VMware Identity Manager를 사용한 VMware Workspace ONE 배포 가이드

2018년 9월

VMware Workspace ONE

vmware®

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.
https://docs.vmware.com/kr/
VMware 웹 사이트에서는 최신 제품 업데이트도 제공합니다.
본 문서에 대한 의견이 있으시면 다음 주소로 피드백을 보내주십시오.
docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware 코리아
서울시 강남구
영동대로 517
아셈타워 13층
(우) 06164
전화: +82 2 3016 6500
팩스: +82 2 3016 6501
www.vmware.com/kr

목차

VMware Workspace ONE 배포 정보

VMware Identity Manager를 사용하는 VMware Workspace™ ONE™ 배포 가이드는 AirWatch에서 Workspace ONE에 대한 SSO(Single Sign-On), Workspace ONE UEM의 디바이스 관리 및 VMware Workspace ONE을 애플리케이션 카탈로그로 제공하기 위해 VMware Identity Manager™ 및 VMware Workspace ONE UEM™을 통합하는 방법에 대한 정보를 제공합니다.

Workspace ONE UEM와 VMware Identity Manager가 통합되면 Workspace ONE UEM에 등록된 디바이스의 사용자가 여러 암호를 입력하지 않고도 사용 설정된 애플리케이션에 안전하게 로그인할 수 있습니다.

대상

이 정보는 Workspace ONE UEM 및 VMware Identity Manager 서비스 모두에 익숙한 관리자를 위해 작성되었습니다.

2018년 9월 릴리스는 VMware Identity Manager Cloud 2018년 9월, VMware Identity Manager 3.3 및 Workspace ONE UEM 9.7에 적용됩니다.

1 Workspace ONE 소개

VMware Workspace® ONE®은 iOS, Android 및 Windows 10 디바이스에서 애플리케이션을 제공 및 관리하는 보안 엔터프라이즈 플랫폼입니다. ID, 애플리케이션 및 엔터프라이즈 모빌리티 관리는 Workspace ONE 플랫폼에 통합됩니다.

VMware Workspace ONE UEM® 및 VMware Identity Manager™는 애플리케이션 및 모바일 액세스 관리 서비스의 Workspace ONE 카탈로그에 통합됩니다.

VMware Identity Manager 서비스는 리소스에 SSO(Single Sign-On)하는 사용자에 대한 인증을 비롯한 ID 관련 구성 요소를 제공합니다. 네트워킹 및 인증에 관련된 정책 집합을 생성하여 이러한 리소스에 대한 액세스를 제어합니다.

Workspace ONE UEM 서비스는 디바이스 등록, 애플리케이션 배포 및 규정 준수 검사 도구를 제공하여 원격 액세스 디바이스가 회사 보안 표준을 준수하도록 합니다. Workspace ONE UEM에 등록된 디바이스의 사용자는 여러 암호를 입력하지 않고도 사용 설정된 애플리케이션에 안전하게 로그인할 수 있습니다.

본 장은 다음 항목을 포함합니다.

Workspace ONE 아키텍처 개요

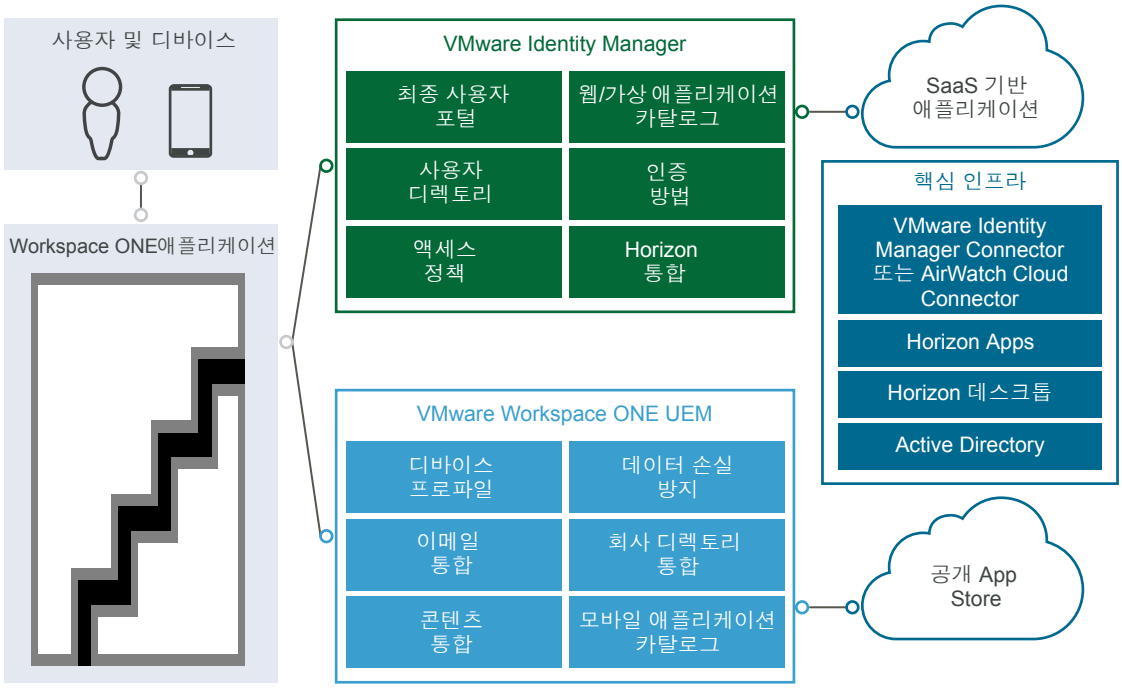
Workspace ONE을 사용하면 통합 카탈로그에서 관리되는 클라우드, 모바일 및 Windows 애플리케이션에 안전하게 액세스할 수 있습니다. 디바이스 액세스의 경우, iOS, Android 및 Windows 10 디바이스에서 Workspace ONE 기본 애플리케이션을 사용할 수 있습니다.

Workspace ONE이 배포되면 다음 VMware Identity Manager 및 Workspace ONE UEM 서비스를 구현해야 합니다.

- VMware Identity Manager Connector 구성 요소 또는 ACC(AirWatch Cloud Connector) 구성 요소를 구성할 수 있습니다.
- Active Directory의 사용자 및 그룹을 Workspace ONE 서비스와 동기화하기 위해 VMware Identity Manager 또는 Workspace ONE UEM Cloud Connector와 회사 Active Directory를 통합합니다.

- Workspace ONE UEM API 키 및 관리자 루트 인증서를 사용하고, Workspace ONE UEM를 통해 Workspace ONE 카탈로그, 규정 준수 검사 및 사용자 암호 인증을 사용하도록 설정하여 VMware Identity Manager를 구성합니다.

그림 1-1. Workspace ONE 아키텍처 개요



요구 사항

Workspace ONE 시스템 요구 사항은 다음과 같습니다.

표 1-1. Workspace ONE 시스템 요구 사항

Workspace ONE 요구 사항	세부 정보
Active Directory	Windows Server 2008 및 2008 R2 Windows Server 2012 및 2012 R2
VMware Identity Manager 및 Workspace ONE 콘솔에 액세스하기 위한 웹 브라우저	Windows용 Internet Explorer 11 Google Chrome 4.0 이상 Mozilla Firefox 40 이상 Safari 6.2.8 이상
VMware Identity Manager Connector 또는 AirWatch Cloud Connector가 설치되어 있음.	Windows Server 2008 R2 Windows Server 2012 또는 2012 R2 .NET Framework 4.6.2 VMware Identity Manager 커넥터 설치 가이드에 대해서는 VMware Identity Manager 설명서 센터를 참조하십시오. AirWatch Cloud Connector 설치 가이드에 대해서는 Workspace ONE UEM 설명서 센터를 참조하십시오.

Workspace ONE 기능 세부 정보

Workspace ONE의 주요 기능은 아래에 설명되어 있습니다.

기본 모바일 Workspace ONE 애플리케이션

사용자는 모바일 디바이스에 Workspace ONE 애플리케이션을 설치하고 회사 자격 증명을 사용하여 회사, 클라우드 및 모바일 애플리케이션에 SSO(Single Sign-On) 액세스할 수 있습니다.

웹, Horizon 및 Citrix 리소스에 대한 셀프 서비스 앱 카탈로그

Workspace ONE을 사용하면 통합 카탈로그를 사용하는 클라우드, 모바일 및 Windows 애플리케이션에 액세스할 수 있습니다. 이 카탈로그에는 VMware Identity Manager 및 VMware Workspace ONE UEM에 게시된 애플리케이션이 포함되어 있습니다. 지원되는 애플리케이션 유형에는 내부 웹, SaaS, 기본 모바일, 내부적으로 개발된 모바일, 레거시 및 최신 Windows, Horizon 7, VMware Horizon Cloud Service™, Citrix 게시된 패키지 및 ThinApp 패키지가 포함됩니다. 또한 애플리케이션 스토어에는 가상화된 데스크톱도 포함되어 있습니다.

SSO(Single Sign-on)를 사용하여 웹 및 가상 애플리케이션 실행

Workspace ONE에서는 모바일 애플리케이션에 대한 원터치 로그인 구현인 모바일 SSO(Single Sign-On)를 제공합니다. 모바일 SSO는 Android, iOS 및 Windows 10 디바이스에서 사용할 수 있습니다.

디바이스 규정 준수에 따른 조건부 액세스

Workspace ONE을 사용하여 인증에 네트워크 범위, 플랫폼 및 애플리케이션별 기준에 따라 조건부 액세스를 적용할 수 있습니다. 디바이스는 보안 규칙 준수를 입증해야만 애플리케이션에 대한 액세스 권한을 받을 수 있습니다. VMware Identity Manager에는 사용자가 디바이스에서 로그인할 때 Workspace ONE UEM 서버에서 디바이스 규정 준수 상태를 검사하도록 구성할 수 있는 액세스 정책 옵션이 있습니다.

다단계 인증

Workspace ONE에서는 VMware Verify 애플리케이션을 통해 다단계 인증을 제공합니다. 사용자가 강력한 인증이 요구되는 Workspace ONE 카탈로그 또는 애플리케이션에 액세스하려고 하면 VMware Verify에서 사용자 휴대폰으로 알림을 전송합니다. 사용자가 Workspace ONE에 대해 시도된 액세스를 확인하려면 [동의]를 쓸어넘겨 애플리케이션에 액세스해야 합니다.

어댑티브 관리

기본 수준의 보안만 요구하는 애플리케이션에서는 디바이스를 Workspace ONE UEM Mobile Device Management™에 등록할 필요가 없습니다. 사용자는 Workspace ONE 모바일 애플리케이션을 다운로드하고 설치하려는 애플리케이션을 선택할 수 있습니다. 더 높은 수준의 보안을 요구하는 애플리케이션의 경우 Workspace ONE 모바일 애플리케이션에서 직접 Workspace ONE UEM에 디바이스를 등록할 수 있습니다.

Workspace ONE 마법사 시작

Workspace ONE 시작 마법사를 사용하여 Workspace ONE UEM 및 VMware Identity Manager 서비스를 통합하여 Workspace ONE 환경을 만들기 위한 많은 구성 단계를 진행할 수 있습니다.

시작 마법사는 개별 설정을 구성하거나 편집하는 기능을 대신하지 않지만, 대부분의 고객은 초기 설정 작업을 대폭 자동화할 수 있습니다.

Workspace ONE 시작 마법사를 사용하여 다음을 설정할 수 있습니다.

- 엔터프라이즈 커넥터 및 디렉토리. 이 마법사는 회사 디렉토리에서 사용자 및 그룹을 가져오도록 Workspace ONE UEM Cloud Connector에서 VMware Enterprise System Connector를 설정하고 Active Directory 연결을 구성하는 단계를 안내합니다. 엔터프라이즈 커넥터를 설정하는 데 도움을 얻으려면 VMware Workspace ONE 빠른 구성 가이드를 참조하십시오.
- 자동 검색. 이 마법사를 사용해 자동 검색 서비스에 이메일 도메인을 등록하여, 최종 사용자가 Workspace ONE 애플리케이션을 통해 애플리케이션 포털에 더욱 쉽게 액세스하도록 할 수 있습니다. 최종 사용자는 조직 URL 대신 해당 이메일 주소를 입력할 수 있습니다.
- Workspace ONE 카탈로그. Workspace ONE 카탈로그 마법사에서는 Workspace ONE 카탈로그를 설정하는 단계를 안내합니다. Workspace ONE 사용자 지정 브랜딩 단계를 사용하여 회사 브랜드 정보를 Workspace ONE 카탈로그 및 애플리케이션에 추가할 수도 있습니다. Workspace ONE 카탈로그를 설정하는 데 도움을 얻으려면 VMware Workspace ONE 빠른 구성 가이드를 참조하십시오.
- 어댑티브 관리. 어댑티브 관리를 설정하여 사용자 디바이스에 프로파일이 설치되도록 요구함으로써 특정 애플리케이션을 제한합니다. 이 프로파일은 필요한 경우 회사 애플리케이션 및 데이터를 제거할 수 있도록 합니다. 또한 공개 애플리케이션을 App Store에서 수동으로 다운로드하여 이러한 애플리케이션을 개별적으로 관리 및 사용되도록 할 수도 있습니다.

시작 마법사는 충돌 가능성이 있는 기존 구성이 Workspace ONE UEM 또는 VMware Identity Manager 서비스에서 이미 사용되도록 설정된 경우 경고할 수 있습니다. 이러한 경우 또는 시작 마법사가 단계를 부분적으로만 완료한 경우 기능을 수동으로 구성할 수 있습니다. 이 가이드를 사용하여 Workspace ONE에 Workspace ONE UEM 및 VMware Identity Manager 서비스를 수동으로 구성할 수 있습니다.

VMware Identity Manager 에 Workspace ONE UEM 통합

2

사용자의 Single Sign-On 및 ID 관리를 위해 VMware Identity Manager 서비스를 사용하여 디바이스에 Workspace ONE UEM 모바일 관리 서비스를 설정하려면 서비스를 통합해야 합니다.

Workspace ONE UEM와 VMware Identity Manager가 통합되면 Workspace ONE UEM에 등록된 디바이스의 사용자가 여러 암호를 입력하지 않고도 Workspace ONE에 로그인하고 사용 설정된 애플리케이션에 안전하게 액세스할 수 있습니다.

Workspace ONE 시작 마법사는 Workspace ONE UEM 및 VMware Identity Manager를 통합하기 위한 여러 구성 단계를 안내할 수 있습니다. Workspace ONE 마법사를 실행하려면 VMware Workspace ONE 빠른 구성 가이드를 참조하십시오.

본 장은 다음 항목을 포함합니다.

- Workspace ONE UEM 콘솔에서 통합 설정
- VMware Identity Manager에서 Workspace ONE UEM 인스턴스 설정
- Workspace ONE UEM에 Workspace ONE 카탈로그 사용
- Workspace ONE UEM 관리 디바이스에 대한 규정 준수 검사 사용
- Workspace ONE UEM을 통한 사용자 암호 인증 사용
- 규정 준수 검사 규칙 구성
- Workspace ONE UEM 업그레이드 후 VMware Identity Manager 업데이트
- AirWatch Cloud Connector를 사용하여 인증 구현

Workspace ONE UEM 콘솔에서 통합 설정

VMware Identity Manager 서비스와 통합하려면 Workspace ONE UEM 콘솔에서 이러한 설정을 구성합니다.

- VMware Identity Manager 서비스와 통신하기 위한 Rest API 관리 키
- VMware Identity Manager가 구성되어 있는 동일한 조직 그룹에서 생성된 AirWatch Cloud Connector 암호 인증을 위한 REST 등록 사용자 API 키.
- VMware Identity Manager에 대한 API 관리 계정 및 Workspace ONE UEM에서 내보내고 VMware Identity Manager 콘솔의 AirWatch 설정에 추가되는 관리 인증 인증서.

Workspace ONE UEM 에서 REST API 키 만들기

VMware Identity Manager를 Workspace ONE UEM과 통합하려면 Workspace ONE UEM 콘솔에서 REST 관리 API 액세스 및 등록된 사용자 액세스를 사용하도록 설정해야 합니다. API 액세스를 사용하도록 설정하면 API 키가 생성됩니다.

절차

1 Workspace ONE UEM 콘솔에서 [글로벌] > [고객 수준 조직 그룹]을 선택하고 **그룹 및 설정 > 모든 설정 > 시스템 > 고급 > API > Rest API**로 이동합니다.

2 [일반] 탭에서 **추가**를 클릭하여 VMware Identity Manager 서비스에서 사용할 API 키를 생성합니다. 계정 유형은 **관리자**여야 합니다.

고유한 서비스 이름을 제공합니다. 설명(예: **IDM용 AirWatchAPI**)을 추가합니다.

3 등록 사용자 API 키를 생성하려면 **추가**를 다시 클릭합니다.

4 [계정 유형] 드롭다운 메뉴에서 **등록 사용자**를 선택합니다.

고유한 서비스 이름을 제공합니다. 설명(예: **IDM용 UserAPI**)을 추가합니다.

5 두 API 키를 복사하여 파일에 저장합니다.

VMware Identity Manager 콘솔에서 Workspace ONE UEM(AirWatch)을 설정할 때 이러한 키를 추가합니다.

6 **저장**을 클릭합니다.

VMware Workspace ONE UEM 관리자 루트 인증서 내보내기

관리 API 키를 만든 후에 Workspace ONE UEM 콘솔에서 관리자 계정을 추가하고 인증서 인증을 설정합니다.

REST API 인증서 기반 인증의 경우 Workspace ONE UEM 콘솔에서 사용자 수준 인증서가 생성됩니다. 사용되는 인증서는 Workspace ONE UEM 관리 루트 인증서에서 생성된 자체 서명된 Workspace ONE UEM 인증서입니다.

사전 요구 사항

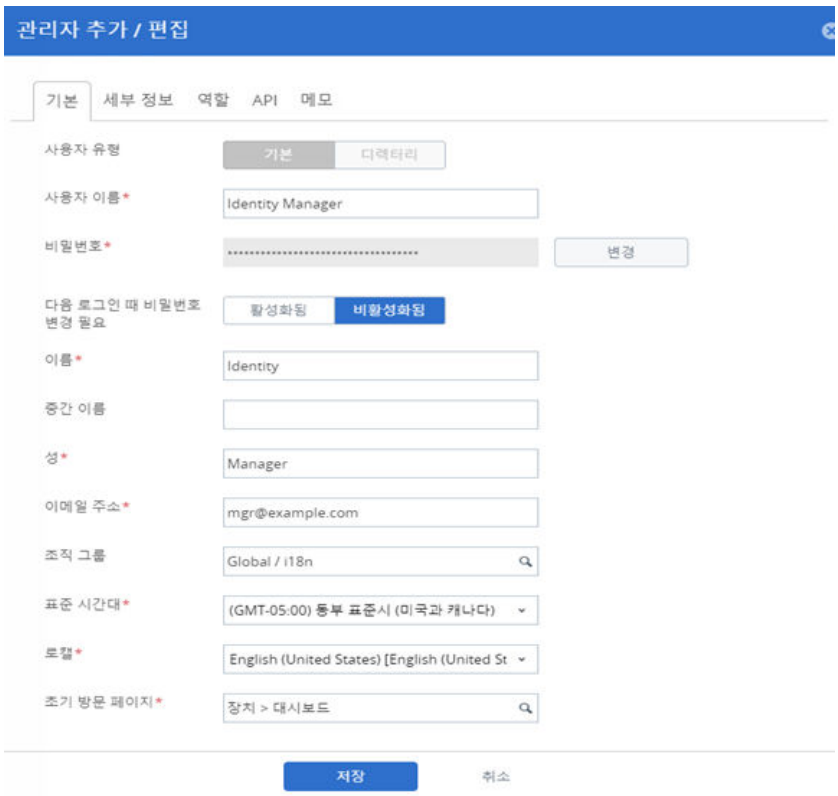
Workspace ONE UEM REST 관리 API 키가 만들어져 있습니다.

절차

1 Workspace ONE UEM 콘솔에서 [글로벌] > [고객 수준 조직 그룹]을 선택한 후 **계정 > 관리자 > 목록 보기**로 이동합니다.

2 **추가 > 관리자 추가**를 클릭합니다.

3 [기본] 탭의 필수 텍스트 상자에 인증서 관리자 이름과 암호를 입력합니다.



4 [역할] 탭을 선택하고 현재 조직 그룹을 선택한 후 두 번째 텍스트 상자를 클릭하고 **AirWatch 관리자**를 선택합니다.

5 [API] 탭을 선택하고 [인증] 텍스트 상자에서 **인증서**를 선택합니다.

6 인증서 암호를 입력합니다. 암호는 [기본] 탭에서 관리자에 대해 입력한 암호와 같습니다.

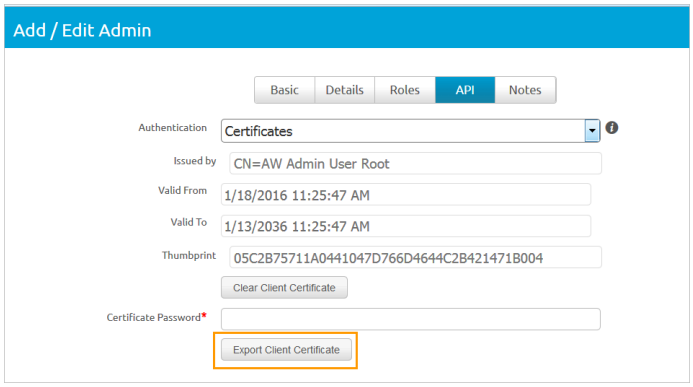
7 **저장**을 클릭합니다.

새 관리자 계정 및 클라이언트 인증서가 만들어집니다.

8 [목록 보기] 페이지에서 생성한 관리자를 선택하고 [API] 탭을 다시 엽니다.

인증서 페이지에 인증서에 대한 정보가 표시됩니다.

9 [인증서 암호] 텍스트 상자에 설정한 암호를 입력하고 **클라이언트 인증서 내보내기**를 클릭한 후 파일을 저장합니다.



클라이언트 인증서가 .p12 파일 유형으로 저장됩니다.

다음에 수행할 작업

VMware Identity Manager 콘솔에서 Workspace ONE UEM URL 설정을 구성합니다.

VMware Identity Manager 에서 Workspace ONE UEM 인스턴스 설정

Workspace ONE UEM 콘솔과 VMware Identity Manager 콘솔의 [ID 및 액세스 관리] 페이지에서 설정을 구성한 후에 Workspace ONE UEM URL, API 키 값 및 인증서를 입력합니다. Workspace ONE UEM 설정이 구성된 후에는 Workspace ONE에서 사용할 수 있는 기능 옵션을 사용하도록 설정할 수 있습니다.

VMware Identity Manager 에 Workspace ONE UEM 설정 추가

Workspace ONE UEM을 VMware Identity Manager와 통합하고 Workspace ONE UEM 기능 통합 옵션을 사용하도록 VMware Identity Manager의 Workspace ONE UEM 설정을 구성합니다. Workspace ONE UEM을 사용한 VMware Identity Manager 권한 부여를 위해 Workspace ONE UEM API 키 및 인증서가 추가됩니다.

사전 요구 사항

- 관리자가 Workspace ONE UEM 콘솔에 로그인하는 데 사용하는 Workspace ONE UEM 서버 URL.
- 통합 설정을 위해 VMware Identity Manager에서 Workspace ONE UEM 서버로 API 요청을 보내는 데 사용되는 Workspace ONE UEM 관리 API 키.
- API 호출을 하고 인증서 암호를 만드는 데 사용되는 Workspace ONE UEM 인증서 파일. 인증서 파일은 .p12 파일 형식이어야 합니다.

- Workspace ONE UEM 등록 사용자 API 키.
- Workspace ONE UEM에서 사용되는 테넌트 식별자인 테넌트의 Workspace ONE UEM 그룹 ID.

