Installatie ADFS MFA Extensie

SURFnet heeft een multifactor authenticatie (MFA) extensie ontwikkeld voor Microsoft AD FS voor gebruik met SURFsecureID. Met deze extensie kan de tweede factor van een gebruiker in SURFsecureID worden gebruikt voor MFA authenticatie in AD FS. De registratie, activatie en het beheer van de tweede factors blijft via SURFsecureID lopen. De authenticatie van een relying party (RP) die aangesloten is op de AD FS server blijft lopen via de AD FS server. Op de AD FS server wordt geconfigureerd wanneer er voor RP MFA authenticatie nodig is. Als de ADFS MFA extensie voor SURFsecureID door AD FS wordt aangeroepen, dan verzorgd deze de authenticatie van de tweede factor van een gebruiker bij SURFsecureID.

Op deze pagina staat de installatie procedure van deze extensie beschreven. Ook geven we aan waar meer informatie over de extensie gevonden kan worden. Deze pagina beschrijft installatie van versie 1.0 van de MFA extensie op ADFS 3.0 (Windows 2012 R2) en ADFS 4.0 (Windows 2016). Eerdere versies van de extensie (0.1 en 0.2) worden niet meer ondersteund.

Voor gebruik van de plugin zijn nodig:

- Een productie koppeling van een eigen identity provider op de SURFconext productie of test omgeving
- Een Microsoft Windows domain met AD FS versie 3 of 4
- Een koppeling van de plugin aan de SURFsecureID productie, pilot of test omgeving

We werken momenteel aan een nieuwe installatiehandleiding en een nieuwe installatie methode voor de ADFS MFA extensie voor SURFsecureID.

Installatieprocedure

De MFA extensie moet op iedere AD FS server worden geïnstalleerd waarop MFA plaats moet vinden. De installatie procedure voor de 2e, 3e etc AD FS server wijkt af van de eerste.

Stap 1 - Download SetupPackage.zip

Download `SetupPackage.zip` van https://github.com/SURFnet/ADFS-MFA-SAML2.0-Extension/releases/download/1.0/SetupPackage.zip en pak deze uit op de eerste AD FS server.

Stap 2 - Pas SurfnetMfaPluginConfiguration.json aan

In de `Setup` directory van de uitgepakte `SetupPackage.zip` staat `SurfnetMfaPluginConfiguration.json`. Hierin staan de configuratie parameters die door het installatie script gebruikt worden om de plugin te installeren. Pas dit bestand aan.

Hieronder staat een gedeeltelijk ingevulde `SurfnetMfaPluginConfiguration.json` voor gebruik met de SURFsecureID **Pilot** omgeving, de lege waarden zijn specifiek voor de organisatie. Behalve `SigningCertificate` moeten deze allemaal ingevuld worden. In de tabel hieronder staat beschreven hoe deze waarden ingevuld moeten worden.

SurfnetMfaPluginConfiguration.json voor SURFconext SA Pilot

```
{
  "Settings": {
    "SecondFactorEndpoint": "https://gateway.pilot.stepup.surfconext.nl/second-factor-only/single-sign-on",
    "MinimalLoa": "http://pilot.surfconext.nl/assurance/sfo-level2",
    "schacHomeOrganization": "",
    "ActiveDirectoryName": "",
    "ActiveDirectoryUserIdAttribute": ""
  },
  "ServiceProvider": {
    "SigningCertificate": "",
    "EntityId": ""
  },
  "IdentityProvider": {
    "EntityId": "https://gateway.pilot.stepup.surfconext.nl/second-factor-only/metadata",
    "Certificate": "sa_pilot_saml_signing_certificate_pem.crt"
  }
}
```

