Installatie ADFS MFA Extensie

SURF 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 een 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.

De ADFS MFA Extensie is dus alleen voor gebruik van diensten – ook wel services, service providers, SPs, relying party of RPs genoemd – die direct op de eigen AD FS server van de instelling zijn aangesloten. Voor diensten die op SURFconext zijn aangesloten is de ADFS MFA extensie niet nodig.

Op deze pagina staat de installatie procedure van versie 2.0 van deze extensie beschreven. Ook geven we aan waar meer informatie over de extensie gevonden kan worden. Deze pagina beschrijft installatie van de extensie voor Windows 2012 R2, Windows 2016 en Windows 2019.

Voor gebruik van de extensie zijn nodig:

- Een koppeling van een eigen identity provider (typisch AD FS) op de SURFconext productie of test omgeving
- De instelling moet gebruik maken van de SURFsecureID dienst op de productie of test omgeving.

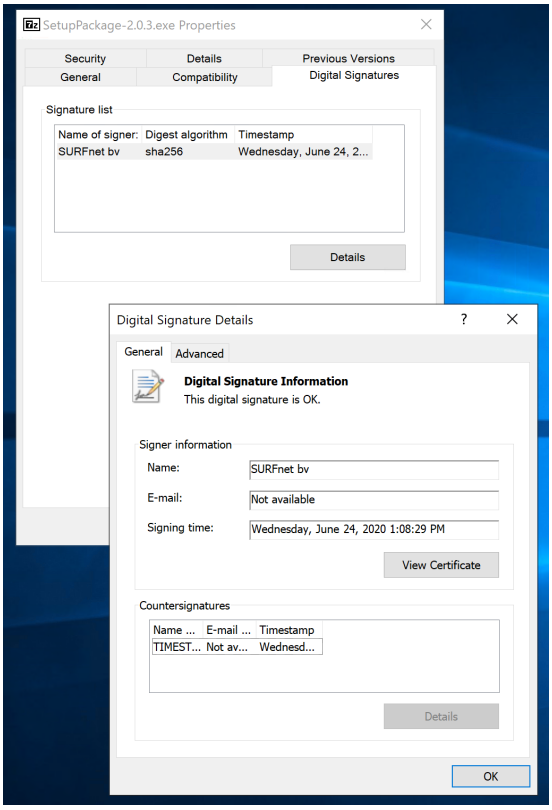
Download de SURFsecureID ADFS MFA extensie

Releases van de extensie worden gepubliceerd op github in en self-extracting zip: `SetupPackage-`*versie*`.exe`

De laatste productie release is https://github.com/SURFnet/ADFS-MFA-SAML2.0-Extension/releases/download/2.0.3/SetupPackage-2.0.3.exe

Validatie

De `SetupPackage-`*versie*`.exe` en de Setup.exe in het package zijn ondertekend door SURFnet bv of SURF B.V. Controleer de status van de signature door de eigenschappen van het bestand te bekijken:



Documentatie

De extensie komt met uitgebreide documentatie: zie de INSTALL, UPGRADE, KNOWN_ISSUES, CONFIGURATION en CHANGELOG bestanden in de setup package. Hierin staat meer informatie over de extensie dan we op deze pagina kwijt kunnen. Voor de laatste versie van deze bestanden:

- INSTALL.md
- UPGRADE.md
- CONFIGURATION.md
- KNOWN_ISSUES.md
- CHANGELOG

Installatieprocedure

De MFA extensie moet op iedere AD FS server worden geïnstalleerd waarop MFA plaats moet vinden, dus typisch iedere AD FS server in de Farm. Deze instructies gaan er van uit dat de configuratie van AD FS in de Windows Internal Database (WID) staat. Daarbij is altijd één AD FS server in de Farm de primary, en dit is de enige server die in AD FS configuratiewijzigingen kan maken. De extensie moet eerst op de primaire AD FS server geïnstalleerd worden. De installatie procedure voor de 2e, 3e etc AD FS server wijkt iets af van die op de eerste server. Gedurende de installatie is een herstart van de AD FS service nodig.

Staat er al een versie de extensie geïnstalleerd, voer dan een upgrade van de SURFsecureID ADFS extensie uit

Voorbereiding

Backup

We raden aan een backup of snapshot te maken van de AD FS server(s) voorafgaand aan de installatie.

Download SetupPackage

Download de SURFsecureID ADFS MFA extensie en pak deze uit op de primary AD FS server. Het SetupPackage bevat het installatieprograma (Setup.exe), de MFA extensie en de benodigde configuratie voor de verschillende SURFsecureID omgevingen: productie en test.

