SiteMinder

엔터프라이즈의 페더레이션

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.

- 더 이상 지원되지 않는 SAML 가맹 에이전트에 대한 모든 참조가 제거되었습니다.
- 페더레이션 사용 사례 및 솔루션 (페이지 13) - 페더레이션된 파트너 관계의 개념을 더 명확하게 보여 주도록 사용 사례가 업데이트되었습니다.
- 페더레이션 트랜잭션 프로세스 흐름 (페이지 79) - 트랜잭션 다이어그램 및 흐름이 새로운 검사점 로그 메시지를 포함하여 수정 및 업데이트되었습니다.

목차

제 1 장: SiteMinder Federation 배포

페더레이션 배포 모델

CA SiteMinder Federation 에는 다음 두 가지 배포 모델이 있습니다.

- 파트너 관계 페더레이션

  파트너 관계 페더레이션은 페더레이션 표준에 기초한 엔터프라이즈 간 파트너 관계 구성에 기초합니다. 파트너 관계 모델에는 도메인, 영역, 정책 등의 SiteMinder 관련 개체 구성이 필요하지 않습니다. 이 모델은 SiteMinder Federation 을 사용하는 새 구성에 권장됩니다.

- 레거시 페더레이션

  레거시 페더레이션(이전의 Federation Security Services)

  레거시 페더레이션은 가맹 도메인, 인증 체계 및 페더레이션된 리소스 보호 정책 등의 SiteMinder 개체 구성을 기반으로 합니다. 이 모델은 이전 배포와의 호환성을 위해 주로 사용됩니다.

두 배포 모두 SAML 어설션의 형태로 사용자 인증 데이터를 제공합니다. 어설션을 소비하는 엔터티는 어설션을 사용하여 사용자를 식별합니다. 인증 작업이 성공하면 소비하는 엔터티가 요청된 리소스를 제공합니다. 결과적으로 사용자 환경이 원활해집니다.

어느 모델을 사용하든 SiteMinder 정책 서버, 관리 UI 및 웹 에이전트 옵션 팩을 설치하십시오.

참고: 페더레이션은 SiteMinder 와는 별개로 라이선스가 부여됩니다.

페더레이션 사양

SiteMinder 는 다음과 같은 페더레이션 사양을 지원합니다.

SAML(Security Assertion Markup Language)

SAML(Security Assertion Markup Language)은 OASIS(Organization for the Advancement of Structured Information Standards)의 표준입니다. 이 산업 표준은 인증 및 권한 부여 정보를 교환하기 위한 XML 프레임워크를 정의합니다.

SAML 은 엔터티 간에 사용자 관련 보안 정보를 전달하는 수단으로 어설션을 정의합니다. SAML 어설션은 사용자와 같은 특정 주체에 대한 정보를 포함하는 XML 문서입니다. 어설션에는 인증, 권한 부여 및 특성과 관련된 몇 가지 서로 다른 내부 설명이 포함될 수 있습니다.

SAML 은 SSO(싱글 사인온)를 원활하게 하기 위해 SAML 어설션이 파트너 간에 전달되는 방식을 지정하는 브라우저 기반의 두 가지 프로토콜을 정의합니다.

이 두 프로토콜은 다음과 같습니다.

- 브라우저/아티팩트 프로필 - SAML 어설션에 대한 참조로 SAML 아티팩트를 정의합니다.
- 브라우저/POST 프로필 - 어설션이 포함된 응답을 반환합니다.

참고: SAML 2.0 에서는 아티팩트 프로필과 POST 프로필을 HTTP 바인딩이라고 합니다.

SAML 사양과 SAML 프로필 관련 정보는 OASIS(Organization for the Advancement of Structured Information Standards) 를 참조하십시오.

SiteMinder 는 다음과 같은 SAML 표준 및 프로필을 지원합니다.

- SAML 1.0 아티팩트 프로필만(레거시 페더레이션만 해당)
- SAML 1.1 아티팩트 및 POST 프로필
- SAML 2.0 아티팩트 및 POST 프로필

WS-페더레이션

ADFS(Active Directory Federation Services)는 페더레이션된 SSO(싱글 사인온)를 지원하기 위한 Microsoft 의 웹 서비스 기반 솔루션입니다. ADFS 는 Windows 서버에서 실행되며 파트너들이 보안 네트워크를 통해 사용자 아이덴티티 정보와 액세스 권한을 안전하게 공유하게 하여 SSO 를 가능하게 합니다. ADFS 는 SSO 기능을 인터넷 응용 프로그램으로 확장하여 사용자가 조직의 웹 기반 응용 프로그램에 액세스할 때 웹 SSO 상호 작용을 원활하게 수행할 수 있도록 합니다.

ADFS 는 통신에 WS-페더레이션 사양을 사용합니다. WS 사양과 배경 설명서 및 ADFS 프로필에 대한 정보는 Microsoft 웹 사이트를 참조하십시오.

페더레이션된 네트워크의 엔터티

페더레이션된 네트워크에서 한 엔터티가 SAML 어설션 또는 어설션이 들어 있는 WS-페더레이션 토큰을 생성합니다. 어설션에는 해당 어설션을 생성하는 사이트에서 로컬로 유지 관리되는 아이덴티티를 가진 사용자에 대한 정보가 포함됩니다. 다른 엔터티는 어설션을 사용하여 사용자를 인증하고 해당 사용자에 대한 세션을 설정합니다.

프로토콜에 따라 이러한 엔터티 두 개가 다르게 명명되지만 수행하는 기능은 동일합니다.

프로토콜	어설션을 생성하는 엔터티	어설션을 소비하는 엔터티
SAML 1.0 및 1.1	생산자	소비자
SAML 2.0	IdP(아이덴티티 공급자)	SP(서비스 공급자)
WS-페더레이션(파트너 관계)	IP(아이덴티티 공급자)	RP(리소스 파트너)
WS-페더레이션(레거시)	AP(계정 파트너)	RP(리소스 파트너)

단일 사이트는 어설션 당사자이자 신뢰 당사자일 수 있습니다.

제 2 장: 페더레이션 사용 사례 및 솔루션

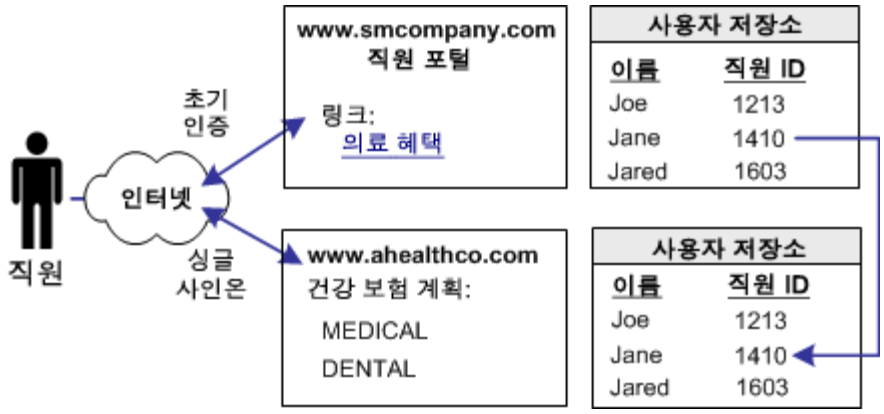
이 섹션은 다음 항목을 포함하고 있습니다.

사용 사례: 계정 연결에 기반한 싱글 사인온

이 사용 사례에서 smcompany.com 은 파트너인 ahealthco.com 과 직원 의료 혜택 관리 계약을 맺었습니다.

smcompany.com 의 직원은 이 회사 웹 사이트의 직원 포털(smcompany.com)에서 인증을 받은 다음 ahealthco.com 의 의료 혜택 정보를 보기 위해 링크를 클릭합니다. 이 직원은 ahealthco.com 웹 사이트에 연결되며 웹 사이트에 사인온할 필요 없이 해당 직원의 올바른 의료 혜택 정보가 제공됩니다.

다음 그림에서는 이 사용 사례를 보여 줍니다.

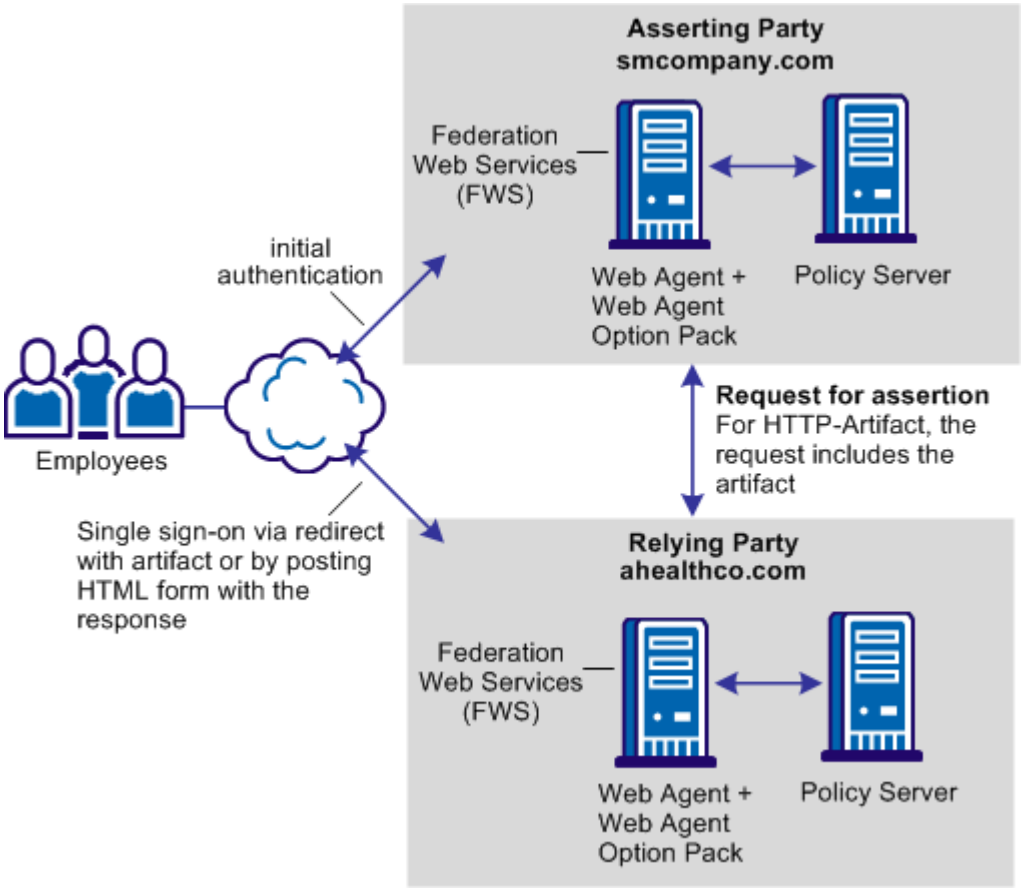


회계 연결은 브라우저 기반 싱글 사인온에 사용될 수 있으며, 이 경우 각 파트너가 동일한 사용자에 대해 별도 사용자 계정을 유지 관리합니다. 회계 연결은 페더레이션된 식별자를 파트너의 로컬 아이덴티티와 연결하기 위해 SAML 어설션을 사용합니다.

이 경우, ahealthco.com 은 smcompany.com 의 모든 직원에 대한 모든 보건 관련 정보 및 사용자 아이덴티티를 유지 관리합니다. smcompany.com 의 직원이 ahealthco.com 에 액세스하면 해당 직원에 대한 식별자가 안전한 방식으로 smcompany.com 에서 ahealthco.com 으로 전달됩니다. 이 식별자를 통해 ahealthco.com 은 사용자를 확인하고 해당 사용자에 대해 허용할 액세스 수준을 결정할 수 있습니다.

솔루션: 계정 연결에 기반한 싱글 사인온

페더레이션을 smcompany.com 및 ahealthco.com 에 배포하여 사용 사례: 계정 연결에 기반한 싱글 사인온 (페이지 13)을 해결할 수 있습니다.



SiteMinder 는 두 사이트 모두에 배포됩니다. 웹 서버 시스템에는 웹 에이전트 옵션 팩이 있는 웹 에이전트가 설치되고 다른 시스템에는 정책 서버가 설치됩니다. 설치는 smcompany.com 과 ahealthco.com 의 경우 모두 동일합니다.

FWS 응용 프로그램은 HTTP-아티팩트 프로필에 대한 어설션을 검색하고 어설션을 소비하는 서블릿을 제공합니다.

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.

계정 연결 솔루션: SAML 1.1 HTTP-아티팩트 프로필

이 예에서 smcompany.com 은 생산자입니다. smcompany.com 의 관리자가 smcompany.com 과 ahealthco.com 사이에 SAML 1.1 생산자-소비자 파트너 관계를 구성합니다. 이 파트너 관계는 싱글 사인온에 HTTP-아티팩트 프로필을 사용합니다.

smcompany.com 의 파트너 관계에는 다음과 같은 정보가 있습니다.

- ahealthco.com 에서 어설션 소비자 서비스의 위치
- 고유한 이름 ID
- 어설션에 추가되는 어설션 특성

smcompany.com 의 직원이 회사 사이트에 로그인하면 처음에 웹 에이전트에 의해 인증됩니다. smcompany.com 의 직원이 직원 포털 웹 사이트에 액세스할 때 이벤트 순서는 다음과 같습니다:

1. 직원이 smcompany.com 에서 링크를 클릭하여 ahealthco.com 의 의료 혜택을 봅니다. 이 링크는 smcompany.com 의 사이트 간 전송 서비스에 요청합니다.
2. 사이트 간 전송 서비스는 정책 서버를 호출하고 정책 서버에 어설션 및 아티팩트를 생성하라는 요청을 보냅니다. 정책 서버는 어설션을 생성하고 어설션을 세션 저장소에 저장합니다. 또한 아티팩트를 생성해 서비스에 반환합니다.
3. 웹 에이전트는 SAML 아티팩트를 사용해 사용자를 ahealthco.com 으로 리디렉션합니다.

ahealthco.com 은 소비자 사이트입니다. ahealthco.com 의 관리자는 smcompany.com 과 소비자-생산자 파트너 관계를 구성합니다. 이 파트너 관계는 싱글 사인온에 HTTP-아티팩트 프로필을 사용합니다.

파트너 관계 구성에는 다음과 같은 정보가 있습니다.

- smcompany.com 의 아티팩트 검색 서비스 위치
- 사용자 디렉터리에서 사용자를 찾는 데 사용되는 어설션의 특성
- 로컬 디렉터리에서 사용자 레코드를 찾는 검색 문자열. 이 레코드는 어설션의 값과 일치해야 합니다.
- 대상 리소스

ahealthco.com 이 어설션을 받으며 이벤트 순서는 다음과 같습니다.

1. 브라우저가 응답을 SAML 자격 증명 수집기 URL 에 포스트합니다.
2. 서비스는 요청을 SAML 아티팩트와 함께 smcompany.com 의 어설션 검색 서비스로 보냅니다. 어설션 검색 서비스는 아티팩트에서 세션 ID 를 추출합니다.
3. 어설션 검색 서비스는 세션 저장소에서 어설션을 가져옵니다. 이 어설션을 ahealthco.com 의 SAML 자격 증명 수집기에 아티팩트 응답으로 보냅니다.
4. SAML 자격 증명 수집기는 어설션의 유효성을 검사합니다. 정책 서버는 세션을 만들고 ahealthco.com 도메인의 브라우저에 세션 쿠키를 저장합니다.
5. SAML 자격 증명 수집기는 사용자를 ahealthco.com 의 대상 리소스로 리디렉션합니다.

계정 연결 솔루션: SAML 1.x POST 프로필

이 예에서 smcompany.com 은 생산자입니다. smcompany.com 의 관리자는 생산자-소비자 파트너 관계를 구성합니다. 이 파트너 관계는 싱글 사인온에 SAML 1.x POST 프로필을 사용합니다.

파트너 관계 구성에는 다음과 같은 정보가 있습니다.

- ahealthco.com 에서 어설션 소비자 서비스의 위치
- 고유한 이름 ID
- 어설션에 추가되는 어설션 특성

smcompany.com 의 직원이 직원 포털 사이트에 액세스할 때 이벤트 순서는 다음과 같습니다:

1. 웹 에이전트가 초기 인증을 제공합니다.
2. 직원이 smcompany.com 에서 링크를 클릭하여 ahealthco.com 의 의료 혜택을 봅니다. 이 링크는 smcompany.com 의 사이트 간 전송 서비스에 요청합니다.
3. 사이트 간 전송 서비스가 어설션 생성기를 호출하면 어설션 생성기가 SAML 어설션을 생성하고 SAML 응답에 서명합니다.

4. 그런 다음 서명된 응답이 자동 POST HTML 양식에 포함되어 사용자 브라우저에 전송됩니다.
5. 브라우저가 응답이 포함된 양식을 ahealthco.com 의 어설션 소비자 서비스에 포스트합니다.

ahealthco.com 은 소비자 사이트입니다. ahealthco.com 의 SAML 자격 증명 수집기 서비스가 SAML 응답을 처리합니다. ahealthco.com 의 관리자는 싱글 사인온에 SAMl 1.1 HTTP-POST 프로필을 사용하는 smcompany.com 과 소비자-생산자 파트너 관계를 구성합니다.

파트너 관계 구성에는 다음과 같은 정보가 있습니다.

- smcompany.com 의 아티팩트 검색 서비스 위치
- 사용자 디렉터리에서 사용자를 찾는 데 사용되는 어설션의 특성
- 로컬 디렉터리에서 사용자 레코드를 찾는 검색 문자열. 이 레코드는 어설션의 값과 일치해야 합니다.
- 대상 리소스

이벤트 순서는 다음과 같습니다.

1. SAML 자격 증명 수집기가 생산자에게서 어설션을 받습니다.
2. SAML 자격 증명 수집기가 ahealthco.com 의 정책 서버를 호출합니다.
3. 정책 서버가 어설션의 서명을 확인한 다음 이를 사용하여 사용자를 인증합니다.
4. 인증에 성공하면 정책 서버는 SMSESSION 쿠키를 생성해 브라우저에 배치합니다.
5. 브라우저가 사용자를 ahealthco.com 의 대상 리소스로 리디렉션합니다.

계정 연결 솔루션: SAML 2.0 아티팩트 프로필

이 예에서 smcompany.com 은 아이덴티티 공급자입니다. smcompany.com 의 관리자는 원격 SP 인 ahealthco.com 과 IdP-SP 파트너 관계를 구성합니다.

파트너 관계 구성에는 다음 정보가 포함됩니다.

- ahealthco.com 에서 어설션 소비자 서비스의 위치
- 고유한 이름 ID
- 어설션에 추가되는 어설션 특성

직원이 직원 포털 사이트에 액세스하면 다음과 같은 순서로 이벤트가 발생합니다.

1. 웹 에이전트가 초기 인증을 제공합니다.
2. 사용자가 링크를 클릭하여 ahealthco.com 의 의료 혜택을 봅니다. 이 요청은 아이덴티티 공급자에서 시작되었으므로 원치 않는 응답을 트리거합니다.
3. FWS(페더레이션 웹 서비스)가 정책 서버에서 SAML 아티팩트를 요청합니다.
4. 정책 서버가 SAML 어설션 및 아티팩트를 생성합니다. 정책 서버가 어설션을 세션 저장소에 저장하고 아티팩트는 URL 매개 변수로 저장합니다.
5. 정책 서버가 SAML 아티팩트가 포함된 응답을 FWS 에 반환합니다.
6. 웹 에이전트가 사용자를 SAML 아티팩트와 함께 ahealthco.com 으로 리디렉션합니다.

ahealthco.com 은 서비스 공급자입니다. ahealthco.com 의 관리자는 아티팩트 프로필을 사용하는 smcompany.com 과의 SP-IdP 파트너 관계를 구성합니다. 파트너 관계 구성에는 다음과 같은 정보가 있습니다.

- smcompany.com 의 싱글 사인온 서비스 위치
- 사용자 디렉터리에서 사용자를 찾는 데 사용되는 어설션의 특성
- 로컬 디렉터리에서 사용자 레코드를 찾는 검색 문자열. 이 레코드는 어설션의 값과 일치해야 합니다.
- 대상 리소스

이벤트 순서는 다음과 같습니다.

1. 어설션 소비자 서비스가 아티팩트를 수신합니다. 이 서비스는 smcompany.com 의 파트너 관계 구성에서 아티팩트 레졸루션 서비스의 위치를 가져옵니다.
2. 어설션 소비자 서비스가 백 채널을 통해 smcompany.com 의 아티팩트 레졸루션 서비스를 호출합니다.
3. 정책 서버가 세션 저장소에서 어설션을 검색하고 응답을 ahealthco.com 의 어설션 소비자 서비스에 반환합니다.
4. 어설션 소비자 서비스가 응답의 유효성을 검사하고 ahealthco.com 에 대한 세션을 생성합니다. 세션 쿠키가 브라우저에 기록됩니다.
5. 브라우저가 사용자를 ahealthco.com 의 대상 리소스로 리디렉션합니다.

계정 연결 솔루션: SAML 2.0 POST 프로필

이 예에서 smcompany.com 은 아이덴티티 공급자입니다. smcompany.com 의 관리자는 IdP-SP 파트너 관계를 구성합니다. 이 파트너 관계는 싱글 사인온에 SAML 2.0 HTTP-POST 프로필을 사용합니다.

파트너 관계 구성에는 다음과 같은 정보가 있습니다.

- ahealthco.com 에서 어설션 소비자 서비스의 위치
- 고유한 이름 ID
- 어설션에 추가되는 어설션 특성

smcompany.com 의 직원이 직원 포털 사이트에 로그인합니다.

초기 인증에 성공하면 다음과 같은 순서로 이벤트가 발생합니다.

1. smcompany.com 의 웹 에이전트가 처음에 사용자를 인증합니다.
2. 직원이 ahealthco.com 에 대한 링크를 클릭하여 의료 혜택을 봅니다. 정책 서버가 SAML 2.0 SP 구성을 읽습니다.

   아이덴티티 공급자가 요청을 시작하므로, 원치 않는 응답을 트리거합니다.
3. 요청이 smcompany.com 의 SSO(싱글 사인온) 서비스로 전송됩니다.
4. SSO 서비스가 선택한 프로필에 기반하여 SAML 2.0 어설션/아티팩트를 생성하도록 정책 서버에 요청합니다. HTTP-POST 의 경우 정책 서버는 SAML 어설션을 생성합니다.
5. SSO 서비스가 선택한 프로필에 대한 어설션 응답을 받습니다.
6. 그러면 서명된 응답이 자동 POST HTML 양식에 포함되어 브라우저에 전송됩니다.
7. 브라우저가 응답을 ahealthco.com 의 어설션 소비자 서비스에 포스트합니다.

ahealthco.com 은 서비스 공급자입니다. ahealthco.com 의 관리자는 smcompany.com 과 SP-IdP 파트너 관계를 구성합니다. 이 구성에서는 싱글 사인온에 SAML 2.0 HTTP-POST 프로필을 사용합니다.

파트너 관계 구성에는 다음과 같은 정보가 있습니다.

- smcompany.com 의 아티팩트 검색 서비스 위치
- 사용자 디렉터리에서 사용자를 찾는 데 사용되는 어설션의 특성
- 로컬 디렉터리에서 사용자 레코드를 찾는 검색 문자열. 이 레코드는 어설션의 값과 일치해야 합니다.
- 대상 리소스

ahealthco.com 의 이벤트 순서는 다음과 같습니다.

1. 어설션 소비자 서비스가 Post 데이터에서 응답 메시지를 가져옵니다.
2. 어설션 소비자 서비스가 IdP 구성을 읽어 대상 URL 을 가져옵니다.
3. 어설션 소비자 서비스가 서명된 SAML 응답을 ahealthco.com 의 정책 서버에 자격 증명으로 전달합니다.
4. 정책 서버가 서명을 확인한 다음 사용자를 인증합니다.
5. 로그인이 성공합니다.
6. 정책 서버가 ahealthco.com 도메인에 대한 SMSESSION 쿠키를 만들고 쿠키를 브라우저에 배치합니다.
7. 브라우저가 사용자를 ahealthco.com 의 대상 리소스로 리디렉션합니다.

계정 연결 솔루션: WS-페더레이션 피동 요청자 프로필

이 예에서 smcompany.com 은 아이덴티티 공급자입니다. smcompany.com 의 관리자는 WSFED IP-RP 파트너 관계를 구성합니다. 이 파트너 관계는 싱글 사인온에 WS-페더레이션 피동 요청자 프로필을 사용합니다. 이 사용 사례에서는 리소스 파트너인 ahealthco.com 이 싱글 사인온을 시작합니다.

SAML 토큰 유형은 SAML 1.1 입니다. 이것은 IP 엔터티 구성의 일부입니다.

파트너 관계 구성에는 다음과 같은 정보가 있습니다.

- ahealthco.com 에서 보안 토큰 소비자 서비스의 위치
- 고유한 이름 ID
- 어설션에 추가되는 어설션 특성

smcompany.com 의 직원이 직원 포털에 액세스할 때 다음과 같은 순서로 이벤트가 발생합니다.

1. 사용자가 ahealthco.com 의 보호되지 않은 사이트 선택 페이지를 방문합니다. 웹 에이전트가 초기 인증을 제공합니다.
2. 사용자가 smcompany.com 의 싱글 사인온 서비스를 가리키는 링크를 클릭합니다. 브라우저가 사용자를 smcompany.com 으로 리디렉션합니다.
3. SSO 서비스가 정책 서버를 호출합니다. 정책 서버가 어설션을 생성합니다.
4. 정책 서버가 요청 보안 토큰 응답의 어설션 요소에 서명하고 응답을 반환합니다.
5. 브라우저가 자동 POST HTML 양식의 응답을 ahealthco.com 의 보안 토큰 소비자 서비스에 포스트합니다.

ahealthco.com 은 리소스 파트너입니다.

파트너 관계 구성에는 다음과 같은 정보가 있습니다.

- smcompany.com 의 싱글 사인온 서비스 위치
- 사용자 디렉터리에서 사용자를 찾는 데 사용되는 어설션의 특성
- 로컬 디렉터리에서 사용자 레코드를 찾는 검색 문자열. 이 레코드는 어설션의 값과 일치해야 합니다.
- 대상 리소스

이벤트 순서는 다음과 같습니다.

1. 보안 토큰 소비자 서비스가 보안 토큰 소비자 응답에서 어설션을 추출합니다.
2. 서비스가 대상 리소스를 결정합니다.
3. 보안 토큰 소비자 서비스가 서명된 어설션을 ahealthco.com 의 정책 서버에 자격 증명으로 전달합니다.
4. 정책 서버가 서명을 확인한 다음 사용자를 인증합니다.
5. 성공적인 인증 후 보안 토큰 소비자 서비스가 SMSESSION 쿠키를 생성합니다.
6. 그런 다음 서비스가 쿠키를 브라우저에 넣고 사용자를 ahealthco.com 의 대상 리소스로 리디렉션합니다.

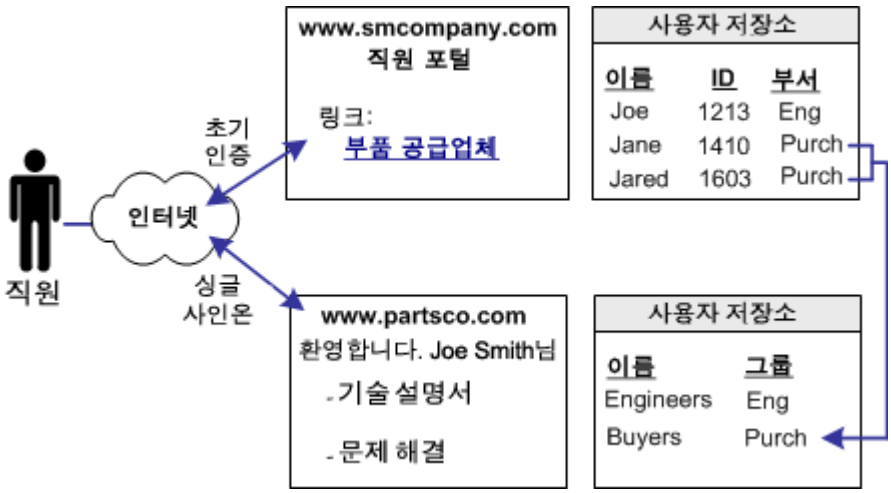
사용 사례: 사용자 특성에 기반한 싱글 사인온

사용 사례 2 에서 smcompany.com 은 partsco.com 이라는 비즈니스 파트너에게 부품을 구매합니다.

엔지니어가 smcompany.com 에서 인증을 받은 다음 partsco.com 의 정보에 액세스하기 위해 링크를 클릭합니다. smcompany.com 의 엔지니어는 로그인할 필요 없이 partsco.com 웹 사이트의 "Specifications"(사양) 부분에 직접 연결됩니다.

smcompany.com 의 구매자가 인증을 받은 다음 partsco.com 의 링크를 클릭합니다. 구매자는 partsco.com 웹 사이트의 "Parts List"(부품 목록) 부분으로 직접 연결됩니다. 구매자는 로그인할 필요가 없습니다.

다음 그림에서는 두 파트너 간의 관계를 보여 줍니다.



개별 사용자에 대한 인터페이스를 개인화하기 위해 사용자 이름 등의 다른 특성이 smcompany.com 에서 partsco.com 으로 전달됩니다.

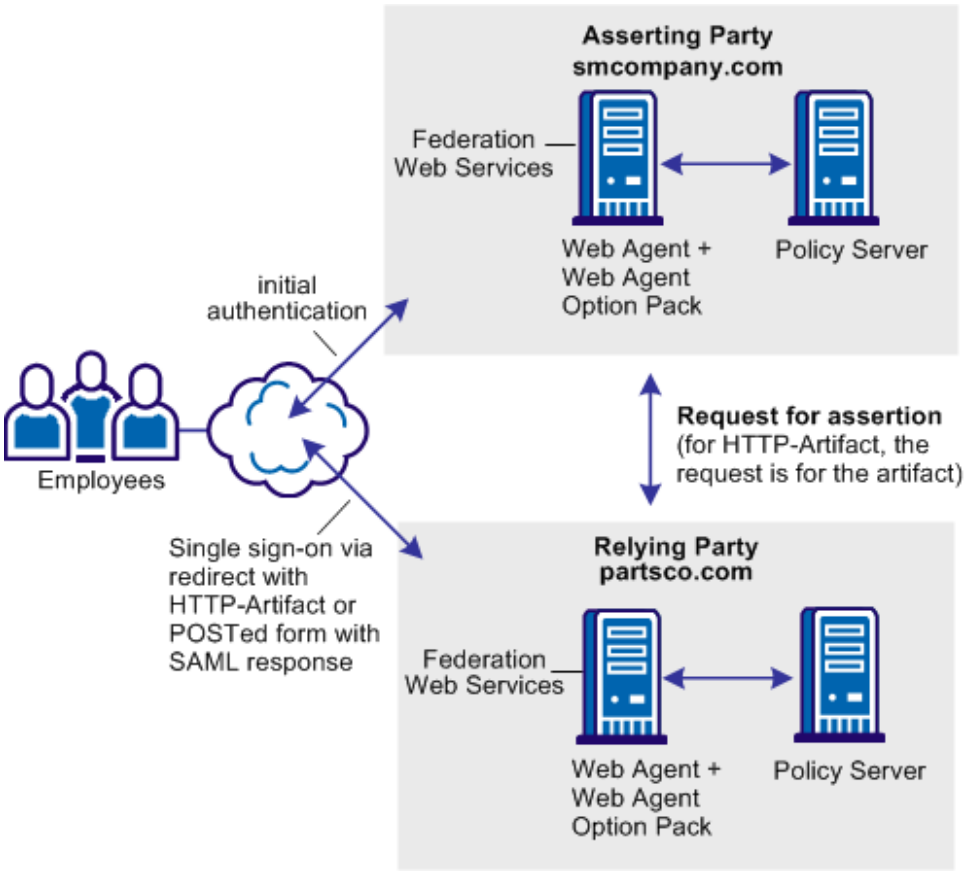
partsco.com 은 smcompany.com 의 일부 직원에 대한 사용자 아이덴티티만 유지 관리하면서 웹 사이트의 중요한 부분에 대한 액세스를 제어하고자 합니다. 액세스를 제어하기 위해 partsco.com 은 smcompany.com 에 있는 사용자에 대해 제한된 수의 아이덴티티를 유지 관리합니다. 엔지니어에 대한 아이덴티티와 구매자에 대한 아이덴티티가 하나씩 유지 관리됩니다.

smcompany.com 의 직원이 partsco.com 에 액세스하면 smcompany.com 이 안전한 방식으로 사용자 특성을 partsco.com 에 보냅니다. partsco.com 은 특성을 사용하여 사용자에 대한 액세스를 제어하는 아이덴티티를 결정합니다.

솔루션: 사용자 특성에 기반한 싱글 사인온

페더레이션을 smcompany.com 및 partsco.com 에 배포하여 사용 사례: 사용자 특성 프로필에 기반한 싱글 사인온 (페이지 23)을 해결할 수 있습니다.

이 그림은 SAML 1.1, SAML 2.0 및 WS-페더레이션의 경우와 유사합니다.



SiteMinder 는 두 사이트 모두에 배포됩니다. 사용자와 각 사이트 간의 상호 작용은 유사합니다. 여기서 partsco.com 은 신뢰 당사자의 역할을 맡고 있습니다. 페더레이션 웹 서비스 응용 프로그램은 트랜잭션 처리에 필요한 모든 서블릿을 포함합니다.

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.

이벤트 순서는 다음 항목을 제외하고 계정 연결에 기반한 싱글 사인온 (페이지 15)에 대한 솔루션과 유사합니다.

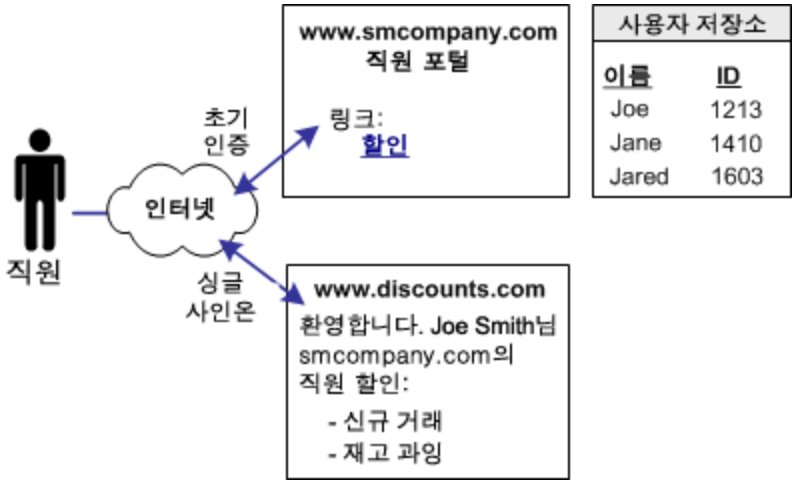
- smcompany.com 의 관리자는 partsco.com 과의 파트너 관계를 구성합니다.
- 파트너 관계 구성에는 *department* 라는 어설션 특성이 포함됩니다. 이 특성은 사용자가 속한 부서를 지정합니다. 정책 서버는 요청하는 사용자에 대해 생성하는 어설션에 이 특성을 포함합니다.
- 관리자는 partsco.com 웹 사이트에 액세스하도록 허용된 각 부서에 대해 사용자 레코드를 하나씩 정의합니다.
- partsco.com 의 관리자는 smcompany.com 과의 파트너 관계를 정의합니다.
- 어설션 소비자 서비스는 어설션에서 부서 특성을 추출합니다. 정책 서버는 partsco.com 의 사용자 디렉터리에서 부서 특성의 값이 일치하는 사용자 레코드를 검색합니다.

사용 사례: 로컬 사용자 계정이 없는 싱글 사인온

이 사용 사례에서 smcompany.com 은 discounts.com 과 파트너 관계를 맺고 직원에게 할인을 제공합니다.

smcompany.com 의 직원은 smcompany.com 에서 인증을 받고 링크를 클릭하여 discounts.com 에 액세스합니다. 이 직원은 discounts.com 웹 사이트에 연결되며 discounts.com 웹 사이트에 로그인하지 않고도 smcompany.com 의 직원에게 제공되는 할인을 제공받습니다.

다음 그림에서는 이 사용 사례를 보여 줍니다.

