OS2faktor

AD FS Connector Vejledning

Version: 1.3.0
Date: 16.04.2019
Author: BSG

Indhold

1 Indledning

Dette dokument beskriver hvordan man installerer og konfigurerer AD FS Connectoren til OS2faktor infrastrukturen.

Dokumentet er rettet mod it-teknikere og driftsfolk der administrerer AD FS servere.

2 Forudsætninger

For at installere AD FS Connectoren skal man have følgende

- Administrator-rettighed til de AD FS servere hvor connectoren skal installeres
- Selve connector softwaren
- Viden om hvor relevante bruger-oplysninger kan findes i AD (til konfigurationen)
- Den API nøgle der gør det muligt for connectoren at kommunikere med OS2faktor infrastrukturen

2.1 Connector softwaren

Man kan altid hente den nyeste udgave af AD FS connectoren fra nedenstående website. Man kan altid se hvilken version af softwaren man har installeret, ved at kigge i registreringsdatabasen (se afsnittet om konfiguration af connectoren for yderligere detaljer)

https://www.os2faktor.dk/download.html

2.2 API nøgle

Under konfiguration skal der indtastes en API nøgle. Denne nøgle kan man få af driftoperatøren til OS2faktor infrastrukturen. Tag kontakt til helpdesk@digital-identity.dk for yderligere detaljer.

Hvis man anvender forskellige OS2faktor Connectors (fx både en VPN Connector og en AD FS Connector), skal man anvende forskellige API nøgler til disse Connectors.

3 Installation

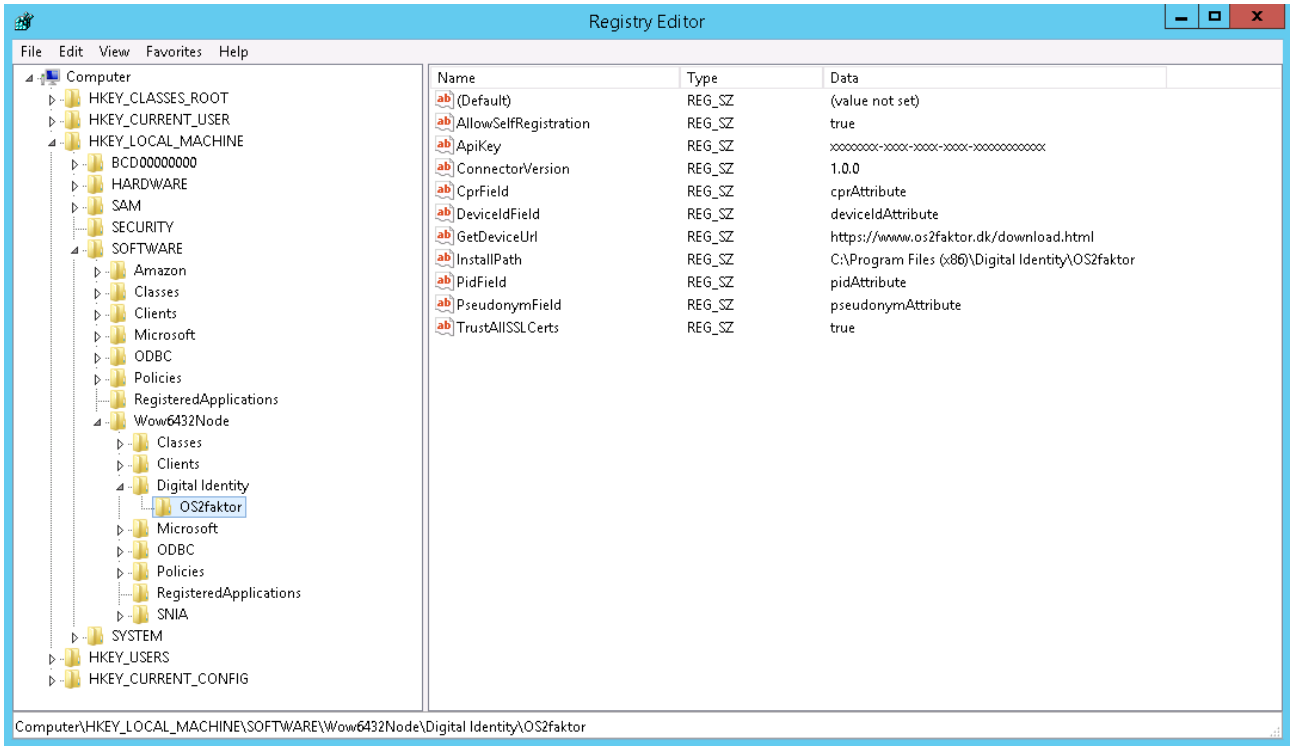
Connectoren distribueres som en MSI installer. Det er vigtigt at softwaren installeres på samtlige servere i AD FS farmen, da der installeres og registreres en række DLL filer.

