Best practice policies voor nieuwe installaties - Endpoint Security

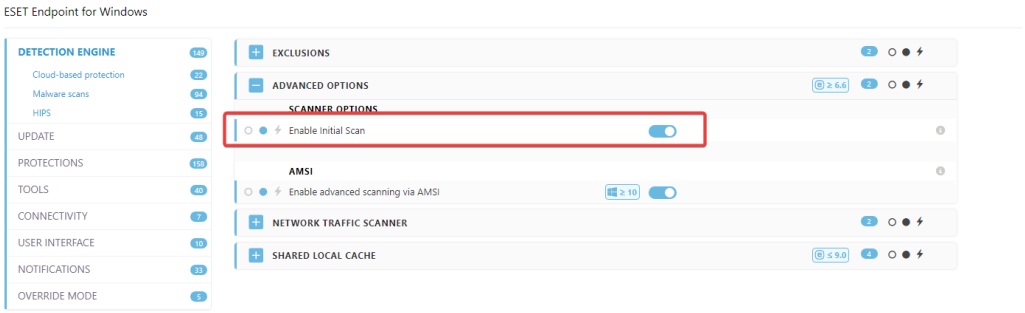
Danny | ESET Nederland - 2023-08-15 - Reacties (0) - Best Practices

In dit artikel bespreken we de best practices voor Endpoint Security.

Wanneer een instelling niet wordt genoemd is de standaardwaarde aangehouden.

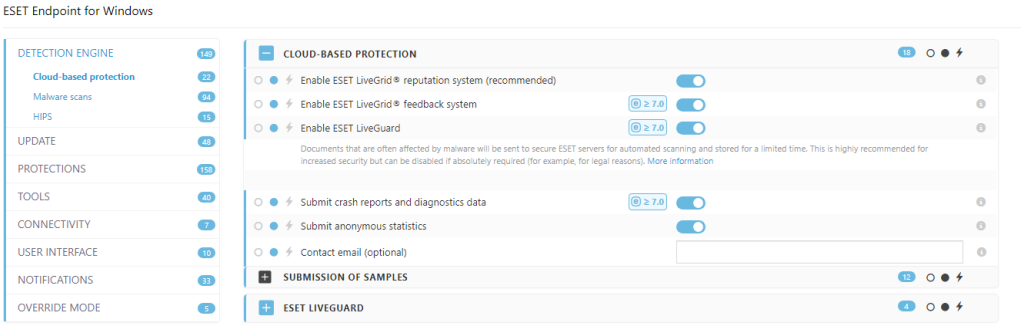
Detection Engine:

- Na installatie en voltooide activatie zal het product een volledige scan van het systeem uitvoeren. Dit levert op langere termijn prestatie-winst op, omdat het product alle bestanden op het systeem al een keer heeft gezien. Voor bredere uitrol op virtuele systemen of wanneer de ESET installatie onderdeel is van een geautomatiseerd imaging-proces kan worden overwogen om deze setting uit te schakelen.

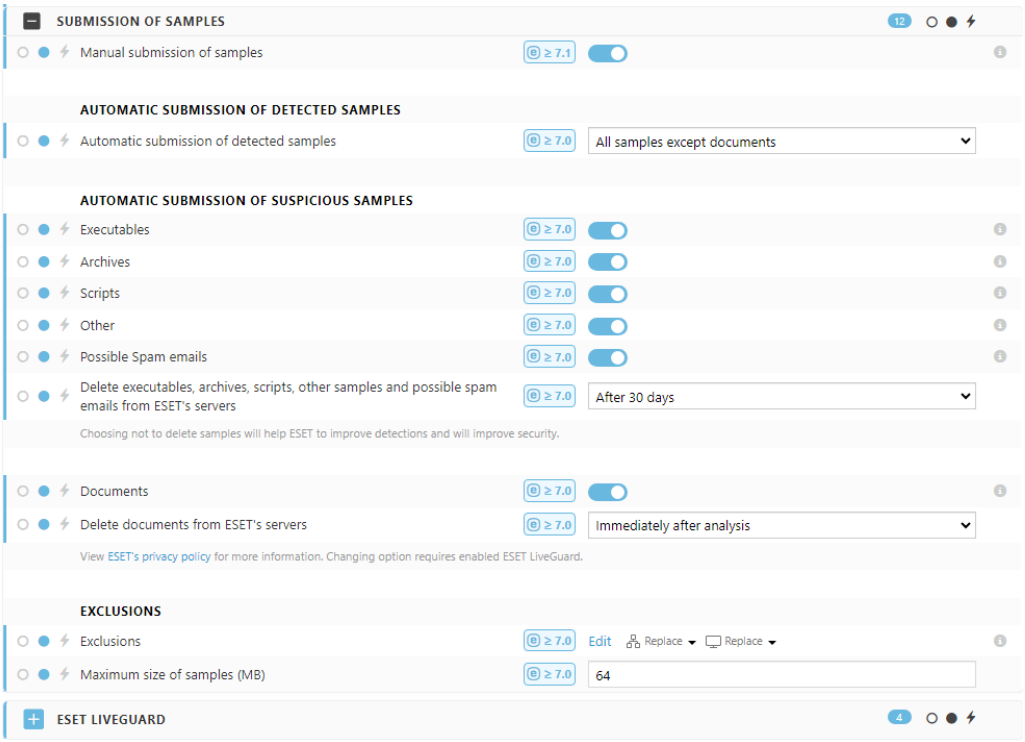


Cloud based Protection:

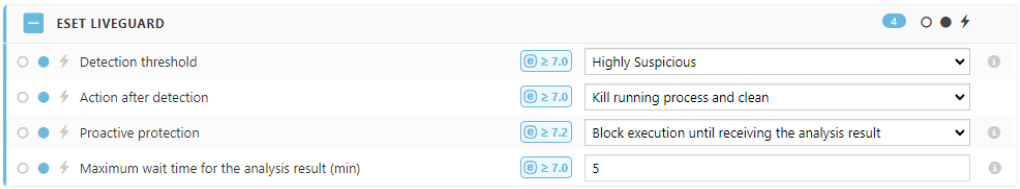
- Dankzij het ESET LiveGrid cloud reputatiesysteem is het ESET product in staat om zeer snel en met minimale impact bestanden, processen en websites te classificeren zonder dat hier daadwerkelijk scanning voor nodig is. Hashes van files worden tegen LiveGrid gehouden om hier de reputatie van te achterhalen.



- LiveGrid feedback helpt ESET door naast enkel hashes ook gehele bestanden te uploaden voor een analyse en het resultaat met alle ESET klanten te delen. Het uploaden van bestanden kan verder worden ingesteld zodat bepaalde files/folders hier ook van kan worden uitgezonderd. Wanneer gebruik gemaakt wordt van ESET LiveGuard Advanced kan ook data-retentie worden meegegeven zodat bestanden direct, of 30 dagen na analyse worden opgeschoond.

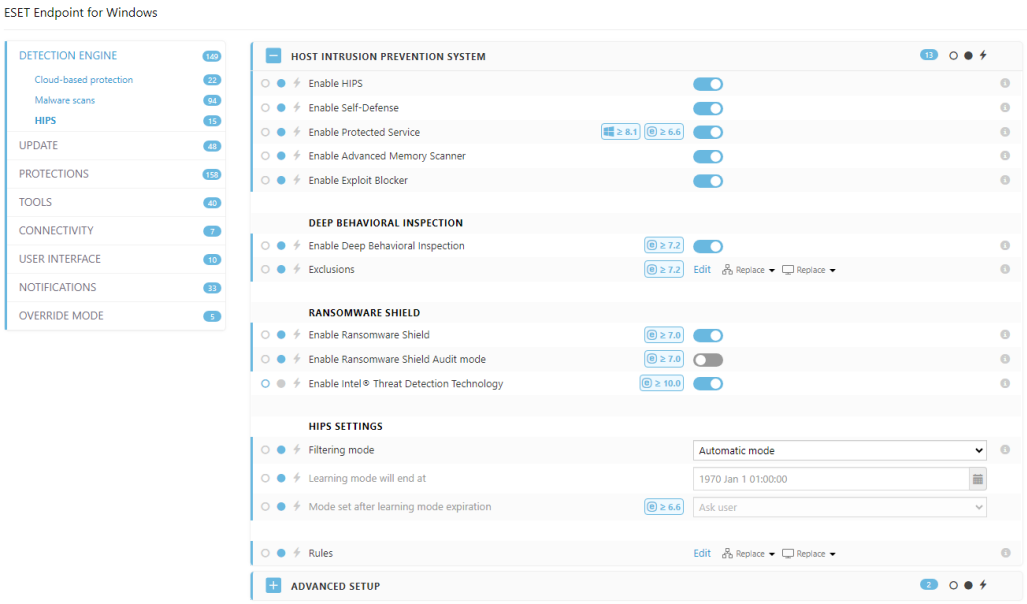


- Schakel binnen ESET LiveGuard Advanced **Proactive protection** in. Deze instelling biedt een krachtige extra laag bescherming door bestanden welke “nieuw“ op het systeem komen, geen reputatie hebben en verdacht zijn te blokkeren voor de eindgebruiker totdat de Cloud - Sandbox hier een oordeel over heeft. De eindgebruiker wordt ook op de hoogte gesteld van deze acties.



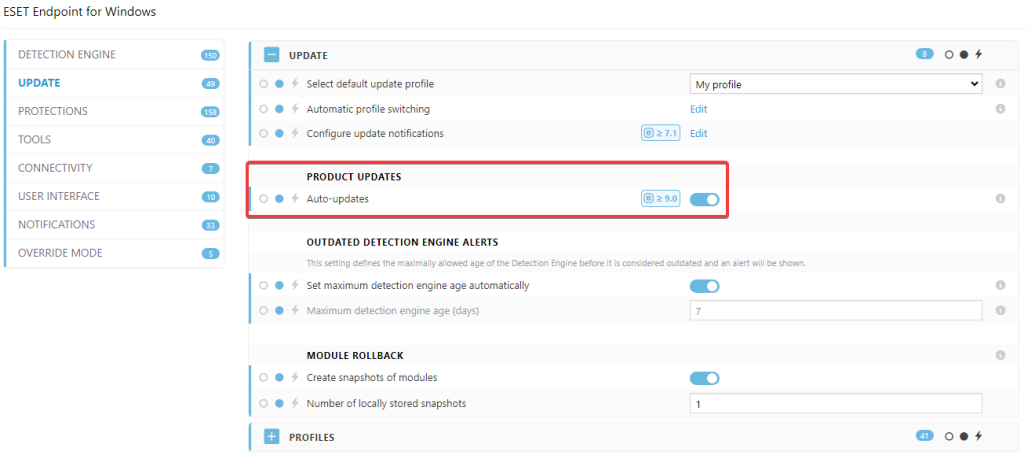
Host-Based Intrusion Prevention System (HIPS):

