멀티팩터 인증(MFA)

SnapCenter Software 5.0

NetApp
April 04, 2024

목차

멀티팩터 인증(MFA)

멀티팩터 인증(MFA) 관리

AD FS(Active Directory Federation Service) 서버 및 SnapCenter 서버에서 MFA(Multi-Factor Authentication) 기능을 관리할 수 있습니다.

멀티팩터 인증(MFA) 활성화

PowerShell 명령을 사용하여 SnapCenter Server에 MFA 기능을 사용하도록 설정할 수 있습니다.

이 작업에 대해

- SnapCenter는 다른 애플리케이션이 동일한 AD FS에 구성되어 있을 때 SSO 기반 로그인을 지원합니다. 특정 AD FS 구성에서 SnapCenter는 AD FS 세션 지속성에 따라 보안상의 이유로 사용자 인증을 요구할 수 있습니다.
- cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 를 실행하여 얻을 수 있습니다 `Get-Help command_name`. 또는 를 볼 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

시작하기 전에

- Windows AD FS(Active Directory Federation Service)가 해당 도메인에서 실행 중이어야 합니다.
- Azure MFA, Cisco Duo 등과 같은 AD FS 지원 다중 요소 인증 서비스가 있어야 합니다.
- SnapCenter 및 AD FS 서버 타임 스탬프는 시간대와 상관없이 동일해야 합니다.
- SnapCenter 서버에 대해 승인된 CA 인증서를 조달하고 구성합니다.

  CA 인증서는 다음과 같은 이유로 필수입니다.

  - 자체 서명된 인증서가 노드 수준에서 고유하므로 ADFS-F5 통신이 끊어지지 않도록 합니다.
  - 독립 실행형 또는 고가용성 구성에서 업그레이드, 복구 또는 재해 복구(DR) 중에 자체 서명된 인증서가 다시 만들어지지 않으므로 MFA 재구성이 방지됩니다.
  - IP-FQDN 해상도를 확인합니다.

    CA 인증서에 대한 자세한 내용은 을 참조하십시오 "CA 인증서 CSR 파일을 생성합니다".

단계

1. AD FS(Active Directory Federation Services) 호스트에 연결합니다.
2. 에서 AD FS 페더레이션 메타데이터 파일을 다운로드합니다 "https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml".
3. 다운로드한 파일을 SnapCenter 서버에 복사하여 MFA 기능을 활성화합니다.
4. PowerShell을 통해 SnapCenter 관리자로 SnapCenter 서버에 로그인합니다.
5. PowerShell 세션을 사용하여 _New-SmMultactorAuthenticationMetadata-path_cmdlet을 사용하여 SnapCenter MFA 메타데이터 파일을 생성합니다.

   path 매개 변수는 SnapCenter 서버 호스트에 MFA 메타데이터 파일을 저장할 경로를 지정합니다.

6. 생성된 파일을 AD FS 호스트에 복사하여 SnapCenter를 클라이언트 엔터티로 구성합니다.
7. 를 사용하여 SnapCenter 서버에 대해 MFA를 활성화합니다 `Set-SmMultiFactorAuthentication` cmdlet.
8. (선택 사항) 를 사용하여 MFA 구성 상태 및 설정을 확인합니다 `Get-SmMultiFactorAuthentication` cmdlet.
9. MMC(Microsoft Management Console)로 이동하여 다음 단계를 수행하십시오.
   a. 파일 * > * Snapin 추가/제거 * 를 클릭합니다.
   b. 스냅인 추가/제거 창에서 * 인증서 * 를 선택한 다음 * 추가 * 를 클릭합니다.
   c. 인증서 스냅인 창에서 * 컴퓨터 계정 * 옵션을 선택한 다음 * 마침 * 을 클릭합니다.
   d. 콘솔 루트 * > * 인증서 – 로컬 컴퓨터 * > * 개인 * > * 인증서 * 를 클릭합니다.
   e. SnapCenter에 바인딩된 CA 인증서를 마우스 오른쪽 단추로 클릭한 다음 * 모든 작업 * > * 개인 키 관리 * 를 선택합니다.
   f. 권한 마법사에서 다음 단계를 수행합니다.
      i. 추가 * 를 클릭합니다.
      ii. Locations * 를 클릭하고 관련 호스트(계층 구조의 맨 위)를 선택합니다.
      iii. Locations * (위치 *) 팝업 창에서 * OK * (확인 *)를 클릭합니다.
      iv. 개체 이름 필드에 'IIS_IUSRS'를 입력하고 * 이름 확인 * 을 클릭한 다음 * 확인 * 을 클릭합니다.

