사용자 관리

Virtual Desktop Service

NetApp
February 01, 2022

목차

사용자 관리

사용자 계정 관리

새 사용자 생성

관리자는 작업 영역 > 사용자 및 그룹 > 추가/가져오기를 클릭하여 사용자를 추가할 수 있습니다

사용자는 개별적으로 또는 대량 불러오기로 추가할 수 있습니다.

[너비 = 25%]

이 단계에서 정확한 이메일 및 휴대폰 번호를 포함하여 나중에 MFA를 활성화하는 프로세스를 크게 개선할 수 있습니다.

사용자를 만든 후에는 해당 이름을 클릭하여 만든 시기, 연결 상태(현재 로그인되어 있는지 여부) 및 특정 설정의 내용과 같은 세부 정보를 볼 수 있습니다.

기존 **AD** 사용자에 대해 가상 데스크톱을 활성화합니다

사용자가 AD에 이미 있는 경우 이름 옆의 톱니바퀴를 클릭한 다음 데스크톱을 활성화하여 사용자의 가상 데스크톱을 간단히 활성화할 수 있습니다.[너비 = 50%]

Azure AD 도메인 서비스 전용: 로그인이 작동하려면 Azure AD 사용자의 암호 해시를 NTLM 및 Kerberos 인증을 지원하도록 동기화해야 합니다. 이 작업을 수행하는 가장 쉬운 방법은 Office.com 또는 Azure 포털에서 사용자 암호를 변경하는 것입니다. 이렇게 하면 암호 해시 동기화가 강제로 수행됩니다. 도메인 서비스 서버의 동기화 주기는 최대 20분 정도 걸릴 수 있으므로 Azure AD의 암호 변경은 일반적으로 AADDS에 반영되는 데 20분 정도 소요되므로 VDS 환경에서 반영됩니다.

사용자 계정 삭제

사용자 정보를 편집합니다

사용자 세부 정보 페이지에서 사용자 이름 및 연락처 세부 정보와 같은 사용자 세부 정보를 변경할 수 있습니다. 이메일 및 전화 값은 셀프 서비스 암호 재설정(SSPR) 프로세스에 사용됩니다.

[]

사용자 보안 설정을 편집합니다

- VDI 사용자 설정 – 활성화된 경우 전용 VM 세션 호스트를 구축하고 이 사용자를 해당 호스트에 연결하는 유일한 사용자로 할당하는 RDS 설정입니다. 이 확인란을 활성화할 때 CWMS 관리자에게 VM 이미지, 크기 및 스토리지 유형을 선택하라는 메시지가 표시됩니다.
  - Avd VDI 사용자는 AVD 페이지에서 VDI 호스트 풀로 관리해야 합니다.
- 계정 만료 활성화 – CWMS 관리자가 최종 사용자 계정에 만료 날짜를 설정할 수 있습니다.
- 다음 로그인 시 암호 재설정 강제 적용 - 최종 사용자가 다음 로그인 시 암호를 변경하도록 요청합니다.

- 다단계 인증 사용 – 최종 사용자에 대해 MFA를 활성화하고 다음 로그인 시 MFA를 설정하라는 메시지를 표시합니다.
- 모바일 드라이브 사용 - RDS 또는 AVD의 현재 배포에서 사용되지 않는 레거시 기능입니다.
- 로컬 드라이브 액세스 사용 – 최종 사용자가 복사/붙여넣기, USB 대용량 저장 장치 및 시스템 드라이브를 비롯한 클라우드 환경에서 로컬 장치 저장소에 액세스할 수 있습니다.
- 필요할 때 깨우기 활성화 – Windows용 CW 클라이언트를 통해 연결하는 RDS 사용자의 경우, 이 기능을 활성화하면 워크로드 일정에 정의된 정규 근무 시간 이외의 시간에 연결할 때 최종 사용자가 자신의 환경을 사용할 수 있습니다.

