Secquard Onboarding & Installatie

Voorwoord

Beste (toekomstige) Secquard gebruiker,

Gefeliciteerd met het besluit om Secquard te gebruiken in uw organisatie!

In dit document beschrijven wij het normale proces rondom het aansluiten van onze gebruikers.

De installatie van onze applicatie is vaak al binnen enkele dagen gerealiseerd! Om het proces zo gestroomlijnd mogelijk te laten verlopen is het belangrijk dat u vooraf weet welke voorbereidingen u dient te treffen en wat u kunt verwachten tijdens de installatie.

Dit document is dan ook bedoeld om u de kans te geven de installatie op de juiste manier voor te bereiden én om u een overzicht te geven van hoe de installatie verloopt. Wij verzoeken u daarom vriendelijk de eerste twee hoofdstukken aandachtig te bestuderen en de rest in ieder geval globaal te bekijken.

Alvast hartelijk dank en wij of onze partners kijken ernaar uit u te zien bij de installatie!

Namens Team Secquard,

Marcel Kiffen, CEO

1 Overzicht Onboarding Proces

1.1 Doornemen Secquard onboarding en installatie document

In dit eerste hoofdstuk van dit document bekijken we het verloop van de installatie van de Secquard applicatie binnen een organisatie. De eerste stap ten aanzien van een vlekkeloze installatie heeft u al gezet, dat is namelijk het lezen van dit document! De laatste paragraaf van dit hoofdstuk beschrijft de inhoud van de volgende hoofdstukken.

1.2 Intake formulier

Om uw installatie zoveel mogelijk te stroomlijnen hebben wij een beperkte hoeveelheid informatie van u nodig. Wanneer u het onboarding en installatie document heeft doorgenomen willen wij u daarom vriendelijk verzoeken het intake formulier in te vullen. Hier verzamelen wij onder andere contactgegevens van de betrokken persoon, verstrekken wij informatie (zie volgende paragraaf) en kunt u direct een afspraak inplannen voor de kick-off meeting en om de installatie uit te voeren.

1.3 Kick-off meeting

Voor de installatie plaatsvindt, wordt een kick-off-meeting ingepland van 15-30 minuten. Hierin kunnen alle betrokken personen bij elkaar komen om het proces van de installatie en de daarvoor vereiste voorbereidingen (te vinden in dit installatie document en het intake formulier) door te spreken.

1.4 Installatie

Als u alle voorbereidingen heeft getroffen kan er worden begonnen met het installeren van de applicatie en het aansluiten van de scripts. Vaak is dit proces binnen één of een paar dagen gerealiseerd. Dit maakt de planning zeer eenvoudig en snel!

1.5 User Workshop

Hoewel ons product eenvoudig is in gebruik, vinden wij het belangrijk dat onze gebruikers er goed mee overweg kunnen.

Daarom hebben wij een workshop ontwikkeld waarin de meest voorkomende scenario's worden behandeld. Zo weten onze gebruikers precies hoe zij de meeste waarde uit onze applicatie halen. Daarnaast krijgt u uiteraard toegang tot onze handleidingen waarin alle functies van onze applicatie op overzichtelijke manier zijn uiteengezet en toegelicht.

1.6 Oplevering

Tijdens de oplevering tekent u het oplevering document. Hiermee gaat u er mee schriftelijke akkoord dat de installatie is volbracht en uw systemen zijn aangesloten.

1.7 Follow-up

Wanneer u een tijdje 'up and running' bent, zullen wij contact met u opnemen om te polsen hoe u het gebruik van onze applicatie ervaart. Dit doen wij om mogelijke opportunities voor verbetering te identificeren én om zelf zicht te houden op hoe onze applicatie bijdraagt aan het verbeteren van de levens van onze klanten. Deze informatie kunnen wij weer gebruiken om andere gebruikers te helpen.

1.8 Vervolg hoofdstukken

In het tweede hoofdstuk wordt aangegeven wat er moet worden klaargezet om de Secquard installatie te kunnen uitvoeren. Het derde hoofdstuk beschrijft een normale installatie van de Secquard applicatie. De volgende hoofdstukken beschrijven hoe systemen worden aangesloten op de applicatie en hoe u deze configureert zodat de gebruiker ermee aan de slag kan. Tenslotte wordt uitlgelegd hoe u een aantal taken kunt automatiseren, en wordt u herinnerd aan het invullen van het intake-formulier.

Let op! Het is van essentieel belang dat u het requirements hoofdstuk zorgvuldig bekijkt en de benodigde voorbereidingen treft alvorens de installatie begint. U bent zelf verantwoordelijk voor deze voorbereidingen. Tijdens de installatie moet iemand van uw organisatie aanwezig zijn met de juiste (administrator) rechten.

Voor de installatie van de applicatie en het aansluiten van uw systemen, vragen wij u vriendelijk om de daarbij behorende informatie globaal bekijkt. Een specialist van Secquard en/of van een van onze partners zal aanwezig zijn om uw installatie te begeleiden. Hoofdstukken 3, 4 en 5 en 6 zijn bedoeld om u een idee te geven van de procedure, zij bieden u kans om eventuele aanvullende voorbereidingen te treffen.

- Vereiste voorbereiding installatie
- Applicatie installatie
- Aansluiten Windows systemen
- Aansluiten Linux systemen
- Automatiseren verscheidene taken

2 Voorbereiding Installatie

Om van Secquard gebruik te maken, dienen er 2 onderdelen te worden geïnstalleerd. De Secquard applicatie (1) wordt geïnstalleerd op een lokale server en de Secquard scripts (2) worden geïnstalleerd op ieder systeem dat geaudit wordt. Daarnaast wordt er gebruik gemaakt van een Microsoft SQL-server, deze is gratis beschikbaar en, net als de scripts en de applicatie, eenvoudig te installeren. In deze gids wordt beschreven hoe de installatie van de Secquard applicatie normaal gezien verloopt.

De installatie wordt gedaan op een dedicated server bij de opdrachtgever. Het is belangrijk dat deze server bereikbaar is voor alle servers die geaudit moeten worden. Het beste is dat deze server via een host-name bereikt kan worden (in plaats van via alleen een IP-adres).

Bij de installatie heeft u een licentie key nodig, deze kunt u via Secquard verkrijgen. Zorgt u ervoor dat u deze vooraf aan de installatie heeft ontvangen.

Wanneer het netwerk van uw organisatie is ingedeeld in verschillende segmenten (bijvoorbeeld DMZ's) kan het voordelen bieden om met een relay server te werken. Zo'n server verzamelt informatie van alle aangesloten systemen uit één segment en stuurt dit door naar de Secquard server. Dit zorgt er bijvoorbeeld voor dat u maar één keer een uitzondering hoeft te maken voor uw firewall.

2.1 Vereiste Technische Specificaties

2.1.1 Secquard Server

De aanbevolen specificaties van de server waarop de applicatie wordt geïnstalleerd zijn als volgt:

- OS: Minimaal Windows 2016
- Processor: 2 CPUs
- Intern geheugen: 16 GB
- Opslag: minimaal 50 GB

Let op! Er dient er een Microsoft SQL Server te zijn geïnstalleerd voor de opslag van de data. Gebruik hiervoor SQL Server 2017 Express of nieuwer, en installeer bij voorkeur op dezelfde server als de Secquard applicatie.

2.1.2 Relay Server (Optioneel)

Als u gebruik wilt maken van een relay server om verschillende segmenten uit uw netwerk (zoals DMZ's) aan te sluiten, gebruik dan een systeem met minimaal de volgende specificaties:

- OS: Minimaal Windows 2016
- Processor: 2 CPUs
- Intern geheugen: 16 GB
- Opslag: minimaal 50 GB

2.2 Additionele Voorbereidingen

2.2.1 Connectivity aanpassingen door de opdrachtgever

- Extern: De applicatieserver dient toegang naar buiten te hebben via poort 443 (HTTPS) met de Easy2Audit Licentie server: https://www.easy2audit.com
- Extern: Voor de updates van de software en de content dient de applicatie server toegang naar buiten te krijgen via poort 443 (HTTPS) met de Easy2Audit Update server: https://updates.easy2audit.com
- Extern: Voor installatie van software onderdelen van Microsoft dient er toegang te zijn tijdens installatie van de Secquard applicatie naar Microsoft sites:
  https://*.microsoft.com
- Intern: Alle audit-objecten (servers, clients en databases) die periodiek geaudit moeten worden dienen toegang via poort 443 (HTTPS) te hebben met de applicatie server.
- Toegang via RDP met het Local Admin account,
- FQDN van de server in de locale DNS,
- SSL Certificaat met 3e partij ROOT-CA (self-signed niet toegestaan).

2.2.2 Benodigde accounts en rechten in geval van aparte SQL DB Server

- Voor de Secquard applicatie moet er een domain/local user worden aangemaakt. Deze user moet db_owner zijn op de Secquard database.
- Deze user dient lees/schrijf rechten hebben voor de applicatie code. Standaard wordt de applicatie geïnstalleerd in de /Program Files folder.
- De user wordt als ApplicationPoolIdentity ingesteld voor de ApplicationPool waarin Secquard in Internet Information Service (IIS) zal gaan draaien. De Installer creëert automatisch de ApplicationPool en stelt zelf deze user in als ApplicationPoolIdentity. Om de ApplicationPool te kunnen draaien dienen aan deze user de volgende rechten toegekend te worden:
  -Logon as a service
  -Logon as a batchjob

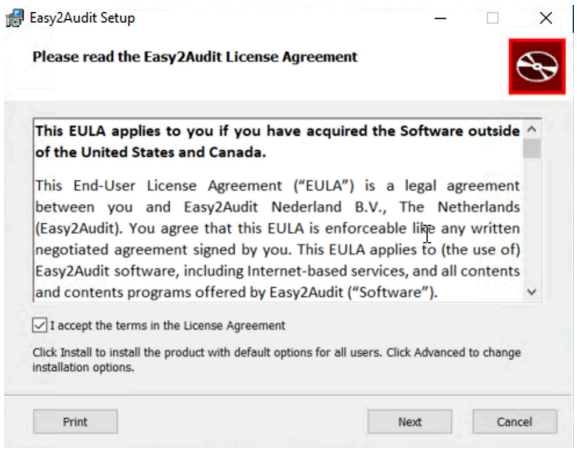
3 Installatie Applicatie

In dit hoofdstuk beschrijven wij hoe de installatie van de applicatie normaal gezien verloopt. U zult dit proces samen met een specialist van Secquard of één van onze partners doorlopen en hoeft hier dus niet zelf mee aan de slag.

De applicatie wordt geïnstalleerd via een installer. De laatste versie van de installer kan worden opgehaald van https://updates.easy2audit.com/Easy2Audit.msi.

Als u de installer start (dubbelklik), krijgt u een overzicht. Klik op more info en vervolgens op Run anyway.

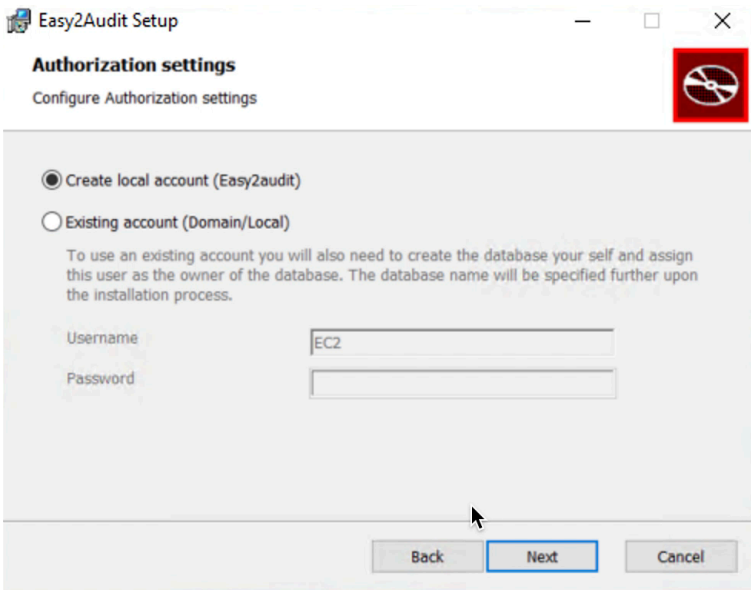
Accepteer, indien akkoord, de voorwaarden met een vinkje en druk op Next.



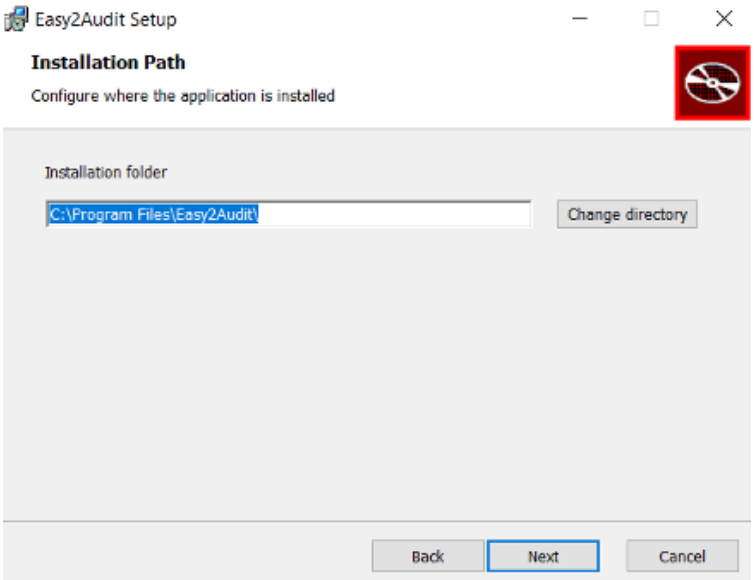
Hierna wordt u gevraagd om een account aan te maken.

Voor een standaardinstallatie maakt u een lokale Easy2Audit gebruiker aan.

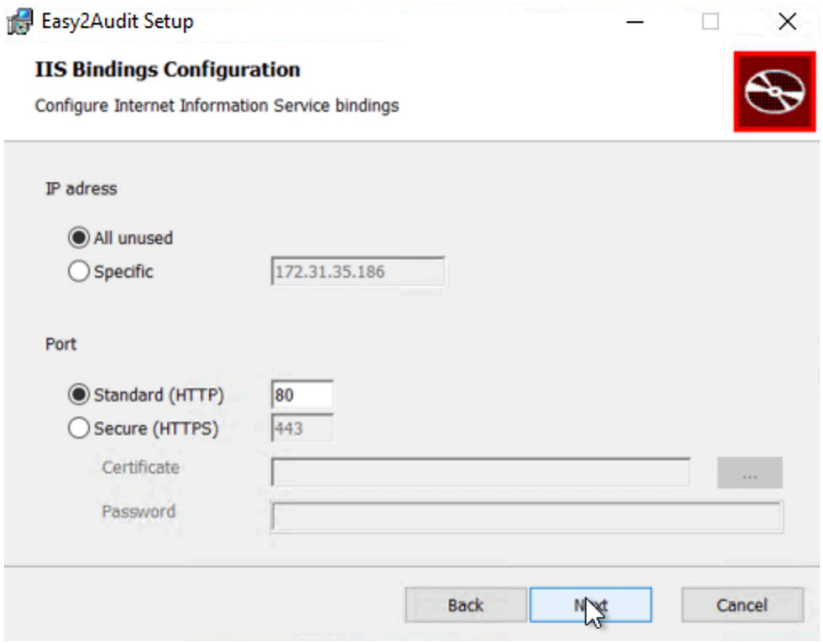
Mocht u de applicatie op een externe database willen aansluiten, dan dient u een gebruiker te kiezen die toegang heeft tot deze database.



Vervolgens kunt u een installatie directory kiezen, standaard is dit de ‘Program Files’ directory.

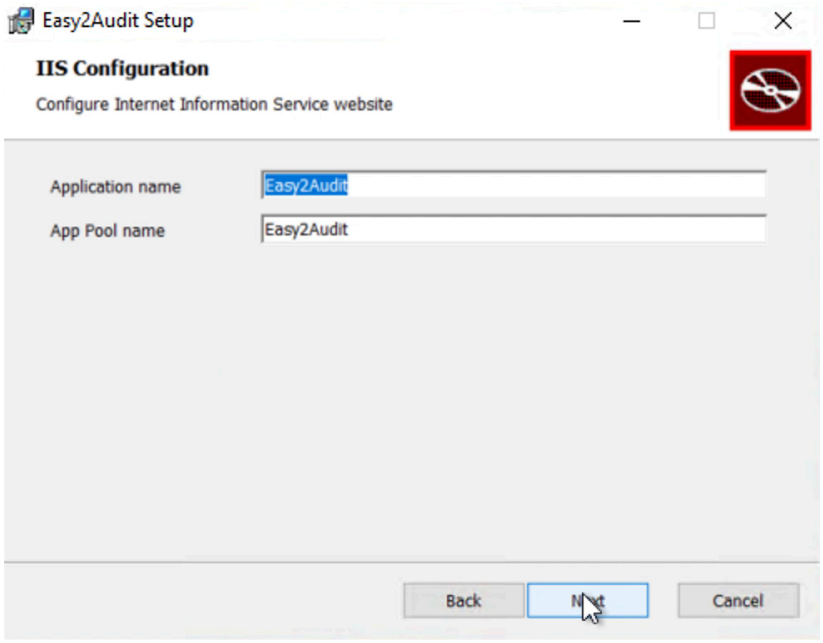


Dan kunt u een IP-adres opgeven en eventueel ook een SSL-certificaat. U kunt deze echter ook op All unused en Standard laten staan.

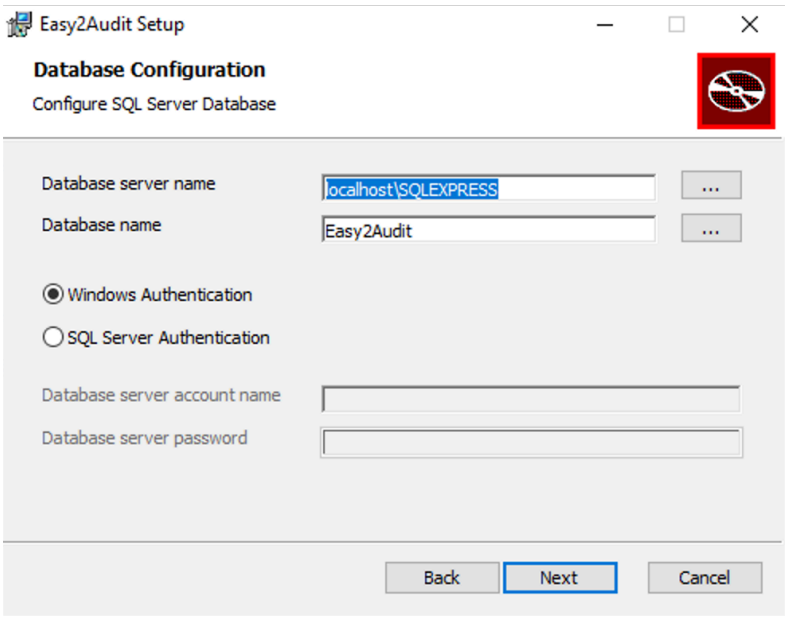


Hierna dient u een naam voor de applicatie en de Applicatie pool voor IIS te kiezen.

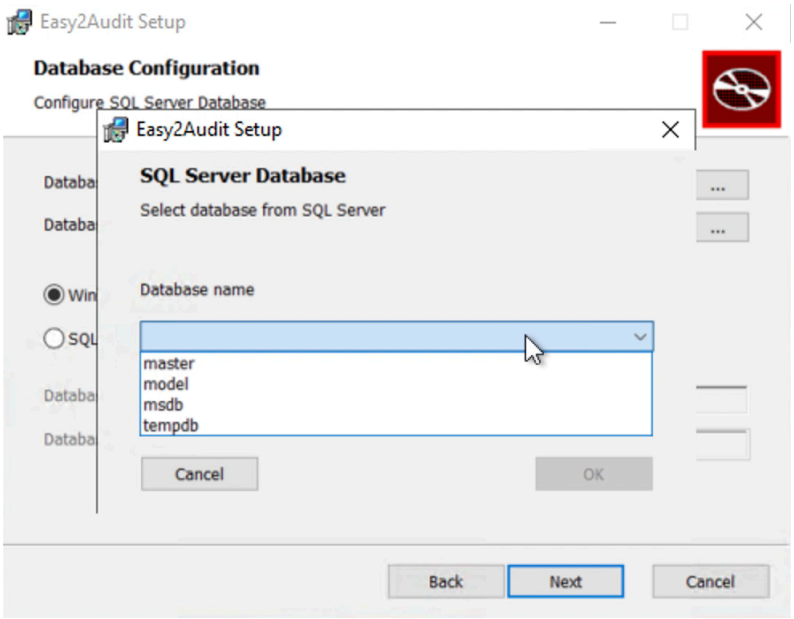
Standaard is dit ‘Easy2Audit’.