      검사가 성공적으로 완료되면 * OK * 를 클릭합니다.
10. AD FS 호스트에서 AD FS 관리 마법사를 열고 다음 단계를 수행합니다.
   a. '신뢰할 수 있는 당사자'를 마우스 오른쪽 버튼으로 클릭 * > * '신뢰할 수 있는 당사자 신뢰 추가' * > * 시작 * 을 클릭합니다.
   b. 두 번째 옵션을 선택하고 SnapCenter MFA 메타데이터 파일을 찾은 후 * 다음 * 을 클릭합니다.
   c. 표시 이름을 지정하고 * 다음 * 을 클릭합니다.
   d. 필요에 따라 액세스 제어 정책을 선택하고 * 다음 * 을 클릭합니다.
   e. 다음 탭에서 기본 설정으로 설정을 선택합니다.
   f. 마침 * 을 클릭합니다.

   SnapCenter는 이제 제공된 표시 이름을 가진 의존자로 반영됩니다.
11. 이름을 선택하고 다음 단계를 수행하십시오.
   a. 청구 발급 정책 편집 * 을 클릭합니다.
   b. 규칙 추가 * 를 클릭하고 * 다음 * 을 클릭합니다.
   c. 청구 규칙의 이름을 지정합니다.
   d. 속성 저장소로 * Active Directory * 를 선택합니다.
   e. 속성을 * User-Principal-Name * 으로 선택하고 발신 클레임 유형을 * Name-ID * 로 선택합니다.
   f. 마침 * 을 클릭합니다.
12. ADFS 서버에서 다음 PowerShell 명령을 실행합니다.

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'
-SigningCertificateRevocationCheck None

Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'
-EncryptionCertificateRevocationCheck None
```

13. 메타데이터를 성공적으로 가져왔는지 확인하려면 다음 단계를 수행하십시오.
    a. 신뢰할 수 있는 상대 신뢰를 마우스 오른쪽 단추로 클릭하고 * 속성 * 을 선택합니다.
    b. 끝점, 식별자 및 서명 필드가 채워져 있는지 확인합니다.
14. 모든 브라우저 탭을 닫고 브라우저를 다시 열어 기존 또는 활성 세션 쿠키를 지우고 다시 로그인합니다.

SnapCenter MFA 기능은 REST API를 사용하여 활성화할 수도 있습니다.

문제 해결에 대한 자세한 내용은 을 참조하십시오 "여러 탭에서 동시 로그인 시도 시 MFA 오류가 표시됩니다".

AD FS MFA 메타데이터를 업데이트합니다

AD FS 서버에 업그레이드, CA 인증서 갱신, DR 등과 같은 수정 사항이 있을 때마다 SnapCenter에서 AD FS MFA 메타데이터를 업데이트해야 합니다.

단계

1. 에서 AD FS 페더레이션 메타데이터 파일을 다운로드합니다 "https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml"
2. 다운로드한 파일을 SnapCenter 서버에 복사하여 MFA 구성을 업데이트합니다.
3. 다음 cmdlet을 실행하여 SnapCenter에서 AD FS 메타데이터를 업데이트합니다.