잠긴 계정

기본적으로 5번의 로그인 시도가 실패하면 사용자 계정이 잠깁니다. Enable Password Complexity _ (암호 복잡성 활성화)가 활성화되지 않은 경우 30분 후에 사용자 계정의 잠금이 해제됩니다. 암호 복잡성이 활성화된 경우 계정이 자동으로 잠금 해제되지 않습니다. 두 경우 모두 VDS 관리자는 VDS의 사용자/그룹 페이지에서 사용자 계정을 수동으로 잠금 해제할 수 있습니다.

사용자 암호를 재설정합니다

사용자 암호를 재설정합니다.

참고: Azure AD 사용자 암호를 재설정(또는 계정 잠금 해제)할 때 Azure AD를 통해 초기화가 전파될 때 최대 20분이 지연될 수 있습니다.

관리자 액세스

이 설정을 사용하면 최종 사용자가 테넌트의 관리 포털에 액세스할 수 없습니다. 일반적인 용도로는 동료의 암호를 재설정하거나 응용 프로그램을 할당하거나 수동 서버 웨이크업 액세스를 허용하는 현장 직원 액세스를 제공하는 것이 있습니다. 콘솔 영역을 제어하는 권한도 여기서 설정할 수 있습니다.

사용자 로그오프

로그인한 사용자는 VDS의 사용자/그룹 페이지에서 VDS 관리자가 로그오프할 수 있습니다.

응용 프로그램

이 작업 영역에 배포된 응용 프로그램을 표시합니다. 이 확인란은 앱을 이 특정 사용자에게 프로비저닝합니다. 전체 응용 프로그램 관리 설명서는 여기에서 찾을 수 있습니다. 응용 프로그램에 대한 액세스는 응용 프로그램 인터페이스 또는 보안 그룹에서도 부여할 수 있습니다.

사용자 프로세스를 보거나 종료합니다

해당 사용자의 세션에서 현재 실행 중인 프로세스를 표시합니다. 이 인터페이스로도 프로세스를 종료할 수 있습니다.

데이터 권한 관리

최종 사용자 관점

가상 데스크톱 최종 사용자는 여러 매핑된 드라이브에 액세스할 수 있습니다. 이러한 드라이브에는 FTPS에서 액세스할

수 있는 팀 공유, 회사 파일 공유 및 홈 드라이브(문서, 데스크톱 등)가 포함됩니다. . 매핑된 모든 드라이브는 스토리지 서비스(예: Azure NetApp Files) 또는 파일 서버 VM의 중앙 스토리지 계층으로 다시 참조됩니다.

구성에 따라 H: 또는 F: 드라이브가 노출되지 않을 수 있습니다. 데스크탑, 문서 등만 볼 수 있습니다. 폴더. 또한 구축 시 VDS 관리자가 다른 드라이브 문자를 설정하는 경우도 있습니다.[]

[]

권한 관리

VDS를 사용하면 관리자가 VDS 포털 내에서 보안 그룹 및 폴더 권한을 편집할 수 있습니다.

보안 그룹

보안 그룹은 그룹 섹션 아래에서 작업 공간 > 테넌트 이름 > 사용자 및 그룹 > 을 클릭하여 관리합니다

이 섹션에서는 다음을 수행할 수 있습니다.

1. 새 보안 그룹을 생성합니다
2. 그룹에 사용자를 추가/제거합니다
3. 그룹에 응용 프로그램을 할당합니다
4. 그룹에 대한 로컬 드라이브 액세스를 활성화/비활성화합니다

[]

폴더 권한

폴더 권한은 폴더 섹션에서 작업 공간 > 테넌트 이름 > 관리 를 클릭하여 관리합니다.

이 섹션에서는 다음을 수행할 수 있습니다.

