SAML 또는 WS-페더레이션 인증 체계가 있는지 확인하십시오. 없는 경우 사용자 지정 체계가 참조할 수 있는 이러한 체계를 구성하십시오.

인증 체계를 생성하려면

1. "인프라", "인증", "인증 체계"로 이동합니다.

   "인증 체계 만들기" 페이지가 표시됩니다.
2. 사용 중인 프로토콜의 절차에 따라 인증 체계를 하나 이상 생성합니다.
3. "확인"을 클릭하여 종료합니다.

추가 정보:

SAML 1.x 인증 체계 (페이지 167)
WS-페더레이션 인증 체계 개요 (페이지 337)
SAML 2.0 인증 체계를 구성하는 방법 (페이지 267)

사용자 지정 인증 체계 만들기

단일 대상 영역이 특정 사용자 지정 인증 체계를 통해 제대로 작동합니다.

단일 대상 영역에 대한 사용자 지정 인증 체계를 구성하려면

1. "인프라", "인증", "인증 체계"로 이동합니다.

   "인증 체계 만들기" 페이지가 표시됩니다.
2. 다음과 같이 필드에 데이터를 입력합니다.

   이름

   사용자 지정 인증 체계의 설명이 포함된 이름(예: SAML Custom Auth Scheme)을 입력합니다.
3. "체계 일반 설정" 섹션의 다음 필드에 데이터를 입력합니다.

   인증 체계 유형

   사용자 지정 템플릿

   보호 수준

   새 수준 설정의 기본값을 적용합니다.
4. 체계 설정 섹션의 다음 필드에 데이터를 입력합니다.

   라이브러리

   smauthsinglefed

암호

이 필드는 비워 둡니다.

암호 확인

이 필드는 비워 둡니다.

매개 변수

다음 매개 변수 중 하나를 지정합니다.

- SCHEMESET=LIST; <*saml-scheme1*>;<*saml_scheme2*>

  사용할 SAML 인증 체계 이름 목록을 지정합니다. artifact_producer1 이라는 아티팩트 체계와 samlpost_producer2 라는 POST 프로필 체계를 구성한 경우 이러한 체계를 입력합니다. 예를 들면 다음과 같습니다.

  SCHEMESET=LIST;artifact_producer1;samlpost_producer2

- SCHEMESET=SAML_ALL;

  구성된 체계를 모두 지정합니다. 그러면 사용자 지정 인증 체계가 모든 SAML 인증 체계를 열거하고 요청에 대해 올바른 공급자 원본 ID 가 있는 체계를 찾습니다.

- SCHEMESET=SAML_POST;

  구성한 SAML POST 프로필 체계를 모두 지정합니다. 그러면 사용자 지정 인증 체계가 POST 프로필 체계를 열거하고 요청에 대해 올바른 공급자 원본 ID 가 있는 체계를 찾습니다.

- SCHEMESET=SAML_ART;

  구성한 SAML 아티팩트 체계를 모두 지정합니다. 그러면 사용자 지정 인증 체계가 아티팩트 체계를 열거하고 요청에 대해 올바른 공급자 원본 ID 가 있는 체계를 찾습니다.

- SCHEMESET=WSFED_PASSIVE;

  올바른 계정 파트너 ID 가 있는 체계를 찾기 위해 모든 WS-페더레이션 인증 체계를 지정합니다.

SiteMinder 관리자에 대해 이 체계 사용

선택 취소된 상태로 둡니다.

5. 제출을 클릭합니다.

사용자 지정 인증 체계가 완료되었습니다.

단일 대상 영역 구성

인증 체계를 구성하여 사용자 지정 체계와 연결한 후 페더레이션 리소스에 대한 단일 대상 영역을 구성하십시오.

다음 단계를 수행하십시오.

1. "정책", "도메인", "도메인"으로 이동합니다.
2. 단일 대상 영역에 대한 정책 도메인을 수정합니다.
3. "영역" 탭을 선택하고 "만들기"를 클릭합니다.

   "영역 만들기" 대화 상자가 열립니다.
4. 다음 값을 입력하여 단일 대상 영역을 생성합니다.

   이름

   이 단일 대상 영역에 대한 이름을 입력합니다.
5. "리소스" 옵션의 다음 필드에 데이터를 입력합니다.

   에이전트

   대상 리소스가 있는 웹 서버를 보호하는 웹 에이전트를 선택합니다.

   리소스 필터

   대상 리소스의 위치를 지정합니다. 이 위치는 페더레이션된 리소스를 요청하는 사용자가 리디렉션되는 위치입니다.

   예를 들면 /FederatedResources 입니다.
6. "기본 리소스 보호" 섹션에서 "보호됨" 옵션을 선택합니다.
7. "인증 체계" 필드에서 이전에 구성된 사용자 지정 인증 체계를 선택합니다.

   예를 들어 사용자 지정 체계의 이름이 "Fed Custom Scheme"(페더레이션 사용자 지정 체계)인 경우 이 체계를 선택합니다.
8. "확인"을 클릭합니다.

단일 대상 영역 태스크가 완료되었습니다.

단일 대상 영역에 대한 규칙 구성

단일 대상 영역을 구성한 후 리소스를 보호하기 위한 규칙을 구성하십시오.

1. 단일 대상 영역에 대한 "수정" 페이지로 이동합니다.
2. "규칙" 섹션에서 "만들기"를 클릭합니다.

   "규칙 만들기" 페이지가 표시됩니다.
3. 규칙 페이지의 필드에 대한 값을 입력합니다.
4. "확인"을 클릭합니다.

단일 대상 영역 구성에 새 규칙이 포함됩니다.

단일 대상 영역을 사용하여 정책 만들기

단일 대상 영역을 참조하는 정책을 생성하십시오. 단일 대상 영역에서는 요청을 적절한 SAML 인증 체계로 보내는 사용자 지정 인증 체계를 사용합니다.

참고: 이 절차에서는 도메인, 사용자 지정 인증 체계, 단일 대상 영역 및 연결된 규칙을 이미 구성했다고 가정합니다.

다음 단계를 수행하십시오.

1. 이전에 구성한 도메인으로 이동합니다.
2. "정책" 탭을 선택하고 "만들기"를 클릭합니다.

   "정책 만들기" 페이지가 열립니다.
3. "일반" 섹션에 정책의 이름과 설명을 입력합니다.
4. "사용자" 섹션에서 사용자를 정책에 추가합니다.
5. "규칙" 탭에서 단일 대상 영역에 대해 생성한 규칙을 추가합니다.

   나머지 탭은 선택 사항입니다.
6. "확인"을 클릭합니다.
7. "제출"을 클릭합니다.

정책 태스크가 완료되었습니다. 요청으로 인해 이 정책이 트리거되는 경우 단일 영역 및 연결된 인증 체계에 따라 사용자가 인증됩니다.

제 18 장: SAML 2.0 가맹 구성

이 섹션은 다음 항목을 포함하고 있습니다.

가맹 개요

SAML 가맹은 단일 프린서펄에 대한 이름 식별자를 공유하는 SAML 엔터티 그룹입니다.

서비스 공급자와 아이덴티티 공급자가 가맹에 속할 수 있습니다. 하지만 단일 엔터티는 하나의 가맹에만 속할 수 있습니다. 서비스 공급자는 가맹에서 이름 ID 정의를 공유합니다. 아이덴티티 공급자는 가맹에서 사용자 명확성 속성을 공유합니다.

가맹을 사용하면 각 서비스 공급자에 필요한 구성이 줄어듭니다. 또한 프린서펄에 대한 이름 ID 를 하나만 사용하면 아이덴티티 공급자에서 저장소 공간이 절약됩니다.

가맹은 다음과 같은 기능을 제공합니다.

- 싱글 사인온
- 싱글 로그아웃

참고: 가맹 구성은 선택 사항입니다.

싱글 사인온에 대한 가맹

싱글 사인온 사용 사례에서는 서비스 공급자가 아이덴티티 공급자에 어설션 요청을 보냅니다. AuthnRequest 에는 가맹 식별자를 지정하는 특성이 포함되어 있습니다.

아이덴티티 공급자가 요청을 받는 경우 다음 작업이 수행됩니다.

- 서비스 공급자가 AuthnRequest 에 식별된 가맹의 구성원인지 확인합니다.
- 가맹이 공유한 이름 ID 를 사용하여 어설션을 생성합니다.
- 이 어설션을 서비스 공급자에 반환합니다.

어설션을 받는 경우 서비스 공급자에서 인증이 수행됩니다.

싱글 로그아웃에 대한 가맹

로그아웃 요청을 생성할 때 서비스 공급자는 아이덴티티 공급자가 가맹의 구성원인지 여부를 확인합니다. 서비스 공급자는 가맹 ID 로 설정되는 특성을 요청에 포함합니다. 요청을 받는 경우 아이덴티티 공급자는 서비스 공급자가 특성에 식별된 가맹에 속하는지 확인합니다.

아이덴티티 공급자는 세션 저장소의 세션 저장소에서 가맹 이름 ID 를 얻습니다. 모든 세션 참여자에게 로그아웃 요청 메시지를 발행할 때 아이덴티티 공급자는 가맹 구성원에 대한 가맹 이름 ID 를 포함합니다.

SAML 2.0 가맹 구성

SAML 가맹을 사용하면 단일 프린서펄에 대한 이름 식별자를 공유할 수 있도록 그룹에 SAML 엔터티를 추가할 수 있습니다. 페더레이션된 네트워크의 양쪽 파트너 어디에서나 가맹을 구성할 수 있습니다.

아이덴티티 공급자의 경우 가맹과 연결된 이름 ID 를 할당하십시오. 공유된 이름 ID 속성은 가맹에 속한 서비스 공급자 모두에 적용됩니다.

서비스 공급자의 경우 가맹은 인증을 위한 사용자 명확성 프로세스를 제공합니다. 신뢰 당사자는 어설션을 받으면 응용 프로그램에서 특성 값을 사용할 수 있도록 만듭니다. 사용자 명확성 설정을 기반으로 서비스 공급자가 아이덴티티 정보와 로컬 사용자 디렉터리를 비교하여 적절한 사용자 레코드를 찾습니다.

다음 단계를 수행하십시오.

1. "페더레이션", "레거시 페더레이션", "SAML 가맹"으로 이동합니다.

   "SAML 가맹 만들기" 페이지가 표시됩니다.

2. 필요한 필드에 데이터를 입력합니다. 다음 정보에 주의하십시오.
   - 아이덴티티 공급자의 경우 "사용자" 설정에는 아무 기능도 없습니다. 이러한 설정은 무시하십시오.
   - 서비스 공급자의 경우 "이름 ID" 설정에는 아무 기능도 없습니다. 이러한 설정은 무시하십시오.

3. 제출을 클릭합니다.

가맹에 속한 서비스 공급자 목록이 가맹 대화 상자의 "SAML 서비스 공급자 연결" 섹션에 표시됩니다. 이 서비스 공급자 목록은 읽기 전용 목록입니다. 이 목록을 편집하려면 서비스 공급자 개체를 수정하십시오.

사용자 명확성을 위해 가맹을 사용하는 SAML 2.0 인증 체계 목록이 "SAML 인증 체계 연결" 섹션에 표시됩니다. 이 인증 체계 목록은 읽기 전용 목록입니다. 이 목록을 편집하려면 특정 체계를 수정하십시오.

아이덴티티 공급자에서 가맹 할당

아이덴티티 공급자의 경우 가맹은 어설션에 있는 이름 ID 를 제공합니다. 또한 아이덴티티 공급자가 가맹 ID 를 어설션에 포함합니다. 서비스 공급자 개체를 구성할 때 가맹을 선택하십시오.

런타임에 아이덴티티 공급자는 가맹에 대한 NameID 를 사용하고 서비스 공급자 개체에 대해 정의된 이름 ID 구성을 무시합니다.

다음 단계를 수행하십시오.

1. 수정할 서비스 공급자 개체로 이동합니다.
2. "이름 ID" 페이지로 이동합니다.
3. 풀다운 목록에서 SAML 가맹을 선택합니다.

   가맹이 목록에 포함되도록 구성되어 있어야 합니다.

서비스 공급자에서 가맹 할당

서비스 공급자의 경우 가맹에 따라 사용자 정보가 결정됩니다. 서비스 공급자에서 인증 체계를 구성할 때 가맹을 선택하십시오.

런타임에 서비스 공급자는 가맹의 사용자 구성을 사용합니다. 인증 체계의 사용자 구성은 무시됩니다.

다음 단계를 수행하십시오.

1. 수정할 SAML 2.0 인증 체계로 이동합니다.
2. "일반" 페이지로 이동합니다.
3. "사용자 명확성" 섹션의 풀다운 목록에서 SAML 가맹을 선택합니다.

   가맹이 목록에 포함되도록 구성되어 있어야 합니다.

제 19 장: 어설션 쿼리에서 가져온 특성으로 사용자 권한 부여

이 섹션은 다음 항목을 포함하고 있습니다.

특성 기관으로 권한 부여 수행

정책 서버는 다음 유형의 정보를 사용하여 사용자에게 권한을 부여할 수 있습니다.

- 정책 구성에 지정된 사용자
- 정책 식
- 활성 정책
- IP 주소 제한
- 시간 제한

또한 정책 서버는 SAML 2.0 특성 기관이 제공하는 사용자 특성을 사용하여 사용자에게 권한을 부여합니다. 사용자가 보호된 리소스에 대한 액세스를 요청하면 정책 서버는 권한 부여 엔터티로서 추가 사용자 특성을 요청할 수 있습니다. 정책 서버는 리소스에 대한 액세스 권한을 부여하기 전에 이러한 특성을 평가합니다.

SAML 2.0 어설션 쿼리/요청 프로필은 **SAML 특성 기관**과 **SAML 요청자**의 두 개 엔터티를 사용합니다.

SAML 특성 기관

SAML 특성 기관은 특성 서비스에 따라 쿼리 메시지를 처리하고 어설션에 특성을 추가합니다. 이러한 어설션에는 SAML 요청자가 보호된 리소스에 대한 액세스 권한을 부여하는 데 사용하는 사용자 특성이 포함되어 있습니다. 특성 서비스는 페더레이션 웹 서비스 응용 프로그램의 일부입니다.

엔터티가 특성 기관에 요청하는 경우 메시지에는 요청자가 검색할 사용자 특성이 포함되어 있습니다. 메시지에는 요청의 이름 ID 와 발급자도 포함되어 있습니다. 특성 서비스는 요청된 특성에 대해 반환할 값을 알 수 있도록 이름 ID 를 사용하여 사용자를 명확히 구분합니다. 특성 서비스는 SOAP 메시지에 래핑된 특성 어설션이 포함된 응답 메시지를 반환합니다. 이 응답에는 사용자 특성이 포함되어 있습니다.

참고: 특성 기관에서 사용자를 인증할 필요는 없습니다. 기관과 요청자 간의 싱글 사인온 관계도 필요하지 않습니다.

SAML 요청자

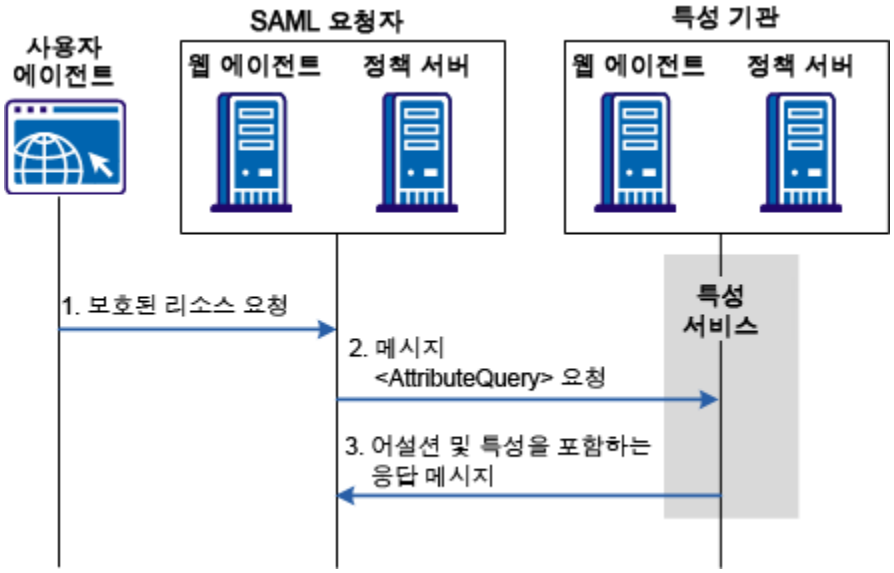
SAML 요청자는 SAML 2.0 어설션 쿼리/요청 프로필을 사용하여 사용자에 대한 특성을 요청하는 SAML 엔터티입니다. SiteMinder 에서 SAML 요청자는 특정 서비스가 아니라 <AttributeQuery> 메시지를 생성하고 처리할 수 있는 정책 서버 기능 그룹입니다. 보호된 대상 리소스가 항상 SAML 요청자에 있으므로 요청자는 특성 기관에 사용자 특성을 요청합니다. 요청자는 이러한 특성을 정책 식이 사용하는 변수로 분석합니다.

참고: SiteMinder 페더레이션 환경에서 SAML 특성 기관은 아이덴티티 공급자이고 SAML 요청자는 서비스 공급자입니다. 하지만 이 조건이 항상 적용되는 것은 아닙니다.