```
Set-SmMultiFactorAuthentication -Path <location of ADFS MFA metadata xml file>
```

4. 모든 브라우저 탭을 닫고 브라우저를 다시 열어 기존 또는 활성 세션 쿠키를 지우고 다시 로그인합니다.

SnapCenter MFA 메타데이터를 업데이트합니다

복구, CA 인증서 갱신, DR 등과 같은 ADFS 서버에 수정 사항이 있을 때마다 AD FS에서 SnapCenter MFA 메타데이터를 업데이트해야 합니다.

단계

1. AD FS 호스트에서 AD FS 관리 마법사를 열고 다음 단계를 수행합니다.
    a. 사용 당사자 신뢰 * 를 클릭합니다.
    b. SnapCenter에 대해 만든 기반 당사자 신뢰를 마우스 오른쪽 단추로 클릭하고 * 삭제 * 를 클릭합니다.

       신뢰할 수 있는 사용자의 사용자 정의 이름이 표시됩니다.

    c. MFA(Multi-factor Authentication)를 활성화합니다.

       을 참조하십시오 "다중 요소 인증을 활성화합니다".
2. 모든 브라우저 탭을 닫고 브라우저를 다시 열어 기존 또는 활성 세션 쿠키를 지우고 다시 로그인합니다.

MFA(Multi-Factor Authentication) 비활성화

단계

1. MFA를 비활성화하고 를 사용하여 MFA를 활성화했을 때 생성된 구성 파일을 정리합니다 `Set-SmMultiFactorAuthentication` cmdlet.
2. 모든 브라우저 탭을 닫고 브라우저를 다시 열어 기존 또는 활성 세션 쿠키를 지우고 다시 로그인합니다.

REST API, PowerShell 및 SCCLI를 사용하여 MFA(Multi-Factor Authentication)를 관리합니다

MFA 로그인은 브라우저, REST API, PowerShell 및 SCCLI에서 지원됩니다. MFA는 AD FS ID 관리자를 통해 지원됩니다. GUI, REST API, PowerShell 및 SCCLI에서 MFA를 사용하도록 설정하고 MFA를 사용하지 않도록 설정하고 MFA를 구성할 수 있습니다.

AD FS를 OAuth/OIDC로 설정합니다

- Windows GUI 마법사를 사용하여 AD FS 구성 *
  1. 서버 관리자 대시보드 * > * 도구 * > * ADFS 관리 * 로 이동합니다.
  2. ADFS * > * 응용 프로그램 그룹 * 으로 이동합니다.
     a. 응용 프로그램 그룹 * 을 마우스 오른쪽 단추로 클릭합니다.
     b. 응용 프로그램 그룹 추가 * 를 선택하고 * 응용 프로그램 이름 * 을 입력합니다.
     c. 서버 응용 프로그램 * 을 선택합니다.
     d. 다음 * 을 클릭합니다.
  3. 복사 * 클라이언트 식별자 *.

     클라이언트 ID입니다. … 리디렉션 URL에 콜백 URL(SnapCenter 서버 URL)을 추가합니다. … 다음 * 을 클릭합니다.

  4. 공유 암호 생성 * 을 선택합니다.

     암호 값을 복사합니다. 클라이언트의 비밀입니다. … 다음 * 을 클릭합니다.

  5. 요약 * 페이지에서 * 다음 * 을 클릭합니다.
     a. 완료 * 페이지에서 * 닫기 * 를 클릭합니다.
  6. 새로 추가된 * 응용 프로그램 그룹 * 을 마우스 오른쪽 단추로 클릭하고 * 속성 * 을 선택합니다.
  7. 앱 속성에서 * 응용 프로그램 추가 * 를 선택합니다.
  8. 응용 프로그램 추가 * 를 클릭합니다.

     웹 API를 선택하고 * 다음 * 을 클릭합니다.

  9. 웹 API 구성 페이지에서 이전 단계에서 만든 SnapCenter 서버 URL 및 클라이언트 식별자를 식별자 섹션에 입력합니다.
     a. 추가 * 를 클릭합니다.

b. 다음 * 을 클릭합니다.

10. 액세스 제어 정책 선택 * 페이지에서 요구 사항에 따라 제어 정책(예: 모든 사용자 허용 및 MFA 필요)을 선택하고 * 다음 * 을 클릭합니다.
11. 응용 프로그램 권한 구성 * 페이지에서 기본적으로 OpenID가 범위로 선택되어 있으면 * 다음 * 을 클릭합니다.
12. 요약 * 페이지에서 * 다음 * 을 클릭합니다.

    완료 * 페이지에서 * 닫기 * 를 클릭합니다.

13. 샘플 응용 프로그램 속성 * 페이지에서 * 확인 * 을 클릭합니다.
14. 인증 서버(AD FS)에서 발급하고 리소스에서 사용하도록 의도된 JWT 토큰입니다.

    이 토큰의 'AUD' 또는 청중의 주장은 리소스 또는 웹 API의 식별자와 일치해야 합니다.

15. 선택한 WebAPI를 편집하고 콜백 URL(SnapCenter 서버 URL)과 클라이언트 식별자가 올바르게 추가되었는지 확인합니다.

    OpenID Connect를 구성하여 사용자 이름을 클레임으로 제공합니다.

16. 서버 관리자 오른쪽 상단의 * 도구 * 메뉴 아래에 있는 * AD FS 관리 * 도구를 엽니다.
    a. 왼쪽 사이드바에서 * Application Groups * 폴더를 선택합니다.
    b. 웹 API를 선택하고 * edit * 를 클릭합니다.
    c. 발행 변환 규칙 탭으로 이동합니다
17. 규칙 추가 * 를 클릭합니다.
    a. 클레임 규칙 템플릿 드롭다운에서 * 청구로 LDAP 속성 보내기 * 를 선택합니다.
    b. 다음 * 을 클릭합니다.
18. 청구 규칙 * 이름을 입력합니다.
    a. 특성 저장소 드롭다운에서 * Active Directory * 를 선택합니다.
    b. LDAP 속성 * 드롭다운에서 * 사용자 - 기본 - 이름 * 을 선택하고 O * uting Claim Type * 드롭다운에서 * UPN * 을 선택합니다.
    c. 마침 * 을 클릭합니다.

PowerShell 명령을 사용하여 애플리케이션 그룹을 생성합니다

PowerShell 명령을 사용하여 애플리케이션 그룹인 웹 API를 생성하고 범위와 청구서를 추가할 수 있습니다. 이러한 명령은 자동화된 스크립트 형식으로 사용할 수 있습니다. 자세한 내용은 <link to KB article> 를 참조하십시오.

1. 다음 comamnd를 사용하여 AD FS에서 새 애플리케이션 그룹을 생성합니다.

   ```
   New-AdfsApplicationGroup -Name $ClientRoleIdentifier
   -ApplicationGroupIdentifier $ClientRoleIdentifier
   ```

   `ClientRoleIdentifier` 애플리케이션 그룹의 이름입니다

   `redirectURL` 인증 후 리디렉션에 대한 유효한 URL입니다

2. AD FS 서버 응용 프로그램을 생성하고 클라이언트 암호를 생성합니다.