1. 폴더 추가/삭제
2. 사용자 또는 그룹에 권한을 할당합니다
3. 읽기 전용, 모든 권한 및 없음에 대한 권한을 사용자 지정합니다

[]

응용 프로그램 소유 권한

개요

VDS에는 강력한 응용 프로그램 자동화 및 사용 권한 기능이 내장되어 있습니다. 이 기능을 통해 사용자는 동일한 세션 호스트에 연결하는 동안 다른 애플리케이션에 액세스할 수 있습니다. 이 작업은 일부 사용자 지정 GPO에서 단축키를 숨기고 사용자 데스크톱에 선택적으로 바로 가기를 배치하는 자동화와 함께 수행됩니다.

이 워크플로는 RDS 배포에만 적용됩니다. AVD 응용 프로그램 자격 설명서는 를 참조하십시오 "AVD에 대한 애플리케이션 사용 권한 워크플로"

응용 프로그램은 직접 사용자에게 할당하거나 VDS에서 관리되는 보안 그룹을 통해 할당할 수 있습니다.

애플리케이션 프로비저닝 프로세스는 높은 수준에서 다음 단계를 따릅니다.

1. App Catalog에 앱을 추가합니다
2. 작업 영역에 앱을 추가합니다
3. 모든 세션 호스트에 애플리케이션을 설치합니다
4. 바로 가기 경로를 선택합니다
5. 사용자 및/또는 그룹에 앱을 할당합니다

3 및 4단계는 아래 그림과 같이 스크립트된 이벤트를 사용하여 완전히 자동화할 수 있습니다

비디오 연습

응용 프로그램을 App Catalog에 추가합니다

VDS Application Entitlement는 App Catalog(앱 카탈로그)로 시작합니다. 이 목록은 최종 사용자 환경에 배포할 수 있는 모든 응용 프로그램 목록입니다.

카탈로그에 응용 프로그램을 추가하려면 다음 단계를 수행하십시오

1. 에서 VDS에 로그인합니다 https://manage.cloudworkspace.com 기본 관리자 자격 증명을 사용합니다.
2. 오른쪽 상단에서 사용자 이름 옆에 있는 화살표 아이콘을 클릭하고 설정 을 선택합니다.
3. 앱 카탈로그 탭을 클릭합니다.
4. 애플리케이션 카탈로그 제목 표시줄에서 앱 추가 옵션을 클릭합니다.
5. 응용 프로그램 그룹을 추가하려면 응용 프로그램 가져오기 옵션을 선택합니다.
    a. 응용 프로그램 목록에 맞는 형식을 만드는 Excel 서식 파일을 제공하는 대화 상자가 나타납니다.
    b. 이 평가의 경우 NetApp VDS에서 가져오기를 위한 샘플 응용 프로그램 목록을 만들었습니다. 이 목록은 여기

에서 찾을 수 있습니다.

c. 업로드 영역을 클릭하고 응용 프로그램 템플릿 파일을 선택한 다음 가져오기 단추를 클릭합니다.

6. 개별 애플리케이션을 추가하려면 앱 추가 버튼을 선택하면 대화 상자가 나타납니다.

a. 응용 프로그램의 이름을 입력합니다.

b. 외부 ID를 사용하여 제품 SKU 또는 청구 추적 코드(선택 사항)와 같은 내부 추적 식별자를 입력할 수 있습니다.

c. 응용 프로그램에 구독 제품으로 보고하려면 구독 상자를 선택합니다(선택 사항).

d. 제품이 버전(예: Chrome)별로 설치되지 않는 경우 버전 필요 없음 확인란을 선택합니다. 이를 통해 "지속적인 업데이트" 제품을 해당 버전을 추적하지 않고 설치할 수 있습니다.

e. 반대로, 제품이 여러 개의 명명된 버전(예: Quickbooks)을 지원하는 경우, 여러 버전을 설치할 수 있고 최종 사용자에게 권한을 부여할 수 있는 응용 프로그램 목록에서 사용 가능한 VDS 특정 버전을 가질 수 있도록 이 확인란을 선택해야 합니다.