Under installationen skal man forholde sig til 2 valg.

1. Hvor softwaren skal installeres. Hvis ikke default værdien er ønsket, så rettes denne til, så softwaren installeres på det ønskede sted
2. Om AD FS setup scriptet skal afvikles. Default er at det afvikles. Hvis man ikke ønsker at det afvikles, skal man selv registrere de fornødne DLL filer i GAC'en via powershell, samt registrere OS2faktor connectoren inde i AD FS konsollen. Det anbefales at man afvikler setup scriptet i stedet

Efter installationen er der indlæst en dummy konfiguration i windows registreringsdatabasen under

`HKEY_LOCAL_MACHINE > SOFTWARE > Wow6432Node > Digital Identity > OS2faktor`



Konfigurationen er beskrevet i følgende afsnit.

4 Konfiguration

Konfigurationen af OS2faktor AD FS Connectoren udføres 2 steder. I Windows regstreringsdatabasen, og i AD FS konsollen.

4.1 Windows registreringsdatabasen

Under følgende nøgle i registreringsdatabasen, er der en række globale indstillinger, der skal opsættes korrekt før Connectoren kan fungere i AD FS.

`HKEY_LOCAL_MACHINE > SOFTWARE > Wow6432Node > Digital Identity > OS2faktor`

Der er indlæst dummy-værdier i registreringsdatabasen, som skal tilpasses. Disse er

Nøgle	**Beskrivelse**
AllowSelfRegistration	Hvis en bruger ikke har knyttet mindst én OS2faktor klient til deres NemID/personnummer, og der ikke allerede er registreret en OS2faktor klient på brugeren i AD, så kan man åbne op for muligheden for at brugerne kan selv-registrere den første OS2faktor klient. Hvis denne værdi er sat til ”true”, og en bruger ikke har nogen klient registreret endnu, så vil brugeren i forbindelse med login, have muligheden for at selv-registrere en OS2faktor klient på deres bruger-konto. Dette forudsætter at nedenstående konfiguration ”DeviceIdField” er udfyldt, samt at den servicekonto der kører AD FS servicen har rettigheder til at skrive til denne attribut på brugere i AD.
ApiKey	Denne konfiguration skal udfyldes med API nøglen, der giver adgang til OS2faktor infrastrukturen. Hvis man ikke har en sådan, kontaktes helpdesk@digital-identity.dk for at fremskaffe en.
ConnectorVersion	Denne værdi er udfyldt at installations-softwaren med versionsnummeret på den version af connectoren der anvendes. Undlad at rette i dette felt, da man ellers ikke nemt kan afgøre hvilken version man har installeret.
CprField	Hvis man har personnumre registreret på sine brugere i AD, så kan man her angive hvilken attribut personnummeret er gemt i. Hvis man ikke har personnumre i AD, så sættes denne konfiguration til blank (tom streng). Bemærk at hvis man har valgt en følsom/beskyttet attribut i AD til at gemme personnummeret, så skal den servicekonto der afvikler AD FS servicen, havde adgang til at læse dette felt.
Debug	Hvis denne indstilling sættes til ”true”, så logges alt netværks-kommunikation foretaget af OS2faktor Connectoren. Dette kan være praktisk til fejlsøgning, men ikke nødvendigvis noget man ønsker slået til under normalt drift.
DeviceIdField	Hvis man ikke anvender personnumre til opslag på brugere (og ikke anvender en pseudonym-tabel), så har man brug for at

