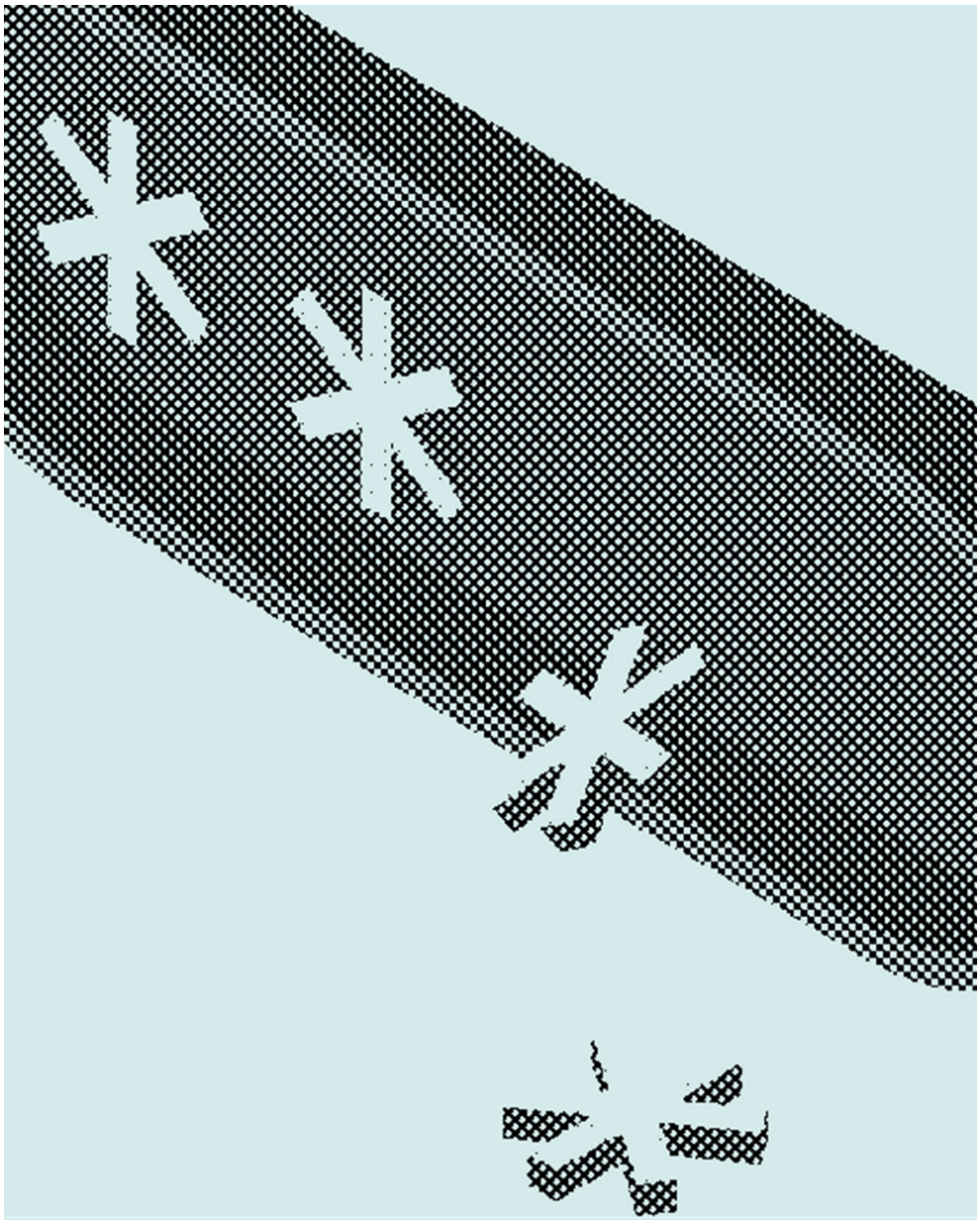
백서
2022년 3월

Okta로 Passwordless Authentication을 구축하는 방법

Okta의 Passwordless Authentication 옵션 요약 가이드

Okta Inc.
서울 강남구 테헤란로 152
강남파이낸스센터 41 층
support.okta.com



서론

Passwordless Authentication은 이미 많은 기업에서 사용 중입니다. 이제 사용자들은 Apple 터치 ID, 페이스 ID, Windows Hello와 같은 일상적인 테크놀로지를 통해 비밀번호를 입력하지 않고도 디바이스에 액세스할 수 있게 되었습니다. 그리고 회사 직원들은 지문 및 카드 판독기나 모바일 인증 앱과 같은 테크놀로지 덕분에 비밀번호 없이 로그인하게 되었습니다.