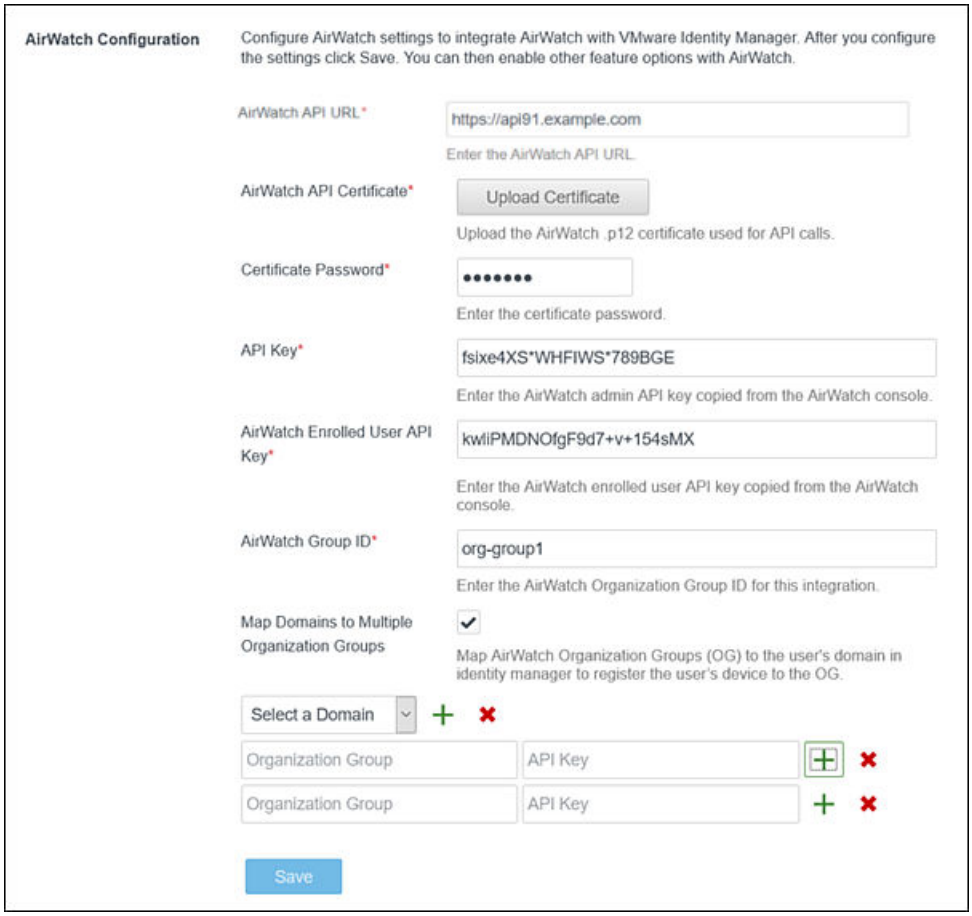
절차

1 VMware Identity Manager 콘솔의 [ID 및 액세스 관리] 탭에서 **설정 > AirWatch**를 클릭합니다.

2 다음 필드에 Workspace ONE UEM 통합 설정을 입력합니다.

필드	설명
AirWatch API URL	Workspace ONE UEM URL을 입력합니다. 예: `https://myco.ws1uem.com`
AirWatch API 인증서	API 호출을 수행하는 데 사용되는 인증서 파일을 업로드합니다.
인증서 암호	인증서 암호를 입력합니다.
AirWatch 관리 API 키	관리자 API 키 값을 입력합니다. API 키 값의 예는 FPseqCSataGcnJf8/Rvahzn/4jwkZENGkZzyc+jveeYs=입니다.
AirWatch 등록 사용자 API 키	등록된 사용자 API 키 값을 입력합니다.
AirWatch 그룹 ID	API 키 및 관리자 계정이 만들어진 조직 그룹의 Workspace ONE UEM 그룹 ID를 입력합니다.

3 **저장**을 클릭합니다.



다음에 수행할 작업

Workspace ONE UEM 카탈로그에 설정된 앱을 Workspace ONE 카탈로그에 병합하려면 기능 옵션 [Workspace ONE 카탈로그]를 사용하도록 설정합니다.

- Workspace ONE UEM 관리 디바이스가 Workspace ONE UEM 규정 준수 정책을 따르는지 확인하기 위해 규정 준수 검사를 사용합니다.

Workspace ONE UEM 관리 디바이스에 대한 규정 준수 검사 사용의 내용을 참조하십시오.

VMware Identity Manager 도메인을 Workspace ONE UEM 의 여러 조직 그룹에 매핑

Workspace ONE UEM에서 사용자 및 디바이스를 설정할 때 Workspace ONE UEM은 OG(조직 그룹)를 사용하여 사용자를 구성 및 그룹화하고 사용 권한을 설정합니다.
Workspace ONE UEM이 VMware Identity Manager에 통합되면 관리자 및 등록 사용자의 REST API 키를 유형이 [고객]인 Workspace ONE UEM 조직 그룹에만 구성할 수 있습니다.

다중 테넌시용으로 구성된 Workspace ONE UEM 환경에서 사용자 및 디바이스에 대해 많은 조직 그룹이 생성됩니다. 디바이스는 조직 그룹에 등록됩니다. 조직 그룹은 다중 테넌시 환경에 고유한 구성으로 설정될 수 있습니다. 예를 들어, 별도의 지리적 위치, 부서 또는 사용 사례별로 조직 그룹을 사용할 수 있습니다.

VMware Identity Manager에 구성된 도메인을 Workspace ONE UEM의 특정 조직 그룹에 연결하여 Workspace ONE을 통해 디바이스 등록을 관리할 수 있습니다. 사용자가 Workspace ONE에 로그인하면 VMware Identity Manager 내에 디바이스 등록 이벤트가 트리거됩니다. 디바이스 등록 중에 사용자 및 디바이스 조합에 사용 권한이 부여된 애플리케이션을 끌어오기 위한 요청이 Workspace ONE UEM로 전송됩니다.

Identity Manager에서 사용자를 찾고 해당 조직 그룹으로 디바이스를 성공적으로 등록하려면 Workspace ONE UEM이 VMware Identity Manager에 통합될 때 디바이스 조직 그룹을 식별해야 합니다.

VMware Identity Manager 서비스에서 Workspace ONE UEM 설정을 구성할 때 디바이스 조직 그룹 ID 및 API 키를 입력하여 도메인에 여러 OG를 매핑할 수 있습니다. 사용자가 디바이스에서 Workspace ONE에 로그인하면 사용자 레코드가 확인되고 디바이스가 Workspace ONE UEM의 해당 조직 그룹에 등록됩니다.

여러 조직 그룹을 구성하는 방법에 대한 자세한 내용은 다중 Workspace ONE UEM 조직 그룹 설정을 위한 배포 전략을 참조하십시오.

참고 Workspace ONE UEM이 VMware Identity Manager와 통합되고 여러 Workspace ONE UEM 조직 그룹이 구성되면 Active Directory 글로벌 카탈로그 옵션을 VMware Identity Manager 서비스에서 사용하도록 구성할 수 없습니다.

Workspace ONE UEM 에 Workspace ONE 카탈로그 사용

Workspace ONE UEM 인스턴스를 통해 VMware Identity Manager를 구성할 경우 Workspace ONE 카탈로그에 Workspace ONE UEM 카탈로그의 앱이 포함되도록 사용 설정할 수 있습니다. 최종 사용자는 Workspace ONE 포털에서 사용 권한이 부여된 모든 애플리케이션을 확인할 수 있습니다.

절차

1 VMware Identity Manager 콘솔의 [ID 및 액세스 관리] 탭에서 **설정 > AirWatch**를 클릭하고 [Workspace ONE 카탈로그] 섹션으로 이동합니다.

2 Identity Manager 카탈로그의 앱에 AirWatch 카탈로그의 앱을 포함하려면 **IDM에서 가져오기** 및 **Airwatch에서 가져오기**를 둘 다 사용하도록 설정합니다.

VMware Identity Manager 서비스를 구성하지 않은 상태로 모바일 디바이스에서 Workspace ONE 카탈로그를 사용할 경우 **AirWatch에서 가져오기**만 선택합니다.

IDM에서 가져오기를 사용하도록 설정하는 것이 기본값입니다.

3 **저장**을 클릭합니다.

다음에 수행할 작업

Workspace ONE UEM 최종 사용자에게 카탈로그에 액세스하고 Workspace ONE 포털을 보는 방법을 알려 줍니다.

Workspace ONE UEM 관리 디바이스에 대한 규정 준수 검사 사용

사용자가 디바이스를 등록한 경우 규정 준수를 평가하는 데 사용되는 데이터가 포함된 샘플이 스케줄에 따라 전송됩니다. 이 샘플 데이터 평가에서는 Workspace ONE UEM(UEM) 콘솔에서 관리자가 설정한 규정 준수 규칙을 디바이스가 준수하는지 확인합니다. 디바이스가 규정을 벗어난 경우 UEM 콘솔에 구성된 해당 작업이 수행됩니다.

VMware Identity Manager 서비스에는 사용자가 디바이스에서 로그인할 때 Workspace ONE UEM 서버에서 디바이스 규정 준수 상태를 검사하도록 구성할 수 있는 액세스 정책 옵션이 있습니다. 규정 준수 검사를 사용하면 디바이스가 규정을 벗어난 경우에 사용자가 애플리케이션에 로그인하거나 Single Sign-On을 통해 Workspace ONE 포털에 들어가는 것을 차단할 수 있습니다. 디바이스가 다시 규정을 준수하게 되면 로그인 기능이 복원됩니다.

디바이스 보안이 침해된 경우 Workspace ONE 애플리케이션이 자동으로 로그아웃되고 애플리케이션에 대한 액세스를 차단합니다. 디바이스가 어댑티브 관리를 통해 등록된 경우 UEM 콘솔을 통해 실행되는 엔터프라이즈 초기화 명령이 디바이스를 등록 해제하고 관리되는 애플리케이션을 디바이스에서 제거합니다. 관리되지 않는 애플리케이션은 제거되지 않습니다.

Workspace ONE UEM 규정 준수 정책에 대한 자세한 내용은 VMware Workspace ONE UEM 설명서 페이지에서 VMware Workspace ONE UEM 모바일 디바이스 관리 가이드를 참조하십시오.

Workspace ONE UEM 을 통한 사용자 암호 인증 사용

AirWatch Cloud Connector를 사용한 인증을 구현하려면 Workspace ONE UEM 기능을 통해 암호 인증을 사용하도록 설정해야 합니다.

사전 요구 사항

- VMware Identity Manager에 Workspace ONE UEM이 구성되어 있습니다.
- AirWatch Cloud Connector가 설치 및 활성화되어 있습니다.
- Workspace ONE UEM 디렉토리 서비스가 Active Directory와 통합되어 있습니다.

절차

1. VMware Identity Manager 콘솔의 [ID 및 액세스 관리] 탭에서 **설정 > AirWatch**를 클릭합니다.
2. [AirWatch를 통한 사용자 암호 인증] 섹션에서 **사용**을 선택합니다.
3. **저장**을 클릭합니다.

다음에 수행할 작업

AirWatch Cloud Connector 인증을 사용하려면 AirWatch Cloud Connector를 사용하여 인증 구현을 참조하십시오.

규정 준수 검사 규칙 구성

규정 준수 검사를 사용하도록 설정한 경우 Workspace ONE UEM에서 관리하는 디바이스에 대해 인증 및 디바이스 규정 준수 검사를 요구하는 액세스 정책 규칙을 만듭니다.

규정 준수 검사 정책 규칙은 iOS용 모바일 SSO, Android용 모바일 SSO 및 인증서 클라우드 배포와의 인증 체인에서 작동합니다. 규칙을 구성할 때 사용할 인증 방법이 디바이스 규정 준수 방법보다 앞에 나와야 합니다.

사전 요구 사항

인증 방법이 구성되고 기본 제공 ID 제공자에 연결되어 있습니다.

규정 준수 검사가 VMware Identity Manager AirWatch 페이지에서 사용되도록 설정되어 있습니다.

절차

1 VMware Identity Manager 콘솔의 [ID 및 액세스 관리] 탭에서 **관리 > 정책**을 선택합니다.

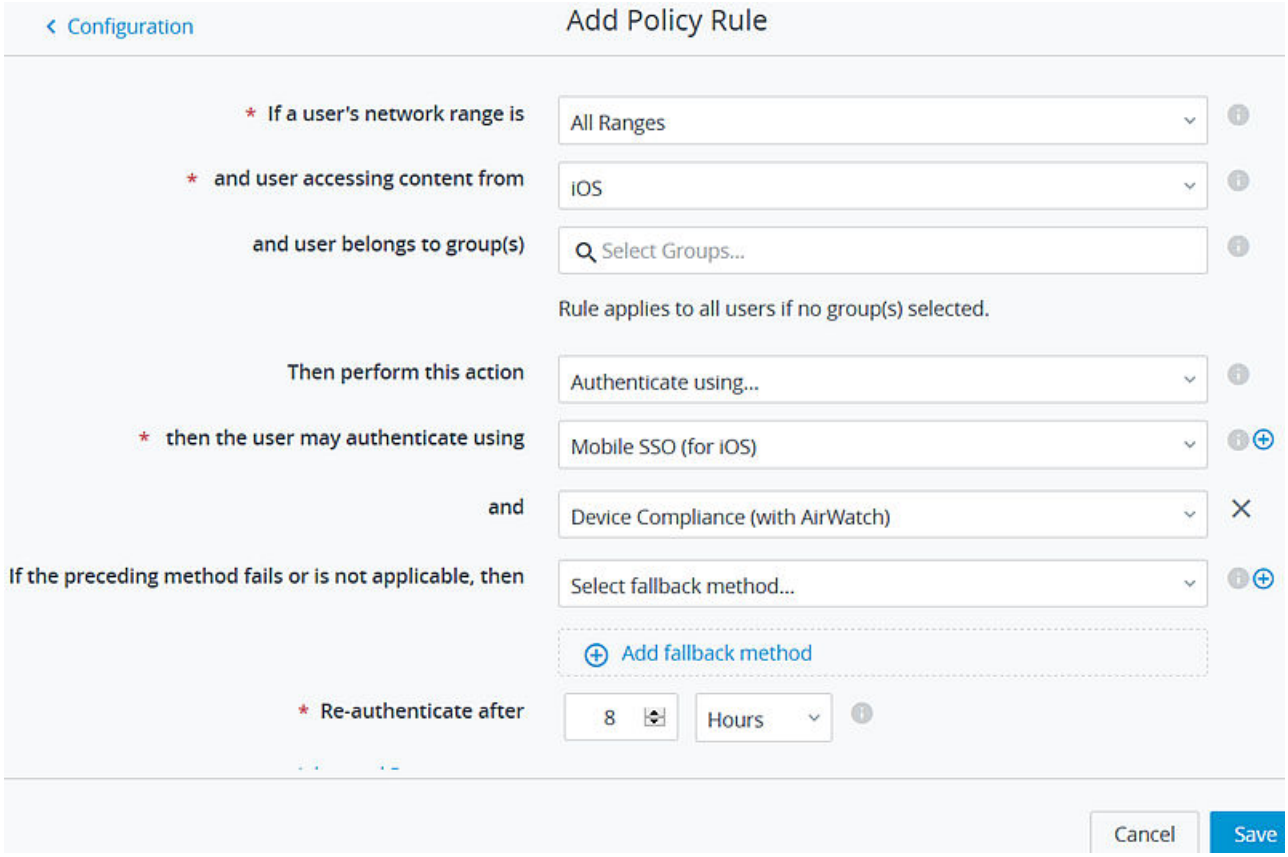
2 **기본 정책 편집**을 클릭합니다.

3 **다음**을 클릭합니다.

4 **정책 규칙 추가**를 클릭하여 규칙을 추가하거나, 편집할 규칙을 선택합니다.

옵션	설명
가령 사용자의 네트워크 범위가	네트워크 범위가 올바른지 확인하고 규칙을 추가하는 경우 네트워크 범위를 선택합니다.
및 사용자가 다음에서 콘텐츠에 액세스:	모바일 디바이스 유형을 선택합니다.
및 사용자 소속 그룹:	이 액세스 규칙을 특정 그룹에 적용하려는 경우 검색 상자에서 그룹을 검색합니다. 그룹을 선택하지 않으면 이 액세스 정책이 모든 사용자에게 적용됩니다.
그런 다음 이 작업 수행	**인증 방법...**을 선택합니다.
및 사용자 인증 방법:	적용할 모바일 디바이스 인증 방법을 선택합니다. +를 클릭하고 드롭다운 메뉴에서 **디바이스 규정 준수(AirWatch 사용)**를 선택합니다.
앞선 방법이 실패하거나 적용되지 않는 경우	필요한 경우 폴백 인증 방법을 구성합니다.
다음 시간 후에 재인증	사용자가 인증을 다시 받아야 하는 세션 길이를 선택합니다.

5 **저장**을 클릭합니다.



Workspace ONE UEM 업그레이드 후 VMware Identity Manager 업데이트

Workspace ONE UEM을 새 버전으로 업그레이드하는 경우 VMware Identity Manager 콘솔의 AirWatch 구성 페이지에서 [Workspace ONE 카탈로그] 및 [사용자 암호 인증] 옵션을 업데이트해야 합니다.

Workspace ONE UEM을 업그레이드한 후에 이러한 옵션을 저장하면 VMware Identity Manager 서비스의 AirWatch 설정이 새 버전의 Workspace ONE UEM으로 업데이트됩니다.

절차

1 Workspace ONE UEM을 업그레이드한 후에 VMware Identity Manager 콘솔에 로그인합니다.

2 [ID 및 액세스 관리] 탭에서 **설정 > AirWatch**를 클릭합니다.

3 페이지를 아래로 스크롤하여 **Workspace ONE 카탈로그** 섹션으로 이동한 후 **저장**을 클릭합니다.

4 **AirWatch를 통한 사용자 암호 인증** 섹션으로 스크롤한 후 **저장**을 클릭합니다.

Workspace ONE UEM 구성이 VMware Identity Manager 서비스의 새 버전으로 업데이트됩니다.

AirWatch Cloud Connector를 사용하여 인증 구현

VMware Enterprise Systems Connector의 ACC(AirWatch Cloud Connector) 구성 요소는 Workspace ONE의 사용자 암호 인증을 위해 VMware Identity Manager에 통합됩니다.

참고 Workspace ONE UEM에서 ACC를 설치하고 ACC 구성 요소를 구성합니다. AirWatch Cloud Connector 설치 및 구성에 대한 자세한 내용은 "VMware Enterprise Systems Connector 설치 및 구성" 가이드를 참조하십시오. ACC가 설치 및 구성된 후에 Workspace ONE UEM 디렉토리 서비스를 Active Directory와 통합합니다. 디렉토리 서비스를 사용하도록 설정하는 방법에 대한 정보는 VMware Workspace ONE UEM 디렉토리 서비스 가이드를 참조하십시오.

Workspace ONE에 대한 AirWatch Cloud Connector 인증을 구현하기 위해 VMware Identity Manager 콘솔에서 암호(Workspace ONE UEM Connector) 인증 방법이 기본 제공 ID 제공자와 연결됩니다.

Workspace ONE UEM에서 Just-In-Time 지원을 사용하도록 설정하여 새 사용자가 처음 로그인할 때 사용자를 VMware Identity Manager 디렉토리에 추가할 수 있습니다. Just-In-Time 지원을 사용하도록 설정하면 Workspace ONE에 액세스하기 위해 Workspace ONE UEM 서버의 예약된 다음 동기화까지 기다릴 필요가 없습니다. 대신 새 사용자는 iOS 또는 Android 디바이스나 해당 데스크톱 컴퓨터에서 Workspace ONE 포털에 로그인한 후 해당 Active Directory 사용자 이름 및 암호를 입력합니다. VMware Identity Manager 서비스는 AirWatch Cloud Connector를 통해 Active Directory 자격 증명을 인증하고 사용자 프로파일을 디렉토리에 추가합니다.

기본 제공 ID 제공자에서 인증 모델을 연결한 후에는 이러한 인증 방법에 적용할 액세스 정책을 만듭니다.

참고 사용자 이름과 암호 인증이 AirWatch Cloud Connector 배포에 통합되어 있습니다. 다른 VMware Identity Manager 지원 인증 방법을 사용하여 사용자를 인증하려면 VMware Identity Manager 커넥터를 구성해야 합니다.

사용자 특성 매핑 관리

Workspace ONE UEM 디렉토리와 VMware Identity Manager 디렉토리 사이의 사용자 특성 매핑을 구성할 수 있습니다.

VMware Identity Manager,의 [사용자 특성] 페이지에 있는 [ID 및 액세스 관리] 탭에는 Workspace ONE UEM 디렉토리 특성에 매핑된 기본 디렉토리 특성이 표시됩니다. 필수 특성은 별표가 표시됩니다. 프로파일에 필수 특성이 누락된 사용자는 VMware Identity Manager 서비스와 동기화되지 않습니다.

표 2-1. 기본 Workspace ONE UEM 디렉토리 특성 매핑

VMware Identity Manager 사용자 특성 이름	Workspace ONE UEM 사용자 특성에 대한 기본 매핑
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeID	employeeID
도메인	도메인
disabled(외부 사용자 사용 안 함)	disabled
phone	telephoneNumber
lastName	lastname*
firstName	firstname*
이메일	Email*
userName	username*

Workspace ONE UEM 디렉토리에서 VMware Identity Manager 디렉토리로 사용자 및 그룹 동기화

Workspace ONE UEM 콘솔에서 VMware Identity Manager 설정을 구성하여 Workspace ONE UEM 디렉토리의 조직 그룹 인스턴스와 VMware Identity Manager 간에 연결을 설정합니다. 이 연결은 VMware Identity Manager 서비스에서 생성한 디렉토리에 사용자 및 그룹을 동기화하는 데 사용됩니다.

사용자 및 그룹은 초기에 VMware Identity Manager 디렉토리에 수동으로 동기화됩니다. Workspace ONE UEM 동기화 스케줄에 따라 사용자 및 그룹을 VMware Identity Manager 디렉토리와 동기화할 시기가 결정됩니다.

사용자나 그룹이 Workspace ONE UEM 서버에서 추가 또는 삭제되면 변경 사항이 VMware Identity Manager 서비스에 즉시 반영됩니다.

사전 요구 사항

- VMware Identity Manager 로컬 관리자 이름 및 암호.
- Workspace ONE UEM 디렉토리에서 매핑할 특성 값을 식별합니다. 사용자 특성 매핑 관리의 내용을 참조하십시오.

절차

1 Workspace ONE UEM 콘솔의 [그룹 및 설정], [모든 설정] 페이지에서 [글로벌] > [고객 수준 조직 그룹]을 선택한 후 **시스템 > 엔터프라이즈 통합** >**VMware Identity Manager**로 이동합니다.

2 [서버] 섹션에서 **구성**을 클릭합니다.

> **참고** 구성 버튼은 같은 조직 그룹에 대해 [디렉토리 서비스]도 구성되어 있는 경우에만 사용할 수 있습니다. [구성] 버튼이 보이지 않으면 올바른 조직 그룹에 있지 않은 것입니다. 조직 그룹은 [글로벌] 드롭다운 메뉴에서 변경할 수 있습니다.

3 VMware Identity Manager 설정을 입력합니다.

옵션	설명
URL	테넌트 VMware URL을 입력합니다. 예: https://myco.identitymanager.com
관리자 이름	VMware Identity Manager 로컬 관리자 이름을 입력합니다.
관리자 암호	VMware Identity Manager 로컬 관리자 암호를 입력합니다.

4 **다음**을 클릭합니다.

5 사용자 지정 매핑을 사용하도록 설정하여 Workspace ONE UEM에서 VMware Identity Manager 서비스로의 사용자 특성 매핑을 구성합니다.

6 **연결 테스트**를 클릭하여 설정이 올바른지 확인합니다.

7 모든 사용자와 그룹을 VMware Identity Manager 서비스로 수동으로 동기화하려면 **지금 동기화**를 클릭합니다.

참고 시스템 로드의 제어를 위해 수동 동기화는 이전 동기화를 수행한 후 4시간이 지난 경우에만 수행할 수 있습니다.

VMware Identity Manager 서비스에서 Workspace ONE UEM 디렉토리가 생성되고 사용자 및 그룹이 VMware Identity Manager의 디렉토리에 동기화됩니다.

다음에 수행할 작업

VMware Identity Manager 콘솔의 [사용자 및 그룹] 탭을 검토하여 사용자 및 그룹 이름이 동기화되는지 확인합니다.

Workspace ONE UEM 에 대한 암호 인증 구성 관리

Workspace ONE UEM을 설치하고 VMware Identity Manager 서비스를 추가할 때 설정한 암호(AirWatch Connector) 구성을 검토하고 관리할 수 있습니다.

암호(AirWatch Connector) 인증 방법은 [ID 및 액세스 관리] > [인증 방법] 페이지에서 관리되며 [ID 제공자] 페이지의 기본 제공 ID 제공자와 연결됩니다.

중요 AirWatch Cloud Connector 소프트웨어가 업그레이드되면 VMware Identity Manager 콘솔 AirWatch 페이지에서 Workspace ONE UEM 구성을 업데이트해야 합니다.

절차

1 VMware Identity Manager 콘솔의 [ID 및 액세스 관리] 탭에서 **인증 방법**을 선택합니다.

2 **암호(AirWatch Connector)** 구성 열에서 연필 모양 아이콘을 클릭합니다.

3 구성을 검토합니다.