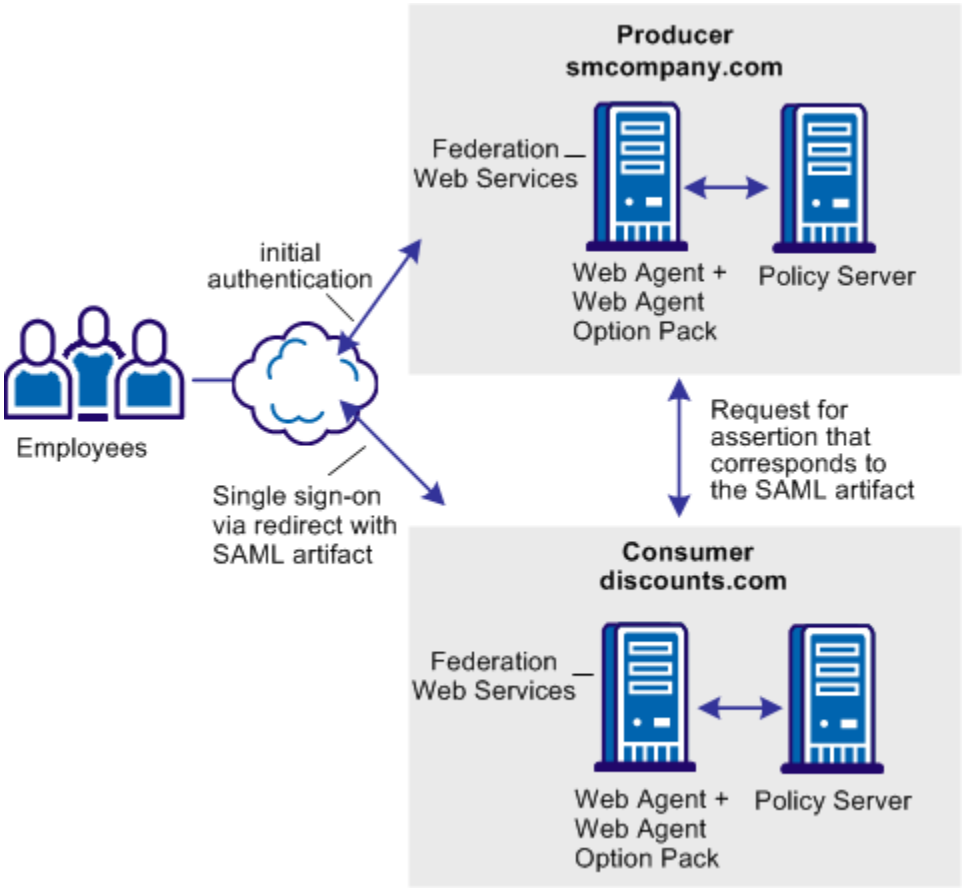


discounts.com 은 smcompany.com 에 대한 아이덴티티를 유지 관리하지 않습니다. 이 회사는 smcompany.com 의 모든 직원이 smcompany.com 에서 인증을 받은 경우 discounts.com 에 액세스하도록 허용합니다. smcompany.com 은 리소스를 요청하는 사용자에 대한 인증 정보를 discounts.com 에 안전하게 전송하여 액세스가 허용되게 합니다.

솔루션: 로컬 사용자 계정이 없는 싱글 사인온

페더레이션을 smcompany.com 및 discounts.com 에 배포하여 사용 사례: 로컬 사용자 계정 없는 싱글 사인온 (페이지 25)을 해결합니다.

다음 그림에서는 로컬 사용자 계정이 없는 싱글 사인온을 보여 줍니다. 사용 중인 SSO 프로필은 SAML 1.1 입니다.



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.

이 배포에서는 SiteMinder 가 두 사이트 모두에 있습니다. smcompany.com 은 SAML 1.1 생산자입니다. smcompany.com 의 관리자는 discounts.com 을 나타내는 원격 엔터티가 포함된 SAML 1.1 파트너 관계를 구성합니다. 파트너 관계에서 구성된 모든 특성이 어설션에 포함됩니다.

이 솔루션이 작동하려면 단일 사용자를 기본적으로 익명 사용자로 만들어 모든 사용자를 단일 사용자 계정에 매핑해야 합니다.

smcompany.com 직원이 직원 포털에 액세스할 때 다음 프로세스가 수행됩니다.

1. 웹 에이전트가 초기 인증을 제공합니다.
2. 직원이 링크를 클릭하여 discounts.com 의 거래에 액세스합니다. 이 링크는 사용자를 다른 사이트로 전송하는 결과를 가져오므로 사이트 간 전송 URL 이라고 합니다.
3. 사이트 간 전송 URL 이 웹 에이전트에 요청합니다. 이 URL 에는 SAML 자격 증명 수집기 위치와 소비자 사이트의 대상 URL 이 포함됩니다.
4. smcompany.com 의 웹 에이전트가 정책 서버를 호출합니다. 정책 서버는 어설션 및 아티팩트를 생성하고 어설션을 세션 저장소에 저장합니다.
5. 정책 서버가 아티팩트를 FWS 응용 프로그램에 반환하고, 이 응용 프로그램은 응답을 생성합니다.
6. 브라우저가 사용자를 아티팩트 응답과 함께 discounts.com 으로 리디렉션합니다.

discounts.com 은 소비자 사이트입니다. discounts.com 의 관리자는 SP-IdP 파트너 관계를 구성합니다. 이 파트너 관계 구성은 smcompany.com 의 어설션 검색 서비스 위치와 보호된 대상 리소스를 지정합니다.

파트너 관계에 대한 사용자 ID 구성에서는 단일 사용자를 조회하는 사용자 지정 사용자 검색 사양을 지정해야 합니다. 예를 들어 사용자 디렉터리가 LDAP 인 경우 검색 사양은 uid=user1 입니다.

중요! 모든 사용자를 단일 사용자에 매핑하려면 discounts.com 에 사용자 디렉터리가 있어야 합니다. 이 사용자 디렉터리에는 단일 사용자 레코드가 포함되어 있어야 합니다. 다른 방법은 정책 서버 API 를 사용하여 동일한 사용자 레코드를 반환하는 사용자 레코드를 만드는 것입니다.

다음 프로세스가 수행됩니다.

1. 브라우저가 응답을 SAML 자격 증명 수집기에 포스트하고, 이 수집기는 smcompany.com 의 어설션 검색 서비스 위치를 가져옵니다.
2. SAML 자격 증명 수집기가 smcompany.com 의 어설션 검색 서비스에 대한 백 채널 호출을 수행합니다. 세션 ID 가 아티팩트에서 추출됩니다.
3. 정책 서버가 세션 저장소에서 어설션을 검색하여 discounts.com 의 SAML 자격 증명 수집기에 반환합니다.

4. 그런 다음 SAML 자격 증명 수집기가 SAML 어설션의 유효성을 검사하고 브라우저에 세션 쿠키를 발급합니다.
5. 브라우저가 사용자를 discounts.com 의 대상 리소스로 리디렉션합니다.

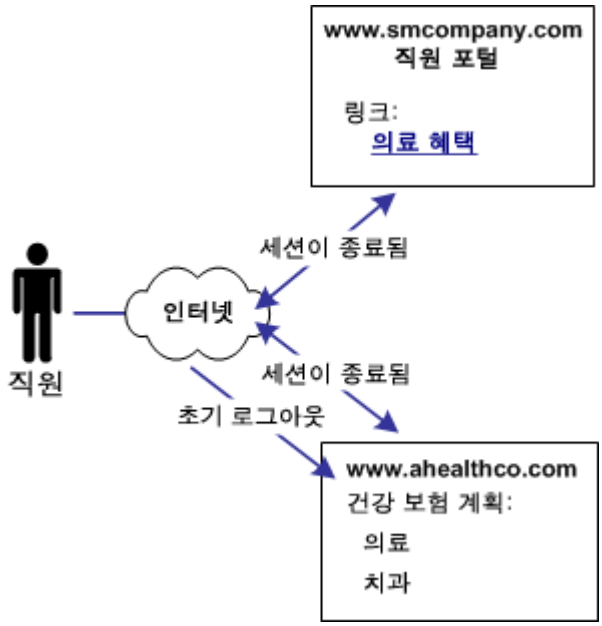
사용 사례: SAML 2.0 싱글 로그아웃

이 사용 사례에서는 smcompany.com 의 직원이 직원 포털에서 인증받은 다음 ahealthco.com 의 의료 혜택 정보를 보기 위해 링크를 선택합니다. 이 직원은 ahealthco.com 웹 사이트에 연결되며 사이트에 로그인할 필요 없이 의료 혜택 정보가 제공됩니다.

직원이 ahealthco.com 에서 로그아웃한 후 사이트는 사용자 세션이 ahealthco.com 과 smcompany.com 에서 종료되었는지 확인하고자 합니다. 두 세션을 모두 종료하면 권한 없는 직원이 기존 세션을 사용하여 smcompany.com 의 리소스에 액세스하거나 권한 있는 직원의 혜택 정보를 보지 못하게 됩니다.

참고: 이 사례에서는 초기 로그아웃이 ahealthco.com 에서 발생하고 결과적으로 두 세션이 모두 종료됩니다.

다음 그림에서는 이 사용 사례를 보여 줍니다.



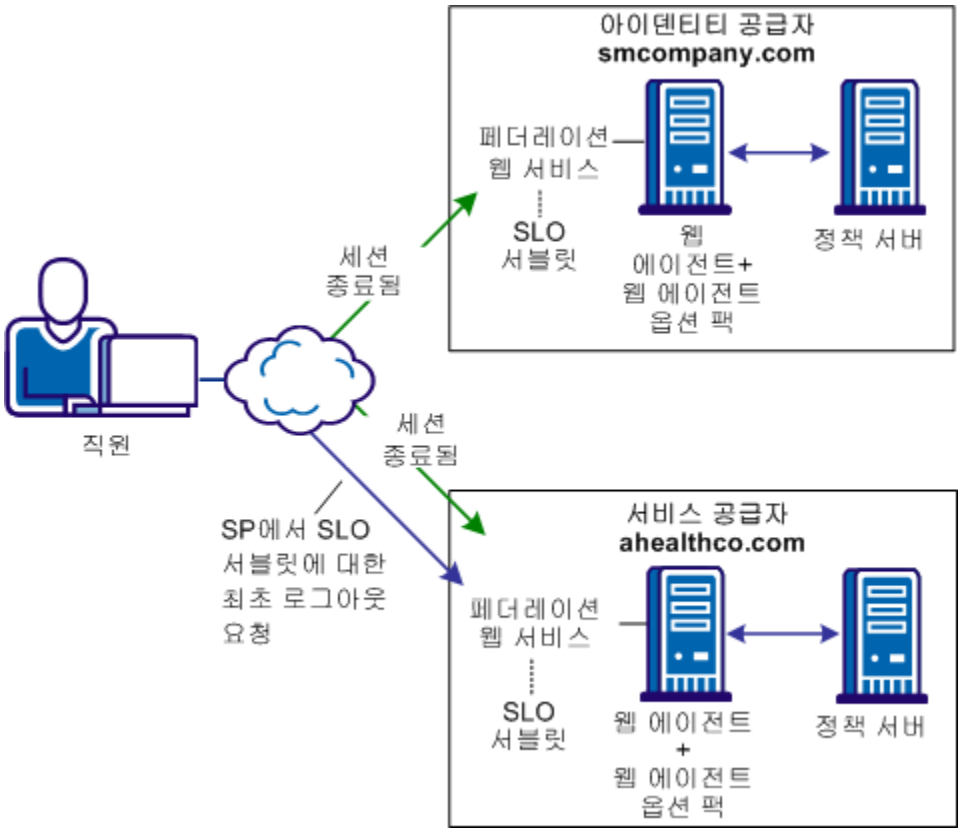
솔루션: SAML 2.0 싱글 로그아웃

페더레이션을 사용하여 사용 사례: SAML 2.0 싱글 로그아웃 (페이지 29)을 해결할 수 있습니다.

이 솔루션에서

- smcompany.com 은 아이덴티티 공급자입니다.
- ahealthco.com 은 로그아웃 요청을 시작하는 서비스 공급자입니다.
- 싱글 로그아웃은 아이덴티티 공급자와 서비스 공급자에서 사용되도록 설정됩니다.

다음 그림에서는 싱글 로그아웃에 대한 솔루션을 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.

SP 에서 시작되는 싱글 로그아웃에 대해 다음과 같은 순서로 이벤트가 발생합니다.

1. 직원이 smcompany.com 에서 인증을 받은 다음 페더레이션된 싱글 사인온을 통해 ahealthcom.com 의 의료 혜택에 액세스합니다. smcompany.com 이 ahealthco.com 에 대한 정보를 해당 세션 저장소에 넣습니다. ahealthco.com 이 smcompany.com 에 대한 정보를 해당 세션 저장소에 넣습니다.
2. 직원이 의료 혜택에 대한 검토를 마치고 ahealthco.com 에서 로그아웃 링크를 클릭합니다. 브라우저가 싱글 로그아웃 서블릿에 액세스합니다.
3. ahealthco.com 의 FWS 응용 프로그램이 기존 SMSESSION 쿠키의 이름을 SESSIONSIGNOUT 으로 바꾸어 사용자의 현재 세션을 무효화합니다.
4. ahealthco.com 측에서 사용자 세션이 종료됩니다.

   참고: 종료되었다고 해서 세션이 세션 저장소에서 제거되는 것은 아니며 상태가 LogoutInProgress 로 설정될 뿐입니다.
5. 정책 서버가 로그아웃 요청을 생성하여 smcompany.com 에서 사용자 세션을 무효화합니다. 정책 서버는 smcompany.com 의 공급자 ID 도 반환합니다.
6. 브라우저가 smcompany.com 의 싱글 로그아웃 서블릿으로 로그아웃 요청을 리디렉션하고, 로그아웃 요청 메시지가 쿼리 매개 변수로 추가됩니다.
7. FWS 응용 프로그램이 로그아웃 요청 메시지를 검색하고 SMSESSION 쿠키 이름을 SESSIONSIGNOUT 으로 바꿉니다.
8. FWS 가 해당 사용자 세션과 연결된 모든 서비스 공급자에서 사용자 세션을 무효화합니다. 로그아웃 요청을 시작한 ahealthco.com 의 세션만 제외합니다.
9. 결국 모든 서비스 공급자가 로그아웃을 확인하고 smcompany.com 이 세션 저장소에서 사용자 세션을 제거합니다. FWS 가 SESSIONSIGNOUT 쿠키를 삭제합니다.

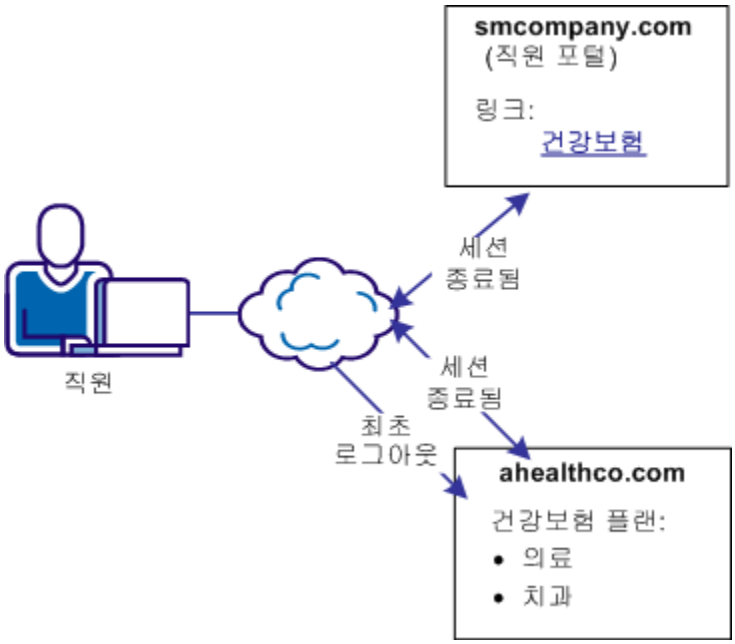
   참고: 다른 서비스 공급자는 그림에 나와 있지 않습니다.
10. smcompany.com 이 ahealthco.com, 즉 시작하는 서비스 공급자에게 로그아웃 응답 메시지를 반환하고 사용자 세션이 세션 저장소에서 제거됩니다.
11. 마지막으로 사용자가 ahealthco.com 의 SLO 구성 페이지에 전송됩니다.

사용 사례: WS-페더레이션 사인아웃

이 사용 사례에서는 smcompany.com 직원이 직원 포털에서 인증을 받습니다. 직원은 링크를 클릭하여 ahealthco.com 의 의료 혜택을 봅니다. 이 직원은 ahealthco.com 웹 사이트에 연결되며 사이트에 사인온할 필요 없이 의료 혜택 정보가 제공됩니다.

직원이 로그아웃할 때 ahealthco.com 은 자사 사이트 및 smcompany.com 모두에서 사용자 세션이 종료되게 하려고 합니다. 두 세션을 모두 종료하면 권한 없는 사용자가 기존 세션을 사용하여 smcompany.com 또는 ahealthco.com 의 리소스에 액세스하지 못하게 됩니다.

다음 그림에서는 이 사용 사례를 보여 줍니다.



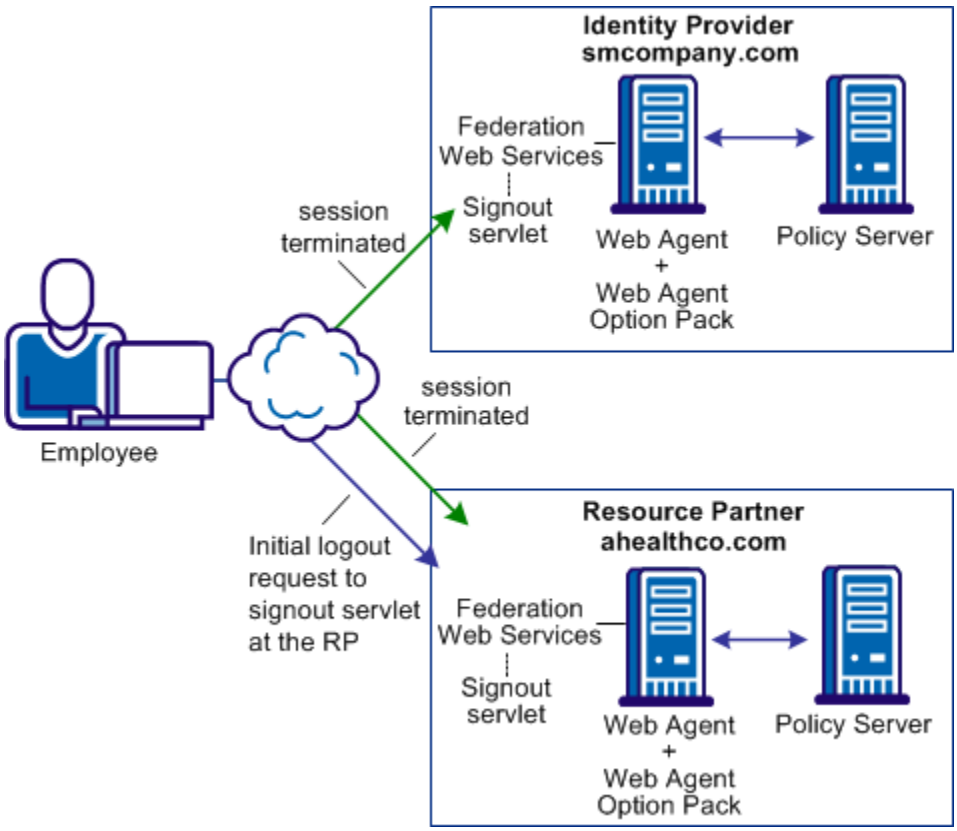
솔루션: WS-페더레이션 사인아웃

다음의 페더레이션된 배포로 사용 사례: WS-페더레이션 사인아웃 (페이지 32)을 해결합니다.

이 솔루션에서

- smcompany.com 은 아이덴티티 공급자입니다.
- ahealthco.com 은 리소스 파트너이며 사인아웃 요청을 시작합니다.
- 싱글 사인온이 사용되도록 smcompany.com 과 ahealthco.com 간에 WSFED IP-RP 파트너 관계가 구성되어 있습니다.
- 아이덴티티 공급자 및 리소스 파트너에서 HTTP 바인딩을 사용한 WS-페더레이션 사인아웃이 사용되도록 설정되었습니다.

다음 그림에서는 WS-페더레이션 사인아웃을 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.

다음과 같은 순서로 이벤트가 발생합니다.

1. 직원이 smcompany.com 에서 인증을 받고 ahealthco.com 에 페더레이션되어 의료 혜택에 액세스합니다. 트랜잭션 중에 smcompany.com 이 ahealthco.com 에 대한 정보를 해당 세션 저장소에 넣습니다. ahealthco.com 이 smcompany.com 에 대한 정보를 해당 세션 저장소에 넣습니다.
2. 직원이 의료 혜택 정보 보기를 마치고 ahealthco.com 의 로그아웃 링크를 클릭합니다. 사인아웃 서비스가 사인아웃 요청을 받습니다.
3. 사인아웃 서비스가 SMSESSION 쿠키에서 세션 정보를 가져오고 사용자 세션과 연결된 아이덴티티 공급자를 결정합니다.
4. 사인아웃 서비스가 정책 서버를 호출하여 세션을 무효화합니다.
5. 사인아웃 서비스가 사인아웃 요청을 생성하고 사인아웃 요청을 smcompany.com 의 사인아웃 URL 로 전달합니다.
6. smcompany.com 의 사인아웃 서비스가 요청을 받습니다.
7. 사인아웃 서비스가 SMSESSION 쿠키에서 세션 정보를 가져오고 사용자 세션과 연결된 리소스 파트너를 결정합니다.
8. 사인아웃 서비스가 정책 서버를 호출하여 세션을 무효화합니다.
9. 사인아웃 서비스가 사인아웃 요청을 생성하고 SignoutConfirmURL JSP 에 사인아웃 메시지와 여러 RP-SignoutCleanup 위치를 post 데이터로 포스트합니다.

   SignoutConfirm 페이지는 프레임 기반 HTML 페이지를 생성합니다. 각 프레임에는 사용자 세션과 연결된 각 리소스 파트너의 사인아웃 삭제 URL 이 포함됩니다.
10. ahealthco.com 이 사인아웃 요청을 사용자 세션과 연결된 리소스 파트너로 전달합니다. 각 RP 에서 세션이 세션 저장소에서 종료됩니다.
11. 각 RP 가 사인아웃을 완료하기 위해 시작 파트너인 사인아웃 삭제 URL ahealthco.com 으로 브라우저를 리디렉션합니다.

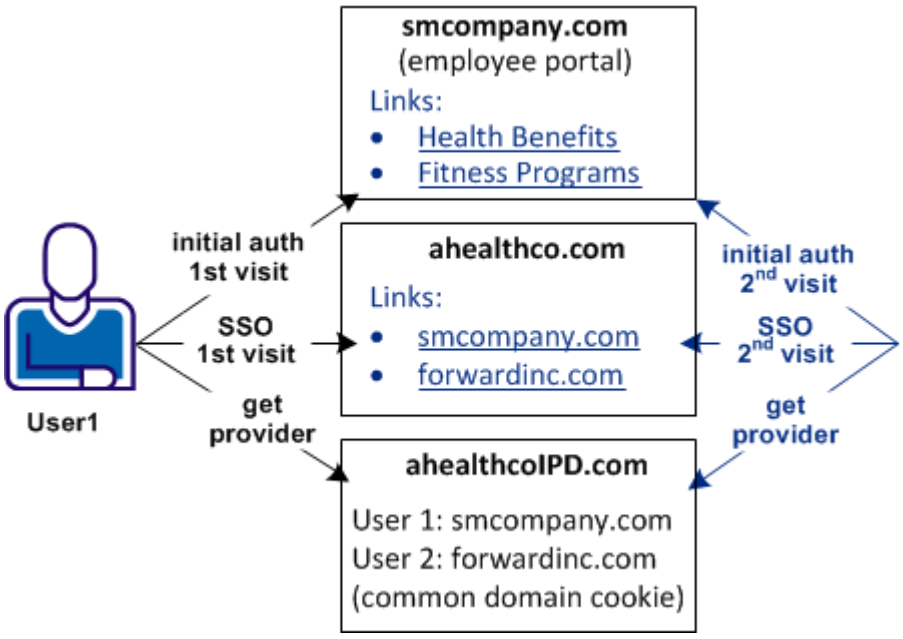
사용 사례: 아이덴티티 공급자 검색 프로필

이 사용 사례에서는 여러 회사가 ahealthco.com 의 의료 혜택 계약을 맺습니다. 사용자는 ahealthco.com 에 로그온하여 의료 혜택 정보를 봅니다. ahealthco.com 은 특정 사용자에 대해 인증 요청을 보낼 아이덴티티 공급자를 결정해야 합니다.

IdP 검색은 어설션을 제공하는 파트너가 둘 이상 있는 페더레이션된 네트워크에 유용합니다. 이 프로필은 필요한 사용자 레코드가 있는 아이덴티티 공급자를 서비스 공급자가 동적으로 결정할 수 있도록 지원합니다.

다음 그림에서는 아이덴티티 공급자 검색 프로필을 사용 중인 네트워크를 보여 줍니다.

참고: 모든 사이트가 아이덴티티 공급자 검색 서비스와 상호 작용하도록 허용하는 사전 비즈니스 계약이 이 네트워크의 사이트 간에 존재합니다.



이 예에서는 사용자 1 이 ahealthco.com 에 도달합니다. ahealthco.com 은 사용자 1 이 smcompany.com 소속인지 확인합니다. ahealthco.com 은 ahealthco.com 의 일반 도메인 쿠키에 smcompany.com 에 대한 쿠키를 설정합니다. forwardinc.com 과 같은 다른 회사는 ahealthco.com 을 의료 공급자로 이용하는 다른 아이덴티티 공급자입니다. forwardinc.com 의 사용자가 ahealthco.com 에 오면 역시 일반 도메인 쿠키에 쿠키가 설정됩니다.

솔루션: 아이덴티티 공급자 검색 프로필

페더레이션은 사용 사례: 아이덴티티 공급자 검색 프로필 (페이지 35)을 해결할 수 있습니다.

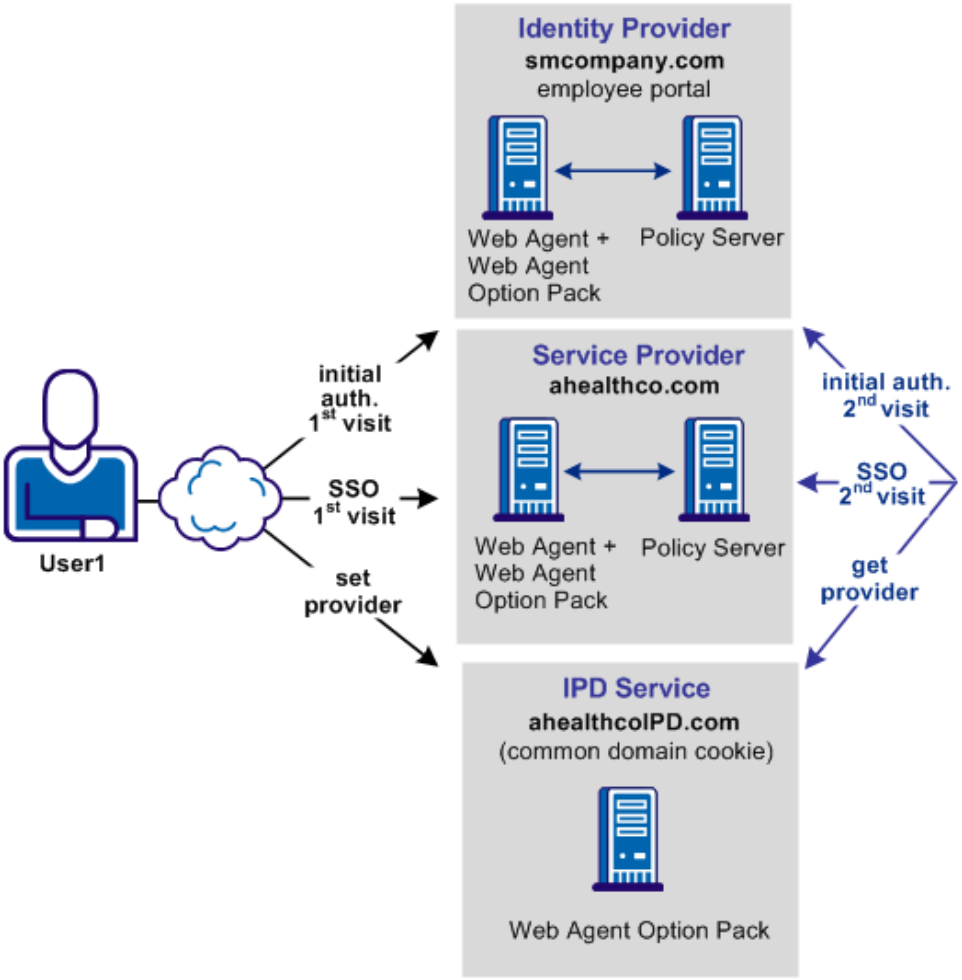
IdP 검색 프로필(SAML 2.0 에만 해당)은 두 페더레이션된 파트너에 공통적인 쿠키 도메인을 사용하여 구현됩니다. 약정된 도메인의 쿠키에는 사용자가 방문한 IdP 목록이 포함되어 있습니다.

참고: 서비스 공급자가 인증할 사용자는 서비스 공급자에 도달하기 전에 아이덴티티 공급자를 방문하여 인증을 받은 상태여야 합니다.

이 솔루션에서

- smcompany.com 은 사용자 1 에 대한 어설션을 발급하고 ahealthco.com 은 이 회사의 서비스 공급자로 구성되어 있습니다.
- ahealthco.com 은 smcompany.com 에 대한 서비스 공급자입니다. 이 사이트에는 해당 서비스를 사용하는 각 아이덴티티 공급자와 SAML 2.0 SP-IdP 파트너 관계가 구성되어 있습니다.
- ahealthcoIPD.com 은 ahealthco.com 에 대한 아이덴티티 공급자 검색 서비스입니다. 웹 에이전트 옵션 팩과 함께 설치되는 페더레이션 웹 서비스 응용 프로그램은 IPD 서비스를 제공합니다. 이 서비스는 ahealthco.com 에 대한 모든 관련 아이덴티티 공급자를 포함하는 일반 도메인 쿠키를 읽습니다.

다음 그림에서는 이 솔루션에 대한 페더레이션된 네트워크를 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.

트랜잭션 흐름은 다음과 같습니다.

1. 사용자 1 이 처음에 smcompany.com 에서 로그인하여 인증받습니다. 이후 사용자는 다시 인증할 필요 없이 ahealthco.com 에 페더레이션됩니다.

   smcompany.com 과 ahealthco.com 간에 ahealthcoIPD.com 을 IPD 서비스로 사용하는 계약이 존재합니다.

2. smcompany.com 의 FWS 응용 프로그램이 아이덴티티 공급자 ID 를 전달하여 정책 서버에서 IPD(아이덴티티 공급자 검색 프로필) 구성을 요청합니다.

3. 정책 서버가 IPD 구성과 함께 IPD 서비스 URL, 일반 도메인 쿠키, 일반 도메인 쿠키 지속 정보 등을 반환합니다.

4. smcompany.com 의 FWS 응용 프로그램이 사용자를 IPD 서비스 URL 로 리디렉션하여 일반 도메인 쿠키를 설정합니다. smcompany.com 의 아이덴티티 공급자 ID 는 IPD 서비스의 일반 도메인 쿠키에 기록됩니다.

5. IPD 서비스가 사용자를 다시 smcompany.com 의 싱글 사인온 서비스로 리디렉션합니다. 이 리디렉션에는 인증 요청이 포함됩니다.

6. smcompany.com 의 FWS 응용 프로그램이 정책 서버에서 어설션을 요청합니다. 정책 서버가 ahealthco.com 에 맺고 있는 파트너 관계 구성을 기반으로 하는 어설션을 생성합니다.

7. FWS 응용 프로그램이 어설션 응답을 다시 ahealthco.com 에 반환합니다.

8. 이제 사용자 1 이 ahealthco.com 에 로그온하여 의료 혜택 정보를 조회할 수 있습니다. 사용자가 의료 혜택 검토를 마치고 로그아웃합니다.

9. 다른 날에 별도의 트랜잭션에서 사용자 1 이 ahealthco.com 에 직접 로그인합니다. 사용자 1 이 링크를 클릭하여 의료 혜택을 다시 봅니다. ahealthIPD.com 에는 사용자 1 이 방문한 모든 아이덴티티 공급자에 대한 쿠키가 있습니다. ahealthco.com 이 IPD 검색 서비스를 호출하여 아이덴티티 공급자 ID 를 가져옵니다.

10. ahealthco.com 에서 사용자 1 에게 인증할 수 있는 회사를 선택하는 사이트 선택 페이지를 표시합니다. 사용자 1 이 smcompany.com 을 선택합니다.

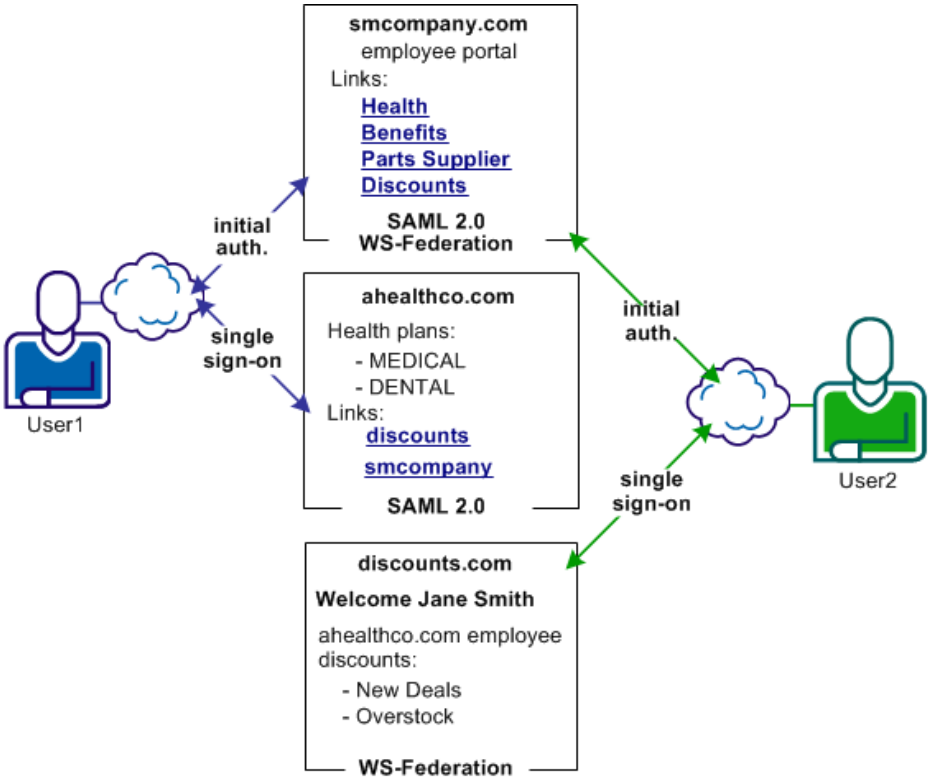
11. ahealthco.com 이 smcompany.com 에 인증 요청을 보냅니다. smcompany.com 의 정책 서버는 어설션을 생성하여 ahealthco.com 의 어설션 소비자 서비스에 다시 보냅니다.

12. 사용자가 성공적으로 로그인되어 요청된 리소스로 리디렉션됩니다.

사용 사례: 여러 SSO 프로필을 사용한 페더레이션

이 사용 사례에서 smcompany.com 은 ahealthco.com 과 discounts.com 에 대한 어설션을 발급합니다. ahealthco.com 은 SAML 2.0 프로필을 사용합니다. discounts.com 은 WS-페더레이션 프로필을 사용합니다. 발급된 어설션이 적절한 프로필에 따라 생성되어야 신뢰 당사자가 어설션을 소비할 수 있습니다.

다음 그림에서는 다중 프로토콜 사용 사례를 보여 줍니다.



솔루션: 여러 SSO 프로필을 사용한 페더레이션

다음 페더레이션 배포로 사용 사례: 여러 SSO 프로필을 사용한 페더레이션 (페이지 39)을 해결합니다.

참고: 이 솔루션의 싱글 사인온 트랜잭션은 계정 연결 트랜잭션을 사용하는 것과 유사합니다.