비밀번호 방식에서 탈피하는 것은 보안과 IAM(Identity Access Management)을 개선하는 데 중요한 절차이며, 모든 로그인 요청의 상황을 고려해 인증을 강화하는 것도 이에 못지않게 중요합니다.

문제는 이 Passwordless Authentication을 구현하는 방식입니다. MFA(Multi-Factor Authentication) 구현은 궁극적으로 Passwordless Authentication을 구축하기 위한 훌륭한 기반이 됩니다. FIDO2.0/WebAuthn나 생체 인증을 지원하는 모바일 인증 앱과 같은 보안 인증요소들은 Passwordless Authentication을 전사적으로 구축할 수 있는 길을 열어줍니다. 이러한 보안 인증요소를 로그인 컨텍스트와 함께 사용하면 인증 프로세스에서 비밀번호 요건을 생략할 수 있습니다.

이 과정을 Okta가 도와드리겠습니다. 기업은 Okta에 통합된 SSO(Single Sign-On)와 적응형 MFA 솔루션을 통해 Passwordless Authentication을 포함한 액세스 결정 시 컨텍스트(사용자, 위치, 디바이스, 네트워크 등)에서 도출된 위험 평가 결과를 고려할 수 있습니다.

예를 들어, 위험 수준이 낮은 로그인 환경에서만 Passwordless Authentication을 허용하도록 선택할 수 있습니다. 그리고 위험 수준이 높은 로그인 환경에서는 강력한 인증요소를 한 가지 이상 요구할 수 있습니다. 본 백서에서는 직원과 고객 및 소비자(B2E, B2B, B2C)에게 Passwordless Authentication을 제공할 수 있게 해주는 Okta의 다양한 기능들을 살펴보겠습니다.

Passwordless Authentication 구축은 어디서부터 시작해야 하나요?

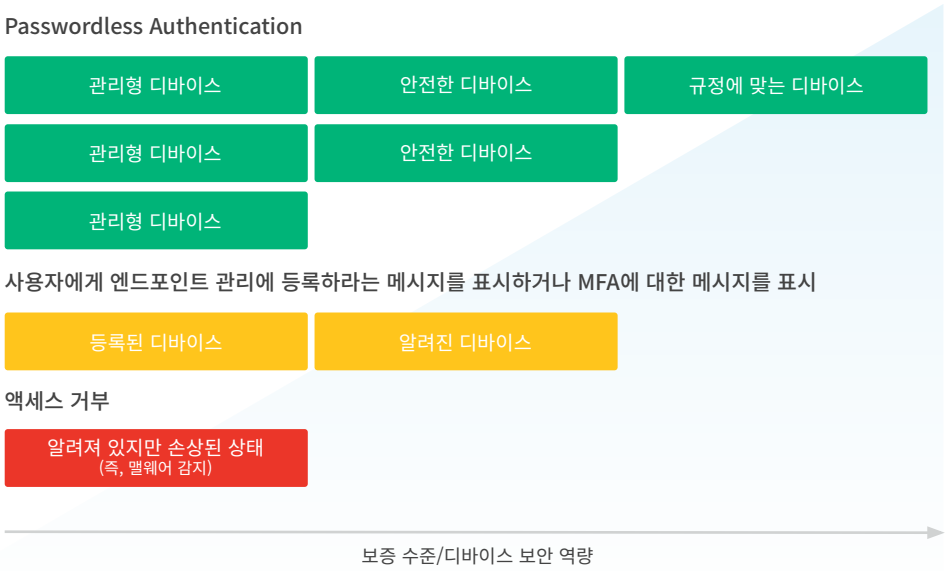
서론에서 언급했듯이, MFA 구현은 Passwordless Authentication을 구축하기 위한 기반입니다.

MFA는 지식, 소유, 그리고 속성의 세 가지 인증요소 범주 가운데 두 가지로 정의됩니다. 예를 들어 비밀번호와 SMS OTP를 함께 사용하는 것은 지식과 소유 인증요소를 조합한 것이고, 비밀번호와 생체 인식을 함께 사용하는 것은 지식과 속성 인증요소를 조합한 것입니다.

