Elixirr

클라우드 보안 관리자 (Azure Active Directory)

[3강] 다단계 인증과 보안

학습 목표

학습 목표

Azure Active Directory의 **인증 기능**에 대해서 알아 봅니다.

Azure Active Directory에서 **액세스 관리**에 대해서 알아 봅니다.

Azure Active Directory에서 **ID 보호 및 관리**에 대해서 알아 봅니다.

Azure Active Directory

인증 기능

1. Azure의 인증 방법
2. 암호 재설정 (Self Service Password Reconstruction, SSPR)
3. AAD의 암호 보호 및 관리

Azure가 가지는 ID 보안 기능

암호 복잡성 규칙 - 사용자가 추측하기 어려운 암호를 생성하도록 강제

암호 만료 규칙 - 사용자가 주기적으로 암호를 변경하고, 이전에 사용한 암호를 사용하지 않도록 강제

SSPR(Self Service Password Reconstruction) - 사용자가 암호를 잊은 경우 직접 암호 재설정

Azure AD ID 보호 - 조직의 ID를 보호하기 위해 위험한 동작에 자동으로 대응하는 위험 기반 정책 구성

Azure AD 암호 보호 - 전역적으로 금지된 암호 목록을 통해 흔히 사용되고 손상된 암호를 차단

Azure AD 스마트 잠금 - 사용자 암호를 추측하려고 하거나 무차별 암호 대입 공격을 사용하려는 해커를 잠근다.

Azure AD 애플리케이션 프록시 - 회사의 앱 애플리케이션을 회사 밖에서 안전하게 접근하도록 연결해주는 기능

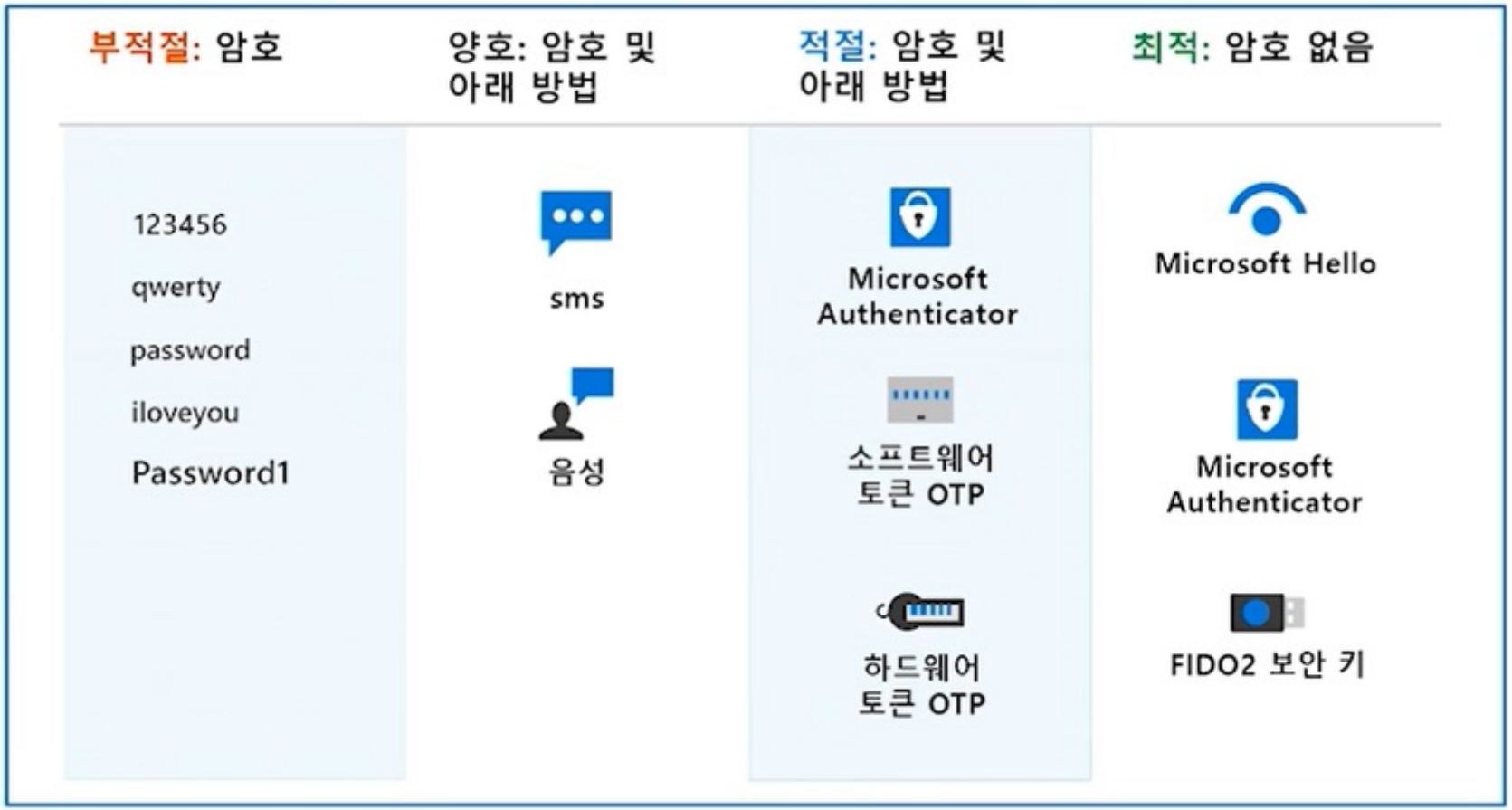
SSO (Single-Sign-On) - 애플리케이션에 대한 SSO 액세스 사용 설정. 수천개의 미리 통합된 SaaS 앱이 포함

Azure AD Connect - 자체 서버와 Azure를 모두 사용하는 기업에서 사용자, 그룹 및 디바이스의 동기화 유지

소셜 엔지니어링이나 키보드 아래에 붙여진 스티커 메모에 있는 암호를 통한 침입을 차단할 수는 없어.

Azure AD의 인증

Azure AD에서는 다양한 인증 방법을 제공한다. 기본 인증으로 암호를 요구하나 이것만으로는 보안에 취약하므로 추가적인 인증으로 요구한다.



셀프 서비스 암호 재설정 (Self Service Password Reconstruction, SSPR)

SSPR은 사용자의 암호를 변경하거나 재설정해야 하는 경우와 계정 잠금을 해제하는 경우 등에 관리자나 보안 지원센터의 도움 없이 직접 사용자가 암호를 재설정할 수 있다.

