eKlient Edge Chromium 1.4

inera

Innehållsförteckning

Revisionshistorik

Ansvarig	Version	Datum
Jörgen Nilsson	1.0	20200127
Jörgen Nilsson	1.1	20200421
Sassan Fanai	1.3	20211111
Sassan Fanai	1.4	20230627

Bakgrund

Syftet med detta dokument är att beskriva hur man bör konfigurera Edge Chromium för att säkra upp denna. Nya Edge Chromium baserar sig på OpenSource Projektet Chromium (https://www.chromium.org/) precis som Google Chrome. Kompatibiliteten med hemsidor räknas med att vara hög eftersom det är samma renderingsmotor som används.

Om man inte aktivt gör någonting, exempelvis hindrar Edge Chromium från att köras på klienterna med Applocker eller med en Group policy så kan användarna själva installera Edge Chromium i sina profiler och använda detta okontrollerat. Detta scenario är inget vi rekommenderar med tanke på alla sårbarheter, botnät och malware som tråkigt nog existerar i Extensions med mera som är samma för Edge Chromium som de är för Google Chrome då båda webbläsarna baseras på Chromium.

När man installerar den officiella versionen av Edge Chromium så byter den ut alla genvägar, taskbar ikoner med mera automatiskt och döljer den ”gamla” Edge som standard.

De rekommenderade inställningarna skall ses som en rekommendation, lokala anpassningar kommer att behöva göras samt måste beslut tas om hur mycket man vill stänga ned Edge Chromium, ska det till exempel tillåtas synk av favoriter med mera till privata Microsoft konto eller till AzureAD konton (kräver Azure AD Premium). Ju mer vi låser ned ju fler saker kommer att sluta fungera och man behöver då förstå hur det påverkar användarupplevelsen.

Att ha en uppdateringsstrategi är otroligt viktigt det med, installerar man Edge Chromium med den inbyggda funktionen som finns i Configuration Manager 1910 stänger den automatiskt av automatiska uppdateringar och dessa måste då skötas via Configuration Manager. Under den första veckan efter att Edge Chromium släpptes har 3 uppdateringar släppts.

Automatiska uppdateringar är tilltalande men har nackdelar som att uppdateringarna i sig laddas ned direkt från Internet på alla datorer (DO stöds dock) samt att det kan ju vara bra att kunna testa Major versions av Edge med innan man uppgraderar dem ute.

Övergripande

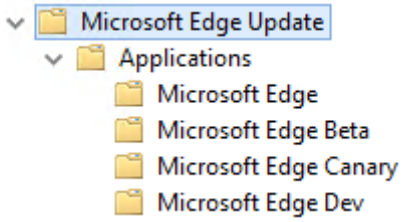
Eftersom Edge Chromium bygger på Project Chromium (https://www.chromium.org/) är alla inställningar snarlika de som finns i Google Chrome. Rekommendationerna i detta dokument är baserade på samma inställningar som eKlient använde när vi tog fram inställningar för Google Chrome. De stora funktionella skillnaderna är exempelvis IEMode, hantering av profiler och synkronisering av inställningar. Den första versionen som släpptes var version 79.

