eKlient Mozilla Firefox

inera

Innehållsförteckning

Ansvarig	Version	Datum
Jörgen Nilsson	1.0	2024-02-19

1. Bakgrund

Syftet med detta dokument är att beskriva hur man kan konfigurera Mozilla Firefox ESR för att vara ett komplement till Microsoft Edge. Anledningen till detta arbete är efter önskemål från eKlient kunder att man behöver Mozilla Firefox som ett alternativ, detta för att Microsoft Edge och Google Chrome båda baseras på Chromium, När det varit problem i applikationer och Microsoft Edge så uppstår samma problem i Google Chrome och då behövs en annan browser.

2. Övergripande

Mozilla Firefox baseras inte på Chromium utan har sin egen motor, Quantum som bara används av Firefox. Firefox anses vara det enda professionella alternativet till Chromium som Google Chrome och Microsoft Edge använder. Tidigare begräsningar, exempelvis att det inte gick att använda mot Microsoft tjänster om Conditional Access (CA) och exempelvis krav på compliant device används. Dessa är nu lösta och Firefox har integrerat stöd för CA.
Versionen som eKlient rekommenderar är Firefox Extended Service Release – ESR. Firefox ESR får större uppdateringar i genomsnitt var 42:e vecka med mindre uppdateringar som kraschfixar, säkerhetskorrigeringar och policyuppdateringar efter behov, men minst var fjärde vecka.

3. Automatiska Uppdateringar

I den värld vi lever i och med de hot som ständigt ligger över alla i form av Cyber-relaterad brottslighet är det viktigt att alltid se till att browsers är uppdaterade. Mozilla Firefox har som standard automatiska uppdateringar aktiverat. Det går att styra med Group Policies om man vill stänga av detta och sköta det manuellt i stället, viktigt är att detection metoden som används i Configuration Manager / Intune stödjer automatiska uppdateringar så den inte försöker installera en gammal version efter att den uppdaterats.

Om automatiska uppdateringar används måste man säkerställa att eventuella proxy lösningar med mera tillåter detta.

4. Konfiguration

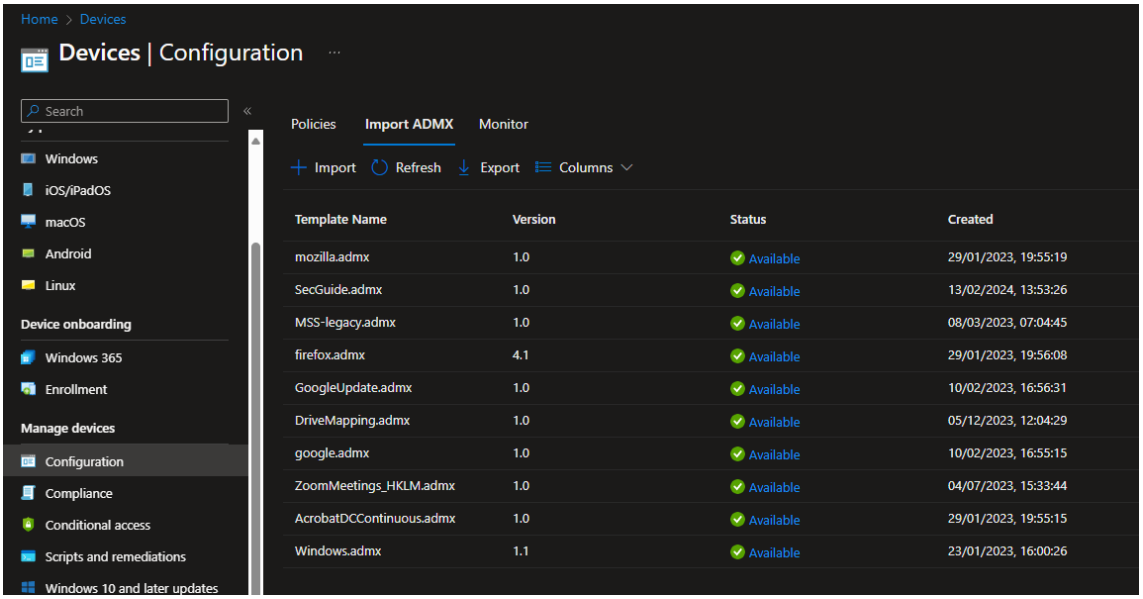
Mozilla tillhandahåller ADMX filer för att konfigurera det som företag har ett behov av att göra. ADMX filerna finns tillgängliga på GitHub där även förändringshantering finns dokumenterad. https://github.com/mozilla/policy-templates/releases

4.1 Group Policy

De ADMX filer som ladas ned kopieras med fördel in i det centrala repository som används.