SSPR의 장점

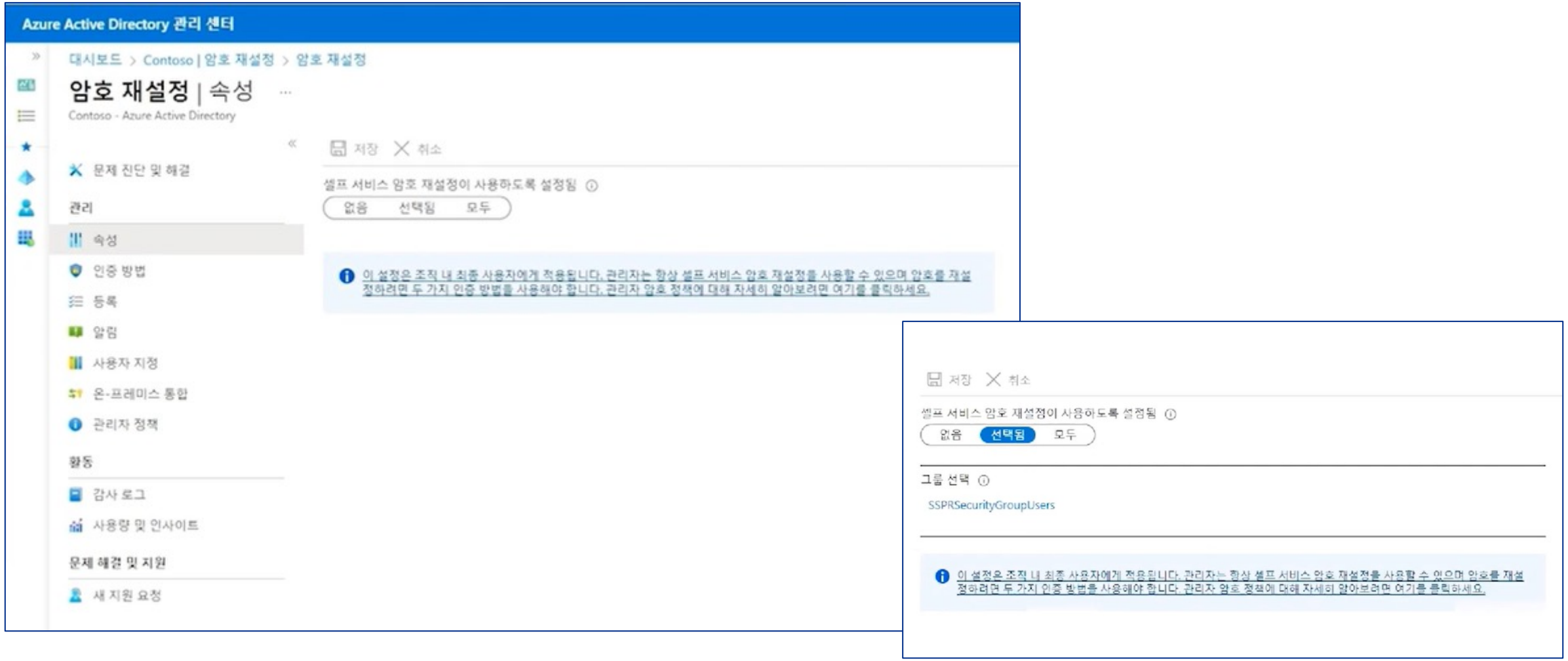
- 관리자의 관리 부담과 비용을 절약
- 관리자는 새로운 보안 요구 사항에 맞추어 설정 변경 가능
- 사용자가 빠르게 작업에 복귀할 수 있으므로 생산성 향상

SSPR의 인증방법

- 모바일 앱 알림
- 모바일 앱 코드
- 이메일
- 휴대폰
- 전화
- 본인 확인 질문

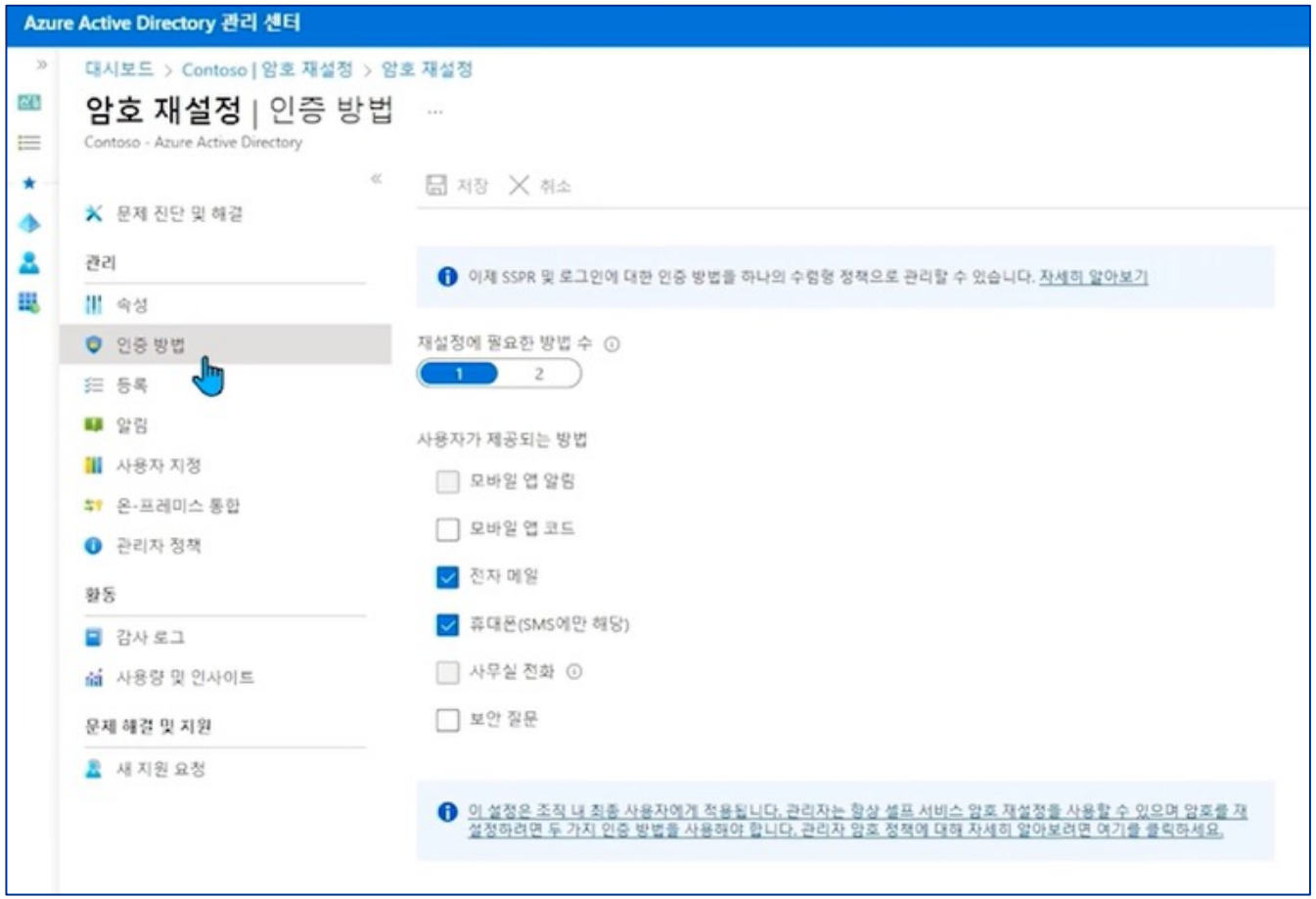
암호 재설정 (SSPR) - 속성

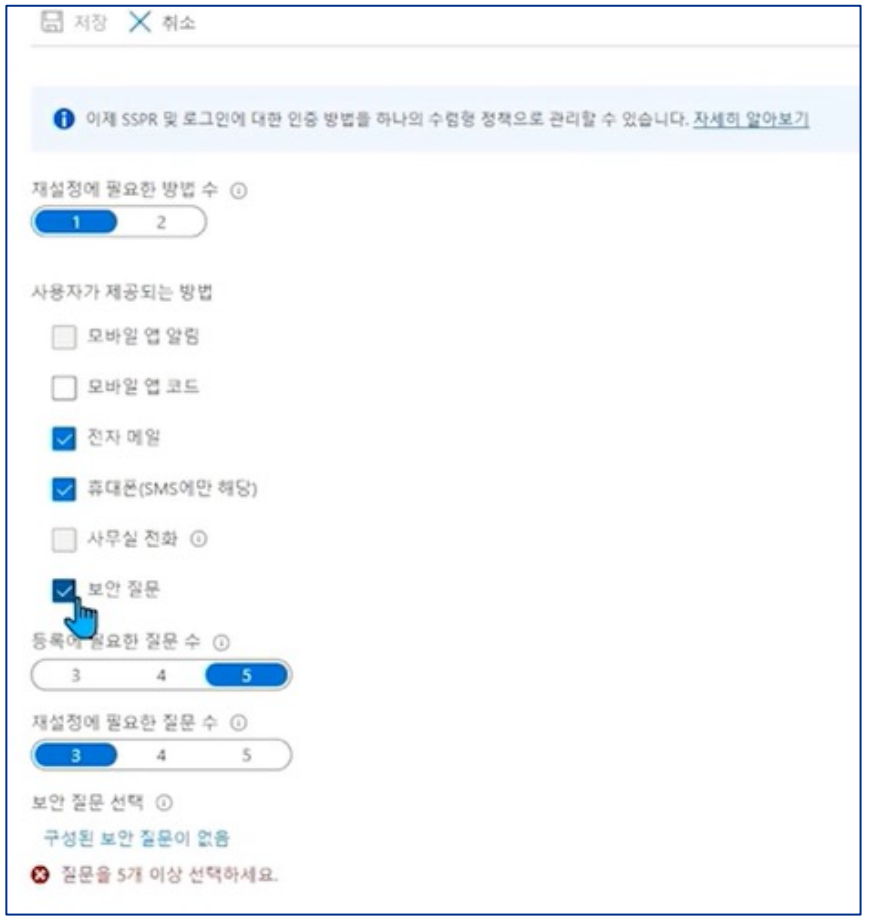
Azure AD의 왼쪽 메뉴에서 '속성'을 선택하면 셀프 서비스 암호 재설정을 설정할 수 있다.