f. VDS가 이 제품에 대해 바탕 화면 아이콘을 제공하지 않도록 하려면 “No User Desktop(사용자 바탕 화면 없음) 아이콘”을 선택합니다. 이 기능은 최종 사용자가 액세스할 수 있는 애플리케이션이 없으므로 SQL Server와 같은 "백엔드" 제품에 사용됩니다.

g. "앱이 연결되어 있어야 함"은 연결된 앱을 설치해야 하는 필요성을 적용합니다. 예를 들어, 클라이언트 서버 응용 프로그램에 SQL Server 또는 MySQL도 설치해야 할 수 있습니다.

h. 라이센스 필요 상자를 선택하면 VDS가 응용 프로그램 상태를 활성으로 설정하기 전에 이 응용 프로그램 설치를 위해 라이센스 파일을 업로드하도록 요청해야 함을 나타냅니다. 이 단계는 VDS의 응용 프로그램 세부 정보 페이지에서 수행됩니다.

i. 모두에게 표시 – 애플리케이션 권한은 다중 채널 계층 구조의 특정 하위 파트너로 제한될 수 있습니다. 평가를 위해 모든 사용자가 사용 가능한 응용 프로그램 목록에서 볼 수 있도록 확인란을 클릭합니다.

Workspace에 응용 프로그램을 추가합니다

배포 프로세스를 시작하려면 앱을 작업 영역에 추가합니다.

이렇게 하려면 다음 단계를 수행하십시오

1. 작업 영역을 클릭합니다
2. 앱 으로 스크롤합니다
3. 추가 를 클릭합니다
4. 응용 프로그램 확인란을 선택하고 필수 정보를 입력한 다음 응용 프로그램 추가를 클릭하고 응용 프로그램 추가를 클릭합니다.

응용 프로그램을 수동으로 설치합니다

애플리케이션이 Workspace에 추가되면 모든 세션 호스트에 해당 애플리케이션을 설치해야 합니다. 이 작업은 수동으로 수행하거나 자동화할 수 있습니다.

세션 호스트에 애플리케이션을 수동으로 설치하려면 다음 단계를 수행하십시오

1. 서비스 보드로 이동합니다.
2. 서비스 보드 작업을 클릭합니다.
3. 로컬 관리자로 연결할 서버 이름을 클릭합니다.

4. 앱을 설치하고 시작 메뉴 경로에 이 앱의 바로 가기가 있는지 확인합니다.
    a. Server 2016 및 Windows 10:C:\ProgramData\Microsoft\Windows\Start Menu\Programs의 경우
5. 서비스 보드 작업으로 돌아가서 찾아보기 를 클릭하고 바로 가기 또는 바로 가기가 포함된 폴더를 선택합니다.
6. 어떤 것을 선택하든 앱이 할당되면 최종 사용자 데스크톱에 표시됩니다.
7. 폴더는 앱이 실제로 여러 응용 프로그램일 때 유용합니다. 예를 들어, "Microsoft Office"는 각 응용 프로그램을 폴더 안에 바로 가기로 사용하여 폴더로 배포하는 것이 더 쉽습니다.
8. 설치 완료 를 클릭합니다.
9. 필요한 경우, 생성된 아이콘 서비스 보드 작업 추가 를 열고 아이콘이 추가되었는지 확인합니다.

사용자에게 응용 프로그램을 할당합니다

응용 프로그램 사용 권한은 VDS에서 처리되며 응용 프로그램은 세 가지 방법으로 사용자에게 할당할 수 있습니다

사용자에게 응용 프로그램을 할당합니다

1. 사용자 세부 정보 페이지로 이동합니다.
2. 응용 프로그램 섹션으로 이동합니다.
3. 이 사용자에게 필요한 모든 응용 프로그램 옆에 있는 확인란을 선택합니다.

응용 프로그램에 사용자를 할당합니다

1. 작업 영역 세부 정보 페이지의 응용 프로그램 섹션으로 이동합니다.
2. 응용 프로그램의 이름을 클릭합니다.
3. 응용 프로그램을 사용하는 사용자 옆에 있는 확인란을 선택합니다.