SAML 2.0 사용자 특성에 기반한 권한 부여 요청을 평가하려면 정책 식에 **페더레이션 특성 변수**라는 특성 유형을 추가하십시오. 대상 리소스를 보호하는 정책이 이 변수를 사용합니다. 정책 변수를 기반으로 SAML 요청자가 특성 기관에 쿼리 메시지를 보냅니다. 이 쿼리 메시지에는 특성이 요청되고 있는 SAML 엔터티에 대한 이름 ID 가 포함되어 있습니다. SAML 특성 기관은 특성 명령문과 함께 어설션이 포함된 응답 메시지를 반환합니다.

사용자가 SAML 요청자에서 세션을 가지고 있어야 하지만 사용자가 로그인하거나 특성 기관에서 사용자를 인증할 필요는 없습니다.

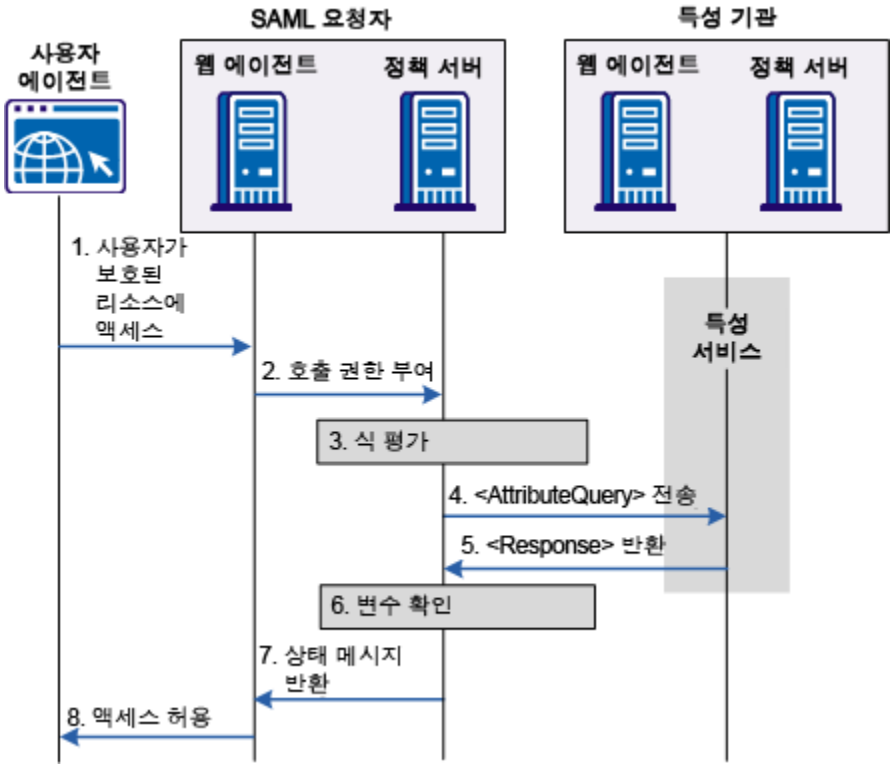
다음 그림에서는 특성 쿼리를 처리하는 방법을 보여 줍니다.



참고: SPS 페더레이션 게이트웨이가 페더레이션 웹 서비스 응용 프로그램 기능을 제공하기 위해 웹 에이전트 및 웹 에이전트 옵션 팩을 대체할 수 있습니다. SPS 페더레이션 게이트웨이 설치 및 구성에 대한 자세한 내용은 *Secure Proxy Server Administration Guide*(보안 프록시 서버 관리 안내서)를 참조하십시오.

사용자 특성을 통한 사용자 권한 부여에 대한 순서도

다음 흐름도에서는 특성 기관을 통한 권한 부여 프로세스를 보여 줍니다.



참고: SPS 페더레이션 게이트웨이가 페더레이션 웹 서비스 응용 프로그램 기능을 제공하기 위해 웹 에이전트 및 웹 에이전트 옵션 팩을 대체할 수 있습니다. SPS 페더레이션 게이트웨이 설치 및 구성에 대한 자세한 내용은 *Secure Proxy Server Administration Guide*(보안 프록시 서버 관리 안내서)를 참조하십시오.

사용자 특성 요청 시퀀스는 다음과 같습니다.

1. 사용자가 보호된 리소스에 액세스합니다. 사용자는 로컬로 로그인하거나 SAML 어설션을 통해 인증을 받을 수 있습니다.
2. SAML 요청자에 있는 웹 에이전트가 로컬 정책 서버를 호출하여 사용자에게 리소스에 액세스할 수 있는 권한이 부여되었는지 여부를 확인합니다. 리소스를 보호하는 정책은 페더레이션된 특성 변수를 통한 권한 부여에 대해 정책 식을 사용합니다.

3. 정책 서버가 해당 변수를 확인하려고 하지만 확인할 수 없습니다. 정책 서버가 로컬 사용자 저장소에서 사용자를 조회하여 사용자의 NameID 를 얻습니다.
4. 특성 쿼리가 특성 기관의 AttributeService URL 로 전송됩니다. AttributeQuery 에는 사용자의 NameID 와 요청된 특성이 포함됩니다.
5. 특성 기관이 요청된 특성과 함께 어설션이 포함된 SAML 응답을 반환합니다.
6. SAML 요청자가 변수 확인을 완료한 다음 정책 식을 평가합니다.
7. 권한 부여 상태 메시지가 웹 에이전트로 반환됩니다.
8. 권한 부여 상태에 따라 웹 에이전트가 요청된 리소스에 대한 액세스를 허용하거나 거부합니다.

특성 기관 및 SAML 요청자를 구성하는 방법

SiteMinder 컨텍스트에서 특성 기관은 아이덴티티 공급자입니다.

SAML 특성 기관으로 작동하도록 SiteMinder 를 구성하려면

1. 사용자를 찾기 위한 검색 사양을 정의합니다. 검색 사양에 NameID 를 입력합니다.
2. 기관이 응답을 쿼리에 보내는 데 사용되는 백 채널을 구성합니다.
3. 쿼리에 대한 응답으로 반환되는 특성을 정의합니다.
4. 사용자에게 특성 기관 서비스에 액세스할 수 있는 권한을 부여합니다.

SiteMinder 컨텍스트에서 SAML 요청자는 서비스 공급자입니다.

SiteMinder 를 SAML 요청자로 구성하려면

1. 특성 쿼리 기능이 사용되도록 설정합니다.
2. 요청자가 기관으로부터 응답을 받는 데 사용되는 백 채널을 구성합니다.
3. 특성 쿼리에서 요청된 특성 목록을 정의합니다.
4. 페더레이션 특성 변수를 구성합니다.
5. 특성 쿼리에 포함하기 위한 NameID 를 구성합니다.

특성 기관 설정

SiteMinder 컨텍스트에서 특성 기관은 특성 기관 서비스가 사용되도록 설정된 아이덴티티 공급자입니다.

참고: 싱글 사인온 등의 다른 아이덴티티 공급자 기능을 구성하지 않아도 아이덴티티 공급자가 특성 기관 역할을 할 수 있습니다.

특성 기관을 구성하려면

1. 관리 UI 에 로그온합니다.
2. SAML 요청자를 나타내는 서비스 공급자 개체로 이동합니다. SAML 요청자가 사용자 특성을 요청합니다.
3. "Modify"(수정)를 선택합니다.

   "SAML 서비스 공급자" 페이지가 열립니다.
4. "특성" 탭을 선택합니다.
5. "특성 서비스" 섹션에서 "사용"을 선택합니다. 이 확인란을 선택하면 특성 기관 기능이 사용되도록 설정됩니다.
6. (선택 사항) "유효 기간" 값을 수정합니다. 기본값인 60 초를 적용할 수 있습니다.

   어설션이 60 초 넘게 유효하도록 하려는 경우에만 이 설정을 수정합니다.

   참고: 필드 설명을 보려면 "도움말"을 클릭하십시오.
7. (선택 사항) 서명 설정 중 하나 또는 둘 모두를 구성합니다. 둘 다 필수 설정이 아닙니다.

   서명된 특성 쿼리 필요

   특성 기관이 SAML 요청자의 서명된 쿼리만 수락하도록 하려는 경우에만 이 옵션을 선택합니다.

   서명 옵션

   SAML 요청자에게 반환될 때 특성 어설션에 서명하거나 SAML 응답에 서명하거나 모두 서명하거나 모두 서명하지 않도록 지정하는 옵션 중 하나를 선택합니다.

8. "사용자 조회" 섹션에서 사용할 네임스페이스에 대한 검색 사양을 지정합니다.

   인증 체계가 검색 문자열로 사용하는 네임스페이스 특성을 입력합니다.

   입력 시 **%s** 를 NameID 를 나타내는 변수로 사용합니다. 예를 들어 NameID 의 값이 user1 이라고 가정합니다. "검색 사양" 필드에서 "Username=%s"를 지정하는 경우 결과 문자열은 Username=user1 입니다. 올바른 인증 기록을 찾기 위해 이 문자열이 사용자 저장소와 비교하여 확인됩니다.

9. "백 채널" 섹션의 다음 필드에 데이터를 입력합니다.

   - 암호
   - 암호 확인

   SAML 2.0 아티팩트 인증을 구성했으면 백 채널에 대한 암호를 이미 구성한 것입니다. 이 암호는 SSO 와 특성 기관 서비스 모두에 사용할 수 있습니다.

10. "제출"을 클릭하여 변경 내용을 저장합니다.

11. 특성 기관에서 특성 구성 (페이지 375)으로 이동합니다.

특성 기관에서 특성 구성

구성하고 있는 특성이 싱글 사인온 요청의 일부인지 아니면 특성 쿼리 요청인지 나타내십시오. "SAML 서비스 공급자 특성" 대화 상자의 "검색 방법" 필드에 따라 특성 기능이 결정됩니다.

동일한 특성을 두 서비스 모두에 사용하려면 동일한 특성 이름과 변수를 사용하는 특성 명령문을 두 개 생성하십시오. 한 특성은 SSO 를 검색 방법으로 사용하고 다른 특성은 특성 서비스를 검색 방법으로 사용합니다.

특성을 구성하려면

1. SSO 어설션에 대한 특성을 구성합니다 (페이지 249).

   특성 기관에서 특성을 구성하는 구성 프로세스는 싱글 사인온 어설션에 대한 특성을 구성하는 것과 동일합니다.

2. SAML 요청자를 나타내는 서비스 공급자 개체에 대한 "특성" 대화 상자로 이동합니다.

3. "특성" 대화 상자의 "특성" 섹션에서 "추가"를 선택합니다.

   "특성 추가" 페이지가 표시됩니다.

4. 페이지의 "특성 설정" 섹션에 있는 "검색 방법" 필드에서 "특성 서비스"를 선택합니다.

   특성 쿼리가 이 특성을 요청하는 경우 "특성 서비스"를 검색 방법으로 선택하면 특성이 특성 어설션에 포함될 대상으로 표시됩니다.

신뢰 파트너에게 특성 기관 서비스에 대한 액세스 권한 부여

특성 기관 서비스가 요청에 대해 응답하려면 신뢰 파트너에게 서비스에 대한 액세스 권한을 부여해야 합니다. 이 작업은 두 단계의 프로세스로 구성됩니다.

1. 페더레이션 에이전트 그룹에 웹 에이전트 추가 (페이지 144)
2. 특성 기관 서비스에 대한 정책에 신뢰 파트너 추가 (페이지 377)

페더레이션 에이전트 그룹에 웹 에이전트 추가

에이전트 그룹 FederationWebServicesAgentGroup 에 FWS 응용 프로그램을 보호하는 웹 에이전트를 추가하십시오.

- ServletExec 의 경우 이 에이전트는 웹 에이전트 옵션 팩이 설치된 웹 서버에 있습니다.
- WebLogic 이나 JBOSS 와 같은 응용 프로그램 서버의 경우 이 웹 에이전트는 응용 프로그램 서버 프록시가 설치된 위치에 설치됩니다. 웹 에이전트 옵션 팩은 다른 시스템에 있을 수 있습니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "인프라", "에이전트", "에이전트"를 차례로 클릭합니다.
3. "에이전트 만들기"를 클릭합니다.
4. 배포에 있는 웹 에이전트의 이름을 지정합니다. "제출"을 클릭합니다.
5. "인프라", "에이전트", "에이전트 그룹"을 차례로 클릭합니다.
6. "FederationWebServicesAgentGroup" 항목을 선택합니다.
7. "추가/제거"를 클릭합니다. 그러면 "에이전트 그룹 구성원" 대화 상자가 열립니다.

8. "사용 가능한 구성원" 목록에서 "선택한 구성원" 목록으로 웹 에이전트를 이동합니다.
9. "확인"을 클릭하여 "에이전트 그룹" 대화 상자로 돌아갑니다.
10. "제출", "닫기"를 차례로 클릭하여 기본 페이지로 돌아갑니다.

특성 기관 서비스에 대한 정책에 신뢰 파트너 추가

특성 기관을 통해 권한 부여를 구현하고 있는 경우 특성 기관 서비스에 액세스할 수 있는 권한이 파트너 관계의 신뢰 당사자에게 필요합니다. SiteMinder 는 정책으로 SAML 2.0 특성 기관을 보호합니다.

정책 서버를 설치하면 FederationWebServicesDomain 이 기본적으로 설치됩니다. 이 도메인에는 특성 서비스에 대한 SAML2FWSAttributeServicePolicy 가 포함되어 있습니다.

모든 관련 신뢰 파트너에게 특성 서비스 정책에 대한 액세스 권한을 부여하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에서 "정책", "도메인", "도메인 정책"으로 이동합니다.

   도메인 정책 목록이 표시됩니다.
2. "SAML2FWSAttributeServicePolicy"를 선택합니다.

   "도메인 정책" 페이지가 열립니다.
3. "수정"을 클릭하여 정책을 변경합니다.
4. "사용자" 탭을 선택합니다.
5. SAML2FederationCustomUserStore 사용자 디렉터리에 대한 대화 상자에서 "구성원 추가"를 클릭합니다.

   "사용자/그룹" 페이지가 열립니다.

   이전에 구성한 가맹 도메인이 "사용자/그룹" 대화 상자에 나열됩니다. 예를 들어 가맹 도메인의 이름이 fedpartners 인 경우 항목은 **affiliate:fedpartners** 입니다.
6. 서비스에 대한 액세스 권한이 필요한 파트너가 있는 가맹 도메인 옆의 확인란을 선택합니다. "확인"을 클릭합니다.

   "사용자 디렉터리" 목록으로 돌아갑니다.

7. "제출"을 클릭합니다.

   정책 목록으로 돌아갑니다.

이제 필요한 신뢰 파트너가 특성 기관 서비스에 액세스할 수 있습니다.

특성 쿼리를 생성하도록 SAML 요청자를 설정하는 방법

SiteMinder 서비스 공급자가 SAML 요청자로 작동하도록 하려면 특성 쿼리를 생성할 수 있도록 SAML 2.0 인증 체계를 구성하십시오. 서비스 공급자 사이트에서 이 구성을 수행하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그온합니다.
2. SAML 2.0 인증 체계 구성으로 이동합니다.
3. 특성 쿼리가 사용되도록 설정하고 특성을 지정합니다 (페이지 378).
4. 특성 쿼리에 대한 이름 ID 를 구성합니다 (페이지 379).
5. 특성 쿼리에 대한 백 채널을 구성합니다. (페이지 380)
6. 페더레이션 특성 변수를 구성합니다. (페이지 380)
7. 페더레이션 특성 변수가 포함된 정책 식을 생성합니다. (페이지 381)

각 단계는 다음 단원에서 자세히 설명합니다.

특성 쿼리가 사용되도록 설정하고 특성 지정

SAML 요청자가 특성 쿼리를 생성하도록 하려면 특성 쿼리 기능이 사용되도록 설정하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그온합니다.
2. SAML 2.0 인증 체계에 대한 인증 구성에 액세스합니다.
3. "특성" 탭을 선택합니다.
4. "특성 쿼리" 섹션에서 "사용"을 선택합니다.

5. (선택 사항) 다음 확인란을 선택합니다.
   - 서명 특성 쿼리
   - 서명된 어설션 필요
   - 모든 특성 가져오기
6. "특성 서비스" 필드에 대한 값을 입력합니다.
7. 페이지의 "특성" 섹션에서 "추가"를 클릭합니다.

   "특성 추가" 페이지가 열립니다.
8. 페이지의 필드에 대한 값을 입력합니다.
9. "확인"을 클릭하여 변경 내용을 저장합니다.

   "특성" 페이지로 돌아갑니다.
10. NameID 를 구성합니다 (페이지 379). 이 NameID 는 특성 기관이 사용하는 특성 쿼리에 포함됩니다.

특성 쿼리에 대한 NameID 구성

특성 기관에 전송되는 쿼리 메시지에는 요청 중인 특성을 가지고 있는 사용자의 이름 ID 가 포함됩니다. 이름 ID 구성에서는 SAML 요청자가 이름 ID 를 얻는 방법을 지정합니다. 그런 다음 요청자가 이름 ID 를 특성 쿼리에 배치합니다.

