

OS2faktor

AD FS Connector Vejledning

Version: 1.9.0

Date: 16.12.2021

Author: BSG

Indhold

1	Indledning	3
2	Forudsætninger	4
2.1	Connector softwaren.....	4
2.2	API nøgle	4
3	Installation.....	5
4	Konfiguration	6
4.1	Windows registreringsdatabasen	6
4.2	AD FS konsollen	8
4.2.1	Slå OS2faktor til i AD FS	9
5	Logfil og fejlsøgning	13

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

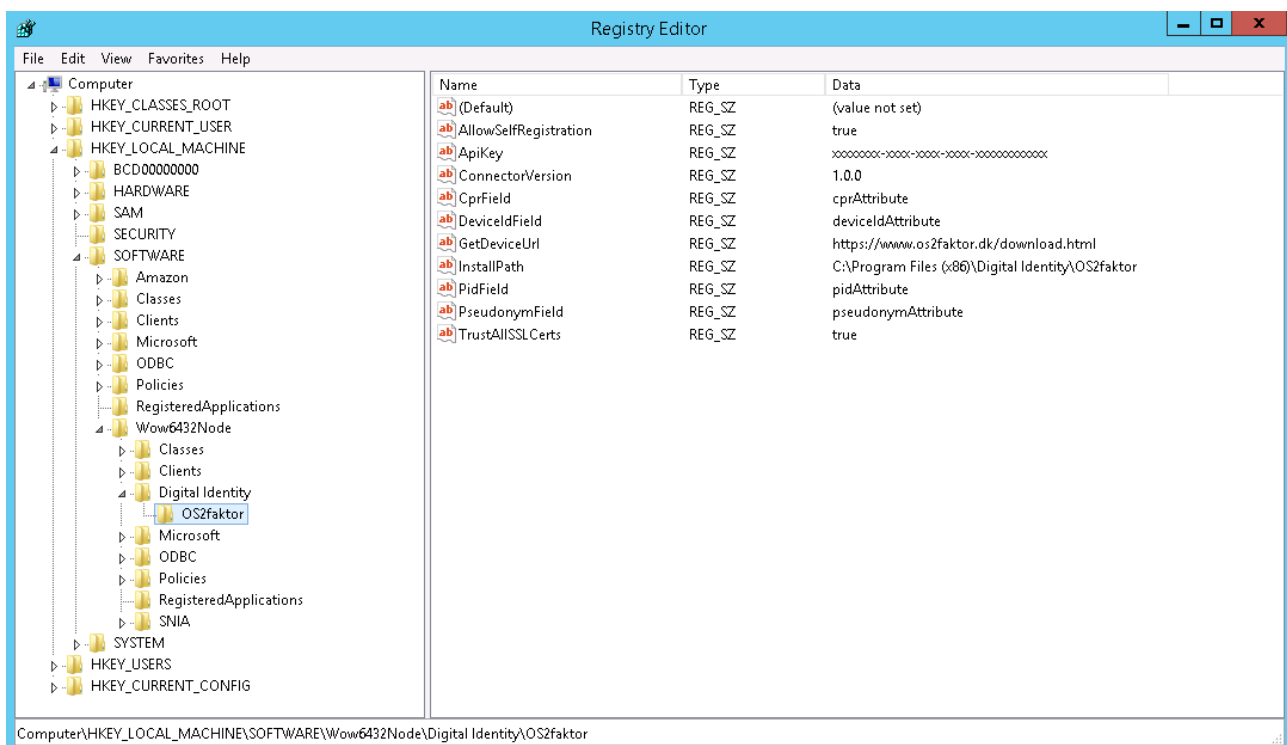
Connectoren distribueres som en MSI installer. Det er vigtigt at softwaren installeres på samtlige servere i AD FS farmen, da der installeres og registreres en række DLL filer.

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 registreringsdatabasen, 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
ApiKey	<p>Denne konfiguration skal udfyldes med API nøglen, der giver adgang til OS2faktor infrastrukturen.</p> <p>Hvis man ikke har en sådan, kontaktes helpdesk@digital-identity.dk for at fremskaffe en.</p>
ConnectorVersion	<p>Denne værdi er udfyldt af 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.</p>
CprField	<p>Hvis man har personnumre registreret på sine brugere i AD, så kan man her angive hvilken attribut personnummeret er gemt i.</p> <p>Hvis man ikke har personnumre i AD, så sættes denne konfiguration til blank (tom streng).</p> <p>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, have adgang til at læse dette felt.</p>
Debug	<p>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.</p>
GetDeviceUrl	<p>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.</p> <p>Denne indstilling indeholder linket. Default værdien er til OS2faktor infrastrukturen. Hvis man ønsker at have bedre kontrol over den information som brugerne ser, så kan man pege på en anden (intern) web-adresse her.</p>
InstallPath	<p>Denne værdi udfyldes af installeren, og angiver hvor softwaren er installeret. Undlad af rette i denne værdi.</p>
TrustAllSSLCerts	<p>OS2faktor Connectoren kommunikerer med OS2faktor infrastrukturen over HTTPS. Som udgangspunkt vil en</p>