Automatiska Uppdateringar

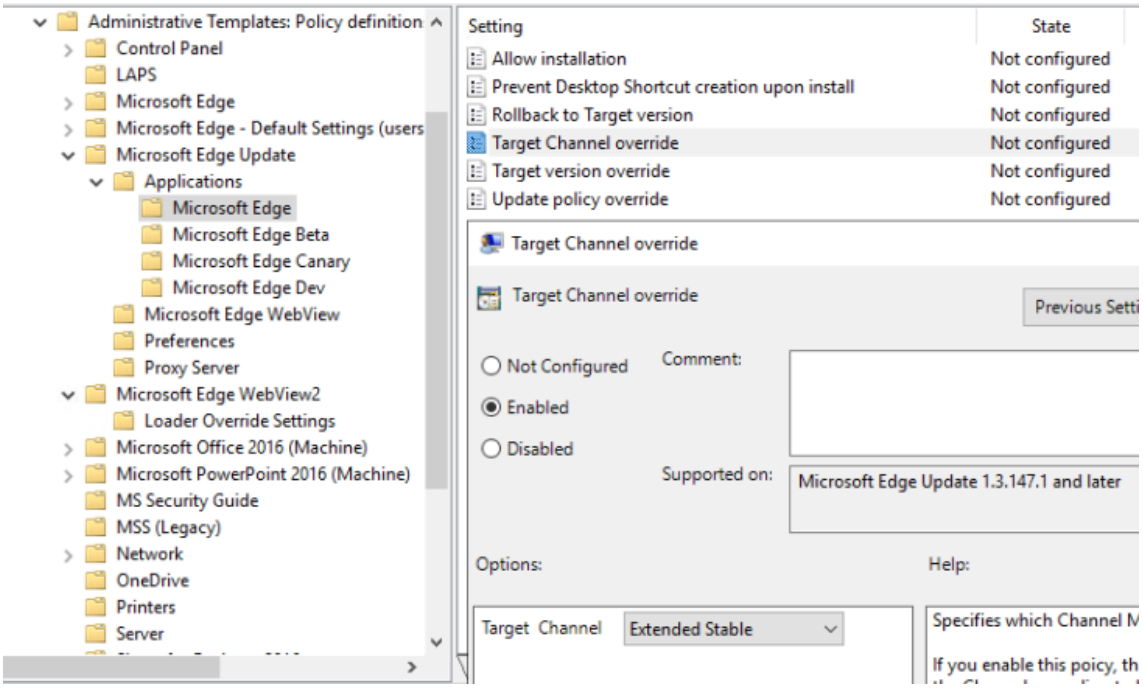
Edge Chromium använder sig av automatiska uppdateringar som standard om man inte aktivt stänger av dessa, detta görs förslagsvis med en Group Policy så att man får kontroll över uppdateringarna. Sköter man det med Configuration Manager får man följande fördelar:

- Nedladdning av uppdatering kommer att ske från en distributionspunkt eller med Peering om man har konfigurerat det.
- Kontroll över vilken version som används, speciellt ”major versions”.
- Rapportering

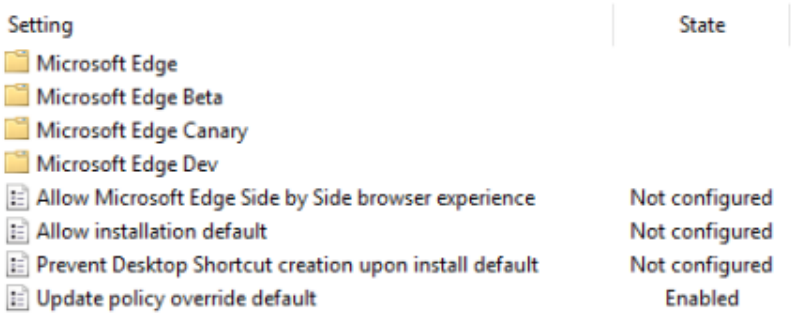
Eftersom Edge levereras i flera ”kanaler” Dev, Beta, Canary, Stable och Extended Stable kan man styra individuellt hur dessa skall uppdateras / tillåtas att installeras.



Till skillnad från kanalerna Stable, Beta, Dev och Canaray är Extended Stable inte tillgänglig som en fristående Edge version. Extended Stable kan konfigureras genom GPO inställningen ”Target Channel override”