이름 ID 를 지정하려면

1. SAML 요청자 인증 체계에 대한 "특성" 대화 상자로 이동합니다.
2. 페이지의 "이름 ID" 섹션에서 다음 설정을 정의합니다.
   - 이름 ID 형식
   - 이름 ID 유형
   - 이름 ID 필드

   필드 설명을 보려면 "도움말"을 클릭하십시오.
3. "확인"을 클릭하여 변경 내용을 저장합니다.
4. 백 채널이 아직 구성되지 않은 경우 백 채널을 구성합니다.

특성 쿼리에 대한 백 채널 구성

특성 쿼리는 보안 백 채널을 통해 특성 기관에 전송됩니다.

서비스 공급자와 아이덴티티 공급자 간에 사용할 수 있는 백 채널은 하나뿐입니다. 따라서 특성 쿼리에 대한 백 채널 구성은 SAML 아티팩트 프로필에 사용되는 동일한 백 채널 구성입니다.

백 채널을 구성하려면

1. SAML 요청자에 대한 인증 체계 페이지로 이동합니다.
2. "암호화 및 서명" 탭을 클릭합니다.
3. "백 채널" 섹션의 다음 필드에 데이터를 입력합니다.
   - 인증
   - SP 이름
   - 암호
   - 암호 확인

   필드 설명을 보려면 "도움말"을 클릭하십시오.
4. "확인"을 클릭합니다.

페더레이션 특성 변수 만들기

정책 식에서 페더레이션 특성 변수를 사용하려면 먼저 특성 변수를 생성하십시오.

페더레이션 특성 변수를 정의하려면

1. "정책", "도메인", "변수"로 이동합니다.

   "변수" 대화 상자가 열립니다.
2. "변수 만들기"를 선택합니다.

   구성 마법사의 첫 번째 단계에서 "도메인" 섹션이 표시됩니다.
3. 변수를 추가할 페더레이션 정책 도메인을 선택하고 "다음"을 클릭합니다.

4. "변수 정의" 단계에서 "일반" 섹션의 필드 두 개에 데이터를 입력합니다.

   이름

   변수를 식별합니다.

   변수 유형

   페더레이션 특성

5. "정의" 섹션의 필드에 데이터를 입력합니다.

   필드 설명을 보려면 "도움말"을 클릭하십시오.

6. "마침"을 클릭하여 변수를 저장합니다.

7. 이 변수를 정책 식에 추가합니다. (페이지 381) 그러면 페더레이션된 리소스를 보호하는 정책에서 정책 식을 사용합니다.

참고: 한 정책 식에서 여러 페더레이션 특성 변수를 사용할 수 있습니다. 이 경우 각 변수는 SAML 2.0 인증 체계와 연관이 있습니다. 따라서 단일 식으로 인해 여러 특성 요청이 여러 특성 기관에 전송될 수 있습니다.

페더레이션 특성 변수가 포함된 정책 식 만들기

권한 부여 프로세스의 일부로 페더레이션 특성 변수를 사용하려면 특성 변수를 정책 식에 추가하십시오. 이 정책 식을 SAML 요청자의 대상 리소스를 보호하는 정책과 연결하십시오.

정책 식 만들기에 대한 자세한 내용은 *정책 서버 구성 안내서*의 "정책" 장을 참조하십시오.

제 20 장: SAML 2.0 공급자 메타데이터를 사용하여 구성 간소화

이 섹션은 다음 항목을 포함하고 있습니다.

SAML 2.0 용 메타데이터 도구

정책 서버는 프로그래밍 방식으로 SAML 2.0 메타데이터를 가져오거나 내보내기 위한 메타데이터 도구를 제공합니다. 메타데이터를 사용하면 SiteMinder 를 사용하는 사이트와 타사 또는 SiteMinder 를 사용하는 파트너 간에 효율적으로 페더레이션 구성을 교환할 수 있습니다. 프로그래밍 방식으로 SAML 2.0 메타데이터를 사용하면 수행하는 구성의 양을 제한할 수 있습니다.

메타데이터 도구를 구성하는 명령줄 유틸리티 두 개는 smfedexport 및 smfedimport 입니다.

메타데이터 내보내기에는 다음 유형의 입력이 포함됩니다.

- 사용자 입력
- 메타데이터에 KeyInfo 를 포함하기 위해 인증서 데이터 저장소에 액세스
- 서명하기 위해 인증서 데이터 저장소에 액세스
- 템플릿으로 사용될 수 있는 유사한 메타데이터를 참조하기 위해 정책 저장소에 액세스

메타데이터 가져오기에는 다음이 포함됩니다.

- 사용자 입력
- 정책 저장소에 액세스
- 서명을 확인하기 위해 인증서 데이터 저장소에 액세스(인증서가 구성된 경우)
- 메타데이터 문서의 XML 메타데이터 구문 분석
- 정책 저장소에 관련 메타데이터 저장
- 인증서 데이터 저장소에 메타데이터의 PKI 정보 저장

메타데이터 내보내기 도구

다음과 같은 경우 내보내기 도구를 사용할 수 있습니다.

- 서비스 공급자가 사용할 아이덴티티 공급자 메타데이터 파일을 생성하는 경우

  도구를 사용하여 아이덴티티 공급자가 지원하는 프로필에 대한 정보가 포함된 메타데이터 파일을 생성하십시오. 내보내기 도구가 생성하는 이 XML 출력은 아이덴티티 공급자를 설명합니다. 서비스 공급자로 작동하는 사이트는 이 메타데이터 파일을 가져와서 아이덴티티 공급자와의 관계를 설정할 수 있습니다.

- 기존 서비스 공급자에서 아이덴티티 공급자 메타데이터 파일을 생성하는 경우

  SiteMinder 아이덴티티 공급자는 기존 서비스 공급자 개체에서 메타데이터 파일을 생성합니다. 서비스 공급자 개체를 사용하면 사용자가 구성해야 하는 필수 데이터의 양이 줄어듭니다. 아이덴티티 공급자 메타데이터 파일에 대한 여러 설정이 기존 서비스 공급자에서 파생될 수 있습니다. 또한 SiteMinder 는 서블릿의 기본 이름을 제공합니다.

메타데이터 파일을 사용하려면 아이덴티티 공급자와 서비스 공급자 간의 기존 관계가 설정하고 있는 관계와 유사해야 합니다.

SSO 및 SLO 서블릿 URL 은 페더레이션 웹 서비스 응용 프로그램의 IP 주소 및 포트 앞에 추가되는 기본 서블릿 이름입니다.

서블릿 이름은 다음과 같습니다.

- http://*idp_server:port*/affwebservices/public/saml2sso
- http://*idp_server:port*/affwebservices/public/saml2slo

idp_server:port

웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하는 웹 서버와 포트를 식별합니다.

- 아이덴티티 공급자가 사용할 서비스 공급자 메타데이터 파일을 생성하는 경우

  SiteMinder 서비스 공급자는 자신이 지원하는 프로필에 대한 정보가 포함된 메타데이터 파일을 생성하여 아이덴티티 공급자로 작동하는 사이트와의 페더레이션을 용이하게 할 수 있습니다. 아이덴티티 공급자는 메타데이터 파일을 가져와서 서비스 공급자와의 관계를 설정할 수 있습니다.

- 기존 SAML 2.0 인증 체계에서 서비스 공급자 메타데이터 파일을 생성하는 경우

  SiteMinder 서비스 공급자는 기존 SAML 2.0 인증 체계 개체에서 메타데이터 파일을 생성합니다. 서비스 공급자 개체를 사용하면 사용자가 구성해야 하는 필수 데이터의 양이 줄어듭니다. SP 메타데이터 파일에 대한 여러 설정이 기존 SAML 2.0 인증 체계에서 파생될 수 있습니다. SiteMinder 는 서블릿의 기본 이름을 제공합니다.

  메타데이터 파일을 사용하려면 서비스 공급자와 아이덴티티 공급자 간의 기존 관계가 설정하고 있는 관계와 유사해야 합니다. SSO 및 SLO 서블릿 URL 은 페더레이션 웹 서비스 응용 프로그램의 IP 주소 및 포트 앞에 추가되는 기본 서블릿 이름입니다.

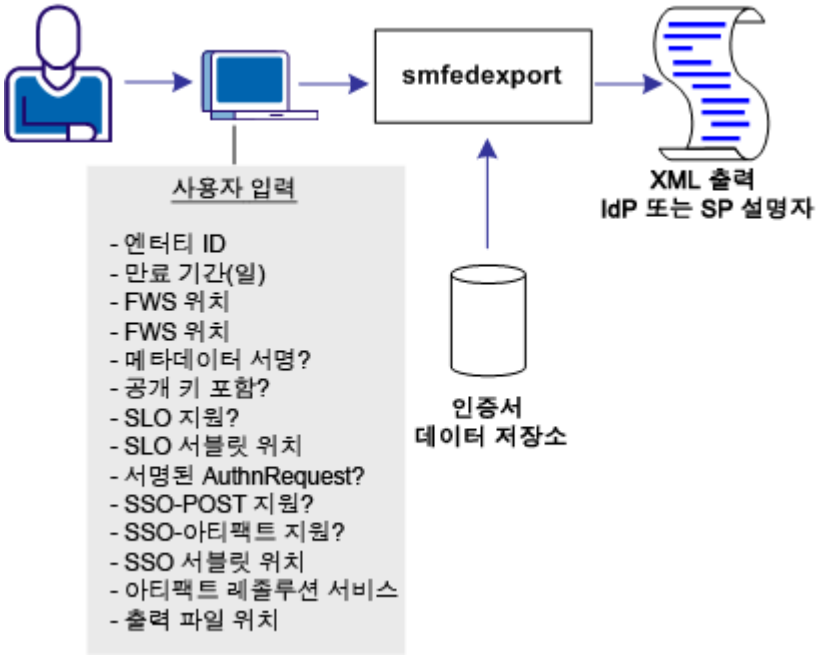
  서블릿은 다음과 같습니다.

  - http://*idp_server:port*/affwebservices/public/saml2sso
  - http://*idp_server:port*/affwebservices/public/saml2slo

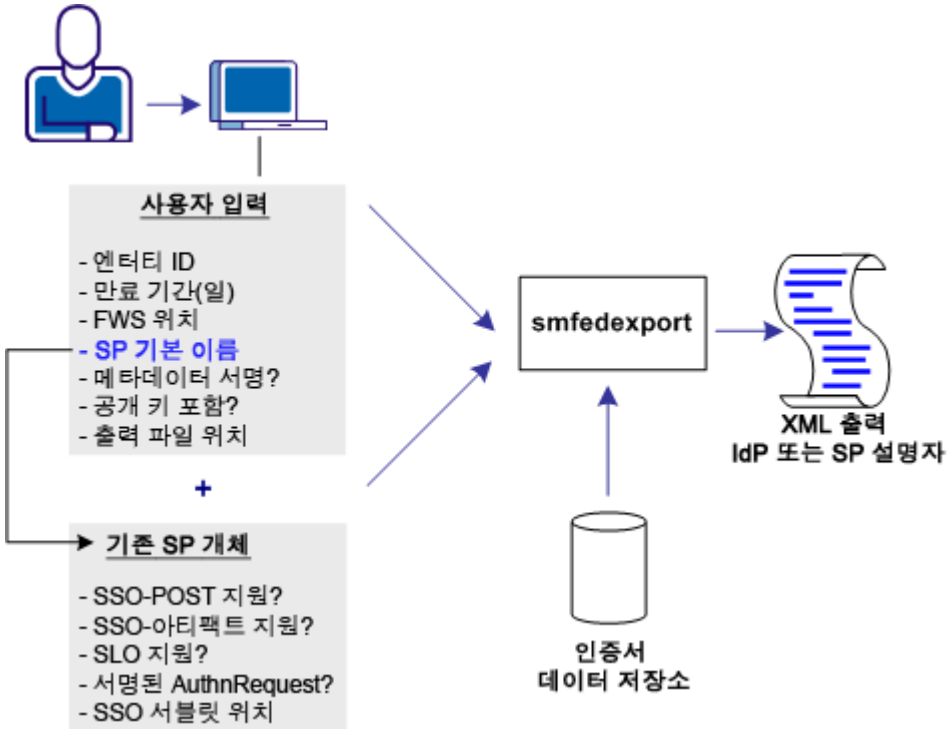
  idp_server:port

  웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하는 웹 서버와 포트를 식별합니다.

다음 그림에서는 사용자 입력에서만 생성되는 메타데이터 파일을 보여 줍니다.



다음 그림에서는 사용자 입력과 기존 서비스 공급자 개체 데이터의 조합에서 생성되는 메타데이터 파일을 보여 줍니다.



smfedexport 도구 실행

smfedexport 도구를 사용하면 SAML 2.0 메타데이터를 XML 파일로 내보낼 수 있습니다.

명령 인수 없이 smfedexport 를 입력하면 모든 명령 인수와 사용법이 표시됩니다.

smfedexport 도구를 실행하려면

1. 정책 서버를 설치한 시스템에서 명령 창을 엽니다.
2. 완료할 태스크에 대한 구문을 사용하여 smfedexport 명령을 입력합니다.

   참고: 대괄호([])로 묶인 명령 인수는 선택 사항입니다.

   SAML 2.0 아이덴티티 공급자 메타데이터 파일을 내보내려면 다음과 같이 입력합니다.

   ```
   smfedexport -type saml2idp [-entityid <entityid>] [-expiredays <num>]
   [-fwsurl <FWS Location> [-spbase <spname>] -username <SiteMinder Admin Name>
   -password <SiteMinder Admin Password>]][-sign][-pubkey]
   [-slo <SLO Service Location> -slobinding <REDIR>] [-reqsignauthr]
   [-sso <SSO Service Location> -ssobinding <REDIR|SOAP>]
   [-ars <Artifact Resolution Service Location>][-output <file>]
   ```

   SAML 2.0 서비스 공급자 메타데이터 파일을 내보내려면 다음과 같이 입력합니다.

   ```
   smfedexport -type saml2sp [-entityid <entityid>] [-expiredays <num>]
   [-fwsurl <FWS Location> [-schemebase <Auth Scheme name>
   -username <SiteMinder Admin Name> -password <SiteMinder Admin Password>]]
   [-sign][-pubkey][-slo <SLO Service Location> -slobinding <REDIR>]
   [-signauthr][-acs <Assertion Consumer Service> -acsbinding <ART|POST|PAOS>
   -acsindex <num>][-acsisdef]][-output <file>]
   ```

   기존 메타데이터 문서에 서명하려면 다음과 같이 입력합니다.

   ```
   smfedexport -type (saml2sp|saml2idp) -sign -input <file> -output <file>
   ```

도구를 실행한 후 XML 파일이 생성됩니다. -type 옵션을 saml2idp 로 설정한 경우 기본 출력 파일 이름은 IDPSSODescriptor.xml 입니다. -type 옵션을 saml2sp 로 설정한 경우 기본 출력 파일 이름은 SPSSODescriptor.xml 입니다.

smfedexport 가 초기 명령 옵션을 처리한 후에는 생성하고 있는 내보내기 파일 유형과 관련된 추가 데이터를 입력하라는 메시지가 표시됩니다. 입력하지 않는 모든 선택적 인수에는 기본값이 사용됩니다.

참고: IdP 메타데이터 파일을 생성하고 있는 경우에는 smfedexport 명령에 정의된 싱글 사인온 서비스가 하나 이상 있어야 합니다. SP 메타데이터 파일을 생성하고 있는 경우에는 smfedexport 명령에 정의된 어설션 소비자 서비스가 하나 이상 있어야 합니다.

smfedexport 에 대한 명령 옵션

다음 표에는 smfedexport 명령줄 옵션이 나열되어 있습니다.