4.2 Intune

Intune har inte inbyggt stöd för Firefox inställningar men med funktionen att importera ADMX filer direkt i Intune och sedan använda det inbyggda stödet för detta så slipper man använda custom policy. Både Mozilla och Firefox ADMX filerna måste importeras med Mozilla före Firefox annars kommer det att misslyckas. Notera att i skrivande stund stöds endast engelska .ADML filer samt max 10 stycken custom ADMX filer. Detta kommer ökas under våren.



5. Inställningar

De rekommenderade inställningar som eKlient har tagit fram i denna version ligger i ett eget Excel ark för att kunna få med all information. Det finns nedladdningsbart tillsammans med en Group Policy export samt Intune Configuration Policies på eKlient Portalen. Intune Configuration Policy har exporterats med Intune Manager verktyget – https://github.com/Micke-K/IntuneManagement

Detta kapitel beskriver några av de inställningar som gjorts samt de som måste konfigureras.

5.1 Firefox konto och Password Managers

I likhet med Google Chrome rekommenderar vi att man inaktiverar funktionen att logga in med ett Firefox konto och synka sina inställningar samt stänger av den inbyggda Password Manager. Detta för att vi inte har kontroll över hur säkert användarnas Firefox lösenord är eller om MFA används eller inte. Det mest uppmärksammade fallet där detta utnyttjats dock i Google Chrome men utmaningen är densamma är Cisco som blev drabbade https://threatpost.com/cisco-network-breach-google/180385/

5.2 Startsida

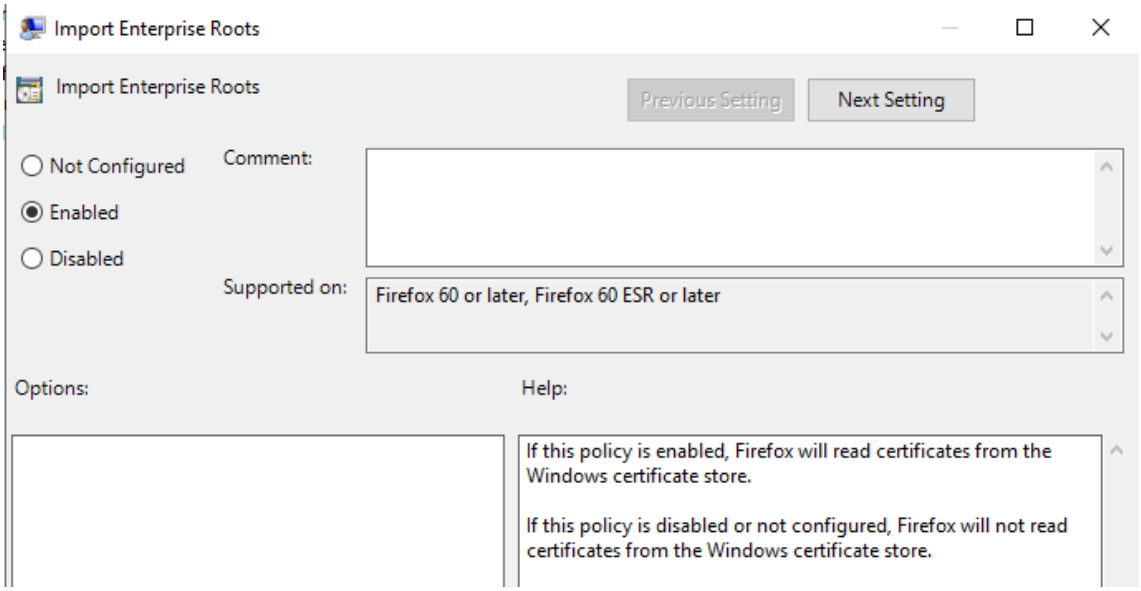
Startsida kan konfigureras och det brukar komma önskemål från verksamheterna om en startsida. Vi aktiverar även Hem knappen precis som i Edge och Google Chrome.