	kunne registrere brugernes OS2faktor ID'er direkte på brugerne i AD. Denne konfiguration udfyldes med det felt i AD hvor man kan udlæse OS2faktor ID'et på brugerne. Hvis man ønsker at tillade selv-registrering (se "AllowSelfRegistration" indstillingen), så skal denne værdi være udfyldt. Hvis man ikke ønsker at gøre brug af denne funktionalitet, så sættes værdien bare til blank (tom streng).
GetDeviceUrl	Hvis en bruger forsøger at logge på, men ikke har nogen OS2faktor klient, så vises et link til en web-side, hvor brugeren kan læse mere om hvordan de anskaffer sig en OS2faktor klient. Denne indstilling indeholder linket. Default værdien er til OS2faktor infrastrukturen. Hvis man ønsker at havde bedre kontrol over den information som brugerne ser, så kan man pege på en anden (intern) web-adresse her.
InstallPath	Denne værdi udfyldes af installeren, og angiver hvor softwaren er installeret. Undlad af rette i denne værdi.
PidField	Som et alternativt vil at anvende personnumre som opslag, kan man anvende PID'en (Person ID) fra brugernes NemID. Hvis man har disse registreret i sit AD, kan man udpege den attribut hvor værdien er gemt her. Hvis man ikke har dette, sættes denne værdi til blank (tom streng).
PseudonymField	Hvis man ikke har personnumre registreret i AD, men stadig ønsker at gøre brug af NemID/personnummer kobling til OS2faktor, så kan man registrere et pseudonym på alle ens brugere i OS2faktor, og så anvende pseudonymet som opslagsnøgle i stedet. Det mest almindelige scenarie er at man bruger AD-kontonavnet som pseudonum (dvs SAMAccountName). I denne konfigurationsindstilling indtastes den attribut fra AD som man ønsker at anvende som pseudonym (fx SAMAccountName). En forudæstning for at dette har nogen effekt, er at man har en integration til pseudonym-snitfladen kørende (se dokumentationen til pseudonym-snitfladen for flere detaljer). Hvis man ikke ønsker at gøre brug af pseudonym'er, så efterlades denne værdi blank (tom streng).
TrustAllSSLCerts	OS2faktor Connectoren kommunikere med OS2faktor infrastrukturen over HTTPS. Som udgangspunkt vil en Windows Server havde fuld tillid til de SSL certifikater der er opsat på OS2faktor infrastrukturen, men hvis man oplever problemer, kan denne værdi sættes til "true", hvorefter Connectoren ikke foretager validering af SSL certifikatet.
RequirePin	Hvis sat til værdien "true", kan brugerne kun vælge OS2faktor klienter som er beskyttet med pinkode.

Når konfigurationen er tilpasset, skal AD FS servicen genstartes, så den tilpassede konfiguration indlæses.