암호 재설정 (SSPR) - 인증 방법

암호 재설정에 필요한 방법 수를 정하고 제공되는 방법을 선택한다. 보안 질문 수와 질문을 등록할 수 있다.

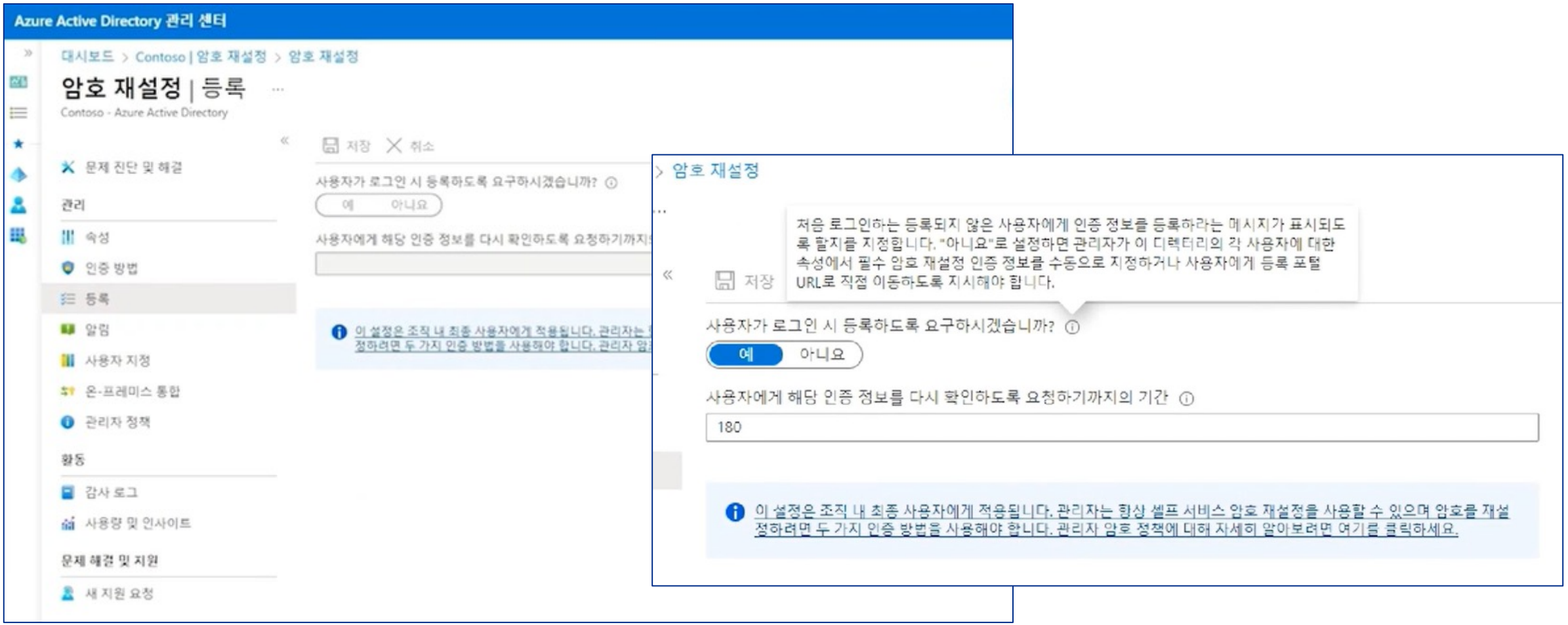




Elixirr

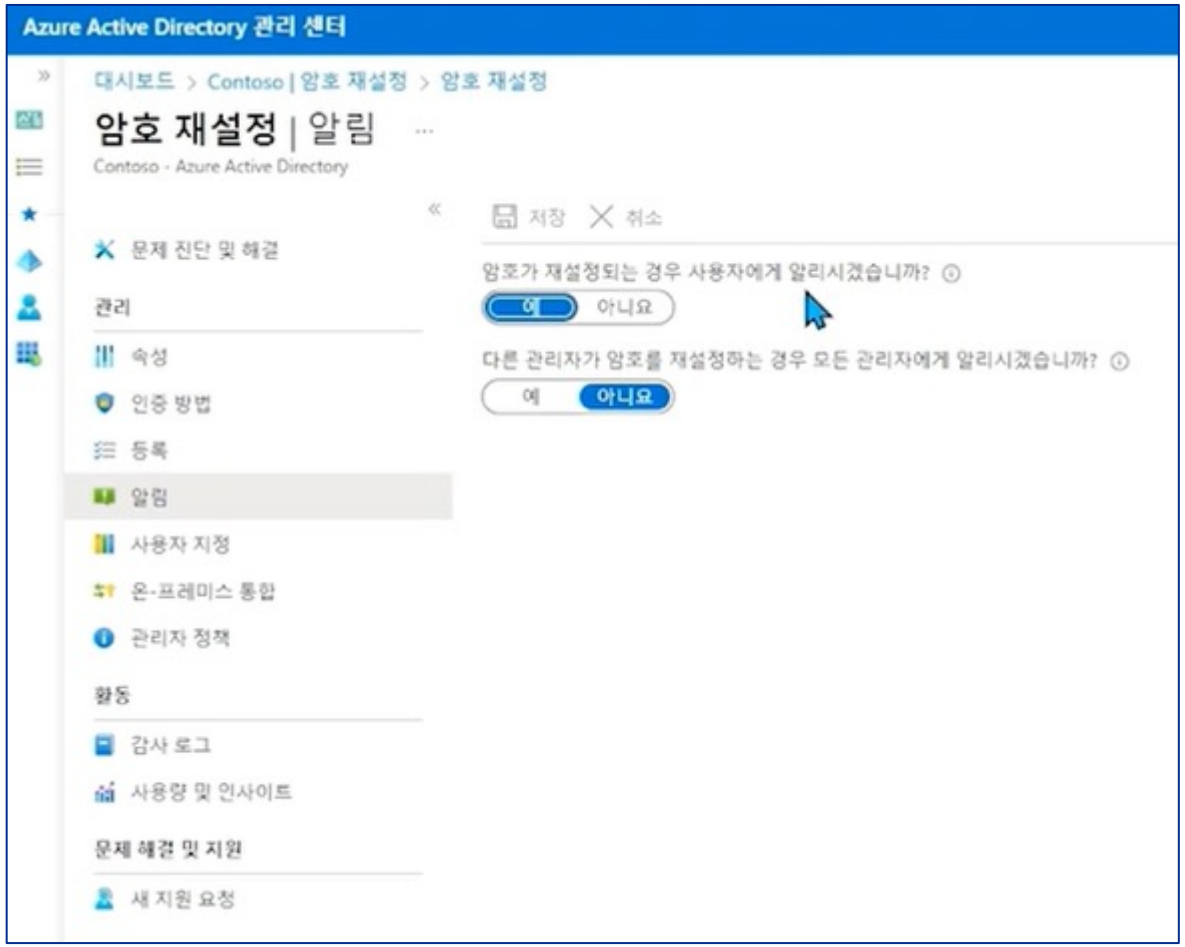
암호 재설정 (SSPR) - 등록

사용자가 처음 로그인할 때 암호를 재설정하도록 요구할 수 있고 사용자에게 해당 인증 정보를 다시 확인하도록 요청하는 기간을 설정할 수 있다.