5.3 Inkognito mode

”Inkognito mode” har diskuterats fram och tillbaka för både Edge och Chrome, det är en svår avvägning mellan användarvänlighet och säkerhet. Rekommendationerna från guiderna som vi hänvisar till nedan samt alla säkerhetskrav är att det inte skall vara tillåtet för att göra en forensisk undersökning möjlig vid exempelvis virus-angrepp och intrångsförsök.
Dock behövs detta i de flesta fall på IT där man har flera identiteter eller behöver testa eller liknande, finns detta behov rekommenderar vi att man gör en egen GPO/Intune policy för dessa individer utan att tillåta det för alla.
I fallet Firefox är inkognito mode representerat i en egen genväg på Start Menyn som vi med inaktiverar med GPO/Intune konfigurationen.

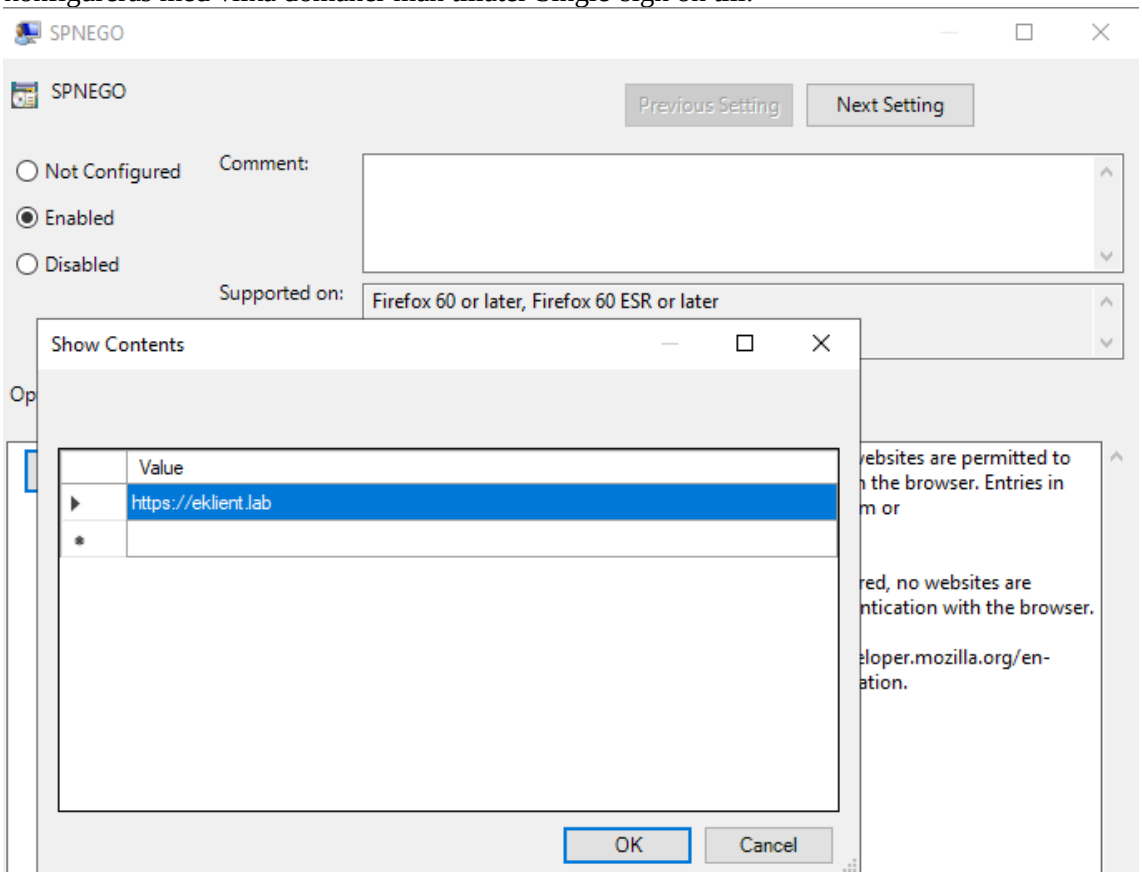
5.4 Certifikat

Som standard läser och använder inte Firefox root-certifikat från Windows utan upprätthåller sin egen lista med betrodda utfärdare. Detta ställer till en hel del med interna webbapplikationer som använder egenutfärdade certifikat, därför konfigurerar vi Firefox att använda betrodda utfärdare från Windows.