```
Add-AdfsServerApplication -Name "$ClientRoleIdentifier - Server app"
-ApplicationGroupIdentifier $ClientRoleIdentifier -RedirectUri $redirectURL
-Identifier $identifier -GenerateClientSecret
```

3. ADFS 웹 API 응용 프로그램을 만들고 사용할 정책 이름을 구성합니다.

```
$identifier = (New-Guid).Guid

Add-AdfsWebApiApplication -ApplicationGroupIdentifier $ClientRoleIdentifier
-Name "App Web API"

-Identifier $identifier -AccessControlPolicyName "Permit everyone"
```

4. 클라이언트 ID와 클라이언트 암호는 한 번만 표시되므로 다음 명령의 출력에서 가져옵니다.

```
"client_id = $identifier"

"client_secret: "$($ADFSApp.ClientSecret)
```

5. AD FS 응용 프로그램에 allat클레임 및 OpenID 권한을 부여합니다.

```
Grant-AdfsApplicationPermission -ClientRoleIdentifier $identifier
-ServerRoleIdentifier $identifier -ScopeNames @('openid')

$transformrule = @"

@RuleTemplate = "LdapClaims"

@RuleName = "AD User properties and Groups"

c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer ==

"AD AUTHORITY"]

⇒ issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =
";userPrincipalName;{0}", param = c.Value);

"@
```

6. 변환 규칙 파일을 작성합니다.

```
$transformrule |Out-File -FilePath .\issueancetransformrules.tmp -force
-Encoding ascii $relativePath = Get-Item .\issueancetransformrules.tmp
```

7. 웹 API 응용 프로그램의 이름을 지정하고 외부 파일을 사용하여 발급 변환 규칙을 정의합니다.

```
Set-AdfsWebApiApplication -Name "$ClientRoleIdentifier - Web API"
```

```
-TargetIdentifier

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

액세스 토큰 만료 시간을 업데이트합니다

PowerShell 명령을 사용하여 액세스 토큰 만료 시간을 업데이트할 수 있습니다.

- 이 작업에 대한 정보 *
- 액세스 토큰은 사용자, 클라이언트 및 리소스의 특정 조합에 대해서만 사용할 수 있습니다. 액세스 토큰은 해지할 수 없으며 만료까지 유효합니다.
- 기본적으로 액세스 토큰의 만료 시간은 60분입니다. 이 최소 만료 시간은 충분하고 크기가 조정됩니다. 지속적으로 발생하는 비즈니스 크리티컬 작업을 방지할 수 있는 충분한 가치를 제공해야 합니다.
- 단계 *

애플리케이션 그룹 WebAPI에 대한 액세스 토큰 만료 시간을 업데이트하려면 AD FS 서버에서 다음 명령을 사용하십시오.