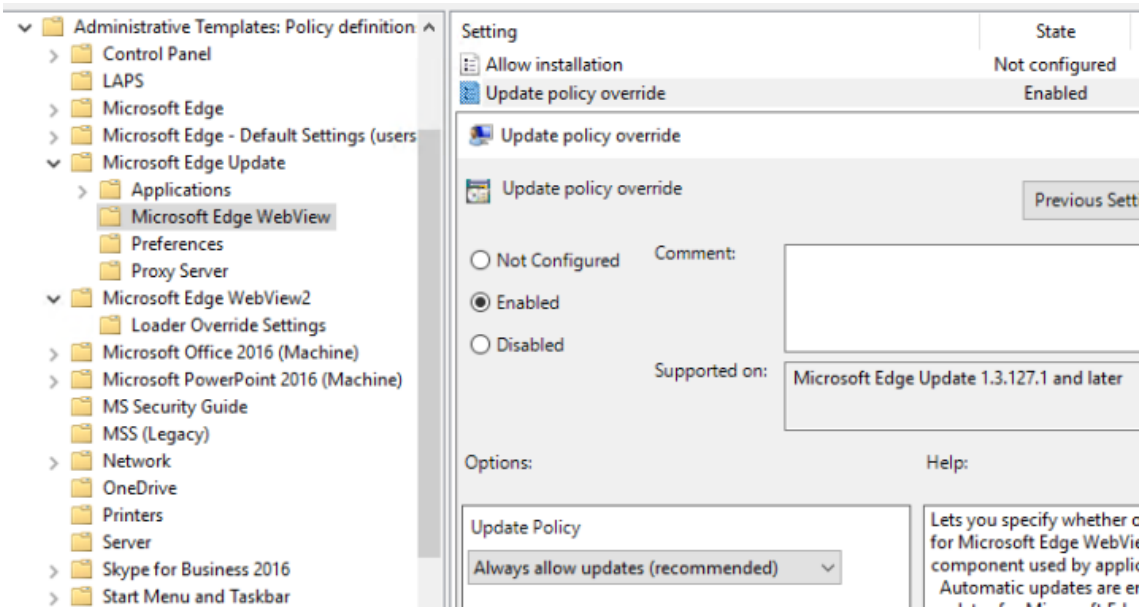
eKlient inaktiverar automatiska uppdateringar i tillhörande GPO, då vi utgår ifrån att uppdateringar sköts via MECM för mer kontroll. Väljer man en annan uppdateringsstrategi kan inställningen behöva ändras.



WebView2

Edge WebView2 använder samma uppdateringsmekanism som Edge och som standard används samma (GPO) uppdateringinställningar för WebView2 som konfigurerats för Edge. Det innebär att automatiska uppdateringar för WebView2 också inaktiveras ifall GPO inställningen ”Update policy ovverride default” används för att inaktivera automatiska uppdateringar för Edge. Det går

dock att konfigurera WebView2 uppdateringar separat via GPO inställningen ”Update Policy Override”.



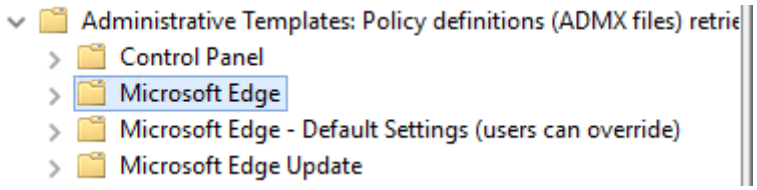
Det är därför viktigt att oavsett scenario också ha en uppdateringsstrategi för WebView2 där man antingen tillåter automatiska uppdateringar eller inkludera dessa i sina Automatic Deployment Rules (ADR) i MECM.

Group Policy

Det behövs nya policy filer för Edge Chromium, dessa är inte en del av Windows 10, åtminstone inte ännu. De kan laddas ned härifrån.

https://www.microsoft.com/en-us/edge/business/download

Kopiera sedan in .ADMX filen och de kataloger med språkstöd som behövs i eran miljö till den centrala Policydefinitions katalogen. När detta är gjort finns Edge och Edge Update listat under Windows Components både för användare och datorer.

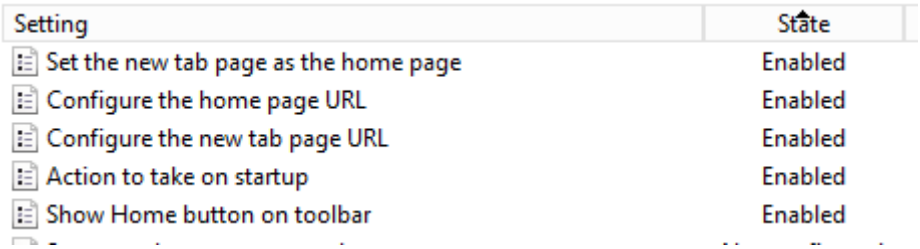


Man kan välja att sätta standardinställningar som användaren kan ändra eller göra alla inställningar tvingande.

Eftersom vi vill hålla så mycket som möjligt av konfiguration riktad till vilken dator användarna loggar in på så gör vi alla inställningarna per dator samt tvingande eftersom de flesta av inställningarna är säkerhetsinställningar.

Startsida

För att konfigurera startsidan behöver både ”hem” och ”ny flik” konfigureras, den ena med en lista över de URL:er som skall öppnas vid start, den andra innehållande den URL som skall öppnas. Inställningar är även med för att aktivera Hem-knappen och vilken URL den skall gå till.