옵션	설명	값
-acs	어설션 소비자 서비스 URL	URL
-acsindex	어설션 소비자 서비스 인덱스 값	정수
-acsisdef	바로 앞의 어설션 소비자 서비스를 기본값으로 만듭니다.	없음
-acsbinding	어설션 소비자 서비스에 대한 SAML 프로토콜 바인딩입니다.	■ ART(아티팩트) ■ POST(POST) ■ PAOS(리버스 SOAP - ECP)
-ars	아티팩트 레졸루션 서비스	URL
-decryptionkeyalias	정책 서버에 인증서(공개 키)를 메타데이터에 포함하도록 지시합니다. 이 인증서는 메타데이터를 암호화합니다. SP 는 해당 개인 키를 사용하여 메타데이터의 암호를 해독합니다.	별칭 이름

옵션	설명	값
-entityid	내보내고 있는 메타데이터가 있는 SP 또는 IDP 의 ID 를 나타냅니다.	URI
-expiredays	메타데이터 문서가 더 이상 유효하지 않을 때까지의 시간(일)입니다.	정수(기본값: 0) 값이 0 이면 메타데이터 문서가 만료되지 않습니다. "validUntil" 요소가 내보낸 XML 에 생성되지 않습니다.
-fwsurl	FWS 응용 프로그램을 가리키는 URL	다음과 같은 형식의 URL: http://*host:port*
-input	기존 XML 파일의 전체 경로	문자열(기본값 없음)
-output	출력 XML 파일의 전체 경로	기본값: IDPSSODescriptor.xml SPSSODescriptor.xml
-password	SiteMinder 관리자 이름 -username 옵션 필요	문자열(기본값 없음)
-pubkey	정책 서버에 인증서(공개 키)를 메타데이터에 포함하도록 지시합니다. 파트너 사이트는 인증서를 서명 암호화 및 확인에 사용합니다. 메타데이터는 서명하지 않아도 되므로 이 설정은 선택 사항입니다.	true(있는 경우) false(그렇지 않은 경우)
-reqsignauthr	서명된 AuthnRequest 필요	true(있는 경우) false(그렇지 않은 경우)
-schemebase	기존 서비스 공급자를 가리킵니다. 프로필/바인딩에 대한 설정은 이 공급자에서 가져옵니다. 다음과 같은 옵션이 필요합니다. -fwsurl -username -password	인증 체계 이름

옵션	설명	값
-spbase	기존 서비스 공급자를 가리킵니다. 프로필/바인딩에 대한 설정은 이 공급자에서 가져옵니다. 다음과 같은 옵션이 필요합니다. -fwsurl -username -password	서비스 공급자 이름
-sign	정책 서버가 메타데이터에 서명하는지 여부를 나타냅니다. 이 설정은 선택 사항입니다.	true(있는 경우) false(그렇지 않은 경우)
-sigalg	SiteMinder 가 어설션 및 어설션 응답, 싱글 로그아웃 요청 및 응답에 서명하는 데 사용하는 서명 해싱 알고리즘을 지정합니다.	rsawithsha1 rsawithsha256
-signauthr	SP 가 AuthnRequest 에 서명하는지 여부를 나타냅니다.	true(있는 경우) false(그렇지 않은 경우)
-signingcertalias	메타데이터에 서명하는 키/인증서 쌍에 대한 별칭을 지정합니다. 인증서 데이터 저장소에 쌍을 저장하십시오. 이 설정은 기본 별칭인 defaultenterpriseprivatekey 를 대신합니다. 이 옵션에 대한 값을 입력하지 않는 경우 정책 서버는 defaultenterpriseprivatekey 별칭을 사용하여 메타데이터에 서명합니다.	별칭 이름
-slo	싱글 로그아웃 서비스 URL	URL
-slobinding	싱글 로그아웃에 사용되는 HTTP 바인딩입니다. HTTP 리디렉션 바인딩이 유일한 옵션입니다.	
-sso	싱글 사인온 서비스 URL	URL

옵션	설명	값
-ssobinding	SSO 서비스 URL 프로토콜 바인딩	■ REDIR(웹 SSO) ■ SOAP(ECP)
-type (필수)	내보내기 파일의 엔터티 유형	saml2idp sam2sp
-username	SiteMinder 관리자 이름 -password 옵션이 필요합니다.	문자열(기본값 없음)

smfedexport 도구 예

예: 아이덴티티 공급자 내보내기

```
smfedexport -type saml2idp -entityid http://www.myidp.com/idp1
-expiredays 30 -sign -pubkey -slohttpredir http://www.mysite.com
/affwebservices/public/saml2slo -reqsignauthr
-ssoart http://www.mysite.com/affwebservices/public/saml2sso
-artressvc http://www.mysite.com/affwebservices/
saml2artifactresolution -output myidpdescription.xml
```

예: 서비스 공급자 내보내기

```
smfedexport -type saml2sp -entityid http://www.myidp.com/sp1
-expiredays 30 -sign -pubkey -slohttpredir http://www.mysite.com/
affwebservices/public/saml2slo -signauthr -aconsvcpost
http://www.mysite.com/affwebservices/public/saml2assertionconsumer
-aconsvcpostindex 12345 -output myidpdescription.xml
```

예: 내보낸 데이터 파일 수정 및 서명

이 예에서는 smfedexport 를 사용하여 XML 파일을 수정하고 디지털로 서명합니다.

메타데이터 파일을 수정하고 서명하려면

1. XML 편집기를 사용하여 기존 XML 파일을 편집합니다.
2. 다음 명령을 입력합니다.

   ```
   smfedexport -sign -input file -output file
   ```

   예:

   ```
   smfedexport -sign -input myspdescription.xml -output newspdescription.xml
   ```

이미 디지털로 서명되어 내보낸 파일을 수정하려면

1. 필요에 따라 XML 편집기를 사용하여 기존 XML 파일을 편집합니다.
2. 파일에서 <Signature> 요소를 삭제합니다.
3. 다음 명령을 입력합니다.

   ```
   smfedexport -sign -input file -output file
   ```

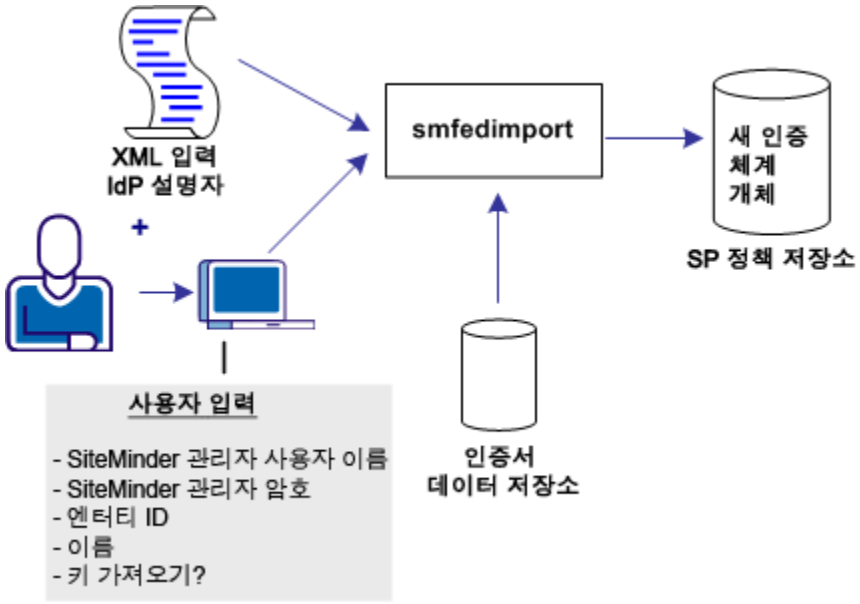
   예:

   ```
   smfedexport -sign -input myspdescription.xml -output newspdescription.xml
   ```

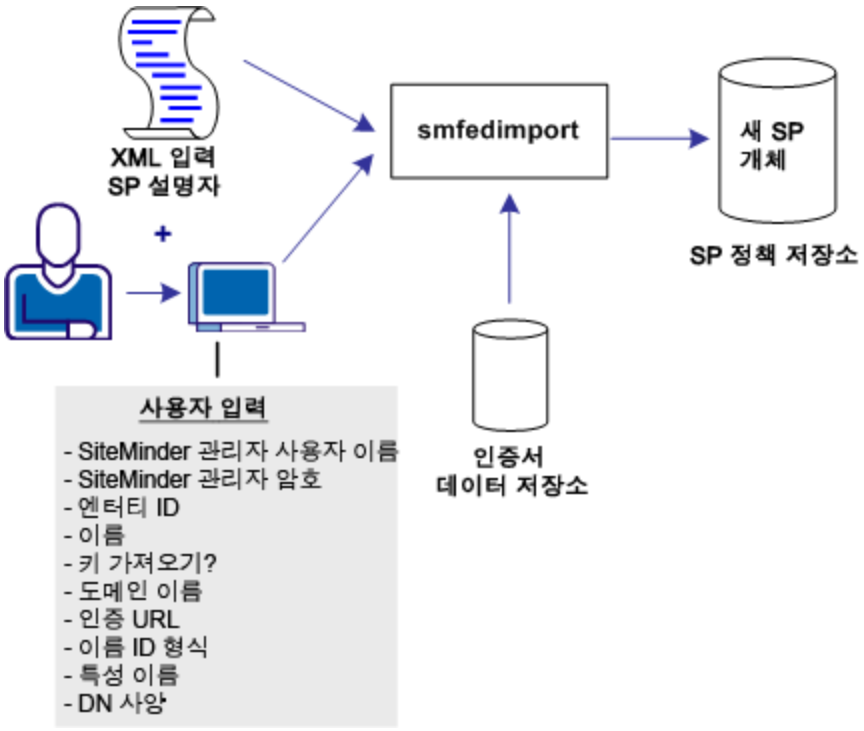
메타데이터 가져오기 도구

가져오기 도구를 사용하여 다음 태스크를 수행할 수 있습니다.

- 다음 그림과 같이 서비스 공급자에 대한 SAML 2.0 인증 체계를 생성합니다.



- 아이덴티티 공급자에 대한 SAML 2.0 서비스 공급자 개체를 생성합니다.



smfedimport 도구 실행

smfedimport 유틸리티에서는 아이덴티티 공급자와 서비스 공급자를 SiteMinder 정책 저장소와 인증서 데이터 저장소로 가져올 수 있습니다. 서비스 공급자 입력 파일을 가져온 결과는 기존 가맹 도메인 내의 새 SiteMinder 서비스 공급자 개체입니다. 아이덴티티 공급자 입력 파일을 가져온 결과는 SiteMinder SAML 2.0 템플릿에 기반한 인증 체계입니다.

smfedimport 명령줄 유틸리티가 실행되는 경우 첫 번째 및 두 번째 매개변수는 SiteMinder 관리자의 사용자 이름 및 암호입니다. 세 번째 및 마지막 인수는 입력 XML 파일의 경로입니다.

smfedimport 도구를 실행하려면

1. 정책 서버를 설치한 시스템에서 명령 창을 엽니다.
2. 다음 구문을 사용하여 명령을 입력합니다.

   SAML2 아이덴티티 공급자 메타데이터 파일을 정책 저장소로 가져오려면 다음과 같이 입력합니다.

   ```
   smfedimport -type saml2idp -username <username>
   -password <password> -entityid <entityid> -name <name>
   [-importkeys <name>] [-silent] -input <file>
   ```

   서비스 공급자 메타데이터 파일을 정책 저장소로 가져오려면 다음과 같이 입력합니다.

   ```
   smfedimport -type saml2sp -username <username>
   -password <password> -entityid <entityid> -domainname <name>
   -authurl <URL> -nameidformat (U|E|X|W|K|N|P|T|U)
   -nameidtype  (S | U | D) -attrname <name> -dnspec <spec>
   -name <name>[-importkeys <name>] [-silent] -input <file>
   ```

   참고: 대괄호([]) 안의 스위치는 선택 사항입니다.

smfedimport 가 초기 명령 옵션을 처리한 후에는 가져오고 있는 파일 유형을 기반으로 추가 데이터를 입력하라는 메시지가 표시됩니다. 명령줄에 입력하지 않는 모든 선택적 인수에는 기본값이 사용됩니다.

smfedimport 도구 예

예: 아이덴티티 공급자 메타데이터 가져오기

```
smfedimport -type saml2idp -username Siteminder

-password siteminderpassword -entityid http://www.myidp.com
-name mynewauthscheme -importkeys keyaliasname -input mypartnersidpinfo.xml
```

예: 서비스 공급자 메타데이터 가져오기

```
smfedimport -type saml2sp -username Siteminder  -password siteminderpassword
-entityid http://www.mysp.com -name mynewsaml2sp -importkeys
keyalisname -domainname myaffiliatedomain
-authurl http://www.mysite.com/login.html -nameidformat U
-nameidtype S -attrname attrname  -input mypartnersspinfo.xml
```

smfedimport 에 대한 명령 옵션

다음 표에는 명령줄 옵션이 나열되어 있습니다.

옵션	설명	값
-attrname	nameID 에 대한 특성 이름	문자열
-authurl	인증 URL	URL
-dnspec	DN 사양(이름 ID 유형만 해당)	문자열
-domainname	가맹 도메인 이름	문자열
-entityid	엔터티 ID	서비스 공급자 ID(가져오기의 경우) 또는 아이덴티티 공급자 ID(내보내기의 경우)
-importkeys	메타데이터에 있는 인증서를 인증서 데이터 저장소로 가져오는지 여부를 나타냅니다.	문자열. 인증서 데이터 저장소에 있는 인증서에 대한 별칭이 되는 이름을 입력하십시오. 인증서가 여러 개 있는 경우 별칭은 name, name1, name2 등으로 추가됩니다.
-input	입력 파일	문자열
-name	서비스 공급자 이름이나 SAML 인증 체계 이름과 같은 SiteMinder 개체 이름을 나타냅니다.	문자열
-nameidformat	이름 ID 형식	(U)지정되지 않음--기본값 (E)전자 메일 주소 (X)509 주체 이름 (W)Windows 도메인 이름 (K)Kerberos 프린서펄 이름 (n)엔터티 식별자 (P)영구 식별자 (T)임시 식별자
-nameidtype	이름 ID 유형	(S)정적 (U)사용자 특성 (D)DN 특성

옵션	설명	값
-password	SiteMinder 관리자 암호	문자열(기본값 없음)
-type (필수)	가져오기 파일의 엔터티 유형	saml2idp sam2sp
-silent	도구가 사용자에게 메시지를 대화형으로 표시하는지 여부를 결정합니다. 이 옵션을 사용하면 도구가 자동 모드로 작동합니다. 도구는 사용자에게 누락된 입력에 대한 메시지를 대화형으로 표시하지 않습니다. 입력 파일의 각 개별 엔터티 가져오기를 수락할지 묻는 메시지도 사용자에게 표시되지 않습니다. 도구는 입력 파일의 모든 엔터티를 가져와야 한다고 가정합니다.	true(있는 경우) false(그렇지 않은 경우)
-username	SiteMinder 관리자 이름	문자열(기본값 없음)

여러 SAML 2.0 공급자가 있는 가져오기 파일 처리

여러 공급자가 가져오기 파일 하나에 지정된 경우 도구는 해당 공급자를 동일한 가맹 도메인으로 가져옵니다. 각 공급자의 이름은 smfedimport 명령 옵션 **-name** 에 대해 지정하는 값을 기반으로 합니다.

예를 들어 가져오기 파일에 서비스 공급자 세 개가 있으면 다음과 같이 지정합니다.

```
-name mySP
```

그러면 가져온 공급자가 mysp, mysp_1 및 mysp_2 로 등록됩니다. 후속 공급자 각각에 대해 정수가 1 씩 증가합니다. 가져오기 파일에 아이덴티티 공급자와 서비스 공급자가 혼합되어 있는 경우에도 여전히 이 명명 규칙이 적용됩니다.

여러 인증서 별칭이 있는 가져오기 파일 처리

가져오기 파일에 여러 인증서가 있는 경우 도구는 해당 인증서를 인증서 데이터 저장소로 가져옵니다. 그런 다음 해당 smfedimport 명령 옵션 **–importkeys** 로 지정하는 값에서 별칭 이름을 할당합니다.

예를 들어 가져오기 파일에 인증서 세 개가 있으면 다음과 같이 지정합니다.

```
-importkeys myalias
```

그러면 가져온 인증서가 myalias, myalias_1 및 myalias_2 로 등록됩니다. 후속 인증서 각각에 대해 정수가 1 씩 증가합니다.

제 21 장: 레거시 페더레이션 추적 로깅

이 섹션은 다음 항목을 포함하고 있습니다.

추적 로깅

SiteMinder 는 웹 에이전트 추적 로깅 기능과 정책 서버 프로파일러를 통해 웹 에이전트 및 정책 서버 성능을 모니터링할 수 있습니다. 이러한 로깅 메커니즘은 성능을 분석하고 문제를 해결할 수 있도록 SiteMinder 프로세스에 대한 포괄적인 정보를 제공합니다.

레거시 페더레이션의 경우 여러 로깅 구성 요소를 사용하여 페더레이션 통신에 대한 추적 메시지를 수집할 수 있습니다. 추적 메시지는 추적, 디버깅 또는 둘 다에 사용할 수 있도록 프로그램 작업에 대한 상세 정보를 제공합니다. 일반적으로 정상 작업 중에는 추적 메시지가 해제됩니다. 추적 메시지가 사용되도록 설정하여 추적 메시지 외에도 상세한 정보를 추출할 수 있습니다. 예를 들어 FWSTrace.log 를 살펴보면 SiteMinder 가 생성하는 SAML 어설션을 확인하거나 현재 사용자의 이름을 수집할 수 있습니다.

수집된 추적 메시지는 추적 로그에 기록됩니다. FWSTrace.log 는 *web_agent_home*/log 디렉터리에 있습니다.

참고: IIS 6.0 서버에서 실행되는 웹 에이전트의 경우 로그 파일은 첫 번째 사용자 요청이 제출된 후에만 생성됩니다. 로그 파일에서 구성을 확인하려면 사용자가 요청을 제출해야 합니다.

웹 에이전트와 정책 서버에서 추적 로그를 설정하여 SiteMinder 작업을 모니터링할 수 있습니다.

추적 로그에 대한 FWS 캐시 플러시

어설션 당사자 또는 신뢰 당사자 측에서 페더레이션 구성을 수정한 경우에는 페더레이션 웹 서비스 캐시를 플러시해야 변경 내용이 추적 로그에 나타납니다. 구성 수정의 예로는 SAML 바인딩이 사용되거나 사용되지 않도록 설정하는 경우를 들 수 있습니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "관리", "정책 서버", "캐시 관리"를 차례로 선택합니다.
3. "모든 캐시" 섹션에서 "모두 플러시"를 클릭합니다.
4. "닫기"를 클릭합니다.

이제 모든 캐시가 지워졌습니다.

Fed_Client 구성 요소에 대한 로그 메시지

웹 에이전트 옵션 팩이 FWS(페더레이션 웹 서비스) 응용 프로그램을 설치합니다. FWS 응용 프로그램은 페더레이션 클라이언트를 나타냅니다. 추적 메시지를 제어하고 FWS 작업을 모니터링하는 구성 요소는 Fed_Client 구성 요소입니다.