옵션	설명
AirWatch 암호 인증 사용	이 확인란을 선택하면 Workspace ONE UEM 암호 인증이 사용되도록 설정됩니다.
AirWatch 관리 콘솔 URL	Workspace ONE UEM URL로 미리 채워집니다.

옵션	설명
AirWatch API 키	Workspace ONE UEM 관리 API 키로 미리 채워집니다.
인증에 사용된 인증서	Workspace ONE UEM Cloud Connector 인증서로 미리 채워집니다.
인증서용 암호	Workspace ONE UEM Cloud Connector 인증서에 대한 암호로 미리 채워집니다.
AirWatch 그룹 ID	조직 그룹 ID로 미리 채워집니다.
허용된 인증 시도 횟수	Workspace ONE UEM 암호 인증을 사용하여 로그인할 경우 최대 로그인 시도 실패 횟수입니다. 실패한 로그인 횟수가 이 값에 도달하면 추가 로그인 시도가 허용되지 않습니다. VMware Identity Manager 서비스에서는 폴백 인증 방법이 구성된 경우 해당 방법을 사용하려고 시도합니다. 기본값은 5회입니다.
JIT 사용	JIT를 사용하지 않도록 설정한 경우 사용자가 처음 로그인할 때 VMware Identity Manager 서비스에서 사용자의 Just-in-Time 프로비저닝을 동적으로 사용하도록 설정하려면 이 확인란을 선택합니다.

4 **저장**을 클릭합니다.

내장 ID 제공자 구성

여러 내장 ID 제공자를 구성한 후 [ID 및 액세스 관리]의 [관리] > [인증 방법] 페이지에서 구성한 인증 방법을 연결할 수 있습니다.

절차

1 [ID 및 액세스 관리] 탭에서 **관리 > ID 제공자**로 이동합니다.

2 **ID 제공자 추가**를 클릭하고 **내장 IDP 생성**을 선택합니다.

옵션	설명
ID 제공자 이름	이 내장 ID 제공자 인스턴스의 이름을 입력합니다.
사용자	인증할 사용자를 선택합니다. 구성된 디렉토리가 나열됩니다.
네트워크	서비스에 구성된 기존 네트워크 범위가 나열됩니다. IP 주소를 기반으로 사용자에 대해 네트워크 범위(인증을 위해 이 ID 제공자 인스턴스로 전송할 네트워크 범위)를 선택합니다.
인증 방법	서비스에 구성된 인증 방법이 표시됩니다. 이 기본 제공 ID 제공자에 연결할 인증 방법에 대한 확인란을 선택합니다. 디바이스 규정 준수(Workspace ONE UEM 사용) 및 암호(AirWatch Connector)의 경우 AirWatch 구성 페이지에서 해당 옵션이 사용되도록 설정되어 있는지 확인합니다.

3 **추가**를 클릭합니다.

다음에 수행할 작업

기본 액세스 정책 규칙을 구성하여 해당 규칙에 인증 정책을 추가합니다. 규정 준수 검사 규칙 구성의 내용을 참조하십시오.

Workspace ONE UEM 관리 iOS 디바이스에 대한 모바일 Single Sign-On 인증 구현

3

iOS 디바이스 인증의 경우 VMware Identity Manager는 VMware Identity Manager 서비스에 기본 제공되는 ID 제공자를 사용하여 모바일 SSO 인증에 대한 액세스를 제공합니다.

이 iOS 디바이스 인증 방법에서는 커넥터 또는 타사 시스템을 사용하지 않고 KDC(키 배포 센터)를 사용합니다. Kerberos 인증은 도메인에 로그인한 사용자가 추가 인증 없이 해당 Workspace ONE 애플리케이션 포털에 액세스할 수 있도록 합니다.

본 장은 다음 항목을 포함합니다.

iOS용 모바일 SSO 구성을 위한 구현 개요

Workspace ONE UEM 관리 iOS 9 이상 디바이스에 대한 모바일 SSO 인증을 구현하려면 다음 구성 단계가 필요합니다.

- iOS용 모바일 SSO를 구성할 발급자 인증서를 다운로드합니다.
  - Active Directory 인증서 서비스를 사용하는 경우 Active Directory 인증서 서비스에서 Kerberos 인증서 배포를 위한 CA(인증 기관) 템플릿을 구성합니다. 그런 다음 Active Directory 인증 기관을 사용하도록 Workspace ONE UEM를 구성합니다. Workspace ONE UEM 콘솔에서 인증서 템플릿을 추가합니다. iOS용 모바일 SSO를 구성할 발급자 인증서를 다운로드합니다.

  - Workspace ONE UEM 인증 기관을 사용하는 경우 VMware Identity Manager [통합] 페이지에서 [인증서]를 사용하도록 설정합니다. iOS용 모바일 SSO를 구성할 발급자 인증서를 다운로드합니다.
- 사용할 KDC(키 배포 센터)를 설정합니다.
- Workspace ONE UEM 콘솔에서 iOS 디바이스 프로파일을 구성하고 단일 로그인을 사용하도록 설정합니다.
- 모바일 SSO(iOS) 인증 방법을 구성합니다.
- VMware Identity Manager 콘솔에서 내장 ID 제공자를 구성한 후 iOS용 모바일 SSO 인증을 연결합니다.

Workspace ONE UEM 에서 Active Directory CA(인증 기관) 구성

Workspace ONE UEM 관리 iOS 9 모바일 디바이스에 대한 Single Sign-On 인증을 설정하려면 Active Directory와 Workspace ONE UEM 간에 신뢰 관계를 설정하고 VMware Identity Manager에서 iOS용 모바일 SSO 인증 방법을 사용하도록 설정하면 됩니다.

Active Directory 인증서 서비스에서 Kerberos 인증서 배포에 대해 CA(인증 기관) 및 인증서 템플릿을 구성한 후에 Workspace ONE UEM을 사용하여 인증에 사용되는 인증서를 요청하고 Workspace ONE UEM 콘솔에 CA(인증 기관)를 추가합니다.

절차

1 Workspace ONE UEM 콘솔 주 메뉴에서 **디바이스 > 인증서 > 인증 기관**으로 이동합니다.

2 **추가**를 클릭합니다.

3 [인증 기관] 페이지에서 다음을 구성합니다.

참고 이 양식을 작성하기 전에 Microsoft AD CS가 기관 유형으로 선택되어 있는지 확인합니다.

옵션	설명
이름	새 CA(인증 기관)의 이름을 입력합니다.
기관 유형	**Microsoft ADCS**를 선택했는지 확인합니다.
프로토콜	프로토콜로 **ADCS**를 선택합니다.
서버 호스트 이름	서버의 URL을 입력합니다. https://{servername.com}/certsrv.adcs/ 형식으로 호스트 이름을 입력합니다. 사이트는 설정 방식에 따라 http 또는 https일 수 있습니다. URL에는 후행 /가 포함되어야 합니다. **참고** URL을 테스트할 때 연결이 실패하면 주소에서 http:// 또는 https://를 제거하고 연결을 다시 테스트합니다.
기관 이름	ADCS 끝점이 연결되는 CA(인증 기관)의 이름을 입력합니다. 이 이름은 CA(인증 기관) 서버에서 CA(인증 기관) 애플리케이션을 실행하여 찾을 수 있습니다.

옵션	설명
인증	**서비스 계정**을 선택했는지 확인합니다.
사용자 이름 및 암호	Workspace ONE UEM에서 인증서를 요청하고 발급하기 위한 충분한 액세스 권한이 있는 AD CS 관리자 계정의 사용자 이름 및 암호를 입력합니다.

4 **저장**을 클릭합니다.

다음에 수행할 작업

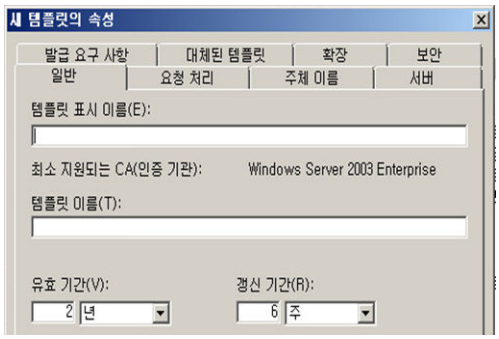
Workspace ONE UEM에서 인증서 템플릿을 구성합니다.

Active Directory CA(인증 기관) 사용을 위한 Workspace ONE UEM 구성

CA(인증 기관) 템플릿은 Kerberos 인증서 배포에 적합하게 구성해야 합니다. AD CS(Active Directory 인증서 서비스)에서는 기존 Kerberos 인증 템플릿을 복제하여 iOS Kerberos 인증에 사용할 새 CA(인증 기관) 템플릿을 구성할 수 있습니다.

AD CS에서 Kerberos 인증 템플릿을 복제할 때, [새 템플릿] 대화상자의 [속성]에서 다음 정보를 구성해야 합니다.

그림 3-1. 새 템플릿 대화상자의 Active Directory 인증서 서비스 속성



- **일반** 탭. 템플릿 표시 이름과 템플릿 이름을 입력합니다. 예: iOSKerberos. 이 이름은 인증서 템플릿 스냅인, 인증서 스냅인, 인증 기관 스냅인에 표시되는 표시 이름입니다.
- **요청 처리** 탭. **개인 키 내보내기 허용**을 사용하도록 설정합니다.
- **주체 이름** 탭. **요청에서 공급** 라디오 버튼을 선택합니다. 주체 이름은 Workspace ONE UEM에서 인증서를 요청할 때 Workspace ONE UEM에서 제공합니다.
- **확장** 탭. 애플리케이션 정책을 정의합니다.
  - [애플리케이션 정책]을 선택하고 [편집]을 클릭하여 새 애플리케이션 정책을 추가합니다. 이 정책의 이름을 Kerberos Client Authentication이라고 지정합니다.
  - 다음과 같이 OID(개체 식별자)를 추가합니다. 1.3.6.1.5.2.3.4. 이를 변경하면 안 됩니다.
  - [애플리케이션 정책 설명] 목록에서 Kerberos Client Authentication 정책과 Smart Card Authentication 정책을 제외한 모든 정책을 삭제합니다.

- **보안** 탭. 인증서를 사용할 수 있는 사용자 목록에 Workspace ONE UEM 계정을 추가합니다. 계정에 대한 사용 권한을 설정합니다. 보안 주체가 인증서 템플릿의 사용 권한을 포함한 인증서 템플릿의 모든 특성을 수정하도록 허용하려면 [모든 권한]을 설정합니다. 그렇지 않은 경우에는 조직의 요구 사항에 따라 사용 권한을 설정합니다.

변경 사항을 저장합니다. Active Directory CA(인증 기관)에서 사용하는 템플릿의 목록에 템플릿을 추가합니다.

Workspace ONE UEM에서 CA(인증 기관)를 구성하고 인증서 템플릿을 추가합니다.

Workspace ONE UEM 에서 인증서 템플릿 추가

사용자 인증서를 생성하는 데 사용되는 CA(인증 기관)를 연결하는 인증서 템플릿을 추가합니다.

사전 요구 사항

Workspace ONE UEM에서 CA(인증 기관)를 구성합니다.

절차

1 Workspace ONE UEM 콘솔에서 **시스템 > 엔터프라이즈 통합 > 인증 기관**으로 이동합니다.

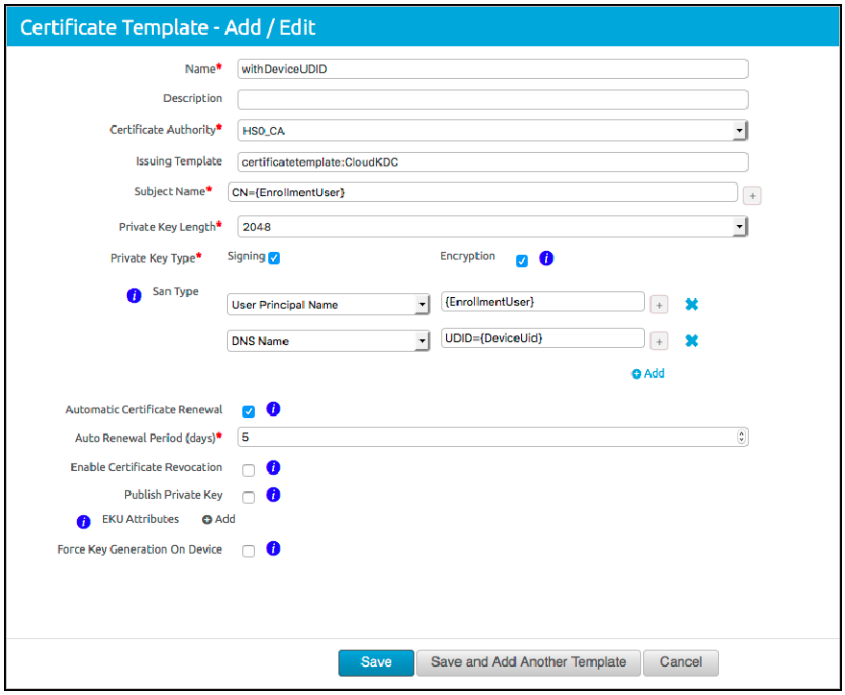
2 **템플릿 요청** 탭을 선택하고 **추가**를 클릭합니다.

3 인증서 템플릿 페이지에서 다음을 구성합니다.

옵션	설명
이름	Workspace ONE UEM에서 새 요청 템플릿의 이름을 입력합니다.
CA(인증 기관)	드롭다운 메뉴에서 만들어진 CA(인증 기관)를 선택합니다.
템플릿 발급	AD CS에서 만든 것과 정확히 동일하게 Microsoft CA 인증서 템플릿 이름을 입력합니다. 예를 들어 **iOSKerberos**를 입력합니다.
주체 이름	템플릿에 대한 주체 이름을 입력합니다. +를 클릭하여 목록에서 조회 값을 선택할 수 있습니다. 텍스트 상자에서 **CN=** 다음에 값을 입력해야 합니다. DeviceUid 조회 유형을 선택하는 경우 값 뒤에 콜론(:)을 입력하고 목록에서 조회 값을 선택합니다. 예를 들어 **CN={DeviceUid}:{lookupvalue}**를 입력합니다. 여기서 {} 텍스트 상자는 Workspace ONE UEM 조회 값입니다. 콜론(:)을 포함해야 합니다. 이 텍스트 상자에 입력한 텍스트는 인증서를 수신한 사용자 또는 디바이스를 확인하는 데 사용할 수 있는 인증서의 주체입니다.
개인 키 길이	이 개인 키 길이는 AD CS에 사용되는 인증서 템플릿의 설정과 일치합니다. 일반적으로 2048입니다.
개인 키 유형	**서명** 및 **암호화** 확인란을 선택합니다.
SAN 유형	**+추가**를 클릭합니다. 주체 대체 이름으로 **사용자 계정 이름**을 선택합니다. 값은 **{EnrollmentUser}**여야 합니다. 디바이스 규정 준수 검사를 Kerberos 인증으로 구성할 때 DeviceUid를 주체 이름 조회 값으로 구성하지 않은 경우 UDID(디바이스 고유 식별자)를 포함할 두 번째 SAN 유형을 추가합니다. SAN 유형 **DNS 이름**을 선택합니다. 값은 **UDID={DeviceUid}**여야 합니다.
자동 인증서 갱신	이 템플릿을 사용하는 인증서가 만료일 전에 자동으로 갱신되도록 하려면 이 확인란을 선택합니다.
자동 갱신 기간(일)	자동 갱신(일)을 지정합니다.

옵션	설명
인증서 해지 사용	해당 디바이스가 등록 취소되거나 삭제될 경우 또는 해당 프로파일이 제거될 경우 인증서를 자동으로 해지하려면 이 확인란을 선택합니다.
개인 키 게시	이 확인란을 선택하여 개인 키를 게시합니다.
개인 키 대상	디렉토리 서비스 또는 사용자 지정 웹 서비스

4 **저장**을 클릭합니다.



다음에 수행할 작업

VMware Identity Provider 콘솔에서 iOS용 모바일 SSO 인증 방법으로 내장 ID 제공자를 구성합니다.

Kerberos 인증을 위한 Workspace ONE UEM 인증 기관 사용

기본 제공 Kerberos 인증을 사용하여 Workspace ONE UEM 관리 iOS 9 모바일 디바이스에 Single Sign-On을 설정하려는 경우 Active Directory CA(인증 기관) 대신에 Workspace ONE UEM 인증 기관을 사용할 수 있습니다. Workspace ONE UEM 콘솔에서 Workspace ONE UEM 인증 기관을 사용하도록 설정하고 VMware Identity Manager 서비스에서 사용할 CA 발급자 인증서를 내보낼 수 있습니다.

Workspace ONE UEM 인증 기관은 SCEP(단순 인증서 등록 프로토콜)를 따르도록 설계되었으며 SCEP를 지원하는 Workspace ONE UEM 관리 디바이스에서 사용됩니다. Workspace ONE UEM과의 VMware Identity Manager 통합은 Workspace ONE UEM 인증 기관을 사용하여 iOS 9 모바일 디바이스에 인증서를 프로파일의 일부로 발급합니다.

Workspace ONE UEM 인증 기관 발급자 루트 인증서는 OCSP 서명 인증서이기도 합니다.

Workspace ONE UEM 인증 기관 사용 설정 및 내보내기

Workspace ONE UEM에 VMware Identity Manager가 사용하도록 설정되어 있으면 Workspace ONE UEM 발급자 루트 인증서를 생성할 수 있고 관리되는 iOS 9 모바일 디바이스에서 iOS용 모바일 SSO 인증에 사용할 인증서를 내보낼 수 있습니다.

절차

1 Workspace ONE UEM 콘솔에서 **시스템 > 엔터프라이즈 통합** > **VMware Identity Manager**로 이동합니다.

Workspace ONE UEM 인증 기관을 사용하도록 설정하려면 조직 그룹 유형이 [고객]이어야 합니다.

팁 그룹 유형을 보거나 변경하려면 [그룹 및 설정]으로 이동한 후 **그룹 > 조직 그룹**> **조직 그룹 세부 정보**를 선택합니다.

2 **구성**을 클릭합니다.

3 [인증서] 섹션에서 **사용**을 클릭합니다.

페이지에 발급자 루트 인증서 세부 정보가 표시됩니다.

4 **내보내기**를 클릭하고 파일을 저장합니다.

다음에 수행할 작업

VMware Identity Manager 콘솔의 내장 ID 제공자에서 Kerberos 인증을 구성하고 인증 기관 발급자 인증서를 추가합니다.

iOS 디바이스의 인증에 키 배포 센터 사용

iOS 디바이스의 경우 서비스를 Kerberos에 통합합니다. Kerberos 인증은 도메인에 로그인한 사용자가 추가 인증 없이 해당 애플리케이션 포털에 액세스할 수 있도록 합니다. 이 iOS 디바이스 인증 방법에서는 커넥터 또는 타사 시스템을 사용하지 않고 KDC(키 배포 센터)를 사용합니다.

VMware Identity Manager 클라우드 테넌트에서는 KDC를 관리하거나 구성할 필요가 없습니다.

온-프레미스 배포의 경우 두 개의 KDC 서비스 옵션을 사용할 수 있습니다.

- 기본 제공 KDC. 기본 제공 KDC를 사용하려면 장치에서 KDC를 초기화하고 Kerberos 클라이언트가 KDC를 찾을 수 있도록 공용 DNS 항목을 생성해야 합니다. 기본 제공된 KDC를 사용하도록 설정하는 방법에 대한 자세한 내용은 VMware Identity Manager 관리 가이드를 참조하십시오.
- VMware Identity Manager 클라우드 호스팅된 서비스로서의 KDC. 클라우드의 KDC를 사용하려면 [iOS 인증 어댑터] 페이지에서 해당 영역 이름을 선택해야 합니다.

참고 VMware Identity Manager가 Windows 환경의 Workspace ONE UEM에서 설치 및 구성되면 VMware Identity Manager 클라우드 호스팅 KDC 서비스를 사용하도록 iOS 모바일 인증 방법을 구성해야 합니다.

클라우드 호스팅된 KDC 서비스 사용

iOS용 모바일 SSO에 대해 Kerberos 인증 사용을 지원하기 위해 VMware Identity Manager는 클라우드 호스팅된 KDC 서비스를 제공합니다.

클라우드에 호스팅된 KDC 서비스는 Windows 환경에서 VMware Identity Manager을 통해 Workspace ONE UEM 서비스를 배포할 때 사용해야 합니다.

VMware Identity Manager 장치에서 관리되는 KDC를 사용하려면 VMware Identity Manager 설치 및 구성 가이드의 "iOS 디바이스에서 Kerberos 인증 사용 준비"를 참조하십시오.

iOS용 모바일 SSO 인증을 구성할 때 클라우드 호스팅된 KDC 서비스의 영역 이름을 구성합니다. 영역은 인증 데이터를 유지 관리하는 관리 엔티티의 이름입니다. [저장]을 클릭하면 VMware Identity Manager 서비스가 클라우드 호스팅된 KDC 서비스에 등록됩니다. KDC 서비스에 저장되는 데이터는 iOS용 모바일 SSO 인증 방법의 구성을 기준으로 하며 CA 인증서, OCSP 서명 인증서 및 OCSP 요청 구성 세부 정보를 포함합니다.

로깅 레코드는 클라우드 서비스에 저장됩니다. 로깅 레코드의 PII(개인 식별 가능 정보)에는 사용자 프로파일의 Kerberos 인증 이름, 주체 DN 및 UPN, 이메일 SAN 값, 사용자 인증서의 디바이스 ID, 사용자가 액세스하는 IDM 서비스의 FQDN이 포함됩니다.

클라우드 호스팅된 KDC 서비스를 사용하려면 VMware Identity Manager를 다음과 같이 구성해야 합니다.

- VMware Identity Manager 서비스의 FQDN은 인터넷에서 연결할 수 있어야 합니다. VMware Identity Manager에서 사용하는 SSL/TLS 인증서는 공개적으로 서명되어야 합니다.
- 아웃바운드 요청/응답 포트 88(UDP) 및 포트 443(HTTPS/TCP)은 VMware Identity Manager 서비스에서 액세스할 수 있어야 합니다.
- OCSP를 사용하도록 설정하는 경우 인터넷에서 OCSP 응답자에 연결할 수 있어야 합니다.

iOS용 모바일 SSO 인증 구성

VMware Identity Manager 콘솔의 [인증 방법] 페이지에서 iOS용 모바일 SSO 인증 방법을 구성합니다. 내장 ID 제공자에서 사용할 모바일 SSO(iOS용) 인증 방법을 선택합니다.

사전 요구 사항

- Workspace ONE UEM 테넌트에서 사용자에게 인증서를 발급하는 데 사용되는 CA(인증 기관) PEM 또는 DER 파일.
- 해지 검사의 경우 OCSP 응답자의 서명 인증서.
- KDC 서비스의 경우 KDC 서비스의 영역 이름을 선택합니다. 기본 제공 KDC 서비스를 사용하는 경우 KDC가 초기화되어야 합니다. 기본 제공된 KDC 세부 정보에 대해서는 "VMware Identity Manager 설치 및 구성"을 참조하십시오.

절차

1 VMware Identity Manager 콘솔의 [ID 및 액세스 관리] 탭에서 **관리 > 인증 방법**으로 이동합니다.

2 **모바일 SSO(iOS용)**에 대한 [구성] 열에서 연필 아이콘을 클릭합니다.