- De HIPS module is een cruciaal onderdeel van de ESET oplossing en biedt zeer belangrijke beschermingsonderdelen zoals Self-Defense, Advanced Memory Scanner en het Ransomware Shield. De standaardinstellingen bieden een goede balans tussen werkbaarheid en bescherming waar middels additionele HIPS regels extra beveiliging aan kan worden toegevoegd. Zie hiervoor ook Anti-ransomware setup. https://techcenter.eset.nl/nl/downloads/files/eset-anti-ransomware-setup-en



UPDATE:

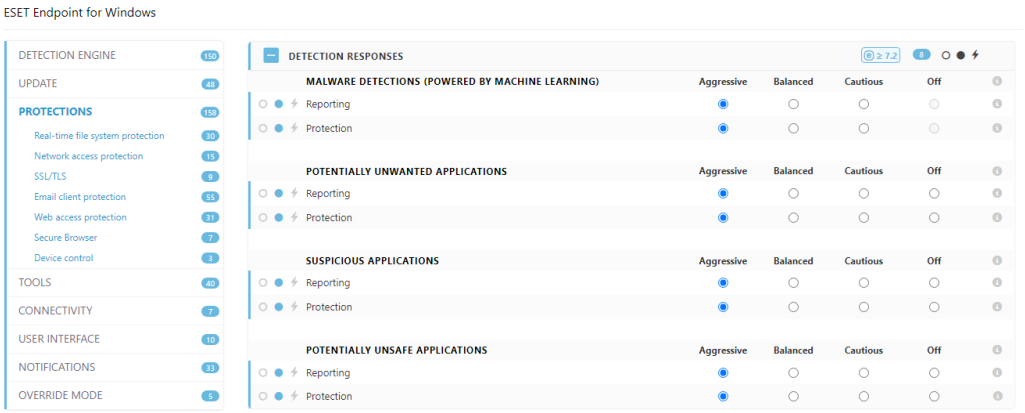
- Wanneer gebruik gemaakt wordt van het automatische upgrade mechanisme **(Sterk aanbevolen)** van ESET Endpoints dient dit ook in de Endpoint policy te worden ingeschakeld.



PROTECTIONS:

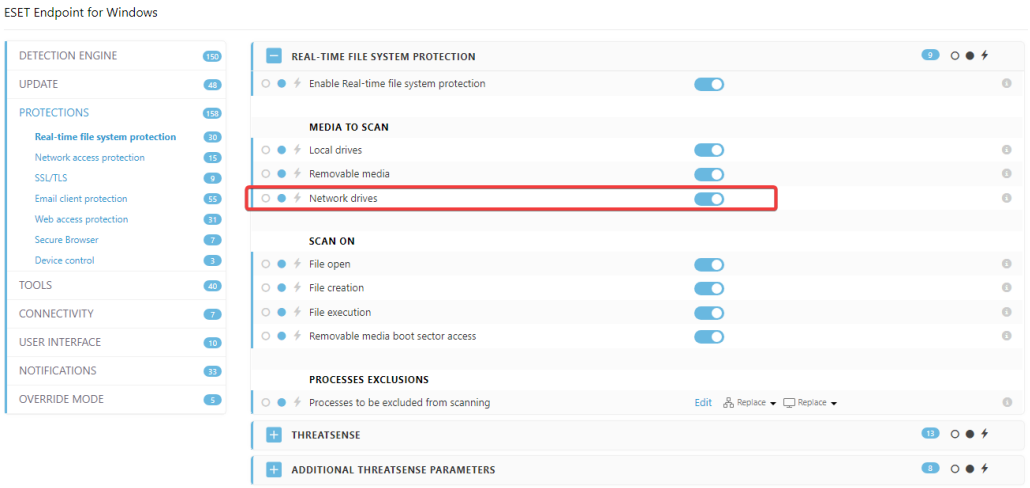
- Zet vanaf de eerste implementatie alle Reporting functionaliteit op Aggressive. Dit zorgt voor maximale zichtbaarheid van malware, verdachte, ongewenste en onveilige software in de omgeving. Vooral bij nieuwe implementaties kan het met Aggressive Reporting voorkomen dat er detecties optreden waar een uitzondering voor nodig is.

- Na een aantal dagen/weken kan ook het Protection niveau worden opgeschaald naar Aggressive om ook maximale bescherming te bieden zonder dat dit onverwachte detecties oplevert.