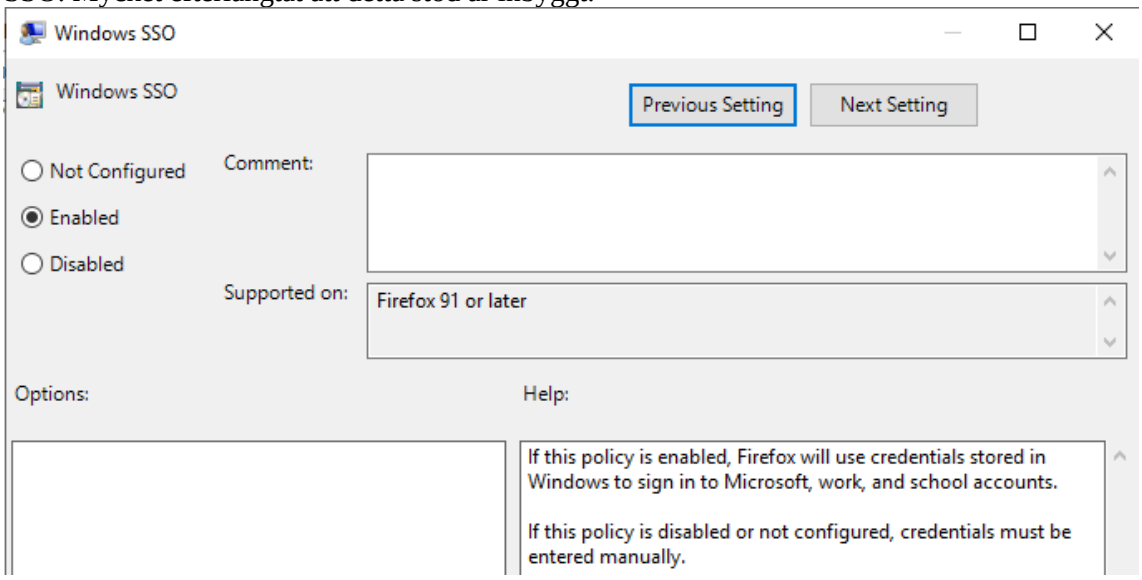
5.5 Single-sign on SPNEGO

För att Single-Sign on till on-premise resurser skall fungera måste policyn SPNEGO konfigureras med vilka domäner man tillåter Single-sign on till.



5.6 Conditional Access

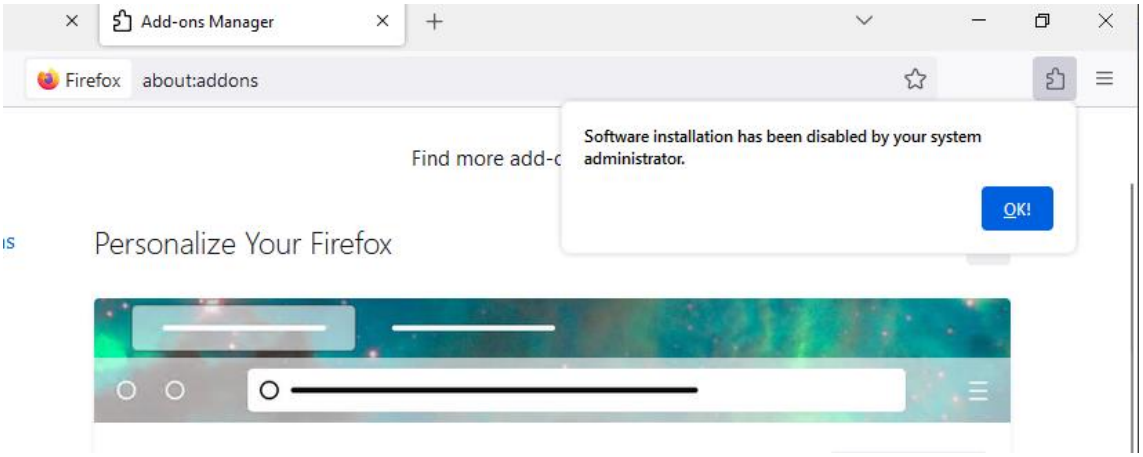
Conditional Access stöd är inbyggt i Firefox och aktiveras med den policy som heter Windows SSO. Mycket efterlängtat att detta stöd är inbyggt.