이 솔루션에서

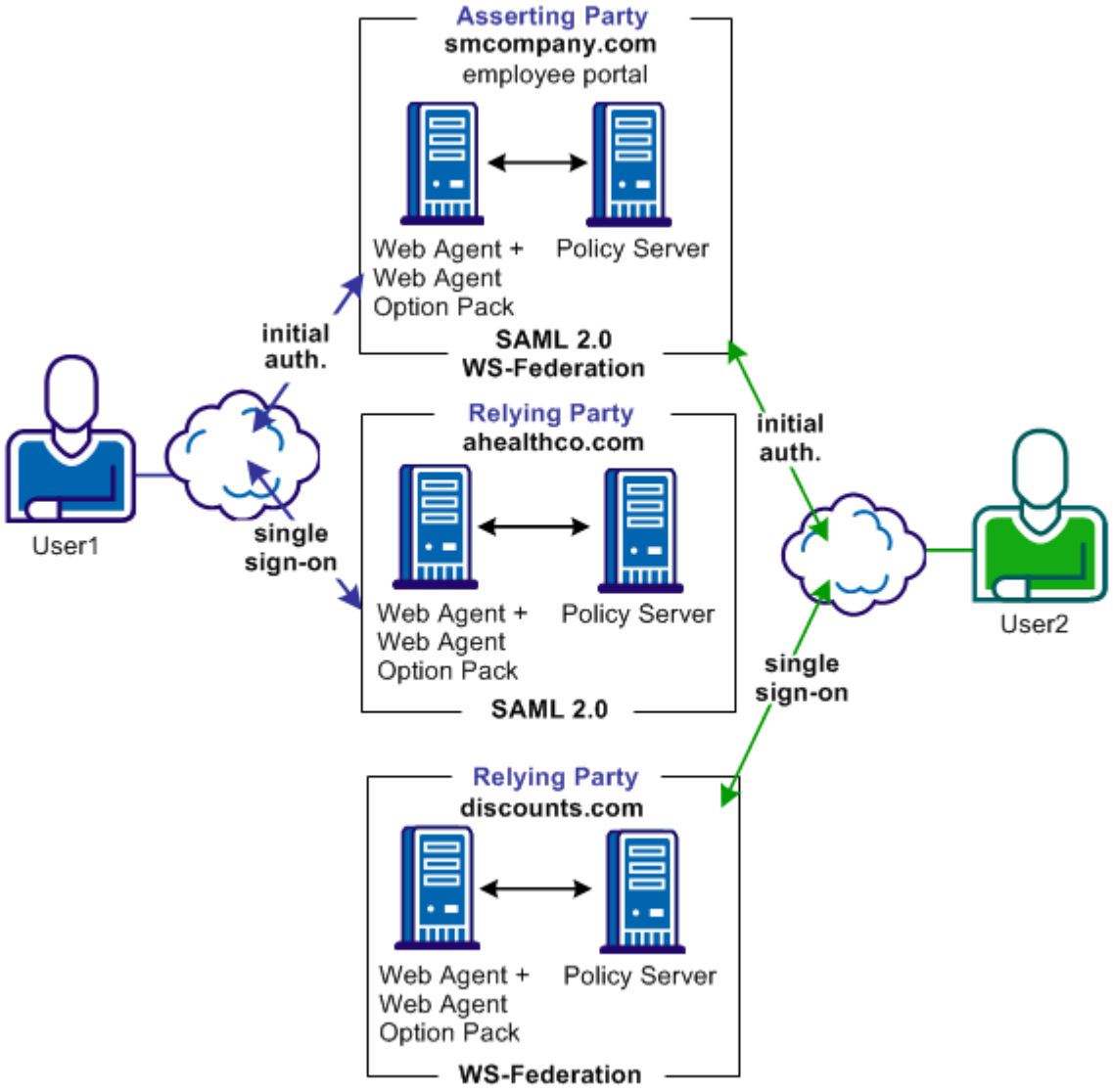
사용자 1

- smcompany.com 은 ahealthco.com 에 대한 SAML 2.0 아이덴티티 공급자입니다.
- ahealthco.com 은 SAML 2.0 서비스 공급자입니다.

사용자 2

- smcompany.com 은 discounts.com 에 대한 WS-페더레이션 아이덴티티 공급자입니다.
- discounts.com 은 WS-페더레이션 리소스 파트너입니다.

다음 그림에서는 다중 프로토콜 지원을 구현하는 페더레이션된 네트워크를 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.

이 다중 프로토콜 솔루션에서 다양한 SSO 프로필에 대한 싱글 사인온 트랜잭션의 흐름은 계정 연결 SSO 트랜잭션과 유사합니다.

- smcompany.com 은 사용자 1 이 ahealthco.com 의 리소스에 액세스하는 데 필요한 SAML 2.0 어설션을 발급할 수 있습니다.
- 또한 smcompany.com 은 사용자 2 가 discounts.com 에서 인증하기 위한 SAML 1.1 어설션을 포함하는 토큰 응답도 발급할 수 있습니다. 어설션에 대한 SSO 프로필은 파트너 관계 구성에 따라 결정되며 초기 인증이 수행되는 동안 설정된 세션 쿠키를 기반으로 합니다.

이 솔루션의 경우 smcompany.com 에서 다음 파트너 관계가 구성됩니다.

- smcompany.com 이 로컬 IdP 이고 ahealthco.com 이 원격 SP 인 IdP-SP 파트너 관계
- smcompany.com 이 로컬 IP 이고 discounts.com 이 원격 RP 인 IP-RP 파트너 관계

ahealthco.com 에서는 다음 파트너 관계가 구성됩니다.

- ahealthco.com 이 로컬 SP 이고 smcompany.com 이 원격 IdP 인 SP-IdP 파트너 관계

discounts.com 에서는 다음 파트너 관계가 구성됩니다.

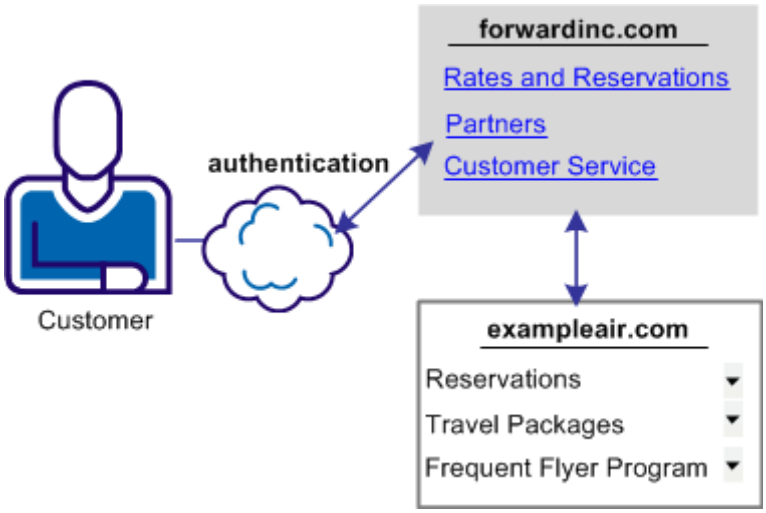
- discounts.com 이 로컬 RP 이고 smcompany.com 이 원격 IP 인 RP-IP 파트너 관계

사용 사례: 사용자 특성에 기반한 SAML 2.0 사용자 권한 부여

이 사용 사례에서 forwardinc.com 은 자동차 대여 업체이고 exampleair.com 은 여행사입니다.

forwardinc.com 의 고객은 forwardinc.com 에 로그인하여 인증을 받은 다음 차량 대여 견적을 받기 위해 링크를 클릭합니다. forwardinc.com 의 고객 프로필에는 exampleair.com 에 대한 고객의 항공 마일리지 점수가 포함되어 있습니다. 항공 마일리지 계정에 따라 forwardinc.com 에서 상태 수준이 결정됩니다. 상태 수준에 따라 고객이 차량 대여 시 받는 할인 혜택이 결정됩니다.

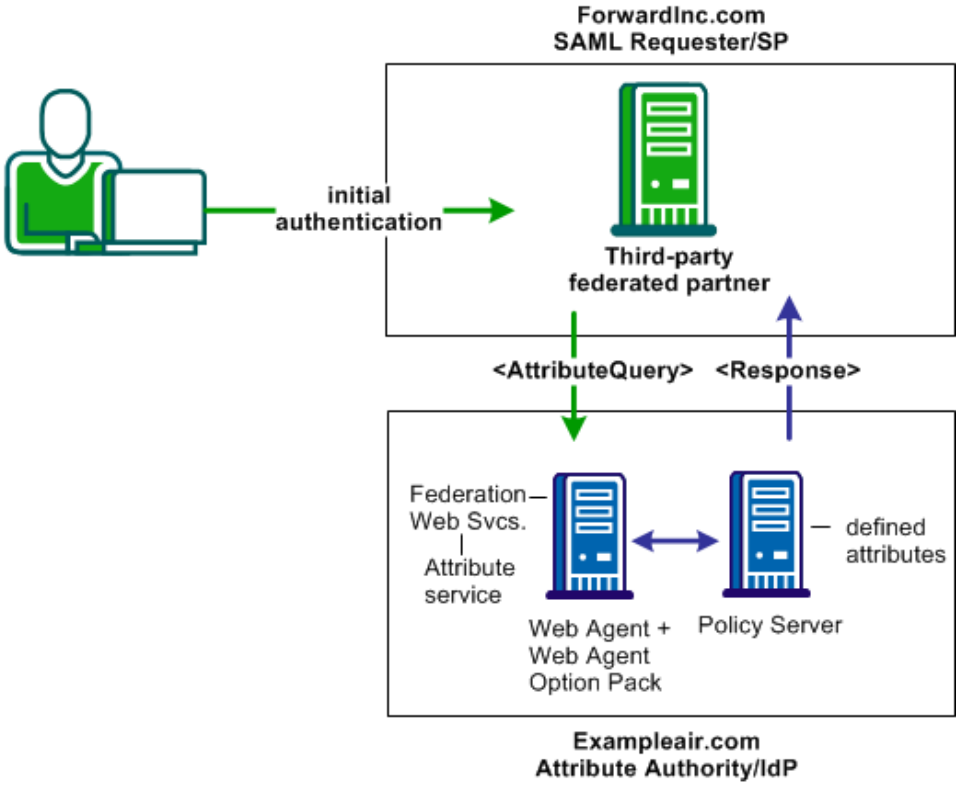
다음 그림에서는 이 사용 사례를 보여 줍니다.



forwardinc.com 은 고객에게 적절한 할인 정보를 표시하려고 합니다. 그러나 고객이 exampleair.com 에 먼저 로그인하고 인증한 다음 forwardinc.com 사이트에 다시 로그인하는 불편을 겪지 않게 하려고 합니다.

솔루션: 사용자 특성에 기반한 SAML 2.0 사용자 권한 부여

SAML 2.0 특성 쿼리/응답 프로필은 사용 사례: 사용자 특성에 기반한 SAML 2.0 사용자 권한 부여 (페이지 42)를 해결할 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.

이 배포에서

- SiteMinder 는 IdP/특성 기관인 Example.air 에만 배포됩니다. 한 시스템에는 웹 에이전트 옵션 팩이 있는 웹 에이전트가 설치되고 다른 시스템에는 정책 서버가 설치됩니다.

  참고: 특성 쿼리 프로필을 구현하려면 SiteMinder 가 IdP 의 역할을 해야 합니다. 즉, SiteMinder 는 특성 기관만 될 수 있으며 특성 쿼리에 응답만 할 수만 있습니다. SiteMinder 는 SP 로 기능할 수 없으며 특성 쿼리를 보낼 수 없습니다.

- forwardinc.com 은 특성 쿼리/응답 프로필을 사용하도록 구성된 타사 서비스 공급자입니다.

forwardinc.com 은 SAML 요청자로 작동합니다. 고객이 이 사이트에 로그인하는 경우 다음과 같은 순서로 이벤트가 발생합니다.

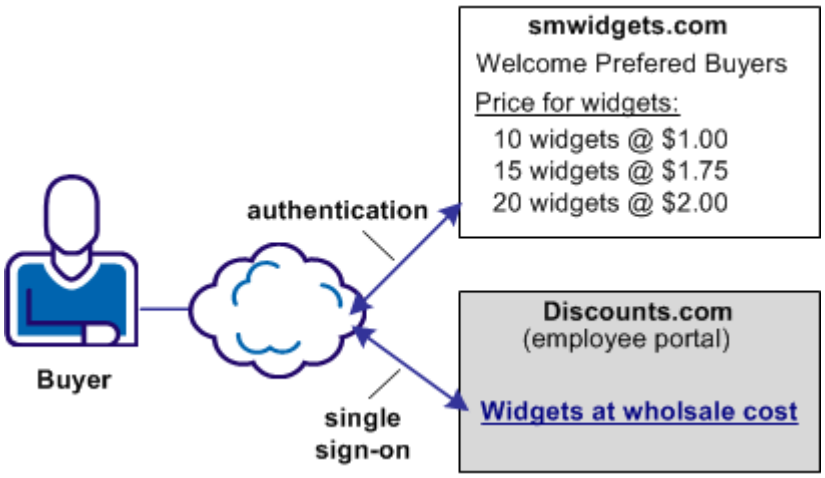
1. 사용자가 forwardinc.com 에 로그인하고 인증받습니다.
2. 사용자가 차량을 대여하기 위해 링크를 클릭합니다. forwardinc.com 이 확인되지 않은 항공 마일리지 특성을 식별합니다.
3. forwardinc.com 이 로컬 사용자 디렉터리에서 해당 사용자를 조회하여 특성을 확인하려 하지만 사용자 특성 변수를 확인할 수 없습니다.
4. forwardinc.com 이 IdP/특성 기관 exampleair.com 에 특성 쿼리를 SOAP 요청으로 보냅니다. 쿼리 요청에는 마일리지 특성이 포함됩니다.
5. exampleair.com 이 자체 사용자 디렉터리 레코드에서 사용자를 조회하고 항공 마일리지 특성을 확인합니다. exampleair.com 이 forwardinc.com 에 어설션을 SOAP 응답으로 반환합니다. 어설션에는 요청된 특성이 포함됩니다.
6. SAML 요청자가 특성을 확인하고 사용자에게 요청된 리소스에 대한 권한을 부여합니다.
7. 사용자가 대상 리소스로 리디렉션됩니다.

사용 사례: IdP 에 이름 ID 가 없는 싱글 사인온

이 사용 사례에서 discounts.com 은 smwidgets.com 에서 위젯을 구매합니다.

discounts.com 의 한 구매자가 smwidgets.com 의 최신 위젯 가격 목록에 액세스하기 위해 링크를 클릭합니다. 이 구매자는 smwidgets.com 웹 사이트에 연결되며 discounts.com 웹 사이트에 로그인할 필요 없이 가격 목록이 제공됩니다.

다음 그림에서는 이 사용 사례를 보여 줍니다.



discounts.com 에는 로컬로 저장된 구매자 아이덴티티가 없으므로 discounts.com 은 구매자에 대한 아이덴티티를 smwidgets.com 에서 얻으려고 합니다. discounts.com 이 인증 요청을 smwidgets.com 에 보냅니다. smwidgets.com 이 요청을 받지만 NameID 특성에 대한 값을 찾을 수 없습니다. smwidgets.com 은 구매자에 대한 고유한 영구 아이덴티티를 생성하고 이 아이덴티티를 어설션에 추가합니다. discounts.com 은 이 고유한 식별자를 사용하여 구매자가 요청된 리소스에 액세스할 수 있게 합니다.

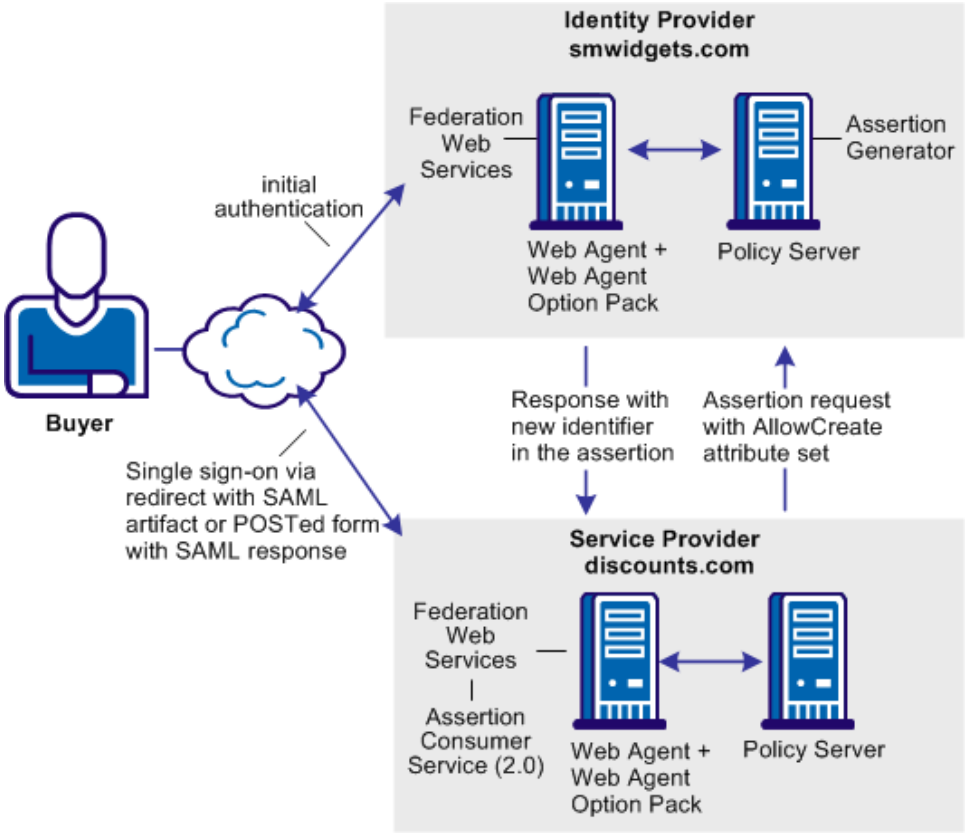
솔루션: IdP 에 이름 ID 가 없는 싱글 사인온

허용/만들기 특성을 사용하여 사용 사례: IdP 에 이름 ID 가 없는 싱글 사인온 (페이지 45)을 해결합니다.

참고: 이 솔루션에는 SAML 2.0 프로필이 필요합니다.

페더레이션은 discounts.com 과 smwidgets.com 에 배포됩니다. 한 시스템에는 웹 에이전트와 웹 에이전트 옵션 팩이 설치되고 다른 시스템에는 정책 서버가 설치됩니다.

다음 그림에서 smwidgets.com 은 아이덴티티 공급자이고 discounts.com 은 서비스 공급자입니다.



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.

아이덴티티 공급자의 사용자 아이덴티티 없이 두 사이트 간에 싱글 사인온을 사용하도록 설정하려면 다음과 같은 순서로 이벤트가 발생합니다.

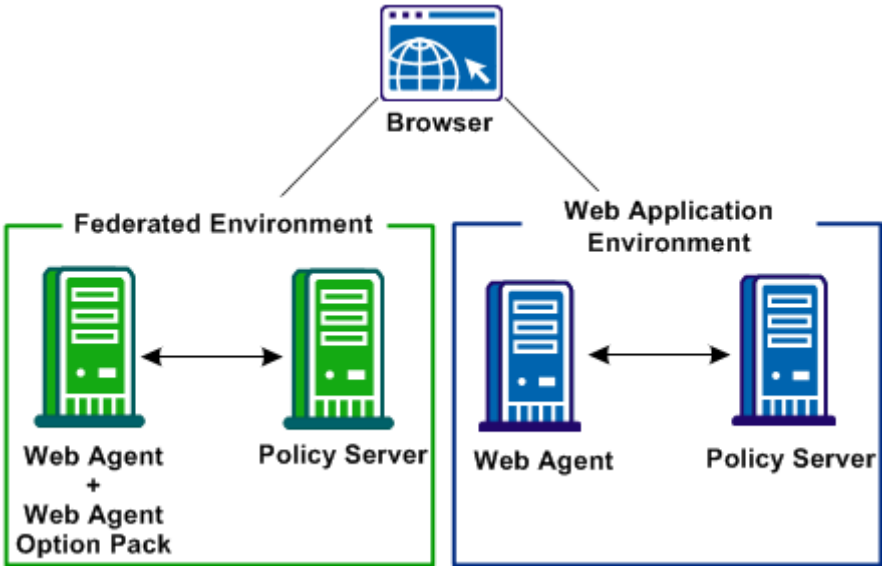
1. 이 사례에서는 구매자인 사용자가 discounts.com 에서 인증을 받습니다. 이 링크는 인증 요청을 시작합니다.
2. discounts.com 의 정책 서버가 구성에 "허용/만들기" 옵션이 있는지 확인합니다. 이 옵션은 discounts.com 의 SP-IdP 파트너 관계에서 사용되도록 설정됩니다.

3. 인증 요청에 AllowCreate 라는 특성이 포함됩니다. 로컬 웹 에이전트의 페더레이션 웹 서비스 응용 프로그램이 인증 요청을 smwidgets.com 으로 리디렉션합니다.
4. smwidgets.com 의 정책 서버가 어설션을 생성합니다. 어설션 생성 중에 정책 서버는 리소스를 요청하는 사용자의 사용자 레코드에서 NameID 특성을 검색합니다. 사용자 레코드에 NameID 값이 없습니다.
5. 정책 서버가 구성에 AllowCreate 옵션이 있는지 확인합니다. 또한 정책 서버는 검색된 AllowCreate 특성에 대한 인증 요청도 확인합니다.
6. 정책 서버가 인증 요청과 자체 구성에 AllowCreate 특성이 있기 때문에 고유한 영구 식별자를 생성합니다. 정책 서버는 이 식별자를 사용자 저장소에 저장합니다.
7. 정책 서버는 discounts.com 의 페더레이션 웹 서비스 응용 프로그램에 어설션을 반환합니다. 페더레이션 웹 서비스 응용 프로그램은 어설션 응답을 수록한 자동 게시 양식을 discounts.com 의 어설션 소비자 서비스로 보냅니다.
8. discounts.com 의 서비스 공급자가 응답 메시지를 사용하여 정책 서버에 로그인하면서 응답을 자격 증명으로 사용합니다.
9. 정책 서버가 사용자 저장소에서 NameID 를 검색하여 응답의 유효성을 검사합니다. 정책 서버가 사용자를 찾아 로그인합니다.
10. 웹 에이전트가 discounts.com 도메인에 대한 SMSESSION 쿠키를 생성합니다.
11. 웹 에이전트가 쿠키를 브라우저에 넣고 사용자를 대상으로 리디렉션합니다.

사용 사례: 보안 영역을 사용하는 SSO

이 사용 사례에서 CompanyA 는 페더레이션되지 않은 웹 응용 프로그램을 보호하고 페더레이션된 싱글 사인온을 지원합니다. SiteMinder 배포에서는 웹 응용 프로그램 환경에서 페더레이션 환경으로 이동하는 단일 사용자에 대해 두 개의 세션이 있을 수 없습니다. 사용자가 각 환경 간에 이동할 때 세션 쿠키가 서로 덮어씁니다.

다음 그림에서는 페더레이션 환경과 웹 응용 프로그램 환경이 결합된 사이트를 보여 줍니다.

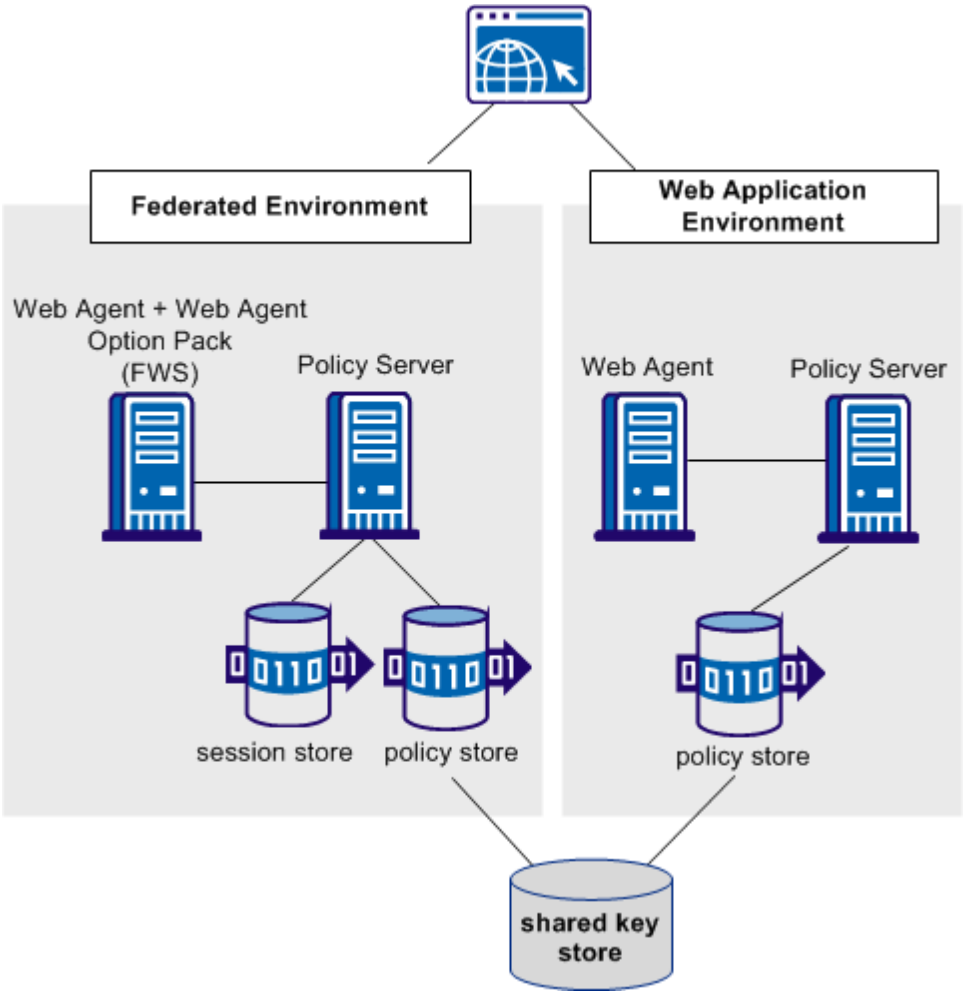


솔루션: 보안 영역을 사용하는 SSO

이 솔루션에서는 보안 영역에서 병렬 웹 응용 프로그램 및 페더레이션 환경을 설정하여 사용 사례: 보안 영역을 사용하는 SSO (페이지 48)를 해결하는 방법을 설명합니다.

보안 영역은 응용 프로그램 분할에 사용되는 단일 쿠키 도메인의 한 세그먼트입니다. 각 영역마다 다른 보안 요구 사항을 할당할 수 있습니다. 보안 영역을 사용하면 정책 서버가 각 환경의 단일 사용자별로 다른 세션 쿠키를 생성할 수 있습니다. 고유한 이름의 세션 쿠키 2 개가 생성되더라도 각 쿠키는 웹 응용 프로그램 및 페더레이션 환경 전체에서 동일한 한 세션을 나타냅니다. 어설션 당사자 측의 웹 에이전트가 보안 영역을 적용합니다.

다음 그림에서는 단일 어설션 당사자 측에서 두 가지 서로 다른 환경을 사용하는 배포를 보여 줍니다. 한 환경은 페더레이션 기능에 사용되고 다른 환경은 웹 응용 프로그램 보호에 사용됩니다.



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.

위 그림에는 다음 설정이 반영되어 있습니다.

웹 응용 프로그램 환경

에이전트 구성 개체 또는 로컬 구성 파일

DefaultAgent

트러스트된 보안 영역

SM(기본 영역)

영역에 대해 웹 에이전트가 읽는 쿠키

DefaultAgent 구성을 사용하면 웹 에이전트가 기본 세션 쿠키(SMSESSION) 읽기/쓰기를 수행할 수 있습니다.

페더레이션 환경

에이전트 구성 개체 또는 로컬 구성 파일

웹 에이전트가 사용하는

트러스트된 보안 영역

- 페더레이션(기본 영역)
- SM

영역에 대해 웹 에이전트가 읽는 쿠키

FedWA 구성을 통해 웹 에이전트는 SMSESSION 쿠키를 읽고 쓸 수 있습니다.

참고: 이 솔루션이 작동하려면 각 환경에 자체 에이전트 구성 개체가 있어야 합니다.

다음과 같은 순서로 이벤트가 발생합니다.

1. 사용자가 페더레이션 환경에 로그인합니다.
2. 페더레이션 환경의 웹 에이전트가 인증 URL 에 요청을 전달하여 사용자 세션을 설정합니다.

   사용자는 웹 응용 프로그램 환경의 이전 인증에서 얻은 SMSESSION 쿠키를 이미 가지고 있습니다.

3. 페더레이션 환경의 웹 에이전트가 SMSESSION 쿠키를 읽습니다. 정책 서버가 새 페더레이션 세션 쿠키를 생성하고 웹 에이전트가 이 새 세션 쿠키를 브라우저에 씁니다. 새 페더레이션 세션 쿠키는 SMSESSION 쿠키에 기반합니다.

   페더레이션에는 세션 저장소에 저장되는 영구 세션이 필요합니다. 웹 응용 프로그램 환경에서 읽은 SMSESSION 쿠키는 영구적이지 않습니다. 정책 서버가 페더레이션 쿠키를 생성하는 경우 쿠키를 수정하고 세션을 영구 세션으로 업그레이드합니다.

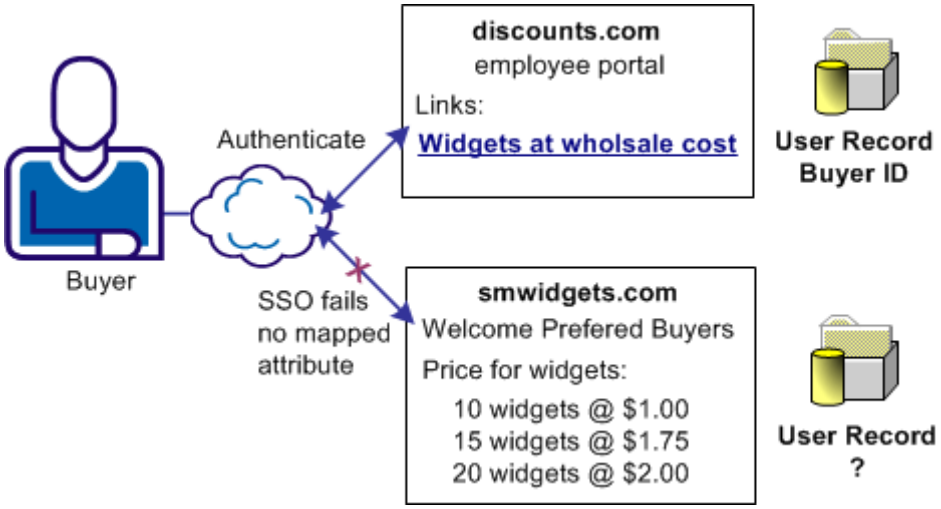
4. 페더레이션 환경의 FWS 응용 프로그램은 페더레이션 쿠키를 읽고 리소스 요청을 성공적으로 처리합니다.

사용 사례: SP 에서 동적 계정 연결을 사용하는 SSO

이 사용 사례에서 IdP 인 discounts.com 은 특정 사용자를 식별하는 구매자 ID 라는 특성을 포함합니다. 구매자 ID 값이 어설션에 NameID 로 입력됩니다. 하지만 구매자 ID 에 대해 매핑된 아이덴티티가 smwidgets.com 에 없습니다. 구매자를 인증하고 보호된 리소스에 대한 액세스 권한을 구매자에게 부여할 수 있도록 Smwidgets.com 은 적합한 사용자 레코드에 특성을 생성해야 합니다.

smwidgets.com 의 관리자는 동적 계정 연결을 사용하여 매핑을 설정합니다. 매핑을 통해 smwidgets 는 구매자를 인증하고 리소스에 대한 액세스 권한을 허용할 수 있습니다. discounts.com 의 구매자가 smwidgets.com 에서 위젯의 최신 정가표에 액세스하는 링크를 선택하면 구매자는 다시 인증하지 않고도 로그인됩니다.

다음 그림에서는 이 사용 사례를 보여 줍니다.



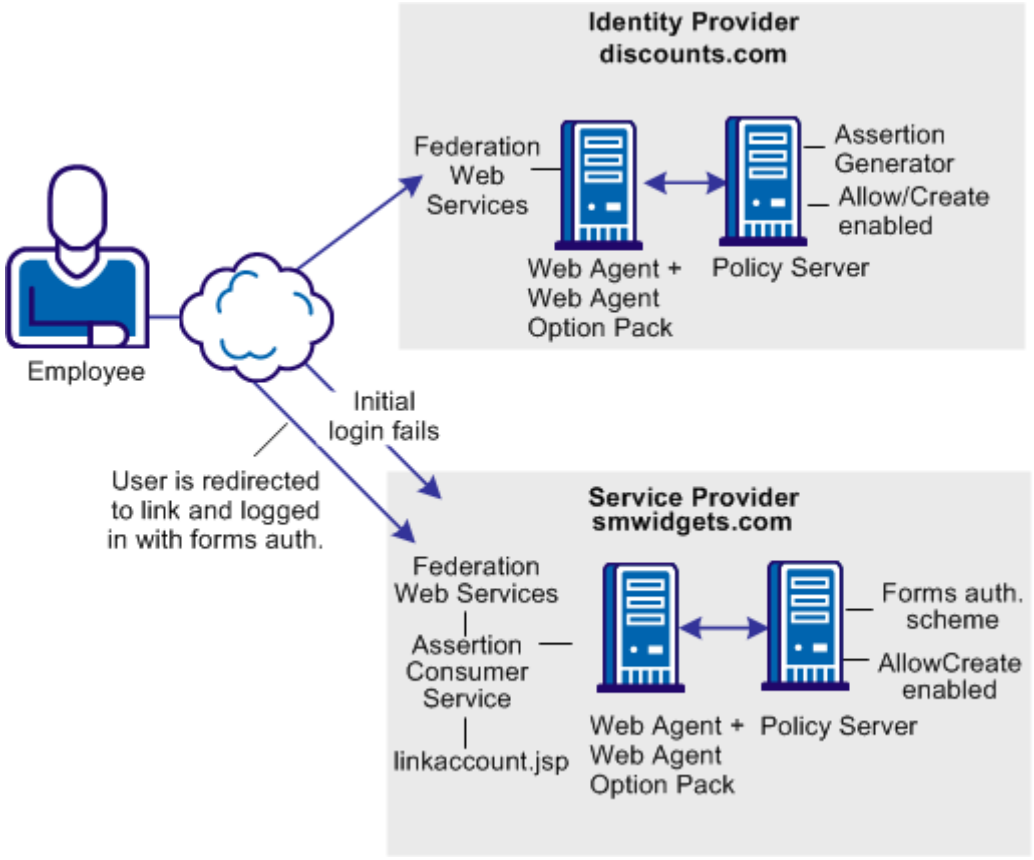
솔루션: SP 에서 동적 계정 연결을 사용하는 SSO

페더레이션을 IdPA.com 및 SPB.com 에 배포하여 사용 사례: SP 에서 동적 계정 연결을 사용하는 SSO (페이지 52)를 해결할 수 있습니다.

참고: 동적 계정 연결은 SAML 2.0 에서만 지원됩니다.

SiteMinder 는 두 사이트 모두에 배포됩니다. 각 사이트의 한 시스템에는 웹 에이전트와 웹 에이전트 옵션 팩이 설치되고 다른 시스템에는 정책 서버가 설치됩니다.

다음 그림에서는 서비스 공급자에서 동적 계정 연결을 사용하는 싱글 사인온을 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.

다음과 같은 순서로 이벤트가 발생합니다.

1. 직원이 처음에 discounts.com 에 로그인하여 인증을 받습니다. discounts.com 이 직원에 대한 어설션을 생성합니다. discounts.com 이 어설션을 포스트하거나(POST 바인딩), 아티팩트와 함께 사용자를 smwidgets.com 의 어설션 소비자 서비스로 리디렉션합니다(아티팩트 바인딩). 이 어설션에는 buyerID 라는 특성이 포함되어 있습니다.
2. smwidgets.com 의 어설션 소비자 서비스는 사용자를 인증하려 시도하지만 buyerID 특성은 로컬 사용자 레코드에 매핑되지 않습니다. 인증이 실패합니다.

3. smwidgets.com 에서 파트너 관계 구성의 일부로, *web_agent_home*/affwebservices/linkaccount.jsp 디렉터리를 가리키는 리디렉션 URL 이 정의됩니다. 직원이 이 URL 로 리디렉션됩니다.

   참고: linkaccount.jsp 파일은 보호된 영역의 일부여야 합니다. 이 파일의 기본 위치는 http://*sp_home*/affwebservices/public/입니다. 이 위치에서 보호된 영역으로 파일을 복사하십시오.

4. 양식 인증 체계를 사용하여 로컬 사용자를 인증하는 웹 에이전트가 이 linkaccount.jsp URL 을 보호합니다. 인증이 성공한 후 smwidgets.com 에 세션이 설정되고 SMSESSION 쿠키가 직원의 브라우저에 포함됩니다.

5. linkacount.jsp 가 브라우저에 로드되고 서비스 공급자 계정에 연결하라는 메시지가 사용자에게 표시됩니다. 단추를 클릭하여 계정 연결을 허용합니다.

6. 사용자가 어설션 소비자 서비스로 리디렉션되면 직원의 브라우저가 SMSESSION 쿠키에 어설션을 제공합니다.

7. 어설션 소비자 서비스가 어설션에서 NameID 를 추출하고 새로 생성된 buyerID 특성에 NameID 값을 삽입합니다. buyerID 특성은 직원의 기존 사용자 레코드에 있습니다. SMSESSION 쿠키에 있는 UserDN 이 사용자를 식별하기 때문에 어설션 소비자 서비스는 매핑할 사용자 레코드를 알고 있습니다.

   SAML 2.0 파트너 관계에 구성된 검색 사양은 NameID 에 매핑되는 특성을 나타냅니다. 이 경우 검색 사양은 buyerID=%s 입니다.

8. 특성이 매핑되면 어설션을 기반으로 사용자가 인증됩니다. 새 사용자 세션이 설정됩니다.

   다음에 동일한 사용자가 어설션에 구매자 ID 를 제공하면 사용자가 요청된 리소스에 성공적으로 액세스할 수 있습니다.