하지만 종종 언급되지 않는 네 번째 요소가 있는데, 바로 암시적 인증요소입니다. 이는 엔드 유저에게 반드시 제시되는 것은 아니지만 액세스 결정을 내리기 전에 고려하는 인증요소입니다. 예를 들어 사용자가 새로운 위치에서 새로운 디바이스로 로그인을 시도하는 경우에는 더욱 강화된 인증요소를 적용해야 할 것입니다. 하지만 알려진 네트워크에서 알려진 디바이스로 로그인을 시도하는 경우에는 보안 강도가 중간 이하인 단일 인증요소가 적합할 것입니다.

궁극적인 목표는 위험 수준에 따라 인증요소를 적절히 연결하여 Passwordless Authentication 여정을 시작하는 것입니다.

예를 들어, 아래 그림에서 알 수 있듯이 다양한 디바이스 보증 수준을 Passwordless Authentication과 연결할 수 있는데, 보증 수준이 중간 이하인 경우에는 강력한 인증요소를 요구하거나, 혹은 로그인을 완전히 거부할 수 있습니다.



Okta에서는 어떤 Passwordless Authentication 옵션을 제공하나요?

Okta는 직원 아이덴티티와 고객 아이덴티티에서 기업의 요구 사항을 충족하기 위해 다양한 Passwordless Authentication 방식을 제공하고 있습니다. 이 섹션에서는 Okta에서 사용할 수 있는 기능들 중 Passwordless Authentication을 달성하는 데 도움이 되는 기능을 비롯해 로드맵의 몇 가지 기능을 살펴봅니다. 더불어 각 기능을 적용하기에 가장 적합한 사용 사례(직원 아이덴티티 vs. 고객 아이덴티티)도 함께 살펴보겠습니다.

Okta FastPass

Okta FastPass를 사용하면 어떤 디바이스에서든 작업을 완료하는 데 필요한 모든 리소스(클라우드 앱, 온프레미스 앱, VPN)에 대해 Passwordless Authentication을 수행할 수 있습니다. SAML, WS-Fed, 또는 OIDC를 지원하는 Okta 연결 리소스의 경우, Okta FastPass를 사용해 로그인 절차를 개선할 수 있습니다. 그 방법은 다음과 같습니다.

1. 사용자가 Okta Verify를 사용해 디바이스를 Universal Directory에 등록합니다.
   이러한 등록 프로세스를 지원하기 위해 Okta는 iOS와 Android 환경에서 기존 Okta Verify 앱을 개선하고 Windows와 MacOS에서 새로운 Okta Verify 앱을 제공하고 있습니다.
2. 관리자는 Okta FastPass의 제공 시점에 대한 정책을 설정합니다.
   관리자는 관리형 디바이스, 또는 Okta에 등록된 디바이스에서만, 혹은 특정 네트워크에서만 Okta FastPass를 사용하도록 지정할 수 있습니다.
3. 사용자가 Okta 리소스에 로그인할 때 사용자 이름/비밀번호 입력 메시지가 표시되지 않습니다. Okta Verify는 관리자가 설정한 정책을 확인하고, 로그인이 올바른 컨텍스트를 충족한다는 가정 하에 사용자가 로그인하도록 허용합니다.
   이러한 Passwordless Authentication은 브라우저(서비스 공급자가 개시한 인증 프로세스와 Okta 대시보드 직접 로그인)와 네이티브 모바일 앱, 그리고 데스크톱 씩 클라이언트에서 수행됩니다.

Okta FastPass는 현재 출시되어 있으며, 자세한 내용은 **Okta FastPass 웹페이지**를 참조하시기 바랍니다.

사용 사례: Workforce Identity

Factor Sequencing

Factor Sequencing을 통해 관리자는 로그인 위험 수준과 컨텍스트에 따라 일련의 인증요소를 요구할 수 있습니다. Okta Adaptive MFA를 사용하면 해당 인증요소를 적합한 위험 수준과 결합하여 안전한 Passwordless Authentication을 달성할 수 있습니다.