사용자 그룹에 응용 프로그램 및 사용자를 할당합니다

1. 사용자 및 그룹 세부 정보로 이동합니다.
2. 새 그룹을 추가하거나 기존 그룹을 편집합니다.
3. 사용자 및 응용 프로그램을 그룹에 할당합니다.

사용자 암호를 재설정합니다

사용자 암호 단계를 재설정합니다

1. VDS에서 사용된 세부 정보 페이지로 이동합니다

    []

2. 암호 섹션을 찾아 새 PW를 두 번 입력한 다음 을 클릭합니다

    []

    []

효력 발휘를 위한 시간

- 환경에서 VM에서 "내부" AD를 실행하는 환경의 경우 암호 변경 사항이 즉시 적용됩니다.
- AADDS(Azure AD Domain Services)를 실행하는 환경의 경우 암호 변경 내용이 적용되는 데 약 20분이 걸립니다.
- AD 유형은 배포 세부 정보 페이지에서 확인할 수 있습니다.

  []

셀프 서비스 암호 재설정**(SSRP)**

NetApp VDS Windows 클라이언트 및 NetApp VDS 웹 클라이언트는 v5.2 이상 가상 데스크톱 배포에 로그인할 때 잘못된 암호를 입력하라는 메시지를 표시합니다. 사용자가 계정을 잠근 경우 이 프로세스는 사용자 계정도 잠금 해제합니다.

참고: 이 프로세스를 사용하려면 사용자가 휴대폰 번호 또는 이메일 주소를 이미 입력해야 합니다.

SSPR은 다음과 같이 지원됩니다.

- NetApp VDS 창 클라이언트
- NetApp VDS 웹 클라이언트

이 지침에서는 사용자가 자신의 암호를 재설정하고 계정의 잠금을 해제할 수 있도록 간단한 방법으로 SSPR을 사용하는 프로세스를 안내합니다.

NetApp VDS Windows 클라이언트

1. 최종 사용자인 경우 암호 분실 링크를 클릭하여 계속합니다.

   []

2. 휴대 전화나 이메일을 통해 코드를 수신할지 여부를 선택합니다.

   []

3. 최종 사용자가 이러한 연결 방법 중 하나만 제공한 경우 이 방법이 유일한 방법으로 표시됩니다.

   []

4. 이 단계를 마치면 모바일 장치 또는 받은 편지함에 수신되는 숫자 값을 입력할 수 있는 코드 필드가 표시됩니다 (선택한 값에 따라 다름). 해당 코드 다음에 새 암호를 입력하고 Reset(재설정) 을 클릭하여 계속 진행합니다.

   []

5. 암호 재설정이 성공적으로 완료되었음을 알리는 메시지가 표시됩니다. 완료 를 클릭하여 로그온 프로세스를 완료합니다.

배포 시 Azure Active Directory 도메인 서비스를 사용하는 경우 20분마다 Microsoft에서 정의한 암호 동기화 기간이 있습니다. 다시 한 번 말하지만 Microsoft에서 제어하므로 변경할 수 없습니다. 이를 염두에 두고 VDS는 사용자가 새 암호가 적용될 때까지 최대 20분 동안 기다려야 한다고 표시합니다. 배포를 Azure Active Directory 도메인 서비스를 사용하지 않는 경우 몇 초 내에 다시 로그인할 수 있습니다.

[]

HTML5 포털

1. HTML5를 통해 로그인할 때 올바른 암호를 입력하지 못하면 암호를 재설정할 수 있는 옵션이 표시됩니다.

   []

2. 비밀번호를 재설정하는 옵션을 클릭하면 재설정 옵션이 표시됩니다.

   []

3. '요청' 버튼을 누르면 생성된 코드가 선택한 옵션(이 경우 사용자의 이메일)으로 전송됩니다. 이 코드는 15분 동안 유효합니다.