암호 재설정 - 알림

암호 재설정을 했을 때 사용자에게 알림을 설정할 수 있고, 관리자가 암호를 재설정하는 경우에도 관리자에게 알리도록 설정할 수 있다.



개요

여러분은 대규모 제조 회사의 보안 엔지니어입니다.

회사는 마이크로소프트를 비롯한 인기 있는 개인용 전자 장비 회사와 계약을 진행하고 있습니다.

클라이언트가 보내는 기밀 디자인은 Azure 인프라에 저장됩니다.

많은 해커가 차세대 디자인을 알아내려고 하며, 이 디자인을 보호하는 것이 담당 업무입니다.

네트워크를 강화하고 올바른 사용자만 클라이언트 데이터에 액세스하도록 작업했지만 아직 사용자 계정 보호가 보안 허점입니다.

권한 없는 사용자가 이름/암호를 사용하여 데이터에 액세스할 수 없도록 방지하는 최상의 보안방법은 다단계 인증입니다.

Azure AD 다단계 인증 (Multi-Factor Authentication, MFA)

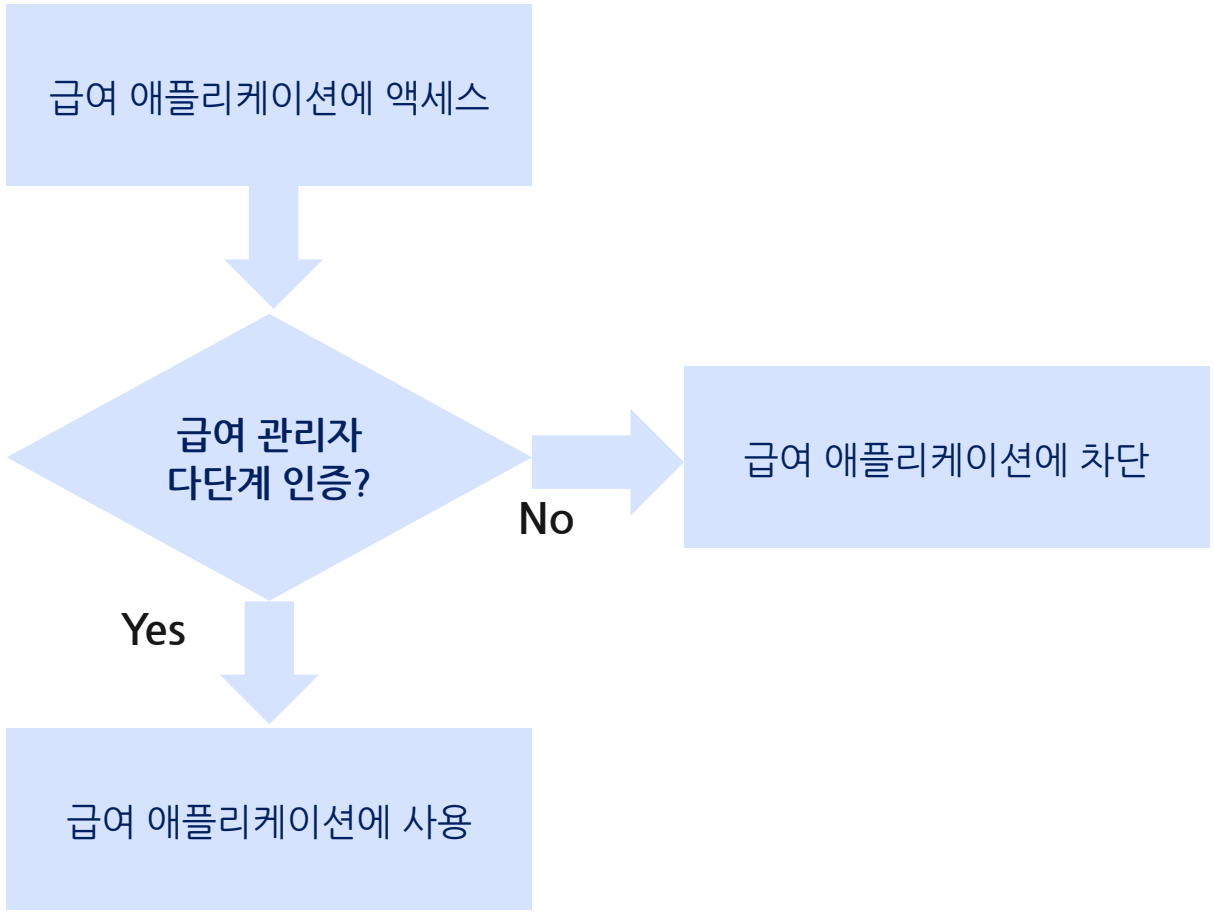
Azure AD MFA는 전체 인증에 아래 열거된 것 중에서 둘 이상의 요소를 요구하여 ID 보안을 강화하는 프로세스이다.

https://learn.microsoft.com/ko-kr/training/modules/secure-aad-users-with-mfa/2-azure-multi-factor-authentication

- 사용자가 알고 있는 것 - 암호 또는 본인 확인 질문에 대한 답변
- 사용자가 소유하고 있는 것 - 알림을 받는 모바일 앱 또는 토큰 생성 디바이스
- 사용자의 신원 정보 - 여러 모바일 디바이스에서 사용되는 지문 또는 얼굴 스캔과 같은 일반적인 생체 인식 속성

Azure AD MFA 정책

Azure AD MFA는 조건부 액세스 정책을 사용하여 적용되며 조건부 액세스 정책은 IF-THEN 문과 같이 동작한다. IF 사용자가 리소스에 액세스 하려는 경우 THEN 작업을 완료해야 한다.