위험 수준이 낮으면 로그인 프로세스를 간소화할 수 있고, 따라서 사용자가 필요한 리소스에 보다 간편하게 액세스할 수 있습니다. 하지만 로그인 시 위험 수준이 높은 경우에는 별도의 인증요소가 요구됩니다. Factor Sequencing의 실행 원리는 다음과 같습니다.

1. 관리자가 적응형 정책과 결합(옵션 사항)된 인증요소 체인을 정의하는 정책을 (조직 수준의 로그인 규칙을 통해) 생성합니다.
   여기에는 앞서 언급한 비밀번호 요건 삭제가 포함됩니다(원하는 경우).

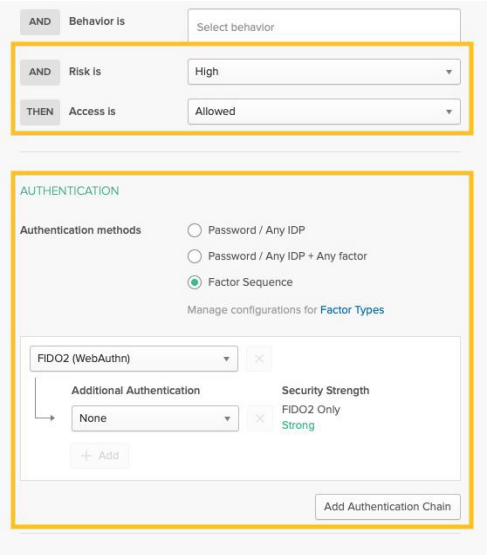
2. 관리자가 정의한 컨텍스트와 인증요소 체인에 따라 로그인 시 엔드 유저에게 인증요소가 표시됩니다.
   관리자가 로그인 프로세스에서 비밀번호 옵션을 제거한 경우에는 엔드 유저가 보조 인증요소를 주 인증요소로 사용할 수 있습니다.

Factor Sequencing을 보면 명확한 MFA 전략이 Passwordless Authentication 달성에 얼마나 도움이 되는지 알 수 있습니다.
Factor Sequencing을 통해 생성할 수 있는 정책은 대표적으로 다음과 같습니다.

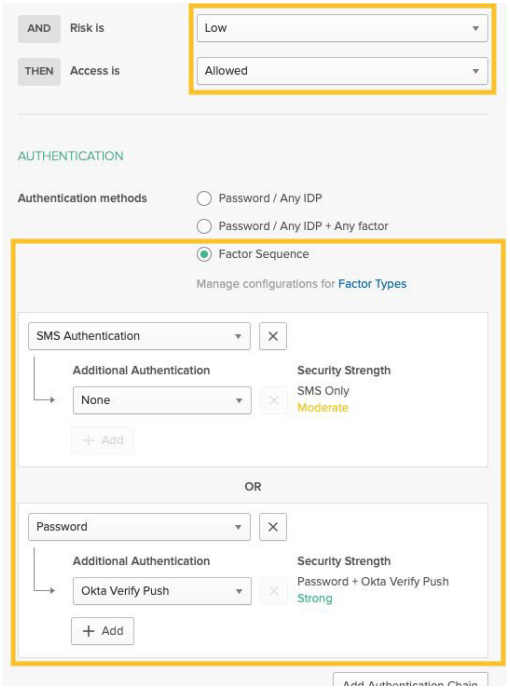
1. 위험 수준이 높은 로그인의 경우 생체 인식 기반 로그인(WebAuthn) 요구

2. 로그인 시 비밀번호 없이 Push 또는 WebAuthn과 함께 Okta Verify를 사용하도록 허용

3. 비밀번호를 요구하기에 앞서 사용자에게 비밀번호가 아닌 인증요소 제시(예: Okta Verify Push 적용 후 비밀번호 요구)
   비밀번호 스프레이 시도를 차단하는 데 효과적인 방법입니다.



4. 위험 수준이 높으면 WebAuthn만 허용합니다.



5. 위험 수준이 낮으면 SMS OTP 또는 비밀번호와 Okta Verify Push를 함께 사용합니다.

사용 사례: Workforce Identity & Customer Identity

WebAuthn

WebAuthn은 웹 애플리케이션이 등록된 디바이스(휴대폰, 노트북 등)를 인증요소로 사용함으로써 사용자 인증을 단순화하고 보호할 수 있게 해주는 브라우저 기반 API입니다. 공개 키 암호화를 사용해 신종 피싱 공격으로부터 사용자를 보호합니다. 현재 피싱을 방지할 수 있는 인증요소는 WebAuthn이 유일합니다.