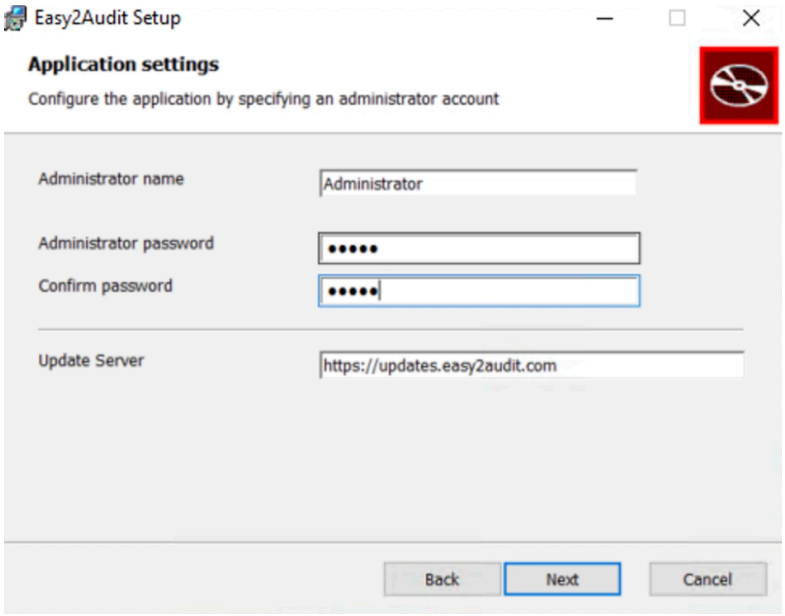
Vervolgens komt u in onderstaand scherm. De informatie die vooraf staat ingevuld kunt u voor de standaard installatie laten staan.



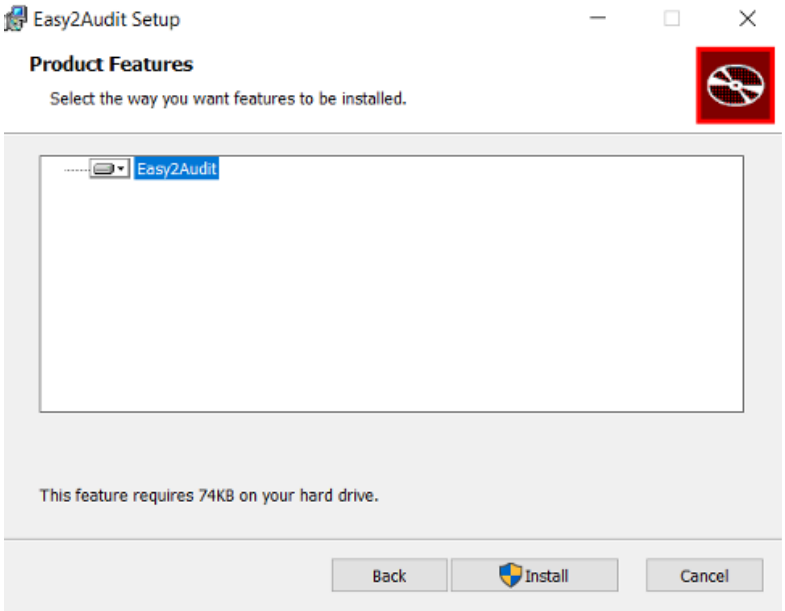
Als u wilt controleren of u de juiste database server name heeft ingesteld, klik dan op de 3 puntjes naast database name (zie hierboven). Wanneer hier onderstaand lijstje verschijnt met master, model etc, dan zit u goed.



Als laatste kiest u een inlognaam en wachtwoord. Die kunt u na de installatie altijd wijzigen.



U kunt de installatie nu starten, druk op ‘Install’.



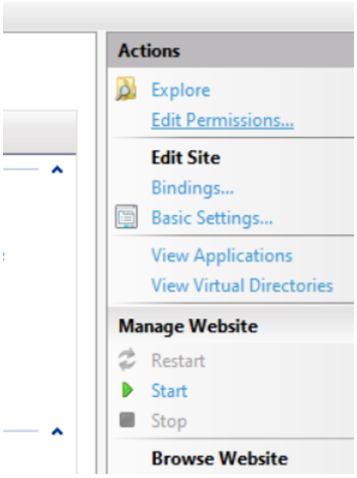
Als de installatie succesvol is verlopen kunt u verder met de inrichting.

3.1 Inrichting

Na installatie Kunt u de applicatie via een webbrowser bereiken. De installer opent automatisch deze pagina. Later kunt u deze via localhost, of het IP-adres van de server bereiken.

Vaak wilt u het adres van de applicatie na de installatie veranderen. Dit kan door via de IIS Manager de binding te wijzigen. Heeft u hier geen behoefte aan, dan kunt u dit gedeelte overslaan.

3.1.1 Binding wijzigen



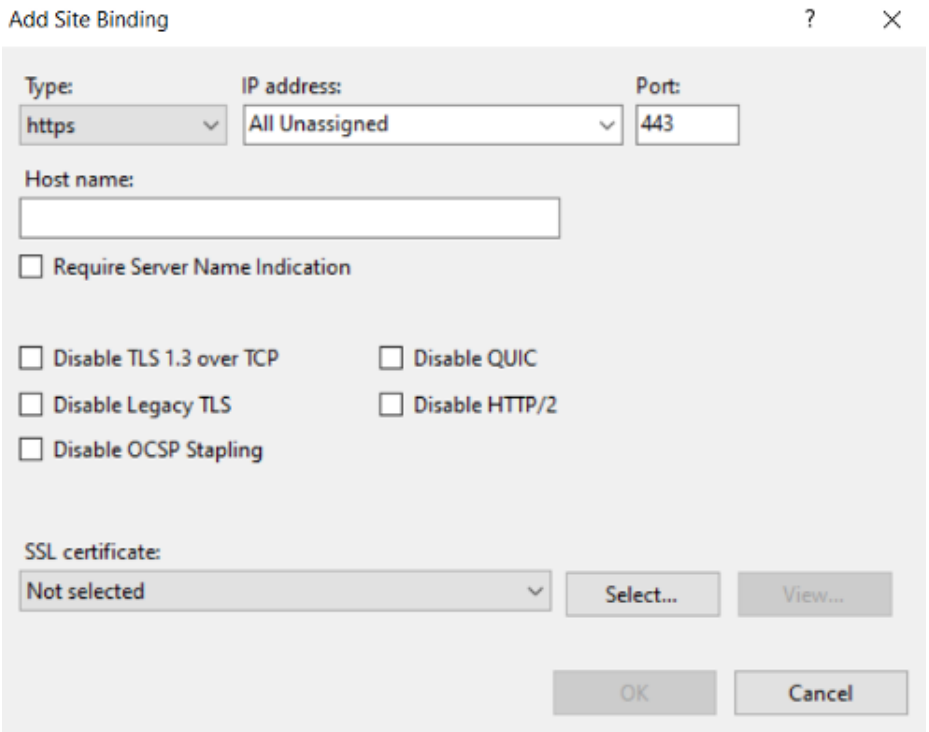
Indien u een eigen hostname wil geven of het IP-nummer wil veranderen dan kan dit via de IIS Manager.

U kunt de IIS Manager opstarten door in de zoekfunctie van uw werkstation te zoeken naar `inetmgr`.

Binnen de IIS Manager selecteert u aan de linkerkant onder sites, de site Easy2Audit.

Vervolgens selecteert u aan de rechterkant de optie **Bindings...**

Hier kunt u de bestaande binding wijzigen of een nieuwe binding aanmaken. Zorg ervoor dat het type op **HTTPS** staat. Hierdoor is al het dataverkeer versleuteld. U moet hier ook het certificaat toevoegen voor de geldigheid van uw HTTPS/SSL-verbinding.



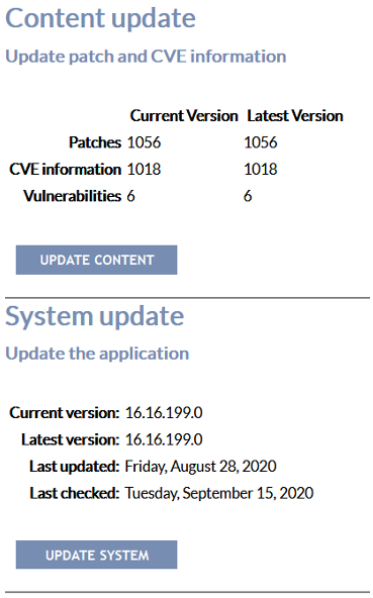
3.2 Starten en configureren van de applicatie

3.2.1 Updates

Het starten van de applicatie via de webbrowser duurt de eerste keer een paar minuten. Dit komt omdat alle recente data wordt ingelezen en geüpdatet.

Updates gebeuren automatisch via de Easy2Audit Service. U kunt dit echter ook handmatig doen.

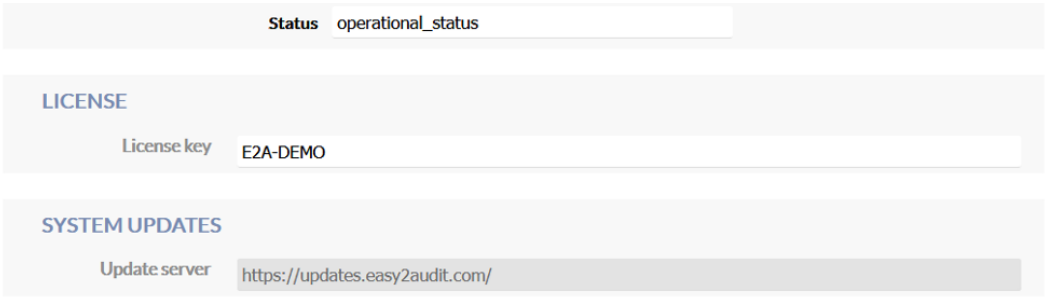
Na inloggen is de status te zien via het menu Options —> Updates:



3.2.2 Licenties

Als laatste dient de licentiesleutel te worden ingesteld. Deze licentiesleutel wordt door Secquard aan u geleverd.

Het instellen van de licentie gaat via het menu: Options->Setup in de Secquard applicatie.

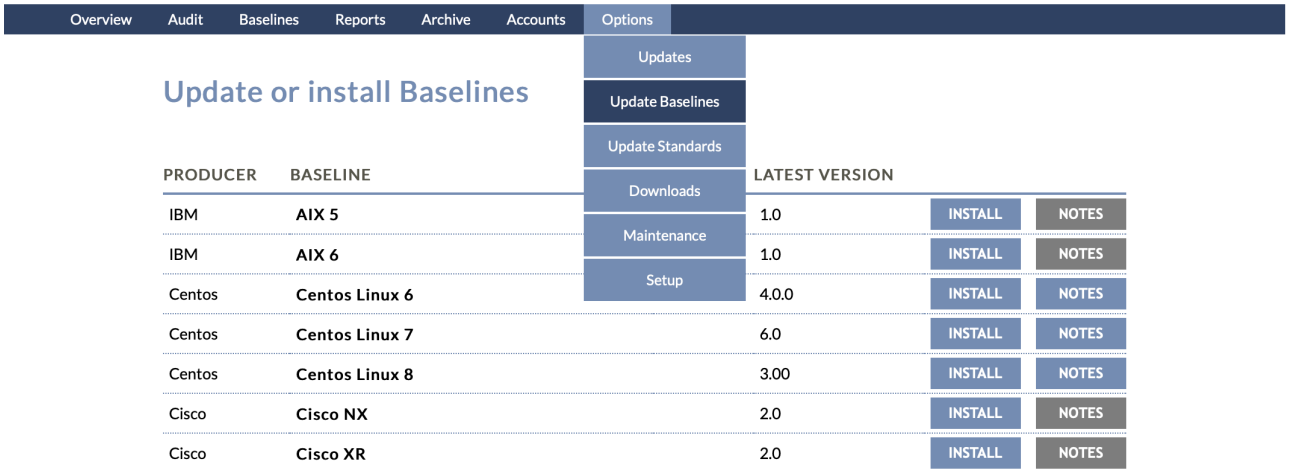


3.2.3 Selecteren van baselines en downloaden van scripts

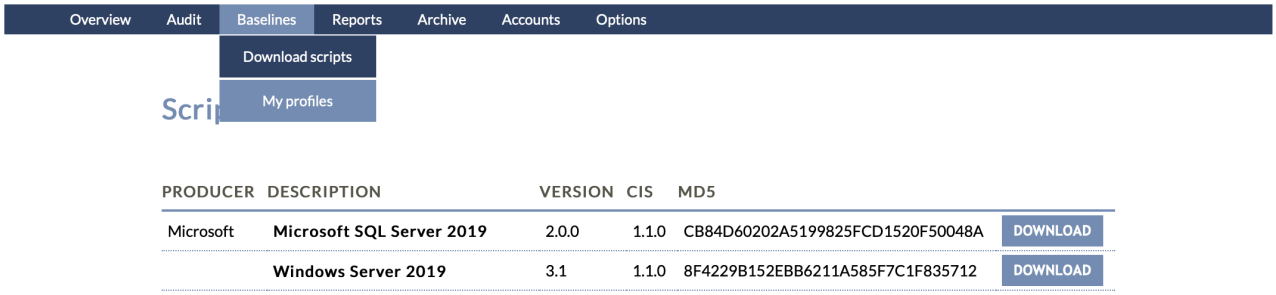
Om de applicatie te kunnen gebruiken, dient u de servers die u wilt auditen aan te sluiten. Dit doet u door middel van scripts. Deze kunt u in de applicatie downloaden, voordat u deze scripts kunt downloaden dient u de baselines te installeren. Het proces is kort en snel en werkt als volgt:

Installeer eerst de benodigde baselines. Inventariseer vooraf welke operating systems aangesloten worden, zodat u direct aan de slag kunt. Ga naar het menu: Options -> Update Baselines.

Hier vindt u een lijst met baselines die u kunt updaten of installeren door op de INSTALL knop te drukken, doe dit voor elke baseline die u nodig heeft.

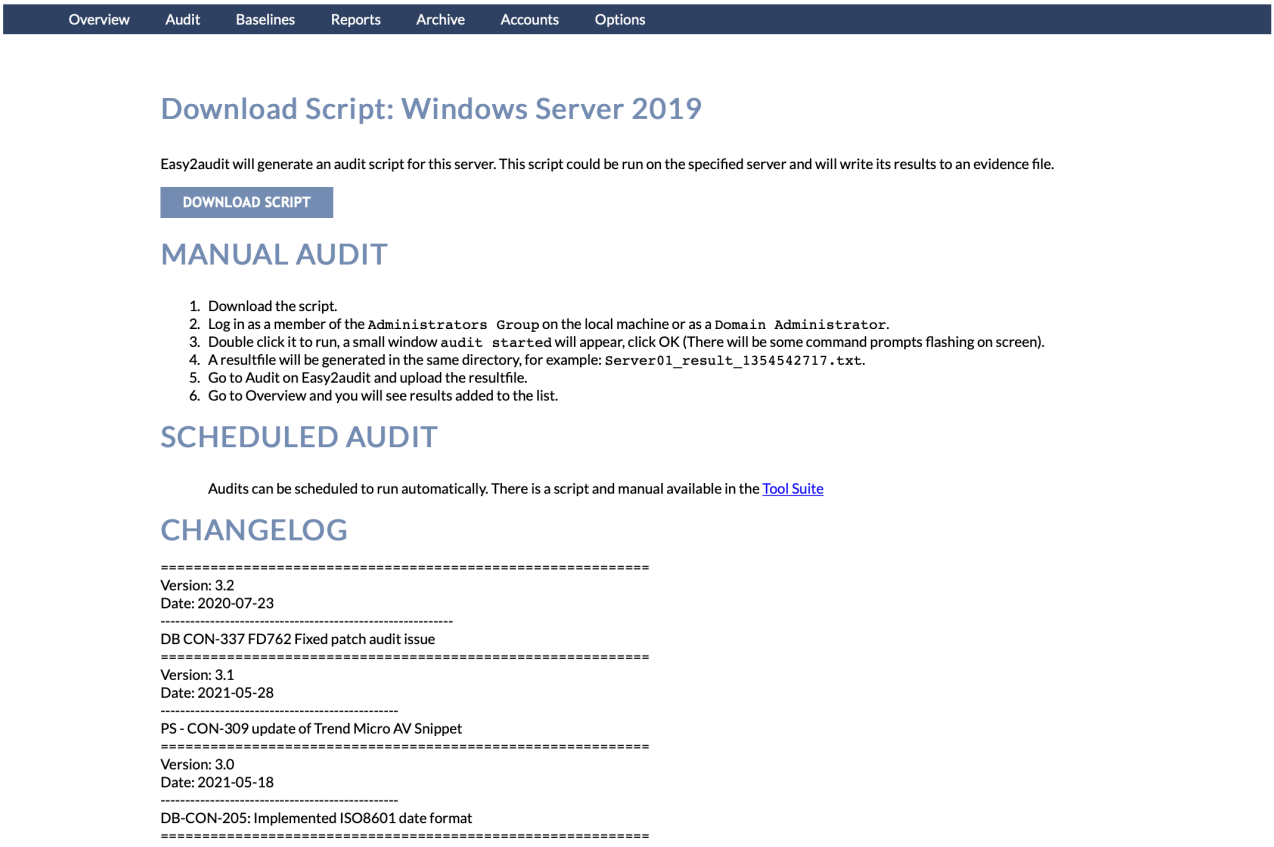


Als u dit heeft gedaan vindt u de bijbehorende scripts onder het menu: Baselines -> Download Scripts.



Klik op download.

U komt nu op onderstaande pagina (of vergelijkbaar), waar u via de DOWNLOAD SCRIPT-knop uw script download. Instructies voor het runnen van het script worden daarnaast in 6 stappen beschreven. Wij raden u aan om eerst de stappen te herhalen zodat u alle benodigde scripts heeft gedownload en daarna het volgend hoofdstuk uit deze handleiding door te nemen, waarin het aansluiten van systemen uitgebreider wordt beschreven.



4 Aansluiten Windows Systemen

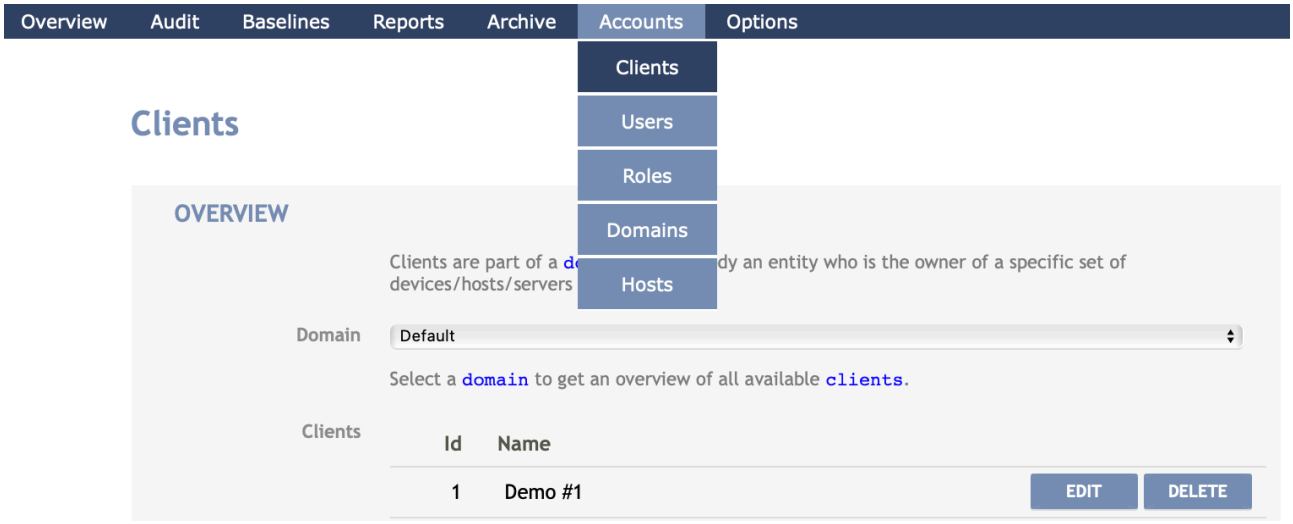
In dit hoofdstuk wordt het aansluiten van Windows systemen op onze applicatie beschreven. Dit proces zult u doorlopen met een specialist van Secquard, of één van onze partners. U kunt het hoofdstuk tevens als naslagwerk gebruiken.

