Secquard Applicatie Referentie Handleiding

Uitleg

In deze handleiding worden alle pagina's van de applicatie besproken en wordt er uitgelegd wat iedere functie betekent. U kunt dit document gebruiken als naslagwerk, of er doorheen lezen om de applicatie te leren kennen. Om de applicatie te leren kennen hebben wij ook een andere gebruikershandleiding, die u snel op weg helpt in de applicatie.

Inlogscherm

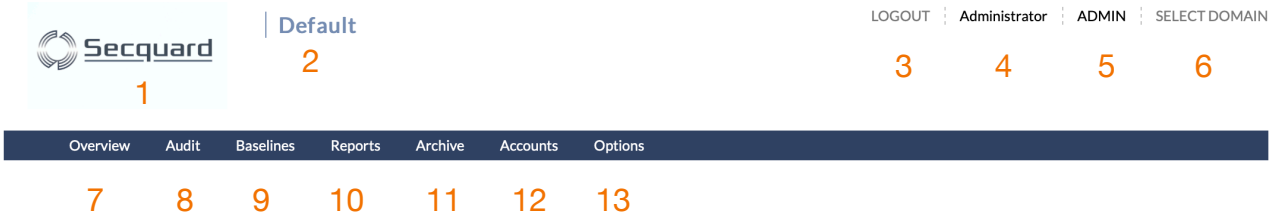
Wanneer u de naam van de host of het ip-adres waar de Secquard applicatie draait intypt in uw browser, komt u bij het inlog-scherm. Hier vult u uw gebruikersnaam en wachtwoord in, en klikt u op login om in te loggen op de applicatie. Er is een user aangemaakt bij de installatie van de applicatie, u kunt deze hiervoor gebruiken. Later in de applicatie kunt u hiervoor het wachtwoord wijzigen. Daarnaast kunt u verschillende andere gebruikers aanmaken, met daarbij behorende rollen en rechten.

Als u wilt, kunt verschillende onderdelen van de inlog-pagina aanpassen, daarover kunt u via het menu naar Options -> Setup, dit staat later ook vermeld in deze handleiding.

Menu

Voor we de losse pagina's bekijken, zullen we kort het menu behandelen, dit menu vind je op iedere pagina van de Secquard applicatie en zorgt ervoor dat je eenvoudig navigeert.

1. Het (Secquard) logo, u kunt dit logo naar wens aanpassen (via Options -> Setup). Wanneer u op dit logo klikt, zult u terugkeren naar het dashboard.
2. Default. Dit is het domein dat u heef geselecteerd.
3. Logout. Een link om uit te loggen van de applicatie.
4. Administrator. De gebruikersnaam waarmee u bent ingelogd.
5. ADMIN. De groep van gebruikers waarmee u bent ingelogd.
6. SELECT DOMAIN. Een link om een ander domein te selecteren.



7. Overview. Toont een lijst met pagina's die te maken hebben met overzichten.
8. Audit. Toont een lijst met pagina's die betrekken hebben tot audits.
9. Baselines. Hier kunt u scripts downloaden en profielen bekijken of aanpassen.
10. Reports. Toont opties voor het uitdraaien van rapporten en geeft een overzicht van uitgevoerde audits.
11. Archive. Toont een lijst met pagina's die te maken hebben met de archieven van uw audits. Deze archieven maken het mogelijk om audits met elkaar te vergelijken.
12. Accounts. Toont een lijst met pagina's die alles te maken hebben met gebruikers accounts, clients, hosts en domeinen.
13. Options. Toont een lijst met pagina's over verschillende instellingen.

Menu: Overview -> Dashboard

Het dashboard is de hoofdpagina van de Secquard applicatie. Hier vindt u een overzicht van de hoofdstukken: Standards, hardening, security patches, vulnerabilities, antivirus en administrators.

Bovenaan de pagina staan 3 dropdown menu's.

- Client. (Filter). Hier kan een client geselecteerd worden hieronder valt een groep systemen, vervolgens zullen alleen systemen die onder deze client vallen getoond worden.
- Baseline. (Filter). Hier kan een baseline geselecteerd worden. Alleen systemen die met deze baseline worden gecontroleerd worden nu getoond.
- Archive. Hier kan een archief geselecteerd worden. Deze selectie bepaalt welke (eerdere) audit er bij Previous audit getoond wordt.

Standards

Hosts 1	Current		Previous audit		Realization	
	Hosts	Level	Hosts	Level	Hosts	Variance
BIO 1.04	1	26.3%		NOT APPLICABLE		0%
CIS Critical Security Controls	1	32.1%		NOT APPLICABLE		0%
COBIT 5	1	26.3%		NOT APPLICABLE		0%

Hardening

Hosts 1 Baselines 1	Current		Previous audit		Realization	
	Hosts	Level	Hosts	Level	Hosts	Variance
Windows Server 2019	1	24.4%	1	24.4%	0	0%

Security Patches

Hosts 1 Baselines 1	Current			Previous audit			Realization		
	Hosts	Compliant	NOT Compliant	Hosts	Compliant	NOT Compliant	Hosts	Compliant	NOT Compliant
Windows Server 2019	1	1		1	1		0	0	0

Vulnerabilities

Hosts 1 Baselines 1	Current				Previous audit				Realization			
	Total hosts	CVE's C	H	M	Affected hosts	Total hosts	CVE's C	H	M	Affected hosts	Total hosts	CVE's C	H	M	Affected hosts
Windows Server 2019	1	3	21		1	1	3	21		1	0				0

Anti-virus

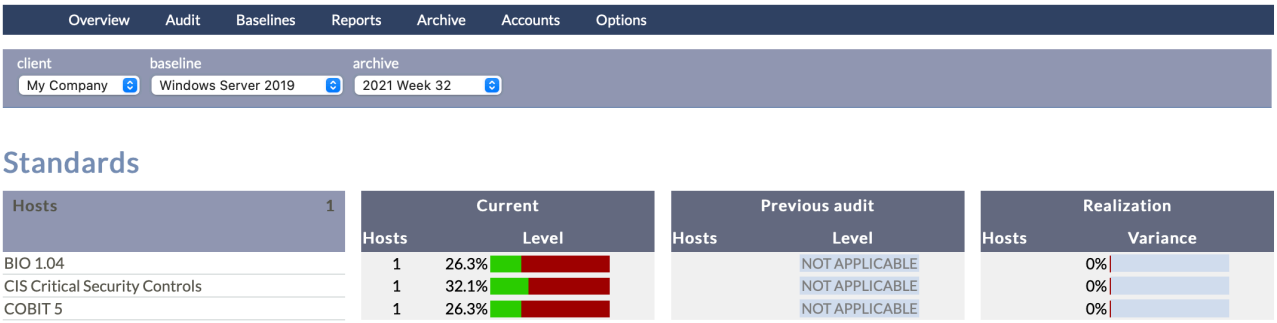
Hosts 1 Baselines 1	Current			Previous audit			Realization		
	Compliant	NOT Compliant	NOT Installed	Compliant	NOT Compliant	NOT Installed	Compliant	NOT Compliant	NOT Installed
Windows Server 2019	1			1					