FWS 는 웹 에이전트가 추적 메시지를 로깅하는 데 사용하는 일반 추적 기능을 사용합니다. 다음 파일은 추적 로깅을 설정합니다.

추적 구성 파일

FWS 가 모니터링하는 구성 요소와 이벤트를 결정하는 구성 파일을 지정합니다. 기본 파일은 fwstrace.conf 입니다.

추적 로그 파일

모든 로깅된 메시지의 출력 파일을 지정합니다. 웹 에이전트 구성 파일에서 이 파일의 이름과 위치를 제공합니다.

웹 에이전트 구성 파일 또는 에이전트 구성 개체

로깅이 사용되도록 설정하고 로그 형식을 지정하는 로깅 매개 변수를 포함합니다. 이 파일에서는 메시지 콘텐츠를 정의하지 않습니다.

Fed_Client 구성 요소는 다음과 같은 하위 구성 요소를 포함합니다.

싱글 사인온

싱글 사인온 작업을 모니터링합니다.

싱글 로그아웃

싱글 로그아웃 요청을 모니터링합니다.

검색 프로필

아이덴티티 공급자 검색 프로필 작업을 모니터링합니다.

관리

관리 관련 메시지를 감시합니다.

요청

요청 및 인증 작업을 모니터링합니다.

일반

다른 하위 구성 요소가 모니터링하고 있지 않은 작업을 모니터링합니다.

구성

SAML 2.0 서비스 공급자 구성 메시지를 모니터링합니다.

FWS 추적 로깅 구성

페더레이션 웹 서비스 응용 프로그램에 대한 추적 메시지를 수집하려면 FWS 추적 로깅을 구성하십시오.

다음 단계를 수행하십시오.

1. 다음 태스크 중 하나를 수행합니다.
   - 기본 템플릿 FWSTrace.conf 의 복사본을 만들고 모니터링할 데이터만 포함하도록 파일을 수정합니다.
   - 미리 구성된 템플릿 중 하나를 복사하고 새 이름을 할당합니다.

   참고: 템플릿을 직접 편집하지 마십시오.

2. *web_agent_home*/affwebservices/WEB-INF/classes 디렉터리에서 LoggerConfig.properties 파일을 열고 다음 매개 변수를 설정합니다.
   - TracingOn 을 Yes 로 설정합니다. 이 옵션은 파일에 메시지를 쓰도록 추적 기능에 지시합니다.
   - TraceFileName 매개 변수를 추적 로그 파일의 전체 경로로 설정합니다. 기본 위치는 *web_agent_home*/config/FWSTrace.log 에 있습니다.
   - TraceConfigFile 매개 변수를 추적 구성 파일(기본 템플릿 FWSTrace.conf 또는 다른 템플릿)의 전체 경로로 설정합니다. 템플릿은 *web_agent_home*/config 에서 찾을 수 있습니다.
3. 선택적으로 로그 출력이 포함되어 있는 파일인 추적 로그 파일의 형식을 지정할 수 있습니다. 다음 매개 변수는 추적 로그 파일의 형식을 지정하는 웹 에이전트 구성 매개 변수입니다.
   - TraceRollover
   - TraceSize
   - TraceCount
   - TraceFormat
   - TraceDelim

   LoggerConfig.properties 파일에는 이 모든 설정에 대한 설명이 포함되어 있습니다.

Fed_Server 구성 요소에 대한 로그 메시지

정책 서버에서 페더레이션 서비스에 대한 추적 메시지를 제어하는 구성 요소는 Fed_Server 구성 요소입니다. 이 구성 요소는 어설션 생성기와 SAML 인증 체계에 대한 작업을 모니터링합니다. 예를 들어 smtracedefault.log 파일에서 생성된 어설션을 볼 수 있습니다.

정책 서버에서 로깅을 구성하려면 정책 서버 프로파일러를 사용하십시오. 프로파일러를 사용하여 추적 로깅을 위한 다음과 같은 구성 요소를 지정할 수 있습니다.

프로파일러 사용에 대한 자세한 내용은 *SiteMinder 정책 서버 관리 안내서*를 참조하십시오.

페더레이션 서비스 추적 로깅(smtracedefault.log)

프로파일러는 로깅용 정책 서버 기능입니다. 프로파일러를 사용하여 페더레이션 서비스에 대한 추적 메시지를 수집하여 smtracedefault.log 파일에 기록할 수 있습니다.

정책 서버에서 페더레이션 서비스에 대한 추적 메시지를 제어하는 구성 요소는 Fed_Server 구성 요소입니다.

정책 서버 프로파일러를 사용하여 내부 정책 서버 진단 및 처리 기능을 추적할 수 있습니다.

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. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "프로파일러" 탭을 클릭합니다.
3. 프로파일링을 사용하도록 "프로파일링 사용" 옵션을 설정합니다.
4. 프로파일러의 구성 설정을 선택하려면 다음 중 하나를 수행합니다.
   - "구성 파일" 드롭다운 목록에 있는 기본 smtracedefault.txt 파일에 지정된 프로파일러 설정을 그대로 사용합니다.
   - "구성 파일" 드롭다운 목록에서 이 관리 세션 중에 이미 선택된 다른 구성 파일을 선택합니다.
   - "찾아보기" 단추를 클릭하여 다른 구성 파일을 선택합니다.
5. 프로파일러 구성 파일에 저장된 프로파일러 설정을 변경한 후 동일한 파일이나 새 파일에 저장하려면 "설정 구성" 단추를 클릭하여 "정책 서버 프로파일러" 대화 상자를 엽니다.
6. "출력" 그룹 상자에 있는 설정을 조정하여 정책 서버 프로파일러에서 생성되는 정보의 출력 형식을 지정합니다.
7. "적용"을 클릭하여 변경 내용을 저장합니다.

참고:

프로파일러 설정에 대한 변경 내용은 자동으로 적용됩니다. 그러나 정책 서버를 다시 시작하면 새 출력 파일이 생성됩니다(프로파일러의 출력 형식이 파일로 구성된 경우). 기존 프로파일러 출력 파일은 버전 번호를 포함하여 자동으로 저장됩니다. 예를 들면 다음과 같습니다.

```
smtracedefault.log.1
```

Windows 에서 콘솔 로깅을 사용하거나 사용하지 않도록 설정할 때처럼 로깅 또는 추적 기능 설정에 대해 변경한 내용이 프로파일 출력 파일과 관련이 없는 경우 하나의 파일 버전이 저장되지 않고 기존 파일에 새 출력이 추가됩니다.

기본적으로 정책 서버는 최대 10 개의 출력 파일(현재 파일과 백업 파일 9 개)을 보존합니다. 파일 제한 10 개에 도달하면 오래된 파일부터 자동으로 최신 파일로 대체됩니다. TraceFilesToKeep DWORD 레지스트리 설정을 필요한 10 진수 값으로 구성하여 보존할 파일 수를 변경할 수 있습니다. TraceFilesToKeep 레지스트리 설정은 다음 레지스트리 위치에 생성해야 합니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\
LogConfig\TraceFilesToKeep
```

"프로파일러" 탭에 있는 "추적 버퍼링" 옵션은 정책 서버 성능을 높이기 위해 기본적으로 설정되어 있습니다. 이 옵션은 Solaris 시스템에만 해당됩니다.

로그의 FWS 데이터 업데이트

페더레이션 구성의 일부를 수정하는 경우 페더레이션 웹 서비스 캐시를 플러시해야 변경 내용이 추적 로그에 나타납니다.

참고: 변경 후 페더레이션 웹 서비스가 정보를 받기 전에 잠시 지연될 수 있습니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "관리", "정책 서버", "캐시 관리"를 차례로 클릭합니다.

3. 페이지의 "모든 캐시" 섹션에서 "모두 플러시"을 클릭합니다.
4. "닫기"를 클릭합니다.

추적 구성 템플릿으로 로깅 단순화

추적 데이터 수집 태스크를 더 단순화하기 위해 일련의 미리 구성된 템플릿이 정책 서버 및 웹 에이전트 옵션 팩과 함께 설치됩니다. 사용자 고유의 추적 구성 파일을 생성하는 대신 이러한 템플릿을 사용하여 추적 로그에 기록되는 데이터를 수집할 수 있습니다.

FWS 에 대한 추적 로깅 템플릿

다음 템플릿은 페더레이션 웹 서비스에 사용할 수 있습니다.

템플릿	수집되는 추적 메시지
WebAgentTrace.conf	기본 템플릿. 지정하는 데이터를 수집합니다.
FWS_SSOTrace.conf	싱글 사인온 메시지를 수집합니다.
FWS_SLOTrace.conf	싱글 로그아웃 메시지를 수집합니다.
FWS_IPDTrace.conf	아이덴티티 공급자 검색 프로필 메시지를 수집합니다.

이 모든 템플릿에는 추적 중인 특정 데이터에 대한 Fed_Client 구성 요소와 하위 구성 요소가 포함되어 있습니다. 정확한 내용을 보려면 각 템플릿을 살펴보십시오. 템플릿은 *web_agent_home*/config 에 있습니다.

추적 로깅에 템플릿을 사용하려면

1. 사용할 템플릿의 복사본을 만들고 복사본의 이름을 변경합니다.

   참고: 템플릿을 직접 편집하지 마십시오.
2. 에이전트 구성 파일이나 에이전트 구성 개체를 엽니다.
3. TraceFile 매개 변수를 Yes 로 설정합니다.
4. TraceFileName 매개 변수를 추적 로그 파일의 전체 경로로 설정합니다. 이 파일에는 로그 출력이 포함되어 있습니다.

5. TraceConfigFile 매개 변수를 새로 명명된 템플릿 파일의 전체 경로로 설정합니다.
6. 추적 로그 파일의 형식을 지정합니다. 다음 매개 변수는 추적 로그 파일의 형식을 지정하는 웹 에이전트 구성 매개 변수입니다.
   - TraceAppend
   - TraceFormat
   - TraceDelimiter
   - TraceFileSize
   - LogLocalTime

   각 로깅 매개 변수에 대한 설명은 *웹 에이전트 구성 안내서*를 참조하십시오.

참고: IIS 6.0 및 Apache 2.0 서버의 웹 에이전트는 에이전트 구성 파일에서 로컬로 설정된 로그 매개 변수의 동적 구성을 지원하지 않습니다. 따라서 매개 변수를 수정한 후 변경 내용을 적용하려면 에이전트를 다시 시작해야 합니다. 에이전트 구성 개체에서 로그 매개 변수를 구성하는 경우에는 이러한 로그 설정을 동적으로 저장하고 업데이트할 수 있습니다.

FWS 템플릿 샘플

다음 텍스트는 FWS_SLOTrace.conf 템플릿에서 발췌한 내용입니다. 파일의 대부분에는 파일 사용 방법, 명령 구문 및 Fed_Client 구성 요소에 대해 사용 가능한 하위 구성 요소에 대한 설명과 지침이 포함되어 있습니다.

발췌한 내용에서는 모니터링되는 구성 요소 Fed_Client 와 하위 구성 요소(Single_Logout 및 Configuration)를 보여 줍니다. 각 메시지의 필수 콘텐츠를 나타내는 특정 데이터 필드(Date, Time, Pid, Tid, TransactionId, SrcFile, Function, Message)도 보여 줍니다.

```
components: Fed_Client/Single_Logout, Fed_Client/Configuration
data: Date, Time, Pid, Tid, TransactionID, SrcFile, Function, Message
```

IdP 및 SP 에 대한 추적 로깅 템플릿

추적 데이터 수집 태스크를 더 단순화하기 위해 일련의 미리 구성된 템플릿이 정책 서버와 함께 설치됩니다. 사용자 고유의 추적 구성 파일을 생성하는 대신 이러한 템플릿을 사용하여 추적 로그에 기록되는 데이터를 수집할 수 있습니다.

다음 템플릿은 어설션 생성, SAML 인증 등의 아이덴티티 공급자 및 서비스 공급자와 관련된 추적 로깅에 사용할 수 있습니다.

템플릿	수집되는 추적 메시지
samlidp_trace.template	아이덴티티 공급자 작업에 대한 메시지 수집
samlsp_trace.template	서비스 공급자 작업에 대한 메시지 수집

정확한 내용을 보려면 각 템플릿을 살펴보십시오. 템플릿은 *siteminder_home*/config/profiler_templates 에 있습니다.

서비스 공급자 템플릿 샘플

다음 텍스트는 samlsp_trace.template 파일입니다.

```
components: Server/Policy_Server_General, IsProtected/Resource_Protection,
Login_Logout/Authentication, Login_Logout/Policy_Evaluation,
Login_Logout/Active_Expression, Login_Logout/Session_Management,
IsAuthorized/Policy_Evaluation, JavaAPI, Fed_Server/Auth_Scheme,
Fed_Server/Configuration
data: Date, Time, Tid, TransactionID, SrcFile, Function, Domain, Resource, Action,
User, Message
```

레거시 페더레이션의 경우 Fed_Server 구성 요소가 Auth_Scheme 및 Configuration 하위 구성 요소와 함께 포함됩니다.

각 메시지의 필수 콘텐츠를 나타내는 데이터 필드는 다음과 같습니다.

Date, Time, Tid, TransactionId, SrcFile, Function, Domain, Resource, Action User 및 Message

아이덴티티 공급자 프로파일러 샘플

아이덴티티 공급자의 경우 정책 서버 관리 콘솔의 "프로파일러" 탭에 있는 "구성 파일" 필드에서 템플릿을 지정합니다. 다음 텍스트는 "구성 파일" 필드에 대한 샘플 입력입니다.