InPrivate mode / Gäst Profil

”InPrivate mode” har diskuterats fram och tillbaka och det är en svår avvägning mellan användarvänlighet och säkerhet. Rekommendationerna från guiderna som vi hänvisar till nedan samt alla säkerhetskrav som finns är att det inte skall vara tillåtet med InPrivate mode. Detta för att göra en forensisk undersökning möjligt vid exempelvis virus-angrepp eller intrångsförsök.

Det finns även en gästprofil vilken ger samma möjlighet som InPrivate, d.v.s. användaren kan skapa en gästprofil, göra det man vill och sedan stänga ner webbläsaren vilket resulterar i all historik försvinner. Har man inget behov av InPrivate så bör denna funktion med stängas av.

Profiler

Profiler gör det möjligt att ha olika profiler där varje profil har egna cookies, favoriter med mera. Detta gör att man kan ha en privat profil och en arbetsprofil till exempel man kan vara inloggad mot molntjänster med olika konton i de olika profilerna. Denna funktionalitet minskar behovet av InPrivate eftersom användarna istället kan skapa en ny profil med olika konton. Varje profil kan individuellt synkronisera sina inställningar mot Microsoft Cloud. Det man får tänka på är att använda profiler gör det även möjligt att kringgå eventuella krav som finns på att spara historik med mera eftersom en användare helt enkelt kan radera sin profil och då är all historik borta. Det går i dagsläget inte att blockera profilskapandet fullt ut.

Javascript

Javascript rekommenderas det i de flesta guider att man stänger av eller begränsar. Det är svårt att göra en generell rekommendation gällande Javascript eftersom det används så flitigt och stänger man av det så kan väldigt mycket sluta att fungera.

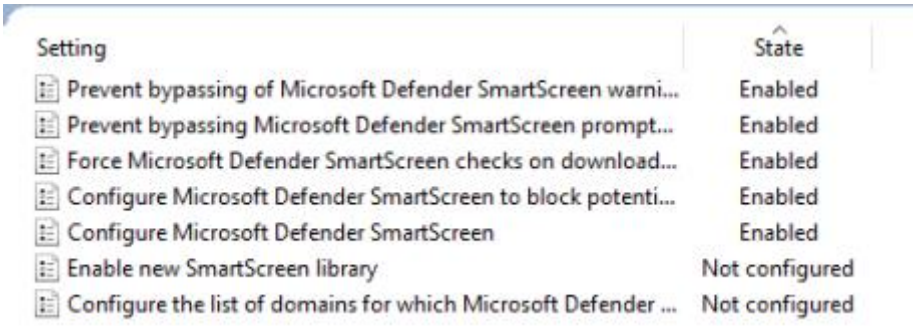
Cookies

Att inte tillåta Cookies eller alternativt blockera/tillåta vissa adresser innebär även det väldigt mycket arbete och är inte direkt användarvänligt. Det går att genomföra om behov finns.

SmartScreen

SmartScreen är Microsoft motsvarighet till Safe Browsing i Google Chrome. SmartScreen bör absolut vara aktiverat eftersom det kan blockera siter med skadlig kod eller siter kända för nätfiske.

Följande rekommenderas att konfigureras för SmartScreen.



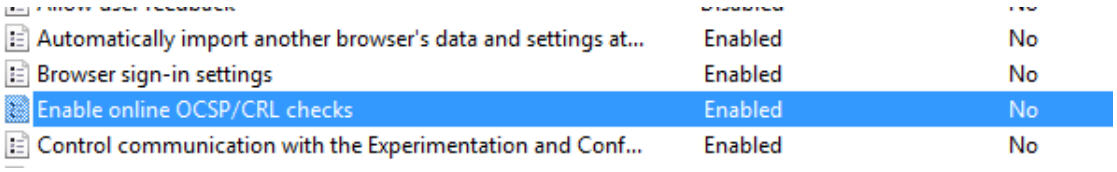
CRLSets

Som standard så kontrollerar varken Google Chrome eller Edge Chromium några CRL:er (Certificate revocation list), utan de har en egen hantering av detta.

Mer information finns här:

http://dev.chromium.org/Home/chromium-security/crlsets

Vi rekommenderar att man slår på CRL list kontroller med följande inställning.