Administrators

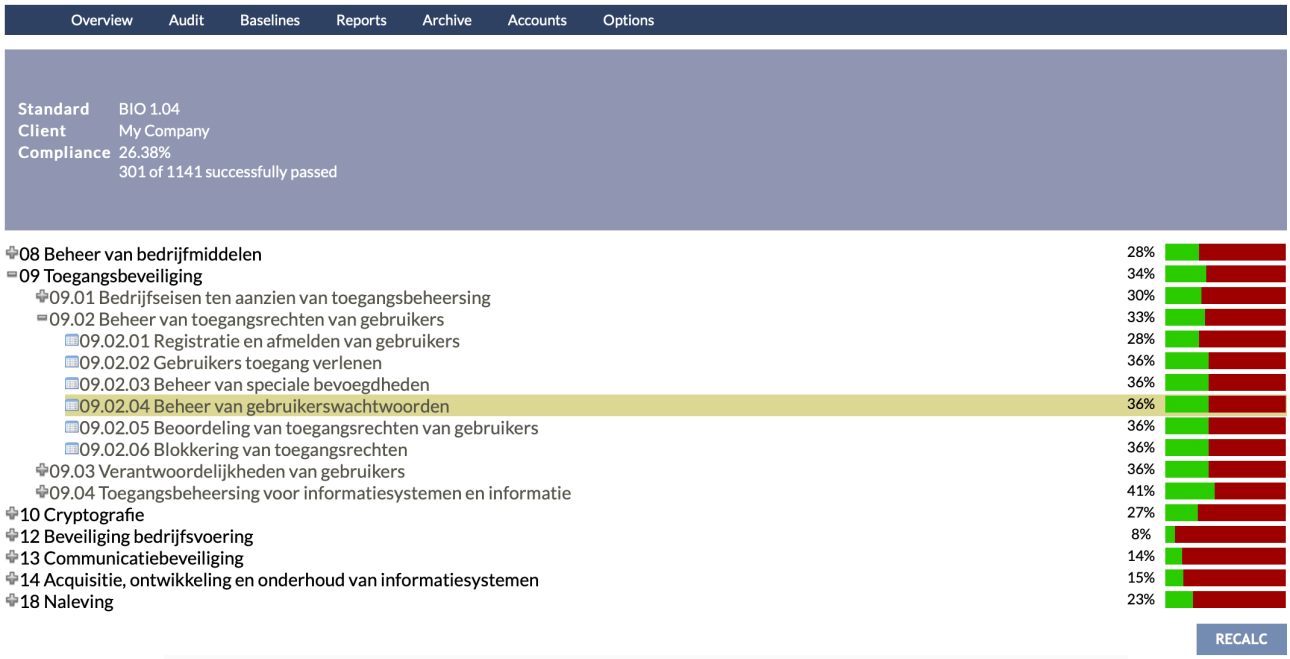
Hosts 2 Domains 1	Current			Previous audit			Differ		
	Enterprise	Domain	Users	Enterprise	Domain	Users	Enterprise	Domain	Users
Windows 2012 R2 - patched	1	1	828						

Standards

Onder standards staat een aantal standaards die u zelf heeft uitgekozen, dit doet u via het menu: Options -> Update standards en wordt later in deze manuaal besproken. De scores laten u zien in hoeverre uw technische maatregelen compliant zijn voor de genoemde standaard. Sommige standaarden, zoals de BIO, bestaan uit meer dan alleen technische maatregelen. Vanzelfsprekend kunnen wij deze niet automatisch auditen, daarom blijven deze buiten beschouwing in onze applicatie. U ziet hieronder dat er verschillende scores worden gehaald op de verschillende standaards. Omdat er bij de vorige audit geen standaards actief waren, verschijnt hier NOT APPLICABLE. Dit verklaart ook direct het verschil van 0%.

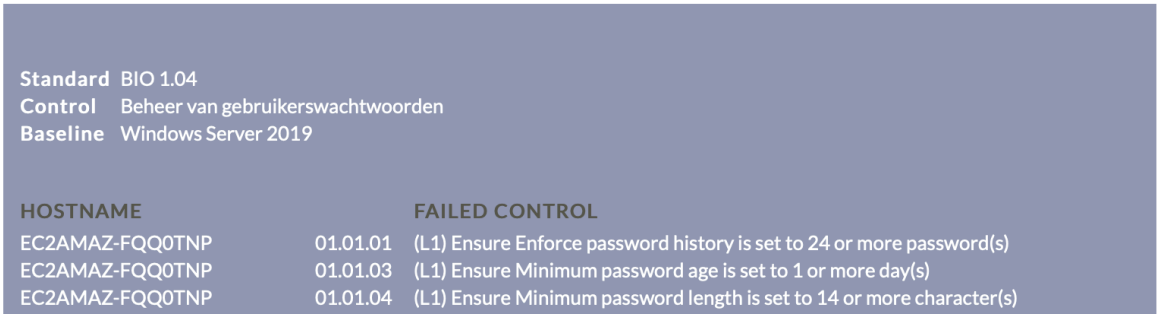


Voor dit voorbeeld klikken we op BIO 1.04 om in onderstaand scherm te komen. Door op de plusjes te drukken, klapt u de subhoofdstukken steeds uit. U kunt van de RECALC knop gebruik maken om alle scores direct opnieuw uit te rekenen. We klikken op paragraaf 09.02.04.

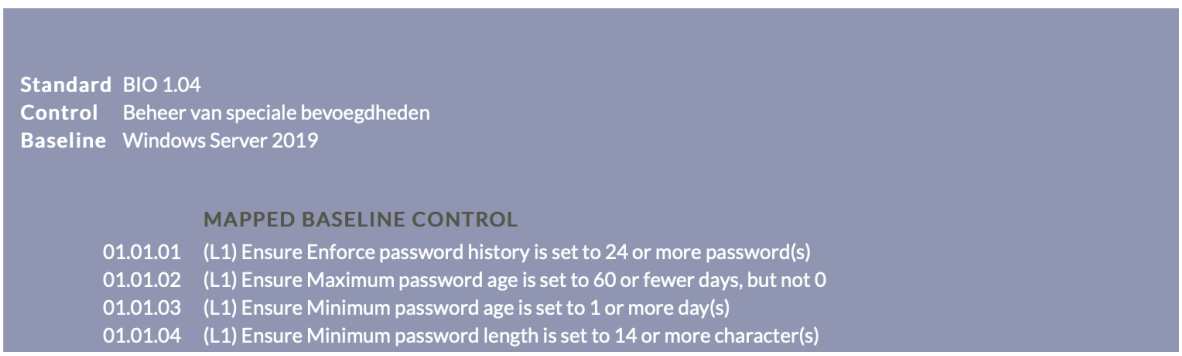


Onderstaande pop-up verschijnt. Hier ziet u informatie over de paragraaf “Beheer van gebruikerswachtwoorden”, met een beschrijving en een compliance score. Daarnaast kunt u onder FAILED zien hoeveel controls niet compliant zijn, en onder MAPPING hoe alle controls gemapped zijn naar de hoofdstukken van de standaard.

Door onder FAILED op 108 control(s) te klikken, verschijnt een nieuwe pop-up. Een deel hiervan ziet u hieronder. Hieruit blijkt bijvoorbeeld dat de minimale wachtwoord lengte van de systemen niet toereikend is, en dus lager staat ingesteld dan 14 karakters.

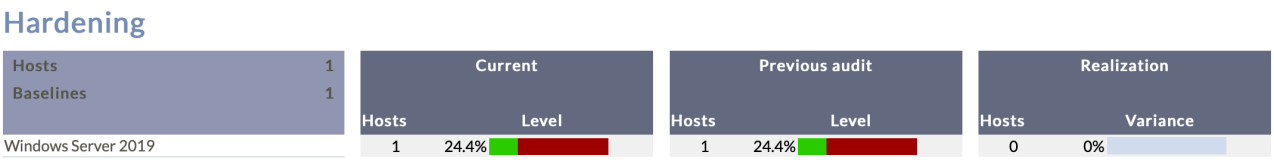


Wanneer we op het kruisje klikken rechtsboven de pop-up (staat niet op bovenstaande afbeelding) komen we terug bij de vorige pop-up en kunnen we onder MAPPING op show control(s) klikken. Hier krijgen wij eenzelfde overzicht als hierboven, nu inclusief controls die compliant zijn. Zo zien wij in onderstaande afbeelding dat ook control 01.01.02 is opgenomen in de lijst.