3 Kerberos 인증 방법을 구성합니다.

옵션	설명
KDC 인증 사용	사용자가 Kerberos 인증을 지원하는 iOS 디바이스를 사용하여 로그인할 수 있게 하려면 이 확인란을 선택합니다.
영역	클라우드의 테넌트 배포에서 영역 값은 읽기 전용입니다. 표시되는 영역 이름은 테넌트에 대한 Identity Manager 영역 이름입니다. 온-프레미스 배포에서 클라우드 호스팅 KDC를 사용하는 경우 제공된 미리 정의된 지원되는 영역 이름을 입력합니다. 이 매개 변수의 텍스트는 모두 대문자로 입력해야 합니다. 예: OP.VMWAREIDENTITY.COM 기본 제공 KDC를 사용하는 경우 KDC를 초기화할 때 구성한 영역 이름이 표시됩니다.
루트 및 중간 CA 인증서	CA(인증 기관) 발급자 인증서 파일을 업로드합니다. PEM 또는 DER 파일 형식을 지원합니다.
업로드된 CA 인증서 주체 DN	업로드된 인증서 파일의 내용이 여기에 표시됩니다. 둘 이상의 파일을 업로드할 수 있고 포함되는 모든 인증서가 목록에 추가됩니다.
OCSP 사용	OCSP(온라인 인증서 상태 프로토콜) 인증서 검증 프로토콜을 사용하여 인증서의 해지 상태를 가져오려면 이 확인란을 선택합니다.
OCSP Nonce 전송	OCSP 요청의 고유한 식별자를 응답으로 전송하려면 이 확인란을 선택합니다.
OCSP 응답자의 서명 인증서	응답자의 OCSP 인증서를 업로드합니다. Workspace ONE UEM 인증 기관을 사용할 경우 발급자 인증서가 OCSP 인증서로 사용됩니다. 여기에서 Workspace ONE UEM 인증서도 업로드합니다.
OCSP 응답자의 서명 인증서 주체 DN	업로드된 OCSP 인증서 파일이 여기에 나열됩니다.
취소 메시지	인증이 너무 오래 걸릴 경우 표시되는 사용자 지정 로그인 메시지를 작성합니다. 사용자 지정 메시지를 만들지 않을 경우 기본 메시지는 Attempting to authenticate your credentials입니다.
취소 링크 사용	인증에 너무 오래 시간이 걸리면 사용자에게 [취소]를 클릭하여 인증 시도를 중지하고 로그인을 취소할 수 있는 기능을 제공합니다. [취소] 링크를 사용하도록 설정하면 표시되는 인증 오류 메시지 끝에 [취소]가 나타납니다.
엔터프라이즈 디바이스 관리 서버 URL	디바이스가 MDM 관리를 위해 Workspace ONE UEM에 등록되지 않아 액세스가 거부될 경우 사용자를 리디렉션할 MDM(모바일 디바이스 관리) 서버 URL을 입력합니다. 이 URL은 인증 실패 오류 메시지에 표시됩니다. 여기에 URL을 입력하지 않으면 일반 액세스 거부 메시지가 표시됩니다.

4 **저장**을 클릭합니다.

다음에 수행할 작업

- 내장 ID 제공자에서 모바일 SSO(iOS용) 인증 방법을 연결합니다.

모바일 SSO iOS 인증을 위한 기본 제공 ID 제공자 구성

기본 제공 ID 제공자를 구성한 후 [ID 및 액세스 관리]의 [관리] > [인증 방법] 페이지에서 구성한 iOS용 모바일 SSO 인증 방법을 연결할 수 있습니다.

사전 요구 사항

[인증 방법] 페이지에 구성된 모바일 SSO(iOS용) 인증

절차

1 [ID 및 액세스 관리] 탭에서 **관리 > ID 제공자**로 이동합니다.

2 **ID 제공자 추가**를 클릭하고 **내장 IDP 생성**을 선택합니다.

옵션	설명
ID 제공자 이름	이 내장 ID 제공자 인스턴스의 이름을 입력합니다.
사용자	인증할 사용자를 선택합니다. 구성된 디렉토리가 나열됩니다.
네트워크	서비스에 구성된 기존 네트워크 범위가 나열됩니다. IP 주소를 기반으로 사용자에 대해 네트워크 범위(인증을 위해 이 ID 제공자 인스턴스로 전송할 네트워크 범위)를 선택합니다.
인증 방법	서비스에 구성된 인증 방법이 표시됩니다. 이 기본 제공 ID 제공자에 연결할 iOS 인증 방법에 대한 확인란을 선택합니다. 다른 인증 방법을 추가합니다. 디바이스 규정 준수(Workspace ONE UEM 사용) 및 암호(Workspace ONE UEM Connector)의 경우 Workspace ONE UEM 구성 페이지에서 해당 옵션이 사용되도록 설정되어 있는지 확인합니다.

3 [KDC 인증서 내보내기] 섹션에서 **인증서 다운로드**를 클릭합니다. Workspace ONE UEM 콘솔에서 액세스할 수 있는 파일에 이 인증서를 저장합니다.

Workspace ONE UEM에서 iOS 디바이스 프로파일을 구성할 때 이 인증서를 업로드합니다.

4 **추가**를 클릭합니다.

다음에 수행할 작업

- iOS 디바이스의 Kerberos 인증에 대한 기본 액세스 정책 규칙을 구성합니다. 이 인증 방법이 규칙에 설정된 첫 번째 방법인지 확인합니다.
- Workspace ONE UEM 콘솔로 이동한 후 Workspace ONE UEM에서 iOS 디바이스 프로파일을 구성하고 VMware Identity Manager에서 KDC 서버 인증서 발급자 인증서를 추가합니다.

Active Directory 인증 기관 및 인증서 템플릿을 사용하여 Workspace ONE UEM 에서 Apple iOS 프로파일 구성

Workspace ONE UEM에서 Apple iOS 디바이스 프로파일을 만들고 배포하여 ID 제공자 설정을 디바이스에 푸시합니다. 이 프로파일에는 디바이스가 VMware ID 제공자에 연결하는 데 필요한 정보와 디바이스가 인증하는 데 사용하는 인증서가 포함되어 있습니다. 각 앱에 대해 인증을 요구하지 않고 원활한 액세스가 가능하도록 Single Sign-On을 사용하도록 설정합니다.

사전 요구 사항

- iOS용 모바일 SSO는 VMware Identity Manager에서 구성됩니다.
- iOS Kerberos 인증 기관 파일이 Workspace ONE UEM 관리 콘솔에서 액세스할 수 있는 컴퓨터에 저장되어 있습니다.

- 사용자의 인증 기관 및 인증서 템플릿이 Workspace ONE UEM에 제대로 구성되어 있습니다.
- iOS 디바이스에서 iOS용 모바일 SSO 인증을 사용하는 URL 및 애플리케이션 번들 ID 목록.

절차

1 Workspace ONE UEM 콘솔에서 **디바이스 > 프로파일 및 리소스 > 프로파일**로 이동합니다.

2 **추가 > 프로파일 추가**를 선택하고 **Apple iOS**를 선택합니다.

3 이름으로 iOSKerberos를 입력하고 **일반** 설정을 구성합니다.

4 왼쪽 탐색 창에서 **자격 증명 > 구성**을 선택하여 자격 증명을 구성합니다.

옵션	설명
자격 증명 소스	드롭다운 메뉴에서 **정의된 인증서 기관**을 선택합니다.
CA(인증 기관)	드롭다운 메뉴의 목록에서 인증 기관을 선택합니다.
인증서 템플릿	드롭다운 메뉴에서 인증 기관을 참조하는 요청 템플릿을 선택합니다. 이는 Workspace ONE UEM의 [인증서 템플릿 추가]에서 만들어진 인증서 템플릿입니다.

5 페이지 오른쪽 아래 모서리의 **+**를 다시 클릭하고 두 번째 자격 증명을 만듭니다.

6 **자격 증명 소스** 드롭다운 메뉴에서 **업로드**를 선택합니다.

7 자격 증명 이름을 입력합니다.

8 **업로드**를 클릭하여 [ID 및 액세스 관리] > [관리] > [ID 제공자] > [기본 제공 ID 제공자] 페이지에서 다운로드한 KDC 서버 루트 인증서를 업로드합니다.

9 왼쪽 탐색 창에서 **Single Sign-On**을 선택하고 **구성**을 클릭합니다.

10 연결 정보를 입력합니다.

옵션	설명
계정 이름	Kerberos를 입력합니다.
Kerberos 계정 이름	**+**를 클릭하고 {**EnrollmentUser**}를 선택합니다.
영역	클라우드에 있는 테넌트 배포의 경우 테넌트에 대한 Identity Manager 영역 이름을 입력합니다. 이 매개 변수의 텍스트는 대문자로 입력해야 합니다. 예: VMWAREIDENTITY.COM. 온-프레미스 배포의 경우 VMware Identity Manager 장치에서 KDC를 초기화할 때 사용한 영역 이름을 입력합니다. 예: EXAMPLE.COM
갱신 인증서	드롭다운 메뉴에서 **Certificate#1**을 선택합니다. 이는 처음에 자격 증명에서 구성된 Active Directory CA 인증서입니다.

옵션	설명
URL 접두사	HTTP를 통한 Kerberos 인증에 이 계정을 사용하기 위해 일치해야 하는 URL 접두사를 입력합니다. 클라우드에 있는 테넌트 배포의 경우 VMware Identity Manager 서버 URL을 https://<tenant>.vmwareidentity.<region>으로 입력합니다. 온-프레미스 배포의 경우 VMware Identity Manager 서버 URL을 https://myco.example.com으로 입력합니다.
애플리케이션	이 로그온을 사용하도록 허용되는 애플리케이션 ID 목록을 입력합니다. iOS 기본 제공 Safari 브라우저를 사용하여 Single Sign-On을 수행하려면 첫 번째 애플리케이션 번들 ID를 com.apple.mobilesafari로 입력합니다. 애플리케이션 번들 ID를 계속 입력합니다. 나열된 애플리케이션은 SAML 인증을 지원해야 합니다.

11 **저장 및 게시**를 클릭합니다.

다음에 수행할 작업

스마트 그룹에 디바이스 프로파일을 할당합니다. 스마트 그룹은 할당된 애플리케이션, 책, 준수 정책, 디바이스 프로파일 또는 프로비전을 수신하는 플랫폼, 디바이스 및 사용자를 결정하는 사용자 지정 가능 그룹입니다.

Workspace ONE UEM 인증 기관을 사용하여 Workspace ONE UEM 에서 Apple iOS 프로파일 구성

Workspace ONE UEM에서 Apple iOS 디바이스 프로파일을 만들고 배포하여 ID 제공자 설정을 디바이스에 푸시합니다. 이 프로파일에는 디바이스가 VMware ID 제공자에 연결하는 데 필요한 정보와 디바이스가 인증하는 데 사용하는 인증서가 포함되어 있습니다.

사전 요구 사항

- VMware Identity Manager에 구성된 기본 제공 Kerberos
- Workspace ONE UEM 콘솔에서 액세스할 수 있는 컴퓨터에 저장된 VMware Identity Manager KDC 서버 루트 인증서 파일.
- Workspace ONE UEM 콘솔의 [시스템] > [엔터프라이즈 통합] > VMware Identity Manager 페이지에서 다운로드되고 사용되도록 설정된 인증서.
- iOS 디바이스에서 기본 제공 Kerberos 인증을 사용하는 URL 및 애플리케이션 번들 ID 목록.

절차

1 Workspace ONE UEM 콘솔에서 **디바이스 > 프로파일 및 리소스 > 프로파일 > 프로파일 추가**로 이동한 후 **Apple iOS**를 선택합니다.

2 프로파일의 **일반** 설정을 구성하고 디바이스의 이름을 iOSKerberos로 입력합니다.

3 왼쪽 탐색 창에서 **SCEP > 구성**을 선택하여 자격 증명을 구성합니다.

옵션	설명
자격 증명 소스	드롭다운 메뉴에서 **AirWatch 인증 기관**을 선택합니다.
CA(인증 기관)	드롭다운 메뉴에서 **AirWatch 인증 기관**을 선택합니다.
인증서 템플릿	**싱글 사인 온**을 선택하여 AirWatch 인증 기관에서 발급한 인증서 유형을 설정합니다.

4 **자격 증명 > 구성**을 클릭하고 두 번째 자격 증명을 만듭니다.

5 **자격 증명 소스** 드롭다운 메뉴에서 **업로드**를 선택합니다.

6 iOS Kerberos 자격 증명 이름을 입력합니다.

7 **업로드**를 클릭하여 [ID 및 액세스 관리] > [관리] > [ID 제공자] > [기본 제공 ID 제공자] 페이지에서 다운로드한 VMware Identity Manager KDC 서버 루트 인증서를 업로드합니다.

8 왼쪽 탐색 창에서 **Single Sign-On**을 선택합니다.

9 연결 정보를 입력합니다.

옵션	설명
계정 이름	Kerberos를 입력합니다.
Kerberos 계정 이름	+를 클릭하고 {**EnrollmentUser**}를 선택합니다.
영역	클라우드에 있는 테넌트 배포의 경우 테넌트에 대한 VMware Identity Manager 영역 이름을 입력합니다. 이 매개 변수의 텍스트는 대문자로 입력해야 합니다. 예: VMWAREIDENTITY.COM. 온-프레미스 배포의 경우 VMware Identity Manager 시스템에서 KDC를 초기화할 때 사용한 영역 이름을 입력합니다. 예: EXAMPLE.COM
갱신 인증서	iOS 8 이상 디바이스에서 사용자의 Single Sign-On 세션이 만료될 때 사용자 조작 없이도 사용자를 자동으로 다시 인증하는 데 사용되는 인증서를 선택합니다.
URL 접두사	HTTP를 통한 Kerberos 인증에 이 계정을 사용하기 위해 일치해야 하는 URL 접두사를 입력합니다. 클라우드에 있는 테넌트 배포의 경우 VMware Identity Manager 서버 URL을 https://<tenant>.vmwareidentity.<지역>으로 입력합니다. 온-프레미스 배포의 경우 VMware Identity Manager 서버 URL을 https://myco.example.com으로 입력합니다.
애플리케이션	이 로그인을 사용하도록 허용되는 애플리케이션 ID 목록을 입력합니다. iOS 기본 제공 Safari 브라우저를 사용하여 Single Sign-On을 수행하려면 첫 번째 애플리케이션 번들 ID를 com.apple.mobilesafari로 입력합니다. 애플리케이션 번들 ID를 계속 입력합니다. 나열된 애플리케이션은 SAML 인증을 지원해야 합니다.

10 **저장 및 게시**를 클릭합니다.

iOS 프로파일이 사용자 디바이스에 성공적으로 푸시되면 사용자는 자격 증명을 입력하지 않고도 기본 제공 Kerberos 인증 방법을 사용하여 VMware Identity Manager에 로그인할 수 있습니다.

다음에 수행할 작업

스마트 그룹에 디바이스 프로파일을 할당합니다. 스마트 그룹은 할당된 애플리케이션, 책, 준수 정책, 디바이스 프로파일 또는 프로비전을 수신하는 플랫폼, 디바이스 및 사용자를 결정하는 사용자 지정 가능 그룹입니다.

Workspace ONE UEM 디바이스 프로파일 할당

디바이스 프로파일을 생성한 후에 스마트 그룹에 프로파일을 할당합니다.

스마트 그룹은 할당된 애플리케이션, 준수 정책, 디바이스 프로파일 또는 프로비전을 수신하는 플랫폼, 디바이스 및 사용자를 결정하는 사용자 지정 가능 그룹입니다. Workspace ONE UEM 모바일 디바이스 관리 가이드를 참조하십시오.

절차

1 Workspace ONE UEM 콘솔에서 **디바이스 > 프로파일 및 리소스** > **프로파일**로 이동합니다.

2 스마트 그룹에 할당하려는 디바이스 프로파일을 선택합니다.

3 [일반] 탭에서 **할당된 그룹** 텍스트 상자를 클릭하고 **할당 그룹 생성**을 선택합니다.

4 [새 스마트 그룹 생성] 페이지에서 스마트 그룹의 이름을 입력합니다.

5 **플랫폼 및 운영 체제**를 선택하고 드롭다운 메뉴에서 올바른 운영 체제 및 버전을 선택합니다.

6 **저장 및 게시**를 클릭합니다.

디바이스 옵션에 스마트 그룹을 할당하면 Workspace ONE에 로그인하고 카탈로그에서 애플리케이션에 액세스할 수 있습니다.

관리 Android 디바이스에 대한 모바일 Single Sign-On 인증 구현 4

Android용 모바일 SSO(Single Sign-On)는 Workspace ONE UEM 관리 Android 디바이스에 대한 인증서 인증 방법을 구현한 것입니다. 모바일 SSO를 사용하여 사용자는 암호를 다시 입력하지 않고도 해당 디바이스에 로그인하고 Workspace ONE 애플리케이션에 안전하게 액세스할 수 있습니다.

VMware Tunnel® 모바일 애플리케이션은 인증 흐름에 인증서 및 디바이스 ID 정보를 추가하기 위해 Android 디바이스에 설치됩니다. 인증을 위해 VMware Identity Manager 서비스에 액세스하도록 Tunnel 설정이 Workspace ONE UEM Console에서 구성되고, 서비스는 인증을 위해 디바이스에서 인증서를 검색합니다.

Workspace ONE UEM Console에서 다음 설정도 구성합니다.

- Android VPN 프로파일. 이 프로파일은 Android에 대해 애플리케이션별 터널링 기능을 사용하도록 설정하는 데 사용됩니다.
- Workspace ONE UEM Console에서 애플리케이션 터널 기능을 사용하는 각 애플리케이션에 대해 VPN을 사용하도록 설정합니다.
- 애플리케이션 VPN에 대해 구성된 모든 애플리케이션 목록, 프록시 서버 세부 정보 및 VMware Identity Manager URL을 사용하여 네트워크 트래픽 규칙을 만듭니다.

온-프레미스에서 VMware Identity Manager 서비스를 사용하여 Android용 모바일 SSO를 구현할 경우 VMware Identity Manager 시스템에서 인증서 프록시 서비스를 구성합니다. 인증서 프록시 서비스가 구성되면 VMware Identity Manager 콘솔의 VMware Identity Manager 내장 ID 제공자에서 인증서 인증을 구성할 수 있습니다.

클라우드에서 VMware Identity Manager 서비스를 사용하여 Android용 모바일 SSO를 구현할 경우 VMware Identity Manager 콘솔의 VMware Identity Manager 내장 ID 제공자에서 인증서 인증을 구성할 수 있습니다. 사용자에 대한 인증서 프록시 서비스가 관리됩니다.

Android 모바일 SSO를 설정하는 방법에 대한 자세한 내용은 Workspace ONE 설명서 센터에서 VMware Workspace One에 대한 Android 모바일 Single Sign-On 자료를 참조하십시오.

지원되는 Android 디바이스

Android 5.1 이상이 지원됩니다.

Android 디바이스에서 액세스되는 애플리케이션은 SAML 또는 Single Sign-On에 대한 다른 지원되는 페더레이션 표준을 지원해야 합니다.

Workspace ONE 애플리케이션을 사용하여 직접 등록

5

Workspace ONE을 통한 직접 등록에서는 Workspace ONE 애플리케이션의 리소스에 액세스하기 위해 디바이스를 등록해야 합니다.

Workspace ONE 애플리케이션을 통해 직접 등록이 수행되면, 모든 사용자에게 해당 애플리케이션 스토어로 이동하고, Workspace ONE 애플리케이션을 다운로드하고, 이메일 주소를 입력하고, 지시에 따라 디바이스에서 Workspace ONE 사용을 시작하도록 할 수 있습니다.

지원되는 디바이스

- Apple iOS 9.0 이상
- Android Enterprise(이전의 Android for Work) 5.1 이상
- Android Legacy 4.1 이상

  Android Legacy 디바이스는 Android Enterprise가 지원되지 않는 Android 디바이스이거나 Android Enterprise가 사용되도록 설정되지 않은 Workspace ONE UEM 인스턴스에 연결되는 Android Enterprise 지원 디바이스입니다.

본 장은 다음 항목을 포함합니다.

직접 등록을 위해 Workspace ONE 사용

OG(조직 그룹)에 대한 Workspace ONE UEM 콘솔의 [등록] > [제한] 페이지에서 Workspace ONE을 통해 직접 디바이스 등록을 사용하도록 설정합니다.

Workspace ONE이 직접 등록용으로 사용하도록 설정되면, 처음으로 로그인된 정규화된 디바이스가 직접 등록됩니다. 직접 등록 자격이 없는 디바이스에는 Workspace ONE 등록 상태에서 모바일 애플리케이션 관리 전용 액세스 권한이 부여됩니다.

절차

1. Workspace ONE UEM 콘솔에서 Workspace ONE에 대해 직접 등록을 사용하도록 설정할 조직 그룹을 선택합니다.
2. **그룹 및 설정 > 모든 설정 > 디바이스 및 사용자 > 일반 > 등록**으로 이동한 후 **제한** 탭을 선택합니다.

3 현재 설정으로 **재정의**를 선택합니다(필요한 경우).

4 Workspace ONE에 대한 관리 요구 사항으로 스크롤한 후 구성 옵션을 선택합니다.

설정	설명
Workspace ONE에 MDM 필요	이 옵션이 사용되도록 설정되어 있으면, 정규화된 디바이스 및 사용자가 Workspace ONE에 로그인할 때 즉시 등록하라는 메시지가 표시됩니다.
할당된 사용자 그룹	모든 사용자는 기본 사용자 그룹입니다. 직접 등록 프로세스에 포함할 특정 사용자 그룹을 선택할 수 있습니다.
iOS	iOS 디바이스를 포함하도록 설정합니다. 이 옵션이 사용되지 않도록 설정되면 iOS 디바이스를 직접 등록할 수 없습니다. 이 옵션이 사용되지 않도록 설정되어도 디바이스를 여전히 관리되지 않는 상태로 Workspace ONE UEM에 등록할 수 있습니다.
Android Legacy	Android Legacy 디바이스를 포함하도록 설정됩니다. 이 옵션이 사용되지 않도록 설정되면 Android Legacy 디바이스를 직접 등록할 수 없습니다. 이 옵션이 사용되지 않도록 설정되어도 디바이스를 여전히 관리되지 않는 상태로 Workspace ONE UEM에 등록할 수 있습니다.
Android Enterprise	Android Enterprise 디바이스를 포함하도록 설정됩니다. 이 옵션이 사용되지 않도록 설정되면 Android Enterprise 디바이스를 직접 등록할 수 없습니다. 이 옵션이 사용되지 않도록 설정되어도 디바이스를 여전히 관리되지 않는 상태로 Workspace ONE UEM에 등록할 수 있습니다.

5 **저장**을 클릭합니다.

6 Workspace ONE에 대해 지원되는 등록 옵션을 사용하여 등록 탭을 계속 구성합니다. Workspace ONE 직접 등록 구성 옵션의 내용을 참조하십시오.

Workspace ONE의 직접 등록을 구성하는 방법에 대한 자세한 내용은 VMware AirWatch Mobile Device Management 가이드의 디바이스 등록 장을 참조하십시오.

Workspace ONE 직접 등록 구성 옵션

Workspace ONE UEM 콘솔에서 Workspace ONE을 사용한 직접 등록을 구성합니다. **그룹 및 설정 > 모든 설정 > 디바이스 및 사용자/일반/등록**으로 이동합니다. Workspace ONE 디바이스 등록 옵션 표에 구성할 수 있는 메뉴 항목이 표시됩니다.

등록 설정 페이지에서 디바이스 및 사용자 등록 관련 옵션을 구성할 수 있습니다. 페이지는 아래에 설명 되어 있는 탭으로 구분됩니다. 디바이스 등록을 구성하는 방법에 대한 자세한 내용은 VMware Workspace ONE UEM Mobile Device Management 가이드를 참조하십시오.

그림 5-1. Workspace ONE UEM 콘솔 등록 페이지

표 5-1. Workspace ONE 직접 등록 구성 가능 메뉴 항목

등록 탭	Workspace ONE의 직접 등록에 대한 구성 가능 메뉴 항목
인증	디렉토리 사용자가 지원됩니다. 또한 SAML과 Active Directory 사용자는 "즉시" 지원됩니다. 초기 로그인 시, Workspace ONE UEM에 사용자 기록이 존재할 경우 LDAP 없는 SAML 사용자가 지원됩니다. 디바이스 등록 모드에서는 **오픈 등록**만 지원됩니다. 등록된 디바이스 전용은 지원되지 않습니다.
사용 약관	직접 등록 프로세스를 진행하기 전에 사용 약관을 생성하여 사용자가 동의하도록 할 수 있습니다.
그룹화	모든 그룹화 메뉴 옵션은 Workspace ONE 직접 등록과 호환됩니다. **Workspace ONE에 대한 실시간 사용자 그룹 동기화**는 기본적으로 사용됩니다. 디바이스를 등록하는 경우 Workspace ONE UEM이(가) Active Directory를 실시간으로 호출하여 사용자의 사용자 그룹을 동기화합니다. 사용자가 Workspace ONE UEM에 없는 경우 Workspace ONE UEM 콘솔이 먼저 사용자를 동기화한 다음 실시간으로 사용자 그룹을 동기화 합니다. 이 기능을 사용하지 않는 경우 Workspace ONE UEM 콘솔은 사용자 그룹을 동기화하지 않습니다. **참고** 이 기능은 CPU를 많이 사용합니다. 사용자 그룹이 자주 변경되지 않거나 사용자 그룹이 이미 Workspace ONE UEM에 있는 경우 Workspace ONE 애플리케이션을 시작할 때 성능 개선과 지연 시간 문제를 방지하기 위해 이 설정을 사용하지 않습니다. 다중 Workspace ONE UEM 조직 그룹 설정을 위한 배포 전략의 "올바른 조직 그룹에 디바이스 배치" 섹션을 참조하십시오.