를 누릅니다 `Set-AdfsWebApiApplication -TokenLifetime 3600 -TargetName "<Web API>"`

AD FS에서 베어러 토큰을 가져옵니다

REST 클라이언트(예: Postman)에서 아래에 언급된 매개 변수를 입력해야 하며 사용자 자격 증명을 입력하라는 메시지가 표시됩니다. 또한, 베어러 토큰을 얻으려면 2차 인증 요소(보유 중인 인증 및 대상 인증)를 입력해야 합니다.

를 누릅니다 베어러 토큰의 유효성은 애플리케이션당 AD FS 서버에서 구성할 수 있으며, 기본 유효 기간은 60분입니다.

필드에 입력합니다	값
허가 유형	인증 코드
콜백 URL	콜백 URL이 없는 경우 응용 프로그램의 기본 URL을 입력합니다.
인증 URL	[ADFS-DOMAIN-NAME]/ADFS/OAuth2/authorize
액세스 토큰 URL	[ADFS-DOMAIN-NAME]/ADFS/OAuth2/TOKEN
클라이언트 ID입니다	AD FS 클라이언트 ID를 입력합니다
클라이언트 암호	AD FS 클라이언트 암호를 입력합니다
범위	OpenID를 선택합니다

클라이언트 인증	기본 AUTH 헤더로 보냅니다
리소스	고급 옵션* 탭에서 JWT 토큰에 "AUD" 값으로 제공되는 콜백 URL과 동일한 값을 가진 자원 필드를 추가합니다.

SnapCenter 서버에서 PowerShell, SCCLI 및 REST API를 사용하여 MFA를 구성합니다

SnapCenter 서버에서 PowerShell, SCCLI 및 REST API를 사용하여 MFA를 구성할 수 있습니다.

SnapCenter MFA CLI 인증

PowerShell 및 SCCLI에서 베어러 토큰을 사용하여 사용자를 인증하는 데 "AccessToken"이라는 필드가 하나 더 있는 기존 cmdlet(Open-SmConnection)이 확장됩니다.

```
Open-SmConnection -Credential <PSCredential> [-SMSbaseUrl <String>] [-Port
<String>] [-RoleName <String>] [ -AccessToken <string>]
```

위의 cmdlet을 실행한 후 해당 사용자가 추가 SnapCenter cmdlet을 실행할 수 있도록 세션이 생성됩니다.

SnapCenter MFA REST API 인증

SnapCenter로부터 성공적인 응답을 얻으려면 _Authorization=Bearer <access token>_in REST API 클라이언트(예: Postman 또는 swagger)의 형식으로 베어러 토큰을 사용하고 헤더에 사용자 RoleName을 언급하십시오.

MFA REST API 워크플로우

MFA가 AD FS로 구성된 경우 액세스(베어러) 토큰을 사용하여 인증하여 REST API를 통해 SnapCenter 애플리케이션에 액세스해야 합니다.

- 이 작업에 대한 정보 *
- Postman, Swagger UI 또는 FireCamp와 같은 REST 클라이언트를 사용할 수 있습니다.
- 액세스 토큰을 가져와 후속 요청(SnapCenter REST API)을 인증하여 작업을 수행합니다.
- 단계 *
- AD FS MFA * 를 통해 인증합니다

  1. 액세스 토큰을 얻기 위해 AD FS 끝점을 호출하도록 REST 클라이언트를 구성합니다.

     버튼을 눌러 응용 프로그램의 액세스 토큰을 가져오는 경우 AD FS SSO 페이지로 리디렉션됩니다. 이 페이지에서 AD 자격 증명을 제공하고 MFA로 인증해야 합니다. AD FS SSO 페이지에서 사용자 이름 텍스트 상자에 사용자 이름 또는 이메일을 입력합니다.

  를 누릅니다 사용자 이름은 user@domain 또는 domain\user 형식으로 지정해야 합니다.

  1. 암호 텍스트 상자에 암호를 입력합니다.