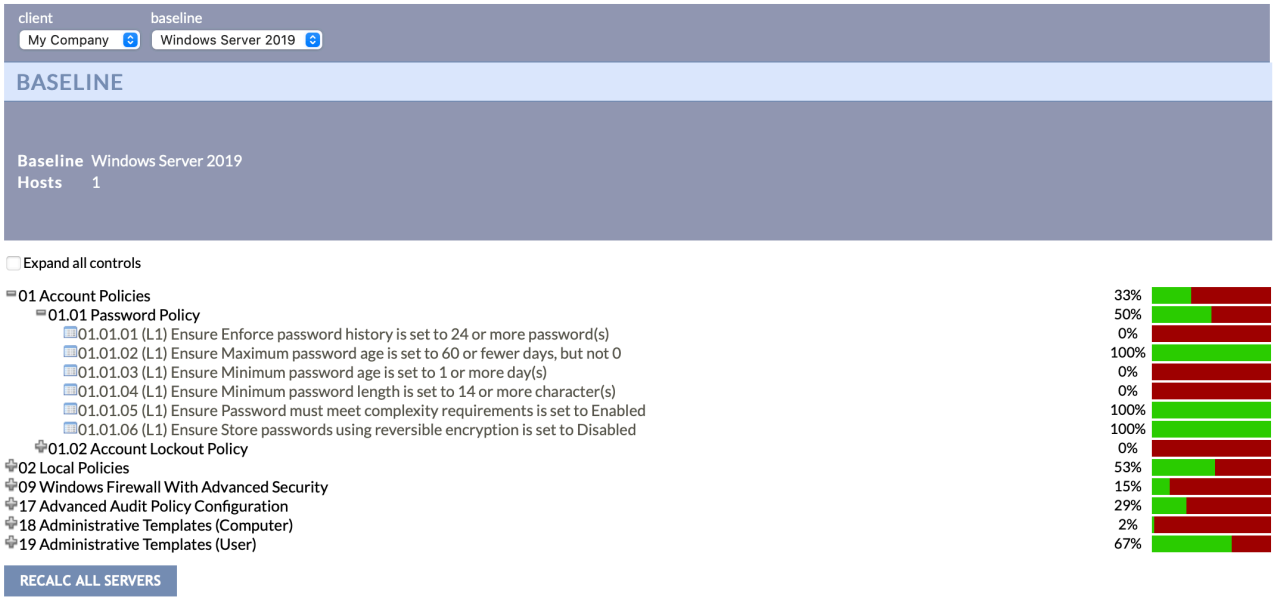
Hardening

Onder het kopje hardening vindt u een overzicht van alle systemen (die overblijven na de filters van client en baseline, zie afbeelding hierboven). In het voorbeeld hieronder is er 1 systeem (host) gevonden waarvan 1 baseline wordt gerapporteerd. In de huidige audit (current) scoort dit systeem 24.4% compliance (ten opzichte van de CIS benchmark). Deze score is hetzelfde als de eerdere audit (previous audit), dit betekent dat er geen verschil is gerealiseerd, de variance bij realization is daarom 0%.



Door op een baseline klikken, in dit geval Windows Server 2019, navigeert u naar een volgende pagina. Op deze pagina ziet u in hoeverre alle controls voldoen aan de CIS benchmark. Als voorbeeld zijn hier het eerste hoofdstuk en subhoofdstuk uitgeklapt door op het plusje te klikken. U kunt er ook voor kiezen om alle controls direct uit te klappen door de checkbox voor “Expand all controls” aan te vinken.

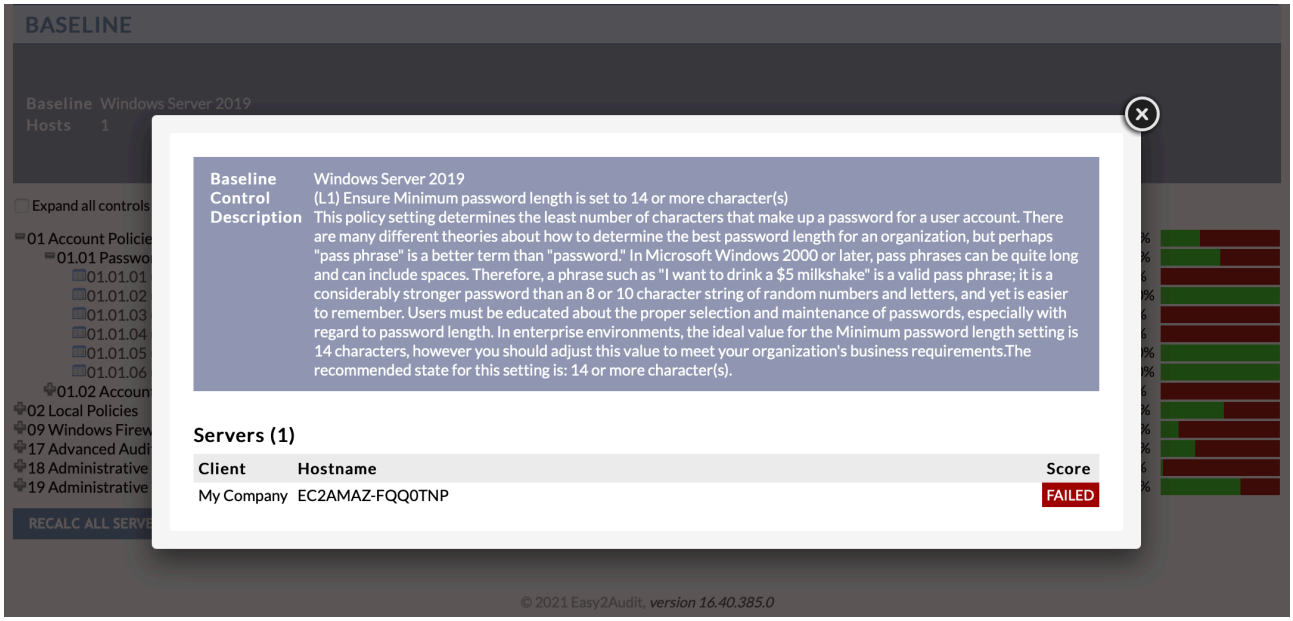
Met de knop RECALC ALL SERVERS worden alle scores opnieuw berekend.



Wanneer wij op control 01.01.04 klikken krijgen wij een pop-up.

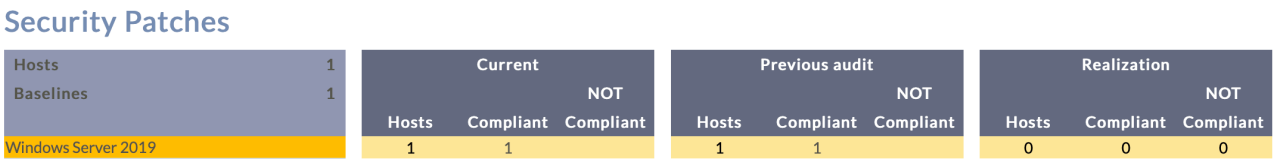
In onderstaande pop-up wordt weergegeven welke baseline het betreft (Windows Server 2019), over welke control het gaat (ensure minimum password length is set to 14 or more character(s)) en bij welk level van de CIS Benchmark deze hoort (L1 = level 1). Daarnaast wordt er een beschrijving getoond van wat deze control inhoudt.

Daaronder een overzicht van alle servers (in dit geval 1). We zien hier dat de server van client “MyCompany” met hostname EC2AMAZ-FQQ0TNP niet voldoet.



Security patches

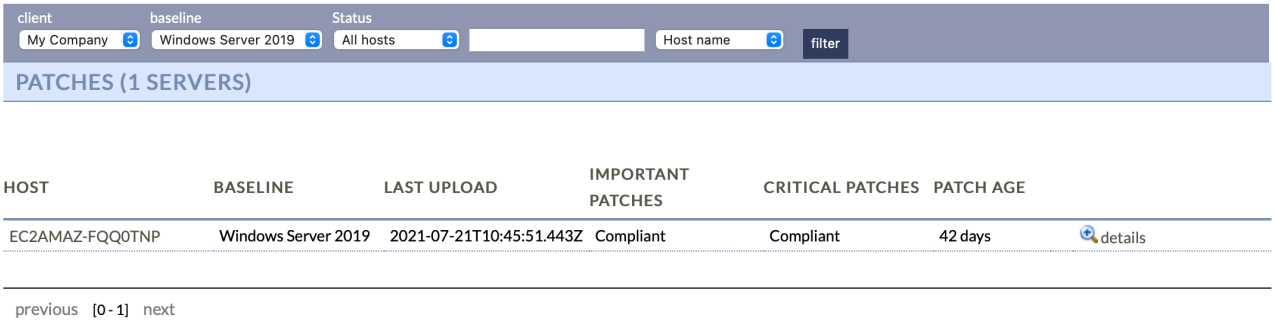
Terug op het dashboard zien we de volgende sectie bij security patches. Hier ziet u een overzicht van alle baselines, hoeveel hosts hierbij horen en hoeveel hiervan wel en niet compliant zijn bij huidige (current) en vorige (previous) audits. Daarnaast ziet u bij realization het verschil tussen de huidige en de vorige audit. In onderstaand voorbeeld ziet u dat er 1 systeem compliant is in zowel de huidige als de vorige audit, wat betekent dat er bij realization geen (0) verschil wordt weergeven.



Wanneer we klikken op de baseline (Windows Server 2019), komen we bij het volgende scherm.