WebAuthn의 실행 원리는 다음과 같습니다.

오프 디바이스 및 로밍 인증자

하드웨어(컴퓨터 또는 휴대폰)에 내장되어 있지 않고 WebAuthn가 지원되는 인증요소입니다.

- YubiKey 5Ci
- FEITIAN BioPass
- HID Crescendo 스마트 카드

온 디바이스 인증자 및 플랫폼 인증자

컴퓨터 또는 휴대폰 하드웨어에 내장되어 있고 WebAuthn가 지원되는 인증요소입니다.

- Windows 10 1903 이상의 Windows Hello
- MacBook의 터치 ID
- Android 7.0+의 지문
- iOS의 터치 ID 및 페이스 ID

WebAuthn 지원은 웹 앱의 인증 프로세스에서 WebAuthn API, 브라우저, OS 및 하드웨어의 지원 여부에 따라 결정됩니다.
복잡하게 보일 수 있지만, 다행히 여러 운영 체제와 디바이스 및 브라우저에서 이미 WebAuthn을 지원하고 있습니다. 그리고 Okta는 적응형 MFA 제품을 통해 WebAuthn을 지원하고 있습니다.

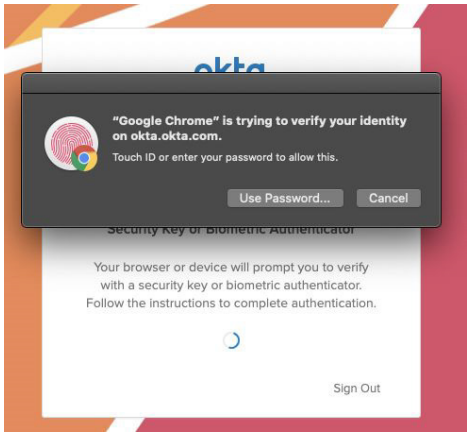
SMS OTP 및 모바일 인증자 앱 대비 WebAuthn의 이점:

- Passwordless Authentication을 보호하기 위한 표준 기반 접근 방식
- 사용자가 등록하는 각각의 WebAuthn 인증요소에 대해 공개 키와 개인 키 쌍을 사용함으로써 피싱을 방지하는 인증요소 유형
- 생체 인식을 사용해 빠르고 원활한 로그인을 보장함으로써 엔드 유저에게 최고의 로그인 경험 제공
- 디바이스 로그인 또는 잠금 해제에 사용하는 생체 인식을 그대로 사용하여 앱에 액세스
- 다양한 디바이스 및 보안 키 옵션

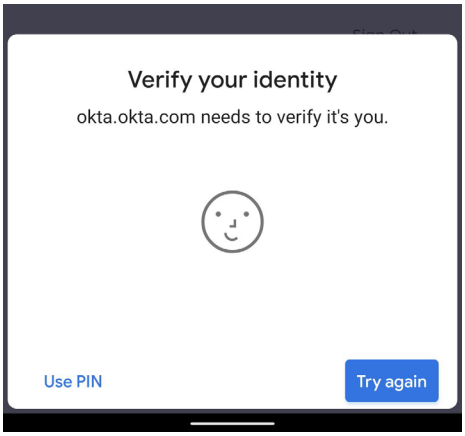
WebAuthn을 지원하는 브라우저, 하드웨어 및 운영 체제 예:

- 터치 ID를 사용하는 MacOS의 Google Chrome
- Windows Hello를 사용하는 Windows 10의 Google Chrome
- Windows Hello를 사용하는 Windows 10의 Microsoft Edge
- Windows Hello를 사용하는 Windows 10의 Firefox
- 지문 인식 디바이스를 사용하는 Android 7.0 이상의 Google Chrome
- 로그인 시 WebAuthn 호환 브라우저를 사용(Windows Hello, 터치 ID 각각 사용)하는 Windows 및 MacOS의 데스크톱 앱
- 지문 인식을 통해 Android 7.0 이상에 로그인 시 WebAuthn 호환 브라우저(예: Chrome)를 사용하는 네이티브 모바일 앱

WebAuthn은 Passwordless Authentication을 전사적으로 구현할 수 있는 안전한 방법입니다.