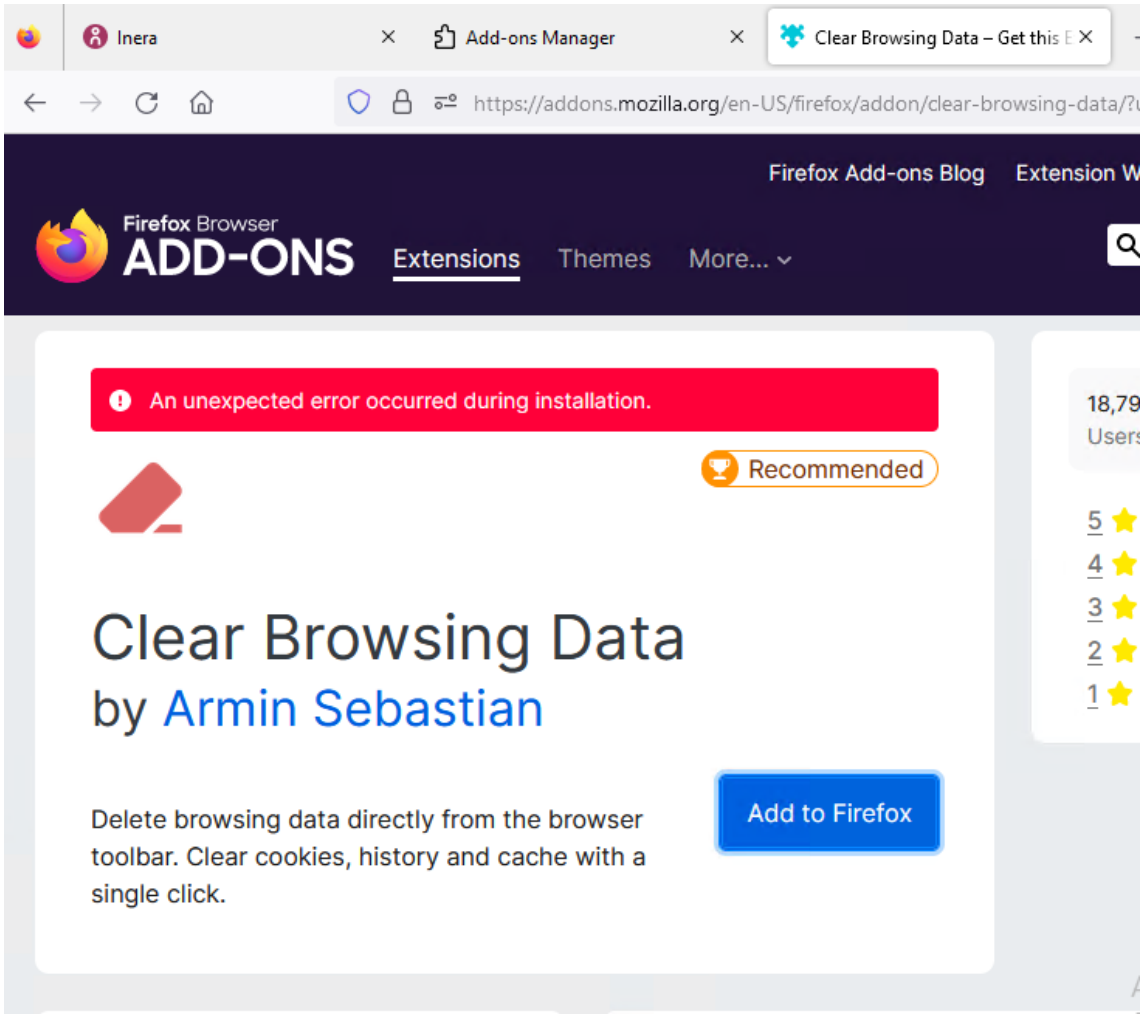
5.7 Add-ons (extensions och teman)

I Firefox följer det med ett helt ekosystem av extensions och teman som man kan installera och använda. Utmaningen med detta är förutom risken, att applikationer används för att spara information som man inte önskar ha i andra system/appar än de som är tilltänkta att användas. Dessa appar och extensions får ofta tillgång till all information man surfar till, även interna system vilket är en risk i sig.

Baserat på detta rekommenderar vi att extensions/teman inaktiveras med en GPO / Intune policy. Det är även möjligt att tillåta/blockera vissa Extensions men detta medför även det extra administration. Det har vid flera tillfällen varit Malware/Adware och informationsstölder i extensions så de bör inte tillåtas.