SP 에서 동적 계정 연결 구성

서비스 공급자 측에서 다음 구성 요소를 구성하여 동적 계정 연결이 사용되도록 설정하십시오.

참고: 동적 계정 연결은 SAML 2.0 에서만 지원됩니다.

- AllowCreate 기능

  기존 사용자 저장소에 특성을 생성할 수 있습니다.

- 리디렉션 URL

  인증 실패 시 사용자를 linkaccount.jsp 파일에 보냅니다. 인증 체계를 통해 리디렉션 URL 이 보호됩니다. 체계는 사용자에게 로그인하여 세션을 생성하도록 요청합니다.

- 웹 에이전트의 POST 보존

  서비스 공급자 웹 에이전트에서 사용하도록 설정해야 합니다.

- 검색 사양

  어설션에 있는 NameID 로 대체되는 특성을 나타냅니다.

서비스 공급자 측에서 SAML 2.0 POST 또는 아티팩트 싱글 사인온에 대해 동적 계정 연결이 사용되도록 설정

다음 단계를 수행하십시오.

1. linkaccount.jsp 파일의 경우 다음을 수행합니다.
   - (선택 사항) 실패한 인증 시도 후 사용자가 리디렉션될 때 사용자 지정 사용자 환경을 제공하도록 linkaccount.jsp 파일을 사용자 지정합니다. 이 파일에서 **accountlinking** 및 **samlresponse** 매개변수를 어설션 소비자 서비스 URL 에 다시 포스트해야 합니다.

     참고: accountlinking 을 yes(accountlinking=yes)로 설정해야 합니다.

     이 파일의 기본 위치는 http://*sp_home*/affwebservices/public/입니다.

- POST 보존을 지원하는 SiteMinder 양식 인증 체계를 사용하여 linkaccount.jsp 파일을 보호합니다. 사용자가 서비스 공급자에 로컬로 로그인한 후 어설션을 포함하는 SAML 응답이 어설션 소비자 서비스에 포스트됩니다. 전체 로컬 인증 프로세스가 진행되는 동안 SAML 응답의 POST 데이터를 보존합니다.

  인증 체계를 사용하여 리소스를 보호하려면 *정책 서버 구성 안내서*에서 인증 체계에 대한 정보를 참조하십시오.

2. 서비스 공급자에서 "허용/만들기" 기능이 사용되도록 설정합니다.
3. 서비스 공급자에 있는 웹 에이전트의 경우 "POST 보존" 매개 변수를 yes 로 설정합니다. 이 설정을 사용하면 SAML 응답의 POST 데이터를 보존할 수 있습니다.
4. 인증이 실패한 경우 사용자를 linkaccount.jsp 파일에 보내는 리디렉션 URL 을 구성합니다. 사용자를 이 파일에만 연결합니다.

   리디렉션 URL 은 서비스 공급자에 설정되는 SAML 2.0 인증 체계의 일부입니다.

   표시된 값을 사용하여 다음 필드에 데이터를 입력합니다.

   Redirect URL for the User Not Found status(사용자를 찾을 수 없음 상태에 대한 리디렉션 URL)

   http://*sp_home*/*protected_realm*/linkaccount.jsp

   예: http://smwidgets.com/partner_resources/linkaccount.jsp

   linkaccount.jsp 파일의 기본 위치는 http://*sp_home*/affwebservices/public/입니다. 이 디렉터리에서 보호된 영역으로 구성된 디렉터리로 파일을 복사합니다.

   모드

   HTTP POST

5. SAML 인증 체계에 대한 검색 사양을 구성합니다. 예를 들어 어설션의 이름 ID 가 buyerID 를 대체하는 경우 검색 사양은 buyerID=%s 입니다.

제 3 장: 페더레이션 배포 고려 사항

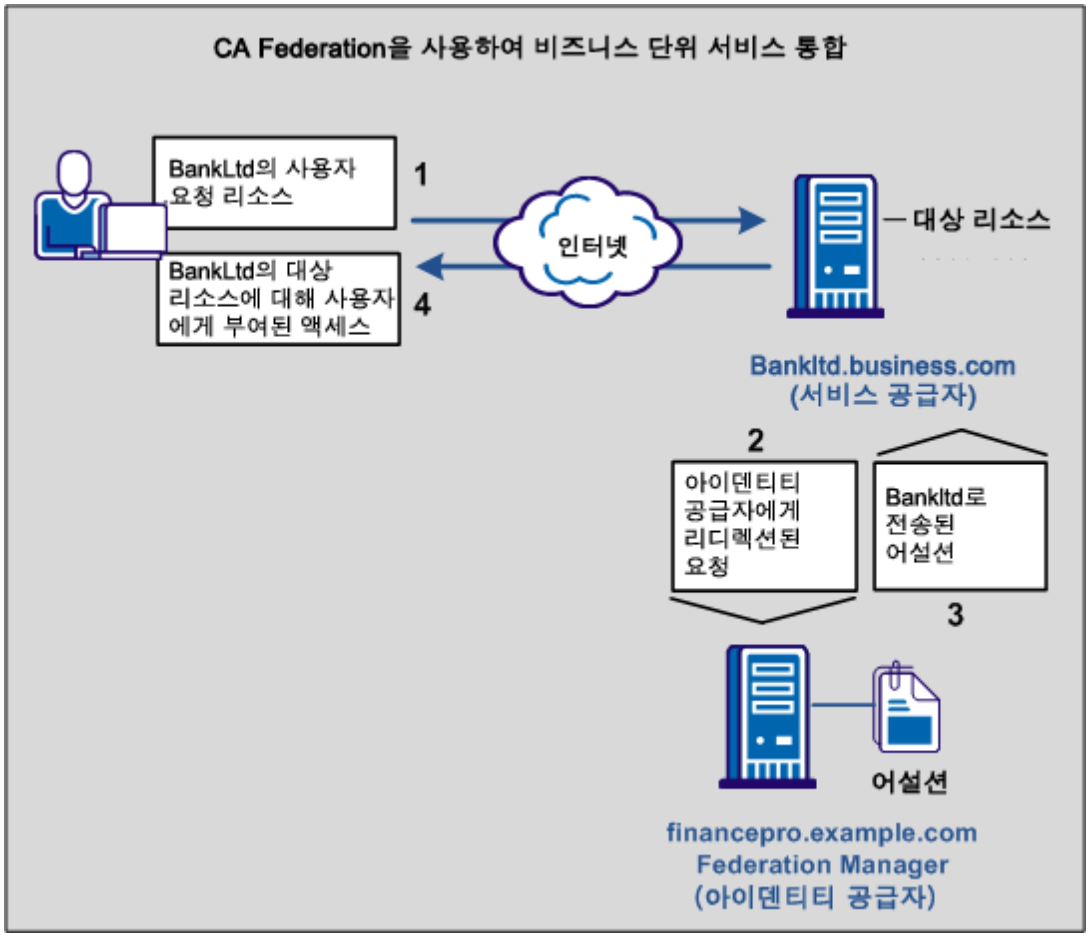
페더레이션 비즈니스 사례

샘플 비즈니스 사례에서는 CA SiteMinder?Federation 로 일반 비즈니스 문제를 해결할 수 있는 방법을 가장 잘 보여 줍니다.

이 비즈니스 사례에서 Financepro 는 최근에 고객에게 프라이빗 뱅킹 서비스를 제공하기 위해 BankLtd 라는 금융 회사를 인수한 재무 계획 회사입니다. 이 두 회사는 서로 다른 정보 인프라를 보유하고 있지만 고객에게 한 회사처럼 보이고자 합니다. 이 문제를 해결하기 위해 두 회사는 페더레이션된 파트너 관계를 설정했습니다.

페더레이션된 파트너 관계를 설정함으로써 두 회사는 싱글 사인온을 사용하여 원활한 고객 환경을 제공할 수 있습니다. 고객은 지속적인 인증 챌린지 없이 Financepro 와 BankLtd 간에 이동할 수 있습니다. 또한 고객 ID 와 고객 정보가 공유되므로 사용자 환경을 추가로 사용자 지정하고 각 파트너의 재무 상품을 상호 홍보할 수 있습니다.

다음 그림에서는 Financepro 와 BankLtd 간의 페더레이션된 파트너 관계를 보여 줍니다. 통신 흐름은 SAML 2.0 서비스 공급자에서 시작되는 싱글 사인온을 기반으로 합니다.



그림에서는 다음과 같은 정보 흐름을 설명합니다.

1. 사용자가 BankLtd 에서 페더레이션된 리소스에 액세스하려고 합니다.
2. 사용자가 인증을 위해 Financepro 로 리디렉션되고 어설션이 생성됩니다.
3. 어설션이 BankLtd 로 다시 전달됩니다.
4. SAML HTTP-아티팩트 또는 HTTP-POST 에 기반한 싱글 사인온이 발생합니다. 사용자가 대상 리소스에 대한 액세스 권한을 얻습니다.

이 파트너 관계가 올바로 작동하도록 하려면 페더레이션을 사용하여 관계를 구현하기 전에 파트너 관계의 작동 방식을 결정하십시오.

고려해야 할 문제는 다음과 같습니다.

- 파트너 관계에서 사용자를 식별하는 방법
- 어설션에서 전송되는 특성 및 전송 목적
- 사용할 페더레이션 바인딩(SAML POST, 아티팩트 또는 WS-페더레이션)

결정한 사항은 비즈니스 파트너 관계를 구성하는 데 도움이 됩니다.

파트너 관계에서의 사용자 식별

비즈니스 파트너는 해당 사용자 저장소에서 자체적인 방법으로 사용자 아이덴티티를 정의합니다. 사용자를 식별하는 방법에 따라 파트너 간에 사용자를 매핑할 수 있는 방법이 결정됩니다.

다음 시나리오를 고려하십시오.

- 사용자 ID 가 각 사이트의 사용자 저장소에서 동일합니다.

  계정 연결이 사용자 식별 방법입니다.

- 사용자 ID 가 각 사이트의 사용자 저장소에서 고유합니다.

  아이덴티티 매핑이 사용자 식별 방법입니다. FinancePro 에서는 고객이 JohnDoe 로 식별되고 BankLtd 에서는 해당 고객이 DoeJ 로 식별됩니다. 파트너가 아이덴티티 매핑에 사용할 사용자 특성 프로필에 동의해야 합니다.

- 사용자 ID 가 신뢰 당사자에 존재하지 않습니다.

  계정 프로비저닝이 사용자 식별 방법입니다. 계정을 프로비저닝하는 경우 사용자에 대한 계정을 생성하거나 단순히 SAML 어설션에 포함된 정보로 기존 사용자 계정을 채워야 할 수 있습니다.

결정한 사용자 식별 방법에 따라 어설션에 포함된 사용자 아이덴티티로 전송되는 정보가 결정됩니다.

사용자 매핑

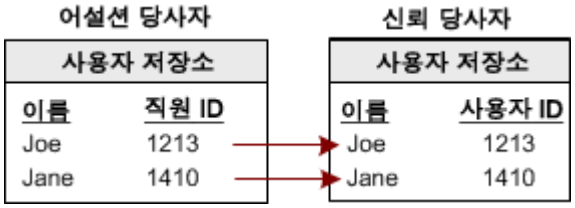
사용자 매핑은 한 회사에 있는 사용자 아이덴티티와 다른 회사에 있는 사용자 아이덴티티 간의 관계를 설정하는 기능입니다. 어설션 당사자의 원격 사용자를 신뢰 당사자의 로컬 사용자에 매핑하십시오.

매핑 유형은 다음과 같습니다.

- 일대일 매핑은 생산하는 기관의 고유한 원격 사용자 디렉터리 항목을 소비하는 기관의 고유한 사용자 항목에 매핑합니다.

  일대일 매핑 또는 계정 연결은 어설션 당사자의 계정을 신뢰 당사자의 계정에 연결합니다.

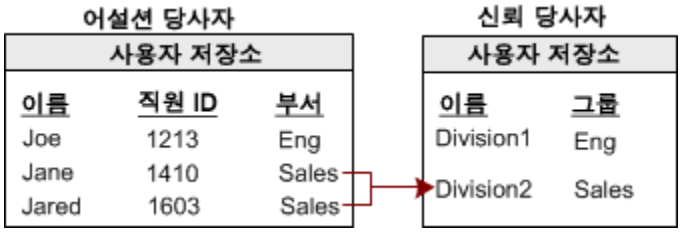
  다음 그림에서는 일대일 매핑을 보여 줍니다.



- N 대일 매핑은 원격 사용자 디렉터리 항목 그룹을 단일 로컬 프로필 항목에 매핑합니다.

  N 대일 매핑을 통해 생산하는 기관의 사용자 레코드 여러 개를 소비하는 기관의 사용자 레코드 또는 프로필 하나에 매핑할 수 있습니다. 신뢰 당사자의 관리자가 원격 사용자 그룹에 대해 N 대일 매핑을 사용하면 각 원격 사용자의 기록을 유지 관리할 필요가 없습니다.

  다음 그림에서는 N 대일 매핑을 보여 줍니다.



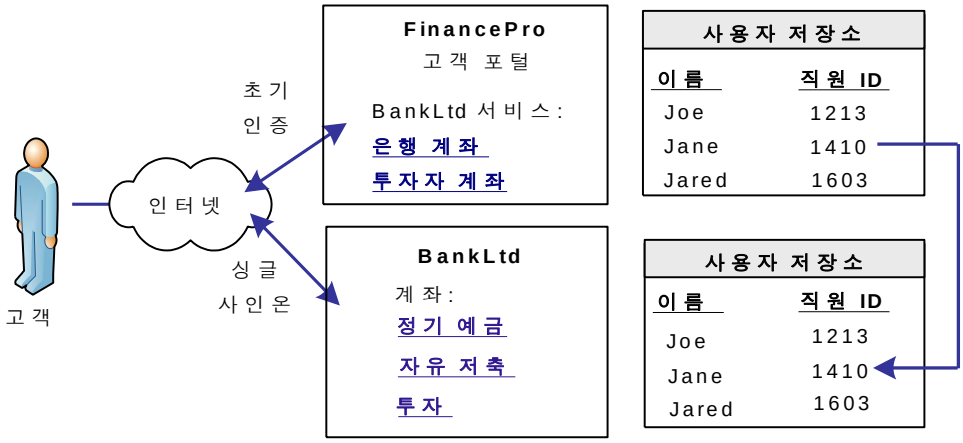
레거시 페더레이션의 경우 사용자 매핑은 페더레이션 인증 체계의 일부로 구성됩니다. 파트너 관계 페더레이션의 경우 사용자 매핑은 이름 ID 및 특성 설정의 일부로 구성됩니다.

페더레이션된 아이덴티티를 설정하기 위한 계정 연결

FinancePro 의 고객이 BankLtd 의 리소스에 액세스하면 NameID 가 어설션에 항상 포함됩니다. 이 식별자를 통해 BankLtd 는 고객을 확인하고 해당 고객에 대해 허용할 액세스 수준을 결정할 수 있습니다.

NameID 는 각 파트너의 사용자 저장소가 동일한 ID 를 사용하여 동일한 방식으로 사용자를 식별할 때 페더레이션된 아이덴티티를 설정할 수 있습니다.

다음 그림에서는 동일한 직원 ID 가 있는 각 사이트의 사용자 저장소를 보여 줍니다.



CA SiteMinder?Federation 을 통해 파트너 관계 구성 프로세스의 일부로 계정 연결을 구성할 수 있습니다. NameID 형식과 이름 ID 유형을 지정합니다. 그러면 이름 ID 유형에 따라 이름을 정의하는 값의 유형이 결정됩니다. 특정 이름 ID 유형을 사용자 디렉터리의 정적, 사용자 또는 DN 특성과 연결합니다. CA SiteMinder?Federation 이 어설션에 포함하는 NameID 는 정의하는 구성을 따릅니다.

신뢰 당사자가 어설션을 받으면 BankLtd 에서 사용자 명확성 프로세스가 발생합니다. 이 프로세스를 통해 어설션의 NameID 값이 해당 사용자 저장소의 기록에 연결됩니다.

페더레이션된 아이덴티티를 설정하기 위한 ID 매핑

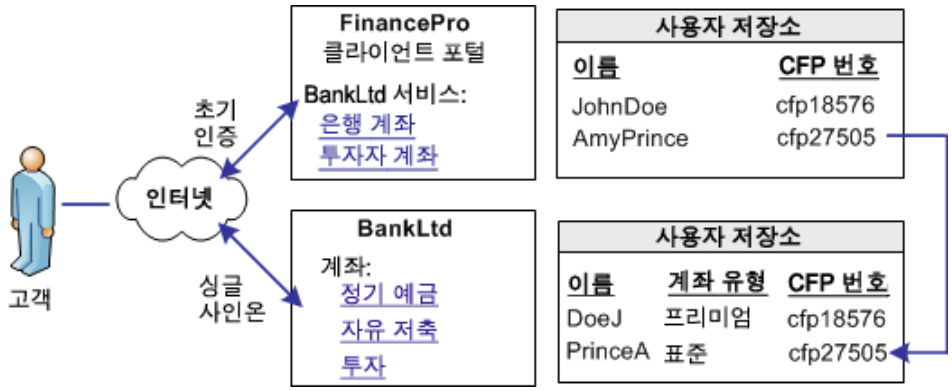
Financepro 에 있는 투자자가 인증을 받은 다음 BankLtd 의 정보에 액세스하기 위해 링크를 선택합니다. 이 투자자는 사인온할 필요 없이 BankLtd 웹 사이트의 계정 영역에 직접 연결됩니다.

BankLtd 가 Financepro 의 모든 고객에 대한 사용자 아이덴티티를 유지 관리하지만 이 아이덴티티는 FinancePro 의 아이덴티티와 다릅니다. 예를 들어 FinancePro 에서는 JohnDoe 가 고객입니다. BankLtd 에서는 해당 고객이 DoeJ 로 식별됩니다. 그럼에도 불구하고 BankLtd 는 회사 웹 사이트의 중요한 부분에 대한 액세스를 제어해야 합니다. 페더레이션된 아이덴티티를 설정하기 위해 파트너가 둘 중 어느 사이트에서나 단일 고객의 해당 아이덴티티에 매핑되는 특성에 동의합니다.

파트너가 대역 외 정보 교환 중에 사용할 특성에 동의합니다. 즉, 이 동의는 채널을 통한 메시지 통신의 일부가 아닙니다. 이 예에서 파트너가 동의하는 특성은 인증된 재무 계획자 라이선스 번호(각 사용자 저장소에서 CFPNum 이라고 함)입니다.

고객이 BankLtd 에서 페더레이션된 리소스에 액세스하려고 하면 요청이 싱글 사인온 프로세스를 트리거합니다. FinancePro 에 생성되는 어설션에는 CFPNum 특성이 포함됩니다. BankLtd 가 어설션을 받으면 해당 사이트에 있는 응용 프로그램이 사용자 명확성 프로세스를 수행해야 합니다. 이 프로세스는 특성을 사용하여 요청에 사용되는 프로필 아이덴티티를 결정합니다.

다음 그림에서는 동일한 사용자가 각 파트너에서 다르게 식별되는 방법을 보여 줍니다.



SiteMinder Federation 을 통해 파트너 관계 구성 프로세스의 일부로 아이덴티티 매핑을 구성할 수 있습니다. NameID 및 특성 구성의 경우 CFPID 라는 특성을 정의합니다. 이 특성을 사용자 특성 CFPNum, 즉 각 파트너의 사용자 저장소에 있는 특성의 이름과 연결하십시오.

SiteMinder Federation 이 특성을 어설션에 포함합니다. BankLtd 가 어설션을 받으면 사용자 명확성 프로세스가 어설션에 포함된 특성을 해당 사용자 저장소의 적절한 기록에 연결합니다.

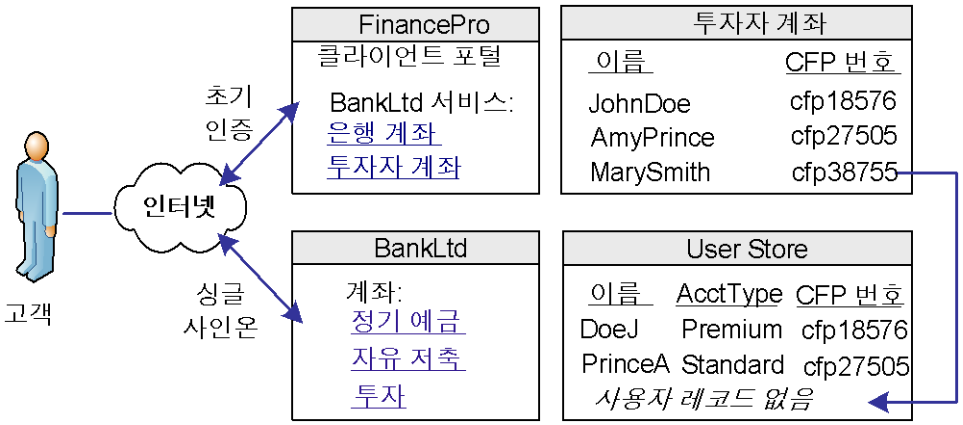
페더레이션된 아이덴티티를 설정하기 위한 사용자 프로비저닝(파트너 관계 페더레이션만 해당)

파트너 관계 페더레이션은 신뢰 당사자의 프로비저닝 응용 프로그램과 함께 작동하여 아이덴티티를 설정할 수 있습니다.

Financepro 에 있는 고객인 Mary Smith 가 인증을 받은 다음 BankLtd 의 정보에 액세스하기 위해 링크를 클릭합니다. 처음에는 BankLtd 가 Mary Smith 의 사용자 계정을 찾을 수 없습니다. BankLtd 는 새 고객을 허용하면서 해당 웹 사이트의 중요한 부분을 보호하고자 합니다.

BankLtd 가 Mary Smith 의 새 페더레이션된 아이덴티티를 설정하기 위한 프로비저닝을 구현하도록 페더레이션을 구성했습니다. SiteMinder 가 Mary Smith 를 BankLtd 의 프로비저닝 서버로 리디렉션합니다. 그러면 프로비저닝 응용 프로그램이 페더레이션된 아이덴티티 정보를 사용하여 사용자 저장소에 사용자 계정을 생성합니다.

다음 그림에서는 FinancePro 와 BankLtd 의 사용자 저장소를 보여 줍니다.



페더레이션을 통해 신뢰 당사자에 있는 파트너 관계 구성의 일부로 프로비저닝을 구성할 수 있습니다. 이 예에서 원격 프로비저닝을 선택하고 어설션 데이터를 BankLtd 프로비저닝 서버에 전달하는 방법을 결정합니다. 이 구성을 사용하면 사용자 저장소에 사용자 항목을 동적으로 생성할 수 있습니다.

응용 프로그램을 사용자 지정하기 위한 특성

CA SiteMinder?Federation 에서는 다음 두 가지 방법으로 특성을 사용하여 대상 응용 프로그램을 사용자 지정할 수 있습니다.

어설션 당사자 측에서 어설션에 특성 추가

응용 프로그램을 사용자 지정하려는 목적으로 사용자 저장소 기록의 특성을 어설션에 포함하여 사용자를 식별할 수 있습니다.

서블릿, 웹 응용 프로그램 및 기타 사용자 지정 응용 프로그램이 특성을 사용하여 사용자 지정된 콘텐츠를 표시하거나 다른 사용자 지정 기능을 사용하거나 사용하지 않도록 설정할 수 있습니다. 웹 응용 프로그램과 함께 사용되는 경우 특성은 대상 사이트의 사용자 활동을 제한하여 세부적인 액세스 제어를 구현할 수 있습니다. 예를 들어 Account Balance 라는 특성 변수를 보내고 BankLtd 에 있는 사용자의 유보 계정 잔액을 반영하도록 설정합니다.

특성은 이름/값 쌍의 형식을 사용합니다. 어설션을 받는 경우 신뢰 당사자는 특성 값을 응용 프로그램에 제공합니다.

신뢰 당사자 측에서 특성 매핑

신뢰 당사자는 대상 응용 프로그램에 전달되고 있는 응용 프로그램 특성 집합에 매핑할 수 있는 어설션 특성 집합을 받습니다.

예를 들어 FinancePro 에는 어설션 특성 CellNo=5555555555 가 포함되어 있습니다. BankLtd 에서 이 특성 이름은 응용 프로그램 특성 Mobile=5555555555 로 변환됩니다. 특성 이름은 변환되지만 값은 동일하게 유지됩니다.

여러 어설션 특성을 단일 응용 프로그램 특성으로 변환할 수도 있습니다. 예를 들어 FinancePro 는 Acct=Savings 및 Type=Retirement 특성이 포함되어 있고 BankLtd 에서 FundType= Retirement Savings 로 변환되는 수신 어설션을 보냅니다.

싱글 사인온에 대한 페더레이션 프로필

각 파트너가 지원하는 바인딩에 따라 파트너 관계에 SAML 을 사용할지 아니면 WS-페더레이션을 사용할지가 결정됩니다.

새 페더레이션의 경우 어느 파트너에 대해서도 필요한 레거시 요구 사항이 없습니다. 따라서 싱글 사인온에 사용하도록 권장되는 SAML 프로필은 SAML 2.0 POST 프로필입니다. SAML 2.0 POST 프로필은 어설션 데이터를 안전하게 전송하며 SAML 아티팩트 프로필에 비해 구성 프로세스가 간단합니다. 하지만 두 파트너의 동의에 SAML 아티팩트가 필요한 경우 이 바인딩도 구현할 수 있습니다.

ADFS(Active Directory Federation Services)를 사용하는 배포의 경우 WS-페더레이션을 구성하십시오.

각 CA SiteMinder® Federation 모델로 페더레이션

레거시 페더레이션 또는 파트너 관계 페더레이션 모델을 통해 Financepro 와 BankLtd 간의 페더레이션된 파트너 관계를 설정할 수 있습니다. 페더레이션을 사용하면 마치 한 회사인 것처럼 각 회사 간에 사용자가 이동합니다.

파트너 관계 페더레이션 모델

파트너 관계 마법사의 안내에 따라 관리 UI 에서 파트너 관계 모델을 구성하십시오. 파트너 관계 개체는 파트너 관계 생성과 싱글 사인온을 수행하기 위한 파트너 관계의 각 파트너 식별에 중점을 둡니다.

파트너 관계 마법사의 단계에는 다음이 포함됩니다.

1. 파트너 관계 구성

   파트너 관계를 명명하고 파트너 관계를 구성하는 엔터티 두 개를 식별합니다.

2. 페더레이션 사용자/사용자 ID 설정

   어설션 당사자가 생성하는 어설션/토큰과 신뢰 당사자가 수행하는 인증의 대상이 되는 사용자를 식별합니다.

3. 이름 ID 및 특성

   페더레이션된 아이덴티티를 설정하는 방법을 결정합니다. 어설션의 콘텐츠를 식별 및 사용자 지정하기 위한 특성을 추가할 수 있습니다.

   NameID 및 특성을 사용하면 적절한 정보가 신뢰 당사자의 응용 프로그램에 제공되도록 할 수 있습니다. NameID 및 특성 단계는 계정 연결과 아이덴티티 매핑을 구성하는 단계이기도 합니다.

4. SSO 및 SLO 또는 사인아웃

   신뢰 당사자 측에서 어설션을 소비하는 서비스 위치를 포함하여 싱글 사인온 바인딩을 정의합니다. SAML 2.0 의 경우 SLO(싱글 로그아웃), 인증 컨텍스트, ECP(향상된 클라이언트 또는 프록시) 프로필, 아이덴티티 공급자 검색 프로필 등의 추가 기능을 구성할 수 있습니다. WS-페더레이션의 경우 사인아웃을 구성할 수 있습니다.

5. AuthnContext(SAML 2.0 에만 해당)

   서비스 공급자가 신뢰 수준을 설정하기 위해 인증 프로세스에 대한 정보를 가져올 수 있도록 합니다. 또한 이 기능을 사용하면 아이덴티티 공급자가 인증 컨텍스트를 어설션에 포함할 수 있습니다.

6. 서명 및 암호화

   다음을 포함하여 데이터를 안전하게 교환하기 위한 서명 및 암호화 옵션을 정의합니다.

   - 어설션
   - 인증 요청
   - SAML 2.0 싱글 로그아웃 요청 및 응답
   - WS-페더레이션 사인아웃 응답

7. 응용 프로그램 통합

   대상 응용 프로그램으로의 리디렉션을 구성할 수 있으며 사용자 레코드 프로비저닝을 설정하고 신뢰 당사자 측 특성 매핑을 정의할 수 있습니다. 실패한 사용자 인증에 대한 리디렉션을 설정할 수도 있습니다.

레거시 페더레이션 모델

레거시 페더레이션 모델은 도메인, 영역, 규칙, 인증 체계 및 정책 개체에 중점을 둡니다.

SiteMinder 가 어설션 당사자인 경우 구성 단계는 다음과 같습니다.

1. 가맹 도메인의 엔터티 구성

   어설션 당사자가 생성하는 어설션의 대상이 되는 파트너를 명명합니다.

2. 페더레이션 사용자 설정

   어설션 당사자가 생성하는 어설션과 신뢰 당사자가 수행하는 인증의 대상이 되는 사용자 디렉터리를 지정합니다.

3. 트랜잭션에 대한 프로필(SAML 또는 WS-페더레이션) 선택

   페더레이션된 아이덴티티가 설정되는 방식을 결정합니다. 프로필 구성에서는 어설션의 콘텐츠를 식별 및 사용자 지정하기 위한 특성을 추가합니다.

   NameID 및 특성을 사용하면 적절한 정보가 신뢰 당사자의 응용 프로그램에 제공되도록 할 수 있습니다. 프로필 구성은 계정 연결과 아이덴티티 매핑을 지정하는 단계이기도 합니다.

   프로필의 일부로 싱글 사인온을 구성하십시오. SAML 2.0 의 경우 SLO(싱글 로그아웃), ECP(향상된 클라이언트 또는 프록시) 프로필, 아이덴티티 공급자 검색 프로필 등의 추가 기능을 구성할 수 있습니다. WS-페더레이션의 경우 사인아웃을 구성할 수 있습니다.

4. 서명 처리 및 암호화(SAML 2.0)

   어설션, 인증 요청, 싱글 로그아웃 요청 및 응답을 안전하게 교환하기 위한 서명 옵션을 정의합니다.

SiteMinder 가 신뢰 당사자인 경우 구성 단계는 다음과 같습니다.

1. SAML 및 WS-페더레이션 인증 체계 설정

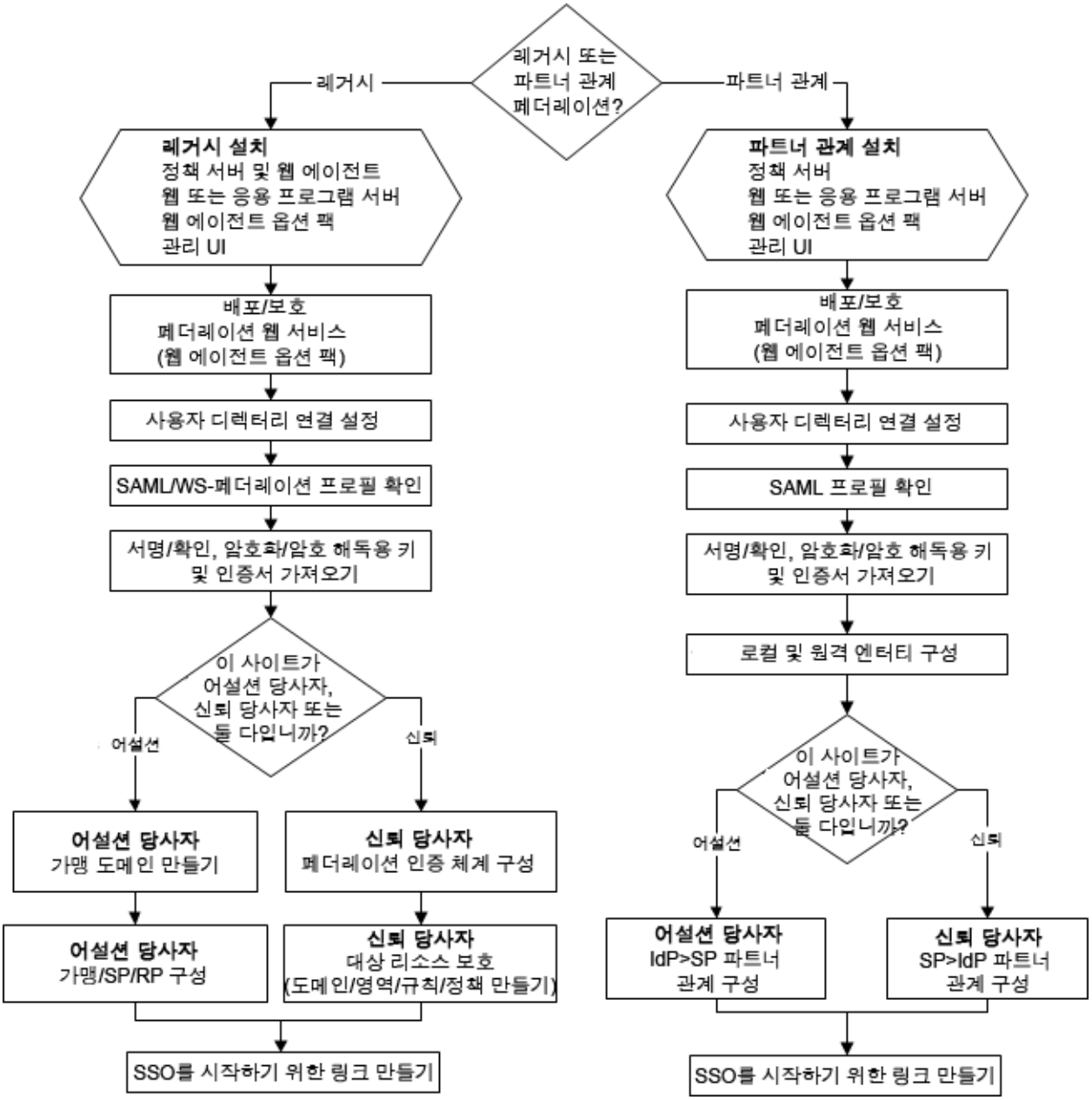
   대상 응용 프로그램으로의 리디렉션을 구성할 수 있으며 사용자 레코드 프로비저닝을 설정하고 신뢰 당사자 측 특성 매핑을 정의할 수 있습니다.

2. 인증 체계에 포함된 싱글 사인온, 싱글 로그아웃, 사인아웃, 암호화, 암호 해독 등의 페더레이션 관련 설정 구성

페더레이션 순서도

페더레이션된 파트너 관계를 올바르게 설정하기 위한 구성 요소를 구성하십시오. 이러한 구성 요소는 대부분 관리 UI 를 사용하여 구성할 수 있습니다.

다음 순서도는 레거시 페더레이션 및 파트너 관계 페더레이션의 일반적인 프로세스를 보여 줍니다.



필수 구성 요소 및 구성 절차에 대한 자세한 내용은 다음 안내서를 참조하십시오.

파트너 관계 페더레이션

파트너 관계 페더레이션 안내서

파트너 관계 페더레이션은 페더레이션의 파트너 관계 모델을 말합니다.

레거시 페더레이션

레거시 페더레이션 안내서

레거시 페더레이션은 Federation Security Services 라는 제품을 말합니다.

제 4 장: 싱글 사인온에 사용되는 페더레이션과 웹 액세스 관리 비교

페더레이션과 웹 액세스 관리의 이점

페더레이션과 WAM(웹 액세스 관리)은 싱글 사인온에 사용되는 경우 서로 다른 이점을 제공합니다. 페더레이션 또는 WAM 싱글 사인온 사용 시기는 사용 중인 배포에 따라 결정됩니다.

페더레이션을 사용하면 WAM 기능을 확장할 수 있지만 해당 기능이 대체되는 것은 아닙니다.

페더레이션의 이점은 다음과 같습니다.

- SAP, SharePoint, WebLogic 등의 많은 응용 프로그램이 기본 제공된 상태 그대로 즉시 페더레이션을 처리할 수 있습니다. 이러한 응용 프로그램은 어설션을 수락합니다.
- 중앙 서버에 대한 직접 연결이 필요하지 않습니다. 생성된 어설션을 얻기 위해 페더레이션 요청이 항상 어설션 당사자를 거칩니다. 사용자가 한 서버의 콘텐츠에 대한 액세스 권한을 얻은 후 페더레이션 허브로 돌아가서 다음 서버로 리디렉션됩니다. 사용자 세션이 허브에서 시간 만료되는 경우에만 사용자가 인증을 다시 받으면 됩니다.
- SiteMinder Federation 모델은 두 가지가 있습니다. 파트너 관계 페더레이션은 비즈니스 중심이며 파트너와의 관계를 중요시합니다. 레거시 페더레이션은 프로토콜 중심이며 프로토콜 사양에 따라 더 구체적으로 사용자 지정할 수 있습니다.

이러한 이점 덕분에 페더레이션된 파트너 관계는 원격 사이트, 액세스할 수 없는 사이트 또는 타사의 제어를 받는 사이트가 있는 환경에 적합합니다.

SiteMinder WAM 싱글 사인온의 이점은 다음과 같습니다.