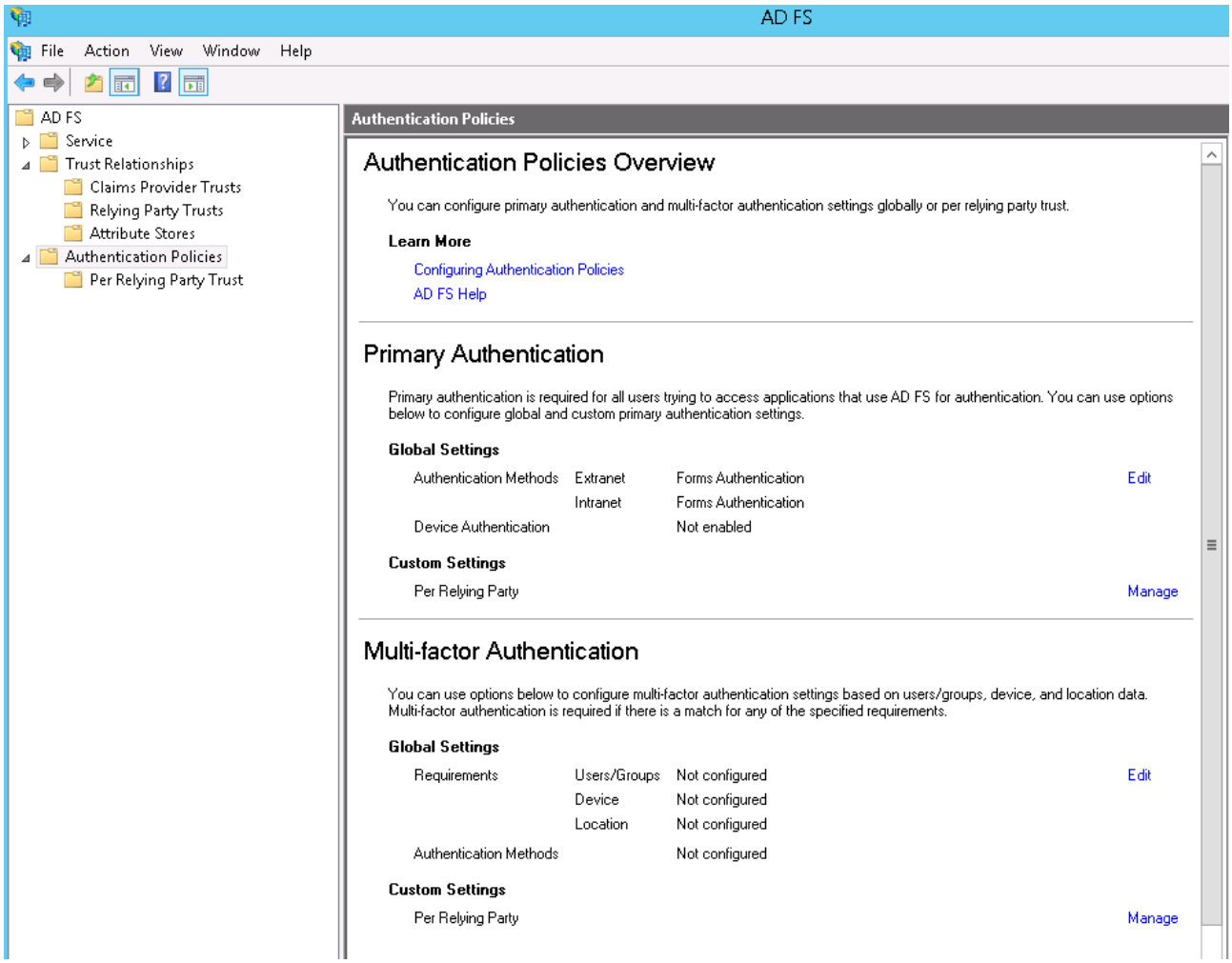
Bemærk at konfigurationen skal foretages på alle servere i AD FS farmen (anvend evt eksport/import fra windows registreringsdatabasen for at lette konfigurationen på de efterfølgende servere)

4.2 AD FS konsollen

OS2faktor Connectoren viderekonfigureres i AD FS konsollen. Denne konfiguration foretages alene på den primære AD FS server i farmen, hvorefter AD FS automatisk distribuere denne konfiguration videre til de andre AD FS servere.