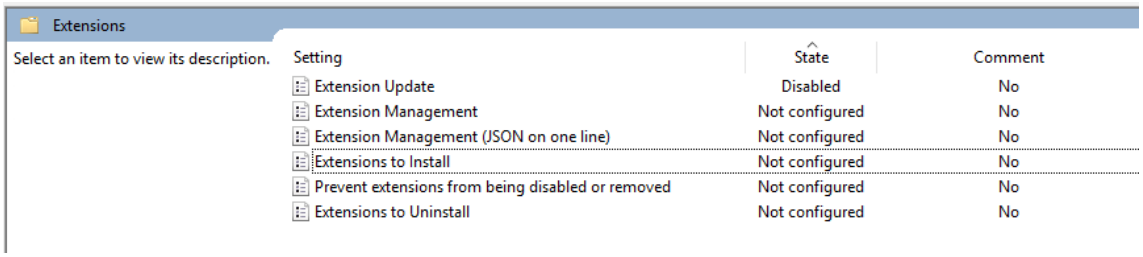


Exempel på blockerat tema installation



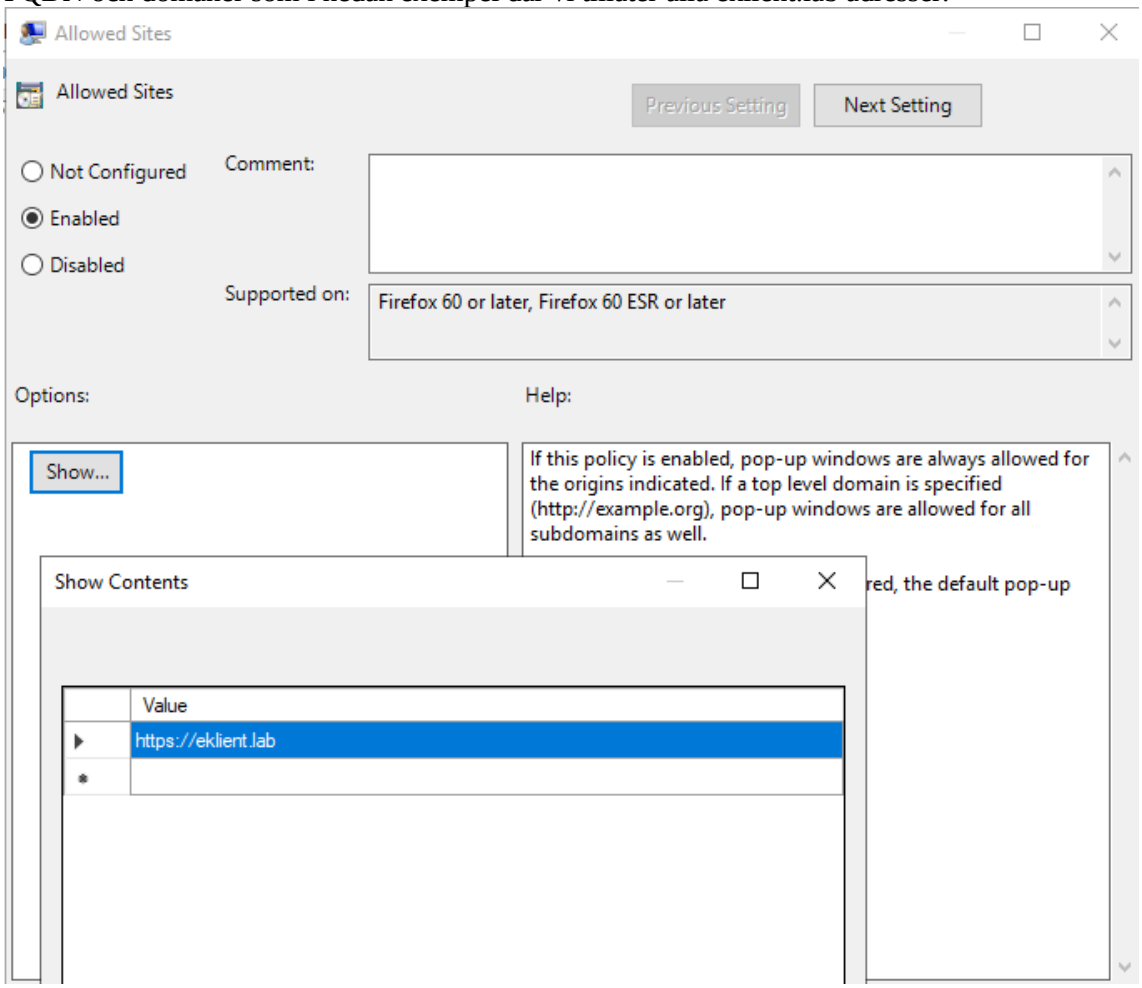
Exempel på blockerad add-on

Det går precis som i Chrome och Edge att tillåta vissa extensions och även installera dessa automatiskt.