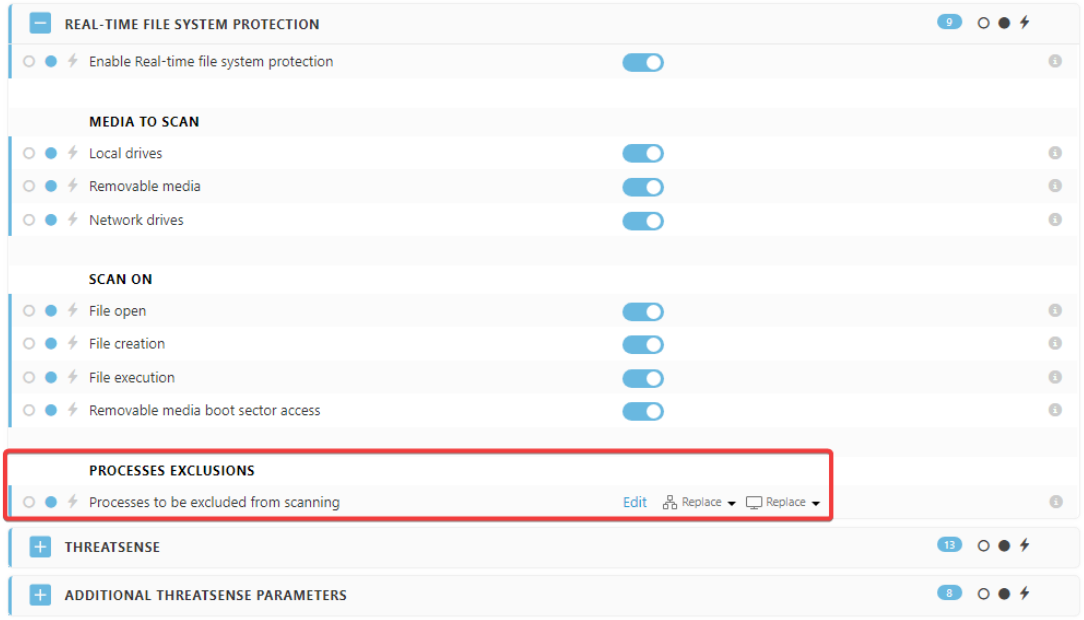


Real-time file system protection:

- Het real-time scannen van network drives is erg belangrijk, en raden we absoluut aan om in te schakelen. In specifieke gevallen, waaronder redirected $home folders en andere vormen van het lokaal koppelen van netwerk drives kan dit echter wel een negatieve performance-impact hebben. Test bij implementatie en per omgeving of dit het geval is.

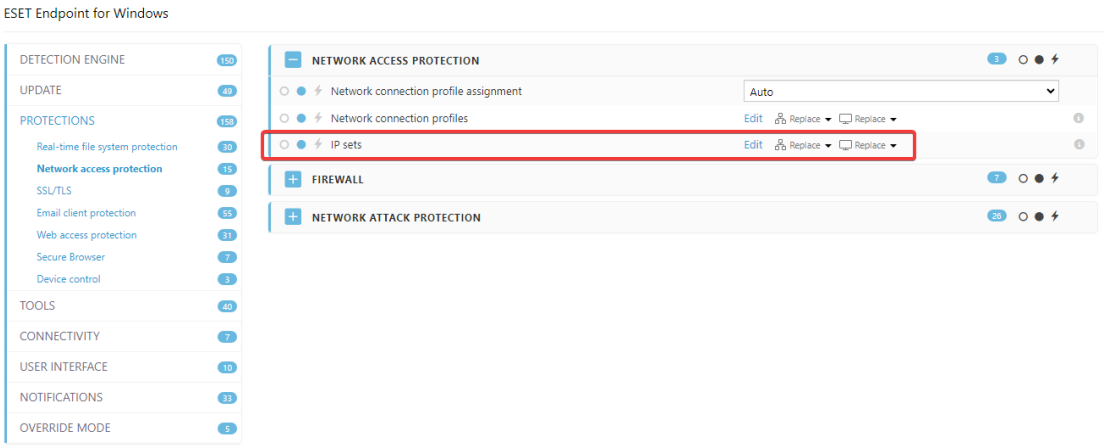


- Binnen ESET producten kan op verschillende manieren uitzonderingen worden gemaakt. Probeer dit altijd tot een minimum te beperken. Mocht een proces toch een uitzondering nodig hebben, zonder deze dan middels een Process Exclusions uit, en niet de gehele folder waar de toepassing zich in bevindt. https://help.eset.com/ees/latest/en-US/idh_config_processes_exclude.html

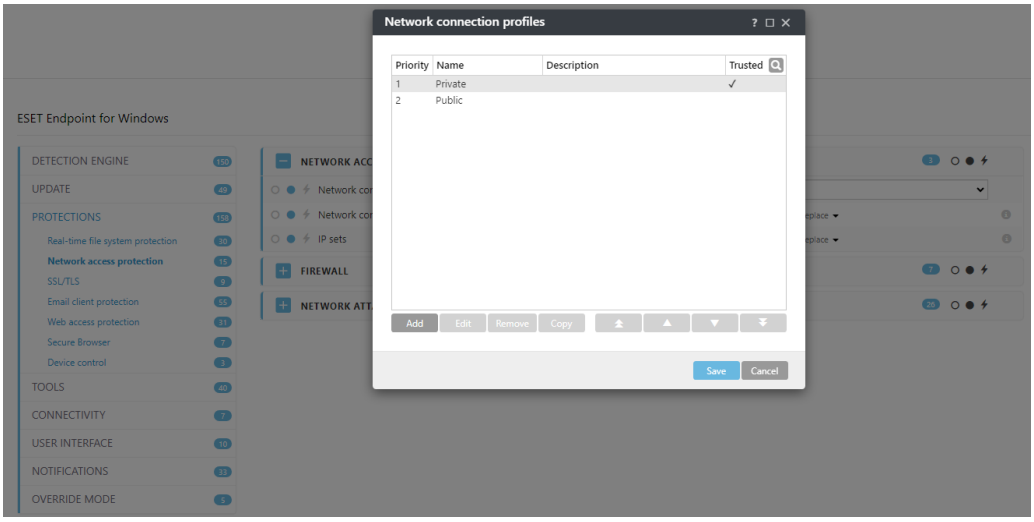


NETWORK ACCESS PROTECTION:

- Een belangrijk concept binnen Network Protection zijn de zogenaamde IP Sets, hierbinnen vallen onder andere de Trusted Zone, een zone waar vanuit veel standaard (domein)verkeer wordt toegestaan.