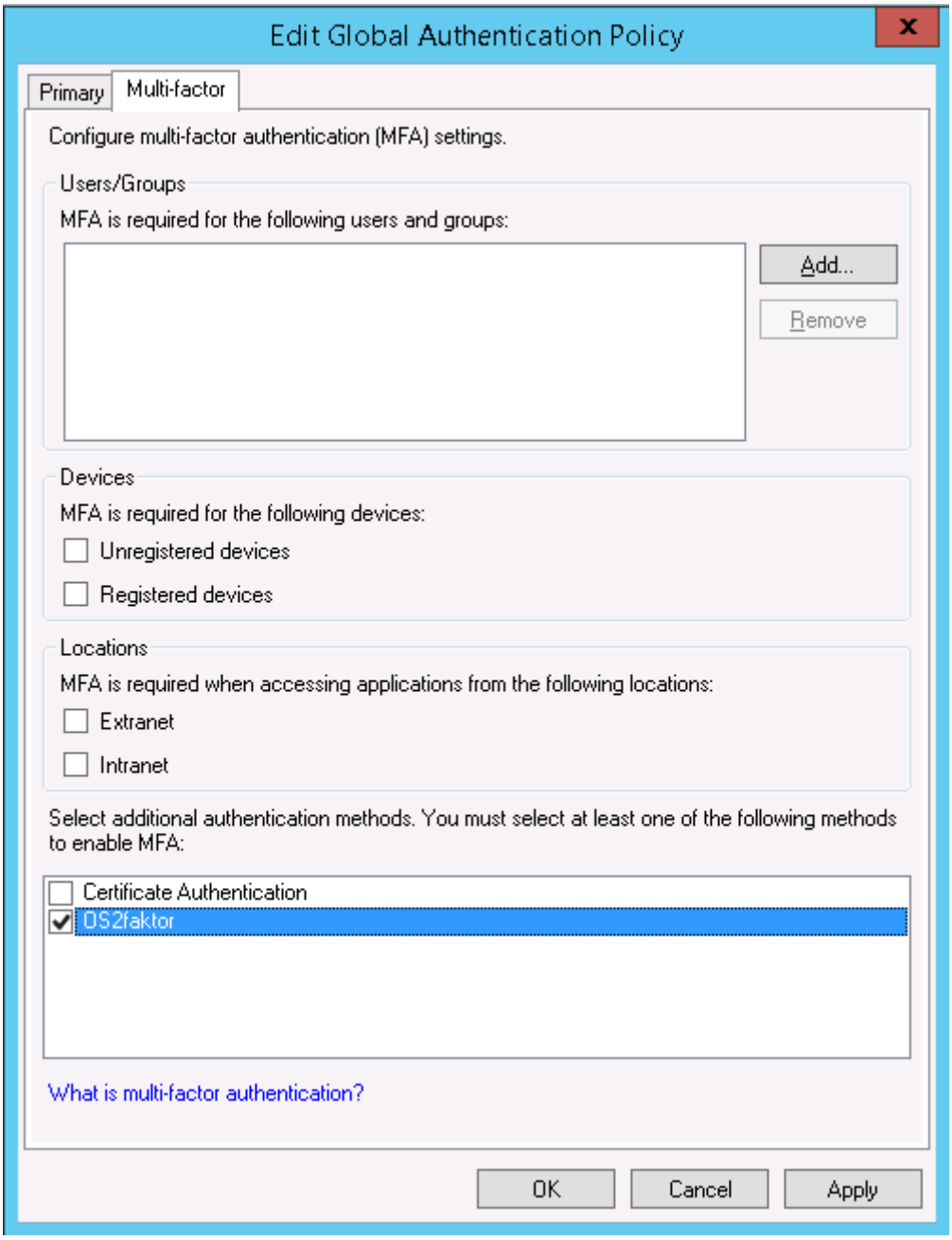
4.2.1 Slå OS2faktor til i AD FS

For at slå OS2faktor til I AD FS, dvs gør den tilgængelig som en "multi-factor authentication" komponent, skal man tilgå menupunktet "Authentication Policies" i venstre menuen, og så klikke på "edit" linket under "global settings" under "multi-factor authentication".