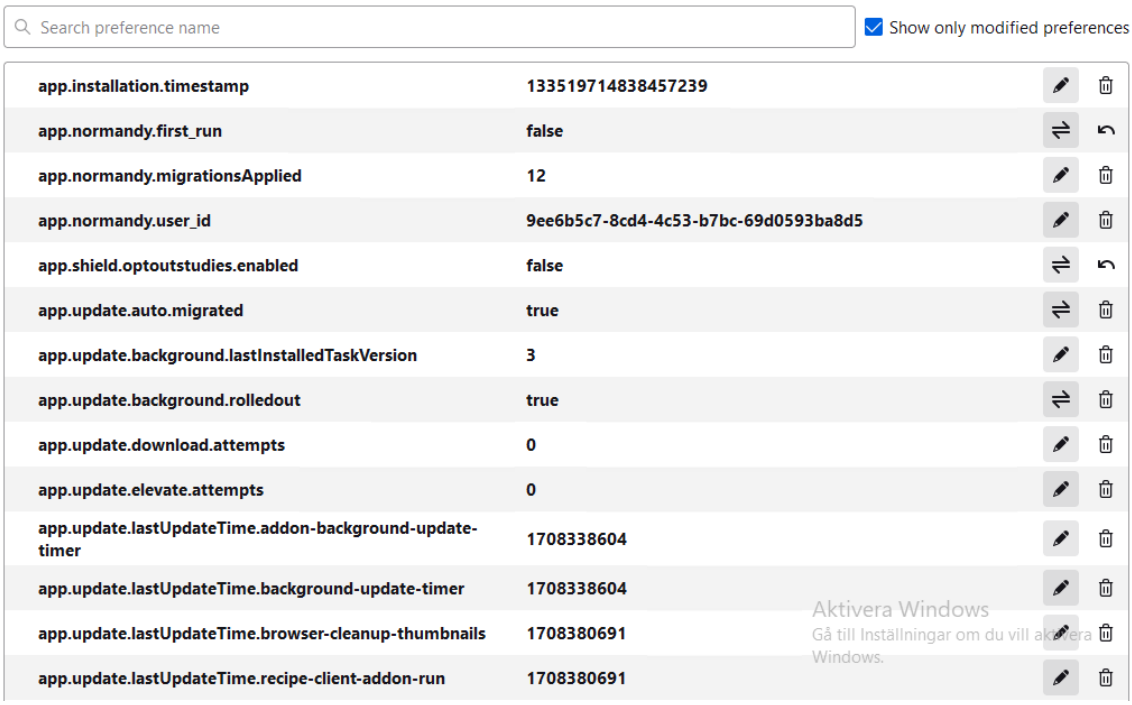
5.8 Pop-ups

Pop-ups är som standard inte tillåtet i de policy vi tagit fram, det går att tillåta både enskilda FQDN och domäner som i nedan exempel där vi tillåter alla eklient.lab adresser.