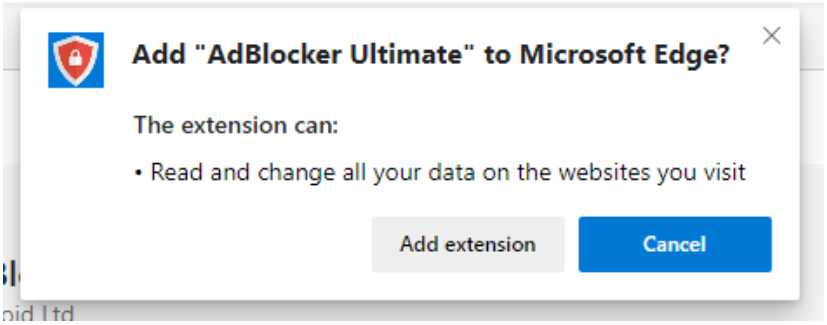


Notera att ”Enable online OSCP/CRL checks” utför så kallad ”soft-fail” kontroll, det vill säga om OSCP/CRL inte är nåbar så kommer certifikatet att ses som giltigt.

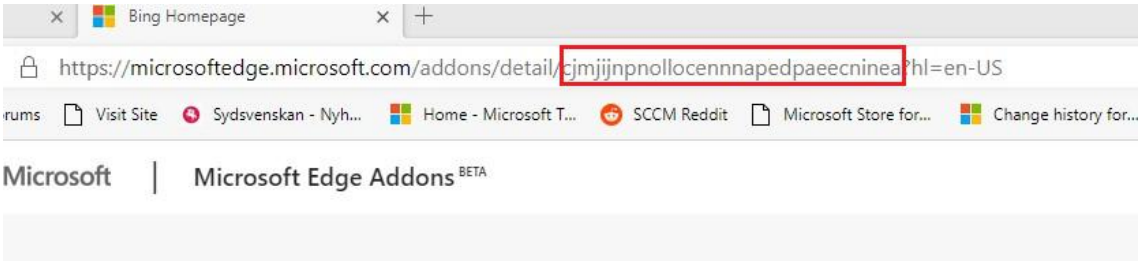
Inställningen ”Specify if online OCSP/CRL checks are required for local trust anchors” är numera inte aktiverad i tillhörande GPO då den till skillnad från inställningen ovan utför en så kallad ”hard-fail” kontroll vilket innebär att certifikat ses om ogiltiga om revokeringsservern inte är nåbar. Ur ett säkerhetsperspektiv bör den här inställningen testas och aktiveras där det är möjligt. Eftersom inställningen kan ställa till problem i scenarion där klienter av olika anledningar inte kan nå revokeringsservern har vi valt att inaktivera den i tillhörande GPO.

Extensions / tillägg

Rekommendationen från alla referenser inklusive Microsofts egna Baselines är att inte tillåta användandet av tillägg eftersom de får tillgång till allting du gör i webbläsaren vilket är ett stort problem för informationsskydd. Eftersom tilläggen för Edge Chromium är samma som för Google Chrome är där samma sårbarheter och ”malicious” tillägg tillgängliga som det har varit upprepade incidenter med.

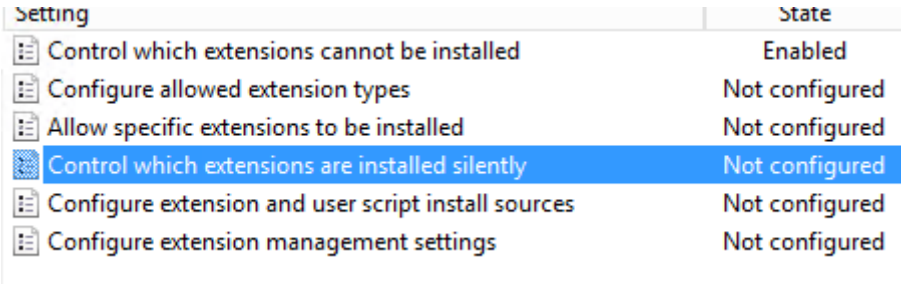


I dessa inställningar stänger vi av alla tillägg med en Group Policy och sedan kan man vitlista de man vill tillåta. Att tillåta tillägg görs med hjälp av ett ExtensionID tillsammans med en Group Policy inställning. ExtensionID hittas i URL:en till tillägget som finns i ”butiken” se nedan.