Waarde		Beschrijving
Settings		
	`SecondFactorEndpoint`	Dit is de SingleSignOnService Location van het SFO endpoint op de SURFsecureID gateway. Deze staat in de SAML metadata van de omgeving en is verschillend voor de test, pilot en productie omgevingen. **Test:** `https://sa-gw.test.surfconext.nl/second-factor-only/single-sign-on` **Pilot**: `https://gateway.pilot.stepup.surfconext.nl/second-factor-only/single-sign-on` **Productie**: `https://sa-gw.surfconext.nl/second-factor-only/single-sign-on`
	`MinimalLoa`	Dit is geeft aan welk nivo van authenticatie vereist is. De ondersteunde identifiers zijn verschillend voor de test, pilot en productie omgevingen. "level2" staat alle type tokens toe, "level3" alleen YubiKey. **Test:** `http://test.surfconext.nl/assurance/sfo-level2` **Pilot**: `http://pilot.surfconext.nl/assurance/sfo-level2` **Productie**: `http://surfconext.nl/assurance/sfo-level2`
	`schacHomeOrganization`	Dit is de waarde van het `urn:mace:terena.org:attribute-def:schacHomeOrganization` dat voor de gebruiker is geregistreerd tijdens de registratie van het token in SURFsecureID. Deze waarde wordt door de extensie gebruikt om de SURFconext identifier van de gebruiker te bepalen voor authenticatie op de gateway. De waarde van het `schacHomeOrganization` attribuut heeft de vorm van een domeinnaam. Bijvoorbeeld: `catharijnecollege.nl`. Geef hier de waarde op die de identity provider (IdP) aan SURFconext meegeeft bij authenticatie. Op https://engine.surfconext.nl/authentication/sp/debug is te zien wat een IdP bij authenticatie aan SURFconext doorgeeft.
	`ActiveDirectoryName`	Dit is de DNS naam van de locale active directory (AD) server. Bijvoorbeeld: `corp.contoso.com` Deze AD wordt gebruikt voor het opzoeken van het `uid` van de door AD FS geauthentiseerde gebruiker te lezen uit het in `ActiveDirectoryUserIdAttribute` opgegeven attribuut. Omdat de extensie wordt geladen door AD FS server, moet de gebruiker waaronder de AD FS service draait toegang hebben tot de hier opgegeven ADFS.
	`ActiveDirectoryUserIdAttribute`	Dit is de naam van het attribuut in de locale active directory (AD) server welke het `urn:mace:dir:attribute-def:uid` van de gebruiker bevat dat de identity provider (IdP) aan SURFconext meegeeft bij authenticatie. De waarde uit dit attribuut wordt door de extensie gebruikt om de SURFconext identifier van de gebruiker te bepalen voor authenticatie op de gateway. Op https://engine.surfconext.nl/authentication/sp/debug is te zien wat een IdP bij authenticatie aan SURFconext doorgeeft.
ServiceProvider		
	`SigningCertificate`	Naam van een .pfx bestand in de `Setup` directory met daarin het X.509 certificaat en de RSA private key waarmee de authenticatie verzoeken van de extensie naar de SURFsecureID gateway worden ondertekend. Voor installatie op de 1e AD FS server kan dit leeggelaten worden, het installatie script zal dan zelf een self signed certificaat en private key genereren, deze exporteren naar een .pfx bestand met password en de `SurfnetMfaPluginConfiguration.json` aanpassen. Het .pfx bestand, het password en het aangepaste `SurfnetMfaPluginConfiguration.json` bestand zijn nodig voor de installatie van de extensie op een 2e, 3e etc AD FS server. Een .pfx bestand is een PKCS#12 in DER formaat.
	`EntityId`	Dit is het SAML EntityID van de extensie welke de extensie uniek identificeert richting SURFsecureID. Deze waarde is vrij te kiezen en heeft de vorm van een URL of een URN. De in de URL gebruikte identifier moet onder eigen beheer zijn. Voorbeeld: `http://catharijnecollege.nl/adfs-mfa-extension`
IdentityProvider		
	`EntityId`	Dit is het SAML EnitityID van de SURFsecureID gateway. Deze staat in de SAML metadata van de omgeving en is verschillend voor de pilot en productie omgevingen. **Test**: `https://sa-gw.test.surfconext.nl/second-factor-only/metadata` **Pilot**: `https://gateway.pilot.stepup.surfconext.nl/second-factor-only/metadata` **Productie**: `https://sa-gw.surfconext.nl/second-factor-only/metadata`
	`Certificate`	Naam van een .crt bestand in de `Setup` directory met daarin het X.509 signing certificaat van de SURFsecureID gateway in PEM formaat. Dit certificaat staat in de SAML metadata van de omgeving en is verschillend voor de pilot en productie omgevingen. Zie de volgende stap (Stap 3).

Stap 3 - Download het SURFsecureID signing certificaat

Download het SAML signing certificaat van de SURFsecureID gateway, zet dit in de `Setup` directory van de extensie op de AD FS server, en zorg dat `Certificate` in de `SurfnetMfaPluginConfiguration.json` (zie ook de vorig stap) naar deze file refereert. Dit certificaat staat in de SAML metadata van de omgeving en is verschillend voor de test, pilot en productie omgevingen. Voor het gemak staan de certificaten hieronder in het juiste formaat ter download gegeven:

- **Test** omgeving: https://wiki.surfnet.nl/download/attachments/65799201/sa_test_saml_signing_certificate_pem.crt
- **Pilot** omgeving: https://wiki.surfnet.nl/download/attachments/50111280/sa_pilot_saml_signing_certificate_pem.crt
- **Productie** omgeving: https://wiki.surfnet.nl/download/attachments/50111280/sa_production_saml_signing_certificate_pem.crt

De authoritative bron voor het certificaat is de metadata op de gateway, verifieer dit certificaat wanner het voor productie doeleinden gebruikt wordt en neem bij vragen contact op met support@surfconext.nl. De metadata van de omgevingen staat op:

- **Test** omgeving: https://sa-gw.test.surfconext.nl/second-factor-only/metadata
- **Pilot** omgeving: https://gateway.pilot.stepup.surfconext.nl/second-factor-only/metadata
- **Productie** omgeving: https://sa-gw.surfconext.nl/second-factor-only/metadata

Stap 4 - Run het Install-SurfnetMfaPlugin.ps1 installatie script op de 1e AD FS Server

Het installatie script herstart de AD FS service.