Verifieer de AD FS configuratie

Voer het `Setup.exe` uit de SetupPackage uit in check mode. Dit voert een aantal checks uit op de AD FS server. De AD FS service moet hiervoor gestart zijn.

1. Open een elevated command prompt op de AD FS server
2. Ga naar de directory waar het SetupPackage is uitgepakt en
    a. voor versie < 2.1.0. voer het "`.\Setup.exe -c`" commando uit
    b. voor latere versies voor het "`.\Setup.exe`" commando uit

Installatie op de primaire AD FS server

Voer het `Setup.exe` uit de SetupPackage uit in installatie/upgrade mode:

1. Open een elevated command prompt op de AD FS server
2. Ga naar de directory waar het SetupPackage is uitgepakt en voer het "`.\Setup.exe -i`" commando uit.

Het installatieprogramma zal om een aantal configuratiegegevens gaan vragen welke nodig zijn voor de configuratie van de extensie. Hieronder lopen we door de vragen die Setup stelt heen.

SURFsecureID omgeving

```
There are different SecondFactorOnly servers, their names suggest their usage.

1. Production (https://sa-gw.surfconext.nl/second-factor-only/metadata)
2. Test (https://sa-gw.test.surfconext.nl/second-factor-only/metadata)

Select a SecondFactorOnly gateway environment (123x?) [1]:
```

Hier configureer je welke SURFsecureID omgeving de MFA extensie moet gebruiken voor de verificatie van de tweede factor.

schacHomeOrganization

```
Every organization has a unique identifier 'schacHomeOrganization'. Together with user ID it is unique in SFO

'schacHomeOrganization' has no value

Provide a value for 'schacHomeOrganization': hartingcollege.nl
```

Geef hier de waarde op van het `urn:mace:terena.org:attribute-def:schacHomeOrganization` attribuut (claim) dat voor de gebruikers in de organisatie door de identity provider naar SURFconext wordt doorgegeven. Deze waarde is onderdeel van het unieke gebruikers ID in SURFsecureID. Het gaat hier om de waarde van dit SAML attribuut, bijvoorbeeld "hartingcollege.nl".

User ID

```
The name of the Active Directory attribute is required that contains the user ID (uid). Together with
schacHomeOrganization it is unique in SFO

'Active Directory SFO userid Attribute' has no value

Provide a value for 'Active Directory SFO userid Attribute': sAMAccountName
```

Geeft hier de naam op van het attribuut in Active Directory waarin het user ID staat dat voor de gebruikers in de organisatie door de identity provider (IdP) in het `urn:mace:dir:attribute-def:uid` attribuut ("claim" in ADFS terminologie) naar SURFconext wordt doorgegeven. Deze waarde is onderdeel van het unieke gebruikers ID in SURFsecureID. Zoek in de configuratie van de IdP (meestal ADFS) van de eigen instelling op welke waarde wordt doorgegevan aan SURFconext voor het `urn:mace:dir:attribute-def:uid` attribuut en zorg dat dat altijd hetzelfde is als dat de MFA extensie gebruikt.

SP EntityID

```
The MFA extension needs a worldwide unique URI as an identifier in SAML2 requestsDefault value for 'MFA
Extension (SP) entityID': http://adfs.hartingcollege.nl/stepup-mfa

Do you want to continue with 'http://adfs.hartingcollege.nl/stepup-mfa'? (ynx?) [y]:
```

Geef hier het SP EntityID van de ADFS extensie op. Dit is het unieke ID van deze MFA extensie in SURFsecureID en is vrij te kiezen. Het formaat is een URI (URL). Zorg dat het voor iedereen duidelijk is dat dit bij deze MFA extensie installatie hoort, en gebruik een domein dat eigendom is van de eigen organisatie. Het setup programma doet zelf al een suggestie op basis van de DNS naam van de ADFS service.

SP Signing certificaat

```
The SFO MFA extension needs a certificate to sign its SAML2 messages

1. Select an existing certificate in the store
2. Import a certificate from a '.PFX' file
3. Create a Self Signed certificate

How do you want to select a certificate (123x?) [1]: 3
```

De MFA extensie heeft een signing certificaat (met bijbehorende public/private keypair) nodig. Met dit certificaat worden de authenticatieverzoeken van de extensie naar SURFsecureID ondertekend. Gebruik hiervoor een self-signed certificaat, een TLS server certificaat dat bij een certificaatverstrekker vandaan komt is dus niet geschikt.