Installera tillägg automatiskt

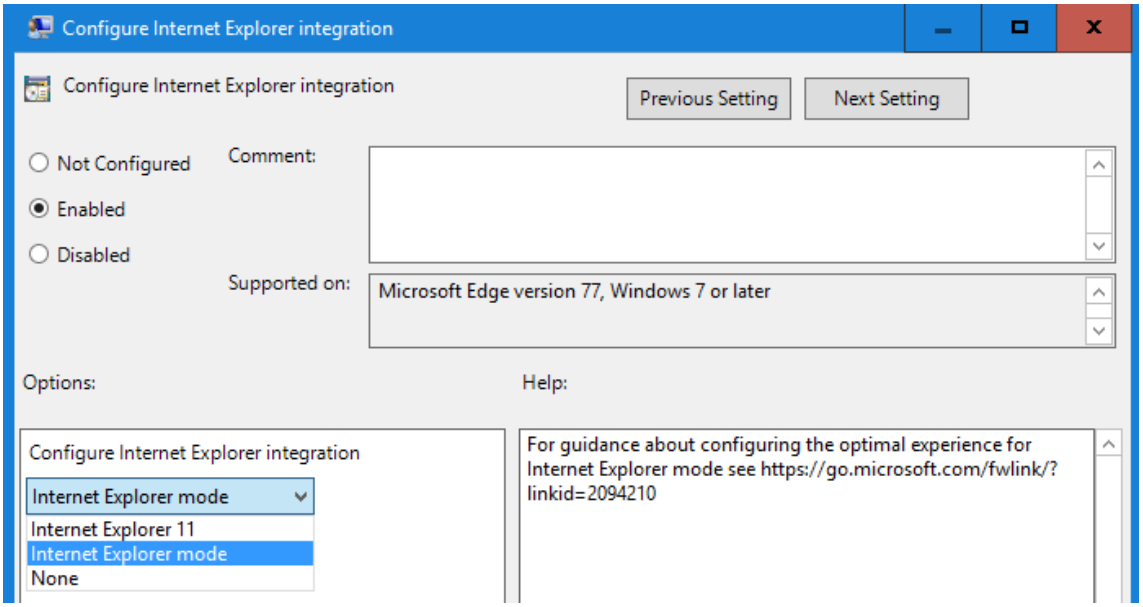
Samma ExtensionID som angavs ovan används här för att installera ett tillägg automatiskt. Behovet av detta är mindre än det var för Google Chrome eftersom SSO mot AzureAD är inbyggt precis som IE11 kompatibilitetsläget.



Vill man ha mer kontroll över distribuering och installation av tillägg så kan dessa även paketeras och skickas ut som ett system via SysMan. eKlient tillhandahåller exempel på wrapper (skapad med WrapperKing) som enkelt kan användas för att paketera Edge tillägg som system/applikation för installation via SysMan.

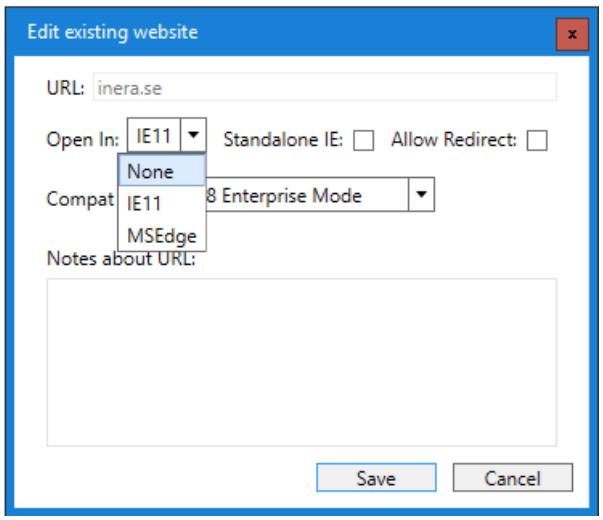
IEMode

IEMode är en av de nya riktigt bra funktionerna, istället för att automatiskt öppna Internet Explorer för sidor som kräver det så kan vi använda samma Enterprise Site Mode list fil som innan men aktivera IEMode. Med IEMode så öppnas sidorna i samma browser, den byter bara renderingsmotor. Detta ger en mycket bättre användarupplevelse än tidigare och tester får utröna om vi äntligen kan slippa Adobe Reader som en Core app i samband med detta.