1. Open, als gebruiker met Administrator rechten, een powershell op de AD FS server.
2. Ga naar de `Setup` directory (van de uitgepakte `SetupPackage.zip`)
3. Run `Install-SurfnetMfaPlugin.ps1`

Bij eerste installatie schrijft het installatiescript een aantal files weg:

- Een backup van de ADFS configuratie (C:\Windows\ADFS\Microsoft.IdentityServer.Servicehost.exe.config)
- Een export van het gegenereerde SAML signing certificaat van de plugin
- De `SigningCertificate` parameter in de `SurfnetMfaPluginConfiguration.json` wordt gevuld met deze file.

Bewaar deze, en bewaar ook de uitvoer van het script, op een veilige plaats.

⚠ Er zit een beperking in het huidige installatiescript. Na een eerste installatie zal de AD FS configuratie bij het nogmaals uitvoeren van het script niet worden aangepast. Wijzigingen in `SurfnetMfaPluginConfiguration.json` worden dus niet overgenomen. Er moet eerste een volledige uninstall worden gedaan om het installatiescript weer te kunnen gebruiken met een aangepaste configuratie. De (aangepaste) `SurfnetMfaPluginConfiguration.json` en het gegenereerde certificaat kunnen wel worden hergebruikt.

Stap 5 - Run het Install-SurfnetMfaPlugin.ps1 installatie script op de andere AD FS Servers

Het installatie script herstart de AD FS service.

1. Kopieer de uitgepakte `SetupPackage.zip` directory, met daarin de `Setup` directory en de bij installatie aangepaste en toegevoegde bestanden van de eerste AD FS server naar deze AD FS server.
2. Ga naar de `Setup` directory (van de uitgepakte `SetupPackage.zip`)
3. Run `Install-SurfnetMfaPlugin.ps1`
4. Het script zal vragen om een password, dit password staat in de uitvoer van het installatiescript script van de eerste server.

Stap 6 - Laat een koppeling maken voor de extensie in SURFsecureID

Stuur een mail aan support@surfconext.nl met daarin de volgende informatie:

1. Om welke instelling gaat het (wat is de waarde van het schacHomeOrganization attribuut?)
2. Aan welke SURFsecureID omgeving moet de extensie gekoppeld worden: Test, Pilot of Productie?
3. Wat is de `Issuer` (het `EntityID`) van de extensie? Dit staat in de uitvoer van het installatiescript
4. Wat is het SAML signing certificaat van de extensie? Dit staat in de uitvoer van het installatiescript
5. Wat is de volledige hostname van de ADFS server? Dit is de hostname waarop de ADFS server SAML responses ontvangt.

Voor het maken van de koppeling is toestemming van de SURFconext verantwoordelijke van de betreffende instelling nodig.

Stap 7 - Configureer MFA in AD FS

Na installatie van de extensie zal deze als MFA methode als "ADFS.SCSA" beschikbaar zijn in AD FS, maar deze wordt nog niet gebruikt voor authenticatie. Daarvoor moet deze methode eerste aangezet worden, en moet aangegeven worden voor welke gebruikers en voor welke Relying Parties MFA vereist is.

Alle configuratie vindt plaats in AD FS Management (Administrative Tools).

Enable de ADFS.SCSA MFA extensie

1. Ga naar "Authentication Policies" en kies voor "Edit Global Multi-factor Authentication"
2. Enable "ADFS.SCSA" door deze aan te vinken.
3. Optioneel kan in dit scherm voor alle alle Relying Parties op basis van groeplidmaatschap MFA aangezet worden

Enable MFA per Relyng Party

1. Ga naar "Authentication Policies" en dan "Per Relying Party Trust", selecteer de Relying Party waarvoor je MFA wil configureren, en kies voor "Edit Custom Multi-factor Authentication".
2. Geef aan voor welke gebruikers / groepen voor authenticatie naar deze Relying Party MFA vereist is. Daarnaast kan op basis van registered / unregistered of intranet / extranet MFA voor een Relying Party worden vereist.

Opmerkingen

De AD FS MFA extensie heeft haar eigen SAML implementatie en configuratie welk lost staat van AD FS. Hoewel de extensie een SAML service provider (SP) voor SURFsecureID is, staat deze dus niet onder de relying parties in de AD FS config.

Meer informatie

Meer technische informatie over de extensie: https://github.com/SURFnet/ADFS-MFA-SAML2.0-Extension

De extensie maakt gebruik van de second factor only (SFO) interface van SURFsecureID. Meer informatie over SFO: Second Factor Only (SFO) Authentication

Meer informatie over de "Authentication Policies" in ADFS: Configure Authentication Policies