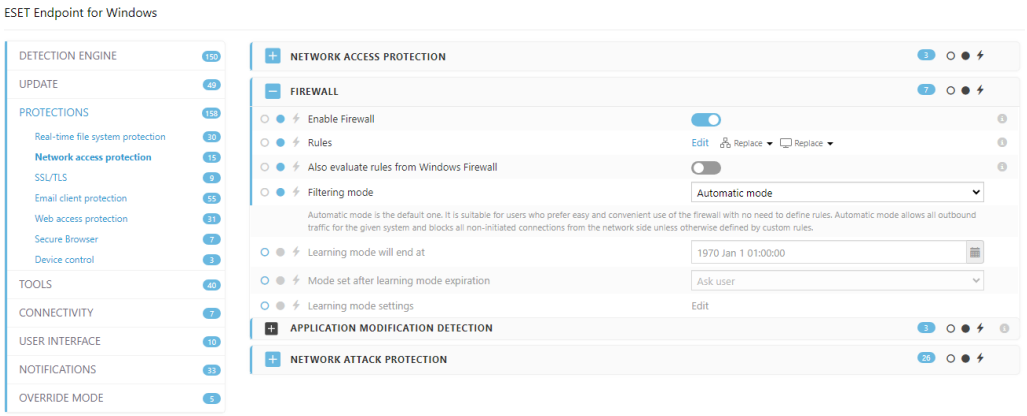


- Voor een strakker firewall beleid kan gebruik gemaakt worden van Network Connection Profiles. Hierin is te definiëren wanneer een machine zich op het bedrijfs/vertrouwde netwerk bevindt door één of meerdere netwerk identificatiemethoden op te geven. Aan deze netwerken zijn ook firewall profielen met daarin aparte regels te koppelen.

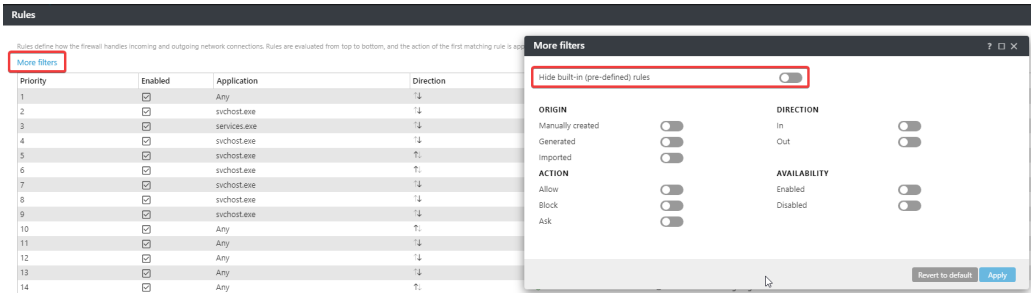


Firewall:

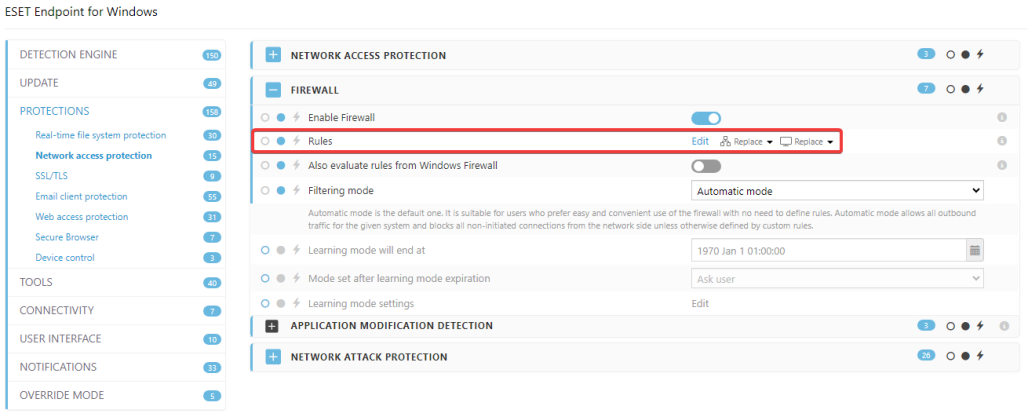
- Met de ESET firewall wordt de standaard Windows Firewall vervangen en is deze te managen via ESET PROTECT. Mochten er veel lokaal aangemaakte Windows Firewall rules aanwezig zijn op verschillende systemen kan gebruik worden gemaakt van de optie om deze regels ook door de ESET firewall te laten evalueren.



- Met de firewall ingeschakeld komt het product standaard met een groot aantal regels uit de doos. Deze zijn terug te vinden in de regel-editor door het het schuifje onder More Filters uit te schakelen wat deze regels onzichtbaar maakt.