4.1 Voorbereiding

Voordat u uw Windows systemen aansluit, dient u de Secquard applicatie te installeren, als u dit nog niet heeft gedaan kunt u hiervoor hoofdstuk 3 van deze handleiding raadplegen.

Het resultaat van de server die u gaat auditen moet aan een client worden toegekend.

Als eerste moeten we de URL van de applicatie server en het client-ID bij de hand hebben. Het client ID kunnen we vinden onder het menu '*Account* > *Clients*'. Let op dat u het ID gebruikt, en niet de naam. Het ID is in onderstaand voorbeeld dus 1.



De server die u audit moet daarnaast toegang hebben tot de applicatie server. Dit kan eenvoudig gecontroleerd worden door vanuit de server met een internetbrowser naar de applicatie-server te gaan. Als het goed is verschijnt de login pagina van de applicatie.

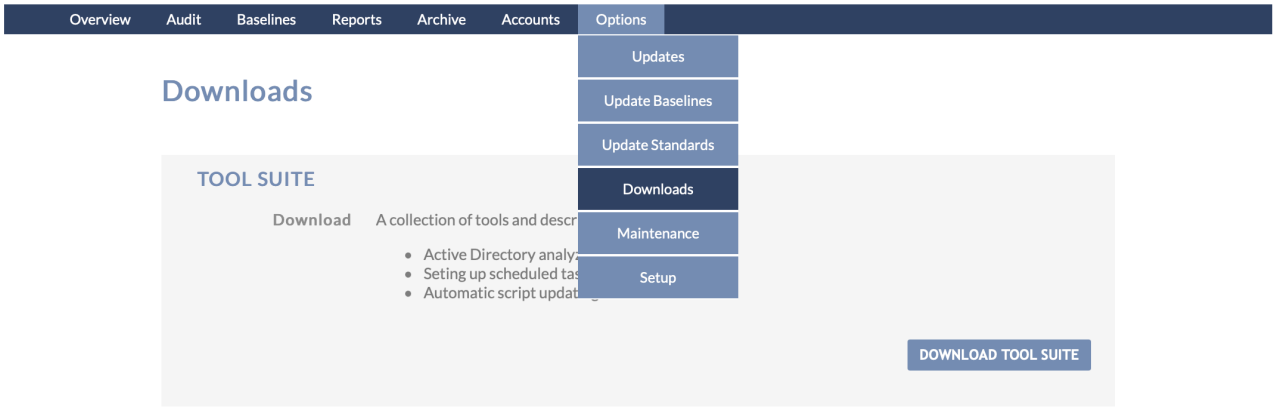
Als de applicatie is geïnstalleerd kunnen er servers op worden aangesloten, dit gebeurt met scripts.

4.2 Aansluiten Windows Systemen

Als voorbeeld nemen we een Windows 2016 Server, maar in de basis geldt dit voor iedere Windows server die geaudit moeten worden.

Voor het instellen van een audit heeft u een aantal bestanden nodig.

Deze bestanden kunt u downloaden via de Secquard tool suite (Options -> Downloads -> DOWNLOAD TOOL SUITE, zie plaatje hieronder). Als u de tool suite heeft gedownload, vindt u een zip-file met daarin een tools map en daarin een aantal mappen met bestanden.



Hiervan heeft u de volgende bestanden nodig, sommige bestanden bestaan ook in andere mappen en dragen dezelfde naam maar kunnen toch van inhoud verschillen, zorg dus dat u bestanden uit de juiste mappen haalt. Wij gaan er in dit geval vanuit dat u uw resultaten naar één Secquard server wilt sturen (als dit niet het geval is, heeft u de MULTI variant nodig)

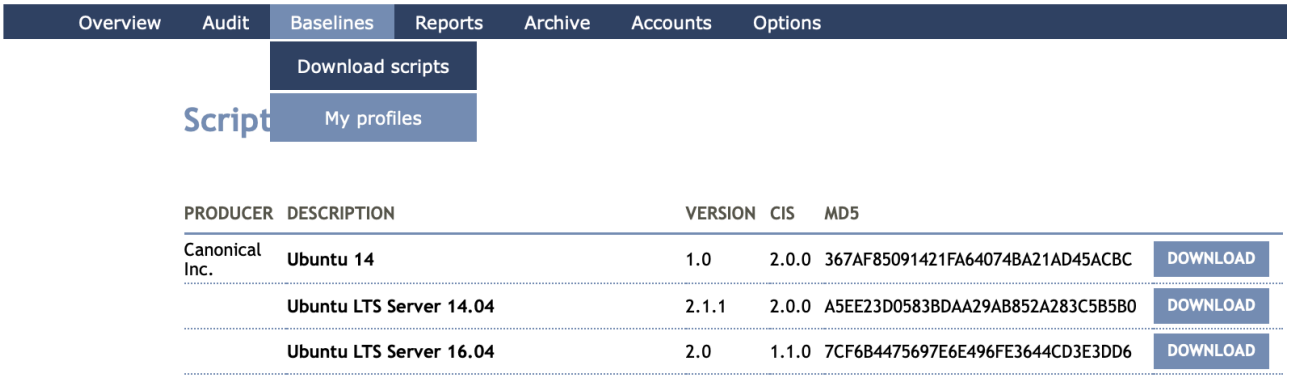
- `tools\SINGLE Client audit scripts\Microsoft Server&Windows SINGLE Client auto script update\`**`audit-start.js`**
- `tools\SINGLE Client audit scripts\Microsoft Server&Windows SINGLE Client auto script update\`**`e2a.cfg`**
- `tools\Scheduled Task Generators\Secquard Microsoft Server&Windows Scheduler\`**`schedule.bat`**

Maak op de server die geaudit moet worden een directory aan (bijvoorbeeld C:\secquard) en zet alle bestanden hierin.

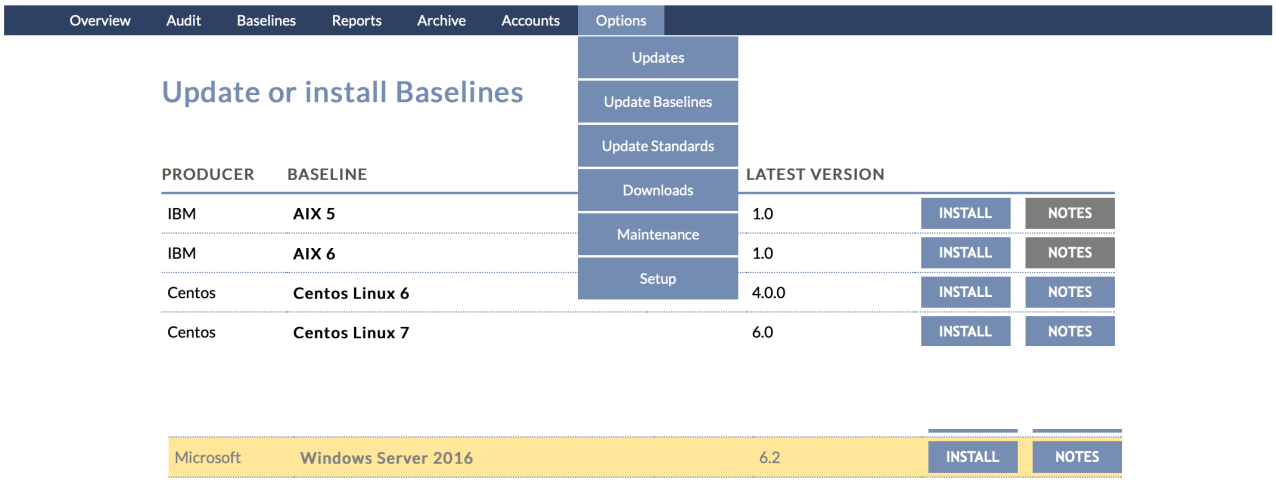
Plaats hierbij ook het `audit.js` bestand. Hoe u deze ophaalt, wordt besproken in de volgende paragraaf.

4.2.1 Basis script

Het basis script (`audit.js`) voert alle controles (de audit) uit. Dit bestand kunt u downloaden via het menu ' *Baseline->Download scripts'*.



Uit deze lijst kunt u het juiste script kiezen, in dit geval scrollt u naar beneden en selecteert u het Windows server 2016 script. Als het benodigde script niet in deze lijst staat, of u wilt controleren of u de laatste versie heeft, navigeert u naar Options -> Update Baselines, klik op Install naast de juiste baseline (in dit geval windows Server 2016).



Als u terug navigeert naar Baseline -> Download scripts klikt u op de DOWNLOAD knop naast Windows Server 2016.

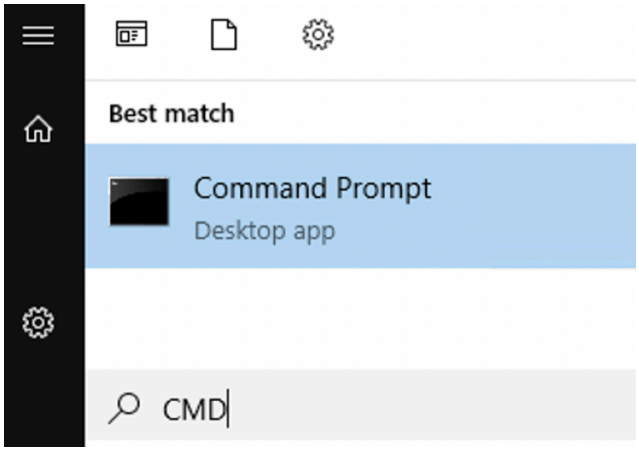
Vervolgens klikt u op DOWNLOAD SCRIPT om het script te downloaden. Deze zal als `audit.js` worden opgeslagen.

Plaats dit bestand bij de andere installatie-bestanden (bijvoorbeeld in C:\secquard).

4.2.2 Handmatige audit

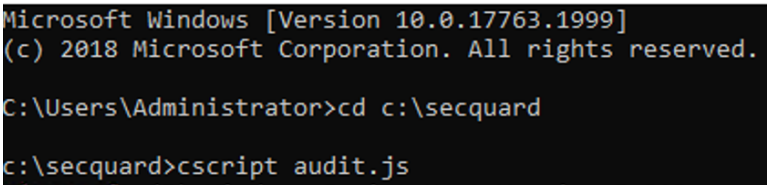
U kunt een handmatige audit uitvoeren door via de **command line** het `audit.js` script uit te voeren. Let op: Als u geautomatiseerd audits wilt uitvoeren, zie volgende paragraaf.

Open hiervoor de Windows zoek functionaliteit (met de windows knop bijvoorbeeld) en typ ‘CMD’ (zonder aanhalingstekens, klik hierop met de rechter muisknop en kies de optie ‘**Run as Administrator**’ (evt. via rechter muisknop).

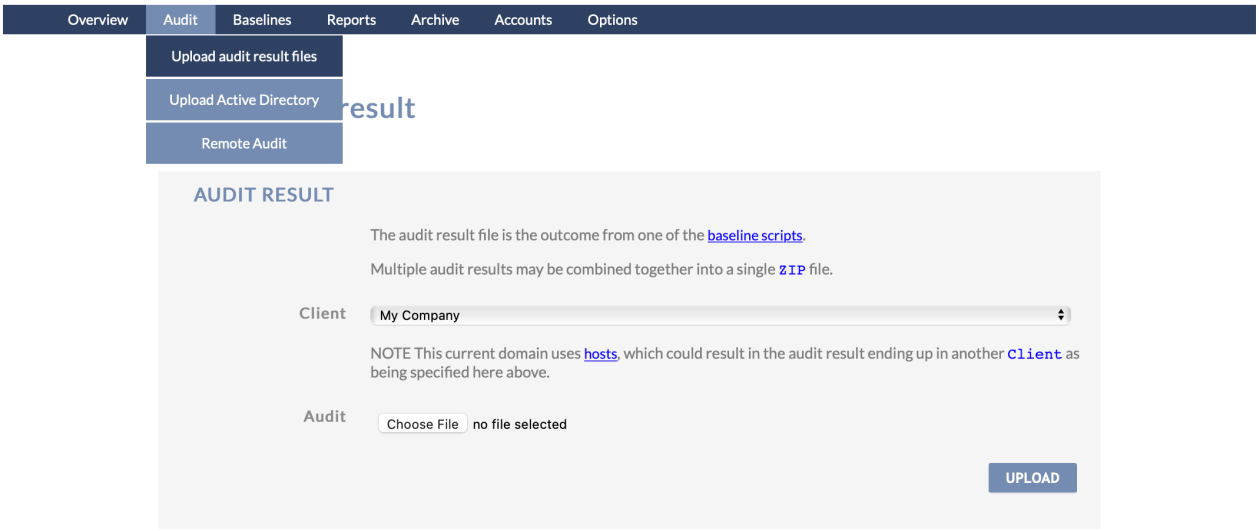


Navigeer naar de directory waar de bestanden staan (bijvoorbeeld met cd c:\secquard) en voer het onderstaande commando uit:

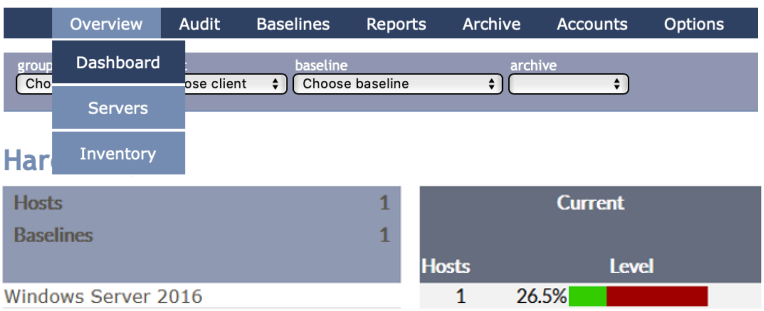
```
cscript audit.js.
```



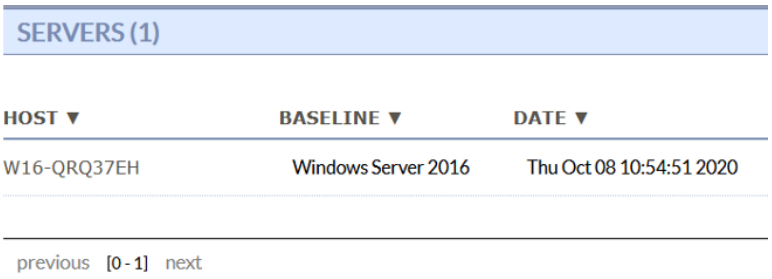
Het script wordt uitgevoerd, dit resulteert in een tekstbestand (.txt). Dit bestand kunt u inlezen in de applicatie via het menu '*Audit-> Upload audit result files*'



Het resultaat kunt u direct vinden op het dashboard (*Overview -> Dashboard*).



Via het menu ‘Overview -> Servers’ kunt u zien wanneer de audit heeft plaatsgevonden:



4.2.3 Automatische audit uploaden

Om een audit resultaat direct naar de applicatie te sturen — dus zonder handmatige upload — kunt u het script `audit-start.js` gebruiken. Stel eerst de configuratie goed in. Dit doet u in het bestand `e2a.cfg`. Dit bestand bevat 3 regels, de eerste regel is de locatie van de applicatie, de 2de regel is het client-ID waarvan u het resultaat wilt inlezen (zie paragraaf 1. Voorbereiding), de derde regel bepaalt of u altijd de laatste baseline versie wilt gebruiken. Wij raden sterk aan deze waarde op update te zetten.

Een `e2a.cfg` bestand ziet er als volgt uit:

```
https://demo.easy2audit.com
1
Update
```

Om te testen of de configuratie werkt, kunt u de audit via de command line uitvoeren, op dezelfde manier waarop u ook een handmatige uitvoert maar nu met het commando:

```
cscript audit-start.js
```

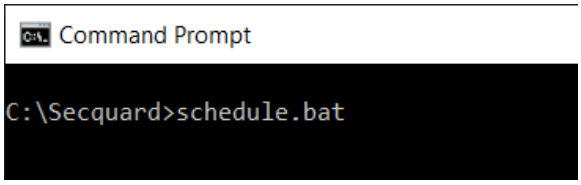
Het resultaat wordt nu automatisch ingelezen, dit kunt u terugvinden op het dashboard en bij de ingelezen servers.

4.2.4 Periodieke automatische audit

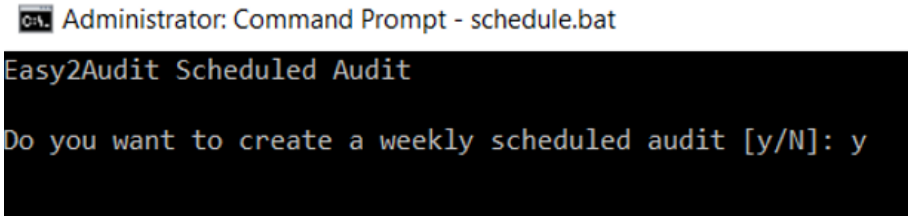
Via een *scheduled task* kan de audit periodiek worden uitgevoerd. Om dit eenvoudig te maken hebben we hiervoor een script gemaakt: `scheduler.bat`. Via dit script stelt u de audit via de Microsoft Task Scheduler in.

Met dit script creëert of wijzigt u dus een scheduled task. Als u het script vaker uitvoert worden alleen de laatste instellingen opgeslagen.

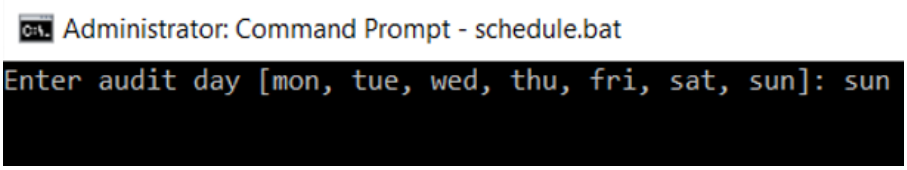
Via de command line kunt u dit batch script uitvoeren. U wordt door een aantal vragen geleid, waarna een volgend script wordt aangemaakt.



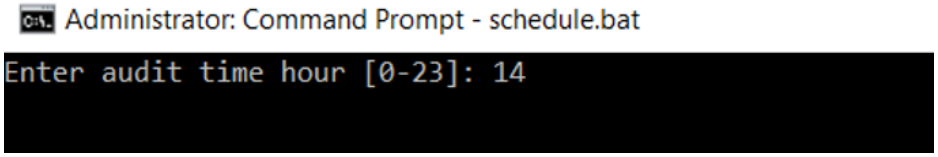
U moet eerst bevestigen of u een taak wilt aanmaken of wijzigen:



Kies vervolgens de dag dat u de audit wilt uitvoeren:

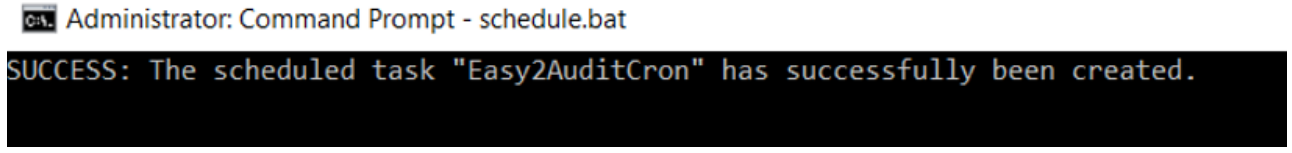


En als laatste het tijdstip dat u de audit uitgevoerd wilt hebben:



Er wordt bij de tijd een willekeurig aantal minuten gekozen om te voorkomen dat veel scripts op exact hetzelfde tijdstip worden uitgevoerd.

De taak is nu aangemaakt en zal periodiek worden uitgevoerd. Om wijzigingen aan te brengen kunt u schedule.bat opnieuw draaien, of de Easy2AuditCron taak in de Windows taakplanner opzoeken. Deze planner bereikt u bijvoorbeeld door Task Scheduler in te typen en uit te voeren via de Windows zoekfunctie.



4.2.5 Deployen van het serverpark

In dit voorbeeld hebben we alles handmatig ingesteld. Als u een groot aantal servers heeft, is het beter om dit geautomatiseerd te doen. Dit kan bijvoorbeeld via de group policy om te zorgen dat alle servers uit het domein automatisch gescheduled worden. U kunt hierbij de `scheduler.bat` gebruiken als uitgangspunt.