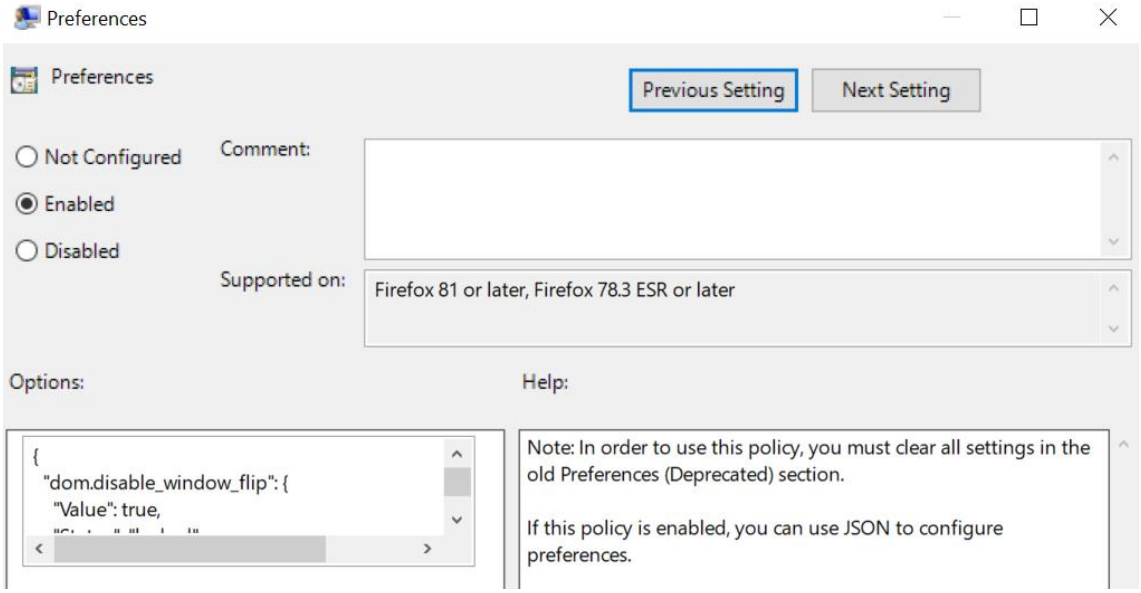
5.9 Preferences

I Firefox kan man konfigurera preferences, vilket egentligen är alla inställningar man kan göra varav många saknar UI, dessa nås via ”about:config” sidan där man kan lista alla preferences. Dessa kan man sedan lägga in i en Group Policy och på så vis konfigurera alla inställningar som inte har en Group Policy inställning.



Lista med alla preferences

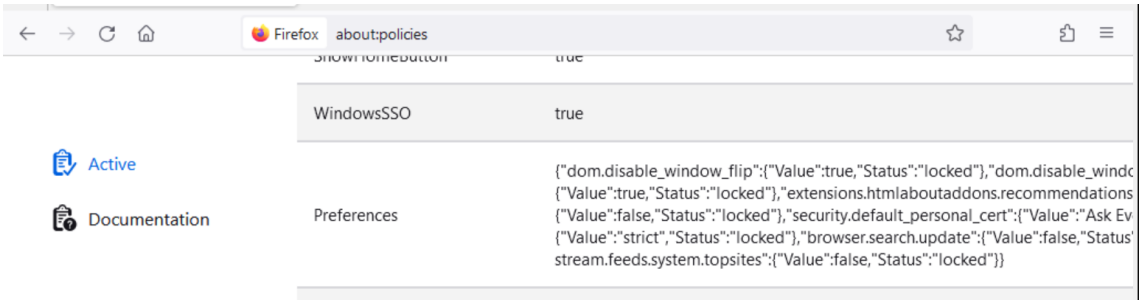
Denna GPO inställning innehåller en .JSON med alla de inställningar som skall konfigureras, samt om de är låsta eller inte.



Exempel .JSON med några av de inställningar vi rekommenderar.

```
{
 "dom.disable_window_flip": {
   "Value": true,
   "Status": "locked"
 },
 "dom.disable_window_move_resize": {
   "Value": true,
   "Status": "locked"
 },
}
```

När man konfigurerar en av dessa preferences verifieras och man vill verifiera att det fungerar görs det enklast med ”about:policies” där alla policies syns även Preferences. Skulle något vara fel i .JSON formateringen eller inställningarna kommer ett utropstecken visas alternativt att den inte är listad alls.



Följande inställningar görs med Preferences:

Från STIG rekommendation:

- dom.disable_window_move_resize = “Firefox must be configured to prevent JavaScript from moving or resizing windows”
- dom.disable_window_flip = “Firefox must not recommend extensions as the user is using the browser.”
- extensions.htmlaboutaddons.recommendations.enabled = “Firefox must not recommend extensions as the user is using the browser.”
- security.default_personal_cert =
- browser.contentblocking.category = “Firefox Enhanced Tracking Protection must be enabled”
- browser.search.update = “Firefox automatically checks for updated version of installed Search plugins”

eKlient rekommenderade inställningar

- browser.newtabpage.activity-stream.feeds.system.topsites = Tar bort sponsrade förslag vid varje sökning i adressfältet
- browser.search.hiddenOneOffs = Tar bort sponsrade sökmotorer från alternativ vid varje sökning i adressfältet

6. Referenser

Vi har tagit fram denna rekommendation baserat på det arbete som gjorts tidigare med Microsoft Edge security baseline samt Google Chrome. Security Technical Implementation Guide (STIG)” för Mozilla Firefox - https://www.stigviewer.com/stig/mozilla_firefox/