Omdat dit een nieuwe installatie is, en we dus nog geen certificaat hebben, laten we het Setup programma een nieuw certificaat voor ons genereren (optie 3) en we kiezen er ook voor om het certificaat met de private key als .pfx bestand te exporteren, we hebben dit certificaat namelijk nodig voor de configuratie van de andere AD FS server(s). Bewaar ook het encryptie password van het .pfx bestand dat door het Setup programma wordt getoond.

```
The new certificate is now in the Certificate Store (Local Computer).
It can be exported at any time.
Other servers in the farm must use the same certificate.

Do you want to export this certificate now as a '.pfx' (ynx?): y

The PFX filepath: C:\Users\surf\Downloads\SetupPackage-2.0.2\Config\SP-SFO-Extension 20200603.pfx
The password is: T+Fl2u/ysle4bk3j
Save it in a safe place.

Did you save it somewhere in a safe place (ynx?): y
Subject: CN=SFO MFA extension http://adfs.hartingcollege.nl/stepup-mfa
Issuer: CN=SFO MFA extension http://adfs.hartingcollege.nl/stepup-mfa
Valid until: 2025-06-02
Thumbprint: FC7D0F8B8A03FC7B445DCBA218A3855B2E5487FB

Continue with this certificate (ynx?) [y]: y
```

Bevestiging

```
The (new) configuration settings are now as follows

SFO server (IdP) entityID : https://sa-gw.surfconext.nl/second-factor-only/metadata
schacHomeOrganization : hartingcollege.nl
Active Directory SFO userid Attribute : sAMAccountName
MFA Extension (SP) entityID : http://adfs.hartingcollege.nl/stepup-mfa
MFA Extension (SP) signing thumbprint : FC7D0F8B8A03FC7B445DCBA218A3855B2E5487FB

Do you want to continue with these settings? (ynx?) [y]:
```

We krijgen nog een overzichtje van de gekozen instellingen

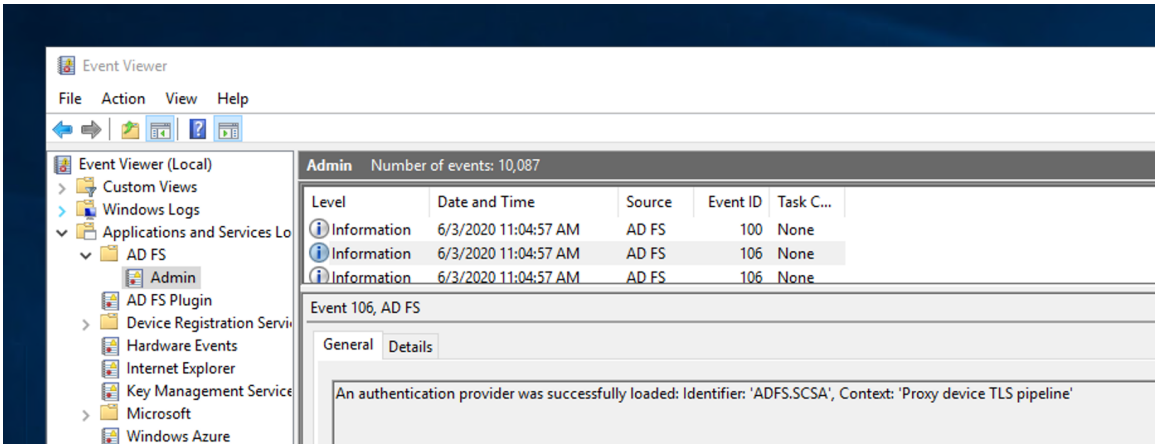
Installatie

```
Install version 2.0.2.0 (ynx?): y

Installation on local disk successful.

Registration Info filepath: C:\Users\surf\Downloads\SetupPackage-2.0.2\Config\MfaRegistrationData.txt


Registration of new adapter successful.
Registration Successful

Stopping ADFS service.

Stopped ADFS service
Starting ADFS service..
Started ADFS service

Everything was OK.
Take a look at the ADFS EventLog and also the
MFA extension EventLog 'AD FS plugin', to verify it.
```