```
c:\program
files\ca\siteminder\config\profile_templates\samlidp_template.trace
```

프로파일러 사용에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

제 22 장: 동일한 값을 사용해야 하는 구성 설정

이 섹션은 다음 항목을 포함하고 있습니다.

구성 설정 테이블을 사용하는 방법

페더레이션 환경을 구성할 때 트랜잭션의 양쪽 모두에서 일치하는 매개 변수 값을 구성해야 하는 경우가 많습니다.

다음 테이블에서는 각각의 일치하는 매개 변수 집합을 명시적으로 설명합니다. 행의 각 셀에서는 행의 다른 셀에 설명된 해당 값과 일치해야 하는 설정을 설명합니다.

참고: 이 정보는 어설션 당사자 및 신뢰 당사자가 SiteMinder 시스템인 환경에만 적용됩니다.

SAML 1.x 의 일치하는 구성 설정

다음 표에는 SAML 1.x 생산자와 소비자에서 동일한 값으로 설정해야 하는 SiteMinder 구성 설정이 나열되어 있습니다. 또한 이러한 설정이 있는 대화 상자나 파일도 나와 있습니다. 이러한 설정의 대부분은 관리 UI 에 있지만 일부 매개 변수는 속성 파일에 있거나 링크의 일부입니다.

- 첫 번째 열에서는 소비자의 관리 UI 에서 구성해야 하는 설정을 설명합니다.
- 두 번째 열에서는 생산자의 관리 UI 에서 구성해야 하고 소비자의 설정과 일치해야 하는 설정을 설명합니다.

중요! URL 을 입력해야 하는 경우 콜론 뒤에 오는 URL 문자열은 대/소문자를 구분합니다. 예를 들어 **http:** 뒤에 오는 텍스트는 모두 대/소문자를 구분합니다. 따라서 모든 대상자 관련 설정과 어설션 소비자 URL 관련 설정에 있는 URL 의 대/소문자가 일치해야 합니다.

SAML 1.x 소비자의 설정	SAML 1.x 생산자의 일치해야 하는 설정
가맹 이름 인증 체계 페이지의 "체계 설정" 섹션(아티팩트 및 POST 프로필)	**이름** 필드 가맹 개체에 대한 일반 설정 값은 소문자여야 함 생산자의 사이트 간 전송 URL 링크에 있는 **NAME** 쿼리 매개 변수
암호 필드 (SAML 아티팩트 인증 체계만 해당) 인증 체계 페이지의 "체계 설정" 섹션	**암호/암호 확인** 필드 가맹 개체에 대한 일반 설정
대상자 필드 기타 모든 SAML 소비자. 인증 체계 페이지의 "체계 설정" 섹션	**대상자** 필드 가맹 개체에 대한 어설션 설정

SAML 1.x 소비자의 설정	SAML 1.x 생산자의 일치해야 하는 설정
어설션 소비자 URL (SAML POST 인증 체계만 해당) 인증 체계 페이지의 "체계 설정" 섹션	**어설션 소비자 URL** 가맹 개체에 대한 어설션 설정 **SMCONSUMERURL** 쿼리 매개 변수 생산자의 사이트 간 전송 URL 링크
발급자 필드 인증 체계 페이지의 "체계 설정" 섹션	**AssertionIssuerID** 매개 변수 생산자의 AMAssertionGenerator.properties 파일
"SAML 버전" 드롭다운 목록의 버전 체계 설정 섹션-- 인증 체계 페이지 (SAML 아티팩트 인증 체계만 해당)	**"SAML 버전" 드롭다운 목록의 버전** 가맹 개체에 대한 어설션 설정
회사 원본 ID 체계 설정 섹션-- 인증 체계 페이지 (SAML 아티팩트 인증 체계만 해당)	**SourceID** 매개 변수 생산자의 AMAssertionGenerator.properties 파일

SAML 2.0 의 일치하는 구성 설정

다음 표에는 SAML 2.0 아이덴티티 공급자 및 서비스 공급자에서 동일한 값으로 설정해야 하는 SiteMinder 구성 설정이 나열되어 있습니다. 이러한 설정이 있는 위치도 나와 있습니다. 이러한 설정의 대부분은 관리 UI 에 있지만 일부 매개 변수는 속성 파일에 있거나 링크의 일부입니다.

- 첫 번째 열에서는 서비스 공급자의 관리 UI 에서 구성해야 하는 설정을 설명합니다.
- 두 번째 열에서는 아이덴티티 공급자의 관리 UI 에서 구성해야 하고 서비스 공급자의 설정과 일치해야 하는 설정을 설명합니다.

중요! URL 을 입력해야 하는 경우 콜론 뒤에 오는 URL 문자열은 대/소문자를 구분합니다. 예를 들어 **http:** 뒤에 오는 텍스트는 대/소문자를 구분합니다. 따라서 모든 SP ID 및 IdP ID 관련 설정의 대/소문자가 일치해야 합니다.

서비스 공급자의 설정	일치해야 하는 아이덴티티 공급자의 설정
특성 이름 SAML 2.0 인증 체계의 "특성" 설정에 있는 "Add/Edit Attribute"(특성 추가/편집) 페이지	**변수 이름** SAML 서비스 공급자 개체에 대한 "특성" 설정에 있는 "특성 추가" 페이지의 "특성 설정" 섹션
대상자 필드 ■ 기타 모든 SAML 서비스 공급자 ■ SAML 2.0 인증 체계의 "SSO" 설정	**대상자** 필드 SAML 서비스 공급자 개체에 대한 "SAML 프로필" 설정의 "SSO" 섹션
IdP ID 필드 SAML 2.0 인증 체계의 "일반" 설정	**IdP ID** 필드 ■ SAML 서비스 공급자 개체에 대한 "일반" 설정 ■ 아이덴티티 공급자에서 시작되는 SSO 의 경우--원치 않는 응답에 있는 **SPID** 쿼리 매개변수
로컬 이름 SAML 2.0 인증 체계의 "특성" 설정에 있는 "Add/Edit Attribute"(특성 추가/편집) 페이지 **로컬 이름** SAML 요청자(서비스 공급자)에서 페더레이션 특성 변수를 생성하기 위한 "페더레이션 특성 변수" 페이지	없음
SP ID 필드 ■ SAML 2.0 인증 체계의 "일반" 설정 ■ 서비스 공급자에서 시작되는 SSO 의 경우--아이덴티티 공급자에 대한 하드 코드된 링크에 있는 **ProviderID** 쿼리 매개변수	**SP ID** 필드 SAML 서비스 공급자 개체에 대한 "일반" 설정
SP Name(Well-Known 이름) SAML 2.0 인증 체계에 대한 "암호화 및 서명" 설정의 "백 채널" 섹션 이 값은 소문자여야 합니다.	**이름** 필드 SAML 서비스 공급자 개체에 대한 "일반" 설정 이 값은 소문자여야 합니다.

WS-페더레이션 구성 설정

다음 표에는 WS-페더레이션 계정 파트너와 리소스 파트너에서 동일한 값으로 설정해야 하는 SiteMinder 구성 설정이 나열되어 있습니다. 다음과 같이 표를 읽으십시오.

- 첫 번째 열에서는 리소스 파트너의 관리 UI 에서 구성해야 하는 설정을 설명합니다.
- 두 번째 열에서는 계정 파트너의 관리 UI 에서 구성해야 하고 소비자의 설정과 일치해야 하는 설정을 설명합니다.

중요! URL 을 입력해야 하는 경우 콜론 뒤에 오는 URL 문자열은 대/소문자를 구분합니다. 예를 들어 **http:** 뒤에 오는 텍스트는 모두 대/소문자를 구분합니다. 따라서 모든 RP ID 및 AP ID 관련 설정의 대/소문자가 일치해야 합니다.

리소스 파트너의 설정	일치해야 하는 계정 파트너의 설정
리소스 파트너 ID WS-페더레이션 인증 체계의 일반 설정	**리소스 파트너 ID** 리소스 파트너 개체의 일반 설정 wtrealm 쿼리 매개 변수는 계정 파트너에서 시작되는 SSO 를 트리거하도록 하드 코드된 링크에 대한 리소스 파트너 ID 로 설정해야 합니다.
계정 파트너 ID WS-페더레이션 인증 체계의 일반 설정	**계정 파트너 ID** 리소스 파트너 개체의 일반 설정

제 23 장: SiteMinder 에서 사용되는 페더레이션 웹 서비스 URL

이 섹션은 다음 항목을 포함하고 있습니다.

페더레이션 서비스 URL

페더레이션 웹 서비스에는 여러 레거시 페더레이션 구현 서비스가 포함되어 있습니다. 관리 UI 를 통해 싱글 사인온, 싱글 로그아웃 또는 아이덴티티 공급자 검색 프로필을 구성하는 경우 다양한 서비스를 참조하는 URL 을 지정해야 합니다.

다음과 같은 서비스 설명이 포함됩니다.

- 서비스에 대한 간단한 설명
- 서비스에 대한 URL
- URL 을 입력하는 관리 UI 의 필드
- Web.xml 파일의 연결된 서블릿 및 서블릿 매핑

Web.xml 파일은 페더레이션 웹 서비스 응용 프로그램에 대한 배포 설명자 중 하나입니다. 이 파일에는 서블릿 및 URL 매핑이 나열되어 있습니다.

어설션 당사자의 서비스 URL

다음 서비스가 어설션 당사자(생산자/아이덴티티 공급자/계정 파트너)에서 제공되지만 신뢰 당사자(소비자/서비스 공급자/리소스 파트너)에서 서비스 URL 을 입력합니다.

페더레이션 웹 서비스 응용 프로그램에서는 다음 서비스를 제공합니다.

- 사이트 간 전송 서비스 (페이지 418)(SAML 1.x 생산자)
- 어설션 검색 서비스 (페이지 419)(SAML 1.x 생산자)
- 아티팩트 레졸루션 서비스 (페이지 420)(SAML 2.0 IdP)
- 싱글 사인온 서비스 (페이지 422)(SAML 2.0 IdP)
- 싱글 로그아웃 서비스 (페이지 424)(SAML 2.0 IdP)
- 아이덴티티 공급자 검색 프로필 서비스 (페이지 426)(SAML 2.0)
- 특성 서비스 (페이지 427)(SAML 2.0)
- 싱글 사인온 서비스 (페이지 423)(WS-페더레이션)
- 사인아웃 서비스 (페이지 425)(WS-페더레이션)
- WSFedDispatcher 서비스 (페이지 428)(WS-페더레이션)

사이트 간 전송 서비스 URL(SAML 1.x)

SAML 1.x POST 및 아티팩트 프로필의 경우 사이트 간 전송 URL 은 생산자에서 소비자로 사용자를 전송하는 생산자 측 구성 요소입니다.

이 서비스에 대한 기준 URL

http://*producer_server:port*/affwebservices/public/intersitetransfer

producer_server:port

웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하는 생산자 시스템의 웹 서버 및 포트 번호를 식별합니다.

사이트 간 전송 URL

생산자의 페이지에 있는 하드 코드된 링크에 URL 을 포함합니다.

Web.xml 파일의 연결된 서블릿 및 서블릿 매핑

```
<servlet>
  <servlet-name>intersiteTransferService</servlet-name>
  <display-name>Intersite Transfer Service</display-name>
  <description>This servlet acts as the Intersite Transfer URL.</description>
  <servlet-class>com.netegrity.affiliateminder.webservices.
    IntersiteTransferService
  </servlet-class>
</servlet>


<servlet-mapping>
  <servlet-name>intersiteTransferService</servlet-name>
  <url-pattern>/public/intersitetransfer/*</url-pattern>
</servlet-mapping>
```

어설션 검색 서비스 URL(SAML 1.x)

어설션 검색 서비스는 SAML 1.x 소비자 사이트에 대한 어설션을 검색합니다.

이 서비스에 대한 기준 URL

- 기본 인증 또는 SSL 을 통한 기본 인증으로 이 서비스를 보호하는 경우의 URL:
  https://producer_server:port/affwebservices/assertionretriever
- 클라이언트 인증서 인증으로 이 서비스를 보호하는 경우의 URL:
  https://producer_server:port/affwebservices/certassertionretriever

producer_server:port

웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하는 생산자 시스템의 웹 서버 및 포트 번호를 식별합니다.

어설션 검색 URL

"어설션 검색 URL" 필드에서 지정됩니다. 이 필드는 SAML 1.x 인증 체계 페이지의 "체계 설정" 섹션에 있습니다.

Web.xml 파일의 연결된 서블릿 및 서블릿 매핑

```
<servlet>
  <servlet-name>assertionretriever</servlet-name>
  <display-name>SAML Assertion Retrieval servlet</display-name>
  <description>This servlet processes the HTTP post based SAML requests and
returns the SAML Response elements. Both SAML Request and Response elements are
SOAP encoded.</description>
  <servlet-class>com.netegrity.affiliateminder.webservices.
     AssertionRetriever</servlet-class>
</servlet>


<servlet-mapping>
  <servlet-name>assertionretriever</servlet-name>
  <url-pattern>/assertionretriever/*</url-pattern>
</servlet-mapping>
<servlet-mapping>

  <servlet-name>assertionretriever</servlet-name>
  <url-pattern>/certassertionretriever/*</url-pattern>
</servlet-mapping>
```

아티팩트 레졸루션 서비스 URL(SAML 2.0)

아티팩트 레졸루션 서비스는 서비스 공급자에 대한 SAML 2.0 어설션을 검색합니다.

이 서비스에 대한 기준 URL

- 기본 인증으로 이 서비스를 보호하는 경우 URL 은 다음과 같습니다.

  http://*idp_server:port*/affwebservices/saml2artifactresolution

- SSL 을 통한 기본 인증이나 X.509 클라이언트 인증서 인증으로 이 서비스를 보호하는 경우 URL 은 다음과 같습니다.

  https://*idp_server:port*/affwebservices/saml2certartifactresolution

idp_server:port

웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하는 웹 서버와 포트를 식별합니다.

레졸루션 서비스 URL

"레졸루션 서비스" 필드에서 지정됩니다. 이 필드는 SAML 2.0 인증 체계에 대한 "SSO" 설정의 "바인딩" 섹션에 있습니다. 필드를 활성화하려면 "HTTP-아티팩트"를 바인딩으로 선택하십시오.

Web.xml 파일의 연결된 서블릿 및 서블릿 매핑

```
<servlet>
  <servlet-name>saml2artifactresolution</servlet-name>
  <display-name>SAML 2.0 Single Sign-On service</display-name>
  <description>This servlet is the SAML 2.0 Artifact Resolution
      service at an IdP.</description>
  <servlet-class>com.netegrity.affiliateminder.webservices.
    saml2.ArtifactResolution</servlet-class>
</servlet>


<servlet-mapping>
<servlet-name>saml2artifactresolution</servlet-name>
<url-pattern>/saml2artifactresolution/*</url-pattern>
</servlet-mapping>


<servlet-mapping>
<servlet-name>saml2artifactresolution</servlet-name>
<url-pattern>/saml2certartifactresolution/*</url-pattern>
</servlet-mapping>
```

싱글 사인온 서비스 URL(SAML 2.0)

싱글 사인온 서비스는 SAML 2.0 에 대한 싱글 사인온을 구현합니다.

이 서비스에 대한 기준 URL

http://*idp_server:port*/affwebservices/public/saml2sso

idp_server:port

웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하는 웹 서버와 포트를 식별합니다.

SSO 서비스 URL

"SSO 서비스" 필드에서 지정됩니다. 이 필드는 SAML 2.0 인증 체계에 대한 "SSO" 설정에 있습니다.

Web.xml 파일의 연결된 서블릿 및 서블릿 매핑

```
<servlet>
  <servlet-name>saml2sso</servlet-name>
  <display-name>SAML 2.0 Single Sign-On service</display-name>
  <description>This servlet is the SAML 2.0 Single Sign-On service at an
IdP.</description>
  <servlet-class>com.netegrity.affiliateminder.webservices.
saml2.SSO</servlet-class>
</servlet>


<servlet-mapping>
  <servlet-name>saml2sso</servlet-name>
  <url-pattern>/public/saml2sso/*</url-pattern>
</servlet-mapping>
```

싱글 사인온 서비스 URL(WS-페더레이션)

WS-페더레이션 싱글 사인온 서비스는 WS-페더레이션에 대한 싱글 사인온을 구현합니다.

이 서비스에 대한 기준 URL

http://*ap_server:port*/affwebservices/public/wsfedsso

ap_server:port

계정 파트너에 있는 시스템의 서버 및 포트 번호를 지정합니다. 시스템은 페더레이션 네트워크에 설치된 구성 요소에 따라 웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하고 있습니다.

SSO 서비스 URL

"SSO 서비스" 필드에서 지정됩니다. 이 필드는 WS-페더레이션 인증 체계의 "SSO" 설정에 있습니다.

Web.xml 파일의 연결된 서블릿 및 서블릿 매핑

```
<servlet>
<servlet-name>wsfedsso</servlet-name>
<display-name>WSFED Single Sign-On service</display-name>
<description>This servlet is the WSFED Single Sign-On service at an Account
Partner.</description>
<servlet-class>com.netegrity.affiliateminder.webservices.wsfed.SSO
  </servlet-class>
</servlet>

<servlet-mapping>
<servlet-name>wsfedsso</servlet-name>
<url-pattern>/public/wsfedsso/*</url-pattern>
</servlet-mapping>
```

IdP 의 싱글 로그아웃 서비스 URL(SAML 2.0)

이 서비스는 SAML 2.0 에 대한 싱글 로그아웃을 구현합니다.

이 서비스에 대한 기준 URL

http://*idp_server:port*/affwebservices/public/saml2slo

idp_server:port

웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하는 웹 서버와 포트를 식별합니다.

SLO 위치 URL/SLO 응답 위치 URL

아이덴티티 공급자에 있는 동일한 이름의 필드에서 지정됩니다. 이러한 필드는 SAML 서비스 공급자 개체에 대한 "SAML 프로필" 설정의 "SLO" 섹션에 있습니다.

Web.xml 파일의 연결된 서블릿 및 서블릿 매핑

```
<servlet>
  <servlet-name>saml2slo</servlet-name>
  <display-name>SAML 2.0 Single Logout service</display-name>
  <description>This servlet is the SAML 2.0 Single Logout service at an
IdP.</description>
  <servlet-class>com.netegrity.affiliateminder.webservices.
     saml2.SLOService</servlet-class>
</servlet>

<servlet-mapping>
  <servlet-name>saml2slo</servlet-name>
  <url-pattern>/public/saml2slo/*</url-pattern>
</servlet-mapping>
```

AP 의 사인아웃 서비스 URL(WS-페더레이션)

이 사인아웃 서비스는 WS-페더레이션 사인아웃 기능을 구현합니다.

이 서비스에 대한 기준 URL

http://*ap_server:port*/affwebservices/public/wsfedsignout

ap_server:port

계정 파트너에 있는 시스템의 서버 및 포트 번호를 지정합니다. 시스템은 페더레이션 네트워크에 설치된 구성 요소에 따라 웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하고 있습니다.

사인아웃 삭제 URL/사인아웃 확인 URL

계정 파트너에 있는 동일한 이름의 필드에서 지정됩니다. 이러한 필드는 리소스 파트너 속성 개체에 대한 "SAML 프로필" 설정의 "사인아웃" 섹션에 있습니다.

Web.xml 파일의 연결된 서블릿 및 서블릿 매핑

```
<servlet>
  <servlet-name>wsfedsignout</servlet-name>
  <display-name>WS-Federation Signout Service</display-name>
  <description>This servlet is the WS-Federation Signout service
      at an AP.</description>
  <servlet-class>com.netegrity.affiliateminder.webservices.wsfed.
    SignoutService</servlet-class>
</servlet>


<servlet-mapping>
<servlet-name>wsfedsignout</servlet-name>
<url-pattern>/public/wsfedsignout/*</url-pattern>
</servlet-mapping>
```

아이덴티티 공급자 검색 프로필 서비스 URL(SAML 2.0)

아이덴티티 공급자 검색 프로필 서비스는 아이덴티티 공급자 검색 기능을 구현합니다.

이 서비스에 대한 기준 URL

https://*idp_server:port*/affwebservices/public/saml2ipd/*

idp_server:port

웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하는 웹 서버와 포트를 식별합니다.

서비스 URL

"서비스 URL" 필드에서 지정됩니다. 이 필드는 아이덴티티 공급자의 SAML 서비스 공급자 개체에 대한 "SAML 프로필" 설정의 "IPD" 섹션에 있습니다.

Web.xml 파일의 연결된 서블릿 및 서블릿 매핑

```
<servlet>
  <servlet-name>saml2ipd</servlet-name>
  <display-name>SAML 2.X Identity Provider Discovery Profile
    service</display-name>
  <description>This servlet is the SAML 2.X Identity Provider Discovery Profile
service at an SP or IdP.</description>
  <servlet-class>com.netegrity.affiliateminder.webservices.
    saml2.IPDService</servlet-class>
</servlet>