MFA를 요구할 수 있는 일반적인 액세스 요청

- 사용자가 특정 네트워크에 액세스하는 경우
- 사용자가 특정 클라이언트 애플리케이션에 액세스하는 경우
- 사용자가 새 디바이스를 등록하는 경우

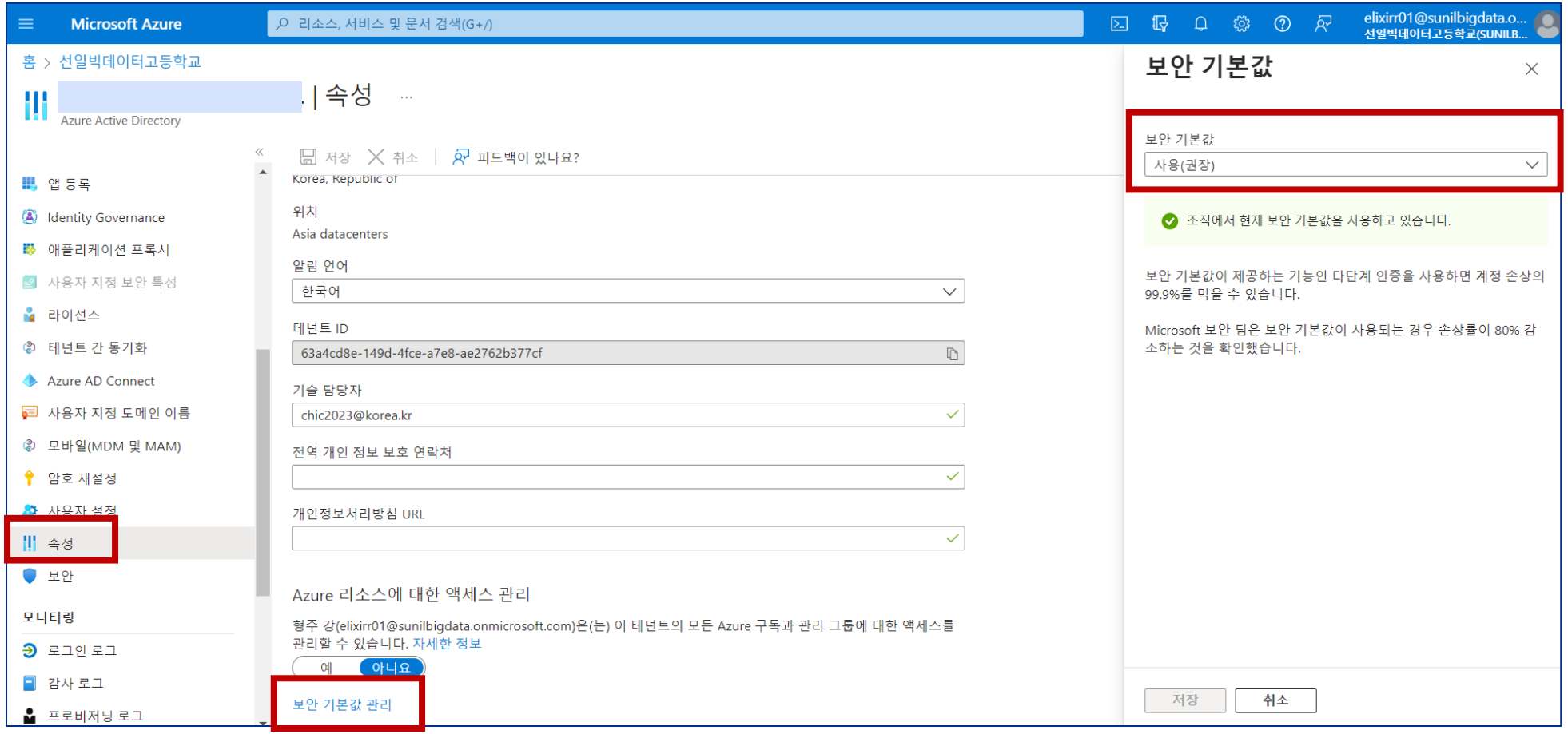
지원되는 인증 방법 결정

Azure AD MFA를 설정할 때 제공할 인증 방법을 선택할 수 있다. 기본 방법을 사용할 수 없는 경우 사용자가 백업 옵션을 이용할 수 있도록 항상 둘 이상의 방법을 지원해야 한다.

모바일 앱 확인 코드	Microsoft Authenticator 앱과 같은 모바일 인증 앱을 사용하여 로그인 인터페이스 작동
모바일 앱 알림	Azure는 Microsoft Authenticator와 같은 모바일 인증 앱에 푸시 알림을 보내 로그인 인터페이스 작동
전화 걸기	Azure는 제공된 전화번호로 전화를 걸고 사용자가 키패드를 사용하여 인증. 백업 방법으로 사용
FIDO2 보안 키	일반적으로 USB 디바이스에 사용되는 인증방법이지만 Bluetooth 또는 NFC를 사용할 수도 있다.
비지니스용 Windows Hello	디바이스에서 암호를 강력한 2단계 인증으로 대체. 디바이스에 연결되어 있고 주로 생체 인식 사용
OATH 토큰	Microsoft Authenticator 앱 및 기타 인증자 앱과 같은 소프트웨어 또는 하드웨어 기반 토큰

MFA 설정

Azure Portal의 Azure AD에 있는 왼쪽 메뉴에서 '**속성**'안에 있는 **보안 기본값 관리**에서 보안 기본값이 MFA를 사용하는 것으로 되어 있다.



Elixirr

Azure AD의 암호 보호 기능

Azure AD는 사용자, 서비스 주체, 관리 ID, 디바이스 등 다양한 유형의 ID를 관리한다.

전역 금지 암호 목록	최신 해킹 트랜드를 반영하는 금지 암호 목록
사용자 지정 암호 목록	조직내에서 금지 암호 목록 설정
암호 스프레이로부터 보호	암호 스프레이는 해킹 공격의 일종으로 여러 개의 사용자 계정에 자주 사용하는 암호를 직접 입력해서 해킹을 시도하는 것으로 이를 방지
하이브리드 보안	클라우드에서 작동하는 방식을 기업의 자체 서버의 Active Directory에도 적용 가능

Azure Active Directory

액세스 관리

1. 조건부 액세스
2. 역할 기반 액세스 제어 (RBAC)

조건부 액세스 (Conditional Access)

최신 보안 경계는 사용자 및 장치 ID를 포함하도록 조직의 네트워크 경계를 넘어 확장되고 있다. 조직은 이제 액세스 제어 결정의 일부로 ID 기반 신호를 사용한다.

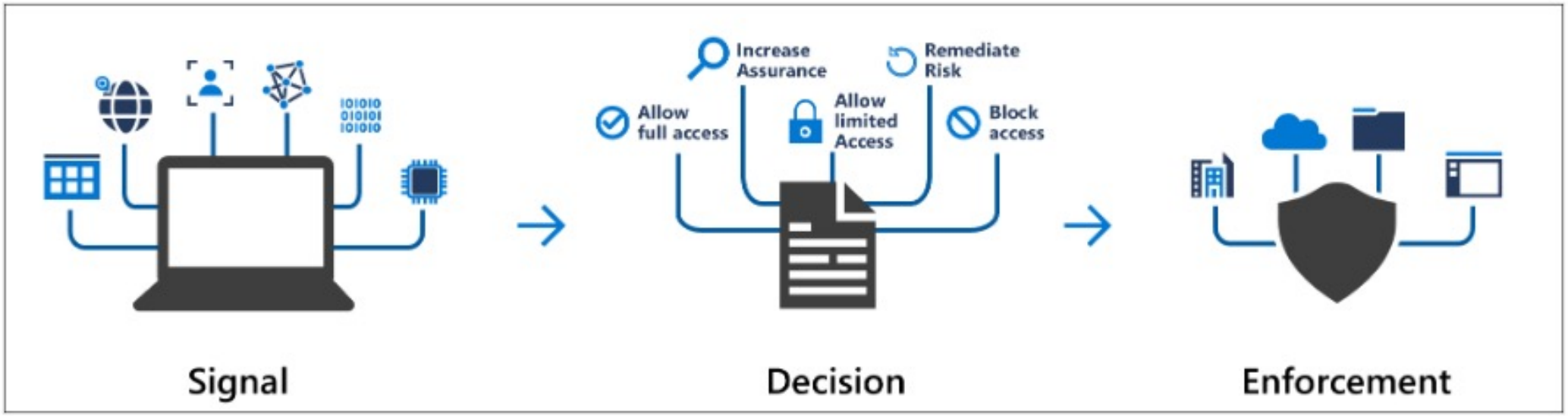
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview

조건부 액세스 정책 결정 과정

Azure AD 조건부 액세스는 사용자와 장치의 신호를 가져와서 결정을 내리고 조직 정책을 적용한다. 이 때 다양한 소스의 신호를 고려하는 Microsoft 제로 트러스트 정책을 사용한다.