- 브라우저 리디렉션이 더 적으므로 트랜잭션이 더 빠릅니다.
- SiteMinder 가 중앙 집중식 권한 부여 및 감사를 제공합니다.
- 사용자가 어설션 생성을 위해 중앙 허브를 거치지 않고 한 웹 서버에서 네트워크의 다른 웹 서버로 직접 연결되는 링크가 존재할 수 있습니다.

- SiteMinder 가 시간 만료 관리를 제공합니다.
- 응용 프로그램이 원격으로 시작되는 트랜잭션에 독립적입니다.

이러한 이점 덕분에 WAM 싱글 사인온은 내부 데이터 센터와 같이 해당 회사의 제어를 받는 사이트가 있는 환경에 적합합니다.

페더레이션이 유리한 배포

페더레이션은 해당 회사가 서버를 제어하지 않는 네트워크에 유리합니다. 예를 들면 웹 서버를 소유한 타사가 서버에 웹 에이전트를 설치하도록 허용하지 않는 경우입니다. 원격 서버가 웹 에이전트와 정책 서버 간의 네트워크 대기 시간이 긴 위치에 있는 경우에도 마찬가지입니다. 해당 회사가 대상 서버를 제어하지 않으면 SAML 어설션이 아이덴티티 정보를 전달하기에 이상적인 방법입니다.

페더레이션된 네트워크에 있는 파트너는 통신에 사용되는 프로토콜에 대해 특정 표준을 따릅니다. 일반 표준을 사용하면 어설션 생성과 소비가 보편화됩니다. 결과적으로 어설션 또는 신뢰 당사자에 있는 공급업체는 중요하지도 않고 각 공급업체의 원격 위치도 아닙니다.

마지막으로 페더레이션은 시간 만료가 주요 관심 사항이 아닐 때 사용하기 좋은 솔루션인데, 이 경우 목표는 아이덴티티 정보를 획득하는 것입니다. 외부 권한 부여 검사는 페더레이션의 주안점이 아닙니다.

웹 액세스 관리가 유리한 배포

WAM 싱글 사인온은 해당 회사가 각 웹 사이트를 제어하는 환경에 가장 적합합니다. 웹 사이트나 다른 내부 싱글 사인온 환경과 동일한 데이터 센터에 SiteMinder 를 두는 배포는 웹 액세스 관리를 사용하기에 좋습니다. 각 웹 사이트에 대한 제어는 네트워크 성능을 감사하고 시간 만료 문제를 모니터링할 때도 중요합니다.

WAM 세션을 통해 WAM 싱글 사인온과 응용 프로그램을 통합할 수 있습니다. 또한 WAM 을 구현하면 페더레이션에 내재된 성능 문제가 다소 줄어듭니다. 예를 들어 어설션 당사자 측에서 시작되는 트랜잭션의 경우 사용자가 요청하기 위해 링크를 선택한 후 여러 리디렉션이 필요할 수 있습니다.

제 5 장: 페더레이션 웹 서비스

페더레이션 웹 서비스 개요

FWS(페더레이션 웹 서비스) 응용 프로그램은 정책 서버에 대한 연결이 있는 서버에 웹 에이전트 옵션 팩과 함께 설치됩니다. 페더레이션 웹 서비스와 웹 에이전트는 다음과 같은 웹 브라우저 싱글 사인온 프로필을 지원합니다. 이러한 프로필은 표준 브라우저를 통해 사이트 간에 정보를 전달합니다.

지원되는 프로필은 다음과 같습니다.

- SAML 아티팩트 프로필 1.0(레거시 페더레이션만 해당)
- SAML 아티팩트 프로필 1.1 및 2.0(레거시 페더레이션 및 파트너 관계 페더레이션)
- SAML POST 프로필 1.x 및 2.0(레거시 페더레이션 및 파트너 관계 페더레이션)
- WS-페더레이션 피동 요청자 프로필(레거시 페더레이션 및 파트너 관계 페더레이션)

SAML 1.x 아티팩트 및 POST 프로필

SAML 1.x 아티팩트 및 POST 프로필의 경우 페더레이션 웹 서비스 응용 프로그램은 다음 서비스를 사용합니다.

어설션 검색 서비스(SAML 1.x 아티팩트만 해당)

생산자 측 구성 요소입니다. 이 서비스는 SiteMinder 세션 저장소에서 어설션을 검색하여 SAML 아티팩트에 해당하는 어설션에 대한 SAML 요청을 처리합니다. SAML 사양은 어설션 검색 요청 및 응답 동작을 정의합니다.

참고: SAML 아티팩트 프로필만 어설션 검색 서비스를 사용합니다.

SAML 자격 증명 수집기(SAML 1.x)

포함된 SAML 응답이 있는 HTTP 양식이나 SAML 아티팩트를 받고 해당 SAML 어설션을 확보하는 소비자 측 구성 요소입니다. 자격 증명 수집기는 사용자 브라우저에 SiteMinder 쿠키를 발급합니다.

사이트 간 전송 서비스(SAML 1.x)

SAML POST 프로필에 대한 생산자 측 구성 요소입니다. 사이트 간 전송 서비스는 생산자 사이트에서 소비자 사이트로 사용자를 전송합니다. SAML 아티팩트 프로필의 경우 웹 에이전트가 사이트 간 전송 서비스와 동일한 기능을 수행합니다.

SAML 2.0 아티팩트 및 POST 프로필

SAML 2.0 아티팩트 및 POST 프로필의 경우 페더레이션 웹 서비스 응용 프로그램은 다음 서비스를 사용합니다.

아티팩트 레졸루션 서비스(SAML 2.0 아티팩트만 해당)

HTTP-아티팩트 바인딩을 사용하는 SAML 2.0 인증에 해당하는 아이덴티티 공급자 측 서비스입니다. 이 서비스는 아이덴티티 공급자의 SiteMinder 세션 저장소에 저장된 어설션을 검색합니다.

참고: HTTP-아티팩트 바인딩만 아티팩트 레졸루션 서비스를 사용합니다.

어설션 소비자 서비스(SAML 2.0)

포함된 SAML 응답이 있는 HTTP 양식이나 SAML 아티팩트를 받고 해당 SAML 어설션을 확보하는 서비스 공급자 구성 요소입니다. 어설션 소비자 서비스는 브라우저에 SiteMinder 쿠키를 발급합니다.

참고: 어설션 소비자 서비스는 AssertionConsumerServiceIndex 값이 0 인 AuthnRequest 를 수락합니다. 이 설정에 대한 다른 값은 모두 거부됩니다.

AuthnRequest 서비스(SAML 2.0)

이 서비스는 SAML 2.0 용으로 배포됩니다. 서비스 공급자가 도메인 간 싱글 사인온을 위해 사용자를 인증할 <AuthnRequest> 메시지를 생성할 수 있습니다. 이 메시지에는 페더레이션 웹 서비스 응용 프로그램이 브라우저를 아이덴티티 공급자의 싱글 사인온 서비스로 리디렉션하는 데 사용되는 정보가 포함되어 있습니다. AuthnRequest 서비스는 POST 및 아티팩트 싱글 사인온에 사용됩니다.

싱글 사인온 서비스(SAML 2.0)

싱글 사인온 서비스를 사용하면 아이덴티티 공급자가 AuthnRequest 메시지를 처리할 수 있습니다. 또한 이 서비스는 서비스 공급자에게 전송되는 어설션을 생성하기 위해 어설션 생성기를 호출합니다.

싱글 로그아웃 서비스(SAML 2.0)

이 서비스는 아이덴티티 공급자나 서비스 공급자가 시작할 수 있는 싱글 로그아웃 기능의 처리를 구현합니다.

아이덴티티 공급자 검색 서비스(SAML 2.0)

SAML 2.0 아이덴티티 공급자 검색 프로필을 구현하고 일반 도메인 쿠키를 설정 및 검색합니다. IdP 는 프린서펄 인증 후 일반 도메인 쿠키를 설정하도록 요청합니다. SP 는 사용자가 사용하고 있는 아이덴티티 공급자를 검색하기 위해 일반 도메인 쿠키를 확보하도록 요청합니다.

WS-Federation 프로필

WS-페더레이션 프로필의 경우 페더레이션 웹 서비스 응용 프로그램은 다음 서비스를 사용합니다.

보안 토큰 소비자 서비스

보안 토큰을 받고 해당 SAML 어설션을 추출하는 리소스 파트너 구성 요소입니다. 보안 토큰 소비자 서비스는 브라우저에 쿠키를 발급합니다.

싱글 사인온 서비스

아이덴티티 공급자가 사인온 메시지를 처리하고 사용자 인증에 필요한 리소스 파트너 정보를 수집하는 데 사용됩니다. 또한 이 서비스는 리소스 파트너에게 전송되는 어설션을 생성하기 위해 어설션 생성기를 호출합니다.

사인아웃 서비스

사인아웃 서블릿을 통해 싱글 사인아웃 트랜잭션의 처리를 구현합니다. 아이덴티티 공급자나 리소스 파트너가 사인아웃을 시작할 수 있습니다.

제 6 장: 페더레이션된 트랜잭션 처리 흐름

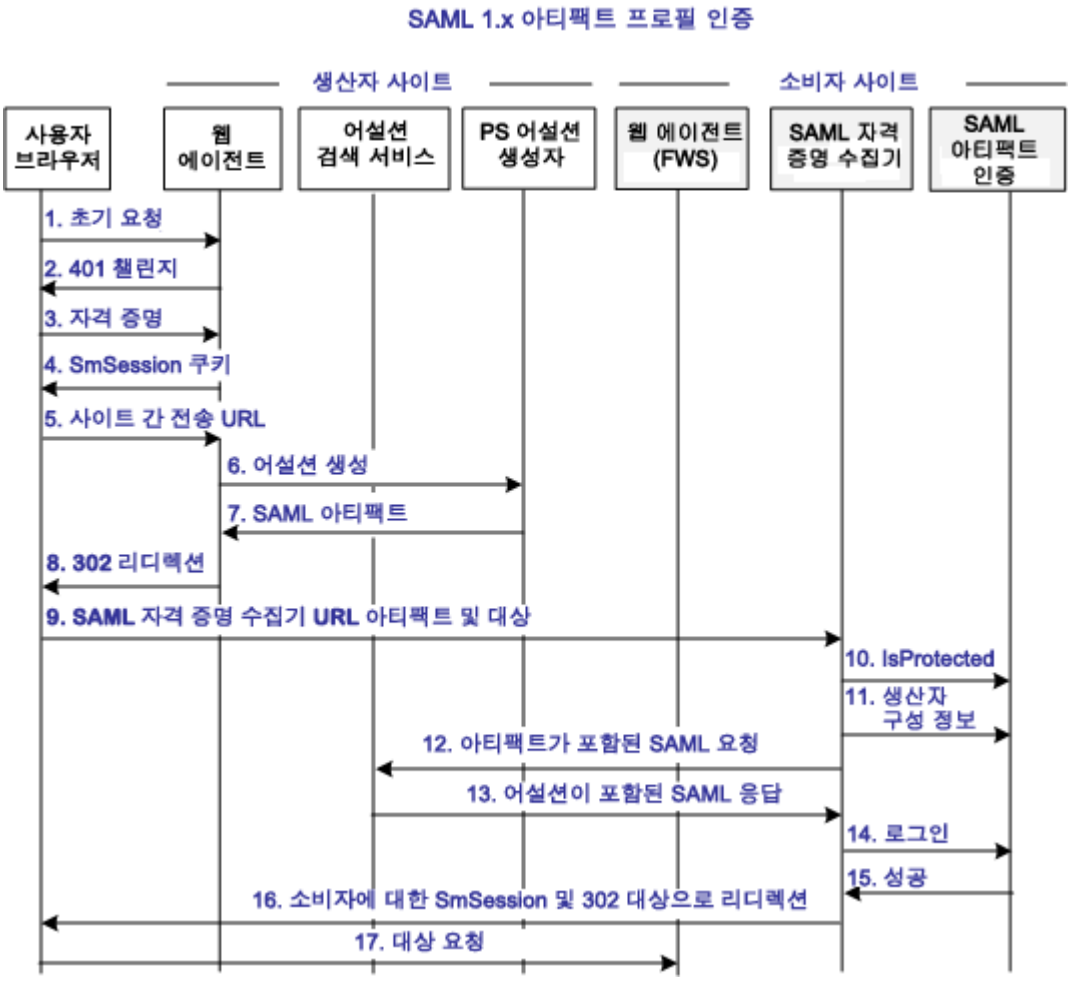
SAML 1.x 아티팩트 SSO 트랜잭션 흐름(생산자 시작)

다음 그림에서는 사용자와 생산자 및 소비자 사이트에 배포된 페더레이션 구성 요소 간의 흐름을 보여 줍니다. 이 흐름은 SAML 어설션을 처리하기 위한 방법으로서 SAML 1.x 아티팩트를 사용하는 사이트 간 싱글 사인온을 보여 줍니다.

흐름도에서는 다음과 같은 정보를 사용한다고 가정합니다.

- 생산자가 트랜잭션을 시작합니다.
- 각 사이트에서 인증 및 권한 부여가 성공했습니다.
- SiteMinder 는 생산자 및 소비자로만 표시되므로 각 파트너에서 프로세스를 볼 수 있습니다. SiteMinder 가 환경에서 생산자인 경우 표에서 생산자 활동을 검토하십시오. SiteMinder 가 소비자인 경우 표에서 소비자 활동을 검토하십시오.

다음 다이어그램은 SAML 1.x 아티팩트 SSO 트랜잭션 흐름을 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.

이벤트 순서는 다음과 같습니다.

작업자	트랜잭션 프로세스
사용자 에이전트(브라우저)	1. 사용자가 생산자 사이트의 보호된 페이지에 대한 초기 요청을 수행합니다.

작업자	트랜잭션 프로세스
생산자로서 SiteMinder	2. 생산자 사이트의 웹 에이전트가 401 챌린지를 사용하여 사용자에게 자격 증명에 대해 응답합니다.
	3. 사용자가 사용자 이름, 암호 등의 자격 증명을 웹 에이전트에 제출합니다.
	4. 웹 에이전트가 생산자 사이트 도메인에 대한 SMSESSION 쿠키를 발급하고 로컬 페이지에 대한 액세스를 허용합니다. **로그 메시지:** Session cookie does not exists, redirecting to authentication url(세션 쿠키가 없습니다. 인증 URL 로 리디렉션합니다). **검사점 코드:** [SSOSAML11_AUTHENTICATIONURL_REDIRECT]
	5. 사용자가 로컬 페이지에 있는 링크를 클릭하여 소비자 사이트를 방문합니다. 이 링크는 사이트 간 전송 URL 입니다. 사이트 간 전송 URL 이 생산자의 웹 에이전트에 요청합니다. 웹 에이전트는 IsProtected 호출을 정책 서버로 전달합니다. 이 URL 에는 SAML 자격 증명 수집기 위치와 소비자 사이트의 대상 URL 이 포함됩니다. **로그 메시지:** SAML11 Consumer Configuration is not in cache. Requesting to get from policy server(SAML11 소비자 구성이 캐시에 없습니다. 정책 서버에서 가져오도록 요청합니다). **검사점 코드:** [SSOSAML11_CONSUMERCONFFROMPS_REQ]
	6. 웹 에이전트는 정책 서버에게 어설션을 생성하도록 요청합니다. **로그 메시지:** Request to policy server for generating saml11 assertion/artifact based on selected profile(선택한 프로필에 기반하여 saml11 어설션/아티팩트를 생성하도록 정책 서버에 요청합니다). **검사점 코드:** [SSOSAML11_GENERATEASSERTIONORARTIFACT_REQ]

작업자	트랜잭션 프로세스
	7. 정책 서버가 어설션을 생성하여 세션 저장소에 넣고 어설션에 대한 SAML 아티팩트를 반환합니다. **로그 메시지:** Policy server generates the saml11 assertion(정책 서버가 saml11 어설션을 생성합니다). **검사점 코드:** [SSOSAML11_PSGENERATEASSERTION_RSP] **로그 메시지:** Policy server stores the assertion in session store(정책 서버가 세션 저장소에 어설션을 저장합니다). **검사점 코드**: [SSOSAML11_PSSTOREASSERTIONINSSTORE_REQ] **로그 메시지:** Policy server returns the wrappedassertion/artifact(based on profile selected) in response message(정책 서버가 응답 메시지에서 선택한 프로필을 기준으로 wrappedassertion/artifact 를 반환합니다). **검사점 코드:** [SSO_PSWRAPPEDASSERTION_RSP]
	8. 웹 에이전트가 302 리디렉션을 사용하여 소비자의 SAML 자격 증명 수집기에 응답합니다. 이 리디렉션에는 아티팩트와 대상 URL 이 쿼리 매개 변수로 포함됩니다. **로그 메시지:** Sending artifact to credential collector service url(아티팩트를 자격 증명 수집기 서비스 url 로 보냅니다). **검사점 코드:** [SSOSAML11_SENDARTIFACTTOCONSUMERURL_RSP]
사용자 에이전트(브라우저)	9. 브라우저가 URL 에 소비자 사이트의 SAML 자격 증명 수집기를 요청합니다.
소비자로서 SiteMinder	10. SAML 자격 증명 수집기는 생산자에 대한 정보를 얻기 위해 정책 서버로 isProtected 호출을 보냅니다. **로그 메시지:** IsProtected call to policy server for producer configuration(생산자 구성을 위해 정책 서버에 IsProtected 호출) **검사점 코드:** SSOSAML11_ISPROTECTEDCALLTOGETPRODUCERCONF_REQ
	11. 정책 서버가 생산자 구성 정보를 반환합니다.
	12. SAML 자격 증명 수집기가 생산자 구성을 사용하여 생산자의 어설션 검색 서비스에 대한 SAML 요청을 수행합니다. **로그 메시지:** Reading producer configuration from property(속성에서 구성을 읽고 있습니다). **검사점 코드:** SSOSAML11_GETPRODUCERCONFFROMPROPERTY_REQ **로그 메시지:** Backchannel call to resolve the artifact(아티팩트를 확인하기 위한 백 채널 호출) **검사점 코드:** [SSOSAML11_RESOLVEARTIFACT_REQ]

작업자	트랜잭션 프로세스
생산자로서 SiteMinder	13. 생산자의 어설션 검색 서비스가 세션 저장소에서 SAML 어설션을 검색합니다. 서비스가 SAML 어설션이 포함된 SAML 응답을 사용하여 응답합니다. 어설션이 소비자에게 전달됩니다. **로그 메시지:** Retrieving assertion from session store(세션 저장소에서 어설션을 가져오고 있습니다.) **검사점 코드:** [SSOSAML11_RETREIVEASSERTIIONFROMSSTORE_REQ] **로그 메시지:** Received the assertion from session store(세션 저장소에서 어설션을 가져왔습니다). **검사점 코드:** [SSOSAML11_RECEIVEDASSERTIONFROMSSTORE_RSP] **로그 메시지:** Sending assertion as artifact response(아티팩트 응답으로서 어설션을 보내고 있습니다). **검사점 코드:** SSOSAML11_SENDARTIFACTRESPONSE_RSP
소비자로서 SiteMinder	14. SAML 자격 증명 수집기는 SAML 어설션을 자격 증명으로서 전달하여 정책 서버로 로그인 호출을 보냅니다. **로그 메시지:** Obtained the SAML11 assertion as response from artifact resolve call(아티팩트 확인 호출에서 응답으로서 SAML11 어설션을 가져왔습니다). **검사점 코드:** [SSOSAML11_GOTARTIFACTRESPONSE_RSP] **로그 메시지:** Passing response message through login call(로그인 호출을 통해 응답 메시지를 전달하고 있습니다). **검사점 코드:** [SSO_RESPONSEMESSAGEINLOGIN_REQ]
	15. 소비자가 어설션의 유효성을 검사합니다. 사용자가 사용자 레코드에서 조회됩니다. 정책 서버가 성공 응답을 반환합니다. **로그 메시지:** Login successful(로그인 성공) **검사점 코드:** [SSO_LOGINSUCEESS_RSP] SAML 어설션이 유효하지 않거나 사용자 레코드를 찾을 수 없으면 실패 응답이 반환됩니다. **로그 메시지:** Login failure(로그인 실패) **검사점 코드:** [SSO_LOGINFAILURE_RSP]

작업자	트랜잭션 프로세스
소비자로서 SiteMinder (계속)	16. 체계가 성공 응답을 반환하는 경우 SAML 자격 증명 수집기가 소비자 도메인에 대한 SMSESSION 쿠키를 브라우저에 발급합니다. 또한 SAML 자격 증명 수집기가 대상 URL 에 302 리디렉션을 발급합니다. **로그 메시지:** Creating the smsession cookie for SP domain(SP 도메인에 대한 smsession 세션 쿠키를 만들고 있습니다). **검사점 코드:** [SSO_SMSESSIONFORSPDOMAIN_REQ] **로그 메시지:** Placing smsession in browser(브라우저에 smsession 을 저장하고 있습니다). **검사점 코드:** [SSO_PLACESMSSESSIONTOBROWSER_REQ] 체계가 실패 응답을 반환하는 경우 SAML 자격 증명 수집기가 액세스 권한 없음 URL 에 302 리디렉션을 발급합니다.
사용자 에이전트(브라우저)	17. 브라우저가 웹 에이전트로 보호되는 소비자의 대상 URL 에 요청합니다.

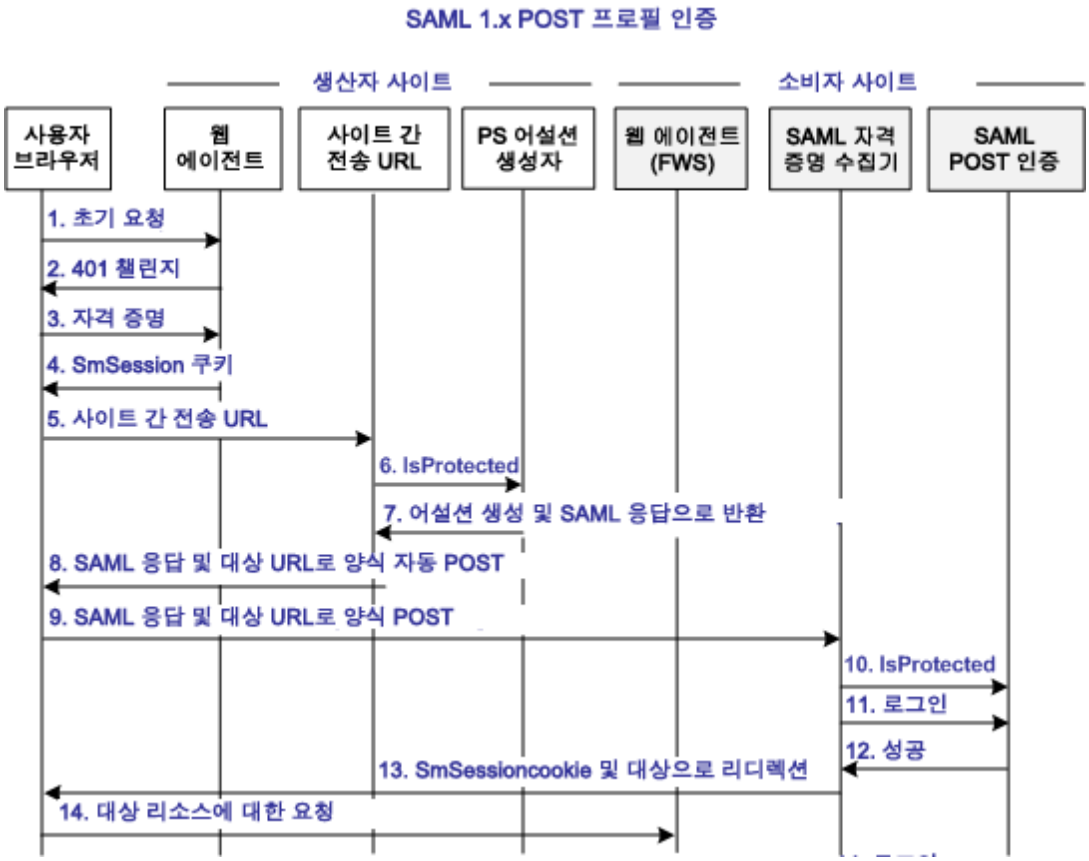
SAML 1.x POST SSO 트랜잭션 흐름(생산자 시작)

다음 그림에서는 사용자와 생산자 및 소비자 사이트에 배포된 페더레이션 구성 요소 간의 흐름을 보여 줍니다. 이 흐름은 SAML 어설션을 처리하기 위한 방법으로서 SAML 1.x 아티팩트를 사용하는 사이트 간 싱글 사인온을 보여 줍니다.

흐름도에서는 다음과 같은 정보를 사용한다고 가정합니다.

- 생산자가 트랜잭션을 시작합니다.
- 각 사이트에서 인증 및 권한 부여가 성공했습니다.
- SiteMinder 는 생산자 및 소비자로만 표시되므로 각 파트너에서 프로세스를 볼 수 있습니다. SiteMinder 가 환경에서 생산자인 경우 표에서 생산자 활동을 검토하십시오. SiteMinder 가 소비자인 경우 표에서 소비자 활동을 검토하십시오.

다음은 SAML 1.x POST 프로필에 대한 프로세스 흐름도입니다.



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.

이벤트 순서는 다음과 같습니다.

작업자	트랜잭션 프로세스
사용자 에이전트(브라우저)	1. 사용자가 생산자 사이트의 보호된 페이지에 대한 초기 요청을 수행합니다.

작업자	트랜잭션 프로세스
생산자로서 SiteMinder	2. 생산자 사이트의 웹 에이전트가 401 챌린지를 사용하여 사용자에게 자격 증명에 대해 응답합니다. **로그 메시지:** SMSESSION cookie does not exist, redirecting to Authentication URL(SMSESSION 쿠키가 없습니다. 인증 URL 로 리디렉션합니다). **검사점 코드:** [REDIRECT_AUTH_URL]
	3. 사용자가 사용자 이름, 암호 등의 자격 증명을 웹 에이전트에 제출합니다.
	4. 웹 에이전트가 생산자 사이트 도메인에 대한 SMSESSION 쿠키를 발급하고 로컬 페이지에 대한 액세스를 허용합니다.
	5. 사용자가 로컬 페이지에 있는 링크를 클릭하여 소비자 사이트를 방문합니다. 이 링크는 사용자를 다른 사이트로 전송하는 사이트 간 전송 URL 입니다. 사이트 간 전송 URL 이 생산자의 웹 에이전트에 요청합니다. 이 URL 은 소비자의 이름, SAML 자격 증명 수집기의 위치, 소비자 사이트의 대상 URL 에 대한 쿼리 매개 변수를 수록합니다. **로그 메시지:** SAML11 Consumer Configuration is not in cache. Requesting to get from policy server(SAML11 소비자 구성이 캐시에 없습니다. 정책 서버에서 가져오도록 요청합니다). **검사점 코드:** [SSOSAML11_CONSUMERCONFFROMPS_REQ]
	6. 사이트 간 전송 서비스가 정책 서버에 대한 IsProtected 호출을 수행하여 리소스를 요청합니다. 이 URL 에는 소비자를 고유하게 식별하는 이름 쿼리 매개 변수가 포함됩니다. **로그 메시지:** Request to policy server for generating saml11 assertion/artifact based on selected profile(선택한 프로필에 기반하여 saml11 어설션/아티팩트를 생성하도록 정책 서버에 요청합니다). **검사점 코드:** [SSOSAML11_GENERATEASSERTIONORARTIFACT_REQ]
	7. 정책 서버가 어설션을 생성하고 디지털로 서명된 SAML 응답에 포함된 상태로 반환합니다. 그런 다음 정책 서버가 응답을 사이트 간 전송 URL 에 반환합니다. **로그 메시지:** Policy server generates the saml11 assertion(정책 서버가 saml11 어설션을 생성합니다). **검사점 코드:** [SSOSAML11_PSGENERATEASSERTION_RSP]

작업자	트랜잭션 프로세스
	8. 사이트 간 전송 URL 서비스가 인코딩된 SAML 응답과 대상 URL 을 양식 변수로 포함하는 자동 POST 양식을 생성합니다. 서비스가 양식을 브라우저에 보냅니다. **로그 메시지:** Adding response in form for HTTP post(HTTP 포스트에 대한 형식으로 응답을 추가하고 있습니다). **검사점 코드:** [FWSBASE_POSTDATAFORM_ADD]
사용자 에이전트(브라우저)	9. 브라우저가 HTML 양식을 소비자 사이트의 SAML 자격 증명 수집기에 게시합니다. 이 URL 은 사이트 간 전송 URL 서비스가 보내는 SAML 응답에서 읽어옵니다.
소비자로서 SiteMinder	10. SAML 자격 증명 수집기는 정책 서버로 isProtected 호출을 보냅니다. **로그 메시지:** IsProtected call to policy server for producer configuration(생산자 구성을 위해 정책 서버에 IsProtected 호출) **검사점 코드:** SSOSAML11_ISPROTECTEDCALLTOGETPRODUCERCONF_REQ
	11. SAML 자격 증명 수집기는 어설션을 자격 증명으로서 전달하여, 요청된 대상 리소스에 대해 정책 서버로 로그인 호출을 보냅니다. **로그 메시지:** Reading the configuration to get the target url(대상 URL 을 가져오기 위해 구성을 읽고 있습니다). **검사점 코드:** [SSOSAML11_READTARGETURL_REQ]
	12. 로그인이 성공하면 SAML 자격 증명 수집기가 소비자 사이트 도메인에 대한 SMSESSION 쿠키를 생성합니다. **로그 메시지:** Login successful(로그인 성공) **검사점 코드:** [SSO_LOGINSUCEESS_RSP] **로그 메시지:** Creating the smsession cookie for SP domain(SP 도메인에 대한 smsession 세션 쿠키를 만들고 있습니다). **검사점 코드:** [SSO_SMSESSIONFORSPDOMAIN_REQ]
	13. SMSESSION 쿠키가 브라우저에 포함되고 사용자를 대상 리소스로 리디렉션합니다. **로그 메시지:** Placing smsession in browser(브라우저에 smsession 을 저장하고 있습니다). **검사점 코드:** [SSO_PLACESMSSESSIONTOBROWSER_REQ]
	14. 브라우저가 소비자 쪽 웹 에이전트에 의해 보호되는 대상 리소스를 요청합니다. 브라우저에 소비자 도메인에 대한 SMSESSION 쿠키가 있으므로 웹 에이전트가 사용자에게 인증을 요청하지 않습니다.

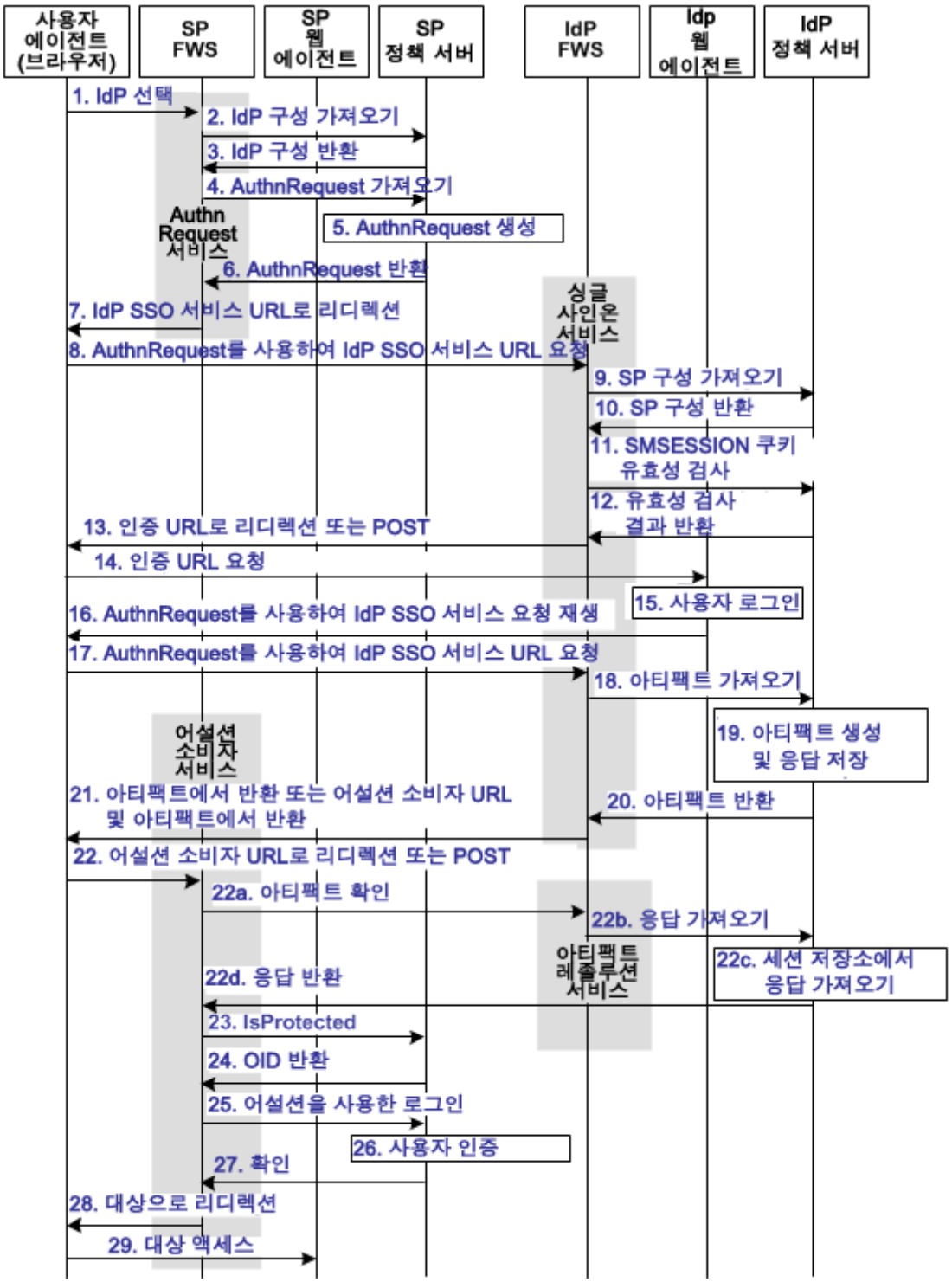
SAML 2.0 아티팩트 SSO 트랜잭션 흐름(SP 시작)

다음 그림에서는 사용자와 아이덴티티 공급자 및 서비스 공급자에 배포된 구성 요소 간의 상세 흐름을 보여 줍니다. 이 흐름은 SAML 어설션을 처리하기 위한 방법으로서 SAML 2.0 아티팩트를 사용하는 사이트 간 싱글 사인온을 보여 줍니다.

흐름도에서는 다음과 같은 정보를 사용한다고 가정합니다.

- SP 가 리소스에 대한 요청을 시작합니다.
- IdP 와 SP 사이트에서 인증 및 권한 부여가 성공했습니다.
- SiteMinder 는 IdP 및 SP 로 표시되므로 각 파트너에서 프로세스를 볼 수 있습니다. SiteMinder 가 환경에서 SP 인 경우 표에서 SP 활동을 검토하십시오. SiteMinder 가 IdP 인 경우 표에서 IdP 활동을 검토하십시오.

다음 다이어그램은 SAML 2.0 아티팩트 SSO 트랜잭션 흐름을 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.

이벤트 순서는 다음과 같습니다.