   []

4. 암호가 재설정되었습니다! Windows Active Directory는 변경 내용을 전파하는 데 시간이 필요한 경우가 많으므로 새 암호가 즉시 작동하지 않을 경우 몇 분 정도 기다렸다가 다시 시도하십시오. 이 기능은 특히 Azure Active Directory 도메인 서비스 배포 시 암호 재설정이 전파되는 데 최대 20분이 걸릴 수 있는 사용자와 관련이 있습니다.

   []

사용자에 대한 셀프 서비스 암호 재설정**(SSPR)** 활성화

SSPR(Self Service Password Reset)을 사용하려면 관리자가 먼저 휴대폰 번호 및/또는 최종 사용자의 이메일 계정을 입력해야 합니다. 가상 데스크톱 사용자의 휴대폰 번호와 이메일 주소를 입력하는 방법은 아래와 같습니다.

이 명령 집합에서 최종 사용자가 암호를 다시 설정할 수 있는 간단한 방법으로 SSPR을 구성하는 과정을 안내합니다.

VDS를 통해 사용자를 대량으로 가져옵니다

작업 영역 모듈로 이동한 다음 사용자 및 그룹, 추가/가져오기 를 차례로 클릭하여 시작합니다.

이러한 값을 하나씩 만들 때 사용자에 대해 다음 값을 입력할 수 있습니다.[]

또는 대량 가져오기 사용자가 미리 구성된 Excel XLSX 파일을 다운로드하여 업로드할 때 다음 내용을 포함할 수 있습니다.[]

VDS API를 통해 데이터 제공

NetApp VDS API – 특히 이 호출입니다 https://api.cloudworkspace.com/5.4/swagger/ui/index#!/User/User_PutUser – 이 정보를 업데이트할 수 있습니다.

기존 사용자 전화를 업데이트하는 중입니다

VDS의 사용자 세부 정보 개요 페이지에서 사용자의 전화 번호를 업데이트합니다.

[]

다른 콘솔 사용

참고: 현재 Azure Console, Partner Center 또는 Office 365 관리 콘솔을 통해 사용자의 전화 번호를 제공할 수 없습니다.

SSPR 전송 주소를 사용자 지정합니다

NetApp VDS는 사용자 정의 주소에서 _from_확인 이메일을 보내도록 구성할 수 있습니다. 이 서비스는 최종 사용자가 자신의 사용자 지정 이메일 도메인에서 보내는 재설정 암호 이메일을 수신하기를 원하는 서비스 공급자 파트너에게 제공됩니다.

이 사용자 지정에는 전송 주소를 확인하는 몇 가지 추가 단계가 필요합니다. 이 프로세스를 시작하려면 사용자 지정 "셀프 서비스 암호 재설정 소스 주소"를 요청하는 VDS 지원 지원 지원 케이스를 여십시오. 다음을 정의하십시오.

- 파트너 코드(오른쪽 상단 아래쪽 화살표 메뉴에서 _settings_를 클릭하여 찾을 수 있습니다. 아래 스크린샷 참조)

  []

- 원하는 "보낸 사람" 주소(유효해야 함)
- 설정을 적용해야 하는 클라이언트(또는 모두)

지원 케이스 열기에 대한 자세한 내용은 VDSsupport@netapp.com 으로 이메일을 보내주십시오

VDS 지원을 받으면 SMTP 서비스로 주소를 검증하고 이 설정을 활성화합니다. 원본 주소 도메인의 공용 DNS 레코드를 업데이트하여 전자 메일 전송 기능을 최대화하는 것이 가장 좋습니다.

비밀번호 복잡성

VDS는 암호 복잡성을 강제로 적용할 수 있도록 구성할 수 있습니다. 이 설정은 클라우드 작업 영역 설정 섹션의 작업 영역 세부 정보 페이지에 있습니다.