제한 사항	■ **사용자 액세스 제어**에서 [알려진 사용자만 등록할 수 있도록 제한] 및 [구성된 그룹에 등록을 제한]을 선택할 수 있습니다.
	■ 최대 디바이스 제한이 지원됩니다.
	■ **정책 설정**이 부분적으로 지원됩니다.
	  ■ **허용되는 소유권 유형**. Workspace ONE은 [직원 소유 및 기업 - 전용]의 경우만 메시지를 표시합니다.
	  참고 컨테이너 허용 등록 유형은 지원되지 않습니다.

옵션형 프롬프트	사용하도록 설정할 수 있는 두 가지 옵션형 프롬프트는 **소유권 유형 입력 프롬프트** 및 **디바이스 자산 번호 프롬프트 사용**입니다. 소유권 유형이 [기업 소유]인 경우 자산 번호 입력만 요구됩니다.
사용자 지정	사용자 지정 메뉴 옵션이 지원됩니다. ■ 등록 후 방문 URL(iOS 전용) ■ MDM 프로파일 메시지(iOS 전용) ■ 사용자 지정 MDM 애플리케이션 사용 각 플랫폼에 대한 특정 메시지 템플릿을 사용하도록 설정할 수 있지만, 특정 Workspace ONE 메시지 템플릿은 Workspace ONE 3.2에 사용할 수 없습니다.

Workspace ONE을 사용하여 Workspace ONE UEM 에 직접 등록할 때의 사용자 경험

모바일 디바이스 관리가 Workspace ONE을 통해 구현되면 사용자는 Workspace ONE 애플리케이션을 다운로드하고, Workspace ONE UEM으로 인증을 받고, 해당 디바이스를 등록합니다. 디바이스를 등록한 후에는 Workspace ONE을 사용하여 사용 권한이 부여된 리소스를 즉시 추가하고 사용할 수 있습니다.

Workspace ONE을 사용하여 해당 디바이스를 등록할 때 진행되는 프로세스는 iOS 및 Android Enterprise 디바이스에서 비슷합니다. Android Legacy 등록은 등록을 위한 AirWatch Agent로 리디렉션됩니다. 등록이 완료되면 AirWatch Agent의 제어 권한이 자동으로 Workspace One으로 다시 전환됩니다. 사용자는 다음 각각의 몇 가지 변형으로 Workspace ONE에 액세스할 수 있습니다.

iOS 디바이스에서 Workspace ONE을 통해 직접 등록

사용자가 Apple App Store에서 Workspace ONE 애플리케이션을 다운로드, 설치 및 실행하도록 지시합니다.

절차

1 사용자는 애플리케이션을 열고, 서버 URL 및 이메일 주소를 입력하고 작업 환경의 구성에 따라 인증됩니다.

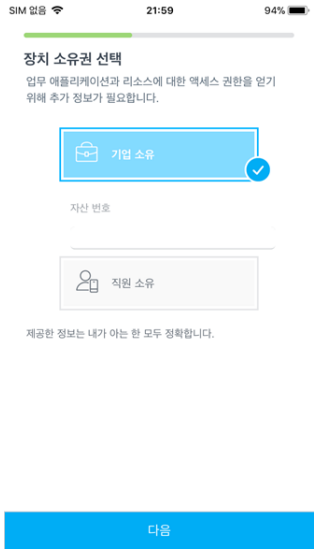
2 **귀사의 추가 설치 필요** 화면이 표시됩니다.

그림 5-2. 디바이스 등록 설정 알림

3 사용 약관이 구성된 경우 계속하기 전에 사용 약관을 수락하라는 메시지가 표시됩니다.

4 디바이스 소유권 유형을 표시하고 디바이스 자산 번호를 요청하도록 선택적 프롬프트를 설정하는 경우 이 정보가 표시됩니다.

그림 5-3. 디바이스 소유권 선택



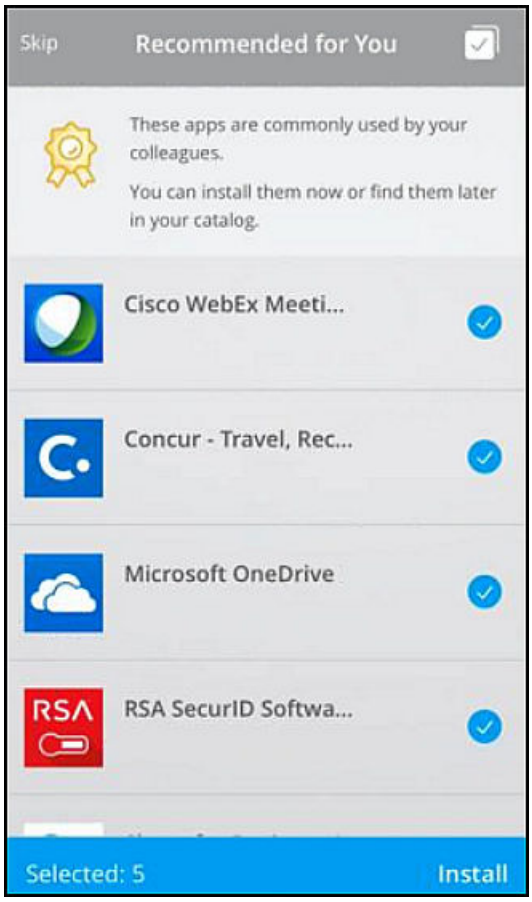
5 Safari가 열리고 **허용**을 클릭하면 [설정] 페이지가 열립니다.

그림 5-4. 구성 프로파일 설정 허용

Workspace 서비스 및 구성 프로파일은 디바이스에 구성됩니다.

디바이스는 이제 Workspace ONE UEM에 등록되었으며 Workspace ONE이 실행됩니다. [권장 사항] 화면이 표시됩니다.

그림 5-5. [권장 애플리케이션] 화면



6 설치하려는 애플리케이션을 선택하거나 이 단계를 건너뛸 수 있습니다.

디바이스는 이제 Workspace ONE UEM MDM을 통해 관리됩니다. 권장 애플리케이션이 설치되도록 선택된 경우 사용자는 해당 애플리케이션에 대한 푸시 알림을 수신하기 시작합니다.

Worksapce ONE을 사용하여 Android Enterprise 디바이스에서 직접 등록

사용자가 Google App Store 또는 저장소에서 Workspace ONE 애플리케이션을 다운로드, 설치 및 실행하도록 지시합니다.

절차

1 사용자는 서버 URL 및 이메일 주소를 입력하고 작업 환경의 구성에 따라 인증됩니다.

2 **귀사의 추가 설치 필요** 화면이 표시됩니다. **계속**을 클릭합니다.

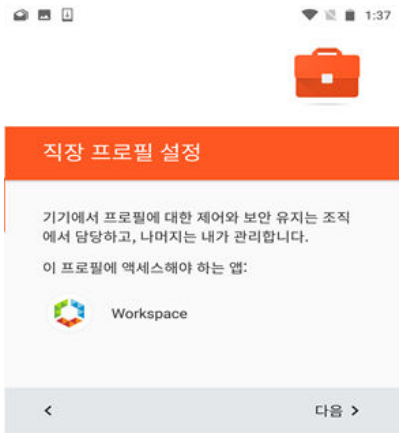
그림 5-6. 디바이스 등록 설정 알림

3 사용 약관이 구성된 경우 계속하기 전에 사용 약관을 수락하라는 메시지가 표시됩니다.

4 디바이스 소유권 유형을 표시하고 디바이스 자산 번호를 요청하도록 선택적 프롬프트를 설정하는 경우 이 정보가 표시됩니다.

5 Workspace 서비스 및 작업 프로파일은 디바이스에 구성됩니다.

그림 5-7. 작업 프로파일 알림 설정

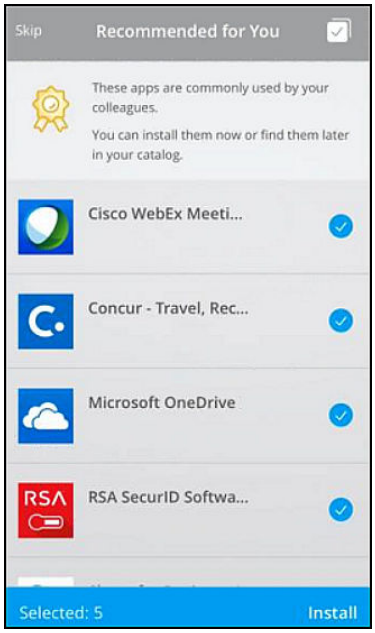


이 작업 프로파일을 사용한 디바이스 관리 제어를 설명하는 메시지가 표시되면 **확인**을 클릭합니다.

Workspace ONE 애플리케이션이 설치되고 Android Work 계정이 등록됩니다.

6 디바이스는 이제 Workspace ONE UEM에 등록되었으며 Workspace ONE이 실행됩니다. [권장 사항] 화면이 표시됩니다.

그림 5-8. [권장 애플리케이션] 화면



7 설치하려는 애플리케이션을 선택하거나 이 단계를 건너뛸 수 있습니다.

디바이스는 이제 Workspace ONE UEM MDM을 통해 관리됩니다. 권장 애플리케이션을 설치하도록 선택한 경우, 배지 Android Enterprise 서류 가방 아이콘이 있는 해당 애플리케이션이 설치되기 시작합니다.

Android Legacy 디바이스에 대한 디바이스 등록

Android Legacy 디바이스에 대한 디바이스 등록은 등록을 위한 AirWatch Agent로 리디렉션됩니다. 등록이 완료되면 AirWatch Agent의 제어 권한이 자동으로 Workspace One으로 다시 전환됩니다.

사용자에게 애플리케이션 스토어로 이동하여 Workspace ONE을 다운로드하도록 지시합니다.

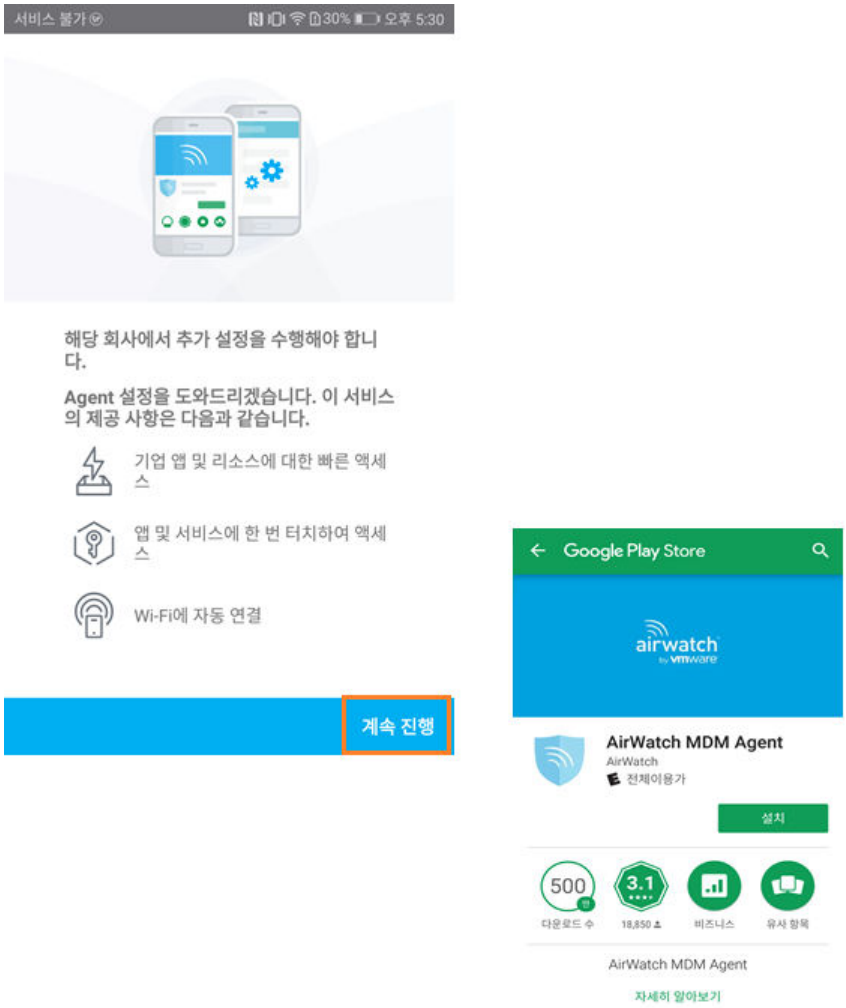
절차

1 사용자는 애플리케이션을 열고, 해당 서버 URL 또는 이메일 주소를 입력하고, 해당 사용자 이름 및 암호를 입력하여 로그인합니다.

이때, Workspace ONE 애플리케이션은 디바이스가 Android Enterprise용으로 설정되어 있지 않음을 감지하고, Workspace ONE의 리소스에 액세스하기 위해 디바이스의 직접 등록이 필요한지 여부를 감지할 수 있습니다.

2 **귀사의 추가 설치 필요** 화면이 표시되고 사용자가 **계속**을 클릭하면 Google Play Store의 AirWatch Agent 애플리케이션으로 리디렉션됩니다.

그림 5-9. AirWatch Agent 애플리케이션 다운로드 요청



3 사용자가 AirWatch Agent 애플리케이션을 다운로드합니다.

참고 AirWatch Agent 애플리케이션이 디바이스에 이미 설치되어 있는 경우 Workspace ONE은 애플리케이션을 자동으로 실행합니다. 앱 스토어로 리디렉션되지 않습니다.

Workspace ONE에 대해 입력한 인증 세부 정보가 AirWatch Agent 애플리케이션으로 전달되므로 사용자는 이 정보를 다시 입력할 필요가 없습니다.

AirWatch Agent 애플리케이션이 실행됩니다. AirWatch Agent로 디바이스를 등록하는 동안, 사용자는 소유권 유형을 선택하고 디바이스 자산 번호(구성된 경우)를 입력합니다.

4 **Agent에서 전화를 걸고 관리하도록 허용**이 표시되면 사용자는 **허용**을 클릭합니다.

AirWatch Agent는 이 디바이스에서 등록의 유효성을 검사하고, 사용자를 인증하고, AirWatch에 대한 권한을 부여합니다.

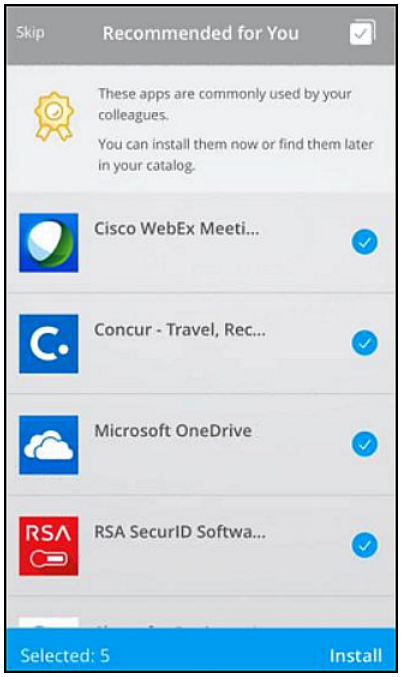
5 **디바이스 관리 애플리케이션을 활성화합니까?** 화면이 표시되면 사용자가 **이 디바이스 관리 애플리케이션 활성화**를 클릭합니다.

그림 5-10. 디바이스 관리 애플리케이션 활성화

6 다양한 디바이스 기능에 액세스하도록 권한을 부여하라는 메시지가 표시됩니다.

디바이스는 이제 Workspace ONE UEM에 등록되었으며 Workspace ONE이 실행됩니다. [권장 애플리케이션] 화면이 표시됩니다.

그림 5-11. [권장 애플리케이션] 화면



7 설치하려는 애플리케이션을 선택하거나 이 단계를 건너뛸 수 있습니다.

디바이스는 이제 Workspace ONE UEM MDM을 통해 관리됩니다. 권장 애플리케이션이 설치되도록 선택된 경우 해당 애플리케이션에 대한 알림이 수신되기 시작합니다.

Workspace ONE을 적용하여 Apple 디바이스 등록 프로그램 통합 지원

6

Apple DEP(디바이스 등록 프로그램)은 고객이 사용자 인증을 위해 SAML을 사용하는 시나리오를 지원하지 않습니다. 그러나 Workspace ONE은 이 사용 사례를 지원하는 고유한 방법을 구현했습니다.

Workspace ONE UEM 디바이스 스테이징을 통해, 관리자는 다중 디바이스 스테이징 사용자에게 디바이스를 할당하고, 사용자가 Workspace ONE 애플리케이션에 로그인되어 있을 때 Workspace ONE을 통해 적합한 사용자에게 디바이스를 다시 할당할 수 있습니다.

Workspace ONE 애플리케이션은 스테이징 사용자 등록의 일부로 디바이스에 설치되어야 합니다. 사용자가 Workspace ONE에 처음 로그인하면 Workspace ONE은 구성된 SAML 제공자를 통해 사용자를 인증합니다. 사용자가 인증을 받은 후에는 디바이스 소유권이 다중 디바이스 스테이징 사용자로부터 인증된 디렉토리 사용자에게 전환됩니다.

전제 조건

디렉토리 사용자는 사용자가 Workspace ONE 애플리케이션에 로그인할 때 Workspace ONE UEM에 존재해야 합니다. CSV 통해 대량 로드 방식으로 사용자를 미리 로드하거나, 다음 API를 적용하여 필요에 따라 사용자를 생성할 수도 있습니다.

참고 보안 유형 값은 디렉토리와 동일해야 합니다.

```
https://<API_SERVER_ADDRESS>/api/help/#!/apis/10006?!/User/User_AddUser
```

DEP 통합의 Workspace ONE 지원 흐름

Workspace ONE을 사용하여 Apple 디바이스 등록 프로그램의 지원을 구현하려면 다음 작업을 완료해야 합니다.

- iOS 디바이스에서 Workspace ONE 애플리케이션을 설치합니다.
- Workspace ONE UEM 콘솔에서 다음 스테이징 구성의 스테이징 사용자가 있는지 확인합니다.
  a **계정 > 사용자 > 목록 보기**로 이동한 후 디바이스 스테이징을 편집할 수 있게 하려는 사용자 계정을 선택합니다.
  b **추가/편집** 사용자 페이지에서 **고급** 탭을 선택합니다. **스테이징** 섹션까지 아래로 스크롤한 후 **디바이스 스테이징** 및 **다중 사용자 디바이스**를 사용하도록 설정합니다.

그림 6-1. Workspace ONE UEM 의 다중 사용자 디바이스 설정

- Apple DEP 포털에서 스테이징 사용자에게 디바이스를 할당하고 최종 사용자에게 디바이스를 전달합니다.

  Apple 장치 등록 프로그램에 대한 자세한 내용은 Apple 장치 등록 가이드를 참조하십시오.

통합 작동 방식

사용자가 디바이스를 처음 켜는 경우 디바이스가 등록되고 다중 디바이스 스테이징 사용자에게 할당됩니다. 사용자는 홈 화면에서 사용할 수 있는 Workspace ONE 애플리케이션을 시작한 후 로그인합니다. Workspace ONE은 구성된 SAML 제공자를 통해 사용자를 인증합니다.

사용자가 인증을 받은 후에는 디바이스 소유권이 다중 디바이스 스테이징 사용자로부터 인증된 디렉토리 사용자에게 전환됩니다. 인증된 사용자에게 할당된 애플리케이션, 프로파일 및 리소스가 디바이스로 푸시됩니다.

참고 디바이스의 조직 그룹은 변경되지 않습니다. 이 기능은 Workspace ONE UEM 콘솔의 [등록 설정] 섹션에 있는 사용자 그룹 매핑(또는 드롭다운 메뉴에 따른 수동 사용자 선택)을 지원하지 않습니다.

VMware Workspace ONE 모바일 애플리케이션 배포 7

모바일 디바이스에 VMware Workspace ONE 애플리케이션을 설치한 사용자는 사용 권한이 부여된 리소스에 액세스할 수 있습니다.

사용자는 ID가 VMware Identity Manager에서 관리될 때 Single Sign-On 기능을 사용하여 사용 권한이 부여된 애플리케이션에 액세스할 수 있습니다. 또한 다른 애플리케이션을 추가할 수 있는 애플리케이션 카탈로그에도 액세스할 수 있습니다.

Workspace ONE 애플리케이션 인터페이스는 스마트폰, 태블릿 또는 데스크톱 컴퓨터에 비슷한 환경 및 옵션을 제공합니다.

디바이스가 MDM(모바일 디바이스 관리)에 등록된 경우 Workspace ONE 애플리케이션을 관리되는 애플리케이션으로 푸시할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- Workspace ONE용 공용 및 내부 애플리케이션에 대한 Workspace ONE UEM의 디바이스 관리 옵션
- 애플리케이션에 대한 액세스 관리
- Workspace ONE 카탈로그에 액세스하기 위한 사용 약관 요구
- Workspace ONE 애플리케이션 가져오기 및 배포
- 자동 검색을 위해 이메일 도메인 등록
- 세션 인증 설정
- 다중 Workspace ONE UEM 조직 그룹 설정을 위한 배포 전략

Workspace ONE 용 공용 및 내부 애플리케이션에 대한 Workspace ONE UEM 의 디바이스 관리 옵션

디바이스 관리 상태에 따라 공용 및 내부 애플리케이션을 배포하도록 구성할 수 있습니다. 모든 디바이스는 오픈 액세스로 구성된 애플리케이션에 액세스할 수 있습니다. 관리되는 액세스용으로 구성된 애플리케이션에는 Workspace 서비스 또는 에이전트 등록을 통해 사용하도록 설정하여 사용 권한을 부여한 디바이스만 액세스할 수 있습니다.

이 표에는 관리 및 비관리 시나리오에서의 기능이 설명되어 있습니다.

액세스 유형	기능	설명	제안되는 사용
오픈 액세스(비관리)	■ 웹, Horizon 및 Citrix 리소스에 대한 셀프 서비스 앱 카탈로그 ■ SSO(Single Sign-On)로 웹/가상 실행 ■ Touch ID/PIN 애플리케이션 보호 ■ 디바이스 해킹 감지 ■ 인증 정책 및 차단 디바이스를 비롯한 VMware Identity Manager 조건부 액세스에 대한 지원 ■ 기본 애플리케이션 액세스 ■ 내부 애플리케이션 및 SDK 애플리케이션 배포	사용자는 디바이스에 액세스하기 위한 관리자 권한 없이 디바이스의 리소스에 액세스합니다. 오픈 액세스 권한이 있는 애플리케이션은 관리 상태에 관계없이 디바이스에서 사용될 수 있습니다. 관리자는 [오픈 액세스]로 설정된 기본 애플리케이션을 시스템에서 제거할 수 없습니다.	■ 최종 사용자가 로그인하면 보안 권한의 격상 없이 애플리케이션 액세스 권한을 즉시 제공합니다. ■ 설치가 필요하지 않은 애플리케이션 사용을 권장합니다. 사용자는 원할 때 디바이스에 애플리케이션을 설치할 수 있습니다. ■ 애플리케이션에 중요한 회사 데이터가 포함되지 않고 보호된 회사 리소스에 액세스할 수 없습니다. ■ Workspace ONE UEM MDM 프로파일 없이 보조 직원에게 애플리케이션 배포.
관리되는 액세스	■ 웹, Horizon 및 Citrix 리소스에 대한 셀프 서비스 앱 카탈로그 ■ SSO(Single Sign-On)로 웹/가상 실행 ■ Touch ID/PIN 애플리케이션 보호 ■ 디바이스 해킹 감지 ■ 인증 정책 및 차단 디바이스를 비롯한 VMware Identity Manager 조건부 액세스에 대한 지원 ■ 기본 애플리케이션의 관리형 설치 및 직접 설치 ■ 내부 애플리케이션 및 SDK 애플리케이션 관리 ■ 애플리케이션 구성 지원 ■ 애플리케이션별 VPN ■ SAML 지원 기본 애플리케이션에 대한 원터치 SSO ■ 디바이스 프로파일 ■ Workspace ONE UEM 규정 준수 엔진	사용자는 디바이스에 관리 프로파일을 설치하여 관리자에게 디바이스에 액세스 권한을 부여합니다. 액세스 권한이 관리되는 애플리케이션은 Workspace ONE UEM에서 관리하는 디바이스에서 사용할 수 있습니다. Workspace ONE UEM에서 디바이스를 관리하지 않는 경우 Workspace ONE은 디바이스의 사용자에게 Workspace ONE UEM에 등록하라는 메시지를 표시합니다. 디바이스가 등록되면 사용자는 디바이스를 사용하여 Workspace ONE을 통해 애플리케이션에 액세스할 수 있습니다.	■ 사용자가 조직을 떠나거나 디바이스를 분실했을 때 디바이스에서 중요한 회사 데이터 제거 ■ 애플리케이션에서 인트라넷에 액세스할 때 인증을 받고 내부 백엔드 리소스와 안전하게 통신하기 위해 앱 터널링이 필요합니다. ■ 애플리케이션에 Single Sign-On을 사용하도록 설정합니다. ■ 애플리케이션에 대한 사용자 채택 및 설치 상태를 추적합니다. ■ 등록 시 애플리케이션을 자동으로 배포합니다.