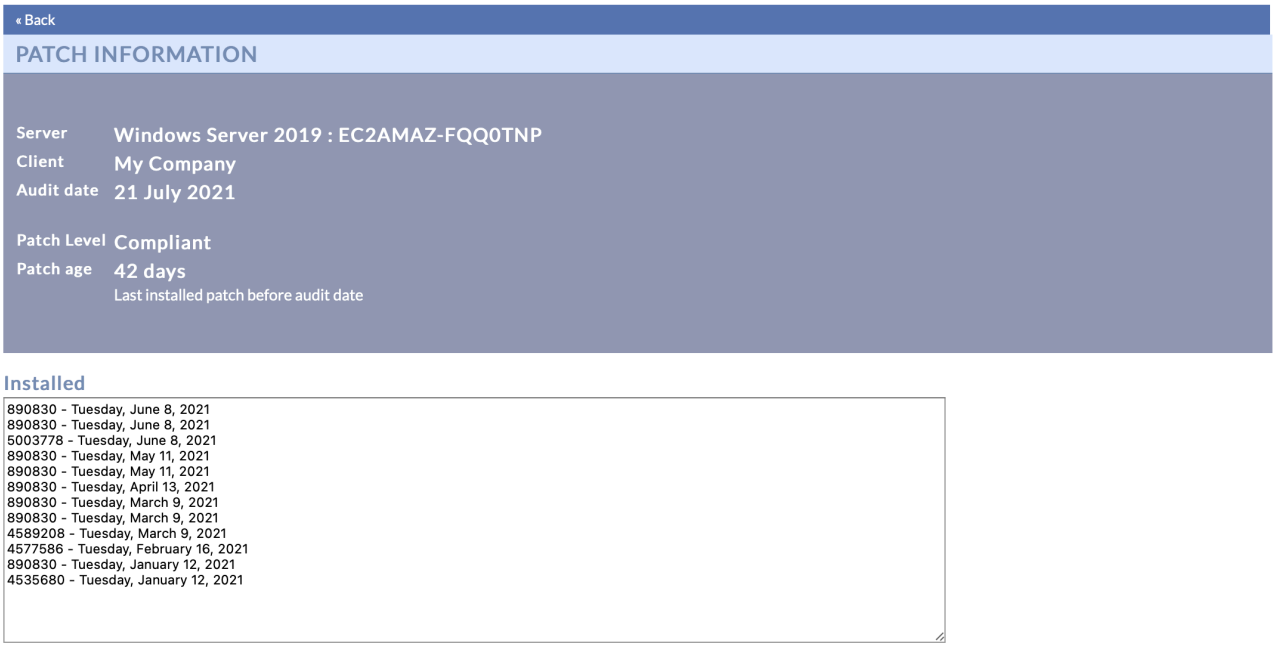
Bovenin kunt u de weergave filteren op client, baseline, status en u kunt zoeken op hostname, installed patch of missing patch.

In dit voorbeeld laten we de filter voor wat het is. Onze lijst geeft 1 systeem weer. Van links naar rechts zien we de naam van de host, de baseline, wanneer voor het laatst een audit is geüpload van dit systeem, of dit systeem compliant is ten opzichte van important en van critical patches, en hoe lang geleden de laatste patch is geïnstalleerd (vanaf de audit datum).



Wanneer we op de naam van de host klikken, of op details, komen we bij het volgende scherm.

Hier wordt informatie getoond over het systeem. We zien de baseline en de naam van de server, tot welke client groep deze behoort, en de datum van de audit. Vervolgens zien we of het patch level wel of niet compliant is en hoeveel dagen voor de laatste audit er is gepatcht. Onder installed zien we een lijst met geïnstalleerde patches.



Vulnerabilities

Terug naar het dashboard, zien we bij de vulnerabilities de volgende sectie (zie afbeelding hieronder). Van links naar rechts zien we hier de baseline, hoeveel hosts hiervan zijn meegenomen in de huidige audit, hoeveel vulnerabilities (CVE's) er zijn gevonden op de volgende niveaus: Critical, High, en Medium. Dit wordt herhaald voor de vorige audit (previous) en daarnaast worden onder realization de verschillen weergegeven, in dit geval geen, omdat de huidige audit overeenkwam met de vorige audit.

Vulnerabilities

Hosts 1 Baselines 1	Current					Previous audit					Realization				
	Total hosts	CVE's C	CVE's H	CVE's M	Affected hosts	Total hosts	CVE's C	CVE's H	CVE's M	Affected hosts	Total hosts	CVE's C	CVE's H	CVE's M	Affected hosts
Windows Server 2019	1	3	21		1	1	3	21		1	0				0

Wanneer we doorklikken door op de baseline te klikken komen we in het volgende scherm. Hier wordt de informatie van het dashboard op uitgebreidere wijze weergegeven.

Wij zien in het voorbeeld nogmaals dat er voor de enkele host met de Windows Server 2019 baseline 3 critical vulnerabilities zijn gevonden, en 21 high. Wanneer we bij het kopje IMPACT op het getal klikken in de rij van critical en de kolom van hosts, krijgen we een overzicht met van alle kritische vulnerabilities per host (in dit geval 3 vulnerabilities onder 1 host). U krijgt voor de andere cellen in deze matrix vergelijkbare pop-ups.

client: My Company baseline: Windows Server 2019

VULNERABILITIES

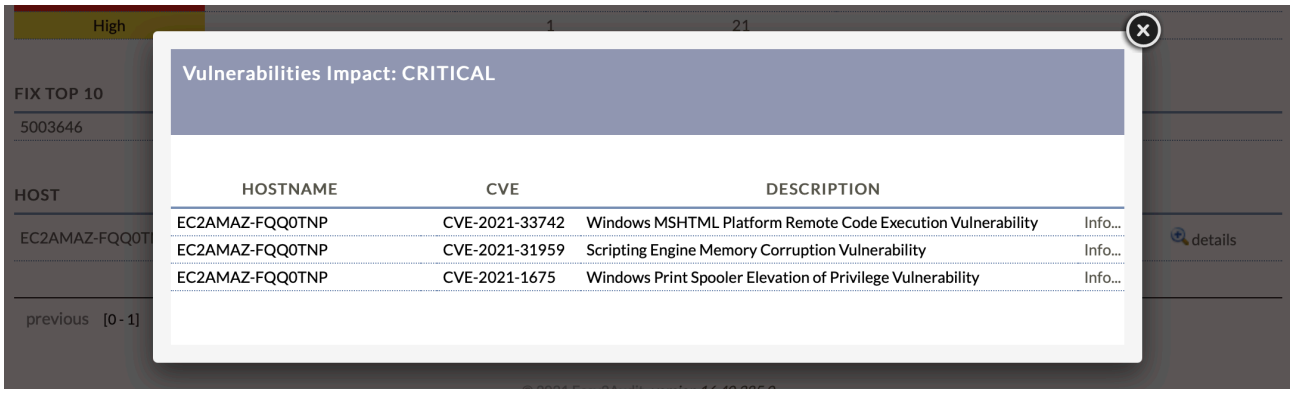
IMPACT	HOSTS	VULNERABILITIES
Critical	1	3
High	1	21

FIX TOP 10	HOSTS	CRITICAL	HIGH	MEDIUM	LOW
5003646	1	3	21		

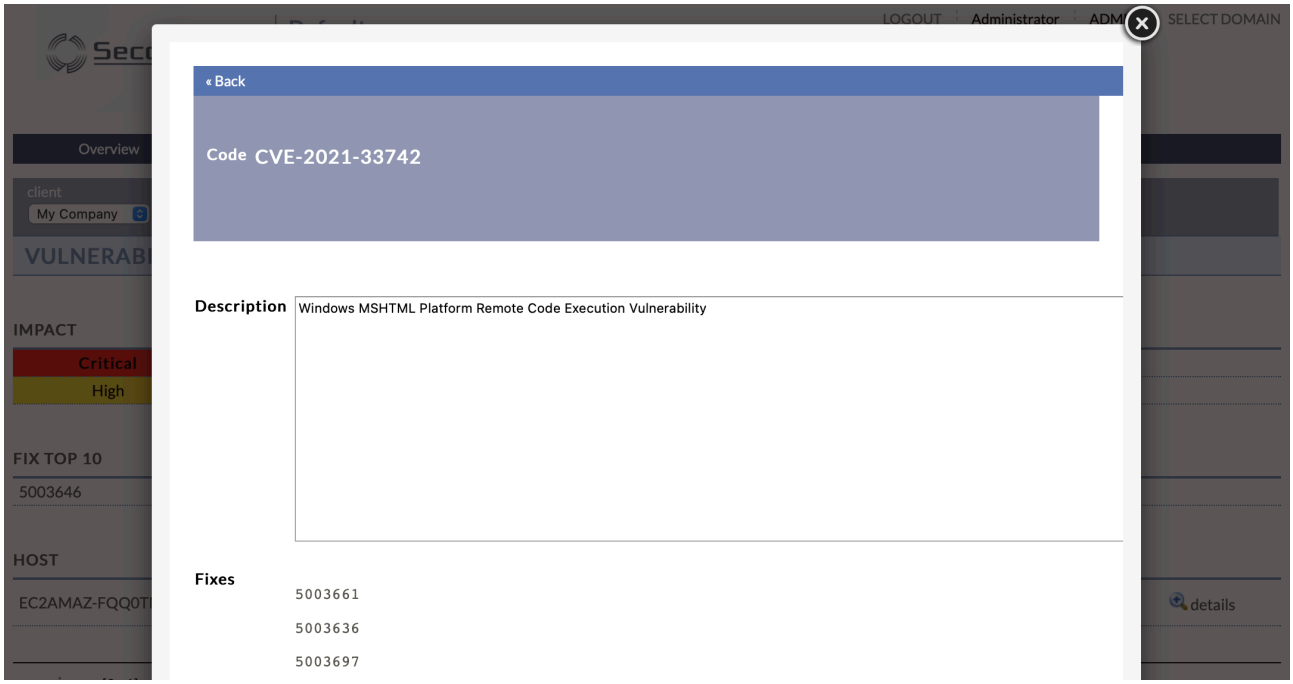
HOST	BASELINE	LAST UPLOAD	CRITICAL	HIGH	MEDIUM	LOW	NONE	STATUS	
EC2AMAZ-FQQ0TNP	Windows Server 2019	2021-07-21T10:45:51.443Z	3	21	0	0	0	24 found	details