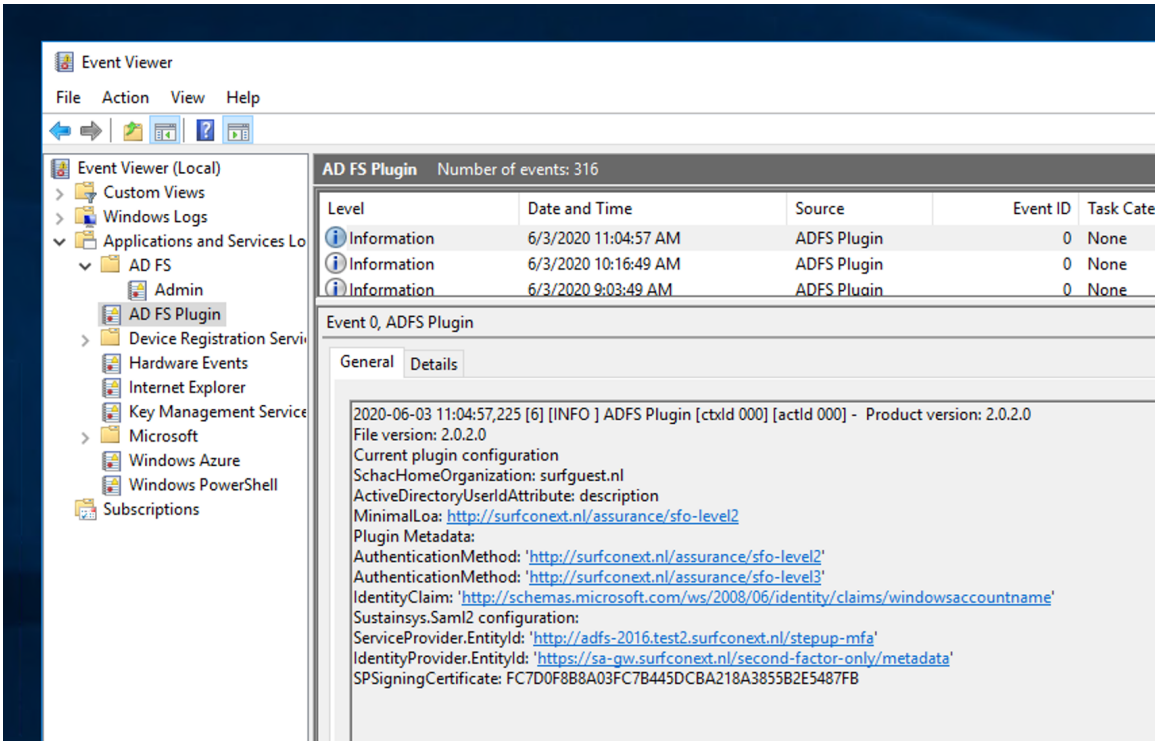
De MFA extensie in nu geregistreerd in AD FS en is geïnstalleerd op de Primary AD FS server. De MFA extensie en de configuratie bestanden voor de MFA extensie staan in de ADFS directory (typisch `C:\Windows\ADFS`).

Checks

De MFA extensie moet nu door de AD FS service geladen zijn. De identifier van de extensie in ADFS is "ADFS.SCSA". Na het starten van de AD FS service staat hierover een bericht in het event log: "`An authentication provider was successfully loaded: Identifier: 'ADFS.SCSA', Context: 'Proxy device TLS pipeline'`". Gebruik de event viewer om dit te controleren. Kijk ook of er geen errors of warnings zijn ontstaan in AD FS:



De extensie zelf heeft ook een event log "`AD FS Plugin`". Hierin wordt bij het laden van de extensie een event weggeschreven met daarin de huidige versie en configuratie van de extensie:



Laat een koppeling maken voor de extensie in SURFsecureID

Tijdens de installatie heeft het Setup programma de configuratiegegevens die nodig zijn om de MFA extensie toe te voegen aan SURFsecureID weggeschreven in de `config` directory in het SetupPackage. De naam van deze file is `MfaRegistrationData.txt`.

- Stuur het `MfaRegistrationData.txt` bestand naar support@surfconext.nl
- Geef daarbij aan met welke SURFsecureID omgeving je wilt koppelen (productie of test). Dit is de omgeving die je bij de configuratie van de extensie gekozen hebt.

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

Installatie op de secondary AD FS server

De extensie moet ook op de andere AD FS servers geïnstalleerd worden. Hiervoor moet precies dezelfde configuratie worden gebruikt als op de Primary AD FS server. Om dit te vergemakkelijken, en om onbedoelde configuratie verschillen te voorkomen, is er tijdens de installatie in de `config` directory van het SetupPackage een `UsedSettings.json` file met daarin de gemaakte configuratie keuzes weggeschreven. Deze gaan we gebruiken tijdens de installatie op de secondary AD FS server(s). Voer de onderstaande stappen uit op iedere secondary AD FS server.