조건부 액세스 정책의 목표

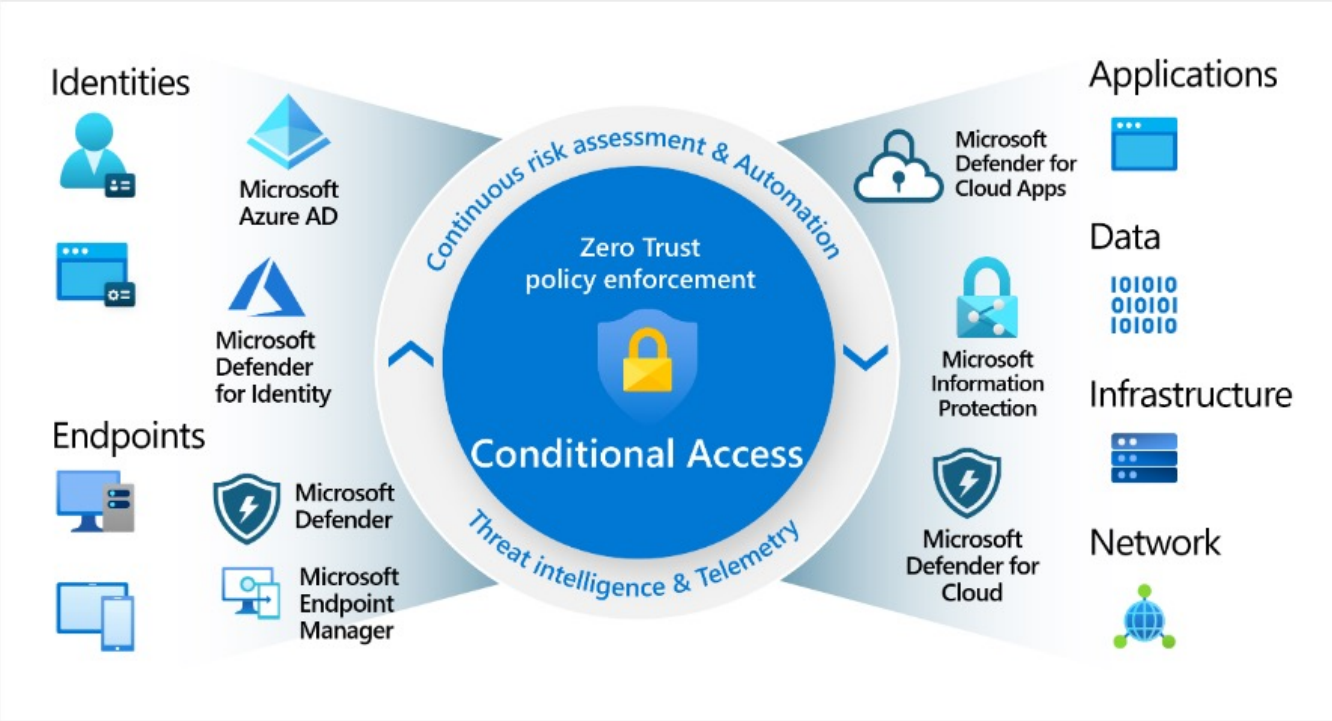
- 사용자가 언제 어디서나 생산성을 발휘할 수 있도록 지원
- 조직의 자산 보호



https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview

신호

조건부 액세스는 액세스 결정을 내릴 때 다양한 소스의 신호를 고려한다.



- 사용자 또는 그룹 구성원
- IP 위치 정보
- 장치
- 애플리케이션
- 실시간 및 예견된 위험 탐지
- 클라우드 앱용 Microsoft Defender

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview

결정

신호를 수집하고 그 신호별로 액세스 허용 여부를 결정한다. 부적절한 신호인 경우에 액세스를 차단하는 가장 제한적인 결정을 내리고 신호에 따라 액세스 권한을 부여할 수 있다. 이때 아래의 옵션을 요구할 수 있다.

다단계 인증 (Multi-Factor Authenticator) 필요

인증 강도 필요

디바이스가 규정 준수로 표시되어야 함

하이브리드 Azure AD 조인 장치 필요

승인된 클라이언트 앱 필요

앱 보호 정책 필요

암호 변경 필요

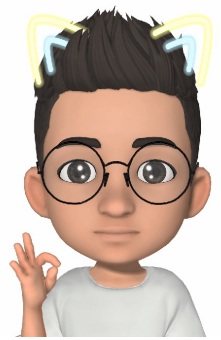
이용 약관 필요

정책

많은 조직에는 아래와 같이 조건부 액세스 정책이 도움이 될 수 있는 다양한 경우가 있고 관리자는 처음부터 정책을 만들거나 Azure Portal의 조건부 액세스 템플릿을 사용해서 시작할 수 있다.

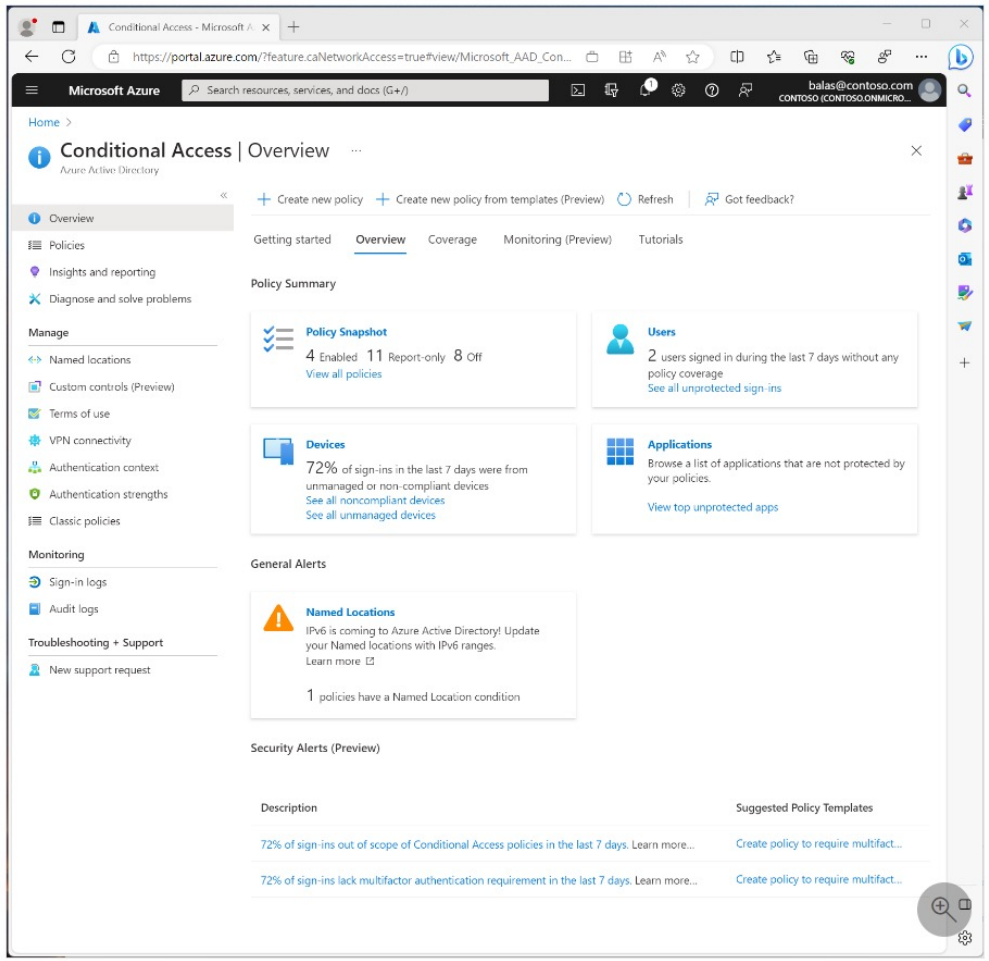
- 관리 역할이 있는 사용자에게 다단계 인증 요구
- Azure 관리 작업에 다단계 인증 요구
- 레거시 인증 프로토콜을 사용하려는 사용자의 로그인 차단
- Azure AD 다단계 인증 등록을 위해 신뢰할 수 있는 위치 요구
- 특정 위치에서 액세스 차단 또는 허용
- 위험한 로그인 동작 차단
- 특정 애플리케이션에 조직에서 관리하는 기기 필요

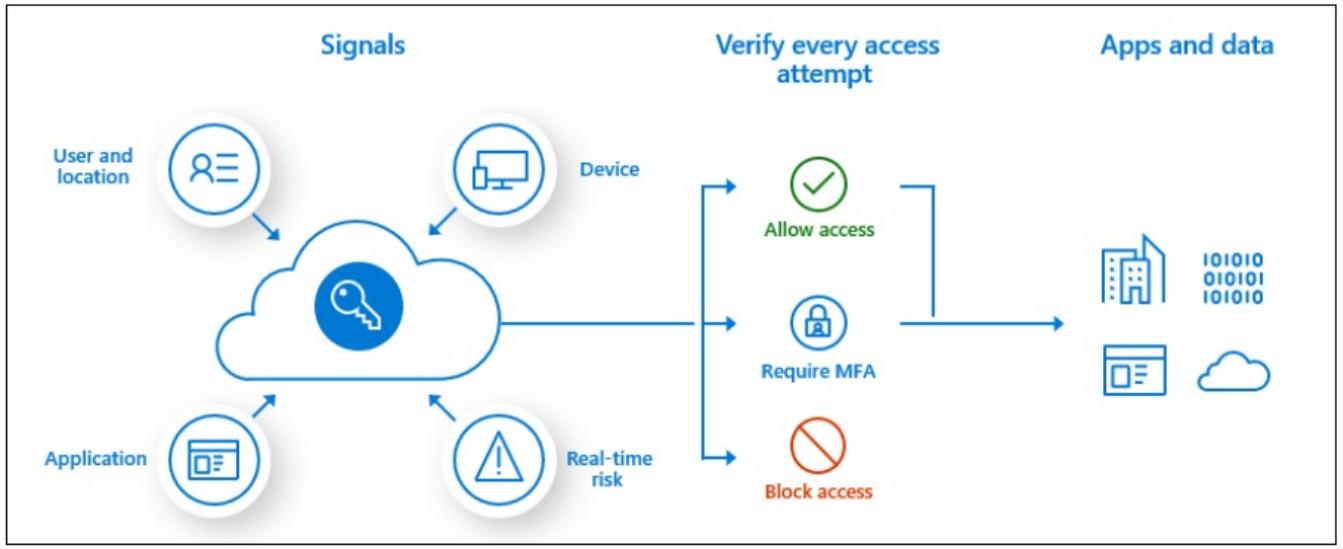
조건부 액세스 기능을
사용하려면 Azure AD
Premium P1라이센스가 필요해