2. 로그인 * 을 클릭합니다.
3. 로그인 옵션 * 섹션에서 인증 옵션을 선택하고 인증(구성에 따라 다름)을 수행합니다.
   - 푸시: 휴대폰에 전송되는 푸시 알림을 승인합니다.
   - QR 코드: AUTH Point 모바일 앱을 사용하여 QR 코드를 스캔한 다음 앱에 표시된 검증 코드를 입력합니다
   - 일회용 암호: 토큰의 일회용 암호를 입력합니다.
4. 인증에 성공하면 액세스, ID 및 토큰 새로 고침이 포함된 팝업이 열립니다.

   액세스 토큰을 복사하고 SnapCenter REST API에서 사용하여 작업을 수행합니다.

5. REST API에서는 헤더 섹션에서 액세스 토큰 및 역할 이름을 전달해야 합니다.
6. SnapCenter는 AD FS에서 이 액세스 토큰을 검증합니다.

   유효한 토큰인 경우 SnapCenter는 해당 토큰을 디코딩하고 사용자 이름을 가져옵니다.

7. SnapCenter는 사용자 이름과 역할 이름을 사용하여 API 실행을 위해 사용자를 인증합니다.

   인증에 성공하면 SnapCenter가 결과를 반환하고 그렇지 않으면 오류 메시지가 표시됩니다.

REST API, CLI 및 GUI에 대해 SnapCenter MFA 기능을 사용하거나 사용하지 않도록 설정합니다

- GUI *
- 단계 *
  1. SnapCenter 서버에 SnapCenter 관리자로 로그인합니다.
  2. 설정 * > * 글로벌 설정 * > * 멀티팩터인증(MFA) 설정 * 을 클릭합니다
  3. 인터페이스(GUI/RST API/CLI)를 선택하여 MFA 로그인을 활성화하거나 비활성화합니다.
- PowerShell 인터페이스 *
- 단계 *
  1. GUI, REST API, PowerShell 및 SCCLI에 대해 MFA를 사용하도록 PowerShell 또는 CLI 명령을 실행합니다.

     ```
     Set-SmMultiFactorAuthentication -IsGuiMFAEnabled -IsRestApiMFAEnabled
     -IsCliMFAEnabled -Path
     ```

     path 매개 변수는 AD FS MFA 메타데이터 XML 파일의 위치를 지정합니다.

  지정된 AD FS 메타데이터 파일 경로로 구성된 SnapCenter GUI, REST API, PowerShell 및 SCCLI에 대한 MFA를 활성화합니다.

  1. 를 사용하여 MFA 구성 상태 및 설정을 확인합니다 `Get-SmMultiFactorAuthentication` cmdlet.

SCCLI 인터페이스 *

- 단계 *
  1. `# sccli Set-SmMultiFactorAuthentication -IsGuiMFAEnabled true`

```
-IsRESTAPIMFAEnabled true -IsCliMFAEnabled true -Path
"C:\ADFS_metadata\abc.xml"
```

2. `# sccli Get-SmMultiFactorAuthentication`

- REST API *

1. GUI, REST API, PowerShell 및 SCCLI에 대해 MFA를 사용하도록 다음 POST API를 실행합니다.

매개 변수	값
요청된 URL입니다	/api/4.9/settings/multipactorauthentication을 참조하십시오
HTTP 메소드	게시
요청 본문	{ "IsGuiMFAEnabled": false, "IsRestApiMFAEnabled": 참, "IsCliMFAEnabled": false, "ADFSConfigFilePath":"C:\\ADFS_METADATA\\abc.xml" }
응답 본문	{ "MFAConfiguration":{을 참조하십시오 "IsGuiMFAEnabled": false, "ADFSConfigFilePath":"C:\\ADFS_METADATA\\abc.xml", "SCConfigFilePath": null, "IsRestApiMFAEnabled": 참, "IsCliMFAEnabled": false, "ADFSHostName":"win-adfs-sc49.winscedom2.com" } }

2. 다음 API를 사용하여 MFA 구성 상태 및 설정을 확인합니다.

매개 변수	값
요청된 URL입니다	/api/4.9/settings/multipactorauthentication을 참조하십시오
HTTP 메소드	가져오기
응답 본문	{ "MFAConfiguration":{을 참조하십시오 "IsGuiMFAEnabled": false, "ADFSConfigFilePath":"C:\\ADFS_METADATA\\abc.xml", "SCConfigFilePath": null, "IsRestApiMFAEnabled": 참, "IsCliMFAEnabled": false, "ADFSHostName":"win-adfs-sc49.winscedom2.com" } }