5 Aansluiten Linux Systemen

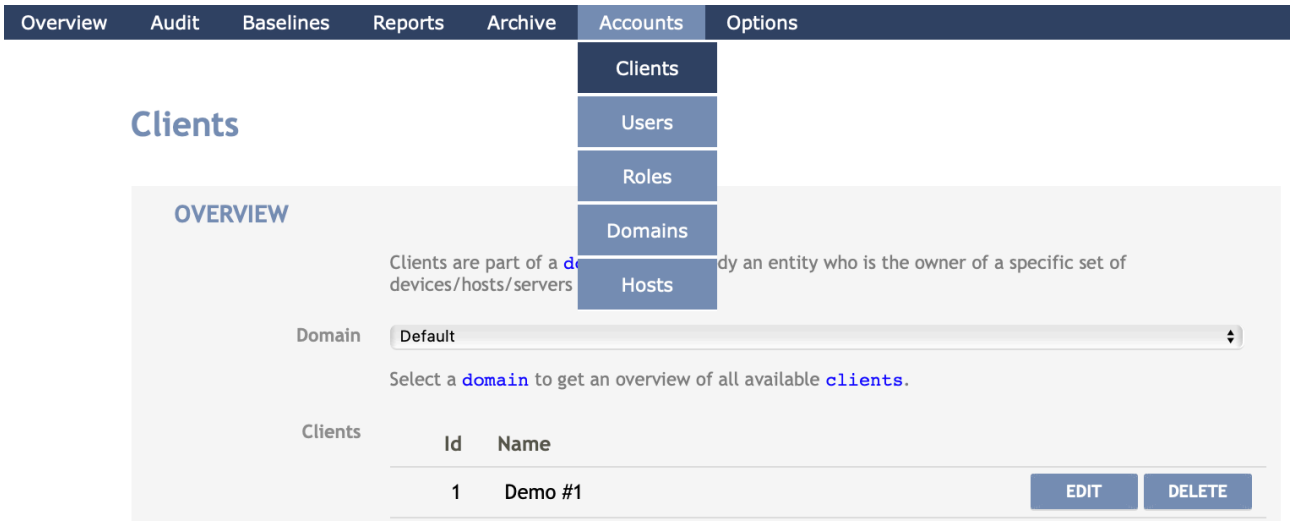
In dit hoofdstuk wordt het aansluiten van Windows systemen op onze applicatie beschreven. Dit proces zult u doorlopen met een specialist van Secquard, of één van onze partners. U kunt het hoofdstuk tevens als naslagwerk gebruiken.

5.1 Voorbereiding

Voordat u uw Linux systemen aansluit, dient u de Secquard applicatie te installeren, als u dit nog niet heeft gedaan kunt u hiervoor de 'Secquard handleiding installatie applicatie' raadplegen.

Het resultaat van de server die u gaat auditen moet aan een client worden toegekend.

Als eerst moeten we de URL van de applicatie server en het client-ID bij de hand hebben. Het client ID kunnen we vinden onder het menu '*Account* > *Clients*'. Let op dat u het ID gebruikt, en niet de naam. Het ID is hier dus 1.



De server die u audit moet daarnaast toegang hebben tot de applicatie server. Dit kan eenvoudig gecontroleerd worden door vanuit de server met de browser naar de applicatie-server te gaan. Als het goed is verschijnt de login pagina van de applicatie.

Nadat de applicatie is geïnstalleerd kunnen er servers op worden aangesloten, dit gebeurt met scripts.

5.2 Aansluiten Systemen

Als voorbeeld nemen we een Red Hat 7 server, maar in de basis geldt dit voor iedere Red Hat Linux variant die geaudit moeten worden.

Voor het instellen van een audit heeft u 3 bestanden nodig, deze vindt u in de Secquard tool suite, die u kunt downloaden via het menu in de applicatie: Options -> Downloads -> DOWNLOAD TOOL SUITE. U vindt de eerste 2 bestanden in de volgende map:

`tools/SINGLE Client audit scripts/Linux SINGLE Client auto script update`

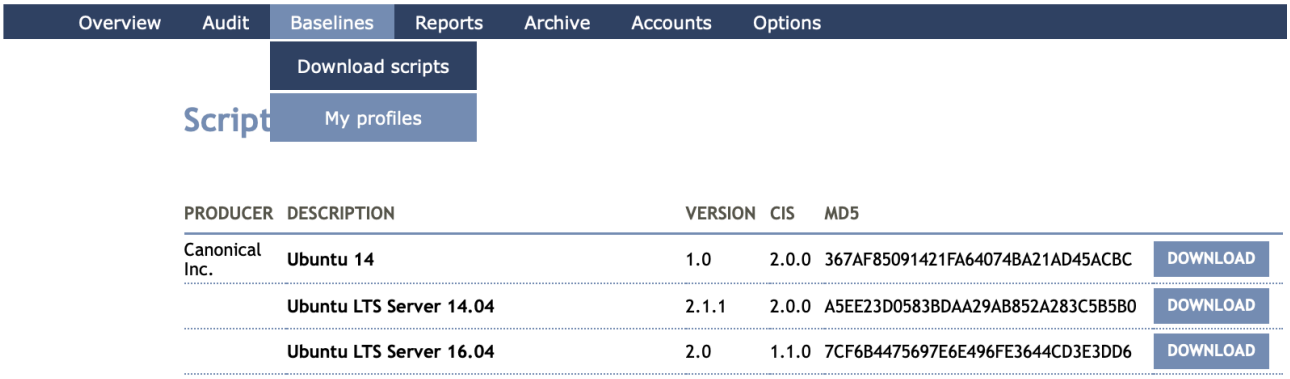
- `e2a.cfg`
- `audit-start.sh`
- `audit.sh`

Maak op de server die u wilt auditen een directory aan (bijvoorbeeld /secquard) en zet de bestanden hierin.

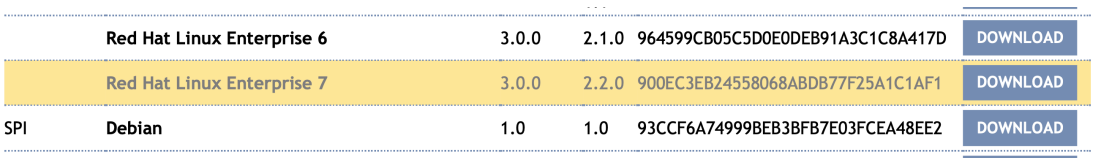
Hoe u het basis script (`audit.sh`) ophaalt, bespreken wij in de volgende paragraaf.

5.2.1 Basis script

Het basis script (`audit.sh`) voert alle controles uit. Dit bestand kunt u downloaden via het menu ‘ *Baseline->Download scripts’*.

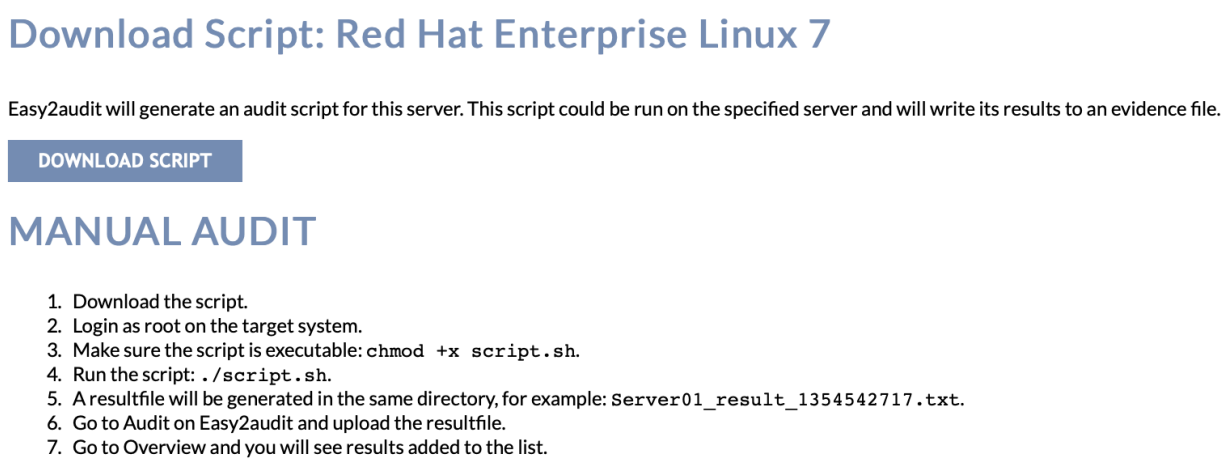


Uit deze lijst kunt u het juiste script kiezen, in dit geval scrollt u naar beneden en selecteert u het Red Hat Enterprise Linux 7 script.



Wanneer u het benodigde script hier niet tussen ziet staan, ga dan naar het menu: Options -> Update baselines, en klik op install bij de juiste baseline. Wanneer u nu terug navigeert naar Baselines -> Download scripts, zal de baseline erbij staan.

Als up op download klikt komt u op de pagina van Red Hat Enterprise Linux 7, vervolgens klikt u op download om het script te downloaden. Deze zal als `audit.sh` worden opgeslagen.



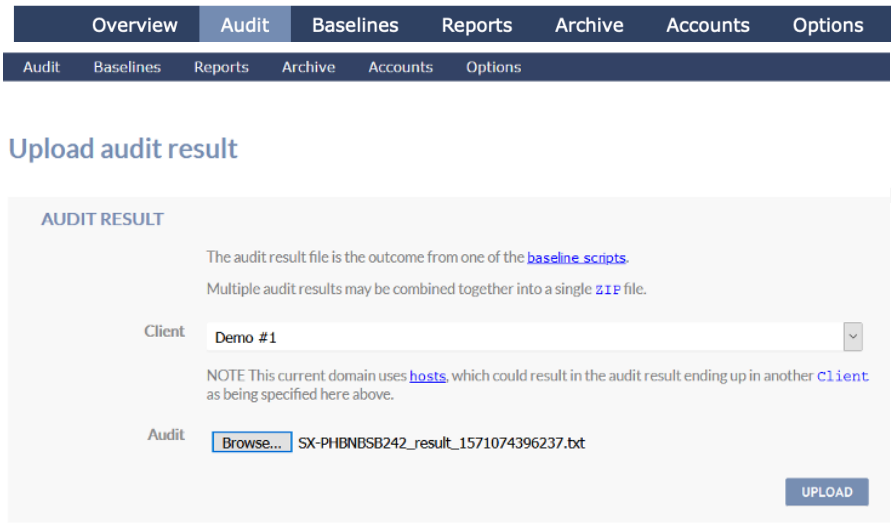
Plaats dit bestand bij de andere installatie-bestanden (bijvoorbeeld in /secquard).

5.3 Handmatige audit

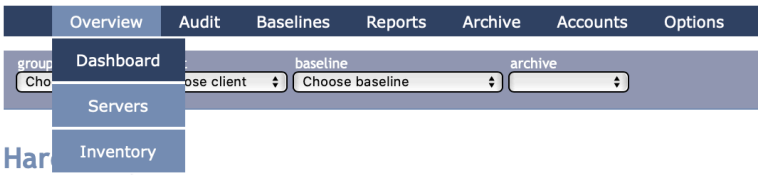
U kunt een handmatige audit uitvoeren door via de command line het audit.sh script uit te voeren.
Zorg er wel voor dat u als **root** (of met root rechten) bent ingelogd.
Ga naar de juiste directory waar de bestanden staan en voer het commando onderstaande commando uit:

```
./audit.sh
```

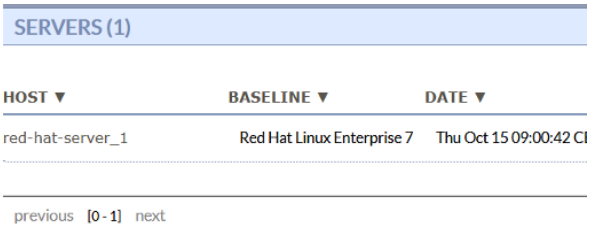
Het script wordt uitgevoerd, dit resulteert in een tekstbestand (.txt). Dit bestand kunt u inlezen in de applicatie via het menu ‘Audit->Upload audit result files’.



Het resultaat kunt u direct vinden op het dashboard (Overview > Dashboard).



En via het menu ‘Overview > Servers’ kunt u ook zien wanneer de audit heeft plaatsgevonden:



5.4 Automatische audit uploaden

Om een audit resultaat direct naar de applicatie te sturen — dus zonder handmatige upload — kunt u het script `audit-start.sh` gebruiken. Stel eerst de configuratie goed in. Dit doet u in het bestand `e2a.cfg`. Dit bestand bevat 3 regels, de eerste regel is de locatie van de applicatie, de 2de regel is het client-ID waar u het resultaat wilt inlezen (zie paragraaf 1. Voorbereiding). De derde regel bepaalt of u altijd de laatste baseline versie wilt gebruiken. Wij raden sterk aan deze waarde op update te zetten.

Een `e2a.cfg` bestand ziet er dus als volgt uit:

```
https://demo.easy2audit.com
1
Update
```

Om te testen of de configuratie werkt kunt u de audit via de command line uitvoeren, op dezelfde manier waarop u ook een handmatige uitvoert maar nu met het commando:

```
./audit-start.sh
```

Het resultaat wordt nu automatisch ingelezen, dit kunt u terugvinden op het dashboard en bij de ingelezen servers.

5.5 Periodieke automatische audit

Via een scheduled task kan de audit periodiek worden uitgevoerd. Hiervoor moet er in de crontab een cronjob regel worden aangemaakt.

Om de audit op zondag om 14 uur uit te voeren dient u de volgende regel toe te voegen:

```
1 14 * * 7 /Secquard/audit-start.sh > /dev/null 2>&1
```

5.6 Deployen van het serverpark

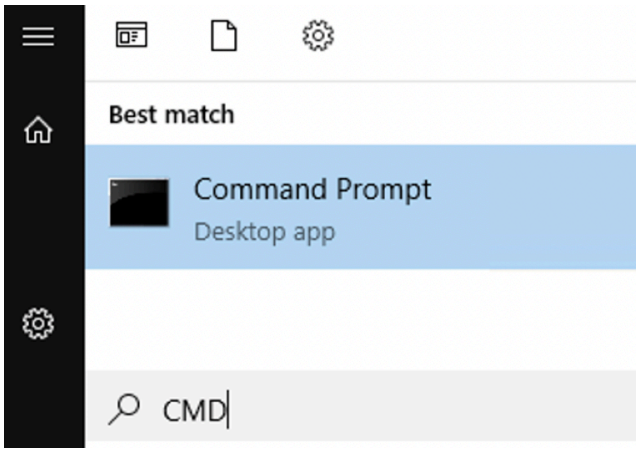
In dit voorbeeld stellen we alles handmatig in. Als u een groot aantal servers heeft is het beter om dit geautomatiseerd te doen. Hiervoor dient u de bestanden op de juiste plek te zetten en de cronjob toe te voegen. Voeg daarvoor deze taken toe aan uw eigen deploy systeem.

6 Het uitvoeren van een active directory (AD) analyse

Het uitvoeren van een AD analyse gebeurt handmatig. Hiervoor heeft u toegang nodig tot de server waar de active directory zich bevindt.

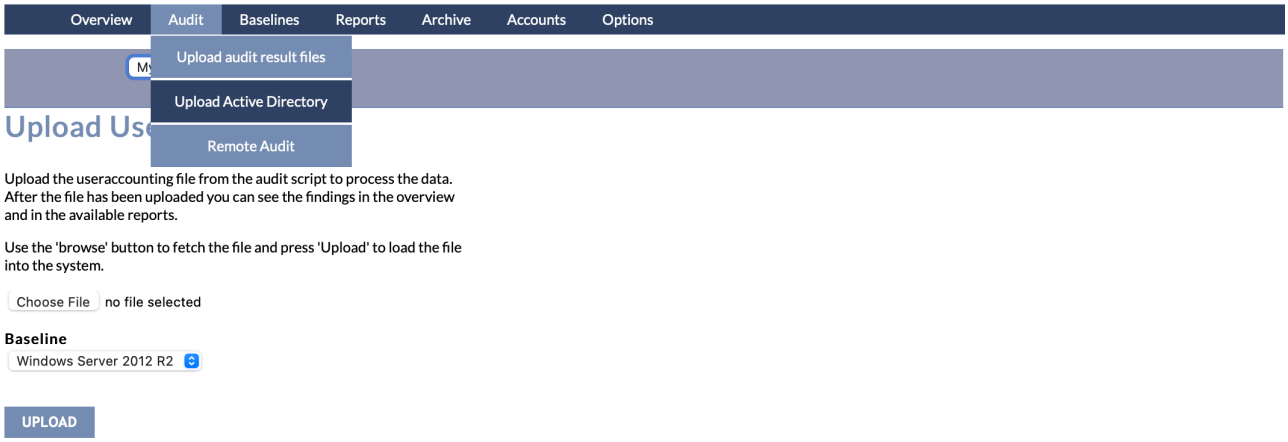
Op deze server kunt u het `e2a_ad.js` script draaien. Dit script kunt u bemachtigen door de tool suite te downloaden, dit doet u in de applicatie via het menu: Options -> Downloads -> Download Tool Suite. U vindt het script in de `Secquard Manual AD Export` map.

Download het script op de server waar de AD zich bevindt en run het daar. Open hiervoor op de betreffende server de Windows zoekfunctie (met de windows knop bijvoorbeeld) en typ ‘CMD’ (zonder aanhalingstekens), klik hierop met de rechter muisknop en kies de optie ‘**Run as Administrator**’ (evt. via rechter muisknop).



Navigeer naar de locatie waar het script zich bevindt of plaats het script op de locatie waar u zich bevindt en run het script middels het volgende commando: `cscript e2a_ad.js`.

Dit resulteert in een .csv bestand dat u kunt uploaden in de Secquard applicatie. Ga hiervoor (nog steeds op dezelfde server) in de Secquard applicatie naar het menu: Audit -> Upload Active Directory. selecteer een baseline en upload het bestand. De resultaten zijn direct beschikbaar via het dashboard overzicht.



7 Het selecteren van profielen

Met Secquard's profielen kunt u de SOLL waarden voor controls wijzigen, of ervoor zorgen dat controls niet worden meegenomen in de audits. Dit kan dus zorgen voor hogere scores, terwijl uw veiligheid er niet op vooruit gaat! Het is dus van cruciaal belang om uiterst zorgvuldig om te gaan met deze functionaliteit.

Een voorbeeld: Als wordt voorgeschreven dat uw wachtwoordlengte minimaal 12 dient te zijn, kunt u ervoor kiezen om deze op 8 te zetten. Zo kunt u er dus voor zorgen dat uw systemen minder streng worden gecontroleerd (en toch positief scoren). Dit kan leiden tot onveilige situaties. Wanneer u toch een uitzondering maakt, zorg er dan voor dat u hiervoor een zeer goede reden heeft en dat u deze zorgvuldig documenteert in de daarvoor bedoelde vakken in de Secquard applicatie.

CIS level 1 en level 2

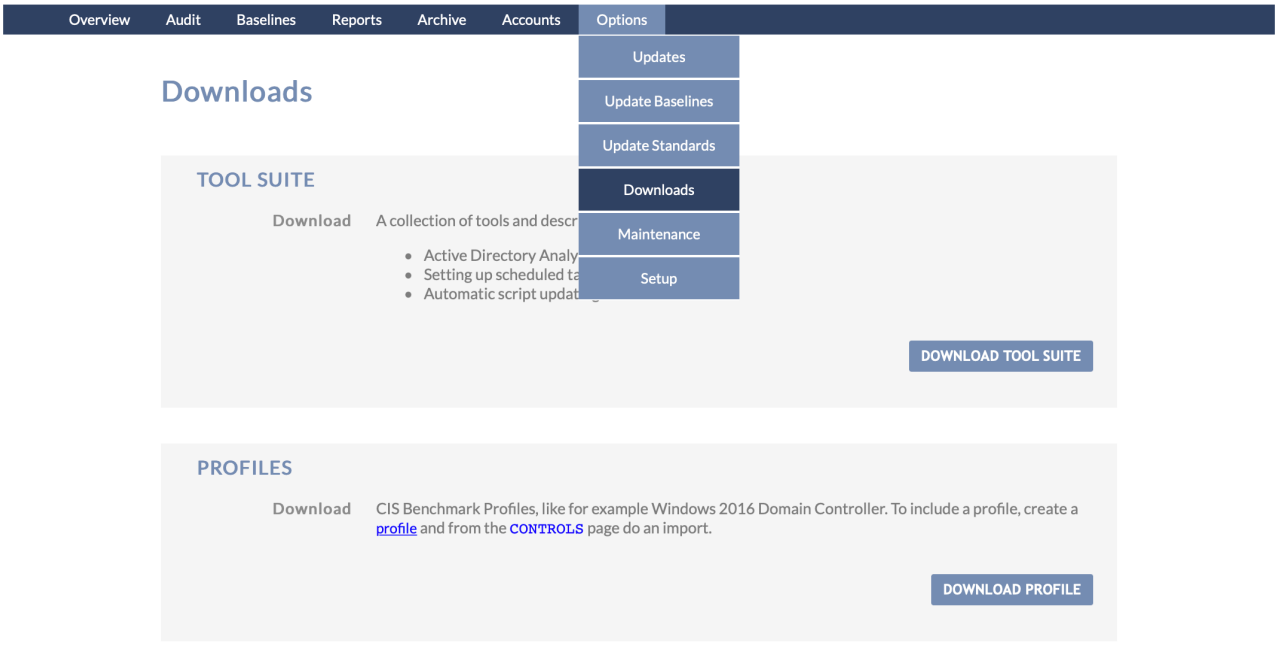
De CIS Benchmarks beschikken over het algemeen over twee niveaus voor iedere OS versie, de zogenoemde Level 1 (L1) en Level 2 (L2) Benchmark. L1 is de basis waarmee u zorgt voor een degelijke security. De L2 benchmarks kunnen extra controls bevatten en SOLL waardes kunnen strenger zijn, hiermee zorgt u voor een extra veilige omgeving.