previous [0 - 1] next

In de afbeelding hieronder vindt u het overzicht van de kritische vulnerabilities per onze enkele host. Door op info… te klikken krijgt u een pop-up met meer informatie over de specifieke vulnerability.

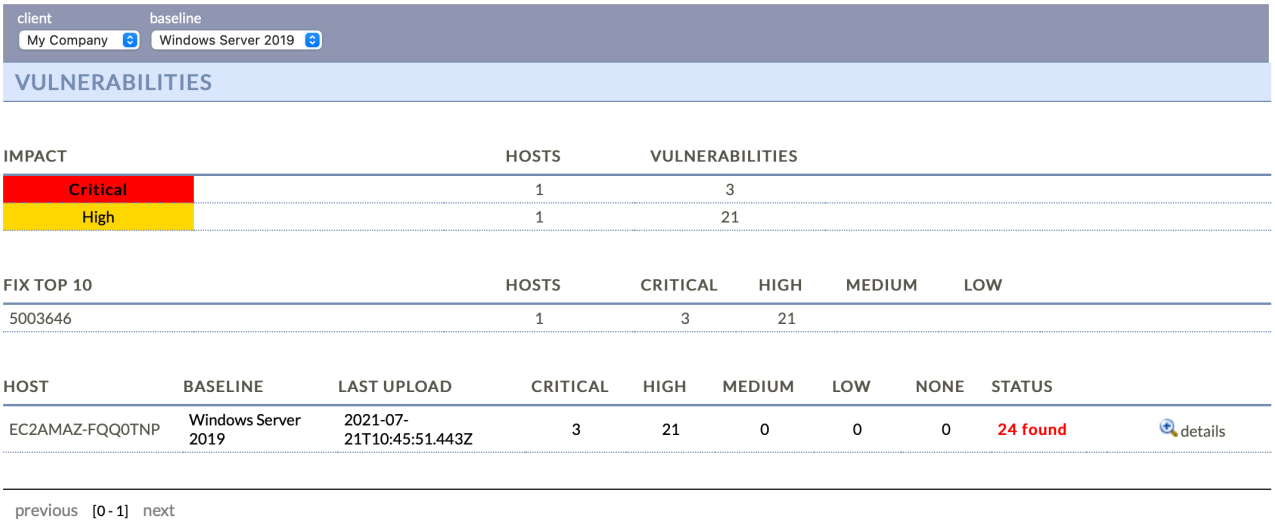


Hieronder ziet u de pop-up die hoort bij de bovenste vulnerability. Bovenaan de identificatie code van de vulnerability (CVE), eronder een beschrijving en daaronder een lijst met fixes die deze vulnerability verhelpen. U kunt deze fixes aanklikken, dan wordt u doorgestuurd naar de website van (in dit geval) Microsoft, waar u meer informatie kunt vinden over de fix.



Wanneer we de pop-ups wegklikken komen we terug bij vulnerabilities.

De FIX TOP 10 is een bijzonder interessante lijst. Aan de hand van een risico-analyse laat deze toptien zien welke fixes het grootste effect hebben op uw cyberweerbaarheid. In dit geval telt de lijst slechts 1 fix omdat deze fix alle gevonden vulnerabilities verhelpt. Ook hier kunt u op verschillende cellen in de matrix klikken voor pop-ups met overzichten.


client: My Company | baseline: Windows Server 2019

VULNERABILITIES

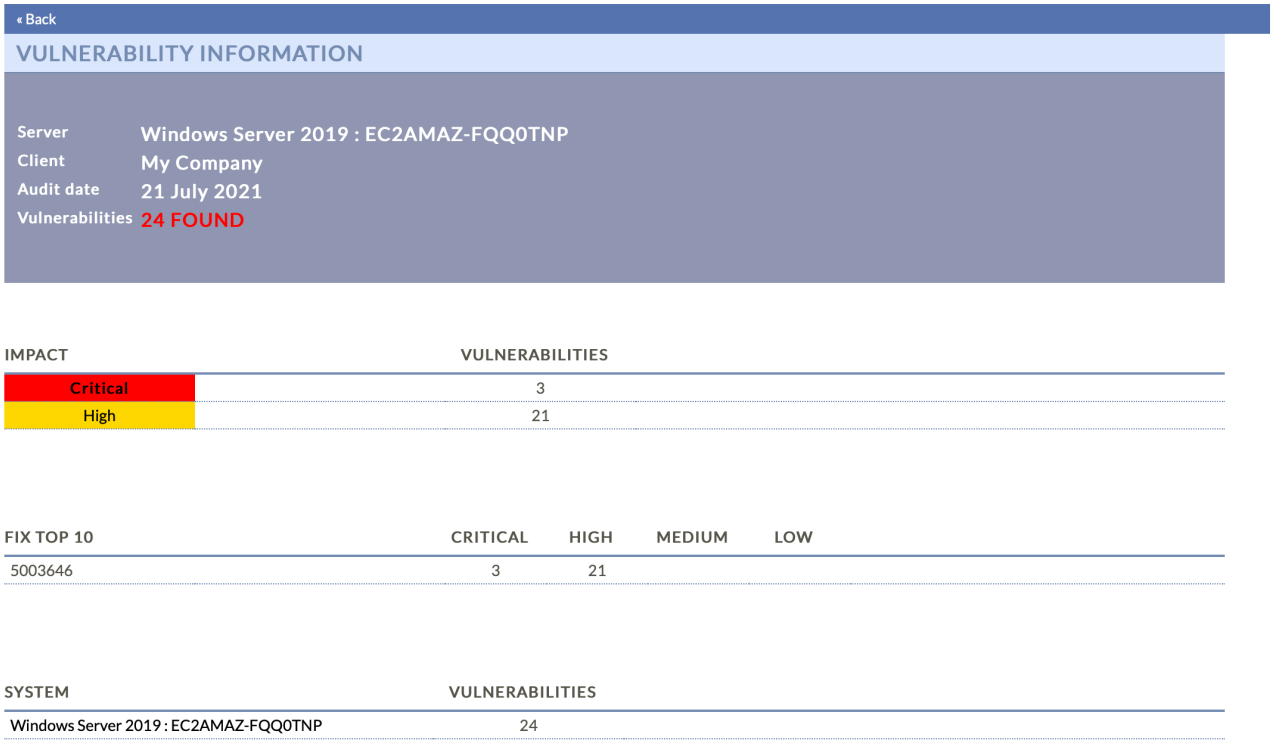
IMPACT	HOSTS	VULNERABILITIES
Critical	1	3
High	1	21

FIX TOP 10	HOSTS	CRITICAL	HIGH	MEDIUM	LOW
5003646	1	3	21		

HOST	BASELINE	LAST UPLOAD	CRITICAL	HIGH	MEDIUM	LOW	NONE	STATUS	
EC2AMAZ-FQQ0TNP	Windows Server 2019	2021-07-21T10:45:51.443Z	3	21	0	0	0	24 found	details

previous [0 - 1] next

Onderaan de pagina staat nog een lijst met hosts (in dit geval 1), met een overzicht van hun baseline, laatste audit upload, critical, high, medium, low en none level vulnerabilities, en het totaal (status). Door op de naam van de host, of op details te klikken komt u op een aparte pagina voor deze specifiek host (systeem). Zie afbeelding hieronder.