Copieer de SetupPackage van de primary naar de secondary server

Kopieer de hele SetupPackage directory van de Primary naar de secondary server(s). Hierin staat `UsedSetting.json` en het gexporteerde .pfx bestand met daarin het SP signing certificaat van de extensie.

Installeer de extensie

Voer het `Setup.exe` uit de SetupPackage uit in installatie/upgrade mode:

1. Open een elevated command prompt op de AD FS server
2. Ga naar de directory waar het SetupPackage-2.x.x is uitgepakt en voer het "`.\Setup.exe -i`" commando uit.

Het installatieprogramma leest de configuratie uit de `UsedSettings.json`. Omdat het certificaat wat in deze configuratie staat niet gevonden kan worden krijgen we de vraag of we een certificaat willen importeren. Dat willen we. Kies de eerder geëxporteerde pfx in de config directory van het setup package en geef het toen getoonde password op:

```
Do you want to import a certificate (ynx?): y
Give password for PFX file: T+Fl2u/ysle4bk3j
Subject: CN=SFO MFA extension http://adfs-2016.test2.surfconext.nl/stepup-mfa
Issuer: CN=SFO MFA extension http://adfs-2016.test2.surfconext.nl/stepup-mfa
Valid until: 2025-06-02
Thumbprint: FC7D0F8B8A03FC7B445DCBA218A3855B2E5487FB

Continue with this certificate (ynx?) [y]: y
```

Setup heeft nu een correct configuratie, en kan door met de installatie:

```
*** Setup did find a CORRECT CONFIGURATION. With settings as follows:

SFO server (IdP) entityID : https://sa-gw.surfconext.nl/second-factor-only/metadata
schacHomeOrganization : surf.nl
Active Directory SFO userid Attribute : sAMAccountName
MFA Extension (SP) entityID : http://adfs-2016.test2.surfconext.nl/stepup-mfa
MFA Extension (SP) signing thumbprint : FC7D0F8B8A03FC7B445DCBA218A3855B2E5487FB

Do you want to continue with these settings? (ynx?) [y]: y

Install version 2.0.2.0 (ynx?): y

Installation on local disk successful.

Registration Info filepath: C:\Users\surf\Downloads\SetupPackage-2.0.2\Config\MfaRegistrationData.txt


Registration of new adapter successful.
Registration Successful

Stopping ADFS service.

Stopped ADFS service
Starting ADFS service..
Started ADFS service

Everything was OK.
Take a look at the ADFS EventLog and also the
MFA extension EventLog 'AD FS plugin', to verify it.
```

Controle

Bekijk weer de beide event logs om te verifiëren dat de extensie goed geladen is door de AD FS server.

Configureer MFA in AD FS

Na installatie van de extensie zal deze als MFA extension 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 Relying 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.

Probleemoplossing

De extensie komt met uitgebreide documentatie: zie de INSTALL, UPGRADE, KNOWN_ISSUES, CONFIGURATION en CHANGELOG bestanden in de setup package. Hierin staat meer informatie over de extensie dan we op deze pagina kwijt kunnen.

Probleemen tijdens de installatie

- Het setup programma schrijft `MFA-extension.SetupLog.txt` naar de SetupPackage. Deze file bevat een log van de installatie
- Tijdens de registratie stap van de extensie door het Setup programma wordt in de dist directory van het SetupPackage `StepUp.RegistrationLog.txt` geschreven.

Bewaar deze bestanden bij problemen met de installatie, configuratie, registratie etc van de extensie voordat je contact opneemt met support@surfconext.nl voor assistentie.

Configuratie aanpassen

Nadat de MFA extensie is geinstalleerd kan de configuratie worden aangepast. Een deinstallatie is hiervoor niet nodig. Zorg er bij het aanpassen van de configuratie voor dat alle AD FS server dezelfde configuratie van de extensie gebruiken. Geef bij wijziging van het SP signing certificaat of de EntityID van de extensie, of bij wijziging van de hostname van de AD FS server opnieuw de `MfaRegistrationData.txt` door aan support@surfconext.nl en geef door om welke SURFsecureID omgeving het gaat (test of productie).

Gebruik Setup.exe in reconfigure mode voor het wijzigen van de configuratie:

1. Open een elevated command prompt op de AD FS server
2. Ga naar de directory waar het SetupPackage-2.x.x is uitgepakt en voer het "`.\Setup.exe -r`" commando uit.

Meer informatie

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

Hier vind je ook de laatste versie van de documentie over de plugin:

- INSTALL.md
- UPGRADE.md
- CONFIGURATION.md
- KNOWN_ISSUES.md
- CHANGELOG
- README.md

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