In de Secquard applicatie kunt u de CIS levels hanteren door gebruik te maken van onze bestaande profielen. Deze staan al voor u klaar en hoeft u dus niet zelf aan te maken!

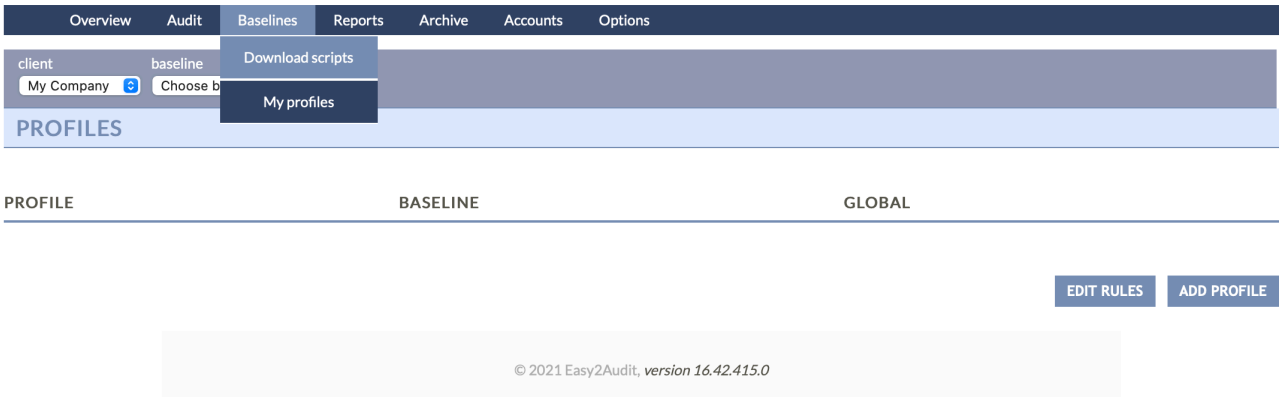
Er bestaan ook verschillende benchmarks voor sommige type server en systeem
- Microsoft Windows: Domain Controller (DC) en Member Server (MS)
- Linux: Server en Workstation

Instructies voor het selecteren van een profiel

Ga naar menu: Options -> Downloads en klik op DOWNLOAD PROFILE om de Secquard profielen te downloaden.

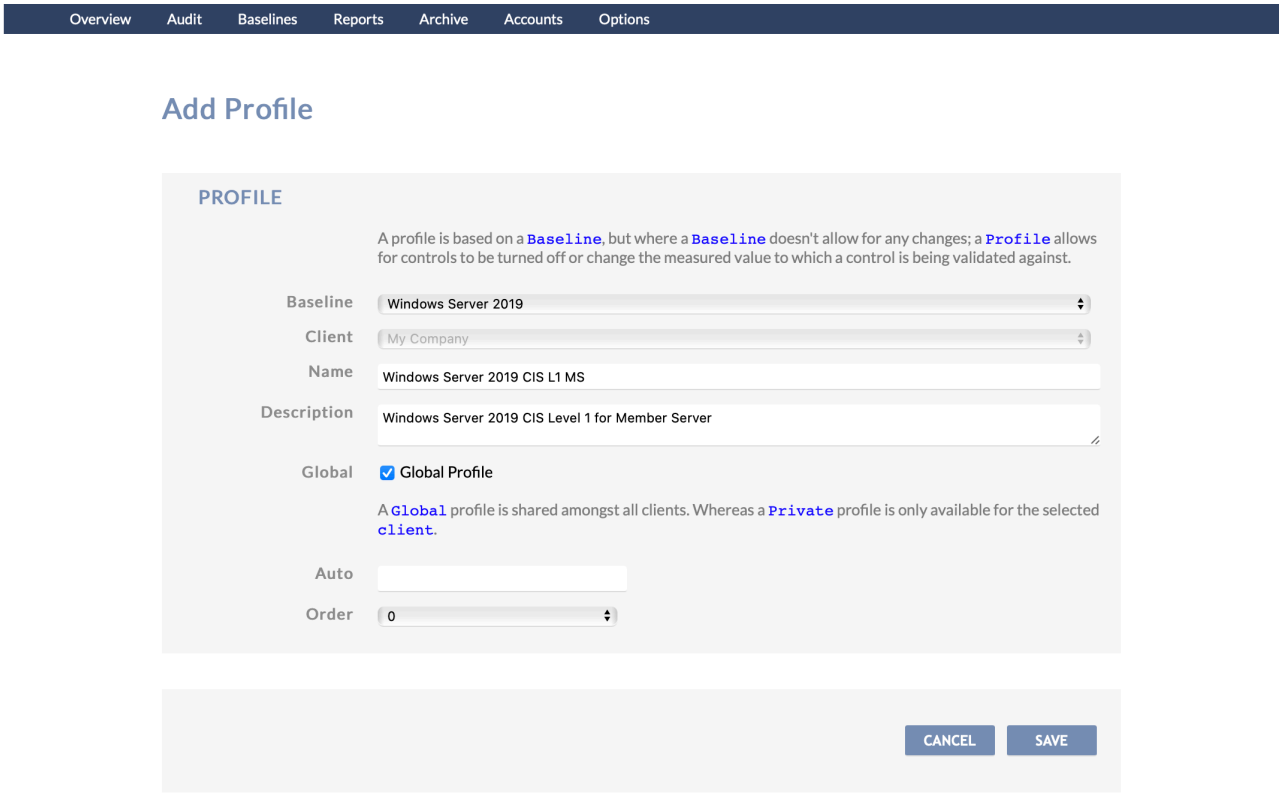


Bedenk vast voor wel OS u een profiel aan wilt maken. Ga vervolgens naar menu: Baselines -> My profiles en klik op ADD PROFILE om een nieuw profiel aan te maken.

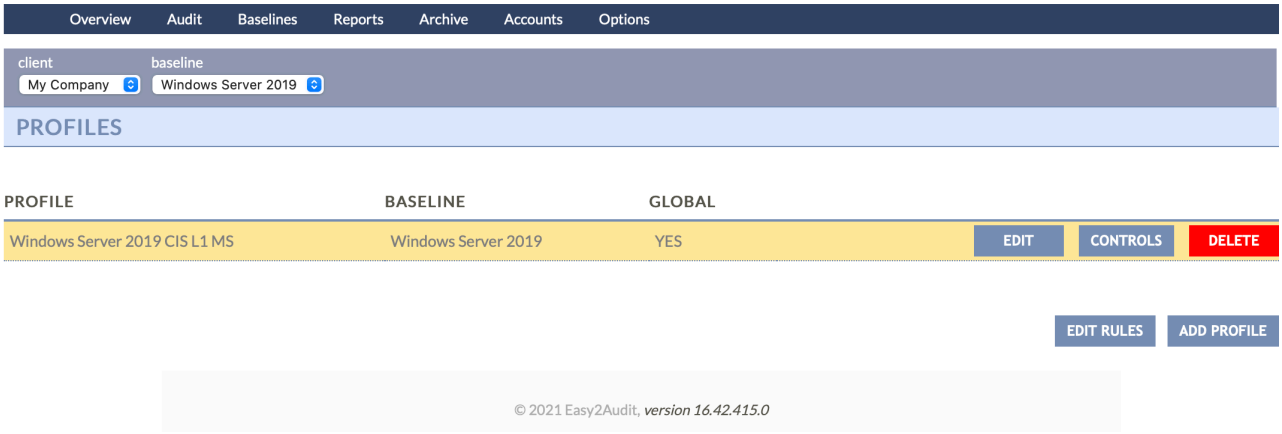


Kies dan de gewenste Baseline uit het dropdown menu. Als u niet de juiste baseline kunt selecteren, kijk dan even terug naar paragraaf 3.2.3 van deze handleiding.

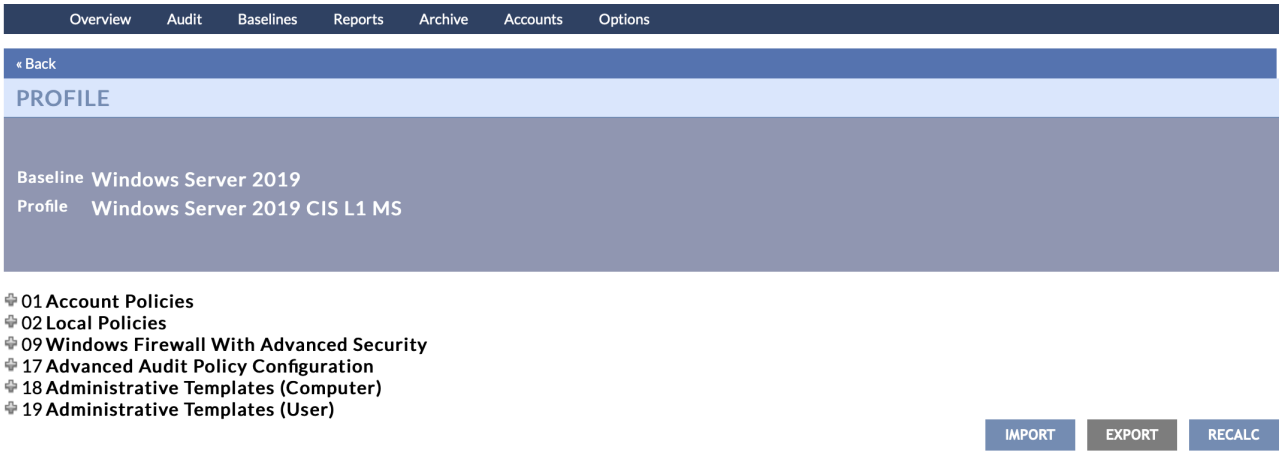
Als u de juiste baseline heeft geselecteerd, kies dan de gewenste client en vul een naam in voor uw profiel. Omdat wij een CIS level 1 profiel voor een Windows Server 2019 Member server willen aanmaken, geven we deze onderstaande naam en beschrijving, zo kunt u deze later eenvoudig herkennen en selecteren. Vink, indien gewenst, global profile aan.



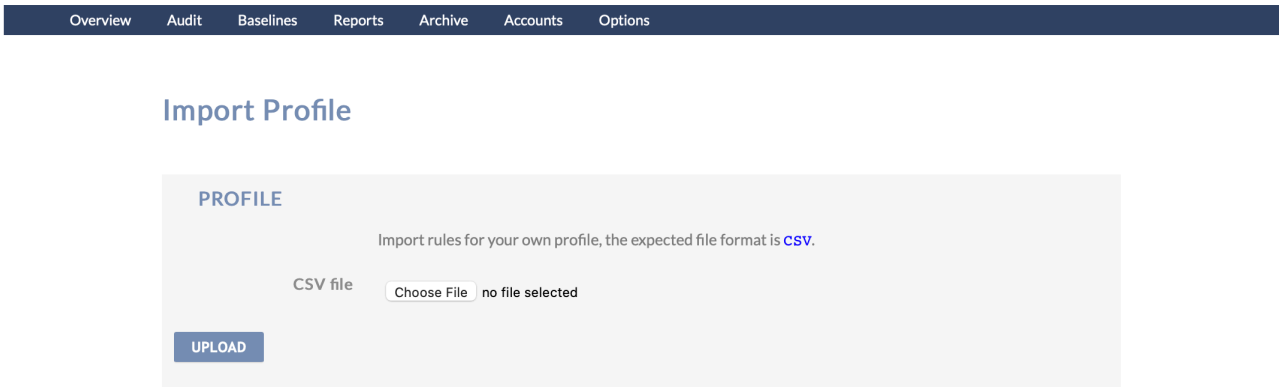
Klik nu op CONTROLS.



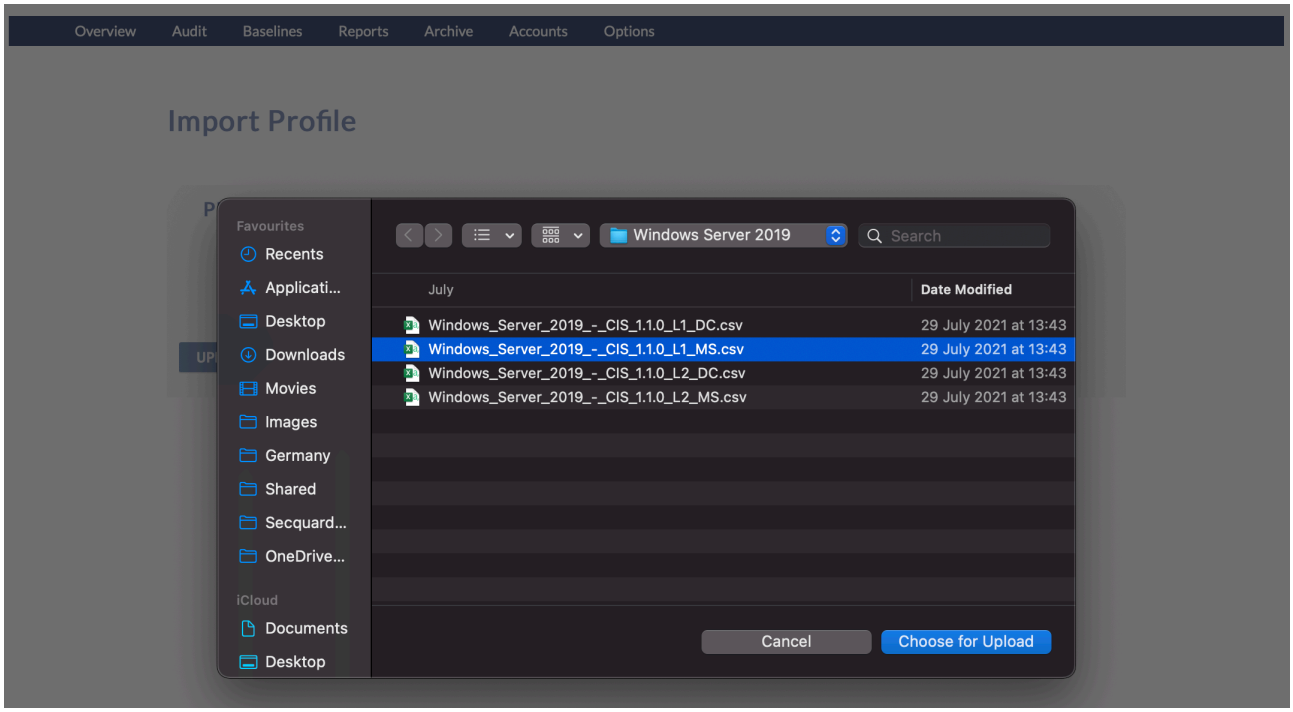
Klik op IMPORT.



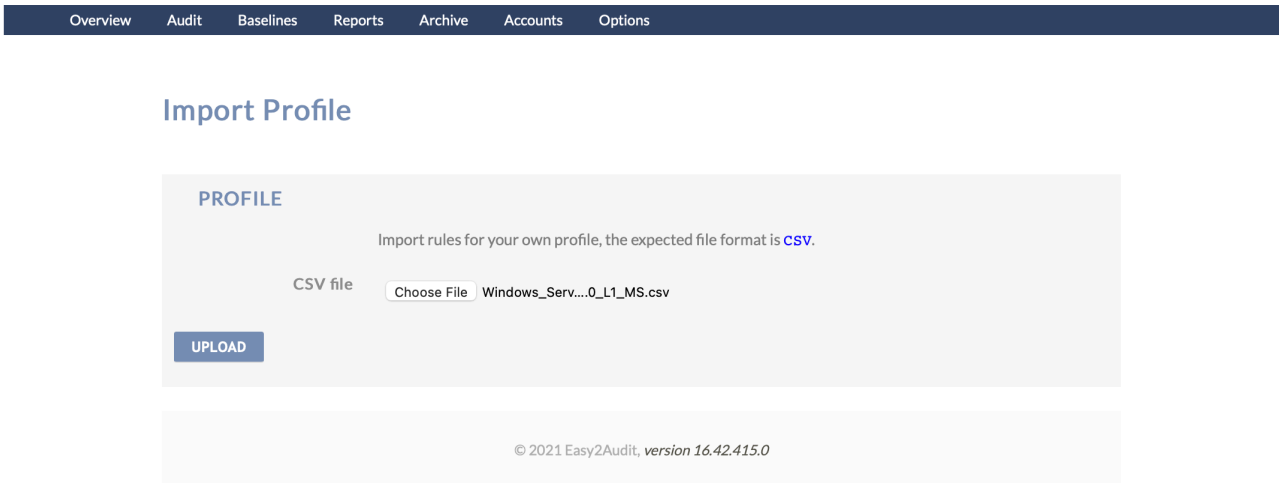
Klik op Choose File.



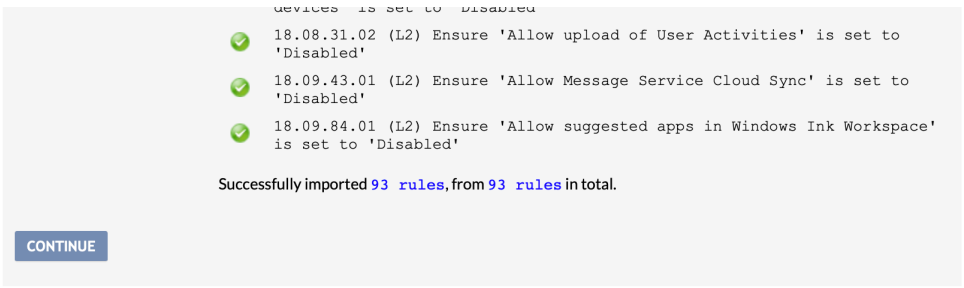
Selecteer het gewenste profiel en kies Choose for Upload.



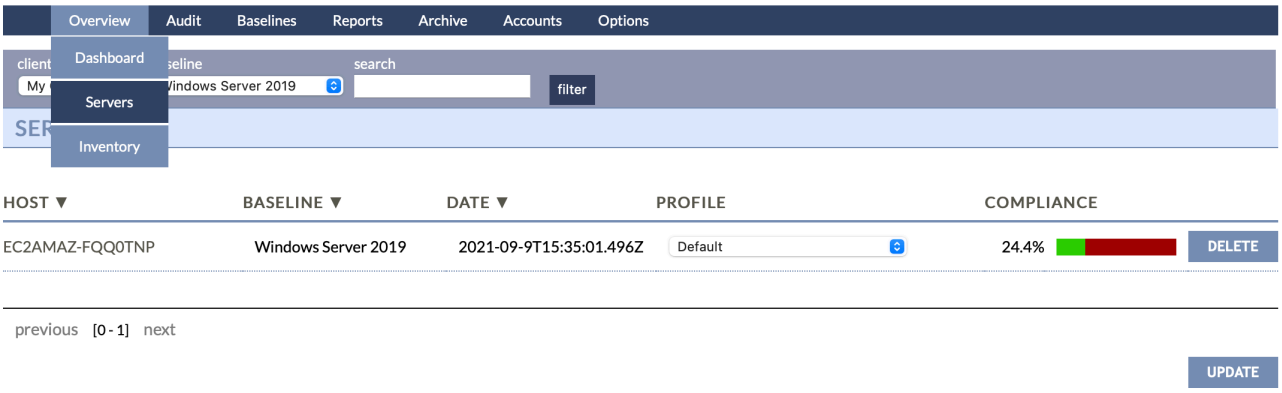
Klik op UPLOAD.