Når man klikker på "edit", åbnes et globalt konfigurationsbillede, der påvirker hele AD FS opsætningen. Med mindre man ønsker at der skal være 2-faktor login på alle fagapplikationer i ens AD FS, så undlades at sætte flueben i nogen af devices/locations kravene. I stedet sættes

bare et flueben ud for ”OS2faktor” som det eneste. Se nedenstående skærmbillede for et eksempel

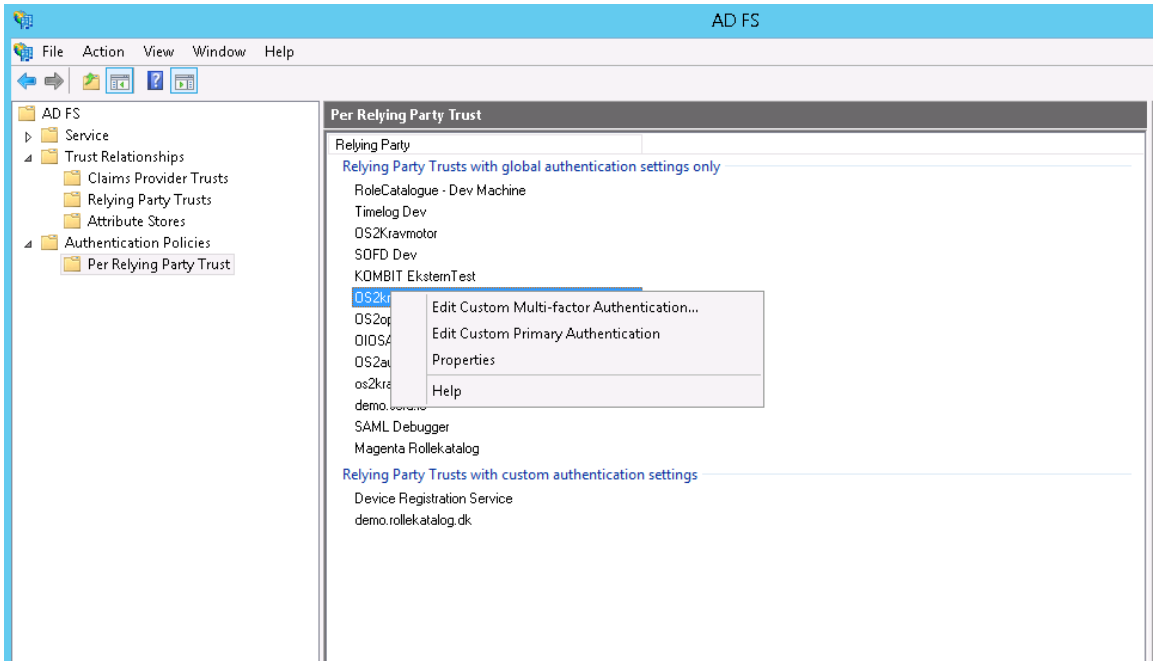


Ved at slå OS2faktor til globalt, kan den anvendes af alle fagapplikationer der ønsker at gøre brug af 2-faktor login. Nogle fagapplikationer efterspørger selv 2-faktor login, og for disse skal man ikke gøre yderligere – de vil nu virke med OS2faktor som login mekanisme.