Azure Portal 사용

조건부 액세스 관리자 역할이 있는 관리자는 Azure AD에서 정책을 관리할 수 있고 Azure Portal의 Azure Active Directory > 보안 > 조건부 액세스에서 사용할 수 있다.



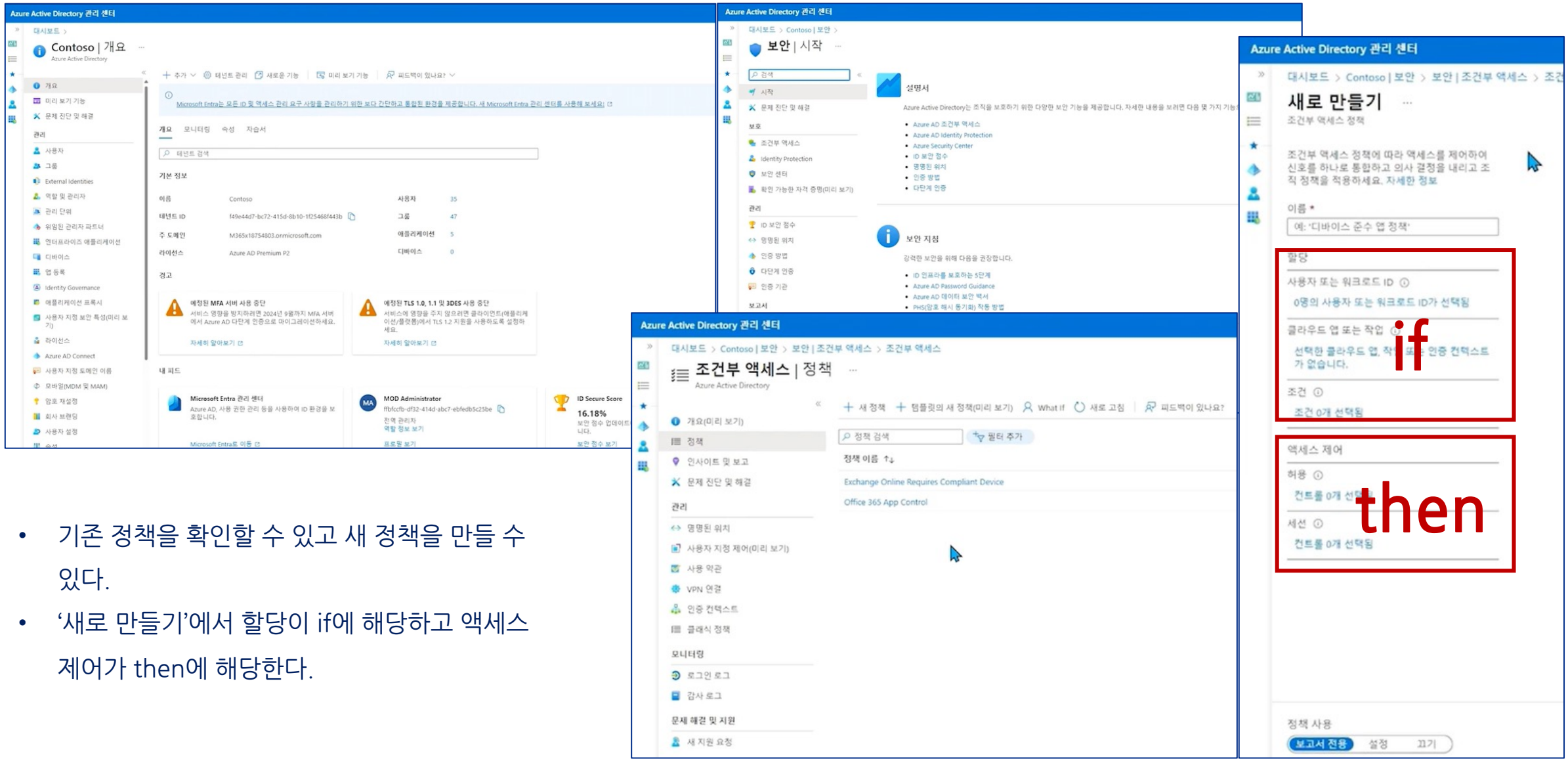


https://learn.microsoft.com/ko-kr/azure/active-directory/authentication/howto-mfa-getstarted#plan-conditional-access-policies

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Elixirr

조건부 액세스 정책 생성



- 기존 정책을 확인할 수 있고 새 정책을 만들 수 있다.
- ‘새로 만들기’에서 할당이 if에 해당하고 액세스 제어가 then에 해당한다.

역할 기반 액세스 제어 (Role Based Access Control, RBAC)

조직내의 인증된 사용자의 권한을 관리하는 경우 Azure AD의 RBAC 기능을 사용한다.

기본 제공 역할	Azure AD에서 기본적으로 제공하는 기능
사용자 지정 역할	사용자가 직접 지정해서 관리하는 경우로서 전역 관리자, 사용자 관리자, 대금청구 관리자가 기본적으로 제공되는 역할
Azure RBAC vs Azure AD RBAC	Azure RBAC - Azure 상의 리소스(ex:가상머신, 스토리지, 웹 앱 등)에 대한 접근 권한을 설정 Azure AD RBAC - Azure AD에 등록된 사용자, 그룹, Microsoft365 등의 접근 권한을 설정
액세스 권한 부여	사용자에게 필요한 액세스 권한을 최소 권한으로 부여