« Back

VULNERABILITY INFORMATION

Server: Windows Server 2019 : EC2AMAZ-FQQ0TNP
Client: My Company
Audit date: 21 July 2021
Vulnerabilities: 24 FOUND

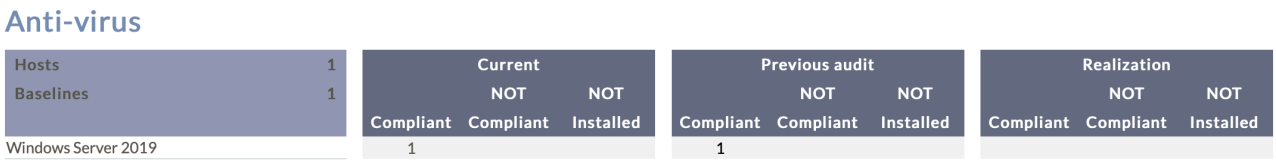
IMPACT	VULNERABILITIES
Critical	3
High	21

FIX TOP 10	CRITICAL	HIGH	MEDIUM	LOW
5003646	3	21		

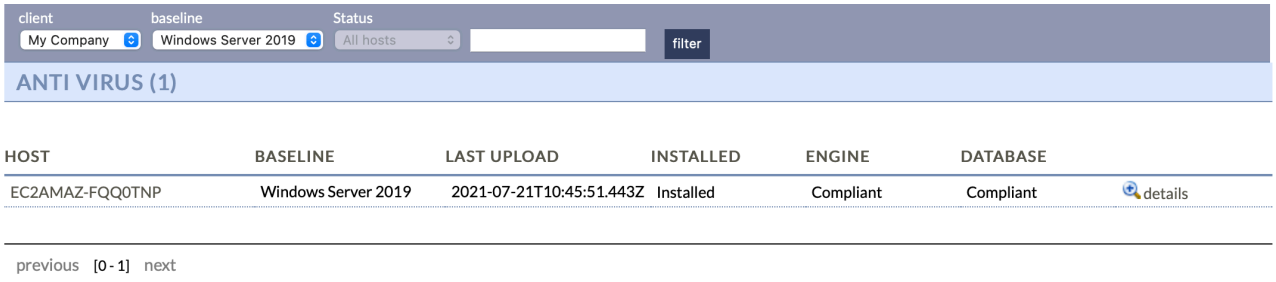
SYSTEM	VULNERABILITIES
Windows Server 2019 : EC2AMAZ-FQQ0TNP	24

Antivirus

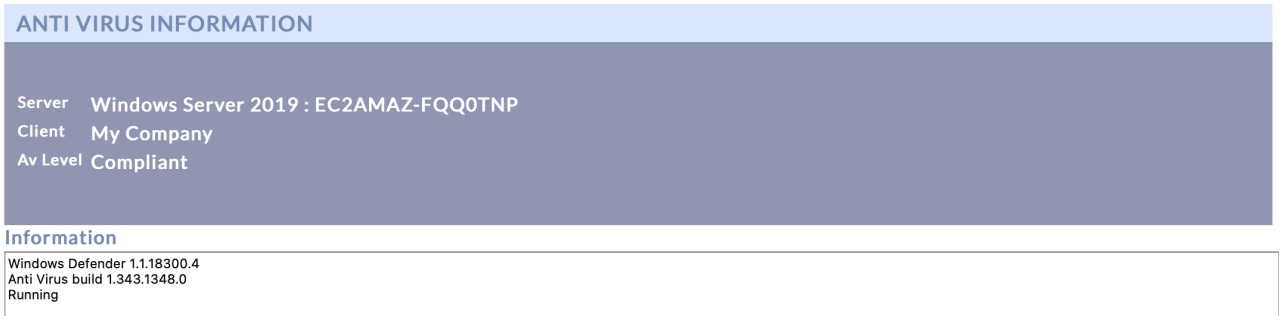
Terug op het dashboard zien we het hoofdstuk anti-virus. Hier beschouwt u een overzicht van de baselines en daarbij behorende hosts, en hoeveel van deze hosts wel en niet compliant zijn. Wederom een overzicht van huidige (current) en een vorige (previous) audit, met de vergelijking tussen huidig en vorig (realization).



Door op de baseline te klikken (Windows Server 2019) komen we in een volgend scherm. Hier zien we de bekende filters bovenaan en daaronder een lijst met hosts en extra informatie. We zien dat deze host compliant is omdat antivirus software is geïnstalleerd. Klikkend op de naam van de host of op details komen we in een volgend scherm .



Dit scherm toont informatie over de geïnstalleerde antivirus software en of deze momenteel draait (running).



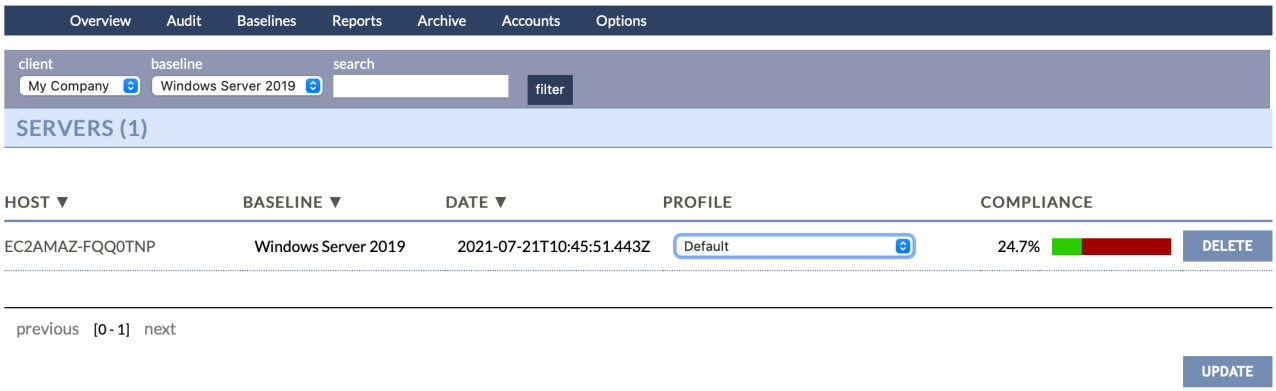
Menu: Overview -> Servers

Wanneer we boven in het menu onze muis op Overview houden, kunnen wij in het dropdown menu “Servers” selecteren. Dit brengt ons naar onderstaande pagina.

Hier wordt een overzicht getoond van alle servers (gefilterd op client, baseline en zoekterm).

In ons overzicht is een enkele server te zien, de baseline, de datum van de laatste audit, we kunnen een profiel kiezen via de dropdown, daarnaast zien we de compliance score op het gekozen profiel (standaard staan alle controls uit de CIS aan).
Via de DELETE knop kan de server uit dit overzicht worden verwijderd.