	<p>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.</p>
<p>ConnectionString</p>	<p>Hvis man ikke har brugernes CPR nummer i Active Directory, men i stedet en i SQL database, så kan man udfylde denne konfigurationsindstilling med en ConnectionString, der peger på den SQL Server hvor CPR numrene ligger</p> <p>ConnectionString skal enten udfyldes med et SQL brugernavn/kodeord, eller den servicekonto der afvikler AD FS skal have adgang til SQL Serveren.</p> <p>Eksempel med brugernavn/kodeord Server=myServerAddress; Database=myDatabase; UserId=myUsername; Password=myPassword;</p> <p>Eksempel med brug af AD FS servicekontoens rettigheder Server=myServerAddress; Database=myDatabase; Integrated Security=True;</p>
<p>SQL</p>	<p>Hvis man har udfyldt ConnectionString ovenfor, så skal der også udfyldes den SQL kommando der skal bruges til at lave opslaget på databasen.</p> <p>Input til queriet er sAMAccountName, og output skal være et CPR nummer i et felt ved navn 'ssn'. Man kan bruge "AS" keywordet til at rename output kolonnen som vist i eksemplet nedenfor</p> <p>Eksempel Hvis der findes en tabel i databasen ved navn "cprnumre", og den har en kolonne ved navn "brugerid", der indeholder sAMAccountName, og en anden kolonnen ved navn "personnummer" der indeholder CPR numemret, så skal SQL kommandoen se sådan her ud</p> <pre>SELECT personsnummer AS ssn FROM cprnumre WHERE brugerid = {sAMAccountName}</pre>
<p>CprWebservice</p>	<p>Hvis man har medarbejdernes CPR numre liggende i et eksternt system, hvor der er udstillet en REST service til opslag vha sAMAccountName, så kan man konfigurere OS2faktor til at bruge webservicen i stedet for at lave opslag i AD.</p> <p>Denne indstilling skal udfyldes med adressen på REST servicen, samt den parameter som skal indeholde sAMAccountName.</p> <p>Eksempel Hvis man har en webservice, hvor man kan finde CPR nummeret på brugeren 'bsg' ved dette kald</p>

	<p>https://minservice/cprLookup?userId=bsg</p> <p>Så skal man konfigurere følgende i denne indstilling</p> <p>https://minservice/cprLookup?userId={sAMAccountName}</p> <p>Forventet output</p> <p>Servicen skal returnere et JSON struktureret payload, der som minimum skal indeholde følgende struktur</p> <pre>{ "result": "xxxxxxxxxxxxx" }</pre> <p>Hvor x'erne er CPR nummeret. Der må gerne være flere data i svaret, disse vil blot blive ignoreret. Men CPR nummeret skal være til stede, og ligge i feltet "result".</p>
RememberDeviceAllowed	<p>Hvis man ønsker at brugerne kun skal bruge MFA hvert x. dag, så kan man slå denne funktion til ved at sætte den til "true".</p> <p>Det er også nødvendigt at udfylde nedenstående 3 indstillinger for at denne funktion fungerer</p>
RememberDeviceDays	<p>Sættes til det antal dage som der skal gå mellem at man skal bruge MFA</p>
RememberDeviceRelyingParties	<p>Dette er en multi-valued værdi, og her kan man angive hvilke Relying Parties som funktionen skal være slået til på. Hvis listen er tom er den ikke slået til for nogen.</p> <p>De værdier man skal indtaste er "Identifier" på de Relying Parties som man ønsker at tillade at MFA kun bruges hver x'ende dag. Dette findes inde i AD FS konsollen ved at gå til egenskaber for en given Relying Party, og så kigge på fanen Identifiers.</p>
HmacKey	<p>Denne værdi skal udfyldes med en hemmelig kode. Koden bruges til at signere de "husk mig" tokens som udstedes til browseren, så den kan huske MFA login'et.</p> <p>Det anbefales at bruge en stærk nøgle, fx et tilfældig valgt UUID eller lignende.</p>