[]

[]

암호 복잡성**:** 끄기

정책	지침
최소 암호 길이	8자
최대 암호 사용 기간	110일
최소 암호 사용 기간	0일
암호 기록 적용	24개의 암호가 기억되었습니다
암호 잠금	5개의 잘못된 입력 후에 자동으로 잠금이 발생합니다

정책	지침
기간 잠금	30분

암호 복잡성: 켬

정책	지침
최소 암호 길이	8자에는 사용자의 계정 이름 또는 사용자 전체 이름의 일부가 포함되어 있지 않으며, 이 이름은 다음 네 가지 범주 중 세 가지 문자를 연속으로 포함합니다. 영어 대문자(A ~ Z) 영어 소문자(a ~ z) 기본 10자리(0 ~ 9) 알파벳이 아닌 문자(예:!, $, #, %) 복잡성 요구 사항은 암호를 변경하거나 생성할 때 적용됩니다.
최대 암호 사용 기간	110일
최소 암호 사용 기간	0일
암호 기록 적용	24개의 암호가 기억되었습니다
암호 잠금	5개의 잘못된 입력 후에 자동으로 잠깁니다
기간 잠금	관리자가 잠금을 해제할 때까지 잠금 상태를 유지합니다

멀티팩터 인증(MFA)

개요

NetApp VDS(가상 데스크톱 서비스)에는 추가 비용 없이 SMS/이메일 기반 MFA 서비스가 포함됩니다. 이 서비스는 다른 서비스(예 Azure Conditional Access)를 사용하여 VDS에 대한 관리자 로그인과 가상 데스크톱에 대한 사용자 로그인을 보호할 수 있습니다.

MFA 기본 사항

- VDS MFA는 admin 사용자, 개별 최종 사용자에게 할당하거나 모든 최종 사용자에게 적용할 수 있습니다
- VDS MFA는 SMS 또는 이메일 알림을 보낼 수 있습니다
- VDS MFA는 셀프 서비스 초기 설정 및 재설정 기능을 제공합니다

가이드 범위

이 가이드에서는 최종 사용자 환경 그림과 함께 MFA 설정을 안내합니다

본 가이드에서는 다음 주제를 다룹니다.

1. 개별 사용자를 위한 MFA 활성화
2. 모든 사용자에 대해 MFA 필요
3. 개별 관리자를 위한 MFA 활성화
4. 최종 사용자 초기 설정

개별 사용자를 위한 MFA 활성화

MFA는 사용자 세부 정보 페이지의 개별 사용자에 대해 _다단계 인증 사용_을 클릭하여 활성화할 수 있습니다

작업 공간 > 작업 공간 이름 > 사용자 및 그룹 > 사용자 이름 > 다중 요소 인증 사용 > 업데이트 를 선택합니다

또한 MFA는 모든 사용자에게 할당될 수 있습니다. 이 설정이 있는 경우 확인란이 선택되며 _ (클라이언트 설정을 통해) _ 이(가) 확인란 레이블에 추가됩니다.

모든 사용자에게 **MFA** 필요

MFA는 모든 사용자에 대해 _MFA 를 클릭하여 작업 영역 세부 정보 페이지의 모든 사용자에게 설정 및 적용할 수 있습니다

작업 영역 > 작업 영역 이름 > 모든 사용자에 대한 MFA 설정 > 업데이트 를 클릭합니다

개별 관리자를 위한 **MFA** 활성화

MFA는 VDS 포털에 액세스하는 관리자 계정에서도 사용할 수 있습니다. 이 기능은 관리자 세부 정보 페이지에서 관리자별로 활성화할 수 있습니다. 관리자 > 관리자 이름 > 다중 요소 인증 필요 > 업데이트

초기 설정

MFA를 활성화한 후 처음 로그인하면 사용자 또는 관리자에게 이메일 주소 또는 휴대폰 번호를 입력하라는 메시지가 표시됩니다. 등록 성공 여부를 입력하고 확인할 수 있는 확인 코드를 받게 됩니다.