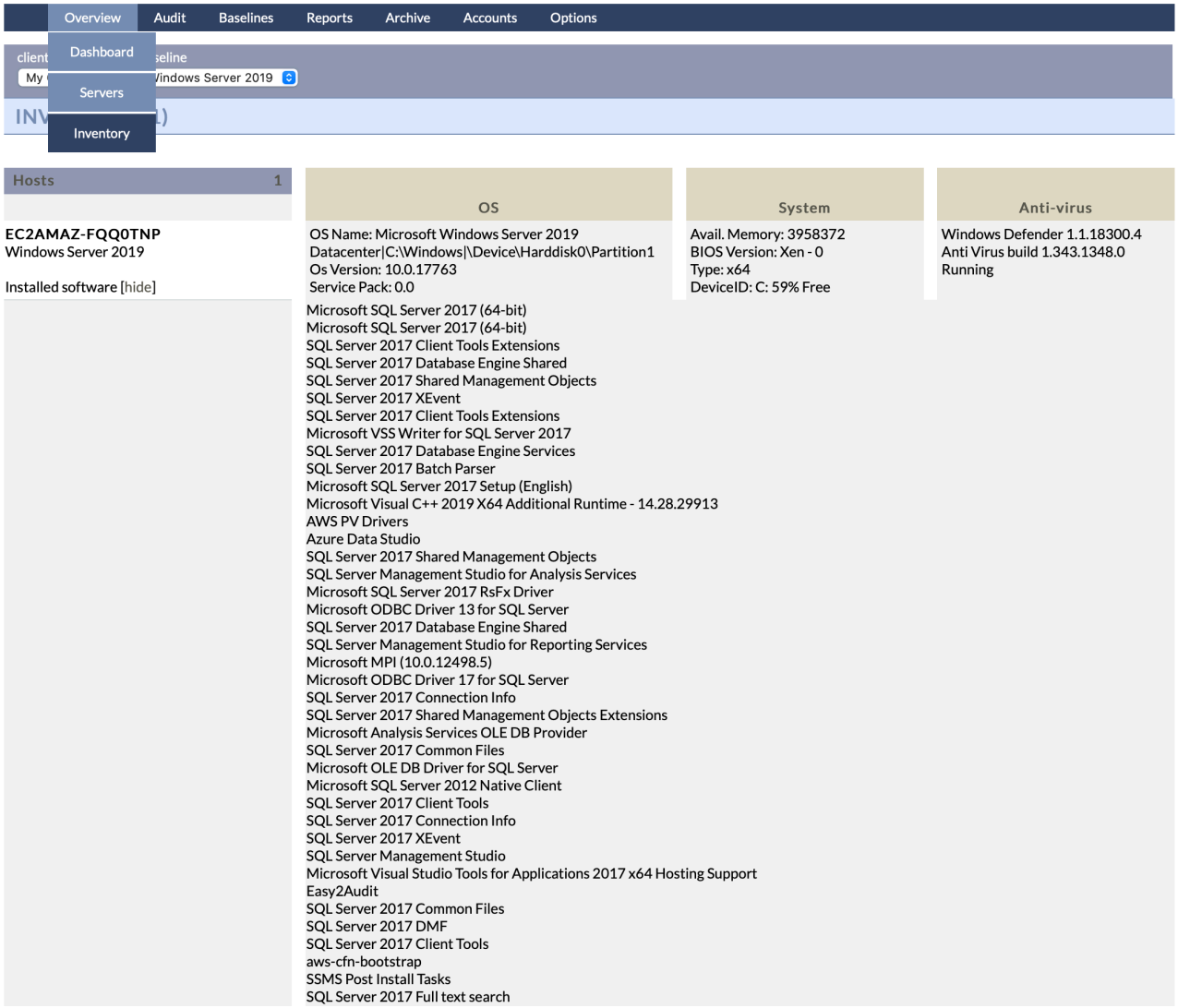
Via de UPDATE knop wordt de compliance score geüpdatet nadat er een ander profiel is geselecteerd.



Als we op de hostname klikken komen wij in een volgend scherm waar wij kunnen zien welke controls zijn uitgeschakeld in het huidige profiel (door ‘show disabled controls’ aan te vinken). Via de EXPAND knop vouwen alle controls uit in onderstaand menu. Door een archief te kiezen (bij choose archive) kunt u de huidige audit vergelijken met een eerdere audit. Met de RECALC knop kunt u nieuwe scores genereren als u een ander profiel heeft geselecteerd.

Menu: Overview -> Inventory

Het inventory overzicht laat per server een aantal kenmerken zien, het operating system (OS), een aantal hardware speciticaties (System), en welke antivirus er draait. Helemaal links in de kolom met hosts, vindt u een tekstknopje [show]/[hide]. Hiermee klapt u de lijst met geïnstalleerde software in en uit.

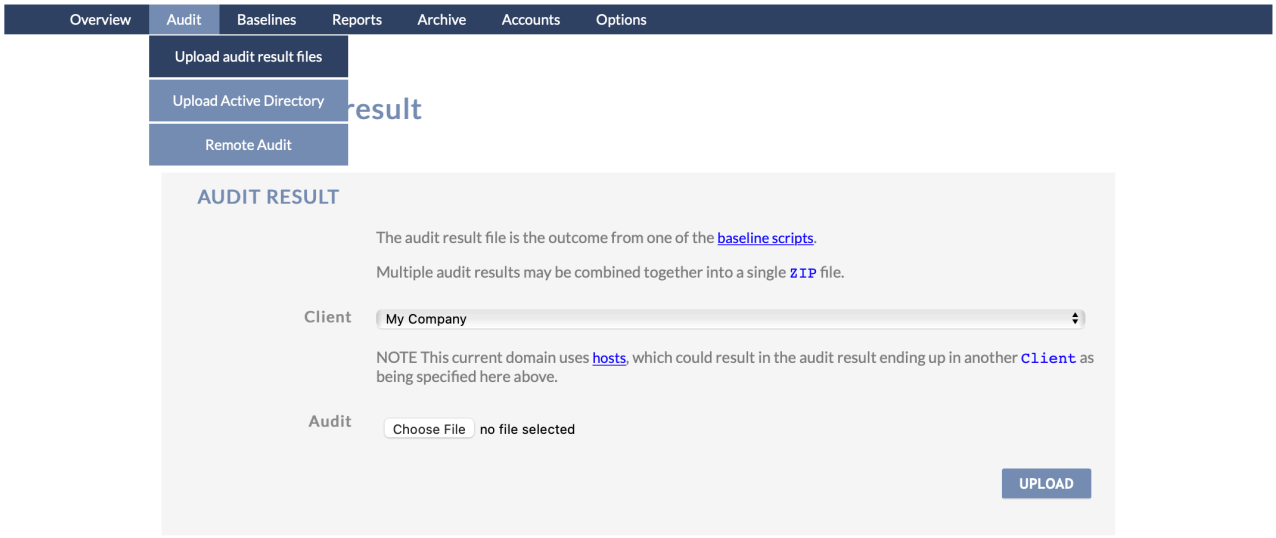


Menu: Audit -> Upload audit result file

Via deze pagina kunt u resultaat files uploaden na handmatige audits. Als u een handmatige audit wilt uitvoeren kunt u hiervoor een script downloaden via de link baseline scripts. Na een handmatige audit kunt u het resulterende tekstbestand opzoeken via de Choose file knop en daarna uploaden via de UPLOAD button.

Note: Wanneer u gebruikmaakt van een hosttabel, zal de audit deze tabel volgen, ook al geeft u op deze pagina een andere client aan.

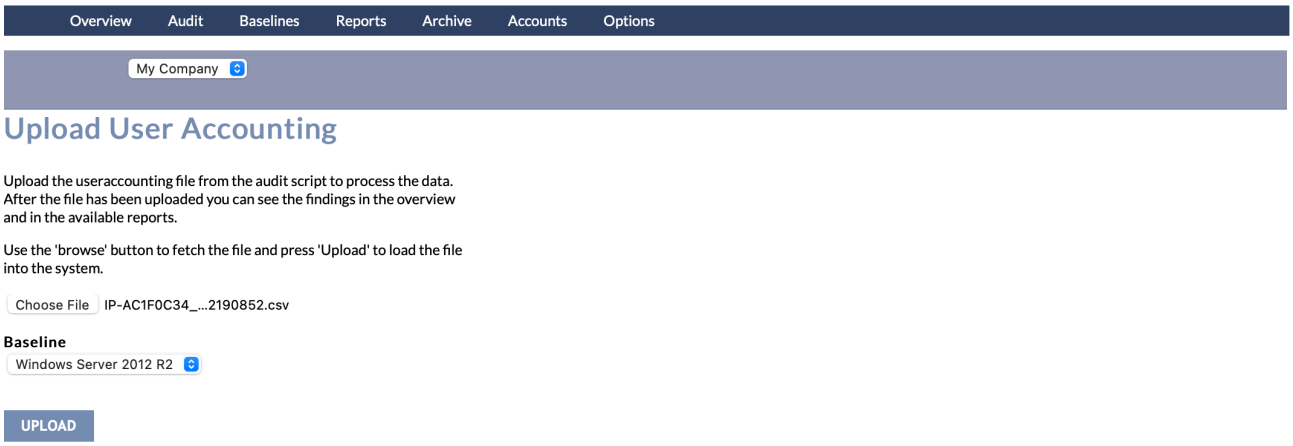
De audit zal nu verschijnen in het dashboard.