MacOS의 터치ID



Android의 안면 인식 잠금 해제

사용 사례: Workforce Identity & Customer Identity

PIV 스마트 카드

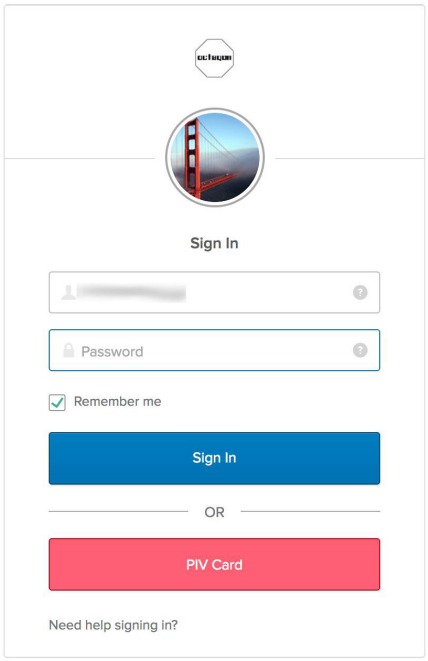
2004년, 조지 W. 부시 대통령은 미국의 모든 연방 기관 직원과 계약자에게 어디서나 사용할 수 있는 공통 신분증을 지급하도록 명령하는 국토 안보부 대통령 지침 12(HSPD 12)을 발표했습니다. 이 지침에 따라 NIST(National Institute of Standards and Technology)의 ITL(Information Technology Laboratory)은 민간 산업 및 기타 연방 기관과 협력해 정부 차원의 공통 신원 확인 시스템에 대한 표준을 마련했습니다.

PIV(Personal Identity Verification) 시스템을 위한 표준인 FIPS(Federal Information Processing Standard)는 X.509 준수 인증서 및 키 쌍과 함께 스마트 카드를 사용할 때 기준이 됩니다. 구체적으로 설명하자면, 실물 카드에는 소유자만이 액세스할 수 있는 디지털 파일이 포함되어 있습니다. 이 카드는 PIV 자격 증명이 공인 기관에서 발급되었고, 아직 기간이 만료되지 않았으며, 사용이 철회되지 않았음을 확인하고, 자격 증명의 소유자와 발급 대상자가 동일인인지 확인하는 데 사용할 수 있습니다.

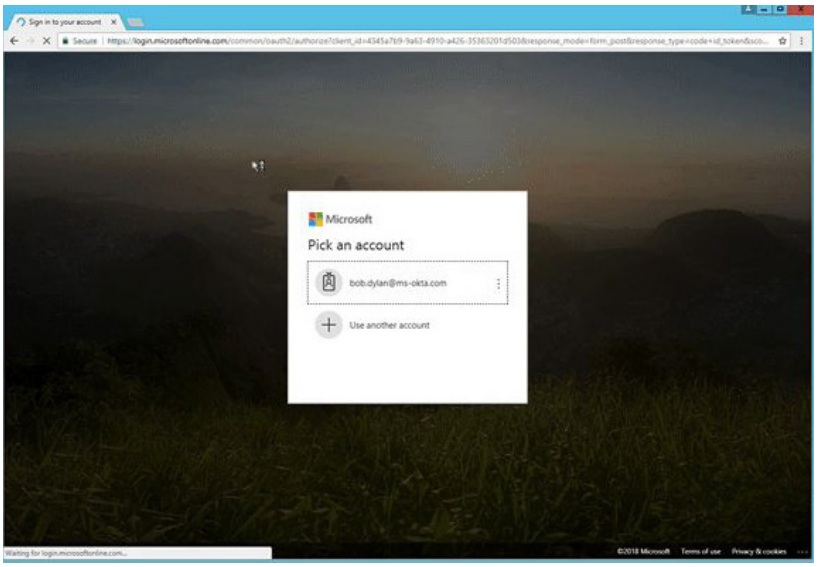
PIV 기반 인증이 적용되지 않는 산업 분야도 있겠지만, Okta는 PIV 인증을 구현하여 또 다른 형태의 Passwordless Authentication을 제공하고 있습니다. 그 방법은 다음과 같습니다.

1. 관리자가 Okta 조직에서 "ID 공급자"로서 스마트 카드를 활성화합니다.
   이를 위해서는 루트 인증서를 Okta에 업로드하고, PIV 또는 스마트 카드를 통한 로그인이 필요한 경우를 정의하도록 라우팅 규칙을 구성하는 작업이 필요합니다.