내부 애플리케이션에 대한 관리되는 액세스 옵션을 구성할 위치 또는 Workspace ONE을 통해 배포용 공용 애플리케이션을 추가하는 방법에 대한 자세한 내용은 Workspace ONE UEM 모바일 애플리케이션 관리 가이드를 참조하십시오.

오픈 액세스 및 관리되는 액세스에 지원되는 플랫폼

플랫폼에 따라 내부 및 공개 애플리케이션에 대한 액세스 유형을 구성합니다.

	관리되는 액세스	오픈 액세스
	내부 애플리케이션	
Android	X	X
iOS	X	X
Windows 10 데스크톱	X	-
Windows 10 휴대폰	X	-
	공개 애플리케이션	
Android	X	X
iOS	X	X
Windows 10 데스크톱	-	X
Windows 10 휴대폰	-	X

애플리케이션에 대한 액세스 관리

단일 사용자가 기본 애플리케이션에 대해 오픈 액세스 또는 관리되는 액세스를 수행할 권한을 부여할 수 있습니다. 어댑티브 관리 접근법은 최종 사용자가 관리 없이도 오픈 액세스 애플리케이션을 사용하도록 합니다. 사용자가 관리가 필요한 기본 애플리케이션을 요구할 경우 어댑티브 관리는 해당 네이티브 애플리케이션을 관리하는 데 필요한 추가적인 보안 및 제어를 제공합니다.

애플리케이션이 관리되는 경우 관리되는 애플리케이션을 설치 및 사용하려면 사용자는 Workspace 서비스를 사용하도록 설정해야 합니다. Workspace ONE UEM 콘솔에서 애플리케이션을 업로드할 때 액세스 상태는 해당 애플리케이션에 대한 구성을 기준으로 오픈 액세스 또는 관리되는 액세스 상태로 표시됩니다. 예를 들어 **애플리케이션 구성 전송** 옵션이 선택되면 애플리케이션은 관리를 요구하도록 설정됩니다.

관리가 필요한 애플리케이션은 카탈로그에서 관리되지 않는 상태로 표시될 때 별 모양 아이콘이 표시됩니다. 애플리케이션을 사용하려면 사용자가 어댑티브 관리 프로세스를 통해 Workspace 서비스를 사용하도록 선택해야 합니다. 별 모양 아이콘이 표시된 애플리케이션을 다운로드하려고 하면 Workspace 서비스를 사용하도록 설정하라는 메시지가 표시됩니다. 사용자는 어댑티브 관리 프로세스를 계속하도록 선택한 경우 개인 정보 보호 알림 링크를 클릭하여 자신의 개인 정보에 미치는 영향을 확인할 수 있습니다. 개인 정보 보호 알림은 등록하려는 Workspace ONE UEM 환경에서 자동으로 설정을 가져옵니다. 개인 정보 보호 설정 정보를 검토한 후 사용자는 Workspace 서비스를 사용하도록 설정하거나, 취소하고 Workspace ONE 애플리케이션을 디바이스에서 관리되지 않는 상태로 계속 사용할 수 있습니다. 사용자가 Workspace 서비스를 사용하도록 설정하면 모든 관리되는 애플리케이션에서 별 모양 아이콘이 제거됩니다.

관리되는 디바이스에서 액세스 제거

[계정 제거] 옵션을 통해 관리되는 디바이스에서 Workspace ONE 애플리케이션을 사용하지 않도록 설정할 수 있습니다. 계정을 제거하면 디바이스의 엔터프라이즈 초기화가 실행되고, 회사 액세스 권한이 제거되고, 사용자가 로그인 화면으로 복귀됩니다. 관리자는 Workspace ONE UEM 콘솔에서 엔터프라이즈 초기화를 수행하여 Workspace ONE 서비스를 사용하지 않도록 설정할 수 있습니다.

관리되는 디바이스에서 [계정 제거] 작업을 실행하면 Workspace ONE 애플리케이션을 통해 부여된 액세스 권한이 취소되고 Workspace ONE UEM에서 디바이스가 등록 취소됩니다. 관리가 필요한 애플리케이션이 디바이스에서 제거되고, Boxer, Browser 및 Content Locker와 같은 Workspace ONE UEM 생산성 애플리케이션에 대한 액세스 권한이 취소됩니다.

Workspace ONE 카탈로그에 액세스하기 위한 사용 약관 요구

조직 자체의 Workspace ONE 사용 약관을 작성하고 최종 사용자가 Workspace ONE을 사용하기 전에 이 사용 약관에 동의하도록 할 수 있습니다.

사용 약관은 사용자가 Workspace ONE에 로그인한 후에 표시됩니다. 사용자는 Workspace ONE 카탈로그로 이동하려면 먼저 사용 약관에 동의해야 합니다.

사용 약관 기능에는 다음과 같은 구성 옵션이 포함됩니다.

- 기존 사용 약관 버전을 생성합니다.
- 사용 약관을 편집합니다.
- 디바이스 유형에 따라 표시될 수 있는 여러 사용 약관을 생성합니다.
- 사용 약관의 언어별 사본을 생성합니다.

설정한 사용 약관 정책은 [ID 및 액세스 관리] 탭에 표시됩니다. 사용 약관 정책을 편집하여 기존 정책을 수정하거나 새 버전의 정책을 생성할 수 있습니다. 새 버전의 사용 약관을 추가하면 기존 사용 약관이 대체됩니다. 정책을 편집할 경우 사용 약관 버전은 관리되지 않습니다.

[사용 약관] 페이지에서 사용 약관을 동의하거나 거절한 사용자의 수를 확인할 수 있습니다. 동의한 수 및 거절한 수를 클릭하면 모든 사용자 및 해당 상태를 볼 수 있습니다.

사용 약관 설정 및 사용

[사용 약관] 페이지에서 사용 약관 정책을 추가하고 사용 매개 변수를 구성합니다. 사용 약관이 추가되면 [사용 약관] 옵션을 사용하도록 설정합니다. 사용자는 Workspace ONE에 로그인할 때 카탈로그에 액세스하기 위해 사용 약관에 동의해야 합니다.

사전 요구 사항

사용 약관 정책 텍스트는 사용 약관 콘텐츠 텍스트 상자에서 복사하고 붙여 넣을 수 있도록 HTML로 형식이 지정되어야 합니다. 사용 약관은 영어, 독일어, 스페인어, 프랑스어, 이탈리아어 및 네덜란드어로 추가할 수 있습니다.

절차

1 VMware Identity Manager 콘솔의 [ID 및 액세스 관리] 탭에서 **설정 > 사용 약관**을 선택합니다.

2 **사용 약관**을 클릭합니다.

3 사용 약관을 설명하는 이름을 입력합니다.

4 사용 약관 정책이 모든 사용자에게 해당되면 **모든 사용자**를 선택합니다. 사용 약관을 디바이스 유형별로 사용하려면 **선택한 디바이스 플랫폼**을 선택하고 이 사용 약관 정책을 표시할 디바이스 유형을 선택합니다.

5 기본적으로 처음에 표시되는 사용 약관 언어는 브라우저 언어 환경설정을 기준으로 합니다. 텍스트 상자에 기본 언어의 사용 약관 콘텐츠를 입력합니다.

6 **저장**을 클릭합니다.

사용 약관 정책을 다른 언어로 추가하려면 **언어 추가**를 클릭하고 다른 언어를 선택합니다. [사용 약관 콘텐츠] 텍스트 상자가 새로 고쳐지며 텍스트 상자에 텍스트를 추가할 수 있습니다.

언어 이름을 끌어 사용 약관이 표시되는 순서를 설정할 수 있습니다.

7 사용 약관의 사용을 시작하려면 표시되는 페이지에서 **사용 약관 사용**을 클릭합니다.

다음에 수행할 작업

사용 약관에 대해 특정 디바이스 유형을 선택한 경우 다른 디바이스 유형에 대한 추가 사용 약관을 생성할 수 있습니다.

사용 약관 동의 상태 보기

[ID 및 관리] > [사용 약관] 페이지에 나열된 사용 약관 정책은 정책을 동의했거나 거절한 사용자 수가 표시됩니다.

절차

1 VMware Identity Manager 콘솔의 [ID 및 액세스 관리] 탭에서 **설정 > 사용 약관**을 선택합니다.

2 [동의함/거절함] 열에서 왼쪽의 [동의함] 횟수 또는 오른쪽의 [거절함] 횟수를 클릭합니다.

상태 페이지에는 수행된 작업(동의함 또는 거절함), 사용자 이름, 디바이스 ID, 확인한 정책의 버전, 사용되는 플랫폼 및 날짜가 표시됩니다.

3 보기를 닫으려면 **취소**를 클릭합니다.

Workspace ONE 애플리케이션 가져오기 및 배포

사용자가 자신의 디바이스 App Store에서 VMware Workspace ONE 애플리케이션을 다운로드하거나, 관리자가 Workspace ONE 애플리케이션을 관리 애플리케이션으로 디바이스에 푸시하도록 Workspace ONE UEM를 구성할 수 있습니다.

Workspace ONE UEM 콘솔에서 조직 내의 특정 그룹 및 사용자에게 Workspace ONE 애플리케이션을 배포합니다. 사용자는 자신의 디바이스에서 Workspace ONE 애플리케이션에 로그인한 후 사용 권한이 있는 웹 및 SaaS 애플리케이션에 액세스할 수 있습니다.

다음 단계는 Workspace ONE UEM 콘솔에서 Workspace ONE 모바일 애플리케이션을 관리 애플리케이션으로 푸시하는 단계입니다. Workspace ONE 시작 마법사를 실행하여 애플리케이션을 푸시할 수도 있습니다.

참고 Workspace ONE UEM에서 관리되는 애플리케이션을 구성하는 방법에 대한 자세한 내용은 리소스 포털(https://resources.air-watch.com)에서 제공되는 VMware Workspace ONE UEM MAM(모바일 애플리케이션 관리) 가이드를 참조하십시오.

사전 요구 사항

Workspace ONE UEM 콘솔에서 Workspace ONE 모바일 애플리케이션을 푸시하려는 경우 애플리케이션 사용 권한이 부여된 최종 사용자의 스마트 그룹을 준비합니다.

절차

1 Workspace ONE UEM 콘솔에서 **애플리케이션 및 설명서 > 애플리케이션** > **목록 보기 > 공개**로 이동한 후 **애플리케이션 추가**를 선택합니다.

2 플랫폼(iOS, Android 또는 Windows)을 선택합니다.

3 **App Store 검색**을 선택하고 **이름** 텍스트 상자에 App Store에서 VMware Workspace ONE을 찾기 위한 키워드로 Workspace ONE을 입력합니다.

4 **다음**을 선택하고 **선택**을 사용하여 [App Store 결과] 페이지에서 Workspace ONE 애플리케이션을 업로드합니다.

5 다음 탭 설정에서 Workspace ONE 사용자에 대한 할당 및 배포 옵션을 구성합니다.

탭	설명
정보	지원되는 디바이스 모델, 등급 및 범주와 관련된 정보를 입력하고 봅니다.
할당	Workspace ONE 모바일 애플리케이션을 자신의 디바이스에서 사용할 수 있는 최종 사용자의 스마트 그룹에 할당합니다.
배포	해당되는 경우 가용성 및 고급 EMM(Enterprise Mobility Management) 기능을 구성합니다. 관리되는 애플리케이션을 자동으로 구성하려면 **애플리케이션 구성 보내기**를 사용하도록 설정하고 ACE(App Configuration for Enterprise) 키 값 쌍을 입력합니다. 엔터프라이즈 키 값 쌍에 대한 Workspace ONE UEM 애플리케이션 구성의 내용을 참조하십시오.
사용 약관	(선택 사항) Workspace ONE 애플리케이션 사용을 위해 **사용 약관**을 사용하도록 설정합니다.

6 사용자가 **저장 및 게시**를 선택하면 해당 애플리케이션을 사용할 수 있게 합니다.

지원되는 각 플랫폼에 대해 이 단계를 완료합니다.

엔터프라이즈 키 값 쌍에 대한 Workspace ONE UEM 애플리케이션 구성

Workspace ONE UEM에서 Workspace ONE 애플리케이션을 관리되는 애플리케이션으로 배포하고 Workspace ONE UEM 콘솔에서 Workspace ONE 애플리케이션을 푸시할 때 [애플리케이션 구성 보내기]를 사용하도록 설정하면 사용자가 Workspace ONE 애플리케이션을 설치 및 시작할 때 적용되는 Workspace ONE 설정을 미리 구성할 수 있습니다.

Workspace ONE 애플리케이션이 Workspace ONE UEM 콘솔에 관리되는 모바일 애플리케이션으로 업로드되면 Android 디바이스에서 VMware Workspace ONE 서버 URL, 디바이스 UID 값 및 인증서 인증에 대한 요구 사항을 구성할 수 있습니다.

표 7-1. Workspace ONE UEM 콘솔의 Workspace ONE 관리되는 디바이스 구성 옵션

플랫폼	구성 키	값 유형	구성 값	설명
모두	AppServiceHost	문자열	<VMware Workspace ONE 서버 URL>	디바이스에서 VMware Workspace ONE에 대한 서버 URL을 구성합니다.
iOS	deviceUDID	문자열	{DeviceUid} 디바이스 UID 값을 입력합니다. [조회 값 입력] 기능을 사용하지 마십시오.	VMware Identity Manager 환경에 대한 인증을 받는 데 사용되는 디바이스를 추적합니다.

표 7-1. Workspace ONE UEM 콘솔의 Workspace ONE 관리되는 디바이스 구성 옵션 (계속)

플랫폼	구성 키	값 유형	구성 값	설명
iOS	SkipDiscoveryScreen	부울	**true**	Workspace ONE 애플리케이션 버전 3.1부터 SkipDiscoveryScreen 구성 키를 구성할 수 있습니다. True로 설정하면 Workspace ONE에서 이메일 주소/서버 URL 화면을 통과하려고 합니다. AppServiceHost 구성 키가 사용될 경우 사용자는 인증 화면으로 즉시 이동됩니다. 모바일 SSO도 사용되도록 설정하면 관리자는 Workspace ONE을 시작하면 Workspace ONE 애플리케이션 로드가 즉시 시작되는 원활한 경험을 최종 사용자에게 제공할 수 있습니다.
Android 및 iOS	RemoveAccountSignOut	정수	0 - [계정 제거] 옵션이 표시됨 1 - [계정 제거] 옵션이 표시되지 않음 값을 설정하지 않으면 [계정 제거] 옵션이 표시됩니다.	값을 1로 설정하면 Workspace ONE 설정 페이지에서 [계정 제거] 옵션이 표시되지 않습니다. 사용자가 디바이스에서 Workspace ONE 계정을 제거할 수 없습니다. 이 값이 0으로 설정되거나 값이 설정되지 않으면 [계정 제거] 옵션이 표시됩니다. 사용자가 [계정 제거]를 클릭하면 Workspace ONE UEM에서 디바이스의 엔터프라이즈 초기화를 수행하고 Workspace ONE UEM에서 디바이스가 등록 취소됩니다.

자동 검색을 위해 이메일 도메인 등록

자동 검색 서비스에 이메일 도메인을 등록하여 최종 사용자가 Workspace ONE 애플리케이션을 통해 애플리케이션 포털에 더욱 쉽게 액세스하도록 할 수 있습니다. 최종 사용자는 조직 URL 대신 해당 이메일 주소를 입력합니다.

조직의 이메일 도메인이 자동 검색에 등록된 경우 최종 사용자는 로그인 페이지에서 이메일 주소만 입력해도 애플리케이션 포털에 액세스할 수 있습니다. 예를 들어 username@myco.com을 입력합니다.

자동 검색을 사용하지 않는 경우 최종 사용자는 Workspace One 애플리케이션을 처음 열 때 전체 조직 URL을 제공해야 합니다. 예를 들어 myco.vmwareidentity.com을 입력합니다.

VMware Identity Manager 에서 자동 검색 설정

도메인을 등록하려면 VMware Identity Manager 콘솔의 [자동 검색] 페이지에서 이메일 도메인 및 이메일 주소를 입력합니다.

활성화 토큰이 포함된 이메일 메시지가 도메인의 사용자 이메일 주소로 전송됩니다. 도메인 등록을 활성화하려면 [자동 검색] 페이지에서 토큰을 입력하고 등록한 도메인이 사용자의 도메인인지 확인합니다.

참고 VMware Identity Manager 온-프레미스 배포에 대해 자동 검색을 설정하려면 VMware Identity Manager 콘솔에 로컬 관리자로 로그인해야 합니다. Workspace ONE UEM 웹 사이트 https://secure.air-watch.com/register에서 생성한 Workspace ONE UEM ID 및 암호를 입력합니다.

절차

1 VMware Identity Manager 콘솔의 [ID 및 액세스 관리] 탭에서 **설정 > 자동 검색**을 클릭합니다.

2 (온-프레미스 배포만 해당) Workspace ONE UEM 자동 검색 URL을 구성합니다.

옵션	설명
자동 검색 URL	URL을 https://discovery.awmdm.com으로 입력합니다.
AirWatch ID	Workspace ONE UEM에 등록한 이메일 주소를 입력하여 웹 사이트에 로그인합니다.
암호	Workspace ONE UEM 계정과 연결된 암호를 입력합니다.

3 **이메일 도메인** 텍스트 상자에 등록할 조직 이메일 도메인을 입력합니다.

4 **확인 이메일 주소** 텍스트 상자에 확인 토큰을 수신할 이메일 도메인의 이메일 주소를 입력합니다.

5 **확인**을 클릭합니다.

이메일 도메인 등록 상태가 [보류 중]으로 표시됩니다. 보류 중인 이메일 도메인은 한 번에 하나만 있을 수 있습니다.

6 해당 이메일로 이동한 후 메시지에 있는 활성화 토큰을 복사합니다.

7 **ID 및 액세스 관리 > 자동 검색** 페이지로 돌아가서 [활성화 토큰] 텍스트 상자에 토큰을 붙여넣습니다.

8 **확인**을 클릭하여 도메인을 등록합니다.

이메일 도메인이 등록되어 [자동 검색] 페이지의 등록된 이메일 도메인 목록에 추가됩니다.

이제 최종 사용자가 Workspace ONE 애플리케이션에 해당 이메일 주소를 입력하여 애플리케이션 포털에 액세스할 수 있습니다.

다음에 수행할 작업

사용하는 이메일 도메인이 2개 이상인 경우 다른 이메일 도메인을 추가하여 등록합니다.

세션 인증 설정

VMware Identity Manager 서비스에는 VMware Identity Manager 리소스에 대한 사용자 액세스를 제어하는 기본 액세스 정책이 포함되어 있습니다.

정책 규칙에 구성된 인증 세션 길이는 애플리케이션 시작 관리자 페이지에 액세스하거나 특정 웹 애플리케이션을 시작하기 위한 마지막 인증 이벤트 이후에 허용되는 최대 시간을 결정합니다. 기본값은 8시간입니다. 인증을 받은 사용자는 다른 인증 이벤트를 시작하여 이 시간을 연장하지 않는 한, 8시간 이내에 웹 애플리케이션을 실행할 수 있습니다.

VMware Identity Manager 관리 콘솔, [ID 및 액세스 관리] 탭, [관리] > [정책]에서 기본 정책을 편집하여 세션 길이를 변경할 수 있습니다. VMware Identity Manager 관리 가이드의 "액세스 정책 관리"를 참조하십시오.

Workspace ONE UEM 관리 디바이스에 대한 규정 준수 검사 사용

사용자가 디바이스를 등록한 경우 규정 준수를 평가하는 데 사용되는 데이터가 포함된 샘플이 스케줄에 따라 전송됩니다. 이 샘플 데이터 평가에서는 Workspace ONE UEM(UEM) 콘솔에서 관리자가 설정한 규정 준수 규칙을 디바이스가 준수하는지 확인합니다. 디바이스가 규정을 벗어난 경우 UEM 콘솔에 구성된 해당 작업이 수행됩니다.

VMware Identity Manager 서비스에는 사용자가 디바이스에서 로그인할 때 Workspace ONE UEM 서버에서 디바이스 규정 준수 상태를 검사하도록 구성할 수 있는 액세스 정책 옵션이 있습니다. 규정 준수 검사를 사용하면 디바이스가 규정을 벗어난 경우에 사용자가 애플리케이션에 로그인하거나 Single Sign-On을 통해 Workspace ONE 포털에 들어가는 것을 차단할 수 있습니다. 디바이스가 다시 규정을 준수하게 되면 로그인 기능이 복원됩니다.

디바이스 보안이 침해된 경우 Workspace ONE 애플리케이션이 자동으로 로그아웃되고 애플리케이션에 대한 액세스를 차단합니다. 디바이스가 어댑티브 관리를 통해 등록된 경우 UEM 콘솔을 통해 실행되는 엔터프라이즈 초기화 명령이 디바이스를 등록 해제하고 관리되는 애플리케이션을 디바이스에서 제거합니다. 관리되지 않는 애플리케이션은 제거되지 않습니다.

Workspace ONE UEM 규정 준수 정책에 대한 자세한 내용은 VMware Workspace ONE UEM 설명서 페이지에서 VMware Workspace ONE UEM 모바일 디바이스 관리 가이드를 참조하십시오.

다중 Workspace ONE UEM 조직 그룹 설정을 위한 배포 전략

Workspace ONE UEM는 OG(조직 그룹)를 사용하여 사용자를 식별하고 사용 권한을 설정합니다. Workspace ONE UEM가 VMware Identity Manager에 통합되면 관리자 및 등록 사용자의 REST API 키가 유형이 [고객]인 Workspace ONE UEM 조직 그룹에 구성됩니다.

사용자가 디바이스에서 Workspace ONE에 로그인할 때 VMware Identity Manager 내에서 디바이스 등록 이벤트가 트리거됩니다. 사용자 및 디바이스 조합에 사용 권한이 부여된 애플리케이션을 끌어오기 위한 요청이 Workspace ONE UEM로 전송됩니다. Workspace ONE UEM 내에서 사용자를 찾고 해당 조직 그룹에 디바이스를 배치하기 위해 REST API를 사용하여 요청이 전송됩니다.

조직 그룹을 관리하기 위해 VMware Identity Manager에서 2가지 옵션을 구성할 수 있습니다.

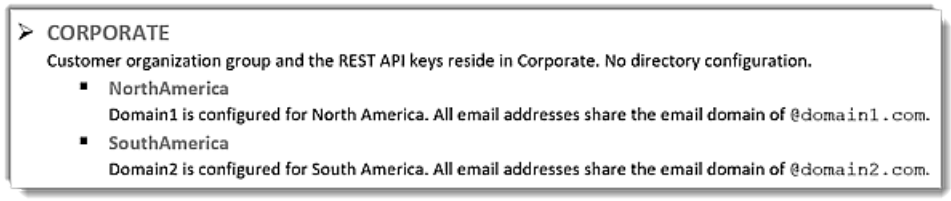
- Workspace ONE UEM 자동 검색 사용
- Workspace ONE UEM 조직 그룹을 VMware Identity Manager 서비스의 도메인에 매핑

이러한 두 옵션을 모두 구성하지 않았다면 Workspace ONE에서 REST API 키가 생성된 조직 그룹에서 사용자를 찾으려고 합니다. 이것이 고객 그룹입니다.

Workspace ONE UEM 자동 검색 사용

단일 디렉토리가 고객 조직 그룹에 대한 하위 그룹으로 구성되어 있거나 여러 디렉토리가 고유한 이메일 도메인을 가진 고객 그룹 아래에 구성되어 있는 경우 자동 검색을 설정합니다.

그림 7-1. 예제 1



예제 1에서는 조직의 이메일 도메인이 자동 검색을 위해 등록됩니다. 사용자는 Workspace ONE 로그인 페이지에 이메일 주소만 입력합니다.

이 예제에서 NorthAmerica 도메인의 사용자가 Workspace ONE에 로그인할 때 전체 이메일 주소를 user1@domain1.com으로 입력합니다. 애플리케이션에서는 도메인을 찾고 사용자가 존재하는지 또는 NorthAmerica 조직 그룹에서 디렉토리 호출로 생성될 수 있는지 확인합니다. 디바이스를 등록할 수 있습니다.