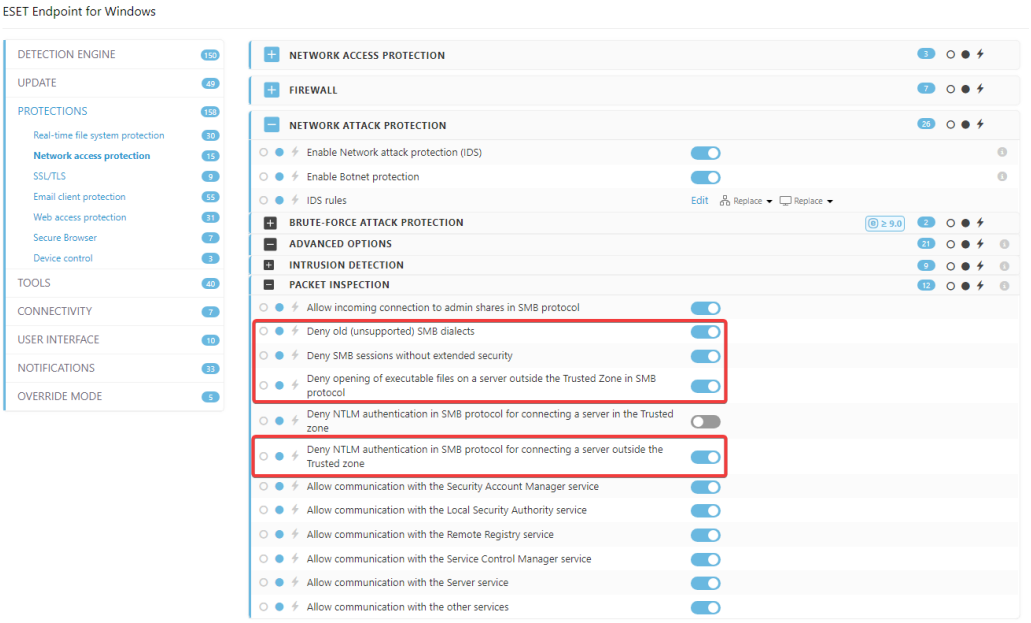
- Een belangrijk detail met betrekking tot hoe deze regels kunnen worden toegepast. In de Baseline policy raden we aan om rules middels “Replace“ in te stellen zodat eventueel lokale regels ook worden overschreven. Een additionele policy waar enkel firewall rules in zitten kan met bijvoorbeeld Prepend worden ingesteld om de regels bovenaan in de te evalueren lijst van firewall rules te plaatsen.



NETWORK ATTACK PROTECTION:

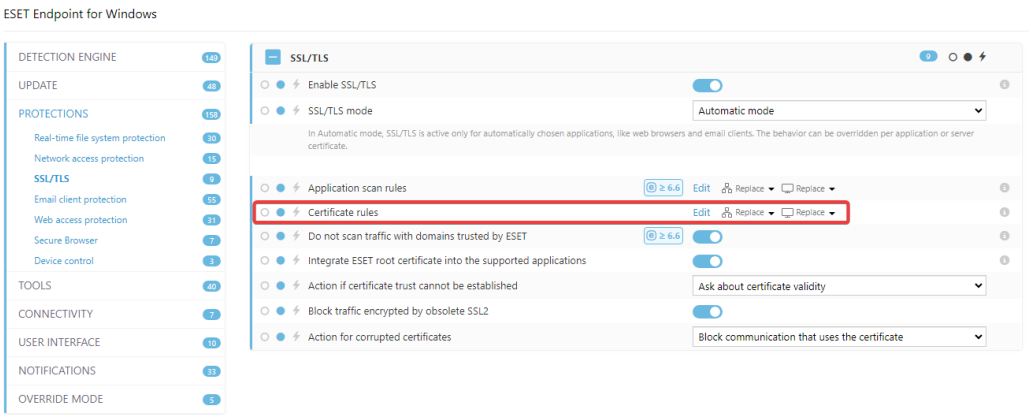
- Een aantal extra aanpassingen kunnen worden gemaakt zoals in het

screenshot is te zien. Deze staan standaard uit voor legacy doeleinden of hebben te maken met het authenticeren naar bijvoorbeeld netwerkshares buiten de trusted zone.



SSL/TLS:

- Het is mogelijk om bepaalde certificaten uit te zonderen van SSL/TLS protocol scanning. Pas dit toe wanneer een applicatie of website hier niet goed mee om kan gaan. Een issue waar dit soms nodig is, is onder andere wanneer een ADFS authenticatie plaats moet vinden. Sluit dan het certificaat van de ADFS servers uit van scanning middels een Certificate Rule.



Web access Protection:

Web Control: Standaard niet ingeschakeld. Uiteraard kan dit worden meegenomen in een baseline policy. Meer informatie is te vinden op de

volgende help pagina:
https://help.eset.com/ees/latest/en-US/?idh_page_setting_parental.html

SECURE BROWSER:

De secure browser is als functionaliteit overgekomen uit de consumentenproducten en heeft binnen het zakelijke product een zeer niche functie. We raden deze functie enkel in te schakelen voor systemen/gebruikers welke veel financiële transacties via bijvoorbeeld bank-websites uitvoeren.