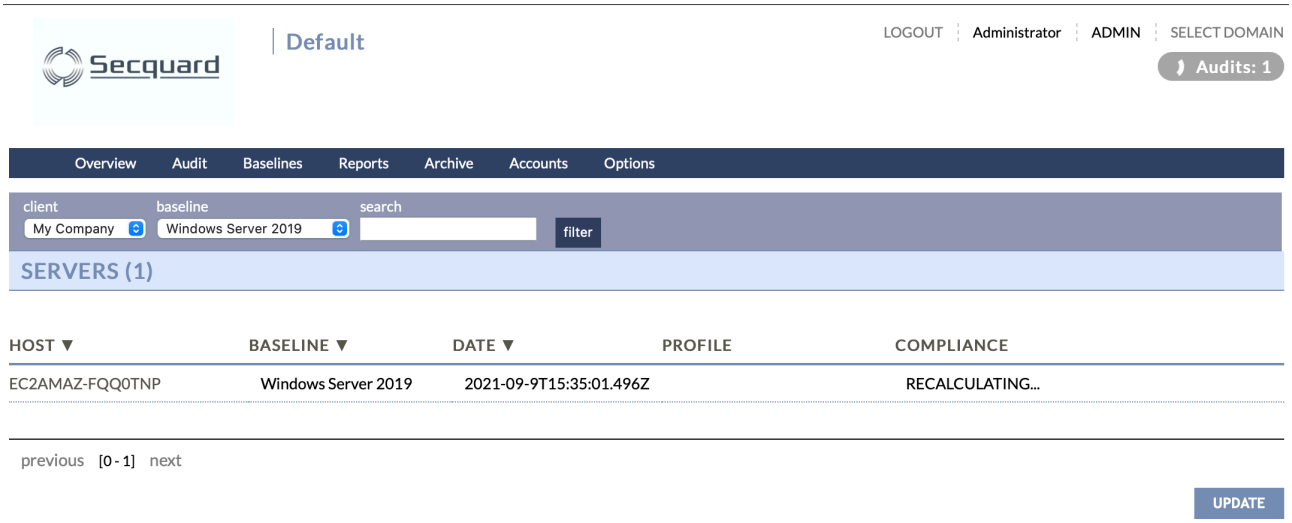
Scroll helemaal naar beneden op de volgende pagina en klik op CONTINUE.



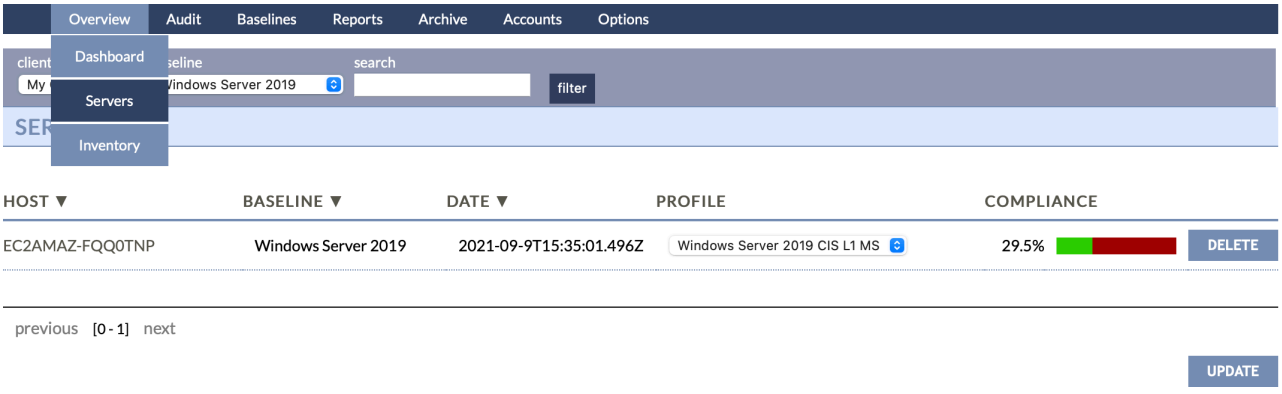
Om uw profiel in actie te zien, gaat u naar menu: Overview -> Servers.



Selecteer bij PROFILE het zojuist aangemaakte profiel en klik op UPDATE. U ziet rechtsboven in beeld een grijs vlakje met Audits: 1. Verschijnen.



Wacht tot dit grijze vlakje verdwijnt en ververs de pagina. Bijvoorbeeld door opnieuw naar het menu: Overview -> Servers te gaan. U zult zien dat uw profiel is geactiveerd. Omdat het L1 MS profiel minder controls bevat, zal uw compliance score (waarschijnlijk) hoger uitvallen dat met het default profiel.



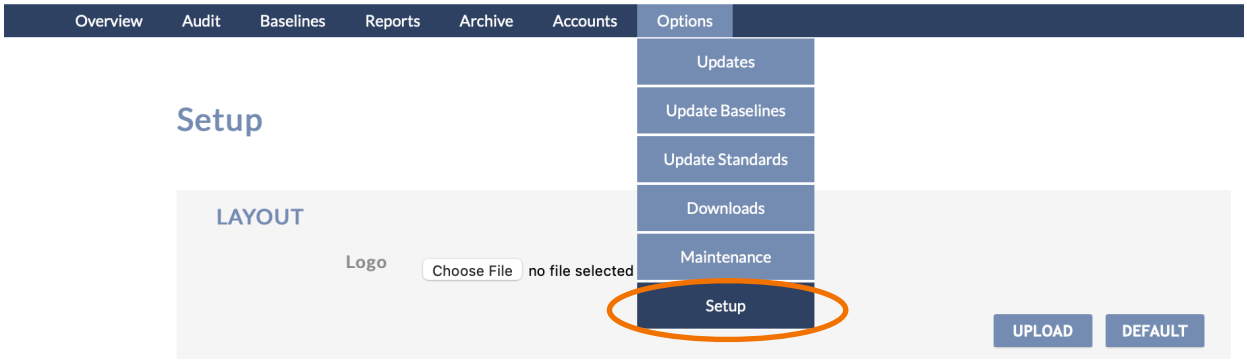
8 Taken automatiseren

Binnen de Secquard applicatie zijn nog een aantal taken die geautomatiseerd kunnen worden uitgevoerd:

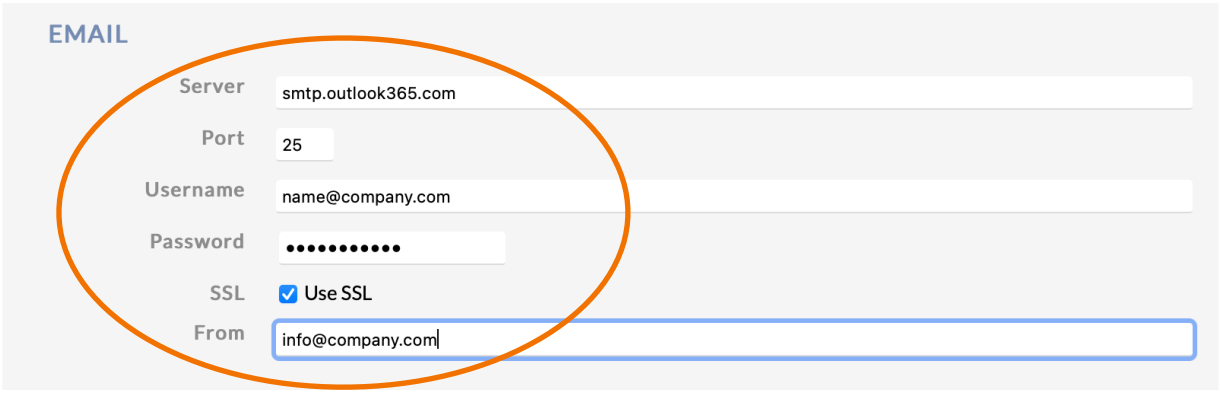
I. Het (maandelijks) afsluiten van een lopende audit periode
II. Het versturen van de management rapportages
III. Het uitvoeren van remote audit sessies

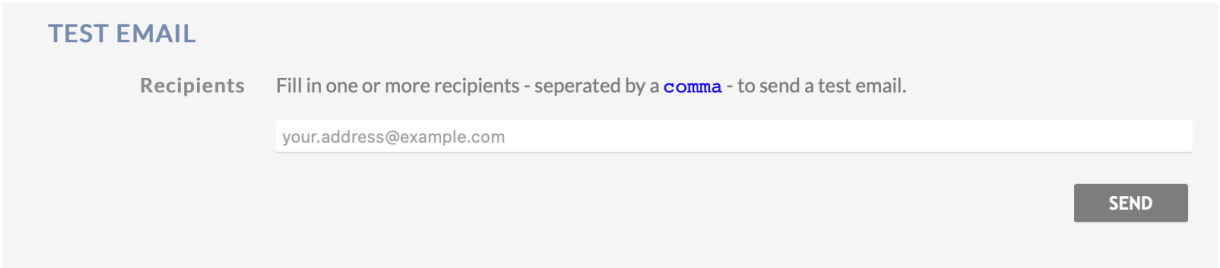
8.1 Voorbereiding

Zorg ervoor dat u de email server heeft ingesteld. U vindt deze instellingen via het Secquard menu: Options -> Setup



Voer hier uw smtp server gegevens in. Indien gewenst (en beschikbaar) kunt u bijvoorbeeld gebruik maken van de outlook 365 smtp server.

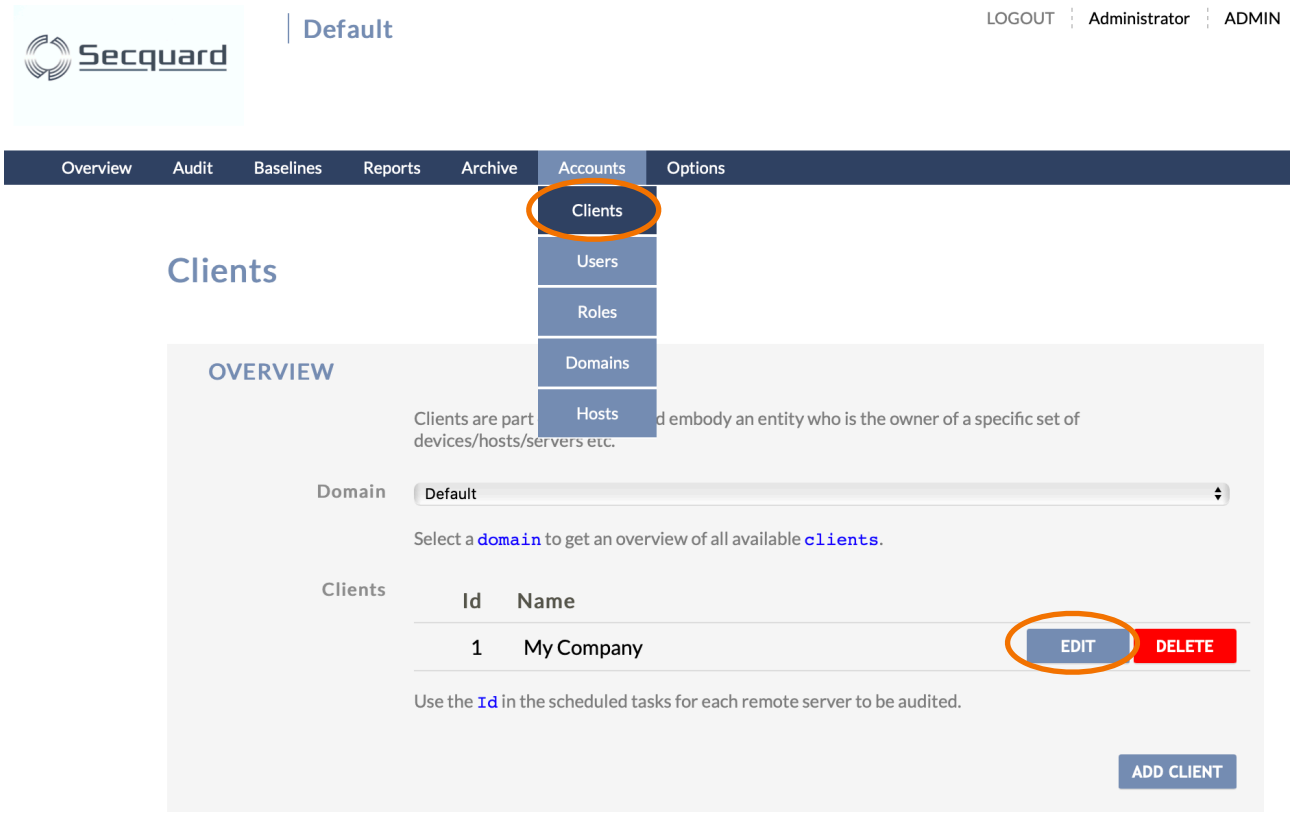




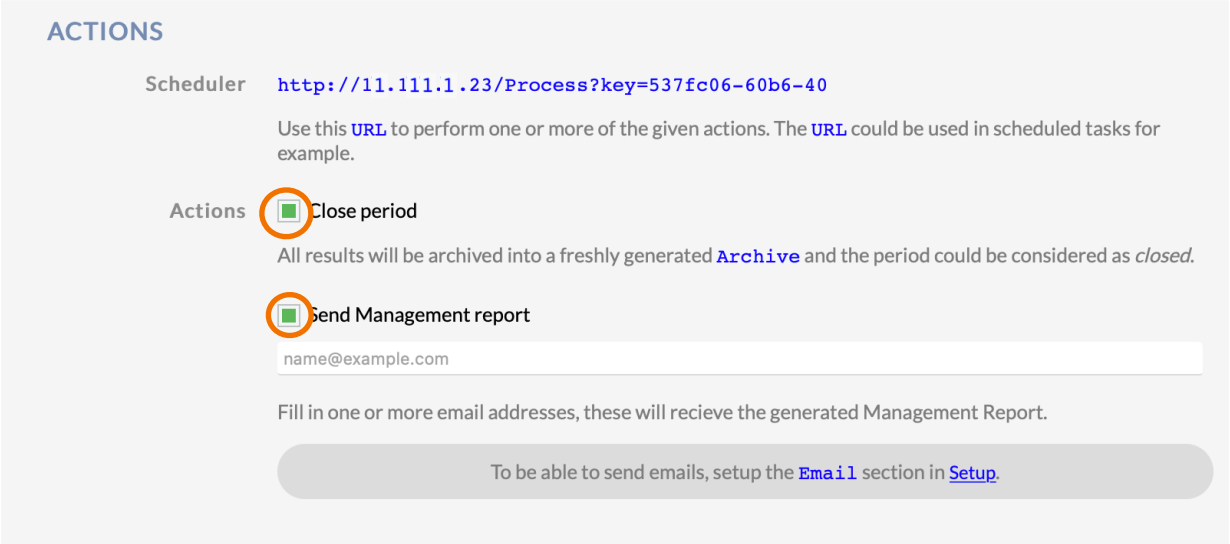
8.2 Automatisch afsluiten audit periode en versturen management rapportages

8.2.1 Instellingen in de applicatie

Om uw audit periodes automatisch af te sluiten en uw management rapportages automatisch te versturen, heeft u een URL nodig. Deze URL vindt u in de Secquard applicatie onder Accounts > Clients, selecteer “EDIT” voor de client waarvoor u een taak wilt automatiseren. Als u dit voor meerdere clients wilt, dient u dit de stappen te herhalen voor de betreffende client.



Geef in onderstaand scherm aan welke taken u wilt automatiseren. Als u de management rapportage aan meerdere e-mail adressen wilt versturen, kunt u deze toevoegen en scheiden met een “;”.

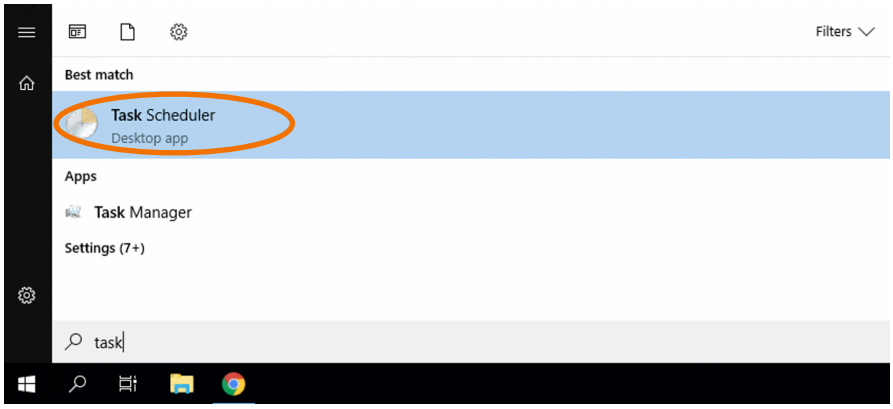


8.2.1 Instellingen in de server

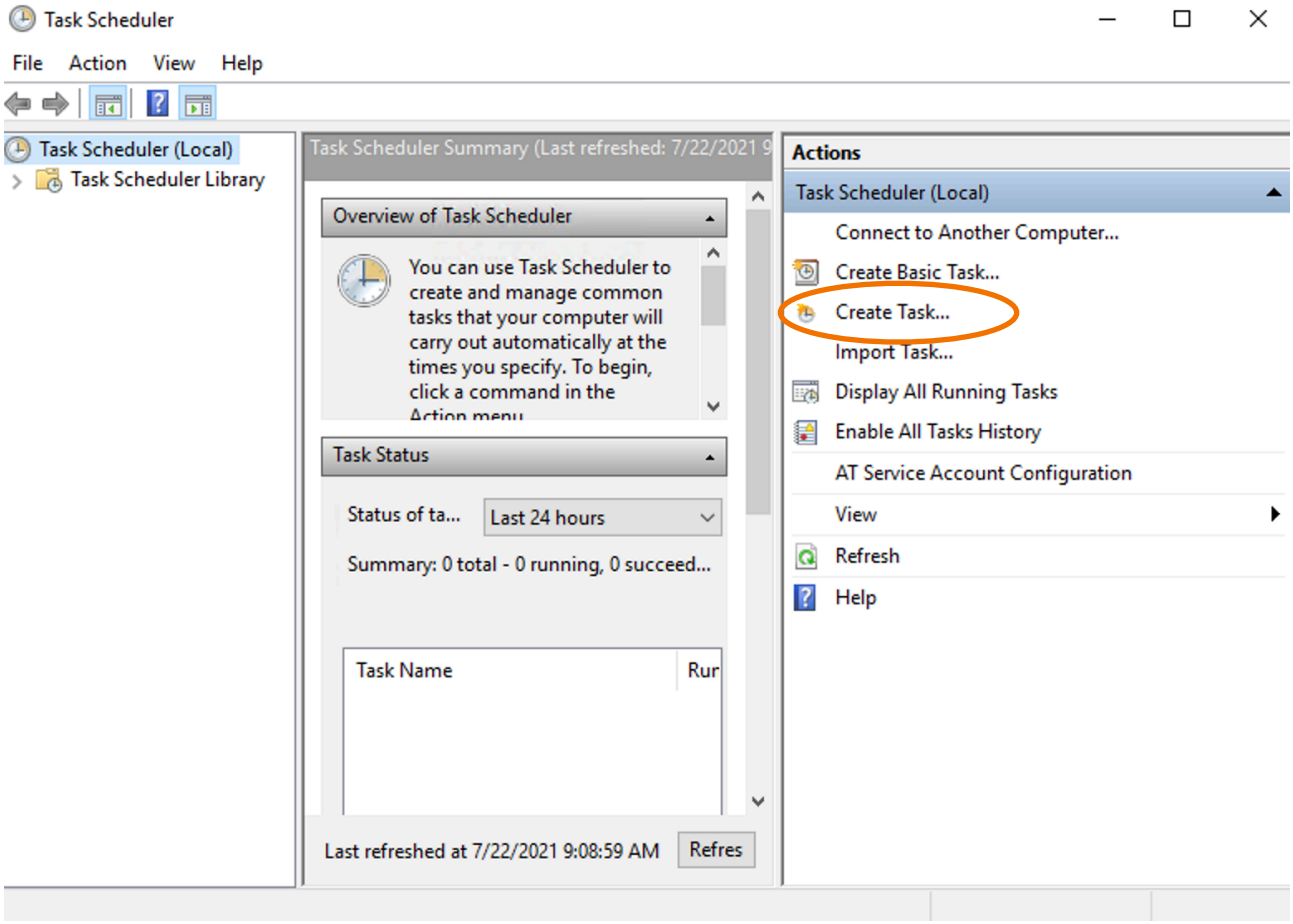
Het automatisch uitvoeren van deze taken gebeurt gebruikelijk maandelijks op de laatste dag van de maand, wekelijks op zondag of op de laatste dag van het kwartaal.

Dit kunnen we realiseren door een taak in te plannen via de Windows Task Scheduler (NL: Taakplanner).