작업자	트랜잭션 프로세스
SP 역할의 SiteMinder	1. 사용자가 특정 IdP 에서 인증을 받기 위해 SP 에 있는 링크를 선택합니다. 이 링크에는 선택한 IdP 를 나타내는 공급자 ID 가 포함되어 있어야 합니다.
	2. SP FWS 가 로컬 정책 서버에 IdP 구성 정보를 요청합니다. **로그 메시지:** SAML2.0 IDP Configuration is not in cache. Requesting to get from policy server(SAML2.0 IDP 구성이 캐시에 없습니다. 정책 서버에서 가져오도록 요청합니다). **검사점 코드:** [SSOSAML2_IDPCONFFROMPS_REQ]
	3. 로컬 정책 서버가 IdP 구성을 SP FWS 응용 프로그램에 반환합니다. FWS 는 이 정보를 캐시합니다. **로그 메시지:** Policy server returns SAML2.0 IDP Configuration(정책 서버가 SAML2.0 IDP 구성을 반환합니다). **검사점 코드:** [SSOSAML2_IDPCONFFROMPS_RSP]
	4. SP FWS 가 터널 호출을 통해 로컬 정책 서버에 AuthnRequest 메시지를 요청하면서 공급자 ID 를 전달합니다. 요청에는 ProtocolBinding 요소 값에 아티팩트 프로필이 수록되어 있습니다. **로그 메시지**: Get authentication request from policy server(정책 서버에서 인증 요청을 가져옵니다). **검사점 코드**: [SSOSAML2_GETAUTHENTICATIONREQFROMPS_REQ]
	5. SP 정책 서버가 AuthnRequest 메시지를 생성하고 SP FWS 응용 프로그램에 반환합니다.
	6. 로컬 정책 서버가 HTTP 리디렉션 바인딩의 AuthnRequest 메시지를 SP FWS 에 반환합니다. **로그 메시지**: Policy server returns authentication request(정책 서버가 인증 요청을 반환합니다). **검사점 코드**: [SSOSAML2_GETAUTHENTICATIONREQFROMPS_RSP]

작업자	트랜잭션 프로세스
	7. SP FWS 응용 프로그램이 AuthnRequest 메시지와 함께 사용자를 구성 정보에서 획득된 IdP 싱글 사인온 서비스 URL 로 리디렉션합니다. **로그 메시지**: Service redirecting to SSO URL(서비스를 SSO URL 로 리디렉션합니다). **검사점 코드**: [SSOSAML2_SSOURL_REDIRECT]
사용자 에이전트(브라우저)	8. 브라우저가 IdP 싱글 사인온 서비스 URL 을 요청합니다.
IdP 역할의 SiteMinder	9. IdP FWS 가 로컬 IdP 정책 서버에 SP 구성 정보를 요청합니다. **로그 메시지:** SAML2.0 SP Configuration is not in cache. Requesting to get from policy server(SAML2.0 SP 구성이 캐시에 없습니다. 정책 서버에서 가져오도록 요청합니다). **검사점 코드:** [SSOSAML2_SPCONFFROMPS_REQ]
	10. 로컬 정책 서버가 구성을 반환하고 이는 FWS 응용 프로그램에 캐시됩니다. **로그 메시지:** Policy server returns SAML2.0 SP Configuration(정책 서버가 SAML2.0 SP 구성을 반환합니다). **검사점 코드**: [SSOSAML2_SPCONFFROMPS_RSP]
	11. IdP FWS 응용 프로그램이 이 IdP 도메인에 대한 SMSESSION 쿠키를 가져옵니다. 그런 다음 FWS 는 정책 서버를 호출하여 해당 쿠키의 유효성을 검사합니다. SMSESSION 쿠키가 없는 경우 FWS 응용 프로그램이 인증 URL 로 리디렉션하거나 포스트합니다. **로그 메시지**: Session cookie does not exists. Redirecting to authentication URL(세션 쿠키가 없습니다. 인증 URL 로 리디렉션합니다). **검사점 코드:** [SSOSAML2_AUTHENTICATIONURL_REDIRECT]
	12. 정책 서버가 SMSESSION 쿠키의 유효성을 검사하고 결과를 반환합니다. **로그 메시지:** Request to validate the session(세션 유효성 검사 요청) **검사점 메시지:** [SSOSAML2_SESSIONCOOKIEVALIDATE_REQ]

작업자	트랜잭션 프로세스
	13. SMSESSION 쿠키가 유효한 경우에는 IDP FWS 가 로컬 정책 서버에 SAML 2.0 아티팩트를 요청합니다(18 단계 참조). SMSESSION 쿠키가 존재하지 않거나 유효하지 않은 경우 IdP FWS 가 인증 URL 로 리디렉션하거나 인증 URL 에 포스트합니다. **로그 메시지:** Session cookie does not exists, redirecting to authentication url(세션 쿠키가 없습니다. 인증 URL 로 리디렉션합니다). **검사점 코드:** [SSOSAML2_AUTHENTICATIONURL_REDIRECT]
사용자 에이전트(브라우저)	14. SMSESSION 쿠키가 유효하지 않은 경우 브라우저는 IdP 웹 에이전트로 보호되는 인증 URL 을 요청합니다.
IdP 역할의 SiteMinder	15. IdP 웹 에이전트가 사용자 로그인을 수행하면서 SMSESSION 쿠키를 설정하고 요청이 인증 URL 에 전달되도록 합니다. **로그 메시지**: Service redirecting to SSO URL(서비스를 SSO URL 로 리디렉션합니다). **검사점 코드:** [SSOSAML2_SSOURL_REDIRECT]
	16. 이 인증 URL 은 AuthnRequest 메시지와 함께 IdP 싱글 사인온 서비스에 대한 요청을 재생하는 redirect.jsp 파일입니다.
사용자 에이전트(브라우저)	17. 브라우저가 IdP 싱글 사인온 서비스 URL 을 요청합니다. 이 요청은 8 단계의 요청과 동일하지만 이제 사용자의 SMSESSION 쿠키가 유효합니다.
IdP 역할의 SiteMinder	18. IdP FWS 가 로컬 정책 서버에 SAML 2.0 아티팩트를 요청합니다. FWS 가 구성 정보에서 획득된 영역에 대한 권한 부여 호출을 통해 AuthnRequest 를 전달합니다. **로그 메시지:** Request to policy server for generating saml2 assertion/artifact based on selected profile(선택한 프로필에 기반하여 saml2 어설션/아티팩트를 생성하도록 정책 서버에 요청합니다). **검사점 코드:** [SSOSAML2_GENERATEASSERTIONORARTIFACT_REQ]

작업자	트랜잭션 프로세스
	19. 정책 서버가 아티팩트와 해당 응답 메시지를 생성합니다. 이 메시지는 서비스 공급자 구성에서 작성합니다. 정책 서버가 응답을 세션 저장소에 저장합니다. 메시지는 세션 변수로 저장되고 아티팩트 메시지 핸들의 문자열 표현을 사용하여 명명됩니다. **로그 메시지:** Policy server generates the artifact for the assertion(정책 서버가 어설션에 대한 아티팩트를 생성합니다). **검사점 코드:** [SSOSAML2_PSGENERATEARTIFACT_REQ] **로그 메시지:** Policy server stores the assertion in session store(정책 서버가 세션 저장소에 어설션을 저장합니다). **검사점 코드:** [SSOSAML2_PSSTOREASSERTIONINSSTORE_REQ]
	20. 정책 서버가 아티팩트를 IdP FWS 에 반환합니다. **로그 메시지:** Policy server returning the wrappedassertion/artifact based on profile selected in response message(정책 서버가 응답 메시지에서 선택한 프로필을 기준으로 wrappedassertion/artifact 를 반환합니다). **검사점 코드:** [SSO_PSWRAPPEDASSERTION_RSP]
	21. 정책 서버가 SP 구성 정보를 반환합니다. **로그 메시지:** Policy server returns SAML2.0 SP Configuration(정책 서버가 SAML2.0 SP 구성을 반환합니다). **검사점 코드:** [SSOSAML2_SPCONFFROMPS_RSP] 정보를 기반으로 IdP FWS 가 다음 작업 중 하나를 수행합니다. ■ 브라우저를 SP 의 어설션 소비자 URL 로 리디렉션합니다. URL 로 인코딩된 아티팩트는 URL 매개 변수입니다. **로그 메시지**: Sending artifact to assertion consumer as url parameter(아티팩트를 URL 매개 변수로서 어설션 소비자에게 보냅니다). **검사점 코드**: [SSOSAML2_SENDINGARTIFACTASURLPARAM_RSP] ■ 양식을 사용자에게 반환합니다. 이 양식에는 응답 메시지, 어설션 소비자 URL, 양식을 브라우저에 자동 POST 할 JavaScript 가 포함됩니다. **로그 메시지:** Adding response in form for HTTP post(HTTP 포스트에 대한 형식으로 응답을 추가하고 있습니다). **검사점 코드:** [FWSBASE_POSTDATAFORM_ADD] **참고:** 어설션 생성기가 현재 세션의 인증 수준이 너무 낮다고 나타낼 수 있습니다. 수준이 너무 낮으면 IdP FWS 가 단계별 인증 강화를 손쉽게 수행하기 위해 인증 URL 로 리디렉션합니다.

작업자	트랜잭션 프로세스
사용자 에이전트(브라우저)	22. 브라우저가 응답 메시지를 SP 의 어설션 소비자 URL 에 포스트합니다.
IdP 역할의 SiteMinder	23. 아티팩트가 URL 의 일부로 전송된 경우 브라우저가 아티팩트와 함께 사용자를 어설션 소비자 URL 로 리디렉션합니다. 아티팩트가 양식에 포함된 상태로 반환된 경우에는 브라우저가 아티팩트를 어설션 소비자 URL 에 포스트합니다. **로그 메시지**: Browser posting the response to assertion consumer url(브라우저가 응답을 어설션 소비자 URL 에 포스트하고 있습니다). **검사점 코드**: [SSOSAML2_POSTASSERTIONTOCONSUMERURL_RSP] SP FWS 어설션 소비자 서비스는 아티팩트를 가져오기 위해 IdP FWS 아티팩트 레졸루션 서비스로 백 채널 호출을 보냅니다. 23a-23d 단계는 백 채널 호출을 반영합니다.
	23a. SP FWS 가 GET 또는 POST 데이터(브라우저를 리디렉션하도록 IdP FWS 를 구성하는 방법에 따라 결정됨)에서 아티팩트를 획득합니다. 그런 다음 FWS 가 IdP 구성에서 아티팩트 레졸루션 서비스의 SOAP 끝점을 획득합니다. 원본 ID 는 아티팩트의 일부입니다. SOAP 끝점이 획득된 후 SP FWS 가 IdP FWS 아티팩트 레졸루션 서비스에 대한 백 채널 호출을 수행하여 아티팩트를 응답 메시지로 확인합니다. **로그 메시지:** Backchannel call to resolve the artifact(아티팩트를 확인하기 위한 백 채널 호출) **검사점 코드:** [SSOSAML2_RESOLVEARTIFACT_REQ] **로그 메시지:** Obtained response message from post data for artifact binding(아티팩트 바인딩을 위해 게시 데이터로부터 응답 메시지를 가져왔습니다). **검사점 코드:** SSOSAML2_READRESPONSEARTIFACTDATA_RSP
	23b. IdP FWS 가 로컬 정책 서버에 응답 메시지를 요청합니다. 세션 변수로 저장되는 메시지가 Java Agent API 를 사용하여 요청됩니다. 세션 ID 가 아티팩트에서 추출됩니다. 세션 변수 이름은 아티팩트 메시지 핸들의 문자열 표현입니다. **로그 메시지:** Extracting session id from artifact(아티팩트에서 세션 ID 를 추출하고 있습니다). **검사점 코드:** [SSOSAML2_EXTRACTSESSIONIDFROMARTIFACT_REQ]

작업자	트랜잭션 프로세스
	23c. 로컬 정책 서버는 세션 저장소로부터 어설션 응답 메시지를 가져옵니다. 정책 서버는 아티팩트를 가져온 후 삭제합니다. **로그 메시지:** Retrieving assertion from session store(세션 저장소에서 어설션을 가져오고 있습니다.) **검사점 코드:** [SSOSAML2_RETREIVEASSERTIIONFROMSSTORE_REQ]
	23d. 로컬 정책 서버는 어설션을 가져와 아티팩트 응답을 IdP FWS 로 반환합니다. IdP FWS 가 아티팩트 응답을 SP FWS 어설션 소비자 서비스에 반환합니다. **로그 메시지:** Obtained the SAML2 asserion as response from artifact resolve call(아티팩트 확인 호출에서 응답으로서 SAML2 어설션을 가져왔습니다). **검사점 코드:** [SSOSAML2_GOTARTIFACTRESPONSE_RSP] **로그 메시지:** Sending assertion as artifact response(아티팩트 응답으로서 어설션을 보내고 있습니다). **검사점 코드:** [SSOSAML2_SENDARTIFACTRESPONSE_RSP] 이제 백 채널 호출이 완료되었습니다.
SP 역할의 SiteMinder	24. SP FWS 가 POST 데이터에서 응답 메시지를 획득합니다. 그런 다음 서비스가 구성에서 대상 리소스를 확인하고 정책 서버에 대한 isProtected 호출을 수행하여 대상 리소스를 요청합니다. **로그 메시지:** Reading the configuration to get the target URL(대상 URL 을 가져오기 위해 구성을 읽고 있습니다). **검사점 코드:** [SSOSAML2_READTARGETURL_REQ] **로그 메시지:** IsProtected call to policy server for target resource realm(대상 리소스 영역을 위해 정책 서버에 IsProtected 호출을 수행합니다). **검사점 코드:** [SSOSAML2_ISPROTECTEDCALLTOPS_REQ] 어설션이 암호화된 경우 FWS 가 터널 호출을 수행합니다. 이 호출은 어설션을 암호화된 상태로 가져와서 일반 텍스트 상태로 반환합니다. **로그 메시지:** Tunnel call to decrypt the assertion(어설션 암호 해독을 위해 터널 호출을 수행합니다). **검사점 코드:** [SSOSAML2_DECRYPTASSERTION_REQ]
	25. 정책 서버가 대상 리소스에 대한 영역 OID 를 반환합니다. **로그 메시지:** Policy server returns the realm OID for target resource(정책 서버가 대상 리소스에 대한 영역 OID 를 반환합니다). **검사점 코드:** [SSOSAML2_REALMOIDFORTARGETFROMPS_RSP]

작업자	트랜잭션 프로세스
	26. SP FWS 가 로그인 호출을 통해 응답 메시지를 로컬 정책 서버에 전달합니다. 응답 메시지는 자격 증명으로 작동하고 영역 OID 는 isProtected 호출에서 획득됩니다. **로그 메시지:** Passing response message through login call(로그인 호출을 통해 응답 메시지를 전달하고 있습니다). **검사점 코드:** [SSO_RESPONSEMESSAGEINLOGIN_REQ] SAML 2.0 인증 체계가 응답 메시지를 자격 증명으로 사용하여 사용자 로그인을 수행합니다. **로그 메시지:** Policy server logs in the user using SAML 2 auth scheme(정책 서버가 SAML 2 인증 체계를 사용하여 사용자 로그인을 수행합니다). **검사점 코드:** [SAML2_AUTH_COMPLETE]
	27. 로컬 정책 서버가 OK 를 SP FWS 에 반환합니다.
	28. 성공 응답이 반환되면 SP FWS 가 SP 도메인에 대한 SMSESSION 쿠키를 생성합니다. 서비스가 쿠키를 브라우저에 저장합니다. **로그 메시지:** Login successful(로그인 성공) **검사점 코드:** [SSO_LOGINSUCEESS_RSP] **로그 메시지:** Creating the smsession cookie for SP domain(SP 도메인에 대한 smsession 세션 쿠키를 만들고 있습니다). **검사점 코드:** [SSO_SMSESSIONFORSPDOMAIN_REQ] 브라우저는 구성 정보에서 가져온 대상 URL 로 사용자를 리디렉션합니다. **로그 메시지:** Redirecting user to target url(대상 URL 로 사용자를 리디렉션합니다). **검사점 코드**: [SSOSAML2_REDIRECTUSERTARGETURL_REQ] 로그인이 실패하면 SP FWS 가 사용자를 액세스 권한 없음 URL 로 리디렉션합니다. **로그 메시지:** Login failure(로그인 실패) **검사점 코드:** [SSO_LOGINFAILURE_RSP]
사용자 에이전트(브라우저)	29. 브라우저가 SP 측 웹 에이전트로 보호되는 대상 URL 로 요청을 보냅니다. 브라우저에 SMSESSION 쿠키가 있으므로 웹 에이전트가 사용자에게 인증을 요청하지 않습니다. 사용자가 리소스에 대한 액세스 권한을 얻습니다.

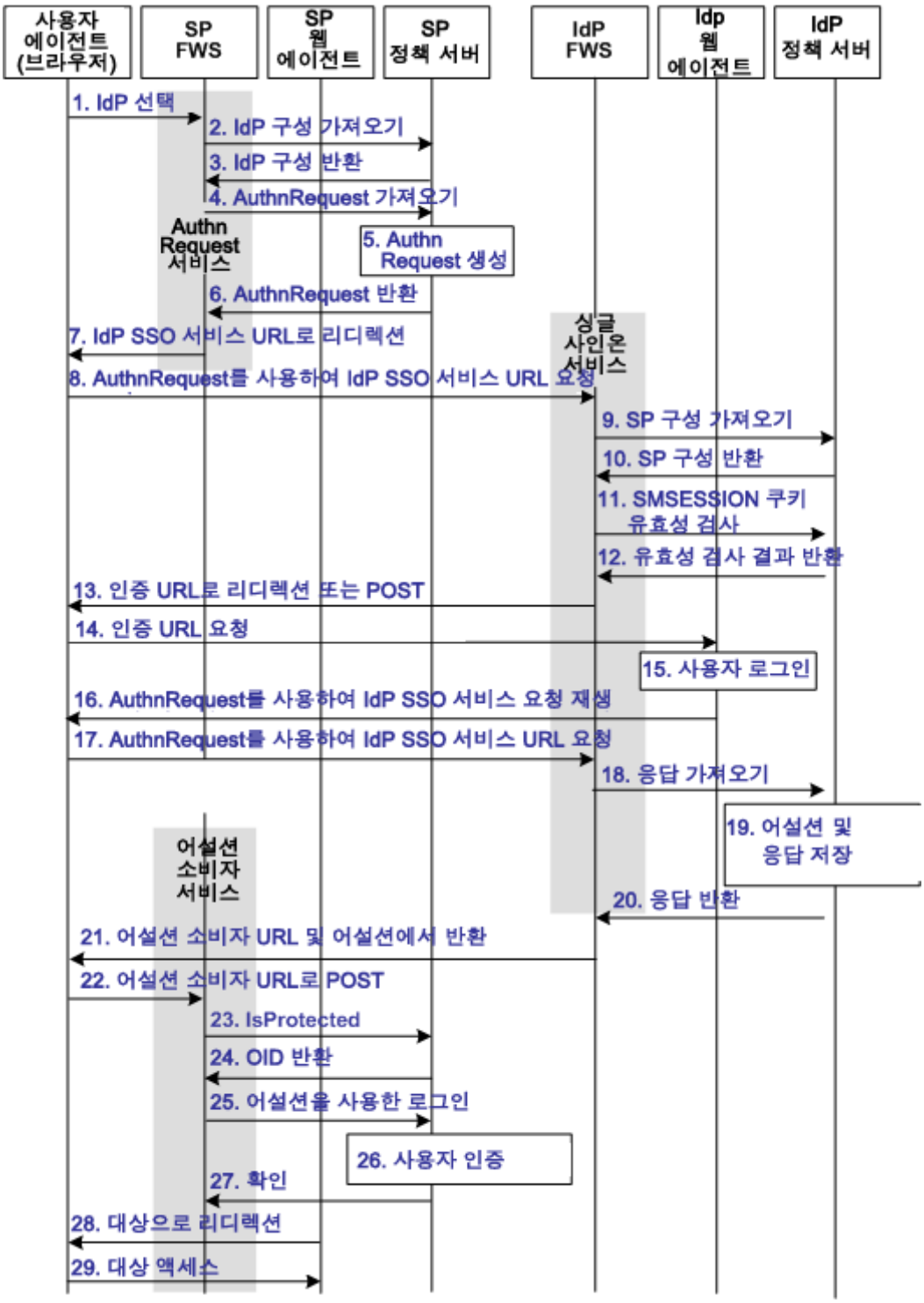
SAML 2.0 POST SSO 트랜잭션 흐름(SP 시작)

다음 다이어그램에서는 사용자와 SiteMinder IdP(아이덴티티 공급자) 및 SP(서비스 공급자) 사이트에 배포된 구성 요소 간의 상세 흐름을 보여 줍니다. 이 흐름은 SAML 어설션을 처리하기 위한 방법으로서 SAML 2.0 POST 를 사용하는 사이트 간 싱글 사인온을 보여 줍니다.

흐름도에서는 다음과 같은 정보를 사용한다고 가정합니다.

- 어설션에 대해 SP 가 시작한 요청
- IdP 와 SP 사이트에서 인증 및 권한 부여가 성공했습니다.
- SiteMinder 는 IdP 및 SP 로만 표시되므로 각 파트너에서 프로세스를 볼 수 있습니다. SiteMinder 가 환경에서 SP 인 경우 표에서 SP 활동을 검토하십시오. SiteMinder 가 IDP 인 경우 표에서 IdP 활동을 검토하십시오.

다음 다이어그램은 SAML 2.0 POST SSO 트랜잭션 흐름을 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.

이벤트 순서는 다음과 같습니다.

작업자	트랜잭션 프로세스
SP 역할의 SiteMinder	1. 사용자가 특정 IdP 에서 인증을 받기 위해 SP 에 있는 링크를 선택합니다. 이 링크에는 선택한 IdP 를 나타내는 공급자 ID 가 포함되어 있어야 합니다.
	2. SP FWS 가 로컬 정책 서버에 IdP 구성을 요청합니다. **로그 메시지:** SAML2.0 IDP Configuration is not in cache. Requesting to get from policy server(SAML2.0 IDP 구성이 캐시에 없습니다. 정책 서버에서 가져오도록 요청합니다). **검사점 코드:** [SSOSAML2_IDPCONFFROMPS_REQ]
	3. 정책 서버가 IdP 구성을 SP FWS 응용 프로그램에 반환합니다. FWS 응용 프로그램이 이 정보를 캐시합니다. **로그 메시지:** Policy server returns SAML2.0 IDP Configuration(정책 서버가 SAML2.0 IDP 구성을 반환합니다). **검사점 코드:** [SSOSAML2_IDPCONFFROMPS_RSP]
	4. SP FWS 응용 프로그램이 터널 호출을 통해 로컬 SP 정책 서버에 AuthnRequest 메시지를 요청하면서 공급자 ID 를 전달합니다. **로그 메시지**: Get authentication request from policy server(정책 서버에서 인증 요청을 가져옵니다). **검사점 코드**: [SSOSAML2_GETAUTHENTICATIONREQFROMPS_REQ]
	5. SP 정책 서버가 AuthnRequest 메시지를 생성하고 SP FWS 응용 프로그램에 반환합니다.
	6. SP FWS 응용 프로그램이 HTTP 리디렉션 바인딩의 AuthnRequest 응답을 가져옵니다. **로그 메시지**: Policy server returns authentication request(정책 서버가 인증 요청을 반환합니다). **검사점 코드**: [SSOSAML2_GETAUTHENTICATIONREQFROMPS_RSP]

작업자	트랜잭션 프로세스
	7. SP FWS 응용 프로그램이 사용자를 IdP 싱글 사인온 서비스 URL 로 리디렉션합니다. **로그 메시지**: Service redirecting to SSO URL(서비스를 SSO URL 로 리디렉션합니다). **검사점 코드**: [SSOSAML2_SSOURL_REDIRECT]
사용자 에이전트(브라우저)	8. 브라우저가 IdP 싱글 사인온 서비스 URL 을 요청합니다.
IdP 역할의 SiteMinder	9. IdP FWS 가 로컬 IdP 정책 서버에 SP 구성을 요청합니다. **로그 메시지:** SAML2.0 SP Configuration is not in cache. Requesting to get from policy server(SAML2.0 SP 구성이 캐시에 없습니다. 정책 서버에서 가져오도록 요청합니다). **검사점 코드:** [SSOSAML2_SPCONFFROMPS_REQ]
	10. 로컬 정책 서버가 구성을 반환하고 이는 FWS 응용 프로그램에 캐시됩니다. **로그 메시지:** Policy server returns SAML2.0 SP Configuration(정책 서버가 SAML2.0 SP 구성을 반환합니다). **검사점 코드**: [SSOSAML2_SPCONFFROMPS_RSP]
	11. IdP FWS 응용 프로그램이 이 IdP 도메인에 대한 SMSESSION 쿠키를 가져옵니다. 그런 다음 FWS 응용 프로그램이 정책 서버를 호출하여 해당 쿠키의 유효성을 검사합니다. SMSESSION 쿠키가 없는 경우 FWS 응용 프로그램이 인증 URL 로 리디렉션하거나 포스트합니다. **로그 메시지**: Session cookie does not exists. Redirecting to authentication URL(세션 쿠키가 없습니다. 인증 URL 로 리디렉션합니다). **검사점 코드:** [SSOSAML2_AUTHENTICATIONURL_REDIRECT]
	12. 정책 서버가 SMSESSION 쿠키의 유효성을 검사하고 결과를 반환합니다. **로그 메시지:** Request to validate the session(세션 유효성 검사 요청) **검사점 메시지:** [SSOSAML2_SESSIONCOOKIEVALIDATE_REQ]
	13. SMSESSION 쿠키가 유효한 경우에는 IdP FWS 가 18 단계로 건너뜁니다. SMSESSION 쿠키가 존재하지 않거나 유효하지 않은 경우 IdP FWS 가 인증 URL 로 리디렉션하거나 인증 URL 에 포스트합니다. **로그 메시지:** Session cookie does not exists, redirecting to authentication url(세션 쿠키가 없습니다. 인증 URL 로 리디렉션합니다). **검사점 코드:** [SSOSAML2_AUTHENTICATIONURL_REDIRECT]

작업자	트랜잭션 프로세스
사용자 에이전트(브라우저)	14. SMSESSION 쿠키가 유효하지 않은 경우 브라우저는 IdP 웹 에이전트로 보호되는 인증 URL 을 요청합니다.
IdP 역할의 SiteMinder	15. IdP 웹 에이전트가 사용자 로그인을 수행하면서 SMSESSION 쿠키를 설정하고 요청이 인증 URL 에 전달되도록 합니다. **로그 메시지**: Service redirecting to SSO URL(서비스를 SSO URL 로 리디렉션합니다). **검사점 코드:** [SSOSAML2_SSOURL_REDIRECT]
	16. 이 인증 URL 은 AuthnRequest 메시지와 함께 IdP 싱글 사인온 서비스에 대한 요청을 재생하는 redirect.jsp 파일입니다.
사용자 에이전트(브라우저)	17. 브라우저가 IdP 싱글 사인온 서비스 URL 을 요청합니다. 이 요청은 8 단계의 요청과 동일하지만 이제 사용자의 SMSESSION 쿠키가 유효합니다.
IdP 역할의 SiteMinder	18. IdP FWS 가 정책 서버에 SAML 2.0 어설션을 요청합니다. AuthnRequest 가 구성에서 획득된 영역에 대한 권한 부여 호출을 통해 이동합니다. **로그 메시지:** Request to policy server for generating saml2 assertion/artifact based on selected profile(선택한 프로필에 기반하여 saml2 어설션/아티팩트를 생성하도록 정책 서버에 요청합니다). **검사점 코드:** [SSOSAML2_GENERATEASSERTIONORARTIFACT_REQ]
	19. 정책 서버가 SP 의 구성에 기반한 어설션을 생성하고 서명한 다음 응답 메시지에 래핑된 상태로 반환합니다. **로그 메시지:** Policy server generates the saml2 assertion(정책 서버가 saml2 어설션을 생성합니다). **검사점 코드:** [SSOSAML2_PSGENERATEASSERTION_RSP]
	20. 응답 메시지가 IdP FWS 에 반환됩니다. **로그 메시지:** Policy server returns the wrappedassertion/artifact(based on profile selected) in response message(정책 서버가 응답 메시지에서 선택한 프로필을 기준으로 wrappedassertion/artifact 를 반환합니다). **검사점 코드**: [SSO_PSWRAPPEDASSERTION_RSP]

작업자	트랜잭션 프로세스
	21. IdP FWS 가 양식을 사용자에게 반환합니다. 이 양식에는 응답 메시지, 어설션 소비자 URL, 양식을 제출할 JavaScript 등이 포함됩니다. **로그 메시지:** Adding response in form for HTTP post(HTTP 포스트에 대한 형식으로 응답을 추가하고 있습니다). **검사점 코드:** [FWSBASE_POSTDATAFORM_ADD] **참고:** 정책 서버가 현재 세션의 인증 수준이 너무 낮다고 나타내면 IdP FWS 가 단계별 인증 강화를 손쉽게 수행하기 위해 13 단계에 설명된 대로 인증 URL 로 리디렉션합니다.
사용자 에이전트(브라우저)	22. 브라우저가 응답을 SP 의 어설션 소비자 URL 에 포스트합니다.
SP 역할의 SiteMinder	23. SP FWS 가 POST 데이터에서 응답 메시지를 획득합니다. 그런 다음 FWS 가 구성에서 대상 리소스를 확인하고 정책 서버에 대한 isProtected 호출을 수행하여 대상 리소스를 요청합니다. 어설션이 암호화된 경우 FWS 가 터널 호출을 수행합니다. 이 호출은 어설션을 암호화된 상태로 가져와서 일반 텍스트 상태로 반환합니다. **로그 메시지:** Reading the configuration to get the target url(대상 URL 을 가져오기 위해 구성을 읽고 있습니다). **검사점 코드:** [SSOSAML2_READTARGETURL_REQ] **로그 메시지:** Get realm oid for target resource from property(속성에서 대상 리소스에 대한 영역 OID 를 가져옵니다). **검사점 코드:** [SSOSAML2_REALMOIDFORTARGETFROMPROPERTY_RSP] **로그 메시지:** Tunnel call to decrypt the assertion(어설션 암호 해독을 위해 터널 호출을 수행합니다). **검사점 코드:** [SSOSAML2_DECRYPTASSERTION_REQ]
	24. 정책 서버가 대상 리소스에 대한 영역 OID 를 반환합니다. **로그 메시지:** Policy server returns the realm oid for target resource(정책 서버가 대상 리소스에 대한 영역 OID 를 반환합니다). **검사점 코드**: [SSOSAML2_REALMOIDFORTARGETFROMPS_RSP]
	25. SP FWS 가 로그인 호출을 통해 응답 메시지를 로컬 정책 서버에 전달합니다. FWS 는 응답 메시지를 자격 증명으로 사용하고 isProtected 호출에서 획득된 영역 OID 도 사용합니다. **로그 메시지:** Passing response message through login call(로그인 호출을 통해 응답 메시지를 전달하고 있습니다). **검사점 코드**: [SSO_RESPONSEMESSAGEINLOGIN_REQ]

작업자	트랜잭션 프로세스
	26. 정책 서버가 응답 메시지를 자격 증명으로 사용하여 사용자 로그인을 수행합니다. **로그 메시지:** Policy server logs in the user using SAML 2 auth scheme(정책 서버가 SAML 2 인증 체계를 사용하여 사용자 로그인을 수행합니다). **검사점 코드:** [SAML2_AUTH_COMPLETE]
	27. 로컬 정책 서버가 OK 를 SP FWS 에 반환합니다. **로그 메시지:** Login successful(로그인 성공) **검사점 코드**: [SSO_LOGINSUCEESS_RSP]
	28. 성공 응답이 반환되면 SP FWS 가 SP 도메인에 대한 SMSESSION 쿠키를 생성합니다. FWS 응용 프로그램이 쿠키를 브라우저에 넣고 사용자를 대상 URL 로 리디렉션합니다. **로그 메시지:** Redirecting user to target url(대상 URL 로 사용자를 리디렉션합니다). **검사점 코드:** [SSOSAML2_REDIRECTUSERTARGETURL_REQ] 로그인이 실패하면 SP FWS 가 사용자를 액세스 권한 없음 URL 로 리디렉션합니다. **로그 메시지:** Login failure(로그인 실패) **검사점 코드:** [SSO_LOGINFAILURE_RSP]
사용자 에이전트(브라우저)	29. 브라우저가 SP 측 웹 에이전트로 보호되는 대상 URL 로 요청을 보냅니다. 브라우저에 SMSESSION 쿠키가 있으므로 웹 에이전트가 사용자에게 인증을 요청하지 않습니다. 사용자가 리소스에 대한 액세스 권한을 얻습니다.

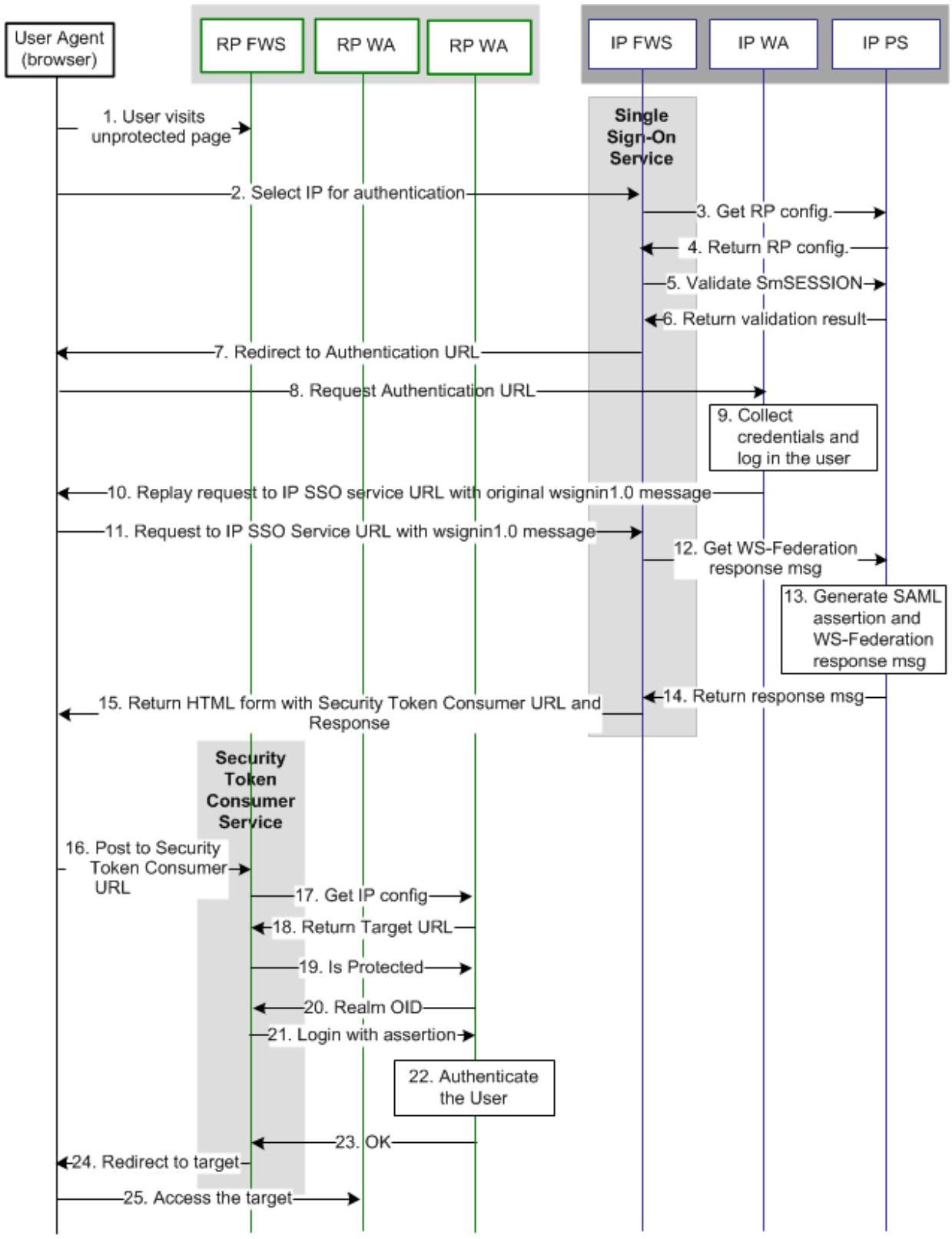
WS-페더레이션 SSO 트랜잭션 흐름(RP 시작)

다음 그림에서는 사용자와 IP(아이덴티티 공급자) 및 RP(리소스 파트너) 사이트에 있는 페더레이션 구성 요소 간의 흐름을 보여 줍니다. 이 흐름은 SAML 어설션을 처리하는 방법으로서 WS-페더레이션 피동 요청자 프로필을 사용하는 사이트 사이의 싱글 사인온을 표시합니다.

흐름도에서는 다음과 같은 정보를 사용한다고 가정합니다.

- 리소스 파트너가 리소스에 대한 요청을 시작합니다.
- 각 사이트에서 인증 및 권한 부여가 성공했습니다.
- SiteMinder 는 IP 및 RP 로만 표시되므로 각 파트너에서 프로세스를 볼 수 있습니다. SiteMinder 가 환경에서 IP 인 경우 표에서 IP 활동을 검토하십시오. SiteMinder 가 RP 인 경우 표에서 RP 활동을 검토하십시오.

다음 다이어그램은 WS-페더레이션 SSO 트랜잭션 흐름을 보여 줍니다.


User Agent (browser)
RP FWS
RP WA
RP WA
IP FWS
IP WA
IP PS
Single Sign-On Service
1. User visits unprotected page
2. Select IP for authentication
3. Get RP config.
4. Return RP config.
5. Validate SmSESSION
6. Return validation result
7. Redirect to Authentication URL
8. Request Authentication URL
9. Collect credentials and log in the user
10. Replay request to IP SSO service URL with original wsignin1.0 message
11. Request to IP SSO Service URL with wsignin1.0 message
12. Get WS-Federation response msg
13. Generate SAML assertion and WS-Federation response msg
14. Return response msg
15. Return HTML form with Security Token Consumer URL and Response
Security Token Consumer Service
16. Post to Security Token Consumer URL
17. Get IP config
18. Return Target URL
19. Is Protected
20. Realm OID
21. Login with assertion
22. Authenticate the User
23. OK
24. Redirect to target
25. Access the target

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.

이벤트 순서는 다음과 같습니다.