DEVICE CONTROL:

Standaard niet ingeschakeld. Uiteraard kan dit worden meegenomen in een baseline policy. Meer informatie is te vinden op de volgende help pagina: https://help.eset.com/ees/latest/en-US/idh_config_devmon.html

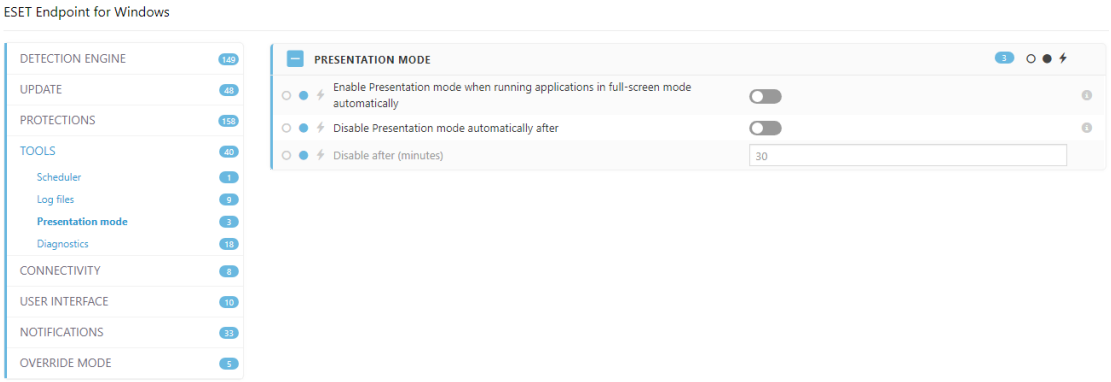
TOOLS:

Binnen het onderdeel Tools zijn een aantal functionaliteiten welke zeer organisatieafhankelijk zijn.

- **Timeslots**, biedt de mogelijkheid om Web Control binnen bepaalde timeslots te laten gelden
- **Microsoft Windows Update:** standaard zal het product waarschuwen als er Windows Updates beschikbaar zijn. Stel deze waarschuwing naar wens en beleid in.

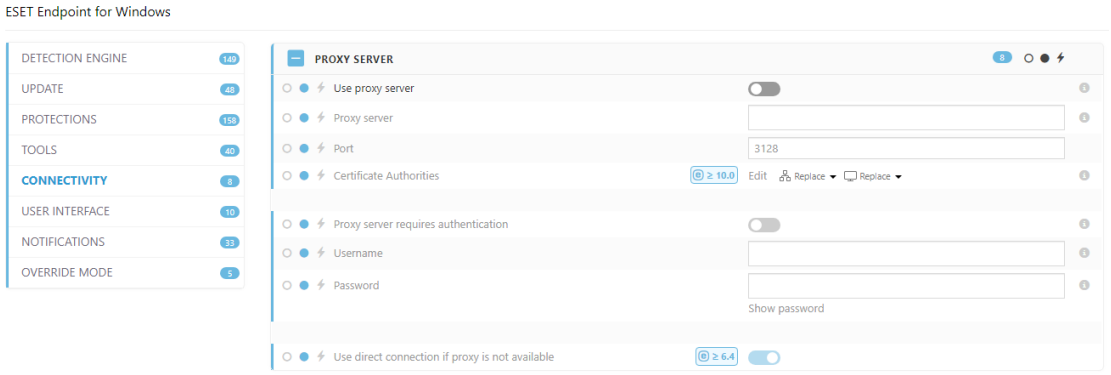
Scheduler: bevat alle geplande taken van het product, zoals het regulier downloaden van updates maar ook de startup scan is hier een onderdeel van.

Presentation mode: Schakel het automatisch inschakelen van Presentatie-modus uit. Dit kan een negatief effect hebben op het ophalen van module-updates, vooral wanneer er veel met remote sessies wordt gewerkt.



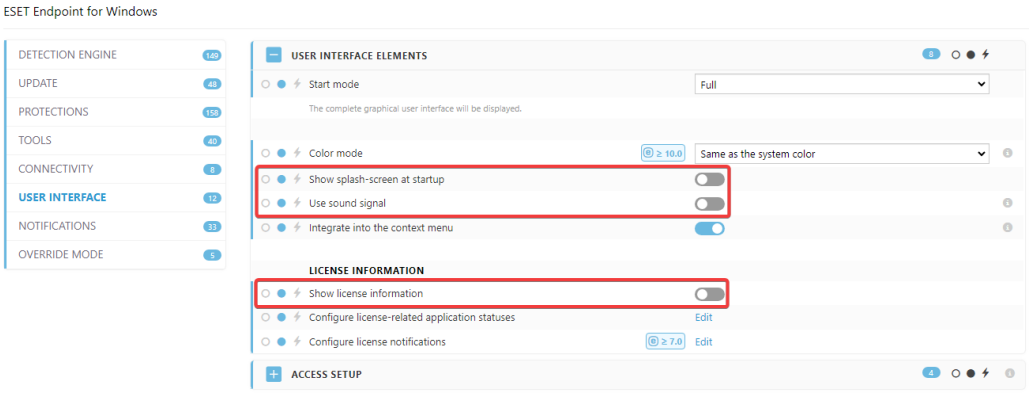
Connectivity:

- **Proxy server:** stel hier, wanneer in gebruik, het adres van de (caching) proxy in. Deze bespaard bandbreedte door alle update en installatiebestanden te cachen. Meer context en uitleg omtrent databesparing is te vinden in de online help:
    - [Installation/Upgrade | ESET PROTECT | ESET Online Help]