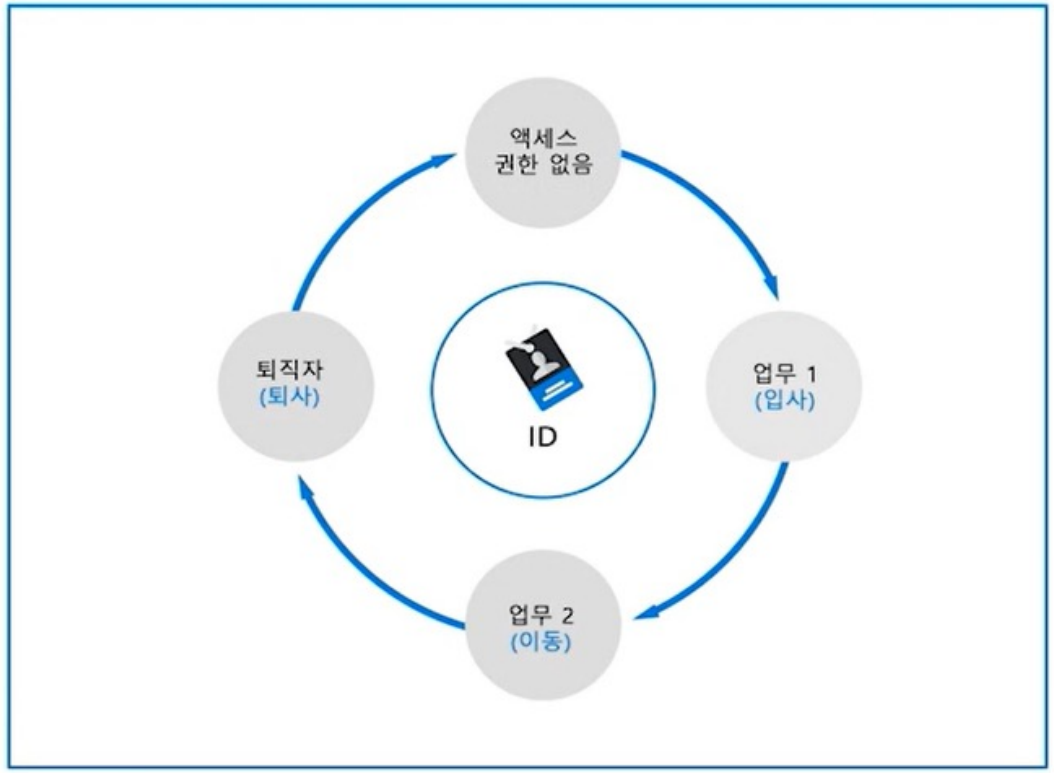
Azure Active Directory

ID 보호 및 관리 기능

1. ID 거버넌스
2. Privileged Identity Management (PIM)
3. ID 보호

ID 거버넌스 (Governance)

ID와 보안에서는 어떤 사용자가 어떤 리소스에 접근할 수 있는지, 해당 사용자가 그 권한으로 무엇을 할 수 있는지, 그 권한을 관리할 수 있는 방법이 있는지, 감사팀에서 이 관리 방법을 검증할 수 있는지를 알 수 있어야 한다.



ID 거버넌스에서 수행되는 작업

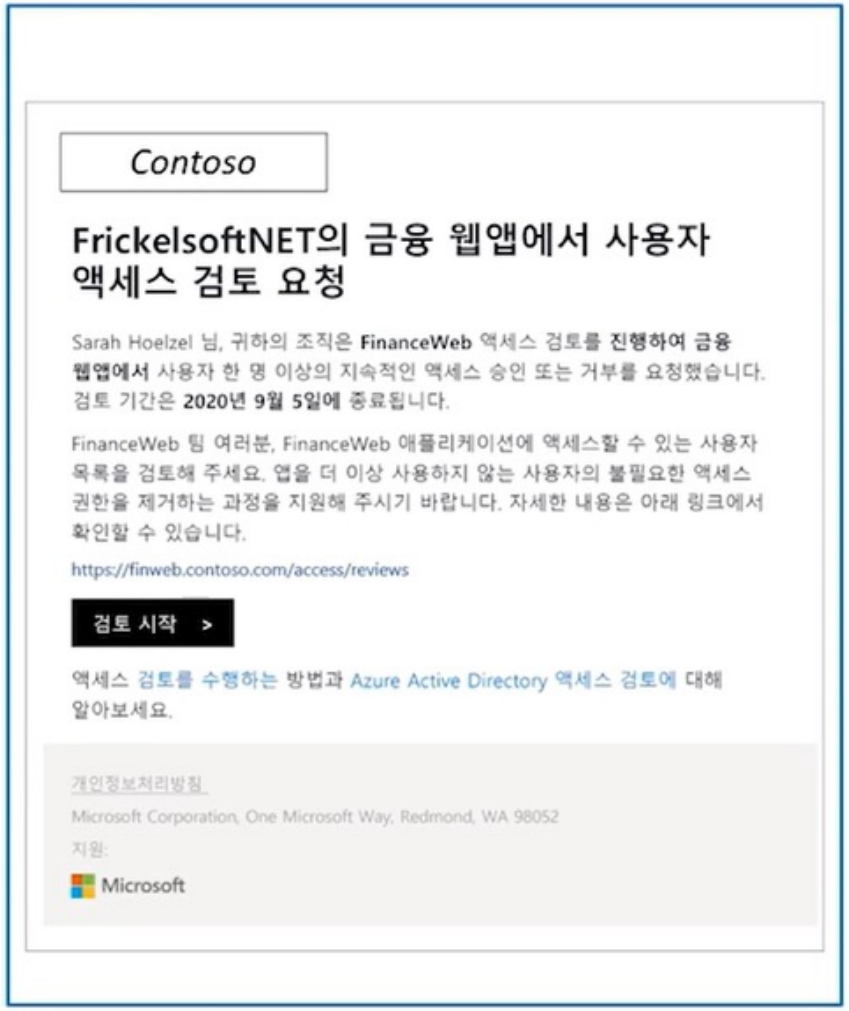
- ID 수명 주기 거버넌스 - 입사와 퇴사
- 액세스 수명 주기 거버넌스 - 근무기간 동안 액세스 관리
- 관리를 위한 권한 있는 액세스 보호 - 사내 또는 사외의 근무자들의 정당한 액세스 관리

ID의 수명주기

- 입사 - 새 디지털 ID 생성
- 이동 - 액세스 권한 부여 업데이트
- 퇴사 - 액세스 권한 제거

권한 관리 및 액세스 검토 - (1)

Azure 클라우드 상의 웹 애플리케이션에 액세스 하려는 사용자가 있는 경우 아래와 같은 검토 요청 메시지가 표시된다.



권한 관리 및 액세스 검토 - (2)

ID 거버넌스는 아래와 같은 기능을 가진다.

권한 관리

- ID 및 액세스 수명 주기를 대규모로 관리하는데 사용할 수 있는 거버넌스 기능
- 새로운 직원이 부서에 합류했을 때 그 부서에서 사용하는 리소스에 대한 권한부여 필요
- 액세스 요청, 액세스 권한 할당, 검토 및 만료 과정이 자동화

액세스 검토

- 새로운 직원들의 그룹 구성원 자격을 효율적으로 관리하고 기업 애플리케이션에 액세스 및 역할 할당 자동화
- 정당한 사용자에게 리소스 액세스 권한이 부여되었는지 확인 가능
- 사용자 및 게스트 액세스 모두 검토 및 관리 가능

사용 약관

- 새로운 직원이 된 사용자가 부서의 데이터나 애플리케이션에 액세스하기 전에 관련 정보를 사용자에게 사전에 표시 가능
- 사용자가 법률 또는 규정 준수 요구 사항에 대한 관련 고지 사항을 사전에 확인 가능

PIM (Privileged Identity Management)

PIM 기능은 역할을 부여하는 기간이나 그 과정을 관리해 주는 서비스로서, 조직에서 중요한 리소스에 대한 액세스를 정밀하게 관리, 제어 및 모니터링하여 해킹이나 사용자의 부주의하거나 부적절한 사용에 대비할 수 있다.

JIT(Just In Time) 방식으로 동작하며 정해진 시간에 정해진 사용자에게만 리소스에 대한 액세스 권한을 부여한다.

사용자가 리소스에 액세스할 수 있는 시간에 제한을 두는 방식으로 사용자의 부적절한 사용을 막을 수 있다.

특정 리소스 예를 들면 스토리지에 액세스 권한을 가진 사용자의 수를 제한하여 악의적인 액세스를 차단할 수 있다.

표시 가능한 권한 있는 역할이 활성화되면 관리자에게 알람을 보낸다.

감사 기능을 두어 사용자의 액세스 기록을 다운로드 받을 수 있다.

Azure ID 보호

Azure ID 보호를 위해서 ID 기반 위험의 감지 및 수정을 자동화하고 포털에서 데이터를 사용하는 위험도를 조사하며 심도 있는 조사를 위해서 타기업으로 위험 감지 데이터를 내보내는 기능을 가진다.

위험을 낮음, 중간, 높음의 세가지 계층으로 분류

분류된 계층별로 후속 조치 설정

위험이 감지되면 사용자에게 다단계 인증, 암호 재설정 또는 액세스 차단 등의 조치가 트리거 되도록 설정

로그인 위험 및 사용자 ID 위험 계산

위험한 사용자, 위험한 로그인, 위험 탐지 의 세가지 보고서 제공

보안에서 ID는 매우 중요하기 때문에 Azure AD에는 ID 보호를 위한 아주 좋은 기능들이 많구나!