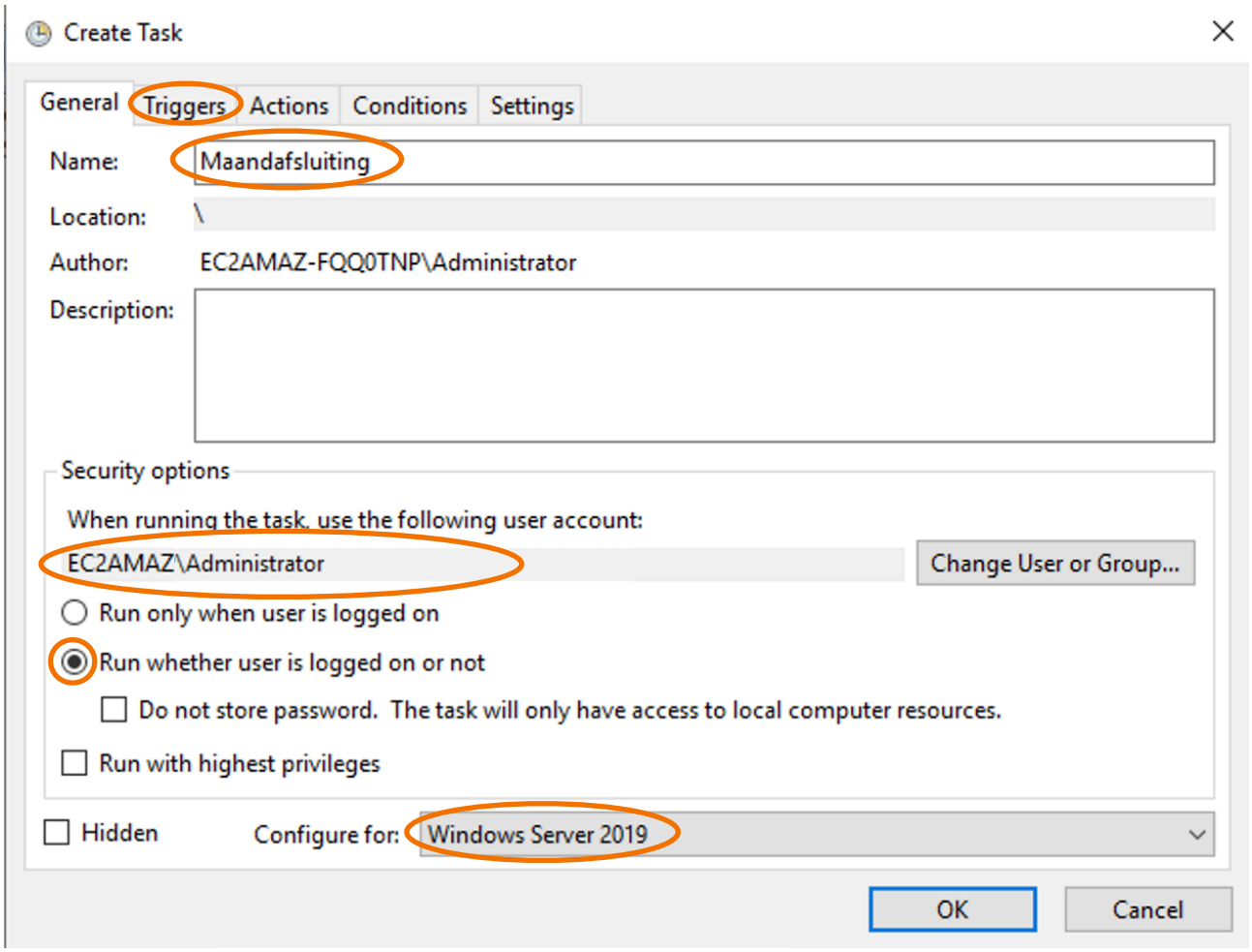
1. Start de Windows Task Scheduler. Dit doe je door naar het Windows-menu te gaan en hier “task” in te typen. Klik op Task Scheduler.



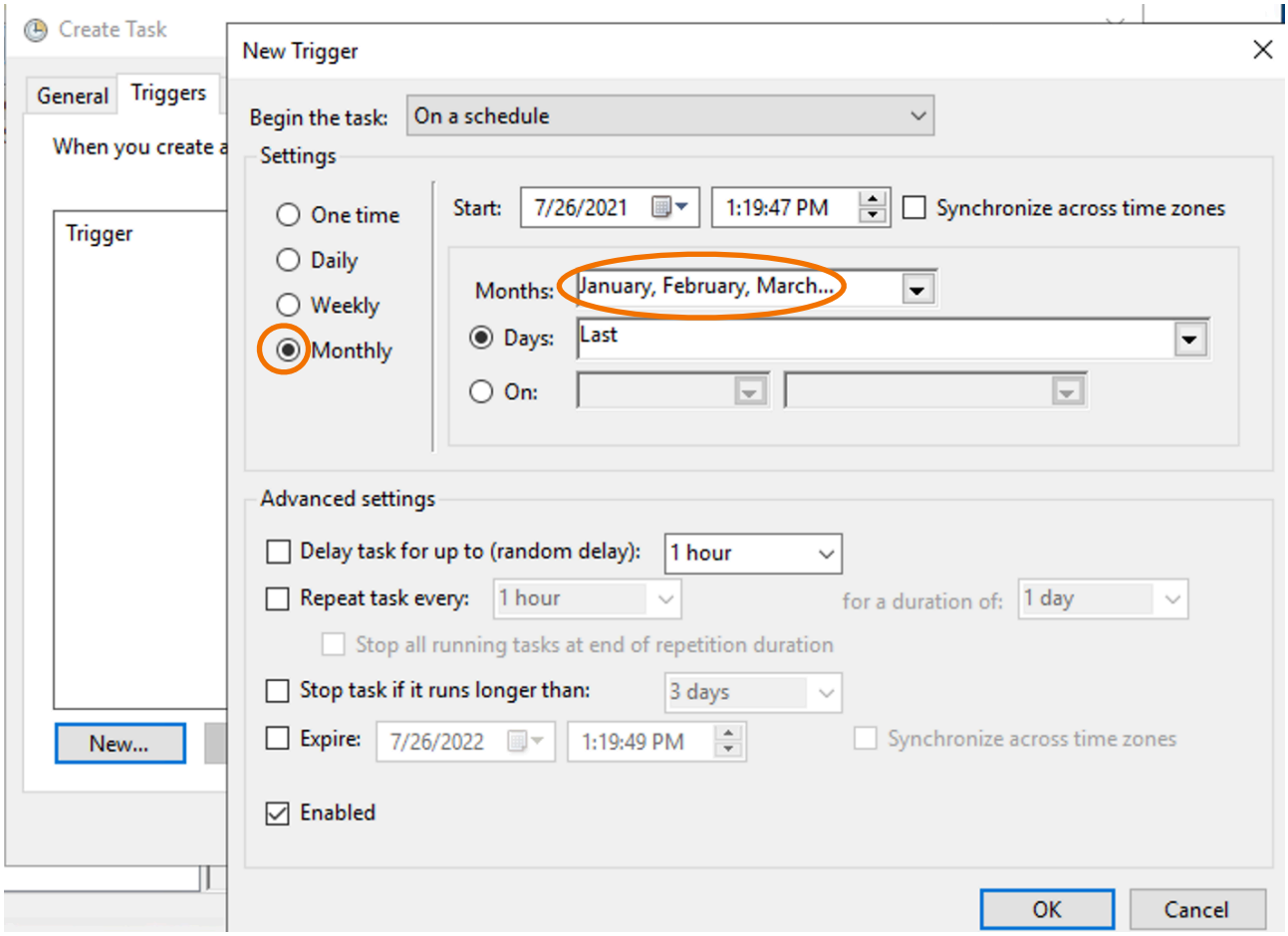
2. Klik op “Create Task”.



3. Vul een omschrijving in, bijvoorbeeld “Maandafsluiting”. Selecteer een local user en “Run whether user is logged on or not”. Selecteer het besturingssysteem waar uw server op draait (in dit geval is dat Windows Server 2019). Klik daarna op “Triggers”.



4. Creëer een trigger voor uw gewenste situatie. Bijvoorbeeld maandelijks op de laatste dag.

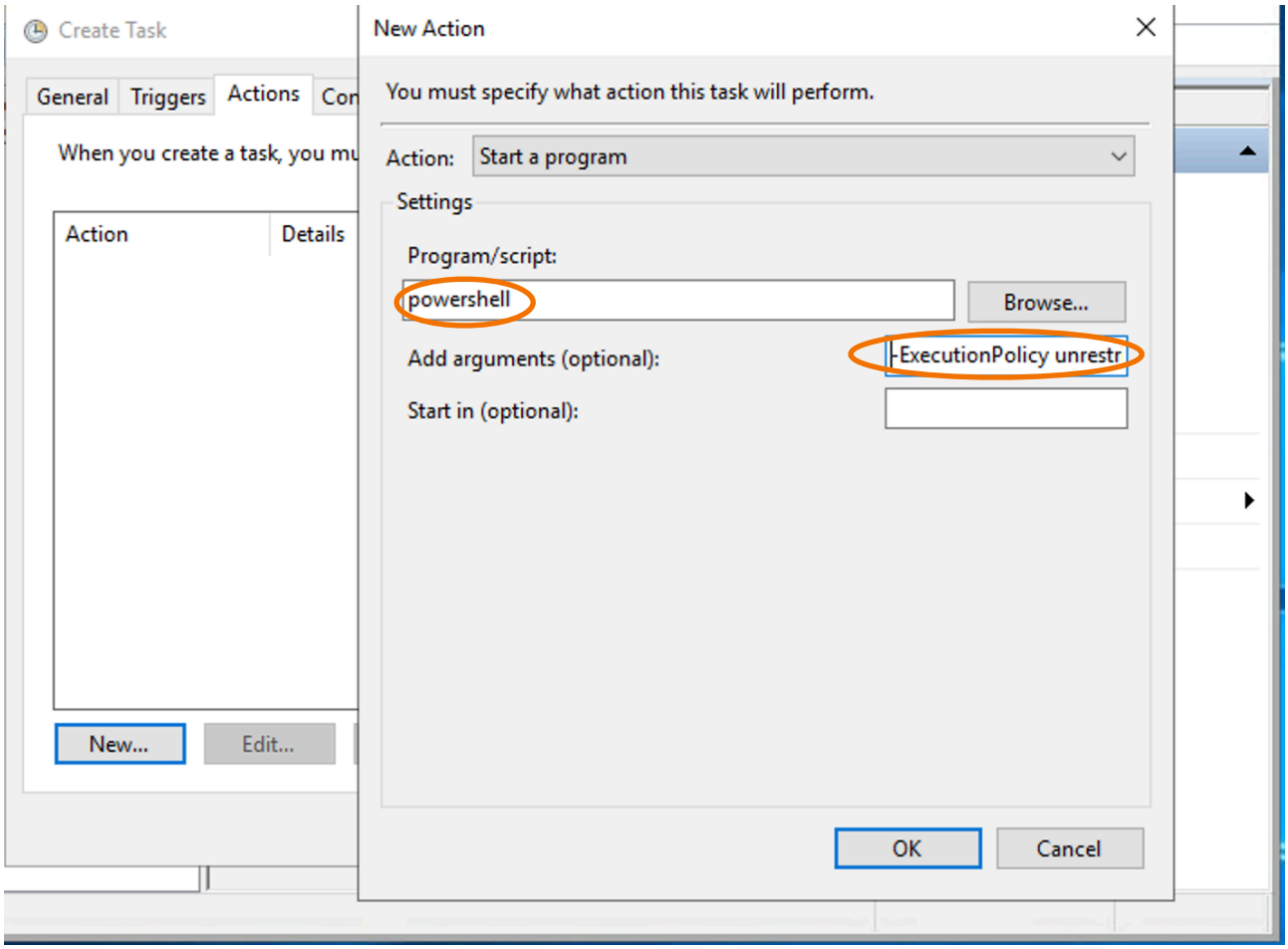


5. Type “powershell” in het Program/script tekstvak. Kopieer de volgende regel en vervang URL voor het adres dat u bij Accounts -> Clients -> ‘EDIT’ -> Actions heeft gezien.

```
-ExecutionPolicy unrestricted -Command "(New-Object Net.WebClient).DownloadString(\"http://URL\")"
```

In ons geval komt de regel er als volgt uit te zien:

```
-ExecutionPolicy unrestricted -Command "(New-Object Net.WebClient).DownloadString(\"http://
11.111.1.23/Process?key=537fc06-60b6-40\")"
```



Note: Als u onderstaande foutmelding krijgt, kan het zijn dat u uw email server niet correct heeft ingesteld. Refereer hiervoor naar het kopje voorbereiding op pagina 2 van deze handleiding.

```
Scheduled Events:Error: The parameter 'from' cannot be an empty string.
Parameter name: from
```

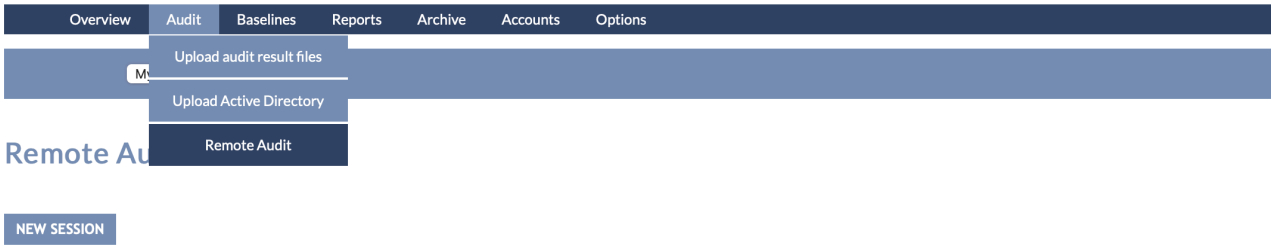
8.3 Het automatisch uitvoeren van remote audit sessies

8.3.1 Instellingen in de applicatie

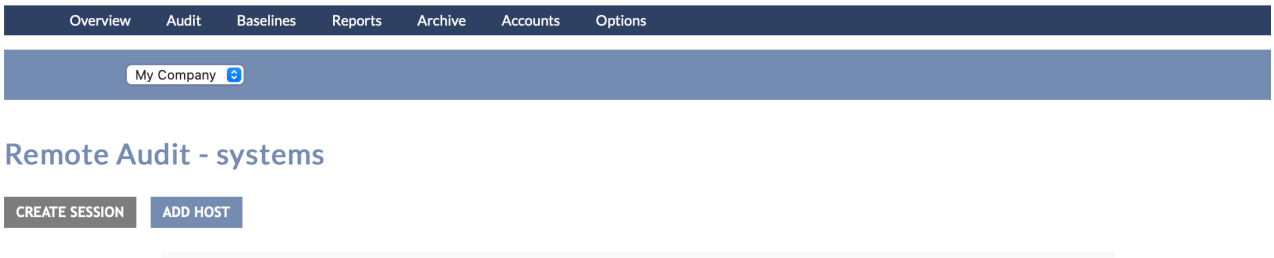
Het inroosteren van remote audits kan worden gebruikt om periodiek (meestal dagelijks) network devices uit te lezen. Op deze devices kan de audit niet via een geïnstalleerd script worden gestart, maar gebeurt dit vanuit de centrale Secquard server, of een Secquard relay server. U heeft hiervoor inlog gegevens nodig van de devices die u wilt auditen.

De benodigde URL wordt gevonden via menu: Audit -> Remote Audit.

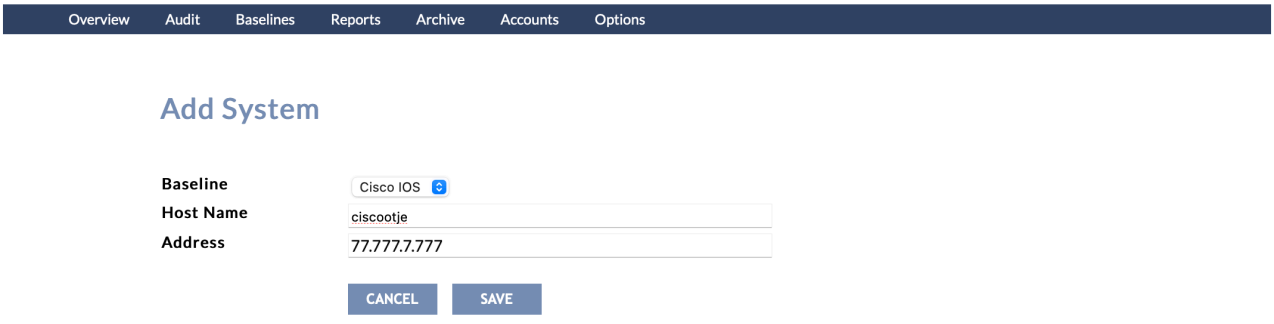
Als er nog geen remote audit is uitgevoerd en opgeslagen, kies dan voor NEW SESSION.



Kies vervolgens voor ADD HOST.

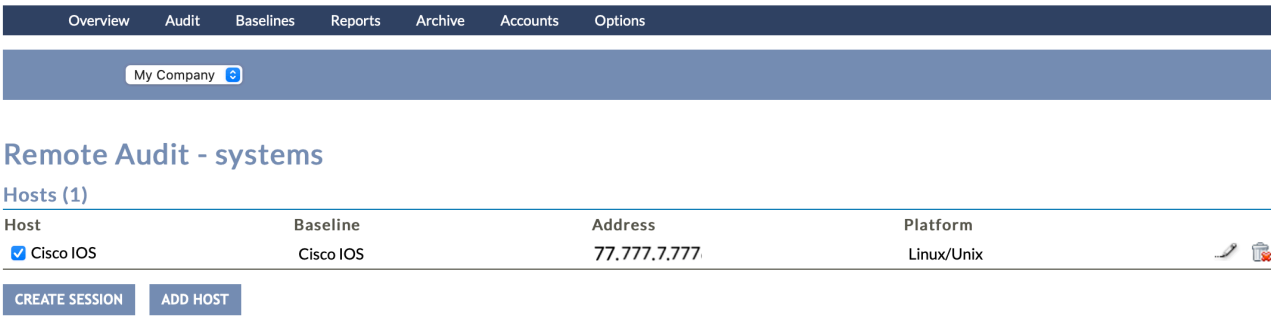


Selecteer vervolgens de correcte baseline. Als deze niet wordt weergegeven, installeer deze dan via het menu: Options -> Update Baseline, en kies voor install bij de juiste baseline. Als u nu terugkeert naar onderstaand scherm (Audit -> remote audit -> new session -> add host), kunt u de baseline wel selecteren. Voer een host name in (kies deze zelf) en het juiste ip-adres van het network device. Klik vervolgens op SAVE.

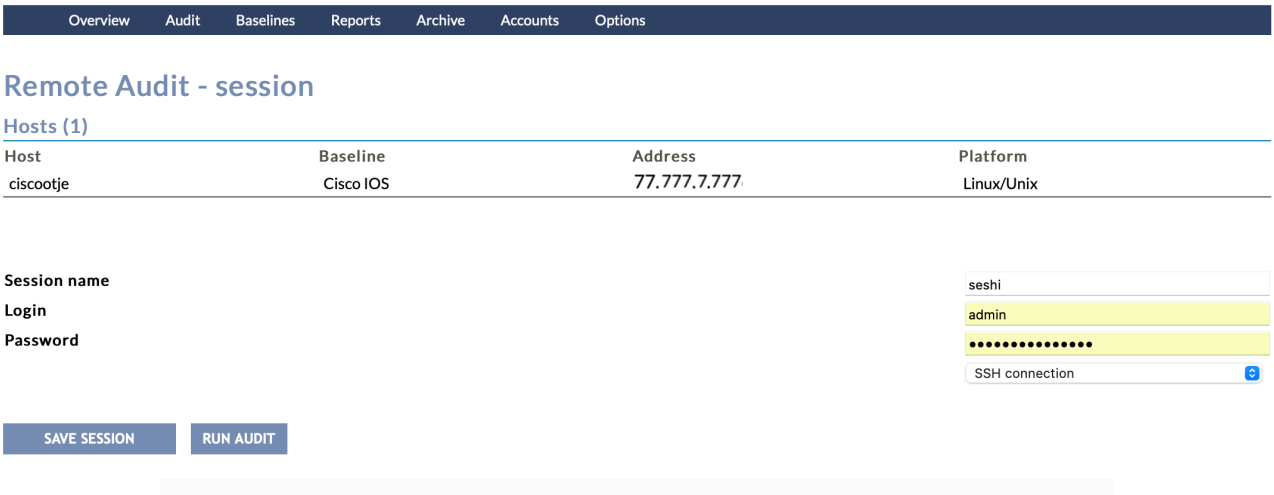


Daarna kunt u terug naar het menu: Audit -> Remote audit -> NEW SESSION.