<servlet-mapping>
  <servlet-name>saml2ipd</servlet-name>
  <url-pattern>/public/saml2ipd/*</url-pattern>
</servlet-mapping>
```

특성 서비스 URL(SAML 2.0)

특성 서비스를 사용하면 특성 기관이 SAML 요청자의 특성 쿼리에 응답할 수 있습니다.

이 서비스에 대한 기준 URL

http://*idp_server:port*/affwebservices/saml2attributeservice

idp_server:port

웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하는 웹 서버와 포트를 식별합니다.

특성 서비스 URL

"특성 서비스" 필드에서 지정됩니다. 이 필드는 서비스 공급자의 SAML 2.0 인증 체계에 대한 "특성" 설정에 있습니다.

Web.xml 파일의 연결된 서블릿 및 서블릿 매핑

```
<servlet>
  <servlet-name>saml2attributeservice</servlet-name>
  <display-name>SAML 2.0 Attribute service</display-name>
  <description>This servlet is the SAML 2.0 Attribute Service
        at an IdP.</description>
  <servlet-class>com.netegrity.affiliateminder.webservices.saml2.
      AttributeService</servlet-class>
</servlet>


<servlet-mapping>
 <servlet-name>saml2attributeservice</servlet-name>
 <url-pattern>/saml2attributeservice/*</url-pattern>
</servlet-mapping>

<servlet-mapping>
 <servlet-name>saml2attributeservice</servlet-name>
 <url-pattern>/saml2certattributeservice/*</url-pattern>
</servlet-mapping>
```

AP 의 WSFedDispatcher 서비스 URL

WSFedDispatcher 서비스는 모든 수신 WS-페더레이션 메시지를 받은 다음 쿼리 매개 변수 데이터를 기반으로 요청 처리를 다른 서비스에 전달합니다.

이 서비스에 대한 기준 URL

https://*ap_server:port*/affwebservices/public/wsfeddispatcher

ap_server:port

계정 파트너에 있는 시스템의 서버 및 포트 번호를 지정합니다. 시스템은 페더레이션 네트워크에 설치된 구성 요소에 따라 웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하고 있습니다.

URL

해당 없음

Web.xml 파일의 연결된 서블릿 및 서블릿 매핑

```
<servlet>
  <servlet-name>wsfeddispatcher</servlet-name>
  <display-name>WS-Federation Dispatcher service</display-name>
  <description>This servlet is the WS-Federation Dispatcher service for all
WS-Federation services.</description>
  <servlet-class>com.netegrity.affiliateminder.webservices.wsfed.
     dispatcher</servlet-class>
</servlet>


<<servlet-mapping>
<servlet-name>wsfeddispatcher</servlet-name>
<url-pattern>/public/wsfeddispatcher/*</url-pattern>
</servlet-mapping>
```

신뢰 당사자의 서비스 URL

다음 서비스는 신뢰 당사자가 제공하지만 신뢰 당사자의 서비스 URL 은 사용자가 입력합니다.

SiteMinder 신뢰 당사자가 제공하는 서비스는 다음과 같습니다.

- SAML 자격 증명 수집기(SAML 1.x) (페이지 429)
- AuthnRequest 서비스(SAML 2.0) (페이지 430)
- 어설션 소비자 서비스(SAML 2.0) (페이지 431)
- 보안 토큰 소비자 서비스(WS-페더레이션) (페이지 432)

- 싱글 로그아웃 서비스(SAML 2.0) (페이지 433)
- 사인아웃 서비스(WS-페더레이션) (페이지 434)
- WSFedDispatcher 서비스(WS-페더레이션) (페이지 435)

SAML 자격 증명 수집기 서비스 URL(SAML 1.x)

SAML 자격 증명 수집기 서비스는 SAML 1.x 어설션 소비를 돕습니다.

이 서비스에 대한 기준 URL

https://*consumer_server:port*/affwebservices/public/samlcc

consumer_server:port

웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하는 웹 서버와 포트를 식별합니다.

어설션 소비자 URL

"어설션 소비자 URL" 필드에서 지정됩니다. 이 필드는 SAML 1.x 가맹 개체에 대한 "어설션" 페이지에 있습니다. 소비자의 SAML 1.x POST 인증 체계에 대한 "체계 설정" 섹션에도 있습니다.

Web.xml 파일의 연결된 서블릿 및 서블릿 매핑

```
<servlet>
  <servlet-name>samlcredentialcollector</servlet-name>
  <display-name>SAML Credential Collector</display-name>
  <description>This servlet acts as the SAML Credential Collector.</description>
  <servlet-class>com.netegrity.affiliateminder.webservices.
     SAMLCredentialCollector</servlet-class>
</servlet>

<servlet-mapping>
  <servlet-name>samlcredentialcollector</servlet-name>
  <url-pattern>/public/samlcc/*</url-pattern>
</servlet-mapping>
```

AuthnRequest 서비스(SAML 2.0)

이 AuthnRequest 서비스를 사용하면 아티팩트 또는 POST 프로필에 대한 싱글 사인온을 구현할 수 있습니다.

이 서비스에 대한 기준 URL

https://*sp_server:por*t/affwebservices/public/saml2authnrequest

sp_server:port

웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하는 서비스 공급자의 서버 및 포트 번호를 지정합니다.

서비스에 대한 URL

해당 없음

AuthnRequest 는 서비스 공급자의 응용 프로그램에 있는 링크입니다. 이 링크는 싱글 사인온을 시작하며 응용 프로그램에 있어야 합니다.

Web.xml 파일의 연결된 서블릿 및 서블릿 매핑

```
<servlet>
  <servlet-name>saml2authnrequest</servlet-name>
  <display-name>SAML 2.0 AuthnRequest service</display-name>
  <description>This servlet is the SAML 2.0 AuthnRequest service at an
SP.</description>
  <servlet-class>com.netegrity.affiliateminder.webservices.
   saml2.AuthnRequest</servlet-class>
</servlet>

<servlet-mapping>
  <servlet-name>saml2authnrequest</servlet-name>
  <url-pattern>/public/saml2authnrequest/*</url-pattern>
</servlet-mapping>
```

어설션 소비자 서비스 URL(SAML 2.0)

어설션 소비자 서비스를 사용하면 어설션을 소비할 수 있습니다.

이 서비스에 대한 기준 URL

https://*sp_server:port*/affwebservices/public/saml2assertionconsumer

sp_server:port

웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하는 서비스 공급자의 서버 및 포트 번호를 지정합니다.

어설션 소비자 URL

"어설션 소비자 URL" 필드에서 지정됩니다. 이 필드는 아이덴티티 공급자의 SAML 서비스 공급자 개체에 대한 "SSO" 설정의 일부입니다.

Web.xml 파일의 연결된 서블릿 및 서블릿 매핑

```
<servlet>
  <servlet-name>saml2assertionconsumer</servlet-name>
  <display-name>SAML 2.0 Assertion Consumer service</display-name>
  <description>This servlet is the SAML 2.0 Assertion Consumer service at an
SP.</description>
  <servlet-class>com.netegrity.affiliateminder.webservices.
    saml2.AssertionConsumer</servlet-class>
</servlet>


<servlet-mapping>
  <servlet-name>saml2assertionconsumer</servlet-name>
  <url-pattern>/public/saml2assertionconsumer/*</url-pattern>
</servlet-mapping>
```

보안 토큰 소비자 서비스 URL(WS-페더레이션)

보안 토큰 소비자 서비스를 사용하면 리소스 파트너의 어설션을 소비할 수 있습니다.

이 서비스에 대한 기준 URL

https://*rp_server:port*/affwebservices/public/wsfedsecuritytokenconsumer

rp_server:port

웹 에이전트 옵션 팩 또는 SPS 페더레이션 게이트웨이를 호스트하는 리소스 파트너의 웹 서버와 포트를 식별합니다.

보안 토큰 소비자 서비스 URL

"보안 토큰 소비자 서비스" 필드에서 지정됩니다. 이 필드는 계정 파트너의 리소스 파트너 개체에 대한 "SAML 프로필" 설정의 일부입니다.

Web.xml 파일의 연결된 서블릿 및 서블릿 매핑

```
<servlet>
  <servlet-name>wsfedsecuritytokenconsumer</servlet-name>
  <display-name>Security Token Consumer service</display-name>
  <description>This servlet is the WS-Federation Security Token
     Consumer service at an RP.</description>
  <servlet-class>com.netegrity.affiliateminder.webservices.wsfed.
     SecurityTokenConsumer</servlet-class>
</servlet>


<<servlet-mapping>
<servlet-name>wsfedsecuritytokenconsumer</servlet-name>
<url-pattern>/public/wsfedsecuritytokenconsumer/*</url-pattern>
</servlet-mapping>
```

SP 의 싱글 로그아웃 서비스 URL(SAML 2.0)

싱글 로그아웃 서비스는 SAML 2.0 에 대한 싱글 로그아웃을 구현합니다.

이 서비스에 대한 기준 URL

http://*sp_server:port*/affwebservices/public/saml2slo

sp_server:port

웹 에이전트 옵션 팩이나 SPS 페더레이션 게이트웨이를 호스트하는 서비스 공급자의 서버 및 포트 번호를 지정합니다.

SLO 위치 URL/SLO 응답 위치 URL

동일한 이름의 필드에서 지정됩니다. 이러한 필드는 서비스 공급자에서 구성하는 SAML 2.0 인증 체계에 대한 "SLO" 설정의 일부입니다.

Web.xml 파일의 연결된 서블릿 및 서블릿 매핑

```
<servlet>
  <servlet-name>saml2slo</servlet-name>
  <display-name>SAML 2.0 Single Logout service</display-name>
  <description>This servlet is the SAML 2.0 Single Logout service at an
SP.</description>
  <servlet-class>com.netegrity.affiliateminder.webservices.
     saml2.SLOService</servlet-class>
</servlet>

<servlet-mapping>
  <servlet-name>saml2slo</servlet-name>
  <url-pattern>/public/saml2slo/*</url-pattern>
</servlet-mapping>
```

RP 의 사인아웃 서비스 URL(WS-페더레이션)

사인아웃 서비스는 WS-페더레이션에 대한 사인아웃 기능을 구현합니다.

이 서비스에 대한 기준 URL:

http://*rp_server:port*/affwebservices/public/wsfedsignout

rp_server:port

웹 에이전트 옵션 팩 또는 SPS 페더레이션 게이트웨이를 호스트하는 리소스 파트너의 웹 서버와 포트를 식별합니다.

사인아웃 삭제 URL/사인아웃 URL

동일한 이름의 필드에서 지정됩니다. 이러한 필드는 리소스 파트너의 WS-페더레이션 인증 체계에 대한 "사인아웃" 섹션에 있습니다.

Web.xml 파일의 연결된 서블릿 및 서블릿 매핑

```
<servlet>
  <servlet-name>wsfedsignout</servlet-name>
  <display-name>WS-Federation Signout Service</display-name>
  <description>This servlet is the WS-Federation Signout service
      at an RP.</description>
  <servlet-class>com.netegrity.affiliateminder.webservices.wsfed.
    SignoutService</servlet-class>
</servlet>


<servlet-mapping>
<servlet-name>wsfedsignout</servlet-name>
<url-pattern>/public/wsfedsignout/*</url-pattern>
</servlet-mapping>
```

RP 의 WSFedDispatcher 서비스 URL

WSFedDispatcher 서비스는 모든 수신 WS-페더레이션 메시지를 받습니다. 그런 다음 쿼리 매개 변수 데이터를 기반으로 요청 처리를 다른 서비스에 전달합니다.

이 서비스에 대한 기준 URL

https://*rp_server:port*/affwebservices/public/wsfeddispatcher

rp_server:port

웹 에이전트 옵션 팩 또는 SPS 페더레이션 게이트웨이를 호스트하는 리소스 파트너의 웹 서버와 포트를 식별합니다.

서비스에 대한 URL

해당 없음

Web.xml 파일의 연결된 서블릿 및 서블릿 매핑

```
<servlet>
  <servlet-name>wsfeddispatcher</servlet-name>
  <display-name>WS-Federation Dispatcher service</display-name>
  <description>This servlet is the WS-Federation Dispatcher service for all
WS-Federation services.</description>
  <servlet-class>com.netegrity.affiliateminder.webservices.wsfed.
     dispatcher</servlet-class>
</servlet>


<<servlet-mapping>
<servlet-name>wsfeddispatcher</servlet-name>
<url-pattern>/public/wsfeddispatcher/*</url-pattern>
</servlet-mapping>
```

Web.xml 파일

Web.xml 파일에는 페더레이션 웹 서비스 응용 프로그램에 대한 서블릿 및 URL 매핑이 나열되어 있습니다.

이 파일의 내용 대부분은 변경할 수 없지만 URL 매핑은 수정할 수 있습니다.

Web.xml 파일을 보려면 해당 파일 위치로 이동하십시오.

- *web_agent_home*/affwebservices/WEB-INF
- *sps_home*/secure-proxy/Tomcat/webapps/affwebservices/WEB-INF

제 24 장: 레거시 페더레이션 문제 해결

이 섹션은 다음 항목을 포함하고 있습니다.

페더레이션 문제 해결에 도움이 되는 트랜잭션 ID

한 파일 내에 수많은 트랜잭션이 기록되어 있는 경우 페더레이션 트랜잭션의 문제를 해결하는 것이 쉽지 않습니다. 트랜잭션 로그에서 단일 트랜잭션을 추적하려면 SAML 트랜잭션 ID 를 사용하십시오. 페더레이션 호출이 발생하면 FWS 응용 프로그램이 먼저 SAML 트랜잭션 ID 를 생성합니다. SAML 트랜잭션 ID 는 한 번만 생성됩니다. 이 고유 SAML 트랜잭션 ID 는 여러 트랜잭션 ID 로 매핑될 수 있습니다.

예를 들어 SAML 2.0 POST 트랜잭션용 fwstrace.log 에서 다음 메시지가 나타날 수 있습니다. 두 트랜잭션 ID 의 매핑을 보여 주는 굵게 표시된 행을 참고하십시오.

```
[08/01/2013][17:33:54][2292][1884][1c2d7650-b006e46a-ed071f41-bbbede33-fe78e2dd-38d][SSO.java][processAuthentication][SAMLTransactionID 2aaf90ec-fdef4897-0ef49d91-63d4031d-f508a3e9-12 maps to TransactionID: 1c2d7650-b006e46a-ed071f41-bbbede33-fe78e2dd-38d.]
```

CA SiteMinder?Federation 시스템은 어설션 당사자로 기능하는 경우에만 새 SAMLTransactionID 를 생성합니다. 이러한 특정 활동은 다음의 경우 발생합니다.

- 페더레이션 웹 서비스가 세션을 구성하기 위해 브라우저를 인증 URL 로 리디렉션하는 경우
- 다음 HTTP-아티팩트 싱글 사인온 트랜잭션의 경우:
  - 어설션 당사자가 신뢰 당사자에 아티팩트를 반환하는 경우
  - 어설션 당사자가 아티팩트를 확인하는 경우
- 사용자가 아이덴티티 검색 프로필 URL 로 리디렉션되는 경우
- 어설션 당사자에서 싱글 로그아웃 중

신뢰 당사자에는 요청 ID 가 있으며, 이 ID 는 로그 파일을 통해 쉽게 추적될 수 있습니다. 요청 ID 는 신뢰 당사자에서 SAMLTransactionID 를 생성하기 위해 CA SiteMinder?Federation 시스템에서 필요하지 않습니다.

각 고유 SAML 트랜잭션 ID 에는 여러 트랜잭션 ID 가 있을 수 있습니다. 새 HTTP 트랜잭션이 발생하면 새 트랜잭션 ID 가 생성됩니다. 이 트랜잭션 ID 는 단일 SAML 트랜잭션 ID 로 매핑됩니다. 예를 들어, 추적 로그에서 다음과 같은 항목을 볼 수 있습니다.

```
SamlTransactionID ["xyz"] maps to TransationID["123"]
["123"] HTTP operation
["123"] HTTP operation
```

A new transaction ID "456" is generated:

```
SamlTransactionID["xyz"] Maps to Transactionid["456"]
["456"] <some operation>
["456"] <some operation>
```

트랜잭션 ID 는 fwstrace.log 및 smtracedefault.log 에 배치됩니다. 즉, 단일 트랜잭션에 대해 동일한 트랜잭션 ID 집합이 이들 로그에 각각 기록됩니다. 이들 로그에서 ID 를 추적하면 트랜잭션을 추적할 수 있습니다. 오류가 발생한 경우 ID 를 사용하여 오류가 발생한 해당 트랜잭션에서 어느 이벤트가 실패했는지 확인할 수 있습니다.

일반 문제

다음 문제 해결 항목은 SAML 1.x 및 SAML 2.0 에 적용됩니다.

잘못된 smjavaagent.dll 로 인해 웹 에이전트 옵션 팩을 초기화하지 못함

증상

다른 CA 제품이 있는 시스템에서 웹 에이전트 옵션 팩을 초기화하지 못합니다. "Java Agent API initialization FAILED"(Java Agent API 초기화 실패) 또는 "unsatisfied link error"(충족되지 않은 링크 오류) 등의 오류 메시지가 표시됩니다.

다음과 유사한 오류 메시지가 페더레이션 웹 서비스 로그 파일에 나타납니다.