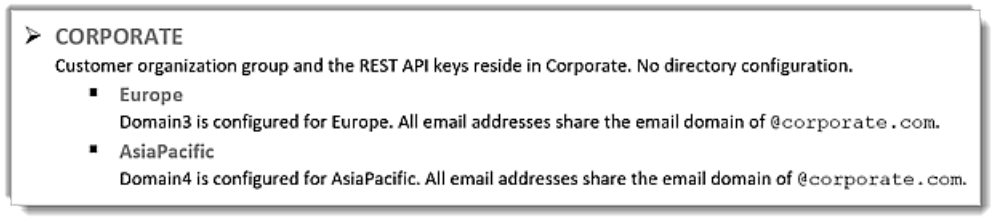
VMware Identity Manager 도메인에 대한 Workspace ONE UEM 조직 그룹 매핑 사용

여러 디렉토리가 동일한 이메일 도메인으로 구성되어 있을 때 Workspace ONE UEM 조직 그룹 매핑에 VMware Identity Manager 서비스를 구성합니다. VMware Identity Manager 콘솔의 AirWatch 구성 페이지에서 **여러 조직 그룹에 도메인 매핑**을 사용하도록 설정합니다.

[여러 조직 그룹에 도메인 매핑] 옵션을 사용하도록 설정하면 VMware Identity Manager에 구성된 도메인을 Workspace ONE UEM 조직 그룹 ID에 매핑할 수 있습니다. 관리자 REST API 키도 필요합니다.

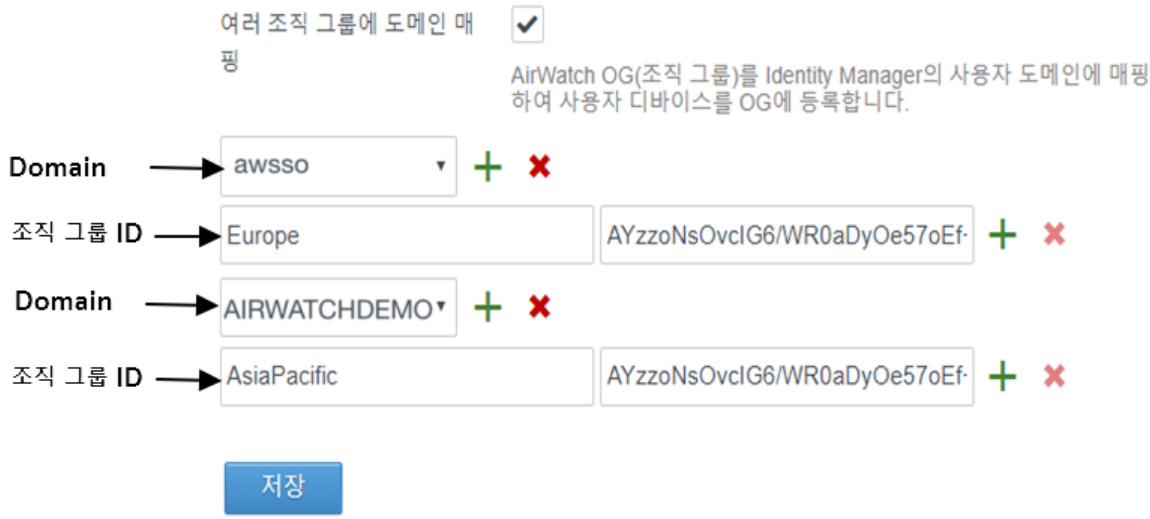
예제 2에서는 2개의 도메인이 서로 다른 조직 그룹에 매핑되어 있습니다. 관리자 REST API 키가 필요합니다. 동일한 관리자 REST API 키가 두 조직 그룹 ID에 사용됩니다.

그림 7-2. 예제 2



VMware Identity Manager 콘솔의 AirWatch 구성 페이지에서 각 도메인에 대해 특정 Workspace ONE UEM 조직 그룹 ID를 구성합니다.

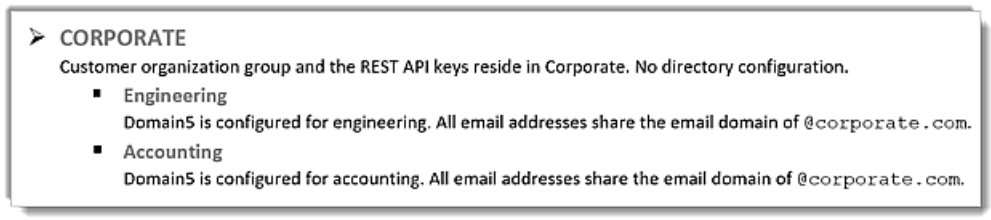
그림 7-3. 예제 2 조직 그룹 구성



이 구성을 사용할 경우, 사용자가 해당 디바이스에서 Workspace ONE에 로그인할 때 디바이스 등록 요청이 조직 그룹 Europe의 Domain3에서 사용자를 찾고 조직 그룹 AsiaPacific의 Domain4에서 사용자를 찾으려고 합니다.

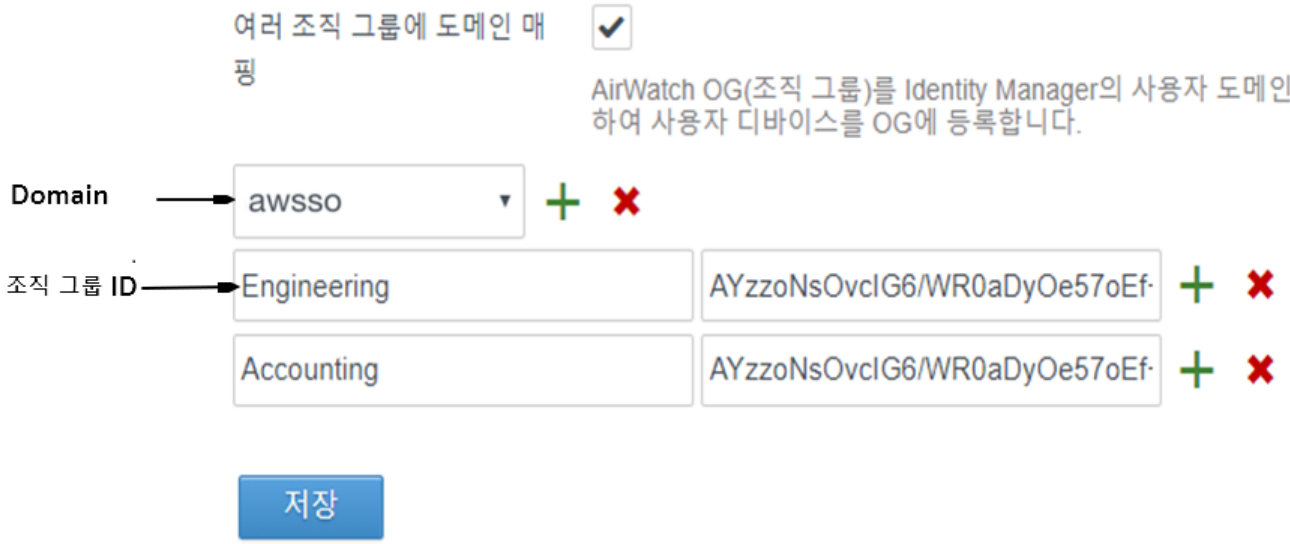
예제 3에서는 하나의 도메인이 여러 Workspace ONE UEM 조직 그룹에 매핑되어 있습니다. 두 디렉토리 모두 이메일 도메인을 공유합니다. 도메인은 동일한 Workspace ONE UEM 조직 그룹을 가리킵니다.

그림 7-4. 예제 3



이 구성에서는 사용자가 Workspace ONE에 로그인할 때 등록하려는 그룹을 선택하라는 메시지가 애플리케이션에 표시됩니다. 이 예제에서 사용자는 Engineering 또는 Accounting을 선택할 수 있습니다.

그림 7-5. 디렉토리에서 동일한 도메인을 공유하는 조직 그룹



올바른 조직 그룹에 디렉토리 배치

사용자 기록을 찾으면 디바이스가 알맞은 조직 그룹에 추가됩니다. Workspace ONE UEM 등록 설정 **그룹 ID 할당 모드**는 디바이스를 배치할 조직 그룹을 결정합니다. 이 설정은 Workspace ONE UEM Console의 [시스템 설정] > [디바이스 및 사용자] > [일반] > [등록] > [그룹화] 페이지에 있습니다.

그림 7-6. 디바이스의 Workspace ONE UEM 그룹 등록

예제 4에서 모든 사용자는 회사 조직 그룹 수준에 있습니다.

그림 7-7. 예제 4

디바이스 배치는 회사 조직 그룹의 그룹 ID 할당 모드에 대해 선택한 구성에 따라 다릅니다.

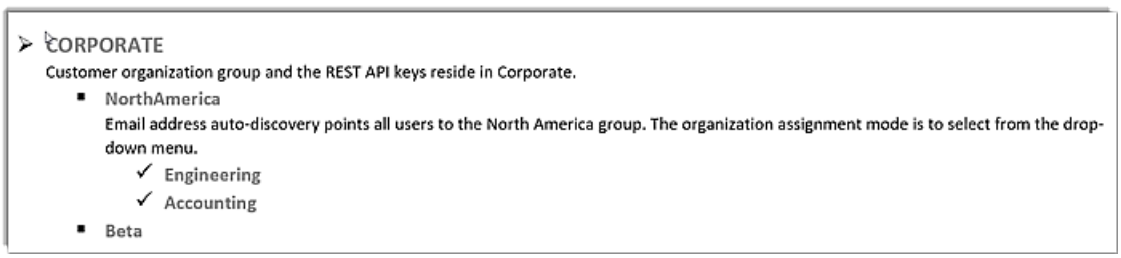
- [기본값]을 선택하면 디바이스는 사용자가 있는 동일한 그룹에 배치됩니다. 예제 4의 경우 디바이스는 Corporate 그룹에 배치됩니다.
- [그룹 ID를 선택하라는 메시지 표시]를 선택하면 디바이스를 등록할 그룹을 선택하라는 메시지가 표시됩니다. 예제 4의 경우 Engineering 및 Accounting이 옵션으로 포함된 드롭다운 메뉴가 Workspace ONE 앱 내에 표시됩니다.
- [사용자 그룹에 따라 자동으로 선택]을 선택하면 디바이스는 Workspace ONE UEM 콘솔의 사용자 그룹 할당 및 해당 매핑에 따라 Engineering 또는 Accounting에 배치됩니다.

숨겨진 그룹에 대한 개념 이해

예제 4에서 등록할 조직 그룹을 선택하라는 메시지가 표시되면 Workspace ONE 애플리케이션에서 제공된 목록에 포함되지 않은 그룹 ID를 입력할 수도 있습니다. 이것이 바로 숨겨진 그룹 개념입니다.

예제 5에서는 Corporate 조직 그룹 구조에서 North America 및 Beta가 Corporate 아래에 그룹으로 구성됩니다.

그림 7-8. 예제 5



예제 5에서 사용자는 Workspace ONE에 해당 이메일 주소를 입력합니다. 인증이 완료되면 사용자에게 선택할 수 있는 Engineering 및 Accounting을 포함하는 목록이 표시됩니다. 표시되는 Beta는 옵션이 아닙니다. 사용자가 조직 그룹 ID를 아는 경우, 그룹 선택 텍스트 상자에 수동으로 Beta를 입력하고 Beta에 디바이스를 성공적으로 등록할 수 있습니다.

8 Workspace ONE 포털에서 작업

Workspace ONE 애플리케이션이 디바이스에 설치되면 사용자는 Workspace ONE에 로그인하여 조직에서 사용 설정한 애플리케이션 카탈로그에 안전하게 액세스할 수 있습니다. 애플리케이션이 Single Sign-On으로 구성된 경우 사용자는 애플리케이션을 실행할 때 로그인 자격 증명을 다시 입력하지 않아도 됩니다.

Workspace ONE 사용자 인터페이스는 휴대폰, 태블릿 및 데스크톱에서 비슷하게 작동합니다. Workspace ONE의 [카탈로그] 페이지에는 Workspace ONE에 푸시된 리소스가 표시됩니다. 탭 또는 클릭하여 애플리케이션을 검색하고, 추가하고, 북마크를 적용하고, 업데이트할 수 있습니다. 애플리케이션을 마우스 오른쪽 버튼으로 클릭하여 북마크가 지정된 페이지에서 제거한 후 [카탈로그] 페이지로 이동하여 사용 권한이 부여된 리소스를 추가할 수 있습니다.

본 장은 다음 항목을 포함합니다.

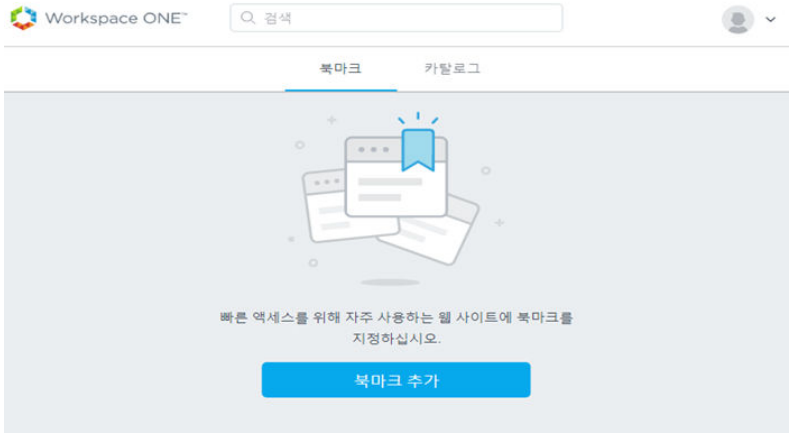
Workspace ONE 에서 애플리케이션 사용

Workspace ONE 사용자 포털은 [카탈로그] 탭 및 [북마크] 탭으로 구성되어 있습니다. 사용자가 Workspace ONE 포털에 처음으로 로그인하면 책갈피 탭이 비어 있는 경우 카탈로그 탭이 표시됩니다.

처음 실행한 후에는 마지막에 방문한 탭으로 곧바로 이동합니다. [카탈로그] 탭에서 시작하고 싶은 경우 카탈로그 보기를 사용할 수 있습니다.

Workspace ONE 포털에서 [카탈로그] 또는 [책갈피] 탭을 숨겨 사용자의 요구 사항에 맞는 사용자 환경을 제공할 수 있습니다. VMware Identity Manager 콘솔의 [카탈로그] > [설정] > [사용자 포털 구성] 페이지에서 포털 구성을 변경할 수 있습니다.

그림 8-1. 북마크 페이지의 초기 보기



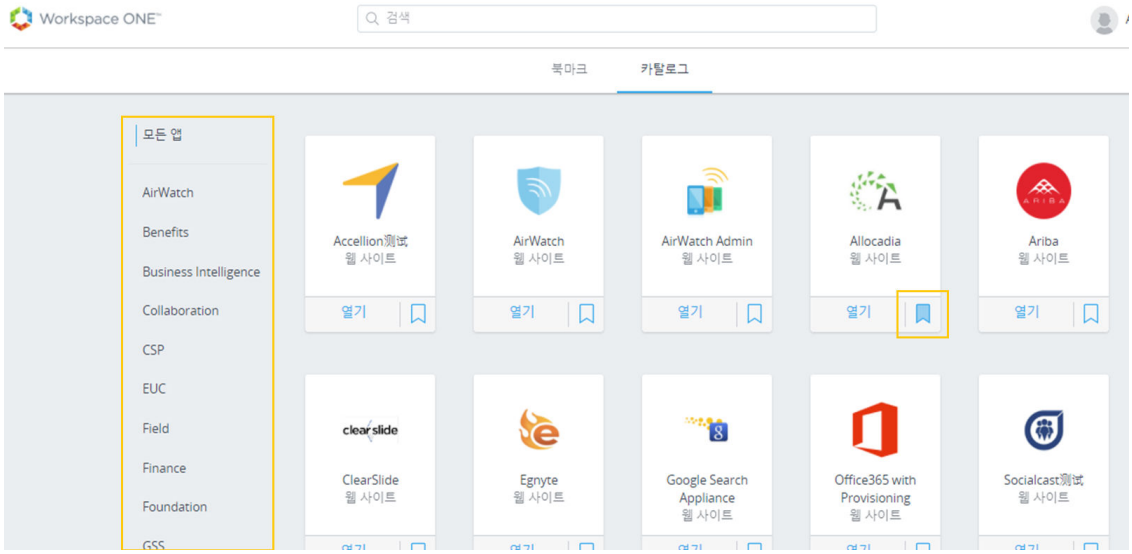
카탈로그에서 사용 권한이 부여된 웹, 모바일 및 가상 애플리케이션을 설치할 수 있습니다. 웹 및 가상 애플리케이션을Workspace ONE 앱의 [카탈로그] 또는 [책갈피] 페이지에서 직접 열 수 있습니다.

iOS 및 Android 같은 기본 애플리케이션은 Workspace ONE 페이지에서 책갈피를 지정하거나 실행할 수 없습니다. 이러한 애플리케이션은 iOS 또는 Android springboard에서 실행됩니다.

[카탈로그] 페이지에서 사용자가 보다 쉽게 필요한 리소스를 찾을 수 있도록 애플리케이션을 논리적인 범주로 그룹화할 수 있습니다. [권장]이라고 하는 하나의 범주가 기본적으로 표시됩니다. 애플리케이션을 [권장]으로 분류하면 **책갈피 탭에 권장 애플리케이션 표시**를 사용하도록 설정하여 책갈피 페이지를 이러한 애플리케이션으로 미리 채울 수 있습니다.

이 구성을 사용하면 사용자에게는 Workspace ONE 포털에 처음 로그인할 때 권장 애플리케이션에 바로 액세스할 수 있는 기능이 제공됩니다.

그림 8-2. Workspace ONE [카탈로그] 페이지



참고 모바일 애플리케이션은 데스크톱 브라우저에서 사용할 수 없습니다.

다음과 같이 웹 애플리케이션을 실행할 수 있습니다.

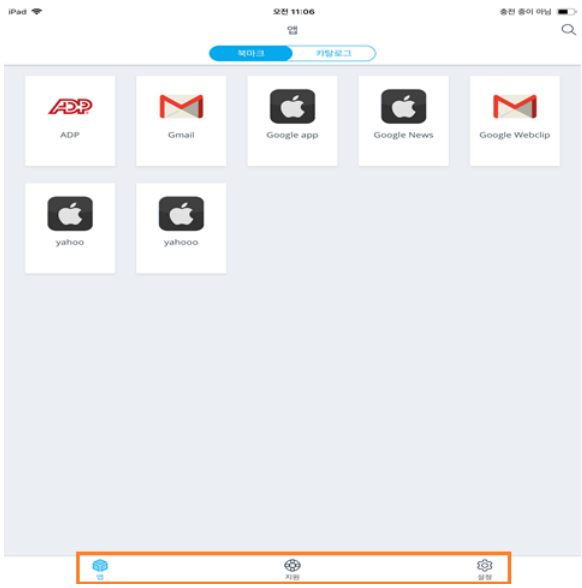
- [북마크] 탭. 애플리케이션 아이콘을 클릭하여 애플리케이션을 실행할 수 있습니다.
- [카탈로그] 탭. 화살표 아이콘이 있는 확인란을 클릭하여 애플리케이션을 엽니다.
- Spotlight 검색 또는 Workspace ONE 내에서 검색. iOS 디바이스의 Spotlight 검색에서 목록에 있는 애플리케이션을 선택합니다. Workspace ONE 검색에서 화살표 아이콘이 있는 확인란을 클릭하여 애플리케이션을 엽니다.

이름 옆에 있는 드롭다운 화살표에서 다음 Workspace ONE 설정에 액세스할 수 있습니다.

- 계정. 이름, 사용자 이름 및 이메일 주소 등 사용자에 대한 프로파일 정보입니다.
- 디바이스. Workspace ONE 애플리케이션에 로그인한 디바이스 목록 및 마지막 로그인 날짜와 시간입니다.
- 애플리케이션 팁. 사용자 디바이스에서 Workspace ONE을 탐색하는 방법에 대한 팁입니다.
- 정보. Workspace ONE 저작권, 특허권 및 라이센스 정보입니다.
- 환경설정. Horizon 원격 애플리케이션에 액세스하고, Horizon Client 또는 브라우저에서 애플리케이션을 볼 때 사용하는 기본 실행 설정입니다.

사용자는 디바이스에서 Workspace ONE 애플리케이션 아이콘을 탭하여 애플리케이션 포털에 로그인합니다. 북마크를 지정한 애플리케이션이 있으면 [북마크] 페이지가 표시됩니다. 디바이스의 Workspace ONE 애플리케이션에는 지원 및 설정에 대한 링크가 포함됩니다.

그림 8-3. Workspace ONE 포털의 디바이스 보기



- [지원] 페이지에는 [디바이스] 및 [보고서 전송] 페이지 링크가 포함되어 있습니다. [디바이스] 페이지에는 디바이스에 마지막으로 로그인한 시기가 표시됩니다. [보고서 전송]에서는 진단 정보 또는 기타 피드백을 전송하는 방법을 제공합니다. 디바이스 설정에서 이 기능을 해제하거나 설정할 수 있습니다.

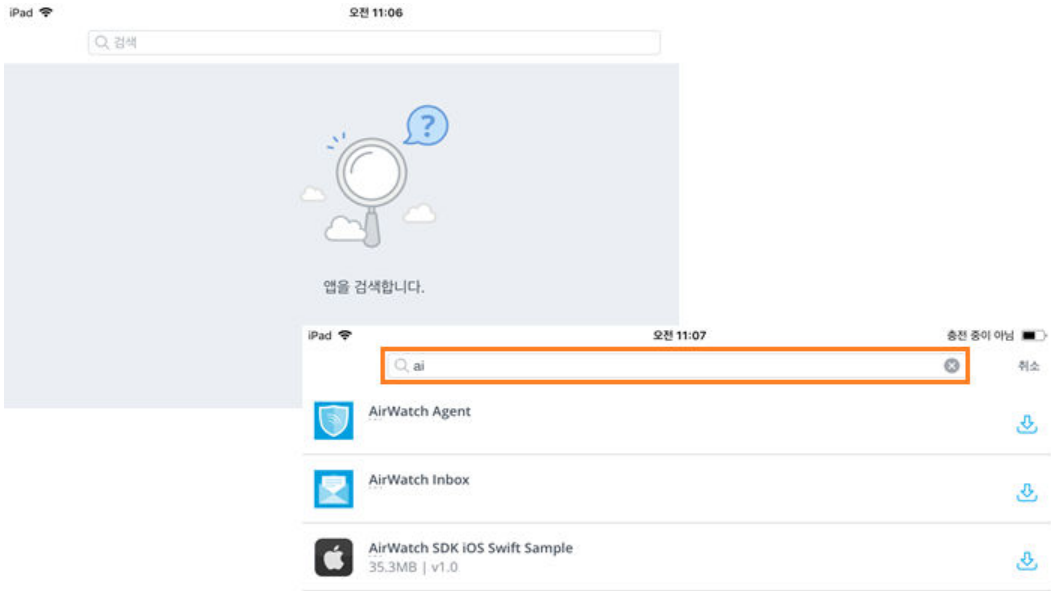
- [설정] 페이지에는 Workspace ONE 애플리케이션 버전 및 VMware Workspace 개인 정보 보호 정책이 표시됩니다. [설정] 페이지에서 계정을 제거하여 Workspace ONE 애플리케이션에서 로그아웃할 수 있습니다.

Workspace ONE 에서 검색 사용

Workspace ONE에서 검색을 사용하여 이름 또는 범주를 기준으로 애플리케이션을 찾을 수 있습니다.

검색 텍스트 상자에 입력하면 입력한 내용과 일치하는 애플리케이션이 표시됩니다.

그림 8-4. 검색에 표시되는 결과



웹 애플리케이션을 실행하거나 검색 결과에서 직접 기본 애플리케이션을 다운로드할 수 있습니다.

iOS 디바이스에서 Spotlight를 사용하여 Workspace ONE 포털에 있는 애플리케이션을 검색할 수 있습니다. iOS 디바이스의 홈 화면에서 손가락으로 화면을 터치하고 아래로 끌어 Spotlight 검색 필드를 표시합니다. Workspace ONE 포털에 있는 애플리케이션 이름을 입력하면 Workspace ONE이 열리고 애플리케이션이 실행됩니다.

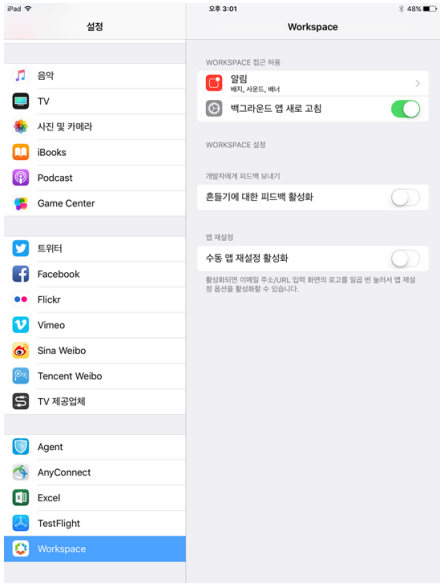
iOS 디바이스에서 사용자 보고서 문제 해결 지원

iOS 디바이스에서 Rage Shake 기능을 사용하여 iOS 애플리케이션 개발자에게 로그를 전송할 수 있습니다.