2. 스마트 카드가 구성되면, 엔드 유저가 Okta에 로그인할 때 PIV 카드 옵션(아래 스크린샷)이 표시됩니다.



3. 그리고 PIV를 로그인 자격 증명으로 사용할 수 있는 Okta 인증 화면으로 넘어갑니다. 엔드 유저는 PIV 카드에 저장된 인증서를 선택하고 PIN을 입력하면 됩니다. 사용자 이름이나 비밀번호는 요구되지 않습니다.



사용 사례: Workforce Identity

DSSO(Desktop Single Sign-On)

DSSO에서는 사용자가 디바이스(Windows, MacOS)에서 Active Directory 네트워크에 로그인할 때 Okta를 통해 자동으로 인증됩니다. 인증을 마친 사용자는 사용자 이름/비밀번호를 추가로 입력하지 않고도 Okta를 통해 애플리케이션에 액세스할 수 있습니다. 사용자가 한 번만 로그인하면 되며 Okta를 통해 액세스하는 각 애플리케이션에 대해 별도의 자격 증명이 필요하지 않다는 점에서 DSSO는 사용자 경험을 개선합니다. DSSO는 두 가지 방식으로 구현할 수 있습니다.

- 에이전트리스(권장 사항)
- 온프레미스에서 IWA 웹 에이전트 실행

Okta DSSO의 실행 원리는 다음과 같습니다.

1. 사용자가 데스크톱 로그인 페이지에서 AD 자격 증명을 입력합니다.
2. 브라우저, 또는 최신 인증을 지원하는 데스크톱 씩(thick) 클라이언트를 통해 Okta에 액세스할 때 별도의 자격 증명 입력 메시지가 표시되지 않습니다(MFA가 필요한 경우 제외).

앞서 설명한 DSSO와 Okta FastPass 기능의 차이점이 무엇인지 궁금하실 것입니다. Passwordless Authentication을 위해 디바이스가 Active Directory 도메인에 연결되어 있거나 네트워크에 상주할 필요가 없으며, Windows, MacOS, iOS 및 Android에서 실행된다는 것이 Okta FastPass의 장점입니다.

사용 사례: Workforce Identity

SAML을 통한 Device Trust 통합

Device Trust는 관리자가 관리형 디바이스와 비관리형 디바이스에 대한 액세스 정책을 설정할 수 있게 해주는 Okta 기능입니다. 대부분의 경우, 관리형 디바이스에서는 Okta에 대한 액세스를 허용하고 비관리형 디바이스에서는 MFA를(최소한으로) 요청하거나 액세스를 거부하도록 정책을 설정합니다. "관리형 디바이스"란 Jamf, VMware Workspace ONE, Microsoft Intune과 같은 엔드포인트 관리 솔루션이 관리하는 디바이스를 말합니다.

VMware Workspace ONE과 같은 일부 솔루션에는 Passwordless Authentication 기능(흔히 모바일 SSO라고 지칭)이 내장되어 있습니다. Okta는 이러한 솔루션들을 통합하여 엔드 유저에게 원활한 액세스 경험을 제공할 수 있습니다. Device Trust SAML 통합 기능의 실행 원리는 다음과 같습니다.

1. 관리자는 Okta의 IdP Discovery 기능을 활용해 로그인을 엔드포인트 관리 솔루션으로 라우팅합니다.
   이를 위해서는 엔드포인트 관리 솔루션이 손쉬운 자체 아이덴티티 솔루션(예: VMware Workspace ONE, MobileIron Access)을 제공해야 합니다.
2. 엔드포인트 관리 도구는 디바이스의 관리 여부를 확인합니다.
   디바이스가 관리되는지 여부에 따라 관리자는 액세스 거부, 등록 요구, 액세스 허용 또는 MFA 요구를 위한 정책을 구성할 수 있습니다.
3. 관리형 디바이스에서는 사용자에게 별도의 자격 증명 요청 메시지가 표시되지 않고, 애플리케이션 로그인이 원활하게 이루어집니다.

Device Trust 통합 기능에 대한 자세한 내용은 Okta 블로그를 참조하시기 바랍니다.