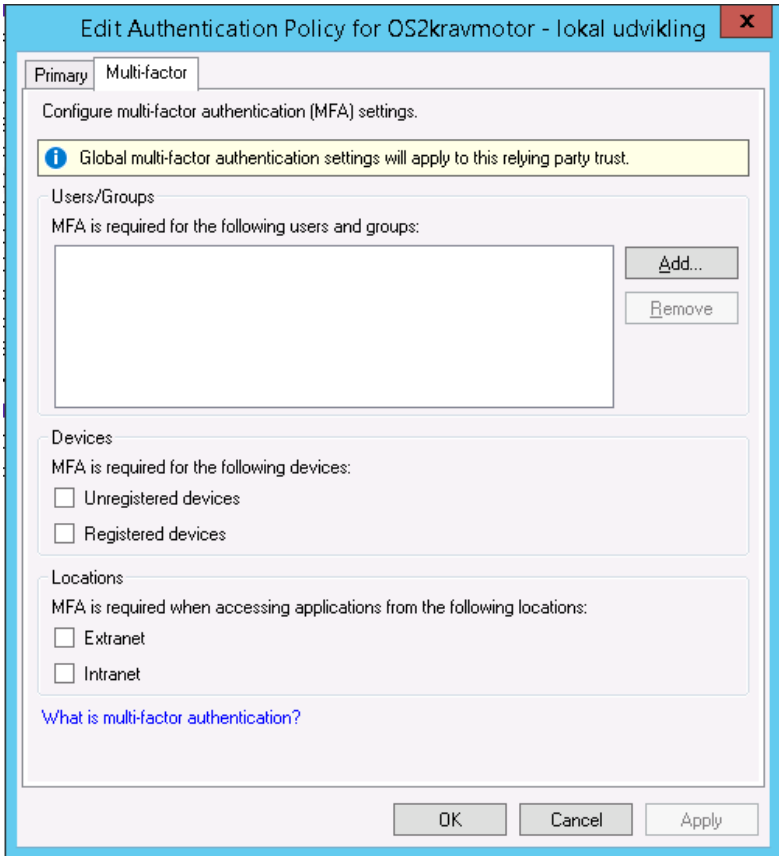
Hvis man har fagapplikationer som man manuelt ønsker at opsætte 2-faktor login til, så gøres det på følgende måde

1. Gå til samme skærmbillede som før, dvs ”Authentication Policies”, men klik i stedet på ”Manage” linket under ”custom settings” i afsnittet om ”Multi-factor authentication”

2. Skærmbilledet der kommer frem har alle relying parties opdelt i 2 afsnit. Dem der følger de globale indstillinger, og der der har tilpassede indstillinger (nederst).
3. Vælg den relying party som det ønskes at 2.faktor login skal slås til for, højreklik på den, og vælg "Edit Custom Multi-factor authentication"



4. I det skærmbillede der kommer frem, vælges hvilke scenarier der kræver 2-faktor login. Man kan både styre om det kun kræves ved login fra internettet, fra ukendte PC'ere eller fra udvalgte bruger-grupper.



På den måde kan man styre præcist hvilke fagapplikationer der kræver 2.faktor login, samt under hvilke forudsætninger at 2.faktor login kræves.

Bemærk at man ikke her konfigurerer hvilke 2.faktor login mekanismer der anvendes. Denne indstilling arves fra de globale indstillinger (hvor vi opsatte at OS2faktor skulle anvendes).

Det er også muligt at anvende flere 2.faktor login løsninger samtidig. I så fald vil brugerne opleve at de skal vælge mellem de forskellige loginløsninger i forbindelse med login.

5 Logfil og fejlsøgning

Der logges til en logfil på c:\logs\os2faktor, hvor man kan se hvis der er opstået nogen fejl i forbindelse med login.

Netværksfejl, opslagsfejl og/eller sikkerhedsfejl vil blive logget i logfilen. Hvis man har problemer under den initielle konfiguration, vil man formodentligt kunne finde årsagen til fejlen i logfilen.

En af de mest almindelige fejl-opsætninger, er API nøglen. Hvis man i logfilen kan se at alle kald til OS2faktor infrastrukturen afvises med fejlbeskeden ”Unauthorized”, så skyldes det at API nøglen er forkert.

Bemærk at konfigurationen ”Debug” bør sættes til ”true” i registreringsdatabasen hvis man fejlsøger, da der så vil være yderligere oplysninger tilgængelig i loggen.