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

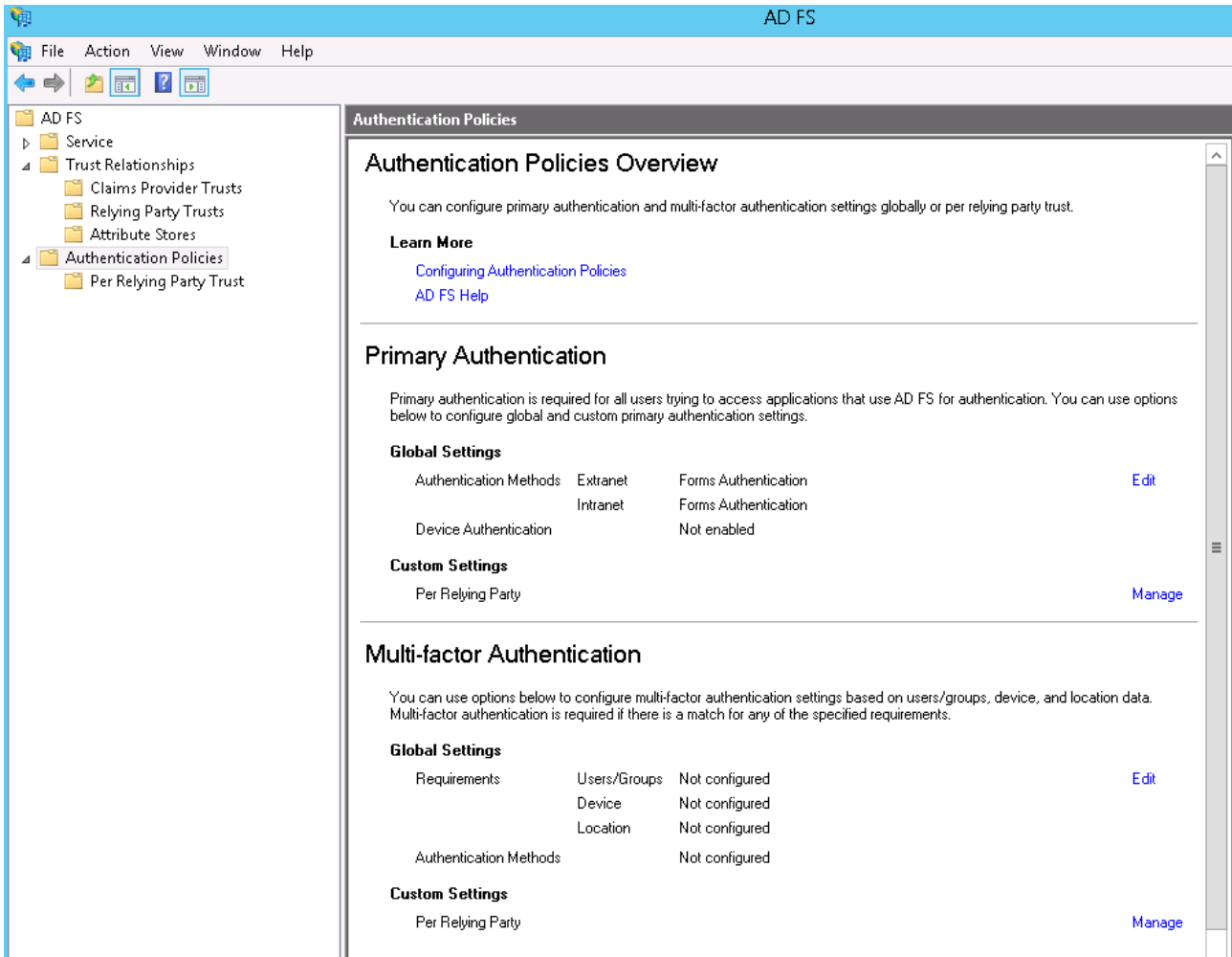
Bemærk at konfigurationen skal foretages på alle servere i AD FS farmen (anvend evt eksport/import fra windows registreringsdatabasen for at lette konfigurationen på de efterfølgende servere)