Neutral sites i IE Site Modelist

”Neutral sites” är exempelvis ADFS som används för autentisering och som inte skall skickas till antingen IE eller Edge. För att detta skall fungera måste man uppgradera till Enterprise Site Mode List manager v.11 eller senare.



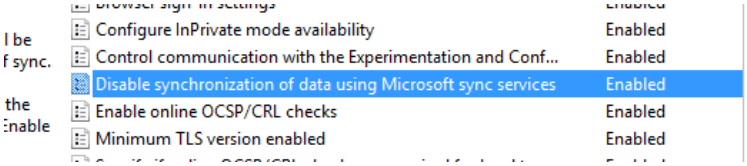
Synkronisering av inställningar

Synkronisering av inställningar konfigureras per profil. Det krävs antingen ett Microsoft konto eller ett Azure AD konto i en tenant med Azure AD Premium för att detta ska fungera.

För AzureAD konton används funktionen för att synkronisera inställningarna som då krypteras med Azure Information Protection automatiskt utan att det krävs någon konfiguration, det är samma funktion som används för att synkronisera inställningar i Windows med AzureAD Premium.

Att synkronisera eller inte är ju en fråga om vad man tillåter att information synkroniseras med och hur man klassar den synkroniserade informationen. Synkronisering av lösenord rekommenderas inte av någon säkerhetsinstans, Microsoft har även med den rekommendationen i sina Security Baselines för Edge.

Man kan dock konfigurera så att kontot som används måste ha exempelvis @inera.se som UPN och på så vis styra vart informationen får synkroniseras.



Inställningar

Följande GPO inställningar är gjorda:

Lokation	Inställning	Värde	Värde	Kommentar
Microsoft Edge	Allow unconfigured sites to be reloaded in Internet Explorer mode	Disabled		MS Baseline
	Allow user feedback	Disabled		STIG Medium, GDPR Privacy
	Allow users to proceed from the HTTPS warning page	Disabled		MS Baseline, Från ett säkerhetsperspektiv en självklar inställning men ur användbarhetsperspektiv svår.
	Always open PDF files externally	Enabled		Användarupplevelse, Beror på om Adobe Reader skall användas eller ej.
	Automatically import another browser's data and settings at first run	Enabled	Automatically imports all supported datatypes and settings from the default browser	Användarupplevelse. Bör anpassas efter vilken browser man använder som standard
	Browser Sign-in settings	Enabled	Enable Browser sign-in	Användarupplevelse, Anpassas efter behov och strategi
	Configure InPrivate mode availability	Enabled	InPrivate mode disabled	STIG Medium, För forensik syfte
	Continue running background apps after Microsoft Edge closes	Disabled		STIG Medium
	Control communication with the	Enabled	Retrieve configurations only	Tvinga standard inställning

	Experimentation and Configuration Service			
	Disable synchronization of data using Microsoft sync services	Enabled		Stänger av synkning med Microsoft Cloud går i nuläget inte att styra till endast Azure AD konto
	Enable AutoFill for payment instruments	Disabled		STIG Medium, GDPR Privacy
	Enable browser legacy extension point blocking	Enabled		MS Baseline
	Enable deleting browser and download history	Disabled		STIG Medium, För förensik syfte
	Enable guest mode	Disabled		STIG Medium, För forensik syfte
	Enable online OCSP/CRL checks	Enabled		STIG Medium
	Enable site isolation for every site	Enabled		MS Baseline
	Enhance images enabled	Disabled		MS Baseline
	Force WebSQL to be enabled	Disabled		MS Baseline
	Enable profile creation from the Identity flyout menu or the Settings page	Disabled		Hindrar skapandet av flera profiler, ur syfte forensik eftersom dessa kan tas bort med och all historik med den.
	Hide the First-run experience and splash screen	Enabled		Användarupplevelse