사용 사례: Workforce Identity

Email Magic Link

출시 예정

이메일 기반의 Passwordless Authentication은 소비자들에게 흔한 사용 방식이 되었습니다. 이 방법의 핵심은 비밀번호 리셋 프로세스로, 기존 비밀번호를 우회하여 새 비밀번호를 설정할 수 있는 비밀 링크가 사용자에게 전송됩니다. 대부분의 사용자에게 친숙한 방식입니다.

Slack이나 Medium과 같은 앱이 사용되면서 이러한 인증 방식이 대중화되었습니다. 진정한 Passwordless Authentication은 비밀번호 리셋 프로세스를 한 단계 발전시킵니다. Email Magic Link 기능의 실행 원리는 다음과 같습니다.

1. 사용자가 이메일 주소만 입력하면 앱에 등록하거나 로그인할 수 있습니다.
2. 받은 편지함으로 전송된 링크를 클릭해서 인증 프로세스를 완료하라는 메시지가 앱에 표시됩니다.
3. 사용자가 받은 편지함을 열어 링크를 클릭하면 앱으로 리디렉션되어 로그인이 완료됩니다.

앱 디자이너는 비밀번호 및 이와 관련된 리셋 절차를 없애고, 사용자의 이메일 주소에 대한 일회용 링크(시간 제한이 있거나 사용 기한이 있는 비밀 링크)를 전송하기만 하면 됩니다. 해당 링크를 클릭하면 사용자에 대한 인증이 수행되고 로그인 상태가 유지되도록 수명이 긴 쿠키가 설정됩니다. 사용자가 비밀번호를 설정, 저장 또는 입력할 필요가 없기 때문에 모바일 디바이스에서 특히 유용한 기능입니다. 이러한 방식의 Passwordless Authentication은 하드웨어에 종속될 일이 없기 때문에 소비자 애플리케이션에 매우 매력적인 옵션입니다.

사용 사례: Customer Identity

기능	사용 사례
Okta FastPass 온프레미스 디렉토리나 특정 엔드포인트 관리 도구에 의존하지 않고 Windows, iOS, Android 및 MacOS에서 디바이스 기반의 Passwordless Authentication 구현	Workforce Identity
Factor Sequencing 사용자, 디바이스 및 위치 컨텍스트를 결합해 인증요소 체인 정의	Workforce Identity 및 Customer Identity
WebAuthn FIDO2.0 표준을 사용하는 피싱 방지 생체 인식 기반 인증	Workforce Identity 및 Customer Identity
PIV 스마트 카드 미국 연방 기관에서 주로 사용하는 x509 인증서를 통한 인증	Workforce Identity
DSSO(Desktop Single Sign-On) AD 도메인 연결 컴퓨터에 대한 Passwordless 로그인	Workforce Identity
Device Trust 통합 엔드포인트 관리 솔루션의 모바일 SSO 기능을 활용해 Passwordless Authentication 제공	Workforce Identity
Email Magic Link(출시 예정) 소비자 앱에 가장 적합한 이메일 기반의 Passwordless Authentication	Customer Identity

자세한 내용은 어디서 알아볼 수 있나요?

본 백서에서는 Okta가 제공하는 다양한 Passwordless Authentication 기능을 간략히 소개합니다. Passwordless Authentication 구축 시 고려해야 할 사항과 이러한 기능 관련 이점 및 문제에 대한 자세한 내용은 **Move Beyond Passwords**를 참조하십시오. MFA를 통해 Passwordless Authentication을 구현하는 자세한 방법은 **Okta Adaptive MFA 웹페이지**를 참조하십시오.

Okta 소개

Okta는 기업 아이덴티티 분야의 독자적인 선두 기업입니다. Okta Identity Cloud는 기업이 적정 권한을 가진 사용자와 테크놀로지를 적시에 안전하게 연결할 수 있도록 지원합니다. 6,500개 이상의 애플리케이션 및 인프라 공급업체가 사전에 통합되어 있어 Okta 고객은 자신의 비즈니스에 가장 적합한 테크놀로지를 손쉽고 안전하게 사용할 수 있습니다. 또한 JetBlue, Nordstrom, Slack, Teach for America, Twilio 등 8,400개 이상의 기업들이 Okta를 통해 자사 직원 및 고객의 아이덴티티를 보호하고 있습니다. 자세한 내용은 **okta.com/kr**을 참조하십시오.