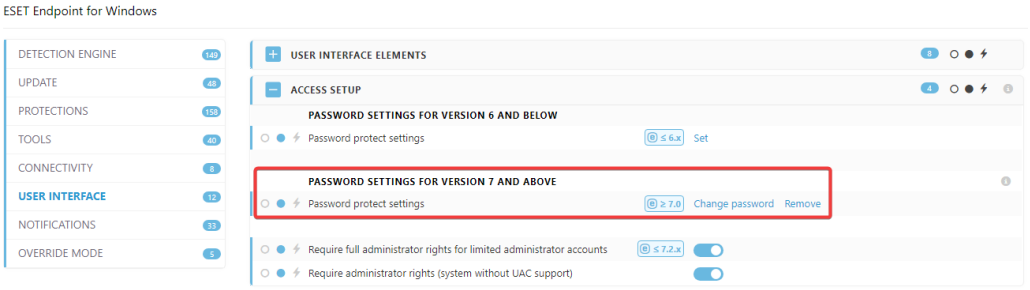
USER INTERFACE:

- Deze settings zijn volledig organisatie afhankelijk. In de regel schakelen we onderstaande opties uit.



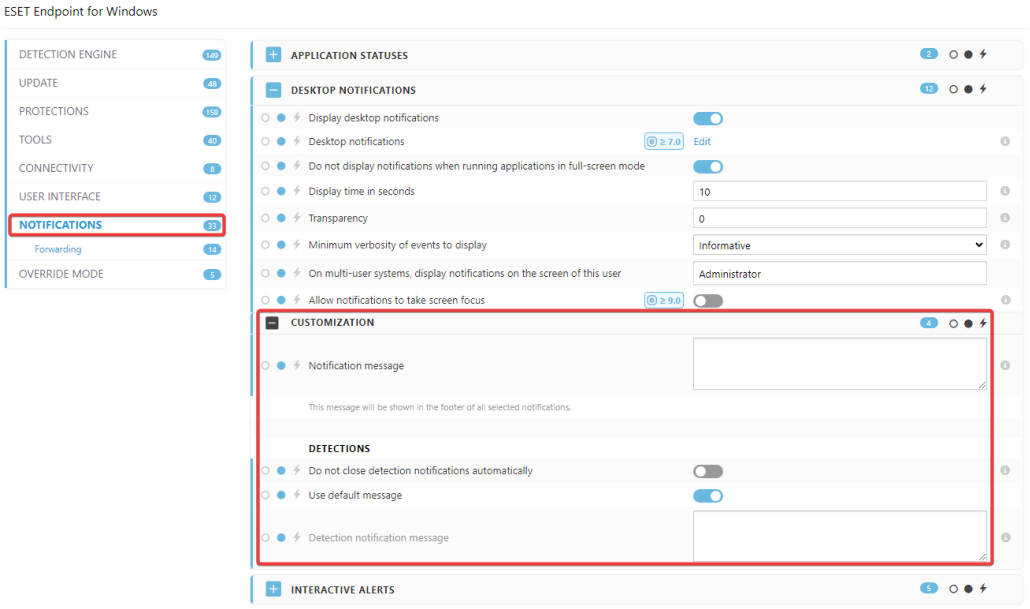
ACCESS SETUP:

- Een zeer belangrijke functionaliteit binnen het product is het instellen van een wachtwoord op de instellingen, maar belangrijker, het verwijderen van de software. Zonder wachtwoord op de settings kan iedereen met de juiste systeemrechten het product verwijderen.



NOTIFICATIONS:

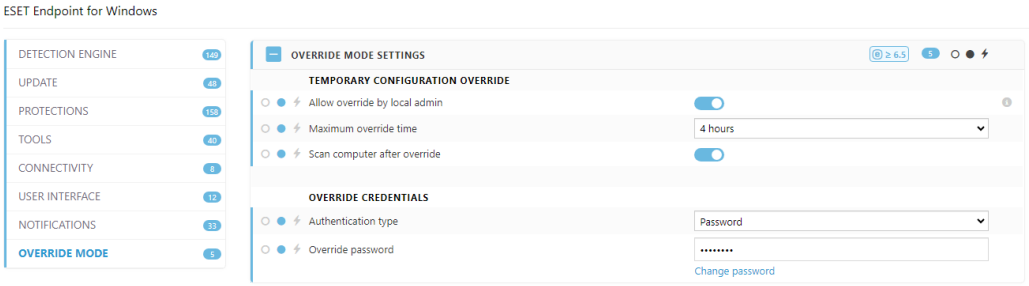
- **Customization:** middels de customization opties zijn extra teksten toe te voegen aan detectiewaarschuwingen. Denk hierbij aan bijvoorbeeld contactgegevens van een helpdesk.



OVERRIDE MODE:

- Door binnen de policy alle settings te voorzien van een blauw balletje (Applied) zijn de settings binnen het endpoint read-only. Om lokale troubleshooting mogelijk te maken raden we dan ook aan om Override Mode in te schakelen waarmee met een (apart) wachtwoord

de instellingen tijdelijk kunnen worden aangepast. Na de opgegeven override tijd valt het product automatisch terug in de standaard instellingen zoals in de policy gedefinieerd.



Gerelateerde inhoud

- Best practice policies voor nieuwe installaties - Mail Security for Microsoft Exchange Server
- Best practice policies voor nieuwe installaties - Server Security for Windows
- Best practice policies voor nieuwe installaties - Intro