```
11:04:46 AM[29959477:E] Exception while reading the WebAgent configuration
information: javaagent_api_getConfig
11:04:46 AM[29959477:E] Java Agent API initialization FAILED.
```

해결 방법

smjavaagentapi.dll 의 잘못된 버전이 시스템 경로에 있을 수 있습니다. 설치된 제품이 모두 서로 호환되고 해당 버전이 호환되는지 확인하십시오.

버전을 확인하려면

1. 기술 지원 사이트에 로그인합니다.
2. "Platform Support Matrix for 12.52 SP1"(12.52 SP1 에 대한 플랫폼 지원표)를 검색합니다.

쿠키 도메인 불일치 오류

증상

소비자/SP 사이트에서 SAML 인증이 성공한 후에도 쿠키 도메인 불일치 때문에 소비자/SP 웹 에이전트가 여전히 사용자에게 챌린지를 표시합니다.

해결 방법

생산자/IdP 및 소비자/SP 가 동일한 쿠키 도메인에 없는지 확인하십시오. 레거시 페더레이션은 동일한 쿠키 도메인 내의 페더레이션을 지원하지 않습니다. 생산자/IdP 사이트와 소비자/SP 사이트에 별도의 쿠키 도메인이 필요합니다. 또한 CookieDomainScope 매개 변수가 사용 중인 환경에 적절한 값으로 설정되어 있는지 확인하십시오. 이 매개 변수는 웹 에이전트 매개 변수입니다(*SiteMinder 웹 에이전트 구성 안내서*의 싱글 사인온 정보 참조).

별도의 쿠키 도메인이 사용되고 있는 경우 에이전트 구성의 쿠키 도메인이 요청된 대상 URL 의 도메인 이름과 일치하는지 확인하십시오.

소비자/SP 에서 성공적으로 인증한 후 오류 발생

증상

소비자 사이트에서 성공적으로 인증한 후 HTTP 404 "Page Not Found"(페이지를 찾을 수 없음) 오류 코드가 브라우저에 반환됩니다.

해결 방법

대상 페이지가 웹 서버 문서 루트에 있는지 확인하십시오. FWS 추적 로그를 검사하여 사용자가 올바른 URL 로 리디렉션되고 있는지 확인하십시오.

소비자에서 어설션을 검색하려고 하면 HTTP 404 오류가 발생함

증상

신뢰 당사자가 어설션을 검색하려고 하면 HTTP 404 "Page Not Found"(페이지를 찾을 수 없음) 오류 코드가 브라우저에 반환됩니다.

해결 방법

페더레이션 웹 서비스 응용 프로그램이 웹 응용 프로그램으로 배포되어 있는지 확인하십시오. 지원되는 응용 프로그램 서버 중 하나를 실행 중인 웹 서버에 응용 프로그램을 배포하십시오. "SiteMinder Platform Support Matrix"(SiteMinder 플랫폼 지원표)에는 웹 에이전트 옵션 팩에 대해 지원되는 플랫폼이 나열되어 있습니다.

페더레이션 웹 서비스에서 생산자/IdP 로 SAML 요청을 보내지 못함

증상

소비자/SP 의 페더레이션 웹 서비스 응용 프로그램에서 생산자/IdP 로 SAML 요청 메시지를 보내지 못했습니다. 소비하는 측에서 웹 서버의 인증서를 트러스트하지 못했습니다.

해결 방법

클라이언트 인증서를 발급한 인증 기관의 인증서를 생산자/IdP 에 있는 웹 서버의 키 데이터베이스에 추가하십시오.

일치하는 매개 변수의 대/소문자 구분 구성 문제

증상

매개 변수가 일치하는 것처럼 보여도 생산자/아이덴티티 공급자와 소비자/서비스 공급자에서 일치해야 하는 구성 매개 변수 간의 충돌로 인해 문제가 발생합니다.

해결 방법

콜론 뒤에 오는 URL 문자열은 대/소문자를 구분합니다. 예를 들어 **http:** 뒤에 오는 텍스트는 대/소문자를 구분합니다. 따라서 모든 해당 설정에 있는 URL 의 대/소문자가 일치해야 합니다.

어설션 당사자와 신뢰 당사자 간에 일치해야 하는 매개 변수 값은 동일한 값을 사용해야 하는 구성 설정 (페이지 411) 항목에 설명되어 있습니다.

로그오프 후 정책 서버 시스템이 실패함

증상

일부 환경에서 정책 서버가 실행되는 동안 로그오프하면 정책 서버가 실패합니다. 이 오류는 JVM 문제로 인해 발생합니다.

해결 방법

JVMOptions.txt 파일에서 -Xrs 명령을 자체 명령줄에 추가하십시오. 이 명령은 대/소문자를 구분하므로 표시된 대로 추가해야 합니다. 이 명령을 사용하면 JVM 의 운영 체제 신호 사용량이 줄어듭니다.

JVMOptions.txt 파일은 *policy_server_home*/config/에 있습니다.

어설션의 멀티바이트 문자가 제대로 처리되지 않음

증상

어설션에 멀티바이트 문자가 있을 경우 문제가 발생할 수 있습니다.

해결 방법

다음과 같이 운영 체제의 LANG 설정을 UTF-8 로 설정하십시오.

LANG=xx_xx.UTF-8

예를 들어 일본어에 대한 항목은 다음과 같습니다.

LANG=ja_JP.UTF-8

ServletExec 를 사용하는 IIS 웹 서버에 대한 추적 로그가 나타나지 않음

증상

LoggerConfig.properties 파일에서 추적 로깅이 사용되도록 설정했지만 affwebservices.log 및 FWStrace.log 파일이 WEB-INF/classes 디렉터리에 기록되고 있지 않습니다.

해결 방법

ServletExec 와 연결된 익명 사용자 계정이 Windows 파일 시스템에 쓸 수 있는 권한을 가지고 있는지 확인합니다. 사용자 계정이 운영 체제의 일부로 작동할 수 있는 권한을 가지고 있지 않으면 ServletExec 에서 로그 파일을 쓸 수 없습니다.

JVM 초기화 중 오류가 발생함

증상

정책 서버 로그(어떤 로그인지 확인해야 함)에 다음 오류 메시지가 표시되는 경우가 있습니다.

```
Error occurred during initialization of JVM
Could not reserve enough space for object heap.
```

그러면 JVM 초기화 오류로 인해 웹 에이전트 옵션 팩 기능이 올바로 작동하고 있지 않은 것입니다.

해결 방법

개체 힙 메모리 크기를 제한하십시오.

메모리 크기를 제한하려면

1. *web_agent_home*/WEB-INF/properties 디렉터리에서 JVMOptions.txt 파일을 엽니다.
2. 파일에 다음 항목을 아래에 기록된 대로 추가합니다.

   ```
   -Xms128M
   ```
3. 파일을 저장합니다.
4. 정책 서버를 다시 시작합니다.

SAML 1.x 만 관련된 문제

다음 문제는 SAML 1.x 기능에만 적용됩니다.

SAML 1.x 아티팩트 프로필 싱글 사인온 실패

증상

SAML 1.x 아티팩트 프로필 싱글 사인온이 구성된 경우 소비자 사이트에서 생산자로 SAML 요청 메시지를 보내지 못합니다. 다음과 유사한 오류 메시지가 페더레이션 웹 서비스 로그 파일에 나타납니다.

```
May 23, 2012 4:20:44.234 PM[28349544:E] Dispatcher object thrown unknown exception while processing the request message. Message: java.net.ConnectException: Connection refused: connect.
May 23, 2012 4:20:44.234 PM[28349544:E] Exception caught. Message: com.netegrity.affiliateminder.webservices.m: Exception occurred while message dispatcher(srca) object trying to send SOAP request message to the SAML producer.
```

해결 방법

어설션 검색 서비스를 호스트하는 웹 서버가 구성된 SSL 포트를 사용하여 실행되고 있는지 확인하십시오.

어설션 검색 서비스에 액세스하기 위한 인증이 실패함

증상

SAML 1.x 아티팩트 싱글 사인온을 사용하는 환경에서 소비자가 생산자의 어설션 검색 서비스에 액세스하려고 하면 인증이 실패합니다.

해결 방법

기본 인증으로 어설션 검색 서비스를 보호하는 경우 가맹 구성에 대한 이름 및 암호가 SAML 아티팩트 인증 체계에 대한 가맹 이름 및 암호와 일치하는지 확인하십시오.

인증 방법 수정 후 인증이 실패함

증상

SAML 1.x 어설션 검색 서비스를 보호하는 인증 방법을 "기본"에서 "클라이언트 인증서"로 변경하는 경우 후속 인증 요청이 실패할 수 있습니다.

SAML 1.x 어설션 검색 서비스를 보호하는 인증 방법을 "클라이언트 인증서"에서 "기본"으로 변경하는 경우 후속 인증 요청이 실패할 수 있습니다.

해결 방법

인증 방법이 변경된 후 웹 서버를 다시 시작하십시오.

SAML 아티팩트 싱글 사인온에 대한 클라이언트 인증이 실패함

증상

생산자에서 SAML 1.x 아티팩트 싱글 사인온에 대한 클라이언트 인증서 인증이 실패했습니다. 다음 오류가 웹 에이전트 추적 로그에 로깅됩니다.

```
Setting HTTP response variable HTTP_consumer_name=from SiteMinder
```

예를 들어 응답의 특성 이름이 LDAP 사용자 디렉터리에 대해 "name"으로 구성된 경우 응답이 실패합니다.

해결 방법

FederationWebServicesDomain 도메인 아래에 웹 에이전트 응답을 생성하는지 확인하십시오. 응답은 다음과 같아야 합니다.

특성 유형

WebAgent HTTP 헤더 변수

특성 종류

사용자 특성

변수 이름

consumer_name

특성 이름

UID(LDAP 의 경우) 또는 이름(ODBC 의 경우)

SAML 2.0x 만 관련된 문제

다음 문제는 SAML 2.0x 기능에만 적용됩니다.

어설션 검색 서비스에 액세스하기 위한 인증이 실패함

증상

SAML 2.0 아티팩트 싱글 사인온을 구성하는 경우 서비스 공급자가 아이덴티티 공급자의 아티팩트 레졸루션 서비스에 액세스할 때 인증하지 못했습니다.

다음과 유사한 오류 메시지가 페더레이션 웹 서비스 로그 파일에 나타납니다.

```
May 23, 2005 4:43:51.479 PM[31538514:E] SAML producer returned error http status code.
HTTP return status: 401. Message: <HTML><HEAD><TITLE>401: Access
Denied</TITLE></HEAD><BODY><H1>401: Access Denied</H1>
Proper authorization is required for this area. Either your browser does not perform
authorization, or your authorization has failed.</BODY></HTML>
```

해결 방법

구성된 인증에 따라 다릅니다.

- 기본 인증의 경우 SAML 서비스 공급자에 대한 이름 및 암호가 SAML 2.0 인증 체계에 대한 가맹 이름 및 암호와 일치하는지 확인하십시오.
- 아티팩트 레졸루션 서비스를 보호하기 위한 클라이언트 인증서 인증의 경우 서비스 공급자에 대한 클라이언트 인증서가 유효한지 확인하십시오. 인증서가 인증서 데이터 저장소에 있는지도 확인하십시오. 또한 클라이언트 인증서를 발급한 인증 기관이 아이덴티티 공급자의 인증서 데이터 저장소에 있는지 확인하십시오.
- 구성된 인증이 없는 경우 아티팩트 레졸루션 서비스 URL 이 보호되지 않는지 확인하십시오.

세션 저장소에서 만료 데이터를 삭제하는 동안 ODBC 오류 발생

증상

이전 버전에서 정책 서버를 업그레이드하는 경우 세션 저장소에서 만료 데이터를 삭제할 때 ODBC 오류가 발생할 수 있습니다.

해결 방법

*SiteMinder 업그레이드 안내서*에 설명된 대로 세션 저장소 스키마를 업그레이드하십시오.

부록 A: 파트너 관계 모델에서 레거시 구성 다시 만들기

레거시 페더레이션에서 [set the pfr variable for your book]으로 직접 마이그레이션하는 경로는 존재하지 않습니다. [set the pfr variable for your book] 모델에서 레거시 페더레이션 구성을 복제하려면 레거시 엔터티를 다시 생성하고 파트너 관계를 구성해야 합니다.

레거시 및 파트너 관계 개체는 일대일 대응 관계를 공유하지 않습니다. 레거시 페더레이션 모델의 페더레이션 구성에는 각 파트너에서 수행되는 다음 태스크가 포함됩니다.

어설션 당사자

- 가맹 도메인을 구성합니다.
- 가맹 도메인에서 신뢰 당사자를 식별하고 이러한 신뢰 당사자와의 통신을 구성합니다. 신뢰 당사자는 SAML 1.x 가맹, SAML 2.0 서비스 공급자, WSFED 리소스 파트너를 포함합니다.

신뢰 당사자

- 신뢰 당사자를 정의하는 인증 체계 구성
- 인증 체계 내에서 신뢰 당사자가 어설션을 소비하는 방법과 신뢰 당사자가 사용자를 대상 응용 프로그램으로 리디렉션하는 방법 지정

파트너 관계 모델의 레거시 구성 다시 생성에는 다음 태스크가 포함됩니다.

- 비즈니스 파트너를 나타내는 어설션 및 신뢰 당사자 엔터티 구성
- 엔터티 간의 파트너 관계 정의

다음 표에서는 레거시 페더레이션 구성 요소와 [set the pfr variable for your book] 구성 요소 간의 관계를 보여 줍니다.

레거시 구성 요소 (어설션 당사자)	파트너 관계 구성 요소 (어설션 당사자)
SAML 1.1 가맹	SAML 1.1 생산자-소비자 파트너 관계 *[set the pfr variable for your book]은 SAML 1.0 을 지원하지 않습니다.*

레거시 구성 요소 (어설션 당사자)	파트너 관계 구성 요소 (어설션 당사자)
SAML 2.0 서비스 공급자	SAML2 IdP-SP 파트너 관계
WSFED 리소스 파트너	WSFED IP-RP 파트너 관계

레거시 구성 요소 (신뢰 당사자)	파트너 관계 구성 요소 (신뢰 당사자)
인증 체계: SAML 아티팩트 또는 POST 템플릿	SAML 1.1 소비자-생산자 파트너 관계
인증 체계: SAML 2.0 템플릿	SAML2 SP-IdP 파트너 관계
인증 체계: WS-Federation 템플릿	WSFED RP-IP 파트너 관계

파트너 관계 모델에서 레거시 페더레이션 개체를 다시 생성하려면 다음 설정에 주의하십시오.

활성

(레거시 페더레이션에 대한 가맹/서비스 공급자 속성 및 "SAML 인증 체계" 대화 상자). 레거시 페더레이션 구성을 사용하고 있는 경우 이 확인란이 선택되어 있는지 확인하십시오. 파트너 관계 페더레이션 모델에서 원본 ID 등의 아이덴티티 설정에 대한 값이 유사한 레거시 구성을 다시 생성하는 경우 파트너 관계 페더레이션 개체를 활성화하기 전에 이 확인란의 선택을 취소하십시오.

SiteMinder 에서는 동일한 아이덴티티 값을 사용하는 레거시 및 파트너 관계 구성을 사용할 수 없습니다. 이 경우 이름 충돌이 발생합니다.

아티팩트 보호 유형

([set the pfr variable for your book]에 대한 "SSO" 설정). HTTP-아티팩트 싱글 사인온에 대한 백 채널이 보호되는 방법을 정의합니다.

[set the pfr variable for your book] 모델에서 레거시 페더레이션 구성을 다시 생성하는 경우 레거시 백 채널 보호 방법을 사용하십시오. 레거시 옵션을 사용하면 구성에서 어설션 검색 서비스(SAML 1.x) 또는 아티팩트 레졸루션 서비스(SAML 2.0)의 기존 URL 을 사용할 수 있습니다.

레거시를 옵션으로 선택하면 SiteMinder 는 요청을 수락합니다. URL 은 수정할 필요가 없습니다. 아티팩트 서비스 URL 을 레거시 구성에서 가져오지만 이 설정에서 파트너 관계 옵션만 선택하는 경우 SiteMinder 는 요청을 거부합니다.

중요! 레거시 페더레이션 옵션의 경우 아티팩트 서비스를 보호하는 정책을 적용하십시오. 아티팩트 서비스는 페더레이션 웹 서비스의 구성 요소입니다. 소프트웨어는 자동으로 페더레이션 웹 서비스에 대한 정책을 생성합니다. 하지만 아티팩트를 검색하는 서비스에 대한 액세스가 허용되는 파트너 관계를 지정해야 합니다. 자세한 내용은 *파트너 관계 페더레이션 안내서*를 참조하십시오.

옵션: 레거시, 파트너 관계

참고: SiteMinder 12.52 SP1 는 FSS UI(Federation Security Services 사용자 인터페이스) 및 관리 UI 와 함께 제공됩니다. 구성을 위해 FSS UI 에서 관리 UI 로 전환하는 경우 구성 개체 수정을 위해 FSS UI 로 돌아가지 마십시오. 관리 UI 로 시작한 후에는 계속해서 관리 UI 만 사용하십시오. 관리 UI 를 사용한 후 FSS UI 로 돌아가면 정책 저장소에 있는 개체로 인해 정책 서버의 기능이 손상될 수 있습니다.