	Show the Reload in Internet Explorer mode button in the toolbar	Disabled		MS Baseline
	Specifies whether SharedArrayBuffers can be used in a non cross-origin-isolated context	Disabled		MS Baseline
	Spell checking provided by Microsoft Editor	Disabled		Privacy
Microsoft Edge Update/Applications	Update policy override default	Enabled	Updates disabled	Beror på vilken uppdateringsstrategi man har valt.
Microsoft Edge/Default search provider	Default search provider search URL	Enabled	{google:baseURL}search?q={searchTerms}&{google:RLZ}{google:originalQueryForSuggestion}{google:assistedQueryStats}{google:searchFieldtrialParameter}{google:searchClient}{google:sourceId}ie={inputEncoding}	Användarupplevelse, Google
	Default search provider URL for suggestions	Enabled	{google:baseURL}complete/search?output=chrome&q={searchTerms}	Användarupplevelse, Google
	Enable the default search provider	Enabled		Användarupplevelse, Google
Microsoft Edge/Extensions	Control which extensions cannot be installed	Enabled	*	MS Baseline, Blockerar alla extensions
Microsoft Edge/HTTP authentication	Allow Basic authentication for HTTP	Disabled		MS Baseline
	Supported authentication schemes	Enabled	ntlm,negotiate	MS Baseline

Microsoft Edge/Native Messaging	Allow user-level native messaging hosts (installed without admin permissions)	Disabled		MS Baseline
Microsoft Edge/Password manager and protection	Enable saving passwords to the password manager	Disabled		Ändrad till Not Configured i MS Baseline v114. Beroende på strategi.
Microsoft Edge\Private Network Request Settings	Specifies whether to allow insecure websites to make requests to more-private network endpoints	Disabled		MS Baseline
Microsoft Edge/SmartScreen settings	Configure Microsoft Defender SmartScreen	Enabled		MS Baseline
	Configure Microsoft Defender SmartScreen to block potentially unwanted apps	Enabled		STIG Medium, Säkerhet
	Force Microsoft Defender SmartScreen checks on downloads from trusted sources	Enabled		Säkerhet
	Prevent bypassing Microsoft Defender SmartScreen prompts for sites	Enabled		MS Baseline
	Prevent bypassing of Microsoft Defender SmartScreen warnings about downloads	Enabled		MS Baseline

Microsoft Edge/Startup, home page and new tab page	Action to take on startup	Enabled	Open a list of URLs	Användarupplevelse
	Configure the home page URL	Enabled	https://www.inera.se/eklient	Användarupplevelse, Exempel
	Configure the new tab page URL	Enabled	https://www.inera.se/eklient	Användarupplevelse. Exempel
	Set the new tab page as the home page	Enabled		Användarupplevelse
	Show Home button on toolbar	Enabled		Användarupplevelse
Microsoft Edge\TyposquattingChecker settings	Configure Edge TyposquattingChecker	Enabled		MS Baseline

Inställningar att hålla koll på och testa

Följande inställningar är i skrivande stund varken med i eKlient eller Microsofts Edge Seurity Baseline (v114), men de har flaggats som eventuella tillägg som kan tillkomma i framtida versioner. Det är med andra ord ingen dum idé att testa dessa i sin miljö både för att säkra upp Edge ytterligare samt vara beredda på kommande förändringar.

Namn	Mer informaton
Enable the network service sandbox (Consider Testing)	Security baseline for Microsoft Edge v102 - Microsoft Community Hub
List of origins that allow all HTTP authentication (Worth Mentioning)	Security baseline for Microsoft Edge v102 - Microsoft Community Hub
Origin-keyed agent clustering enabled by default (Consider Testing)	Security baseline for Microsoft Edge v103 - Microsoft Community Hub
Configure browser process code integrity guard setting (Consider Testing)	Security baseline for Microsoft Edge v104 - Microsoft Community Hub

Enhanced Security Mode configuration for Intranet zone sites (Consider)	Security baseline for Microsoft Edge v107 - Microsoft Community Hub
Allow local MHTML files to open automatically in Internet Explorer mode (Consider)	Security baseline for Microsoft Edge v107 - Microsoft Community Hub

Referenser

Microsoft Edge Security Baseline https://www.microsoft.com/en-us/download/details.aspx?id=55319

Eftersom Edge är baserat på Edge Chromium har vi även utgått från “Google Chrome Security Technical Implementation Guide (STIG)” samt "Microsoft Edge Security Technical Implementation Guide (STIG)”
https://www.stigviewer.com/stig/google_chrome_current_windows/
https://nvd.nist.gov/ncp/checklist/483/download/3918

Microsoft Edge Security Technical Implementation Guide (stigviewer.com)