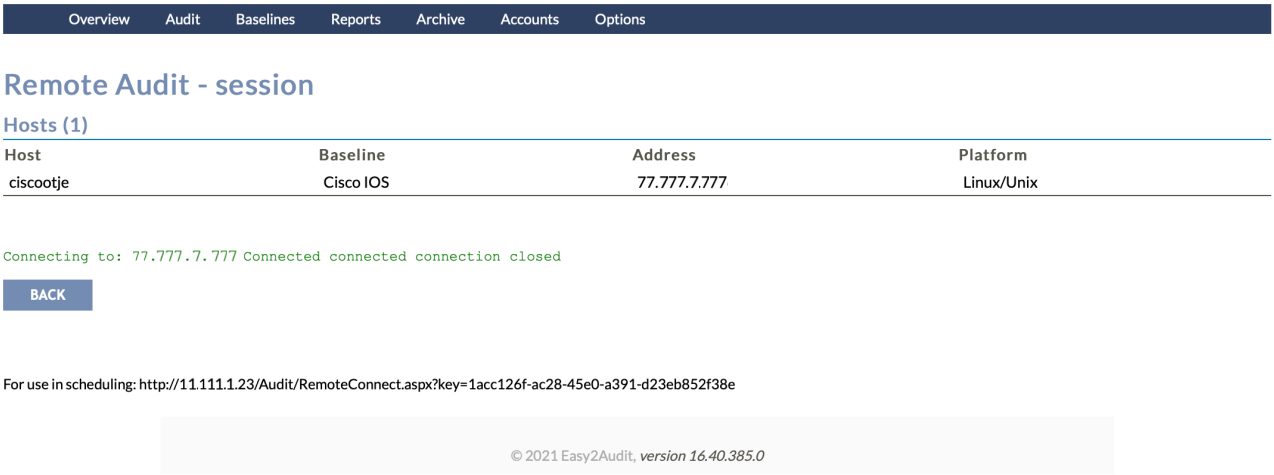
Vink nu het device aan en klik op CREATE SESSION.



Voer een sessie naam in (verzin deze zelf) en de username en password van het netwerk device. Klik op RUN AUDIT.



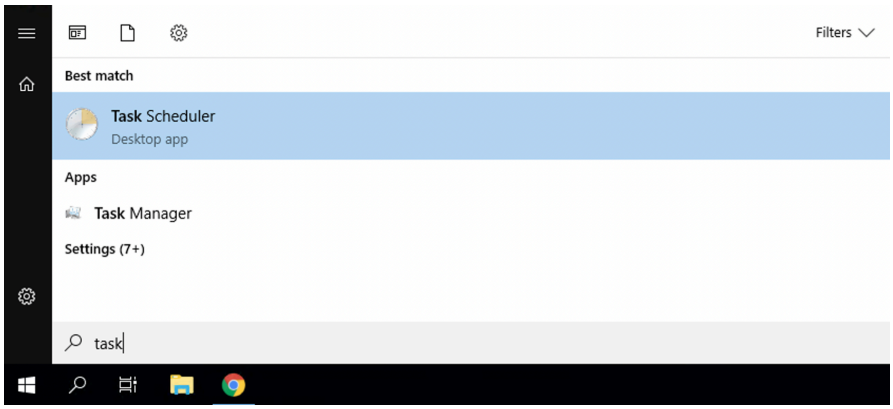
Wacht even tot de audit klaar is. Als deze goed is verlopen zult u onderstaande melding zien. Daaronder verschijnt direct een URL voor het automatisch inplannen.



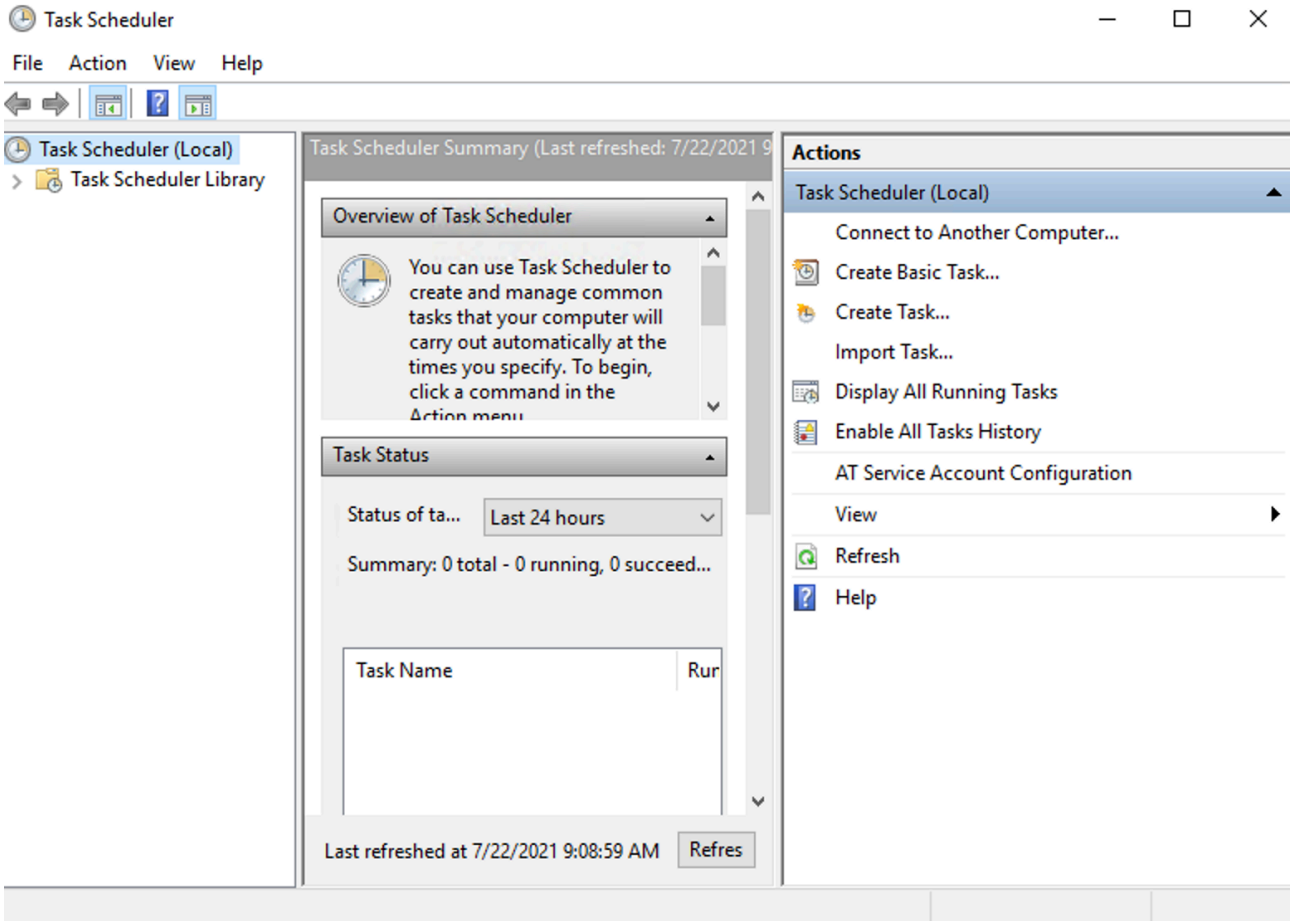
8.3.2 Instellingen in de applicatie server

Dit plannen kunnen we realiseren door een taak in te plannen via de Windows Task Scheduler (NL: Taakplanner).

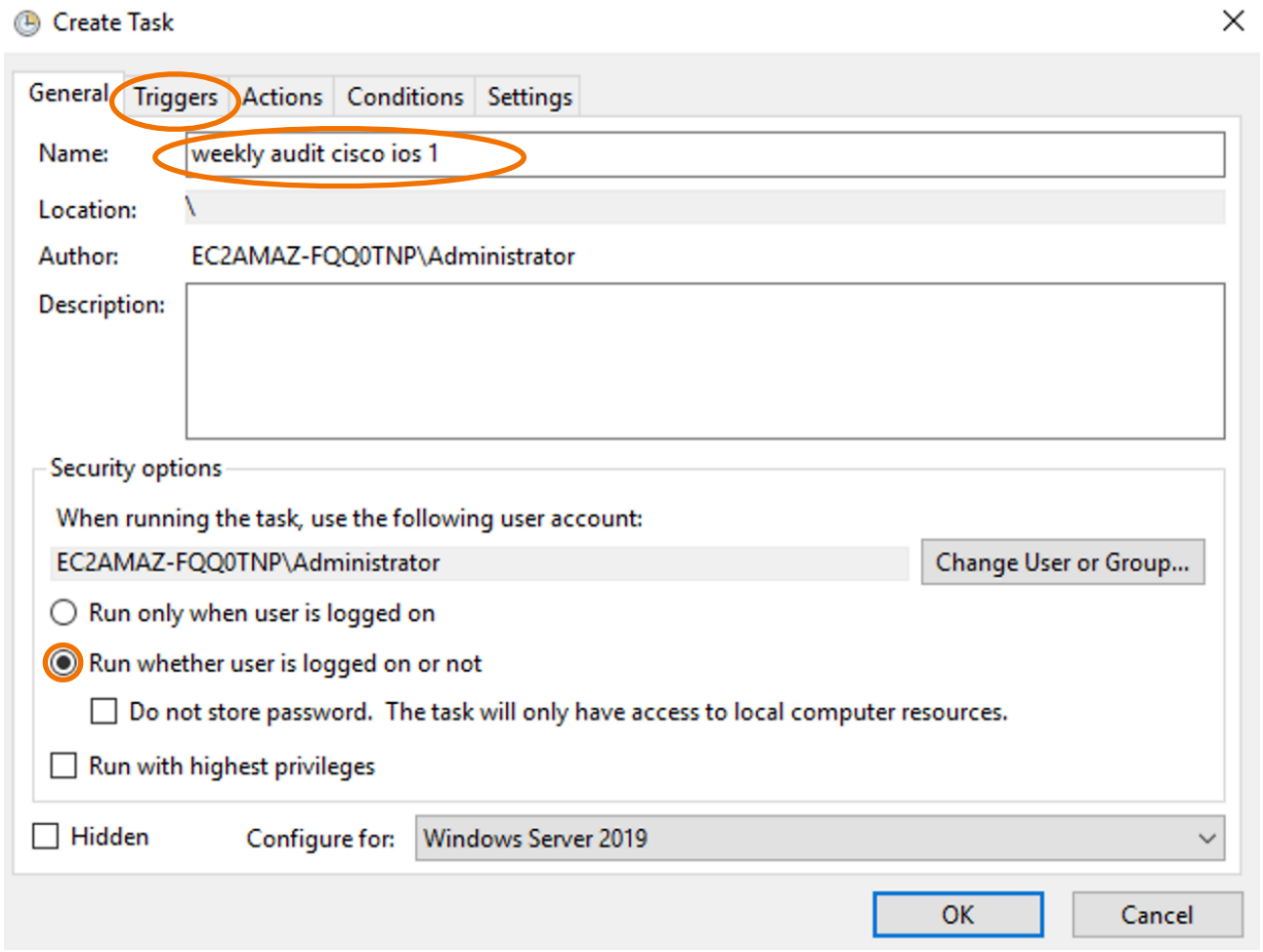
1. Start de Windows Task Scheduler. Dit doe je door naar het Windows-menu te gaan en hier “task” in te typen. Klik op Task Scheduler.



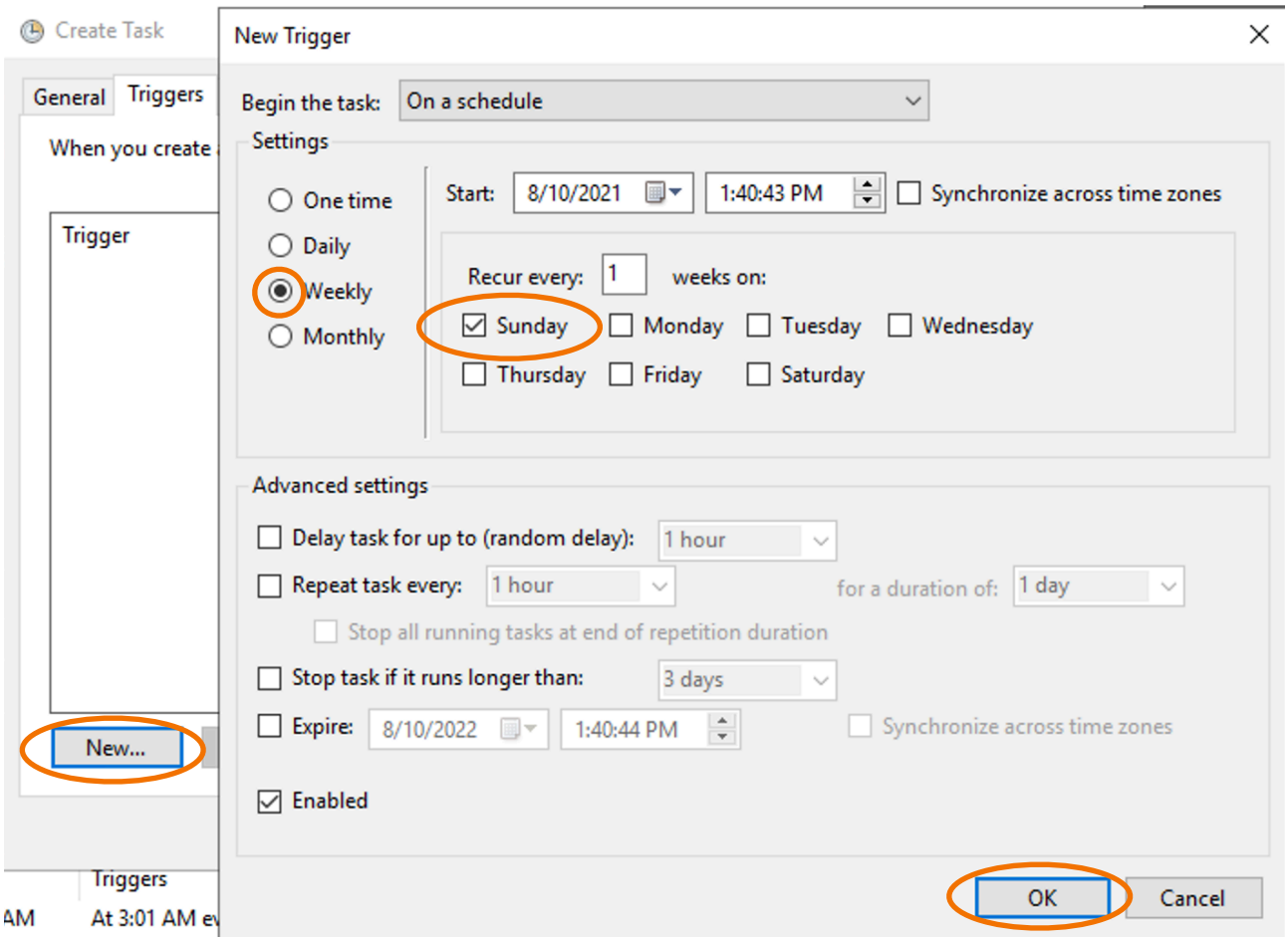
2. Klik op “Create Task”.



3. Vul een omschrijving in, bijvoorbeeld “weekly audit cisco ios 1”. Selecteer een local user en “Run whether user is logged on or not”. Selecteer het besturingssysteem waar uw server op draait (in dit voorbeeld is dat Windows Server 2019). Klik daarna op “Triggers”.

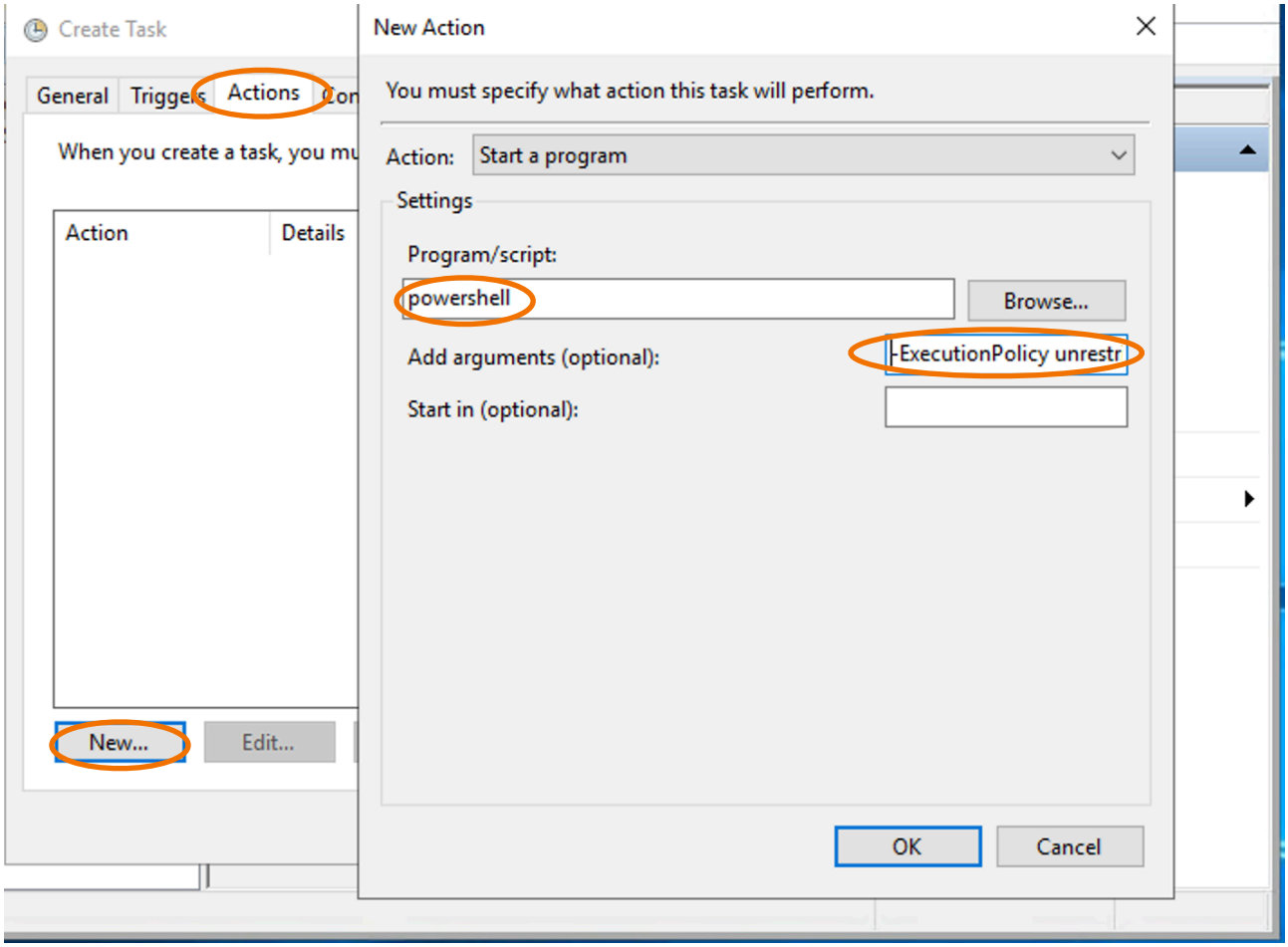


4. Klik op New.. en creëer een trigger voor uw gewenste situatie. Bijvoorbeeld wekelijks op zondag. Klik op OK.



5. Klik op Actions en op New… Type “powershell” in het Program/script tekstvak. Kopieer de volgende regel en vervang het oranje URL voor het adres dat u bij Remote Audit - Session heeft gezien. De rest dient exact hetzelfde te blijven.

```
  -ExecutionPolicy unrestricted -Command "(New-Object Net.WebClient).DownloadString(\"http://
11.111.1.23/Audit/RemoteConnect.aspc?key=1acc126f-ac-45e0-a391-d23eb852f38e\")"
```



Druk daarna op OK en op OK. Voer uw wachtwoord in als hierom wordt gevraagd. U heeft nu de automatische remote audit correct ingesteld!

Note: Als u onderstaande foutmelding krijgt, kan het zijn dat u uw email server niet correct heeft ingesteld. Refereer hiervoor naar het kopje voorbereiding op pagina 2 van deze handleiding.

```
Scheduled Events:Error: The parameter 'from' cannot be an empty string.
Parameter name: from
```

9 Intake-Formulier Invullen

Wanneer u dit document volledig heeft doorgenomen, kunt u ons intake-formulier invullen. Wanneer u het formulier volledig heeft ingevuld, kunt u een afspraak maken voor de kick-off meeting én voor de installatie.

Wij zien u daar graag!