4.2 AD FS konsollen

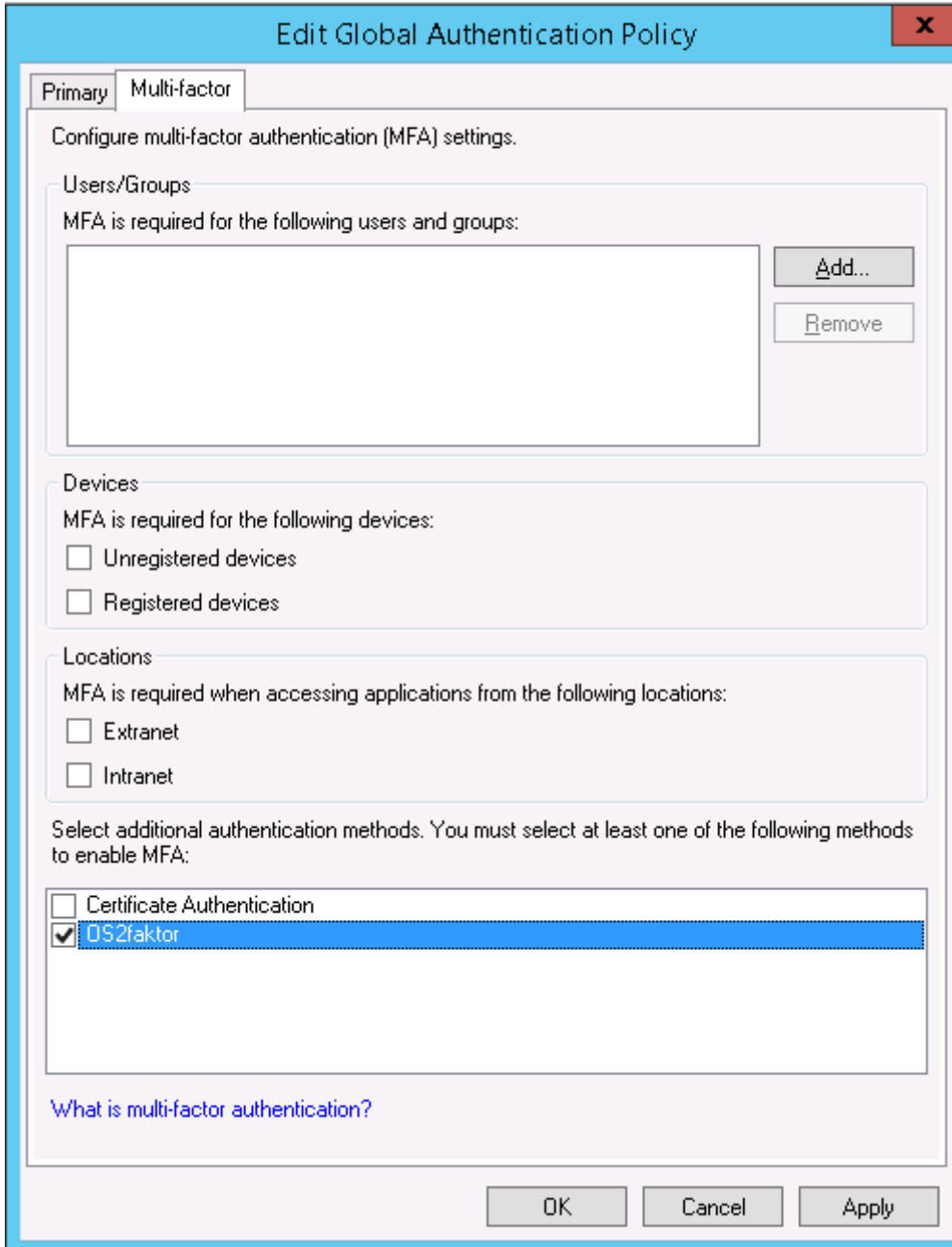
OS2faktor Connectoren viderekonfigureres i AD FS konsollen. Denne konfiguration foretages alene på den primære AD FS server i farmen, hvorefter AD FS automatisk distribuere denne konfiguration videre til de andre AD FS servere.

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



Edit Global Authentication Policy ✕

Primary **Multi-factor**

Configure multi-factor authentication (MFA) settings.

Users/Groups
MFA is required for the following users and groups:

Devices
MFA is required for the following devices:

Unregistered devices
 Registered devices

Locations
MFA is required when accessing applications from the following locations:

Extranet
 Intranet

Select additional authentication methods. You must select at least one of the following methods to enable MFA:

Certificate Authentication

OS2faktor

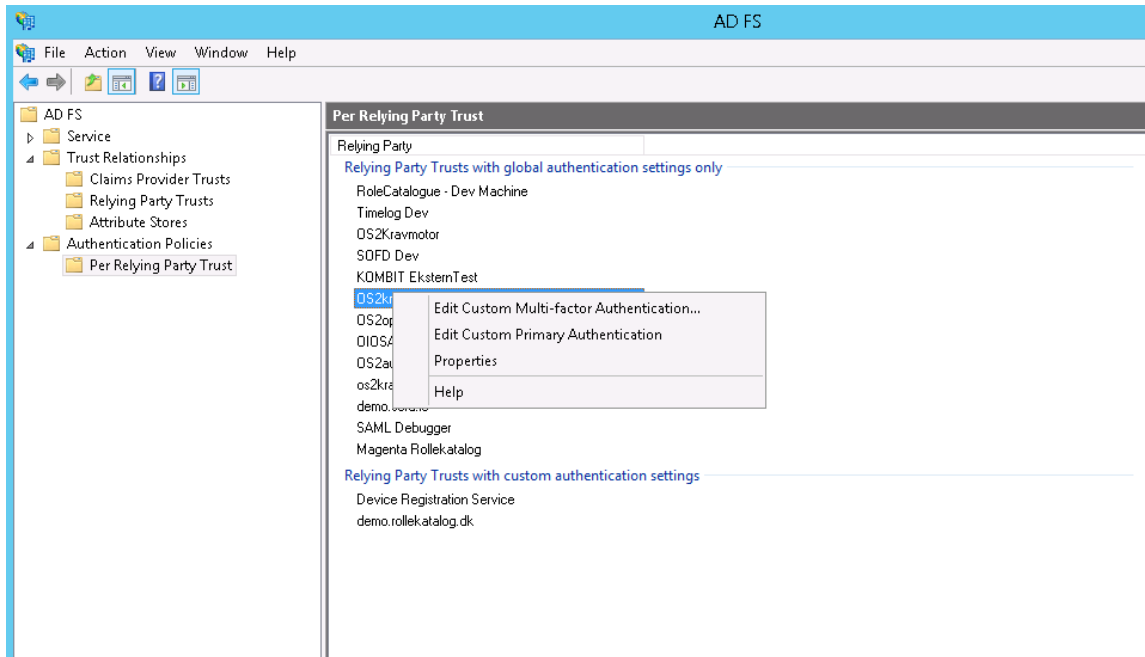
[What is multi-factor authentication?](#)

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.

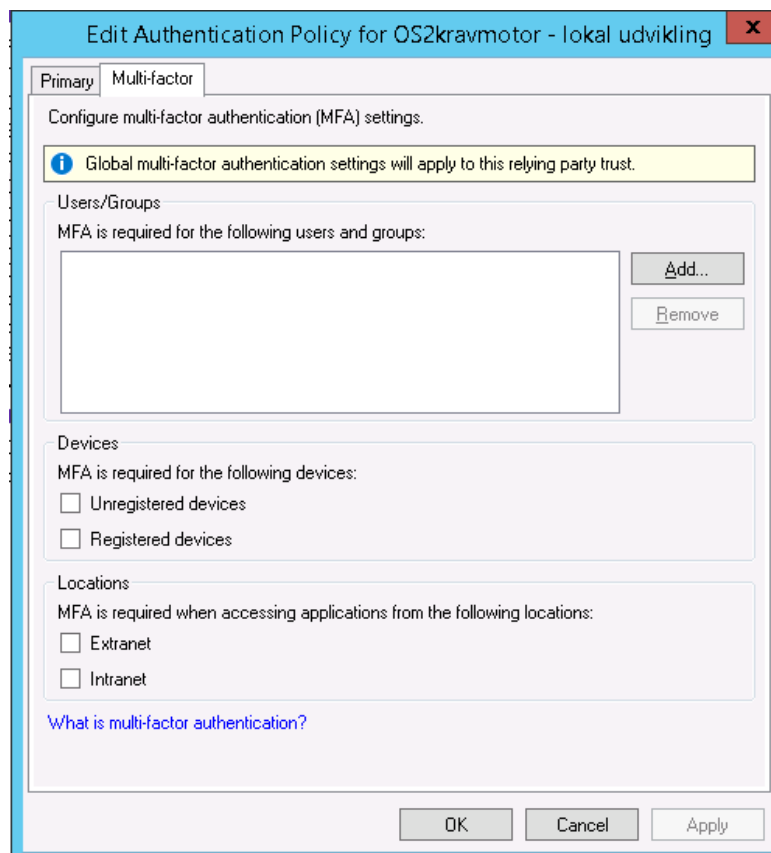
Hvis man har fagapplikationer som man manuelt ønsker at opsætte 2-faktor login til, så gøres det på følgende måde

1. Gå til samme skærbillede som før, dvs "Authentication Policies", men klik i stedet på "Manage" linket under "custom settings" i afsnittet om "Multi-factor authentication"
2. Skærbilledet 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 skærbillede 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 initiale 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.