작업자	트랜잭션 프로세스
RP 역할의 SiteMinder	1. 사용자가 리소스 파트너의 보호되지 않은 사이트 선택 페이지를 방문합니다.
	2. 사용자가 링크를 클릭하여 IP 에서 인증합니다. 이 링크는 IP 의 싱글 사인온 서비스를 가리킵니다. 링크에는 RP 공급자 ID 가 포함되어야 하고 wctx 매개 변수 같은 선택적 매개 변수가 포함될 수 있습니다.
	3. IP FWS 가 로컬 정책 서버에 RP 구성을 요청합니다. **로그 메시지:** Trying to fetch Wsfed Resource Partner Configuration from cache(캐시에서 Wsfed 리소스 파트너 구성을 가져오려고 시도합니다). **검사점 코드:** [SSOWSFED_RESOURCEPARTNERCONFFROMCACHE_REQ] **로그 메시지**: Wsfed Resource Partner Configuration is not in cache. Requesting to get from policy server(Wsfed 리소스 파트너 구성이 캐시에 없습니다. 정책 서버에서 가져오도록 요청합니다). **검사점 코드:** [SSOWSFED_RESOURCEPARTNERCONFFROMPS_REQ]
	4. 로컬 정책 서버가 구성을 반환합니다. **로그 메시지**: Policy server returns Wsfed Resource Partner Configuration(정책 서버가 Wsfed 리소스 파트너 구성을 반환합니다). **검사점 코드**: [SSOWSFED_RESOURCEPARTNERCONFFROMPS_RSP]
	5. IP FWS 가 IP 도메인에 대한 SMSESSION 쿠키를 가져오고 정책 서버를 호출하여 해당 쿠키의 유효성을 검사합니다. SMSESSION 쿠키가 없는 경우 IP FWS 가 7 단계로 건너뜁니다. **로그 메시지:** Request to validate the session(세션 유효성 검사 요청) **검사점 코드**: [SSOWSFED_SESSIONCOOKIEVALIDATE_REQ]
	6. 정책 서버가 SMSESSION 쿠키의 유효성을 검사하고 결과를 FWS 응용 프로그램에 반환합니다.

작업자	트랜잭션 프로세스
	7. SMSESSION 쿠키가 존재하지 않거나 유효하지 않은 경우 IP FWS 가 사용자를 RP 구성에서 획득된 인증 URL 로 리디렉션합니다. SMSESSION 쿠키가 유효한 경우에는 IP FWS 가 12 단계로 건너뜁니다. **로그 메시지:** Session cookie does not exists, redirecting to authentication url(세션 쿠키가 없습니다. 인증 URL 로 리디렉션합니다). **검사점 코드:** [SSOWSFED_AUTHENTICATIONURL_REDIRECT]
사용자 에이전트(브라우저)	8. 브라우저가 IP 웹 에이전트로 보호되는 인증 URL 을 요청합니다.
IP 역할의 SiteMinder	9. IP WA 가 사용자를 인증하고 SMSESSION 쿠키를 설정합니다. IP WA 가 요청이 인증 URL 에 전달되도록 합니다.
	10. 인증 URL 은 원래 wsignin 메시지를 사용하여 IP SSO 서비스에 대한 요청을 재생합니다.
사용자 에이전트(브라우저)	11. 브라우저가 IP SSO 서비스 URL 을 요청합니다. 이 요청은 2 단계의 요청과 동일하지만 이제 사용자의 SMSESSION 쿠키가 유효합니다.
IP 역할의 SiteMinder	12. IP FWS 가 구성에서 획득된 영역에 대한 권한 부여 호출을 통해 정책 서버에 WS-페더레이션 <RequestSecurityTokenResponse>를 요청합니다. **로그 메시지:** Request to policy server for generating Wsfed assertion(Wsfed 어설션을 생성하기 위해 정책 서버에 요청합니다). **검사점 메시지:** [SSOWSFED_GENERATEASSERTION_REQ]
	13. 정책 서버가 RP 구성에 기반한 SAML1.1 어설션을 생성합니다. **로그 메시지:** Policy server generates the samlxx assertion for wsfed12(정책 서버가 wsfed12 에 대한 samlxx 어설션을 생성합니다). **검사점 코드**: [SSOWSFED12_PSGENERATESAML11ASSERTION_RSP]
	14. 정책 서버가 어설션에 서명하고 어설션을 <RequestSecurityTokenResponse> 메시지의 IP FWS 응용 프로그램으로 반환합니다. **로그 메시지:** Policy server signs the Assertion element of the RequestSecurityTokenResponse(정책 서버가 RequestSecurityTokenResponse 의 Assertion 요소에 서명합니다). **검사점 코드:** SAML 프로토콜마다 다릅니다. [SSOWSFED10_PSGENERATELEGACYASSERTION_RSP] [SSOWSFED12_PSGENERATESAML12ASSERTION_RSP] [SSOWSFED_PSSIGNASSERTION_RSP]

작업자	트랜잭션 프로세스
	15. IP FWS 는 URL 로 인코딩된 <RequestSecurityTokenResponse> 메시지, 보안 토큰 소비자 서비스 URL, wsignin 메시지의 옵션 wctx, 양식을 자동 제출하기 위한 JavaScript 를 수록한 양식을 사용자에게 반환합니다. 원래 wsignin 요청에 wreply 매개 변수가 포함된 경우 해당 값은 보안 토큰 소비자 URL 이 됩니다. wreply 값은 보안 토큰 소비자 URL 설정이 RP 구성에 없는 경우에만 URL 이 됩니다. RP 구성의 보안 토큰 소비자 URL 이 wreply 매개 변수보다 우선합니다. **참고:** 정책 서버가 현재 세션의 인증 수준이 너무 낮다고 나타낼 수 있습니다. 수준이 너무 낮으면 IP FWS 응용 프로그램이 단계별 인증 강화를 손쉽게 수행하기 위해 7 단계에 설명된 대로 브라우저를 인증 URL 로 리디렉션합니다. **로그 메시지:** Received the assertion response(어설션 응답을 받았습니다). **검사점 코드:** [SSOWSFED_RECEIVEDASSERTION_RSP]
사용자 에이전트(브라우저)	16. 브라우저가 <RequestSecurityTokenResponse> 메시지와 wctx 를 RP 의 보안 토큰 소비자 URL 에 포스트합니다.
RP 역할의 SiteMinder	17. RP FWS 응용 프로그램이 POST 데이터에서 <RequestSecurityTokenResponse> 메시지와 wctx 를 획득합니다. RP FWS 응용 프로그램이 로컬 정책 서버에 IP 구성 정보를 요청합니다. **로그 메시지:** Browser posting the response to security token consumer service url(브라우저가 응답을 보안 토큰 소비자 서비스 URL 로 포스트합니다). **검사점 코드:** [SSOWSFED_POSTASSERTIONTOSECURITYTOKENCONSUMER_RSP] **로그 메시지:** Extracting the assertion from security token consumer response(보안 토큰 소비자 응답에서 어설션을 추출합니다). **검사점 코드:** [SSOWSFED_EXTARCTASSERTIONFROMSECURITYTOKENRESPONSE_REQ]
	18. RP FWS 가 로컬 정책 서버의 IP 구성에서 대상 리소스를 확인합니다. 대상 리소스가 IP 구성의 일부가 아니고 wctx 매개 변수가 POST 데이터에서 발견되는 경우 wctx 값은 대상 리소스가 됩니다. **로그 메시지:** Request to get the target url realm(대상 URL 영역을 가져오도록 요청합니다). **검사점 코드:** [SSOWSFED_GETTARGETURLREALM_REQ]
	19. FWS 가 정책 서버에 대한 isProtected 호출을 수행하여 대상 리소스를 요청합니다.

작업자	트랜잭션 프로세스
	20. 정책 서버가 대상 리소스에 대한 영역 OID 를 반환합니다.
RP 로서 SiteMinder (계속)	21. RP FWS 응용 프로그램이 로그인 호출을 통해 <RequestSecurityTokenResponse> 메시지를 로컬 정책 서버에 전달합니다. <RequestSecurityTokenResponse> 메시지와 isProtected 호출에서 획득된 영역 OID 가 자격 증명 역할을 합니다.
	22. RP FWS 응용 프로그램이 <RequestSecurityTokenResponse> 메시지를 자격 증명으로 사용하여 사용자 로그인을 수행합니다.
	23. 로컬 정책 서버가 OK 상태 메시지를 RP FWS 응용 프로그램에 반환합니다.
	24. RP FWS 응용 프로그램이 RP 도메인에 대한 SMSESSION 쿠키를 생성합니다. FWS 가 쿠키를 브라우저에 넣고 사용자를 대상 URL 이나 wctx POST 데이터로 리디렉션합니다. 로그인이 실패하면 FWS 응용 프로그램이 사용자를 액세스 권한 없음 URL 로 리디렉션합니다. **로그 메시지:** Redirecting user to target url(대상 URL 로 사용자를 리디렉션합니다). **검사점 코드**: [SSOWSFED_REDIRECTUSERTARGETURL_REQ]
사용자 에이전트(브라우저)	25. 사용자 에이전트가 RP 측 웹 에이전트로 보호되는 대상 URL 을 요청합니다. 브라우저에 RP 도메인에 대한 SMSESSION 쿠키가 있으므로 웹 에이전트는 사용자에게 인증을 요청할 필요가 없습니다.

WS-페더레이션 SSO 트랜잭션 흐름(IP 시작)

IP 시작 싱글 사인온은 RP 시작 트랜잭션과 비슷합니다. 주요 차이점은 사용자가 RP 로 리디렉션되기 전에 IP 에서 수행되는 몇 가지 작업뿐입니다.

IP 에서 다음 작업이 수행됩니다.

1. 사용자가 특정 파트너 사이트에 대한 링크를 선택합니다. 이 링크는 IP 의 HTML 콘텐츠 중 일부로, 다른 RP 사이트로 연결되는 사이트 간 전송 링크를 포함합니다.
2. 해당 링크가 웹 브라우저를 IP SSO 서비스 URL 로 연결합니다.
3. SSO 서비스가 브라우저를 RP 로 리디렉션합니다. 여기서부터 나머지 처리는 RP 시작 SSO 트랜잭션 흐름 (페이지 104)에 설명된 것과 동일합니다.

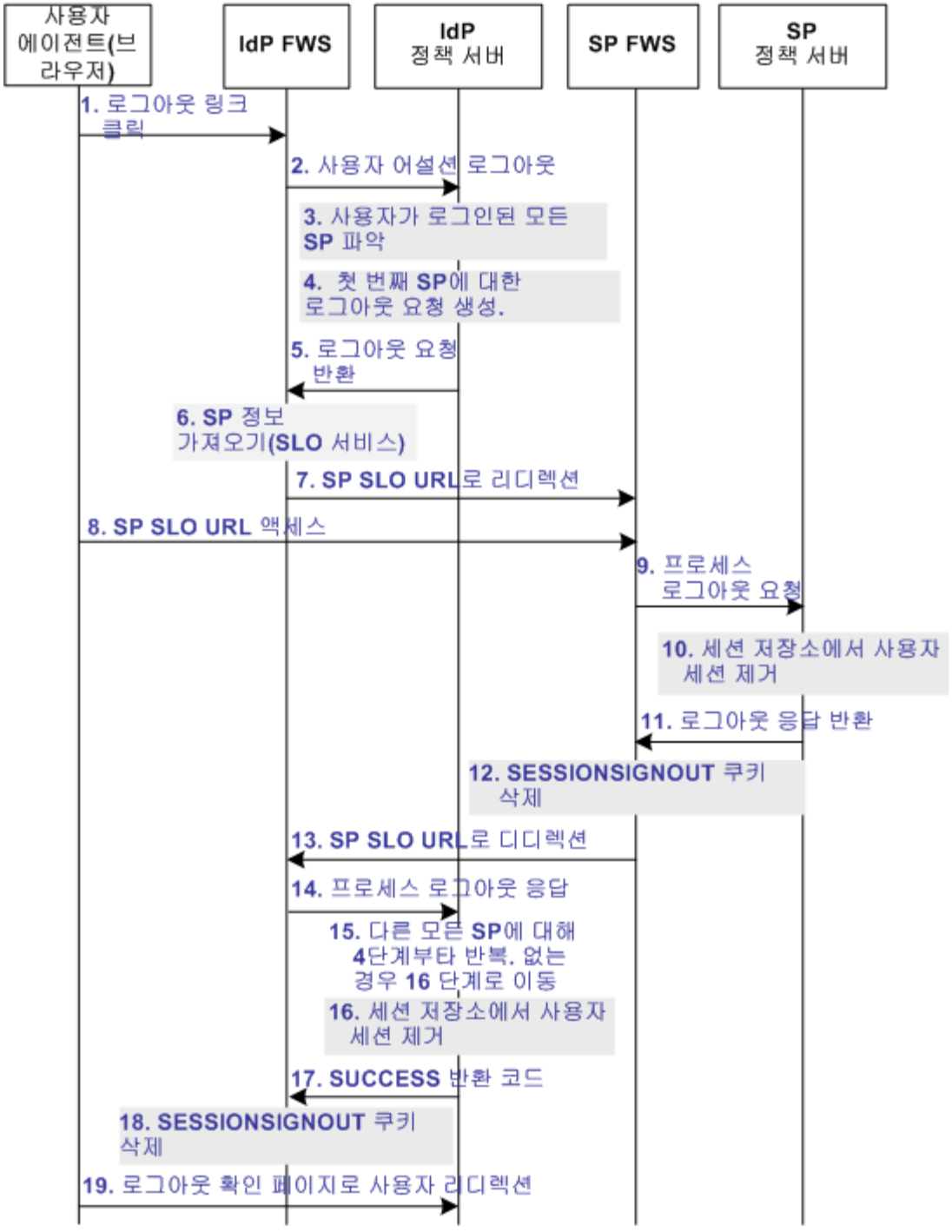
SAML 2.0 싱글 로그아웃 트랜잭션 흐름(IdP 시작)

다음 그림에서는 SiteMinder IdP(아이덴티티 공급자) 및 SP(서비스 공급자)에 배포된 구성 요소와 사용자 간의 SLO(싱글 로그아웃) 요청에 대한 상세 흐름을 보여 줍니다. 이 흐름에서는 특정 사용자의 세션이 있는 모든 엔터티에 대한 싱글 로그아웃을 보여 줍니다.

흐름도에서는 다음과 같은 정보를 사용한다고 가정합니다.

- IdP 가 로그아웃 요청을 시작합니다.
- HTTP-리디렉션 바인딩이 사용되고 있습니다.
- SiteMinder 는 IdP 및 SP 로만 표시되므로 각 파트너에서 프로세스를 볼 수 있습니다. SiteMinder 가 환경에서 SP 인 경우 표에서 SP 활동을 검토하십시오. SiteMinder 가 IDP 인 경우 표에서 IdP 활동을 검토하십시오.

다음 그림에서는 SLO 트랜잭션 흐름을 보여 줍니다. IdP 가 SLO 를 시작하면 여러 SP 에서 SLO 요청을 수신할 수 있습니다.


사용자 에이전트(브라우저)
IdP FWS
IdP 정책 서버
SP FWS
SP 정책 서버
1. 로그아웃 링크 클릭
2. 사용자 어설션 로그아웃
3. 사용자가 로그인된 모든 SP 파악
4. 첫 번째 SP에 대한 로그아웃 요청 생성.
5. 로그아웃 요청 반환
6. SP 정보 가져오기(SLO 서비스)
7. SP SLO URL로 리디렉션
8. SP SLO URL 액세스
9. 프로세스 로그아웃 요청
10. 세션 저장소에서 사용자 세션 제거
11. 로그아웃 응답 반환
12. SESSIONSIGNOUT 쿠키 삭제
13. SP SLO URL로 디디렉션
14. 프로세스 로그아웃 응답
15. 다른 모든 SP에 대해 4단계부타 반복. 없는 경우 16 단계로 이동
16. 세션 저장소에서 사용자 세션 제거
17. SUCCESS 반환 코드
18. SESSIONSIGNOUT 쿠키 삭제
19. 로그아웃 확인 페이지로 사용자 리디렉션

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

이벤트 순서는 다음과 같습니다.

작업자	트랜잭션 프로세스
IdP 역할의 SiteMinder	1. 사용자가 IdP 에서 로그아웃 링크를 클릭합니다. 브라우저가 IdP 의 싱글 로그아웃 서블릿에 액세스합니다. IdP FWS 응용 프로그램이 SMSESSION 쿠키의 이름을 SESSIONSIGNOUT 으로 변경하여 현재 사용자 세션을 무효화합니다. **로그 메시지:** Renaming session cookie to sessionsignout cookie(세션 쿠키의 이름을 sessionsignout 으로 변경합니다). **검사점 코드:** [SLO_SESSION_RENAME]
	2. IdP FWS 응용 프로그램이 SESSIONSIGNOUT 쿠키에서 SessionID 값을 읽고 요청을 IdP 정책 서버에 보내 사용자 세션을 종료합니다. **로그 메시지:** Fetching session details from cookie(세션 상세 정보를 쿠키에서 가져옵니다). **검사점 코드:** [SLO_SESSION_FETCH] 요청 유형(GET 또는 POST)에 따라 해당 검사점 메시지 중 하나가 로깅됩니다. **로그 메시지:** Receiving request at SAML2 SLO Logout URL through GET method(GET 메서드를 통해 SAML2 SLO 로그아웃 URL 에서 요청을 수신합니다). **검사점 코드:** [SLOSAML2_LOGOUTSERVICEGET_RECEIVE] 또는 **로그 메시지:** Receiving request at SAML2 SLO Logout URL through POST method(POST 메서드를 통해 SAML2 SLO 로그아웃 URL 에서 요청을 수신합니다). **검사점 코드:** [SLOSAML2_LOGOUTSERVICEPOST_RECEIVE]
	3. IdP 정책 서버가 사용자가 로그인된 모든 SP 를 확인합니다.

작업자	트랜잭션 프로세스
	4. 세션 저장소 정보를 기반으로 목록에 있는 첫 번째 SP 의 사용자 세션 상태가 LogoutInProgress 상태로 변경됩니다. 정책 서버가 LogoutRequest 요청을 생성하여 SP 의 사용자 세션을 무효화합니다. **로그 메시지**: Generating SAML LogoutRequest(SAML LogoutRequest 를 생성합니다). **검사점 코드:** [SLO_LOGOUTREQUEST_GEN]
	5. 정책 서버가 LogoutRequest 요청을 IdP FWS 에 반환합니다. 정책 서버가 SP 의 공급자 ID 와 공급자 유형도 반환합니다. **로그 메시지**: Generating SAML LogoutRequest(SAML LogoutRequest 를 생성합니다). **검사점 코드:** [SLO_LOGOUTREQUEST_GEN]
	6. IdP FWS 응용 프로그램이 정책 서버에서 SP 의 공급자 구성 데이터를 검색합니다. 이 데이터에는 SP 의 SLO 서비스 URL 이 포함됩니다. **로그 메시지**: Fetching provider information(공급자 정보를 가져옵니다). **검사점 코드**: [SLOSAML2_PROVIDERINFO_FETCH]
	7. IdP FWS 응용 프로그램이 쿼리 매개 변수로 추가된 LogoutRequest 메시지와 함께 사용자를 SP SLO 서비스로 리디렉션합니다. **로그 메시지**: Redirecting to service providers single logout service url(서비스 공급자 싱글 로그아웃 서비스 URL 로 리디렉션합니다). **검사점 코드**: [SLOSAML2_SPSLOSERVICEURL_FORWARD]
사용자 에이전트(브라우저)	8. 브라우저가 SP 의 SLO 서비스에 액세스합니다.

작업자	트랜잭션 프로세스
SP 역할의 SiteMinder	9. SP FWS 응용 프로그램이 LogoutRequest 메시지를 받고 처리합니다. **로그 메시지:** Receiving request at SAML2 SLO Logout URL through GET method(GET 메서드를 통해 SAML2 SLO 로그아웃 URL 에서 요청을 수신합니다). **검사점 코드:** [SLOSAML2_LOGOUTSERVICEGET_RECEIVE] 또는 **로그 메시지:** Receiving request at SAML2 SLO Logout URL through POST method(POST 메서드를 통해 SAML2 SLO 로그아웃 URL 에서 요청을 수신합니다). **검사점 코드:** [SLOSAML2_LOGOUTSERVICEPOST_RECEIVE] SP 가 SMSESSION 쿠키의 이름을 SESSIONSIGNOUT 으로 변경합니다. **로그 메시지:** Renaming session cookie to sessionsignout cookie(세션 쿠키의 이름을 sessionsignout 으로 변경합니다). **검사점 코드:** [SLO_SESSION_RENAME]
	10. SP 가 SP 세션 저장소에서 사용자 세션을 제거합니다. **로그 메시지:** Logging out session cookie(세션 쿠키를 로그아웃합니다). **검사점 코드**: [SLO_SESSIONCOOKIE_LOGOUT] **로그 메시지:** Terminating user session from session store(세션 저장소에서 사용자 세션을 종료합니다). **검사점 코드**: [SLO_USERSESSION_TERMINATE]
	11. SP 정책 서버가 서명된 LogoutResponse 메시지를 SP FWS 응용 프로그램에 반환합니다. 이 응답에는 IdP 의 공급자 ID 와 공급자 유형이 포함됩니다. 또한 정책 서버는 해당 사용자 세션이 더 이상 세션 저장소에 없음을 응용 프로그램에 알립니다. **로그 메시지**: Generating SAML LogoutResponse(SAML LogoutResponse 를 생성합니다). **검사점 코드**: [SLO_LOGOUTRESPONSE_GEN]
	12. 사용자 세션이 세션 저장소에서 제거되었음을 알게 된 후 SP FWS 응용 프로그램이 SESSIONSIGNOUT 쿠키를 삭제합니다. **로그 메시지:** Terminating user session from session store(세션 저장소에서 사용자 세션을 종료합니다). **검사점 코드**: [SLO_USERSESSION_TERMINATE]

작업자	트랜잭션 프로세스
	13. SP FWS 응용 프로그램이 쿼리 매개 변수로 추가된 LogoutResponse 메시지와 함께 사용자를 IdP SLO 서비스로 리디렉션합니다. 브라우저가 IdP 의 SLO 서비스에 액세스합니다. SLO 서비스가 서명된 LogoutResponse 메시지를 처리합니다. **참고:** LogoutResponse 메시지에 SUCCESS 가 아닌 반환 코드가 포함되는 경우 SP 가 SIGNOUTFAILURE 쿠키를 생성합니다. Base 64 로 인코딩된 파트너 ID 가 쿠키 값에 추가됩니다. 쿠키에 여러 ID 가 있는 경우에는 ID 가 공백 문자로 구분됩니다. **로그 메시지:** Redirecting to identity provider single logout service url(아이덴티티 공급자 싱글 로그아웃 서비스 URL 로 리디렉션합니다). **검사점 코드**: [SLOSAML2_IDPSLOSERVICEURL_FORWARD]
IdP 역할의 SiteMinder	14. IdP 정책 서버가 LogoutResponse 메시지를 받고 처리합니다.
	15. SP 정책 서버가 세션 저장소에서 사용자 세션을 제거합니다. **로그 메시지:** Terminating user session from session store(세션 저장소에서 사용자 세션을 종료합니다). **검사점 코드:** [SLO_USERSESSION_TERMINATE]
	16. IdP 정책 서버가 추가 SP 를 확인합니다. 추가 SP 가 있을 경우 흐름이 4 단계부터 반복됩니다. 그렇지 않으면 프로세스가 다음 단계로 진행됩니다.
	17. 세션이 세션 저장소에서 제거된 후 IdP 정책 서버가 SUCCESS 반환 코드를 FWS 응용 프로그램에 보냅니다. 정책 서버가 SP ID 를 최종 LogoutResponse 메시지에 포함합니다.
	18. 처리할 LogoutRequest 또는 LogoutResponse 메시지가 더 이상 없으면 IdP FWS 응용 프로그램이 SESSIONSIGNOUT 쿠키를 삭제합니다.
	19. 브라우저가 사용자를 SP 의 로그아웃 확인 페이지로 리디렉션합니다. **로그 메시지:** Redirecting to SLO confirmation URL(SLO 확인 URL 로 리디렉션합니다). **검사점 코드**: [SLOSAML2_LOGOUTCONFIRMURL_REDIRECT] **로그 메시지:** Displaying local logout message / URL(로컬 로그아웃 메시지/URL 을 표시합니다). **검사점 코드:** [SLO_LOCALLOGOUT_DISPLAY]

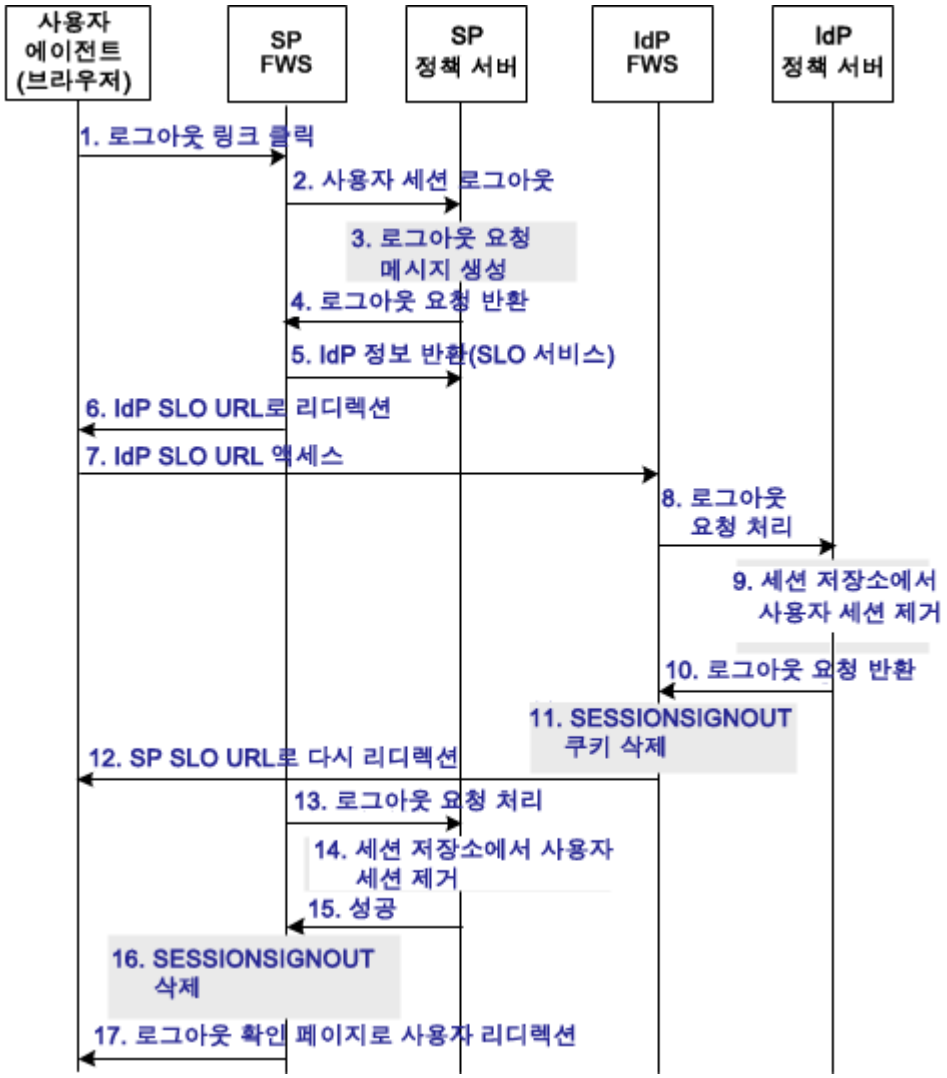
SAML 2.0 싱글 로그아웃 트랜잭션 흐름(SP 시작)

다음 그림에서는 SiteMinder IdP(아이덴티티 공급자) 및 SP(서비스 공급자)에 배포된 구성 요소와 사용자 간의 SLO(싱글 로그아웃) 요청에 대한 상세 흐름을 보여 줍니다. 이 흐름에서는 특정 사용자의 세션이 있는 모든 엔터티에 대한 싱글 로그아웃을 보여 줍니다.

흐름도에서는 다음과 같은 정보를 사용한다고 가정합니다.

- SP 가 로그아웃 요청을 시작합니다.
- HTTP-리디렉션 바인딩이 사용되고 있습니다.
- SiteMinder 는 IdP 및 SP 로만 표시되므로 각 파트너에서 프로세스를 볼 수 있습니다. SiteMinder 가 환경에서 SP 인 경우 표에서 SP 활동을 검토하십시오. SiteMinder 가 IDP 인 경우 표에서 IdP 활동을 검토하십시오.

다음 그림에서는 SLO 트랜잭션 흐름을 보여 줍니다.



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

이벤트 순서는 다음과 같습니다.

작업자	트랜잭션 프로세스
SP 역할의 SiteMinder	1. 사용자가 SP 에서 로그아웃 링크를 클릭합니다. 브라우저가 SP 의 싱글 로그아웃 서블릿에 액세스합니다. SP FWS 응용 프로그램이 SMSESSION 쿠키의 이름을 SESSIONSIGNOUT 으로 변경하여 현재 사용자 세션을 무효화합니다. **로그 메시지:** Renaming session cookie to sessionsignout cookie(세션 쿠키의 이름을 sessionsignout 으로 변경합니다). **검사점 코드:** [SLO_SESSION_RENAME]
	2. FWS 응용 프로그램이 SESSIONSIGNOUT 쿠키에서 SessionId 값을 읽고 요청을 정책 서버에 보내 사용자 세션을 종료합니다. **로그 메시지:** Fetching session details from cookie(세션 상세 정보를 쿠키에서 가져옵니다). **검사점 코드:** [SLO_SESSION_FETCH] 요청 유형(GET 또는 POST)에 따라 해당 검사점 메시지 중 하나가 로깅됩니다. **로그 메시지:** Receiving request at SAML2 SLO Logout URL through GET method(GET 메서드를 통해 SAML2 SLO 로그아웃 URL 에서 요청을 수신합니다). **검사점 코드:** [SLOSAML2_LOGOUTSERVICEGET_RECEIVE] 또는 **로그 메시지:** Receiving request at SAML2 SLO Logout URL through POST method(POST 메서드를 통해 SAML2 SLO 로그아웃 URL 에서 요청을 수신합니다). **검사점 코드:** [SLOSAML2_LOGOUTSERVICEPOST_RECEIVE]

작업자	트랜잭션 프로세스
	3. 세션 저장소 정보를 기반으로 사용자 세션 상태가 LogoutInProgress 상태로 변경됩니다. 정책 서버가 IdP 에서 수신한 어설션을 기반으로 사용자 세션이 생성되었는지 확인합니다. 정책 서버가 LogoutRequest 요청을 생성하여 IdP 의 사용자 세션을 무효화합니다. **로그 메시지**: Generating SAML LogoutRequest(SAML LogoutRequest 를 생성합니다). **검사점 코드:** [SLO_LOGOUTREQUEST_GEN] **로그 메시지**: Identifying providers associated with user session for single logout(싱글 로그아웃에 대해 사용자 세션과 연결된 공급자를 확인합니다). **검사점 코드:** [SLO_PROVIDERFORLOGOUT_IDENTIFY]
	4. 정책 서버가 LogoutRequest 요청을 SP FWS 에 반환합니다. 정책 서버가 IdP 의 공급자 ID 와 공급자 유형도 반환합니다. **로그 메시지**: Generating SAML LogoutRequest(SAML LogoutRequest 를 생성합니다). **검사점 코드:** [SLO_LOGOUTREQUEST_GEN]
	5. SP FWS 응용 프로그램이 정책 서버에서 IdP 의 공급자 구성 데이터를 검색합니다. 이 데이터에는 IdP 의 SLO 서비스 URL 이 포함됩니다. **로그 메시지**: Fetching provider information(공급자 정보를 가져옵니다). **검사점 코드**: [SLOSAML2_PROVIDERINFO_FETCH]
	6. SP FWS 응용 프로그램이 쿼리 매개 변수로 추가된 SAML LogoutRequest 메시지와 함께 사용자를 IdP 의 SLO 서비스로 리디렉션합니다. **로그 메시지:** Redirecting to identity provider single logout service url(아이덴티티 공급자 싱글 로그아웃 서비스 URL 로 리디렉션합니다). **검사점 코드**: [SLOSAML2_IDPSLOSERVICEURL_FORWARD]
사용자 에이전트(브라우저)	브라우저가 IdP 의 SLO 서비스에 액세스합니다.

작업자	트랜잭션 프로세스
IdP 역할의 SiteMinder	7. IdP FWS 응용 프로그램이 LogoutRequest 메시지를 받습니다. 요청 유형(GET 또는 POST)에 따라 해당 검사점 메시지 중 하나가 로깅됩니다. **로그 메시지:** Receiving request at SAML2 SLO Logout URL through GET method(GET 메서드를 통해 SAML2 SLO 로그아웃 URL 에서 요청을 수신합니다). **검사점 코드:** [SLOSAML2_LOGOUTSERVICEGET_RECEIVE] 또는 **로그 메시지:** Receiving request at SAML2 SLO Logout URL through POST method(POST 메서드를 통해 SAML2 SLO 로그아웃 URL 에서 요청을 수신합니다). **검사점 코드:** [SLOSAML2_LOGOUTSERVICEPOST_RECEIVE] IdP 가 SMSESSION 쿠키의 이름을 SESSIONSIGNOUT 으로 변경합니다. **로그 메시지:** Renaming session cookie to sessionsignout cookie(세션 쿠키의 이름을 sessionsignout 으로 변경합니다). **검사점 코드:** [SLO_SESSION_RENAME]
	8. IdP 가 서명된 LogoutRequest 메시지를 처리합니다. 그런 다음 IdP 가 해당 세션의 세션 저장소에 지정된 모든 SP 에서 사용자 세션을 무효화하려고 합니다. 무효화되지 않는 SP 는 원래 LogoutRequest 를 보낸 SP 뿐입니다. **참고:** 각 SP 에서 사용자를 로그아웃하는 프로세스는 2-7 단계에서 동일합니다. **로그 메시지:** Logging out session cookie(세션 쿠키를 로그아웃합니다). **검사점 코드**: [SLO_SESSIONCOOKIE_LOGOUT]

작업자	트랜잭션 프로세스
IdP 로서 SiteMinder (계속)	9. 모든 관련 SP 에서 사용자 세션을 종료한 후 IdP 가 세션 저장소에서 사용자 세션을 제거합니다. **로그 메시지:** Terminating user session from session store(세션 저장소에서 사용자 세션을 종료합니다). **검사점 코드**: [SLO_USERSESSION_TERMINATE] 10. IdP 정책 서버가 서명된 LogoutResponse 메시지를 IdP FWS 응용 프로그램에 반환합니다. 이 응답에는 SP 의 공급자 ID 와 공급자 유형이 포함됩니다. 또한 IdP 정책 서버는 해당 사용자 세션이 더 이상 세션 저장소에 없음을 응용 프로그램에 알립니다. **로그 메시지**: Generating SAML LogoutResponse(SAML LogoutResponse 를 생성합니다). **검사점 코드**: [SLO_LOGOUTRESPONSE_GEN]
	11. 사용자 세션이 세션 저장소에서 제거되었음을 알게 된 후 IdP FWS 응용 프로그램이 SESSIONSIGNOUT 쿠키를 삭제합니다.
	12. IdP 가 쿼리 매개 변수로 추가된 LogoutResponse 메시지와 함께 사용자를 SP 의 싱글 로그아웃 서비스로 리디렉션합니다. 브라우저가 SP 의 SLO 서비스에 액세스합니다. SLO 서비스가 서명된 LogoutResponse 메시지를 처리합니다. **참고:** LogoutResponse 메시지에 SUCCESS 가 아닌 반환 코드가 포함된 경우 SP 가 SIGNOUTFAILURE 쿠키를 발급하고 Base 64 로 인코딩된 파트너 ID 가 쿠키 값에 추가됩니다. 쿠키에 여러 ID 가 있는 경우에는 ID 가 공백 문자로 구분됩니다. **로그 메시지**: Redirecting to service providers single logout service url(서비스 공급자 싱글 로그아웃 서비스 URL 로 리디렉션합니다). **검사점 코드**: [SLOSAML2_SPSLOSERVICEURL_FORWARD]
SP 역할의 SiteMinder	13. SP 정책 서버가 FWS 응용 프로그램에서 LogoutResponse 메시지를 받고 처리합니다.
	14. SP 정책 서버가 세션 저장소에서 사용자 세션을 제거합니다. **로그 메시지:** Terminating user session from session store(세션 저장소에서 사용자 세션을 종료합니다). **검사점 코드:** [SLO_USERSESSION_TERMINATE]
SP 로서 SiteMinder (계속)	15. 세션이 세션 저장소에서 제거된 후 정책 서버가 SUCCESS 반환 코드를 FWS 응용 프로그램에 보냅니다. 정책 서버가 SP ID 를 최종 LogoutResponse 메시지에 포함합니다.