디바이스를 흔들면 디바이스는 기본적으로 현재 상태를 기록하고 세부 정보를 Workspace ONE 애플리케이션 개발자에게 이메일 메시지로 전송합니다. 사용자가 다른 이메일 주소를 수동으로 입력하여 해당 주소로 정보를 전송할 수도 있습니다.

디바이스의 [설정] > [Workspace] 페이지에서 [흔들어 피드백 보내기 사용] 기능을 켤 수 있습니다. Workspace ONE 포털의 임의 화면에서 Rage Shake를 사용하여 보고서를 전송할 수 있습니다.

그림 8-5. 흔들어 피드백 보내기 사용 기능



iOS 디바이스에 이 디바이스가 다른 사용자 또는 환경에 등록되어 있습니다와 비슷한 오류 메시지가 수신되면 [애플리케이션 수동 재설정] 옵션을 사용하여 디바이스에 로컬로 저장된 모든 애플리케이션 데이터를 지울 수 있습니다.

Workspace ONE 애플리케이션에 대한 암호 설정

사용자는 자신의 디바이스에 암호 기능을 사용하도록 설정해야 합니다. 이 기능을 사용하도록 설정하지 않으면 Workspace ONE 애플리케이션을 처음 시작할 때 암호를 만들라는 메시지가 표시됩니다. 이 암호는 사용자가 자신의 디바이스에서 Workspace ONE에 액세스할 때마다 입력해야 합니다.

암호 기능을 사용하지 않는 경우 사용자에게 Workspace ONE 애플리케이션에 액세스하려면 먼저 암호를 설정하라는 메시지가 나타납니다. 암호 설정 위치는 플랫폼에 따라 다릅니다. Android 디바이스의 경우 애플리케이션 수준에서 암호가 설정됩니다. Workspace ONE 3.2 또는 이전 버전을 사용하는 Windows 데스크톱 디바이스 및 iOS 디바이스의 경우 디바이스 수준에서 암호가 설정됩니다.

참고 iOS 및 Android 디바이스는 Touch ID 지문 인식 기능도 지원합니다.

Workspace ONE은 디바이스에서 발생 가능한 보안 문제를 감지할 수 있습니다. 사용자가 디바이스에서 암호를 사용하지 않도록 설정할 경우 다음번에 Workspace ONE 애플리케이션에 액세스할 때, Workspace ONE에 액세스하기 위해 먼저 암호를 설정하라는 메시지가 표시됩니다. 애플리케이션 수준 암호가 사용하도록 설정되어 있으면 최종 사용자는 애플리케이션 수준 암호를 사용하지 않도록 설정할 수 없습니다.

iOS 디바이스의 애플리케이션 수준 암호

4자리 최소 디바이스 암호보다 더 복잡한 암호를 생성할 수 있습니다. 애플리케이션 수준 암호를 다른 생산성 애플리케이션(예: VMware Boxer)과 공유할 수 있습니다.

Workspace ONE UEM 콘솔에서 애플리케이션에 대한 로컬 암호 요구 사항을 지정합니다. [그룹 및 설정] > [모든 설정] > [애플리케이션] > [설정 및 정책] > [보안 정책] > [인증 유형]으로 이동합니다.

암호 인증이 구성되면 다른 생산성 애플리케이션이 없는 경우 사용자에게 애플리케이션 수준 암호를 설정하라는 메시지가 표시되고, 그렇지 않은 경우 다른 생산성 애플리케이션과 공유되는 암호를 입력하라는 메시지가 표시됩니다.

암호 인증이 구성되지 않은 경우 iOS 디바이스에 디바이스 암호가 필요합니다.

기본 애플리케이션 추가

기본 애플리케이션은 특정 모바일 디바이스용으로 개발된 애플리케이션 프로그램입니다. 사용자는 [Workspace ONE 카탈로그] 페이지에서 Workspace ONE UEM 사용 권한이 있는 기본 애플리케이션을 볼 수 있습니다. 예를 들어 사용자가 iOS 디바이스에서 카탈로그를 보는 경우 사용자에게 사용 권한이 있는 iOS 애플리케이션만 표시됩니다.

사용자가 [카탈로그] 페이지에서 [설치]를 눌러 디바이스에 애플리케이션을 설치합니다. [설치]를 누르면 다음에 진행될 작업을 알려주는 팝업이 나타납니다. 표시되는 정보는 애플리케이션 유형 및 플랫폼에 따라 다릅니다. 잠금 아이콘이 표시된 애플리케이션은 Workspace ONE UEM에서 디바이스를 관리해야 합니다. 최종 사용자가 잠금 아이콘이 표시된 애플리케이션을 다운로드하려고 하면 Installation of this app requires enablement of Workspace Services라는 메시지가 나타납니다.

사용자 인증을 위해 VMware Verify 사용

VMware Verify 서비스가 디바이스에서 Workspace ONE으로 로그인하기 위한 2단계 인증의 2번째 인증 방법으로 설정되면 사용자는 디바이스 App Store에서 VMware Verify 애플리케이션을 다운로드해야 합니다.

사용자가 Workspace ONE 애플리케이션에 처음으로 로그인하면 사용자 이름과 암호를 입력하라는 메시지가 나타납니다. 사용자 이름과 암호가 확인되면 VMware Verify 서비스에 등록할 디바이스 전화 번호를 입력하라는 메시지가 나타납니다.

등록을 클릭하면 디바이스 전화 번호가 VMware Verify 서비스에 등록됩니다. VMware Verify 애플리케이션을 다운로드하지 않으면 애플리케이션을 다운로드하라는 메시지가 표시됩니다.

애플리케이션이 설치되면 이전에 입력한 것과 동일한 전화 번호를 입력하고 일회용 등록 코드를 받을 알림 방법을 선택하라는 메시지가 나타납니다. 등록 코드는 [등록 PIN] 페이지에 입력됩니다.

디바이스 전화 번호가 등록된 후 사용자는 VMware Verify 애플리케이션에 표시된 시간 기반 일회용 암호를 사용하여 Workspace ONE에 로그인할 수 있습니다. 이 암호는 디바이스에 생성되는 고유 번호이며 지속적으로 변경됩니다.

사용자는 둘 이상의 디바이스를 등록할 수 있습니다. VMware Verify 암호는 등록된 각 디바이스에 자동으로 동기화됩니다.

Workspace ONE 사용자에게 경고 전송

관리자는 작업을 요청하거나 경고를 전송하기 위해 예정된 시스템 다운타임, 규정 준수 상태를 Workspace ONE 사용자에게 알릴 수 있습니다. 알림은 Workspace ONE UEM 콘솔을 통해 전송됩니다.

사용자는 디바이스에서 알림을 수신하는 방법을 관리합니다.

Android용 Workspace ONE 디바이스 사용

Android Workspace ONE 애플리케이션을 통해 다음 유형의 애플리케이션을 사용하도록 설정할 수 있습니다.

- 웹 애플리케이션
- VMware Identity Manager 서비스에서 사용하도록 설정된 원격 애플리케이션으로, Horizon 가상 애플리케이션, Citrix XenApp 및 ThinApp 등이 있습니다.
- 기본 애플리케이션(관리 및 비관리) 기본 애플리케이션은 Android 플랫폼용으로 개발된 Android 애플리케이션입니다. 2가지 유형을 사용할 수 있습니다.
  - Google Play Store에서 배포된 공개 애플리케이션
  - Workspace ONE UEM를 통해 비공개로 배포되며 Google Play Store에서 제공되지 않는 내부 애플리케이션

  웹 애플리케이션은 브라우저에서 열립니다. 사용자는 VMware Horizon Client 또는 Citrix Receiver를 통해 가상 애플리케이션에 액세스할 수 있습니다.

Android 디바이스에서 Workspace ONE 애플리케이션 등록

올바른 서버 URL 및 자격 증명을 사용하여 Workspace ONE 애플리케이션에 로그인하면 Workspace ONE 통합 카탈로그에 액세스할 수 있습니다. 통합 카탈로그에서 사용자는 자신에게 할당된 모든 애플리케이션을 볼 수 있습니다.

애플리케이션에 액세스하려면 Workspace ONE 애플리케이션을 등록해야 합니다. Workspace ONE 등록 상태에서 사용자는 VMware Identity Manager, Workspace ONE UEM 생산성 애플리케이션 및 관리 기능 없는 SDK 애플리케이션을 통해 사용하도록 설정된 웹 및 가상 애플리케이션을 사용할 수 있습니다.

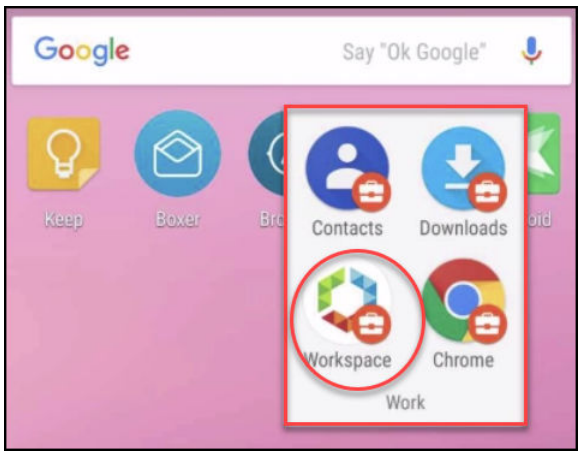
참고 SDK 애플리케이션은 Workspace ONE UEM SDK를 통해 컨테이너화 및 관리되므로 관리를 받기 위한 디바이스가 필요 없습니다.

사용자는 어댑티브 관리를 시작할 수 있습니다. 어댑티브 관리에서는 디바이스에서 Android for Work가 사용하도록 설정되며 디바이스의 프로파일, 정책 및 향상된 애플리케이션 배포가 수행됩니다.

Workspace ONE을 사용하여 Android for Work 관리

디바이스에서 Android for Work를 사용하도록 설정하면 운영 체제 수준에서 작업 데이터와 개인 데이터가 분리됩니다. Android for Work는 작업 및 개인 애플리케이션을 명확히 구분해 줍니다. Android for Work는 고유한 Android 작업 배지를 사용하여 작업 애플리케이션을 생성합니다.

그림 8-6. Android for Work 콘텐츠



관리자는 앱에 액세스하기 위해 먼저 디바이스 관리가 필요한 카탈로그의 애플리케이션을 확인합니다. 관리가 필요한 카탈로그의 애플리케이션은 다운로드 버튼 옆에 고유한 별 모양 기호가 표시됩니다.

사용자가 이러한 애플리케이션 중 하나를 다운로드하려고 하면 관리를 받기 위해 디바이스가 필요한 애플리케이션이라는 메시지가 표시됩니다. 디바이스 관리의 기능 및 이점을 설명하는 화면이 표시됩니다.

그림 8-7. Workspace 서비스 소개 페이지

사용자가 Android for Work 관리를 사용하는 데 동의하면 관리 설정 프로세스가 안내됩니다. 디바이스가 관리된 후에는 디바이스에 Android for Work 컨테이너가 생성됩니다.

Workspace ONE 카탈로그 사용

9

Workspace ONE UEM 및 VMware Identity Manager가 통합되면 Workspace ONE 애플리케이션 카탈로그는 사용자에게 사용 권한을 부여할 수 있는 모든 리소스의 저장소입니다. 사용자는 애플리케이션에 대해 지정한 설정을 기준으로 Workspace ONE 카탈로그에서 관리하는 엔터프라이즈 애플리케이션에 액세스할 수 있습니다.

클라우드, 모바일 및 Windows 애플리케이션은 카탈로그에서 액세스할 수 있습니다. 내부적으로 개발했거나 App Store에서 공개적으로 사용할 수 있는 기본 애플리케이션을 최종 사용자가 Workspace ONE 포털에서 사용하도록 할 수 있습니다.

[Workspace ONE 카탈로그] 페이지에서는 다음과 같은 작업을 수행할 수 있습니다.

- 카탈로그에 새 리소스 추가
- 현재 사용자에게 사용 권한을 부여할 수 있는 리소스 보기
- 카탈로그에 있는 각 리소스에 대한 정보에 액세스

일부 웹 애플리케이션은 [카탈로그] 페이지에서 바로 카탈로그에 추가할 수 있습니다. 다른 리소스 유형의 경우에는 관리 콘솔 외부에서 작업을 수행해야 합니다. 리소스 설정에 대한 자세한 내용은 VMware Identity Manager 리소스 설정 가이드를 참조하십시오.

카탈로그에서 리소스 관리

사용자에게 특정 리소스에 대한 사용 권한을 부여하려면 먼저 카탈로그에 해당 리소스를 채워야 합니다. 카탈로그에 리소스를 채우는 데 사용하는 방법은 리소스 유형에 따라 달라집니다.

사용자에게 사용 권한을 부여하고 배포하기 위해 카탈로그에 정의할 수 있는 리소스의 유형은 웹 애플리케이션, VMware ThinApp 패키지로 캡처된 Windows 애플리케이션, Horizon Client 데스크톱 풀 및 Horizon 가상 애플리케이션 또는 Citrix 기반 애플리케이션입니다.

Horizon Client 데스크톱 및 애플리케이션 풀, Citrix 게시된 리소스 또는 ThinApp 패키징된 애플리케이션을 통합하고 사용하도록 설정하려면 [카탈로그] 탭 드롭다운 메뉴에서 제공되는 [가상 애플리케이션 컬렉션] 기능을 사용합니다.

이러한 리소스에 대한 정보, 요구 사항, 설치 및 구성은 VMware Identity Manager에서 리소스 설정의 내용을 참조하십시오.

조직의 카탈로그에 웹 애플리케이션 추가

클라우드 애플리케이션 카탈로그에서 선택하거나 새로 생성하여 웹 애플리케이션을 카탈로그에 추가할 수 있습니다.

클라우드 애플리케이션 카탈로그에는 일반적으로 사용되는 엔터프라이즈 웹 애플리케이션이 포함됩니다. 이러한 애플리케이션은 부분적으로 구성되어 있으며, 애플리케이션 기록을 완성하기 위한 추가 정보를 제공해야 합니다. 또한 다른 필수 설정을 완료하기 위해 웹 애플리케이션 계정 담당자와 함께 작업해야 할 수도 있습니다.

클라우드 애플리케이션 카탈로그의 많은 애플리케이션은 Workspace ONE에서 웹 애플리케이션으로의 Single Sign-On을 사용하도록 설정하기 위해 SAML 2.0 또는 1.1을 사용하여 인증 및 권한 부여 데이터를 교환합니다.

애플리케이션을 생성할 때는 애플리케이션에 대한 모든 구성 정보를 입력해야 합니다. 구성은 추가하는 애플리케이션 유형에 따라 다릅니다. 페더레이션 프로토콜이 없는 애플리케이션의 경우 대상 URL만 필요합니다.

애플리케이션을 VMware Identity Manager에서 애플리케이션 소스로 구성한 타사 ID 제공자의 애플리케이션은 새 애플리케이션으로 추가됩니다.

애플리케이션을 추가하는 동안 애플리케이션에 대한 사용자 액세스를 제어하기 위한 액세스 정책도 선택합니다. 기본 액세스 정책을 사용할 수 있으며 [ID 및 액세스 관리] > [관리] > [정책] 페이지에서 새 정책을 생성할 수도 있습니다. 액세스 정책에 대한 내용은 VMware Identity Manager 관리를 참조하십시오.

리소스를 범주로 그룹화

리소스를 논리적인 범주로 그룹화하면 사용자가 Workspace ONE 포털에서 필요한 리소스를 더 쉽게 찾을 수 있습니다.

범주를 생성할 때는 조직의 구조, 리소스의 작업 기능 및 리소스의 유형을 고려해야 합니다. 리소스에 범주를 두 개 이상 할당할 수 있습니다. 예를 들어, Sales Associate라는 범주와 Staff Sales Resources라는 범주를 생성할 수 있습니다. Sales Associate를 카탈로그의 모든 판매 리소스에 연결합니다. 또한 Staff Sales Resources를 직원 조합하고만 공유되는 특정 판매 리소스에 연결합니다.

범주를 만든 후에 해당 범주를 카탈로그의 리소스에 적용할 수 있습니다. 같은 리소스에 여러 범주를 적용할 수 있습니다.

Workspace ONE 포털에 로그인하면 해당 보기에서 사용하도록 설정한 범주가 표시됩니다.

VMware Identity Manager 관리 가이드의 "카탈로그 관리"를 참조하십시오.

VMware Identity Manager 서비스에 대한 사용자 지정 브랜딩 10

VMware Identity Manager 콘솔, 사용자 및 관리자 로그인 화면, Workspace ONE 애플리케이션 포털의 웹 보기, 모바일 디바이스에 있는 Workspace ONE 애플리케이션의 웹 보기에 나타나는 로고, 글꼴 및 배경을 사용자 지정할 수 있습니다.

사용자 지정 도구를 사용하여 회사 색상, 로고 및 디자인의 모양과 느낌을 동일하게 구성할 수 있습니다.

본 장은 다음 항목을 포함합니다.

VMware Identity Manager 서비스에서 브랜딩 사용자 지정

관리 콘솔 및 사용자 포털의 주소 표시줄에 회사 이름, 제품 이름 및 즐겨찾기를 추가할 수 있습니다. 로그인 페이지를 사용자 지정하여 회사 색상 및 로고 디자인과 일치하도록 배경색을 설정할 수도 있습니다.

절차

1 VMware Identity Manager 콘솔의 [ID 및 액세스 관리] 탭에서 **설정 > 사용자 지정 브랜딩**을 선택합니다.

2 양식의 다음 설정을 적절히 편집합니다.

양식 필드	설명
	이름 및 로고 탭
회사 이름	[회사 이름]은 데스크톱 및 모바일 디바이스 둘 다에 적용됩니다. 회사 이름을 [브라우저] 탭에 나타나는 제목으로 추가할 수 있습니다. 기존 회사 이름 위에 새 회사 이름을 입력하여 이름을 변경합니다.
제품 이름	[제품 이름]은 데스크톱 및 모바일 디바이스 둘 다에 적용됩니다. 제품 이름은 [브라우저] 탭에서 회사 이름 다음에 표시됩니다.

양식 필드	설명
Favicon	즐겨찾기 아이콘은 브라우저 주소 표시줄에 표시되는 URL과 연결된 아이콘입니다. Favicon 이미지의 최대 크기는 16 x 16픽셀입니다. 형식은 JPEG, PNG, GIF 또는 ICO가 가능합니다. **업로드**를 클릭하여 현재 Favicon을 대체하는 새 이미지를 업로드합니다. 변경 사항을 적용할지 묻는 메시지가 표시됩니다. 변경 사항이 즉시 반영됩니다.
	로그인 화면 탭
로고	**업로드**를 클릭하여 로그인 화면에서 현재 로고를 대신할 새 로고를 업로드합니다. **확인**을 클릭하면 변경 사항이 즉시 반영됩니다. 업로드에 권장되는 최소 이미지 크기는 350 x 100픽셀입니다. 350 x 100픽셀보다 큰 이미지를 업로드하면 이미지 크기가 350 x 100픽셀 크기에 맞게 조정됩니다. 형식은 JPEG, PNG 또는 GIF가 가능합니다.
배경색	로그인 화면의 배경에 표시되는 색상입니다. 배경색을 변경하려면 기존 색상 코드 위에 6자리 16진수 색상 코드를 입력합니다.
상자 배경색	로그인 화면 상자 색을 사용자 지정할 수 있습니다. 기존 색상 코드 위에 6자리 16진수 색상 코드를 입력합니다.
로그인 버튼 배경색	로그인 버튼의 색을 사용자 지정할 수 있습니다. 기존 색상 코드 위에 6자리 16진수 색상 코드를 입력합니다.
로그인 버튼 텍스트 색	로그인 버튼에 표시되는 텍스트 색을 사용자 지정할 수 있습니다. 기존 색상 코드 위에 6자리 16진수 색상 코드를 입력합니다.

로그인 화면을 사용자 지정하는 경우 변경 사항을 저장하기 전에 미리 보기 창에서 변경 사항을 확인할 수 있습니다.

3 **저장**을 클릭합니다.

VMware Identity Manager 콘솔 및 로그인 페이지에 대한 사용자 지정 브랜딩 업데이트 사항은 [저장]을 클릭한 후 5분 이내에 적용됩니다.

다음에 수행할 작업

다양한 인터페이스에서 브랜딩을 변경했을 때의 모양을 확인합니다.

최종 사용자 Workspace ONE 포털 및 모바일/태블릿 보기의 모양을 업데이트합니다. 사용자 포털에 대한 브랜딩 사용자 지정의 내용을 참조하십시오.

사용자 포털에 대한 브랜딩 사용자 지정

로고를 추가하고, 배경색을 변경하고, 이미지를 추가하여 Workspace ONE 포털을 사용자 지정할 수 있습니다.

절차

1 VMware Identity Manager 콘솔 [카탈로그] 탭에서 **설정 > 사용자 포털 브랜딩**을 선택합니다.

2 양식의 설정을 적절히 편집합니다.

양식 항목	설명
로고	마스트 헤드 로고를 VMware Identity Manager 콘솔 및 Workspace ONE 포털의 웹 페이지 상단에 표시되는 배너로 추가합니다. 이미지의 최대 크기는 220 x 40픽셀입니다. 형식은 JPEG, PNG 또는 GIF가 가능합니다.
	포털
마스트 헤드 배경색	마스트 헤드의 배경색을 변경하려면 기존 색상 코드 위에 6자리 16진수 색상 코드를 입력합니다. 새 색상 코드를 입력하면 애플리케이션 포털 미리 보기 화면에서 배경색이 변경됩니다.
마스트 헤드 텍스트 색	마스트 헤드에 표시되는 텍스트의 색을 변경하려면 기존 색상 코드 위에 6자리 16진수 색상 코드를 입력합니다.
배경색	웹 포털 화면의 배경에 표시되는 색상입니다. 배경색을 변경하려면 기존 색상 코드 위에 6자리 16진수 색상 코드를 새로 입력합니다. 새 색상 코드를 입력하면 애플리케이션 포털 미리 보기 화면에서 배경색이 변경됩니다. 배경색을 강조하려면 **배경 강조 표시**를 선택합니다. [배경 강조 표시]를 사용하도록 설정하면 여러 배경 이미지를 지원하는 브라우저가 시작 관리자 및 카탈로그 페이지에서 오버레이를 표시합니다. 배경색에 미리 디자인된 삼각형 패턴을 설정하려면 **배경 패턴**을 선택합니다.
아이콘 배경색	6자리 16진수 색 코드를 입력하여 애플리케이션 아이콘 둘레의 배경색 상자를 변경합니다.
아이콘 배경 불투명도	투명도를 설정하려면 막대에서 슬라이더를 이동합니다.
이름 및 아이콘 색	애플리케이션 포털 페이지에서 아이콘 아래에 표시되는 이름의 텍스트 색을 선택할 수 있습니다. 글꼴 색을 변경하려면 기존 색상 코드 위에 16진수 색상 코드를 입력합니다.
레터링 효과	Workspace ONE 포털 화면에 표시되는 텍스트에 사용할 레터링 유형을 선택합니다.
배경 강조 표시	사용하도록 설정되면 여러 배경 이미지를 지원하는 브라우저의 책갈피 및 카탈로그 페이지에 배경 오버레이가 표시됩니다.
배경 패턴	사용하도록 설정되면 여러 배경 이미지를 지원하는 브라우저의 책갈피 및 카탈로그 페이지에 배경 오버레이가 표시됩니다.
이미지(선택 사항)	애플리케이션 포털 화면의 배경에 색상 대신 이미지를 추가하려면 이미지를 업로드하십시오.

3 **저장**을 클릭합니다.

사용자 지정 브랜딩 업데이트는 사용자 포털에서 24시간 간격으로 새로 고쳐집니다. 변경 내용을 더 빠르게 푸시하려면 관리자 권한으로 새 탭을 열고 다음 URL을 입력합니다. myco.example.com은 사용자의 도메인 이름으로 대체합니다. https://<myco.example.com>/catalog-portal/services/api/branding?refreshCache=true

다음에 수행할 작업

다양한 인터페이스에서 브랜딩을 변경했을 때의 모양을 검토합니다.

11 다른 문서에 액세스

Workspace ONE을 설정하는 경우 VMware Identity Manager와 VMware Workspace ONE UEM 둘 다에 대한 설명서를 참조해야 할 수 있습니다.

다음 설명서 센터에서 추가 설명서를 찾을 수 있습니다.

- VMware Workspace ONE
- VMware Workspace ONE UEM
- VMware Identity Manager