작업자	트랜잭션 프로세스
	16. 처리할 LogoutRequest 또는 LogoutResponse 메시지가 더 이상 없으면 SP FWS 응용 프로그램이 SESSIONSIGNOUT 쿠키를 삭제합니다.
	17. FWS 가 사용자를 SP 의 로그아웃 확인 페이지로 리디렉션합니다. **로그 메시지**: Redirecting to SLO confirmation URL(SLO 확인 URL 로 리디렉션합니다). **검사점 코드**: [SLOSAML2_LOGOUTCONFIRMURL_REDIRECT] **로그 메시지:** Displaying local logout message / URL(로컬 로그아웃 메시지/URL 을 표시합니다). **검사점 코드:** [SLO_LOCALLOGOUT_DISPLAY]

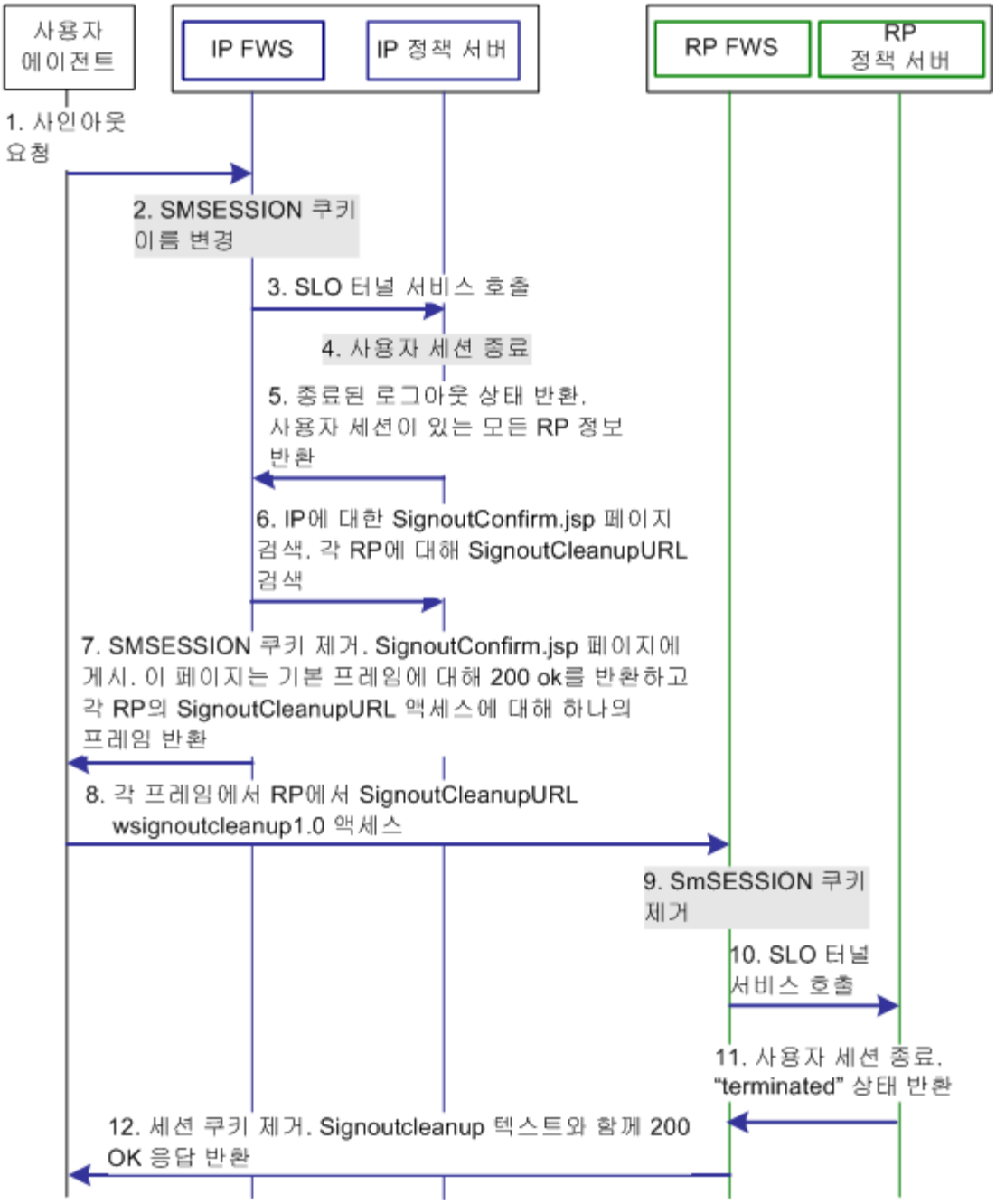
WS-페더레이션 사인아웃 트랜잭션 흐름(IP 시작)

다음 그림에서는 IP(아이덴티티 공급자) 및 RP(리소스 파트너)에 배포된 구성 요소와 사용자 간의 사인아웃 요청 흐름을 보여 줍니다. 이 흐름에서는 특정 사용자의 세션이 있는 모든 WS-페더레이션 엔터티에 대한 사인아웃 트랜잭션을 보여 줍니다.

흐름도에서는 다음과 같은 정보를 사용한다고 가정합니다.

- IP 가 사인아웃 트랜잭션을 시작합니다.
- SiteMinder 는 IP 및 RP 로 표시되므로 각 파트너에서 프로세스를 볼 수 있습니다. SiteMinder 가 환경에서 IP 인 경우 표에서 IP 활동을 검토하십시오. SiteMinder 가 RP 인 경우 표에서 RP 활동을 검토하십시오.

다음 그림에서는 WS-페더레이션 사인아웃 트랜잭션 흐름을 보여 줍니다.



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

사인아웃이 아이덴티티 공급자에서 시작되는 경우 이벤트 순서는 다음과 같습니다.

작업자	트랜잭션 프로세스
IP 역할의 SiteMinder	1. 사용자가 전역 세션을 종료하기 위해 IP 에 있는 링크를 클릭합니다. 브라우저가 HTTP 기반 wsignout 요청을 IP 의 사인아웃 서블릿에 보냅니다.
	2. IP FWS 응용 프로그램이 SMSESSION 쿠키의 이름을 SESSIONSIGNOUT 으로 변경하여 현재 사용자 세션을 무효화합니다. **로그 메시지:** Renaming session cookie to sessionsignout cookie(세션 쿠키의 이름을 sessionsignout 으로 변경합니다). **검사점 코드:** [SLO_SESSION_RENAME]
	3. IP FWS 가 SESSIONSIGNOUT 쿠키에서 SessionId 값을 읽고 SLO 터널 서비스 API 를 호출하여 사용자 세션을 종료합니다. **로그 메시지:** Fetching session details from cookie(세션 상세 정보를 쿠키에서 가져옵니다). **검사점 메시지:** SLO_SESSION_FETCH **로그 메시지:** Performing tunnel call for WSFED signout(WSFED 사인아웃을 위해 터널 호출을 수행합니다). **검사점 코드:** [SLOWSFED_TUNNEL_REQUEST]
	4. SLO 터널 서비스 API 가 세션 저장소에서 사용자 세션 상태를 "Terminated"(종료됨)로 설정합니다. 또한 서비스가 세션 저장소에서 해당 사용자 세션과 연결된 RP 참조를 모두 제거합니다. **로그 메시지**: Setting session to inactive assuming a cleanup state(삭제 상태를 가정하는 비활성 상태로 세션을 설정합니다). **검사점 코드:** [SLOWSFED_INACTIVESTATE_SET]
	5. SLO 터널 서비스 API 가 로그아웃 상태 "Terminated"(종료됨)를 FWS 사인아웃 서블릿에 반환합니다. 또한 터널 라이브러리가 사용자 세션과 연결된 모든 RP 의 RP providerID 및 providerType 을 반환합니다. **로그 메시지:** Terminating user session from session store(세션 저장소에서 사용자 세션을 종료합니다). **검사점 코드**: [SLO_USERSESSION_TERMINATE]

작업자	트랜잭션 프로세스
	6. IP FWS 응용 프로그램이 FWS 가 유지 관리하는 공급자의 캐시에서 RP 의 공급자 구성 데이터를 검색합니다. 이 정보에는 사인아웃 삭제 URL 이 포함됩니다. **로그 메시지**: Validate GET request for necessary parameters(GET 요청에서 필요한 매개 변수를 확인합니다). **검사점 코드**: [SLOWSFED_GETREQUEST_VALIDATE]
	7. IP FWS 가 SESSIONSIGNOUT 쿠키를 제거하고 IP 사인아웃 메시지와 여러 RP-SignoutCleanup 위치를 SignoutConfirmURL JSP 에 POST 데이터로 포스트합니다. **로그 메시지:** Logging out session cookie(세션 쿠키를 로그아웃합니다). **검사점 코드:** [SLO_SESSIONCOOKIE_LOGOUT] SignoutConfirmURL JSP 는 다양한 post 변수 구문 분석과 프레임 기반 HTML 페이지 생성을 담당합니다. 이 HTML 페이지의 메인 프레임에는 IP-사인아웃 메시지가 표시됩니다. 나머지 프레임은 각각 사용자 세션과 연결된 개별 RP 의 SignoutCleanupURL 에 액세스합니다. **로그 메시지**: Sending signout message to Identity Provider (Account Partner)(사인아웃 메시지를 아이덴티티 공급자(계정 파트너)에 보냅니다). **검사점 코드**: [SLOWSFED_IDPSIGNOUTMSG_SEND] **로그 메시지**: Redirecting to signout confirmation URL(사인아웃 확인 URL 로 리디렉션합니다). **검사점 코드**: [SLOWSFED_LOGOUTCONFIRMURL_REDIRECT]
사용자 에이전트(브라우저)	8. 브라우저가 RP 의 SignoutCleanup 서비스에 액세스합니다.
RP 역할의 SiteMinder	9. wsignoutcleanup 요청을 받은 경우 RP FWS 응용 프로그램이 SMSESSION 쿠키의 이름을 SESSIONSIGNOUT 으로 변경합니다. 그런 다음 FWS 가 SLO 터널 서비스 API 를 호출하여 wSignoutCleanup 요청을 처리합니다. **로그 메시지:** Renaming session cookie to sessionsignout cookie(세션 쿠키의 이름을 sessionsignout 으로 변경합니다). **검사점 코드:** [SLO_SESSION_RENAME] **로그 메시지:** Receiving signout request at WSEFD through GET method(GET 메서드를 통해 WSEFD 에서 사인아웃 요청을 수신합니다). **검사점 코드:** [SLOWSFED_LOGOUTSERVICEGET_RECEIVE]

작업자	트랜잭션 프로세스
	10. SLO 터널 라이브러리가 wSignoutCleanup 요청을 처리하고 세션 저장소에서 사용자 세션을 종료합니다. **로그 메시지:** Terminating user session from session store(세션 저장소에서 사용자 세션을 종료합니다). **검사점 코드:** [SLO_USERSESSION_TERMINATE]
	11. SLO 터널 라이브러리가 세션 저장소에 사용자 세션이 더 이상 존재하지 않음을 나타내는 "Terminated"(종료됨) 상태 메시지와 함께 FWS 를 반환합니다. **로그 메시지:** Logging out session cookie(세션 쿠키를 로그아웃합니다). **검사점 코드:** [SLO_SESSIONCOOKIE_LOGOUT]
	12. FWS 사인아웃 서블릿이 SESSIONSIGNOUT 쿠키를 제거하고 프레임에서 200 OK 응답을 반환합니다. **로그 메시지:** Displaying local logout message / URL(로컬 로그아웃 메시지/URL 을 표시합니다). **검사점 메시지:** [SLO_LOCALLOGOUT_DISPLAY]

참고: 8-12 단계는 동일한 HTML 페이지의 다른 프레임에서 개별 RP 에 대해 동시에 반복됩니다.

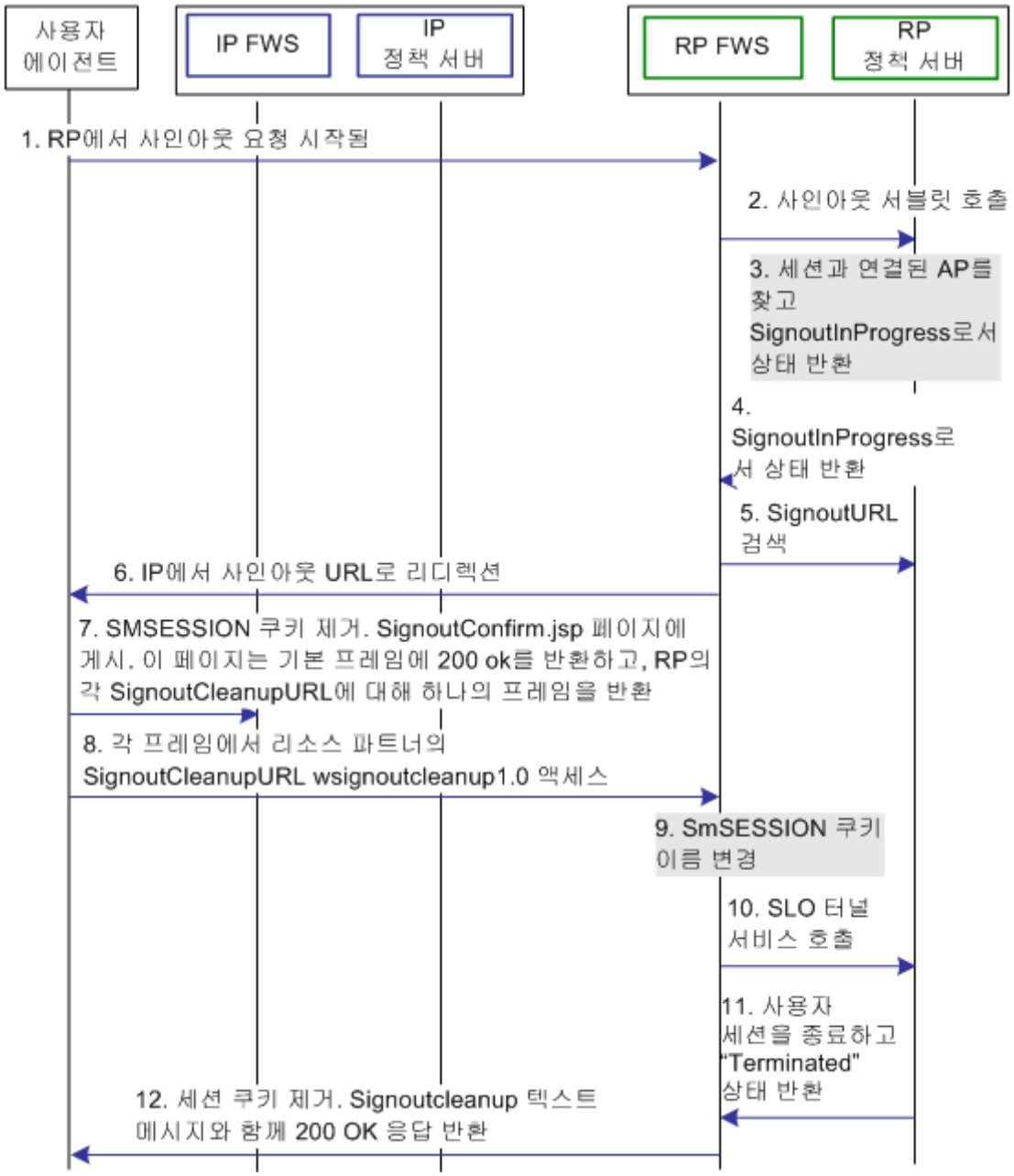
WS-페더레이션 사인아웃 트랜잭션 흐름(RP 시작)

다음 그림에서는 IP(아이덴티티 공급자) 및 RP(리소스 파트너)에 배포된 구성 요소와 사용자 간의 사인아웃 요청 흐름을 보여 줍니다. 이 흐름에서는 특정 사용자의 세션이 있는 모든 WS-페더레이션 엔터티에 대한 사인아웃 트랜잭션을 보여 줍니다.

흐름도에서는 다음과 같은 정보를 사용한다고 가정합니다.

- RP 가 사인아웃 트랜잭션을 시작합니다.
- SiteMinder 는 IP 및 RP 로 표시되므로 각 파트너에서 프로세스를 볼 수 있습니다. SiteMinder 가 환경에서 IP 인 경우 표에서 IP 활동을 검토하십시오. SiteMinder 가 RP 인 경우 표에서 RP 활동을 검토하십시오.

다음 그림에서는 사인아웃 요청 트랜잭션 흐름을 보여 줍니다.



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

사인아웃이 리소스 파트너에서 시작된 경우 프로세스 흐름은 다음과 같습니다.

작업자	트랜잭션 프로세스
RP 역할의 SiteMinder	1. 사용자가 전역 세션을 종료하기 위해 리소스 파트너에 있는 링크를 클릭합니다. 브라우저가 HTTP 기반 wsignout 요청을 리소스 파트너의 사인아웃 서블릿에 보냅니다. **참고:** RP 사이트는 wSignoutCleanup 메시지가 아닌 wsignout 메시지를 받고 있습니다.
	2. RP FWS 응용 프로그램이 SMSESSION 쿠키에서 SessionId 값을 읽습니다. 응용 프로그램이 SMSESSION 쿠키의 이름을 SESSIONSIGNOUT 으로 변경하고 wsignout 요청을 사용하여 SLO 터널 라이브러리를 호출합니다. **로그 메시지:** Renaming session cookie to sessionsignout cookie(세션 쿠키의 이름을 sessionsignout 으로 변경합니다). **검사점 코드:** [SLO_SESSION_RENAME] **로그 메시지:** Performing tunnel call for WSFED signout(WSFED 사인아웃을 위해 터널 호출을 수행합니다). **검사점 코드:** [SLOWSFED_TUNNEL_REQUEST]
	3. 세션 저장소에 있는 정보를 기반으로 터널 라이브러리가 사용자 세션과 연결된 IP 를 확인합니다. SLO 터널 라이브러리가 사용자 세션 상태를 SignoutInProgress 로 설정하지만 사용자 세션을 종료하지는 않습니다. **로그 메시지:** Sending signout message and awaiting response from ap for cleanup(사인아웃 메시지를 보내고 삭제를 위해 ap 의 응답을 기다립니다). **검사점 코드:** [SLOWSFED_AWAITINGRESPONSE_SEND]
	4. 터널 라이브러리가 SignoutInProgress 상태 메시지와 IP providerID 및 providerType 을 반환합니다. **로그 메시지**: Performing tunnel call for WSFED signout(WSFED 사인아웃을 위해 터널 호출을 수행합니다). **검사점 코드:** [SLOWSFED_TUNNEL_REQUEST]

작업자	트랜잭션 프로세스
	5. RP FWS 응용 프로그램이 FWS 캐시 또는 정책 서버에서 사인아웃 URL 이 포함된 IP 구성 데이터를 검색합니다.
	6. RP FWS 응용 프로그램이 브라우저를 사인아웃 URL 로 리디렉션합니다. wsignoutcleanup 요청을 받은 경우 RP FWS(사인아웃 서블릿)가 SMSESSION 쿠키의 이름을 SESSIONSIGNOUT 으로 변경합니다. 그런 다음 서비스가 SLO 터널 서비스 API 를 호출하여 wSignoutCleanup 요청을 처리합니다. **로그 메시지**: Redirecting to signout confirmation URL(사인아웃 확인 URL 로 리디렉션합니다). **검사점 코드**: [SLOWSFED_LOGOUTCONFIRMURL_REDIRECT]
IP 역할의 SiteMinder	7. IP FWS 응용 프로그램이 SESSIONSIGNOUT 쿠키를 제거한 다음 IP 사인아웃 메시지와 여러 RP-SignoutCleanup 위치를 SignoutConfirmURL JSP 에 post 데이터로 포스트합니다. SignoutConfirmURL JSP 는 다양한 post 변수 구문 분석과 프레임 기반 HTML 페이지 생성을 담당합니다. 이 HTML 페이지의 기본 프레임에는 IP-사인아웃 메시지가 표시됩니다. 나머지 프레임은 각각 사용자 세션과 연결된 개별 RP 의 SignoutCleanupURL 에 액세스합니다. **로그 메시지:** Sending signout message and awaiting response from ap for cleanup(사인아웃 메시지를 보내고 삭제를 위해 ap 의 응답을 기다립니다). **검사점 코드**: [SLOWSFED_AWAITINGRESPONSE_SEND] **로그 메시지**: Sending signout cleanup message(사인아웃 삭제 메시지를 보냅니다). **검사점 코드:** [SLOWSFED_CLEANUPMESSAGE_SEND]
사용자 에이전트(브라우저)	8. 브라우저가 개별 프레임에서 리소스 파트너 사이트의 SignoutCleanup 서비스에 액세스합니다.

작업자	트랜잭션 프로세스
RP 로서 SiteMinder (계속)	9. wsignoutcleanup 요청을 받은 경우 RP FWS(사인아웃 서블릿)가 SMSESSION 쿠키의 이름을 SESSIONSIGNOUT 으로 변경합니다. 그런 다음 서비스가 SLO 터널 서비스 API 를 호출하여 wSignoutCleanup 요청을 처리합니다. **로그 메시지:** Renaming session cookie to sessionsignout cookie(세션 쿠키의 이름을 sessionsignout 으로 변경합니다). **검사점 코드:** [SLO_SESSION_RENAME]
	10. SLO 터널 라이브러리가 wSignoutCleanup 요청을 처리하고 세션 저장소에서 사용자 세션을 종료합니다. **로그 메시지:** Terminating user session from session store(세션 저장소에서 사용자 세션을 종료합니다). **검사점 코드**: [SLO_USERSESSION_TERMINATE] 11. 그런 다음 SLO 터널 라이브러리가 세션 저장소에 사용자 세션이 더 이상 존재하지 않음을 나타내는 "Terminated"(종료됨) 상태 메시지와 함께 FWS 를 반환합니다. **로그 메시지**: Redirecting to signout confirmation URL(사인아웃 확인 URL 로 리디렉션합니다). **검사점 코드**: [SLOWSFED_LOGOUTCONFIRMURL_REDIRECT]
	12. FWS 사인아웃 서블릿이 SESSIONSIGNOUT 쿠키를 제거하고 프레임에서 200 OK 응답을 반환합니다. **로그 메시지:** Displaying local logout message / URL(로컬 로그아웃 메시지/URL 을 표시합니다). **검사점 메시지:** [SLO_LOCALLOGOUT_DISPLAY]

참고: 8-12 단계는 동일한 HTML 페이지의 다른 프레임에서 개별 RP 에 대해 동시에 반복됩니다.

아이덴티티 공급자 검색 트랜잭션 흐름

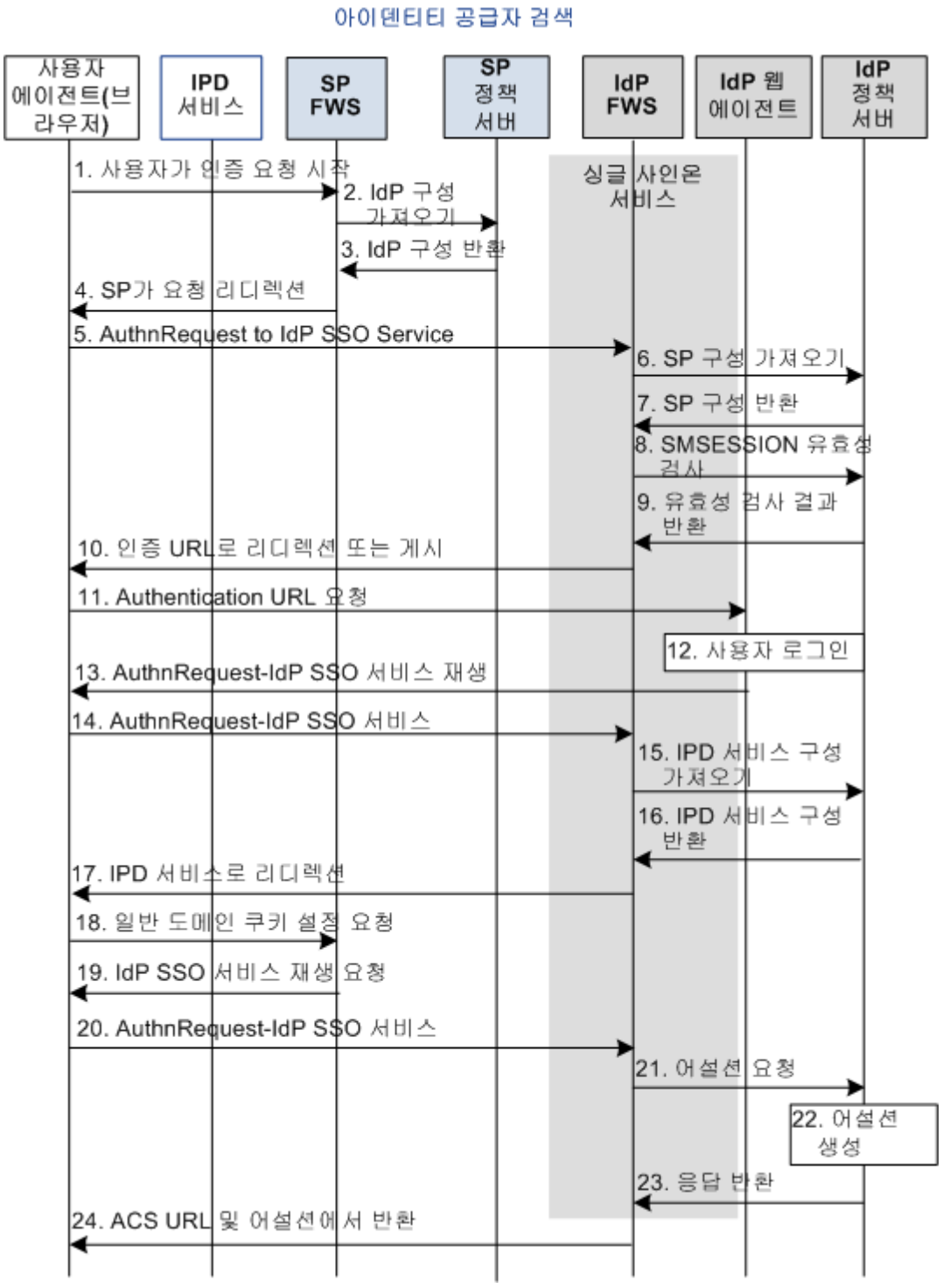
다음 그림에서는 아이덴티티 공급자 검색 프로필을 사용하는 싱글 사인온 트랜잭션의 흐름을 보여 줍니다. IPD(아이덴티티 공급자 검색) 프로필이 제공하는 공통 검색 서비스를 사용하면 서비스 공급자가 인증을 위해 고유 IdP 를 선택할 수 있습니다. 네트워크에 있는 모든 사이트가 아이덴티티 공급자 검색 서비스와 상호 작용하도록 파트너 간의 사전 비즈니스 계약이 설정되어 있습니다.

이 다이어그램에서 아이덴티티 공급자 검색 서비스는 사용자와 SiteMinder 아이덴티티 공급자의 페더레이션 구성 요소 사이에 있습니다. 이 흐름에서는 일반 도메인 쿠키를 설정하기 위해 아이덴티티 공급자의 요청을 아이덴티티 공급자 검색 서비스로 리디렉션합니다.

흐름도에서는 다음과 같은 정보를 사용한다고 가정합니다.

- SP FWS 가 트랜잭션을 시작하기 위해 사용자를 IdP SSO 서비스 URL 로 리디렉션합니다.
- SAML 2.0 HTTP POST 가 싱글 사인온 프로필입니다.
- SiteMinder 는 IdP 로 표시되므로 각 파트너에서 프로세스를 볼 수 있습니다.

다음 그림에서는 아이덴티티 공급자 검색 트랜잭션의 흐름을 보여 줍니다.


아이덴티티 공급자 검색
사용자 에이전트(브라우저)
IPD 서비스
SP FWS
SP 정책 서버
IdP FWS
IdP 웹 에이전트
IdP 정책 서버
싱글 사인온 서비스
1. 사용자가 인증 요청 시작
2. IdP 구성 가져오기
3. IdP 구성 반환
4. SP가 요청 리디렉션
5. AuthnRequest to IdP SSO Service
6. SP 구성 가져오기
7. SP 구성 반환
8. SMSESSION 유효성 검사
9. 유효성 검사 결과 반환
10. 인증 URL로 리디렉션 또는 게시
11. Authentication URL 요청
12. 사용자 로그인
13. AuthnRequest-IdP SSO 서비스 재생
14. AuthnRequest-IdP SSO 서비스
15. IPD 서비스 구성 가져오기
16. IPD 서비스 구성 반환
17. IPD 서비스로 리디렉션
18. 일반 도메인 쿠키 설정 요청
19. IdP SSO 서비스 재생 요청
20. AuthnRequest-IdP SSO 서비스
21. 어설션 요청
22. 어설션 생성
23. 응답 반환
24. ACS URL 및 어설션에서 반환

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.

아이덴티티 공급자 검색 프로세스는 다음과 같습니다.

작업자	트랜잭션 프로세스
사용자 에이전트(브라우저)	1. 사용자가 링크를 클릭하여 인증 요청을 시작합니다.
SP 역할의 SiteMinder	2. SP FWS 가 로컬 정책 서버에 IdP 구성 정보를 요청합니다. **로그 메시지:** Reading SAML 2.0 IDP Configuration(SAML 2.0 IDP 구성을 읽습니다). **검사점 코드:** [SSOSAML2_IDPCONFREAD_REQ]
	3. 로컬 정책 서버가 구성 정보를 반환합니다. **참고:** SP FWS 응용 프로그램이 이 구성 정보를 캐시할 수 있습니다. **로그 메시지:** Policy server returns SAML2.0 IDP Configuration(정책 서버가 SAML2.0 IDP 구성을 반환합니다). **검사점 코드:** [SSOSAML2_IDPCONFFROMPS_RSP]
	4. SP FWS 가 요청을 브라우저로 리디렉션합니다.
사용자 에이전트(브라우저)	5. 사용자 에이전트(브라우저)가 IdP SSO 서비스를 요청합니다.
IdP 역할의 SiteMinder	6. IdP FWS 가 로컬 정책 서버에 SP 구성 정보를 요청합니다. **로그 메시지:** SAML2.0 SP Configuration is not in cache. Requesting to get from policy server(SAML2.0 SP 구성이 캐시에 없습니다. 정책 서버에서 가져오도록 요청합니다). **검사점 코드:** [SSOSAML2_SPCONFFROMPS_REQ]
	7. 로컬 정책 서버가 구성 정보를 반환합니다. **참고:** IdP FWS 응용 프로그램이 이 구성 정보를 캐시할 수 있습니다. **로그 메시지:** Policy server returns SAML2.0 SP Configuration(정책 서버가 SAML2.0 SP 구성을 반환합니다). **검사점 코드:** [SSOSAML2_SPCONFFROMPS_RSP]

작업자	트랜잭션 프로세스
	8. IdP FWS 가 IdP 도메인에 대한 SMSESSION 쿠키를 가져오고 정책 서버를 호출하여 해당 쿠키의 유효성을 검사합니다. SMSESSION 쿠키가 없는 경우 IdP FWS 가 6 단계로 건너뜁니다. **로그 메시지:** Request to validate the session(세션 유효성 검사 요청) **검사점 코드:** [SSOSAML2_SESSIONCOOKIEVALIDATE_REQ]
	9. 정책 서버가 SMSESSION 쿠키의 유효성을 검사하고 결과를 반환합니다.
	10. SMSESSION 쿠키가 존재하지 않거나 유효하지 않은 경우 IdP FWS 가 구성에서 획득된 인증 URL 로 리디렉션하거나 해당 인증 URL 에 포스트합니다. SMSESSION 쿠키가 유효한 경우에는 IdP FWS 가 18 단계로 건너뜁니다. **로그 메시지**: Session cookie does not exists. redirecting to authentication url(세션 쿠키가 없습니다. 인증 URL 로 리디렉션합니다). **검사점 코드**: [SSOSAML2_AUTHENTICATIONURL_REDIRECT]
사용자 에이전트(브라우저)	11. 브라우저가 인증 URL 을 요청합니다. IdP 웹 에이전트가 인증 URL 을 보호합니다.
IdP 역할의 SiteMinder	12. IdP 웹 에이전트가 사용자 로그인을 수행하면서 SMSESSION 쿠키를 설정하고 요청이 인증 URL 에 전달되도록 합니다.
	13. 인증 URL 은 AuthnRequest 메시지를 사용하여 IdP SSO 서비스에 대한 요청을 재생합니다. **로그 메시지**: Policy server returns the authentication request(정책 서버가 인증 요청을 반환합니다). **검사점 코드:** [SSOSAML2_GETAUTHENTICATIONREQFROMPS_RSP] **로그 메시지**: Service redirecting to SSO URL(서비스를 SSO URL 로 리디렉션합니다). **검사점 코드:** [SSOSAML2_SSOURL_REDIRECT]
사용자 에이전트(브라우저)	14. 브라우저가 IdP SSO 서비스를 요청합니다. 이 요청은 8 단계의 요청과 동일하지만 이제 사용자의 SMSESSION 쿠키가 유효합니다.
IdP 역할의 SiteMinder	15. IdP FWS 가 정책 서버에 IPD(아이덴티티 공급자 검색 프로필) 구성을 요청하면서 아이덴티티 공급자 ID 를 전달합니다. **로그 메시지:** Request for IPD configuration(IPD 구성을 요청합니다). **검사점 코드**: [SSOIPD_READIPDCONF_REQ]

작업자	트랜잭션 프로세스
	16. 정책 서버가 IPD 서비스 URL, 일반 도메인 쿠키, 일반 도메인 쿠키 지속 정보 등의 IPD 구성을 반환합니다. **로그 메시지:** Reading IPD service URL from configuration(구성에서 IPD 서비스 URL 을 읽습니다). **검사점 코드**: [SSOIPD_READIPDSERVICEURL_REQ] **로그 메시지:** Reading common domain cookie from configuration(구성에서 일반 도메인 쿠키를 읽습니다). **검사점 코드:** [SSOIPD_READCOMMONDOMAINCOOKIE_REQ] **로그 메시지:** Reading persistence information of the common domain cookie(일반 도메인 쿠키에서 지속 정보를 읽습니다). **검사점 코드:** [SSOIPD_READPERSISTENCEINFOFORCOMMONCOOKIE_REQ]
	17. IdP FWS 응용 프로그램이 호출을 IPD 서비스 URL 로 리디렉션합니다. **로그 메시지**: Redirecting to IPD service URL(IPD 서비스 URL 로 리디렉션합니다). **검사점 코드:** SSOIPD_REDIRECTTOIPDURL_REQ
사용자 에이전트(브라우저)	18. 브라우저가 일반 도메인 쿠키를 설정하기 위해 IPD 서비스로 사용자를 리디렉션합니다.
아이덴티티 공급자 검색 서비스	19. IPD 서비스가 아이덴티티 공급자 ID 를 사용하여 일반 도메인 쿠키를 설정하거나 업데이트합니다. IPD 서비스가 설정 요청을 보낸 IdP FWS 로 사용자 에이전트를 다시 리디렉션합니다. **로그 메시지:** IPD service setting common domain cookie with identity provider id(IPD 서비스가 아이덴티티 공급자 ID 를 사용하여 일반 도메인 쿠키를 설정합니다). **검사점 코드:** [SSOIPD_SETCOMMONDOMAINCOOKIE_REQ]
사용자 에이전트(브라우저)	20. 브라우저가 IdP SSO 서비스에 요청을 제출합니다.
IdP 역할의 SiteMinder	21. IdP FWS 가 정책 서버에 SAML 2.0 어설션을 요청하면서 구성에서 획득된 영역에 대한 권한 부여 호출을 통해 AuthnRequest 를 전달합니다. **로그 메시지:** Request to policy server for generating saml2 assertion/artifact based on selected profile(선택한 프로필에 기반하여 saml2 어설션/아티팩트를 생성하도록 정책 서버에 요청합니다). **검사점 코드:** [SSOSAML2_GENERATEASSERTIONORARTIFACT_REQ]

작업자	트랜잭션 프로세스
	22. 정책 서버가 서비스 공급자의 구성 정보에 기반한 어설션을 생성합니다. 정책 서버가 어설션에 서명하고 어설션을 응답 메시지로 반환합니다. **로그 메시지:** Policy server generates the saml2 assertion(정책 서버가 saml2 어설션을 생성합니다). **검사점 코드:** [SSOSAML2_PSGENERATEASSERTION_RSP] **로그 메시지:** Policy server signs saml2 assertion(정책 서버가 saml2 어설션에 서명합니다). **검사점 코드:** [SSOSAML2_PSSIGNASSERTION_RSP]
	23. 응답 메시지가 IdP FWS 에 반환됩니다. **로그 메시지:** Received the assertion/artifact response based on profile selected(선택한 프로필에 기반하여 어설션/아티팩트 응답을 수신했습니다). **검사점 코드**: [SSOSAML2_RECEIVEDASSERTION_RSP]
	24. IdP FWS 가 응답 메시지, 구성에서 획득된 어설션 소비자 URL 및 양식을 제출할 JavaScript 가 포함된 양식을 사용자에게 반환합니다. **로그 메시지**: Browser posting the response to assertion consumer url(브라우저가 응답을 어설션 소비자 URL 에 포스트합니다). **검사점 코드:** SSOSAML2_POSTASSERTIONTOCONSUMERURL_RSP **참고:** 정책 서버가 현재 세션의 인증 수준이 너무 낮다고 나타낼 수 있습니다. 수준이 너무 낮으면 IdP FWS 가 단계별 인증 강화를 손쉽게 수행하기 위해 인증 URL 로 리디렉션합니다.

흐름도의 최종 단계가 완료된 후 사용자 에이전트가 응답 메시지를 서비스 공급자의 어설션 소비자 URL 에 포스트합니다.