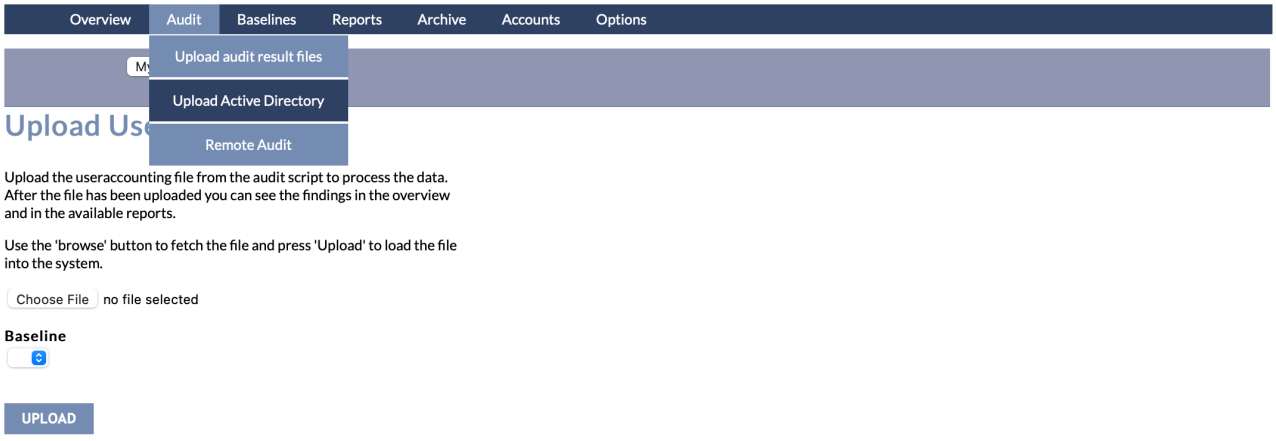


Menu: Audit -> Upload Active Directory

Op deze pagina kunt u uw active directory file uploaden.

Via Options -> Downloads kunt u de tool suite vinden. Als u deze download, vindt u een bestand met uitleg over hoe u de benodigde .csv file verkrijgt.

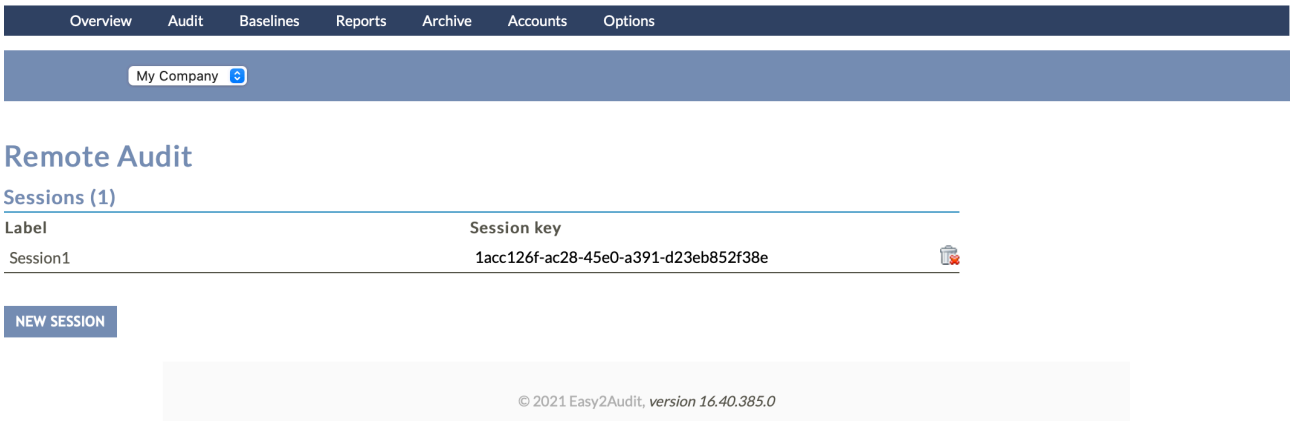




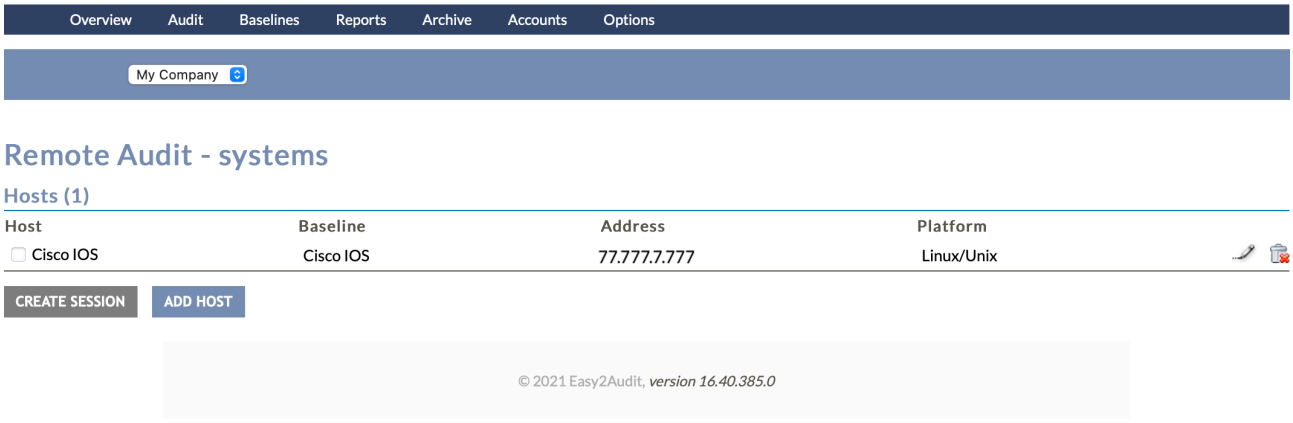
Menu: Audit -> Remote Audit

Op deze pagina kunt u een remote audit uitvoeren. Deze vorm van auditen komt van pas als op het device zelf geen script gedraaid kan worden. Als voorbeeld gebruiken wij in deze handleiding een Cisco switch.

Op de remote audit pagina vindt u een overzicht van eerdere sessies, én kunt u een nieuwe sessie starten door op NEW SESSION te klikken.

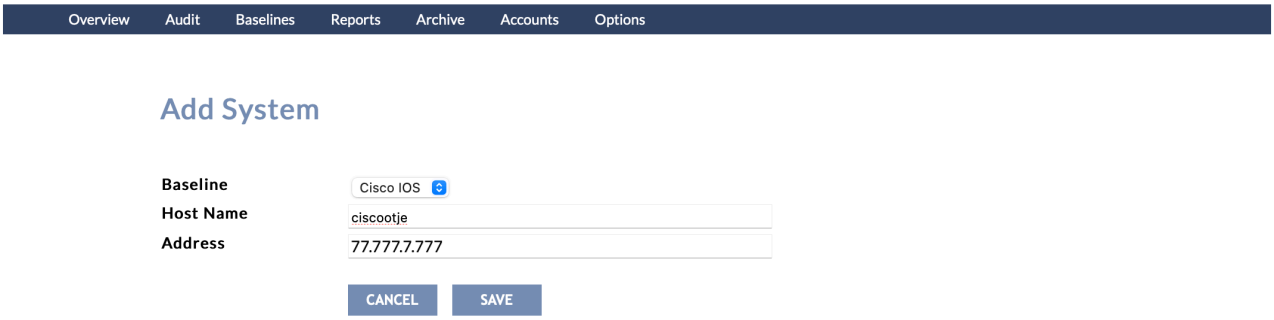


Als u op NEW SESSION heeft geklikt kunt u een bekende host aanvinken om daarop een remote audit uit te voeren met CREATE SESSION, of ervoor kiezen om een nieuwe host toe te voegen via ADD HOST.



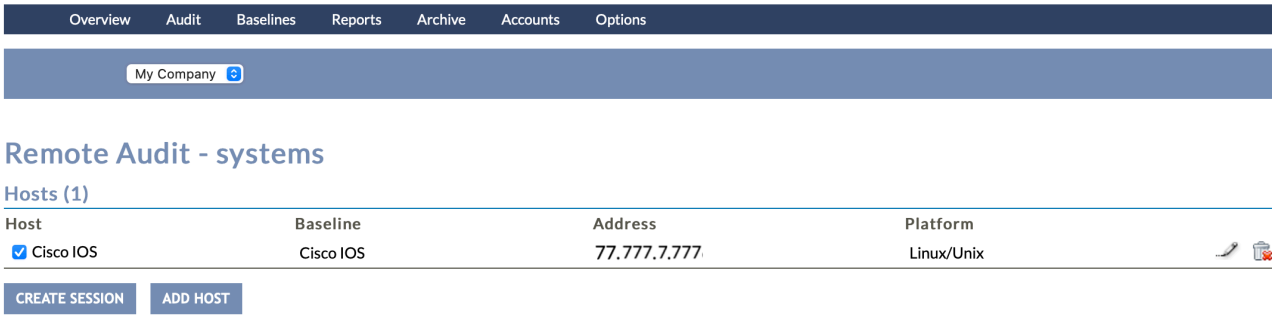
Als u op ADD HOST heeft geklikt wordt u gevraagd om een aantal gegevens in te voeren.

Selecteer eerst 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 selecteren. Voer een host name in (kies deze zelf) en het juiste ip-adres van het network device. Klik vervolgens op SAVE.

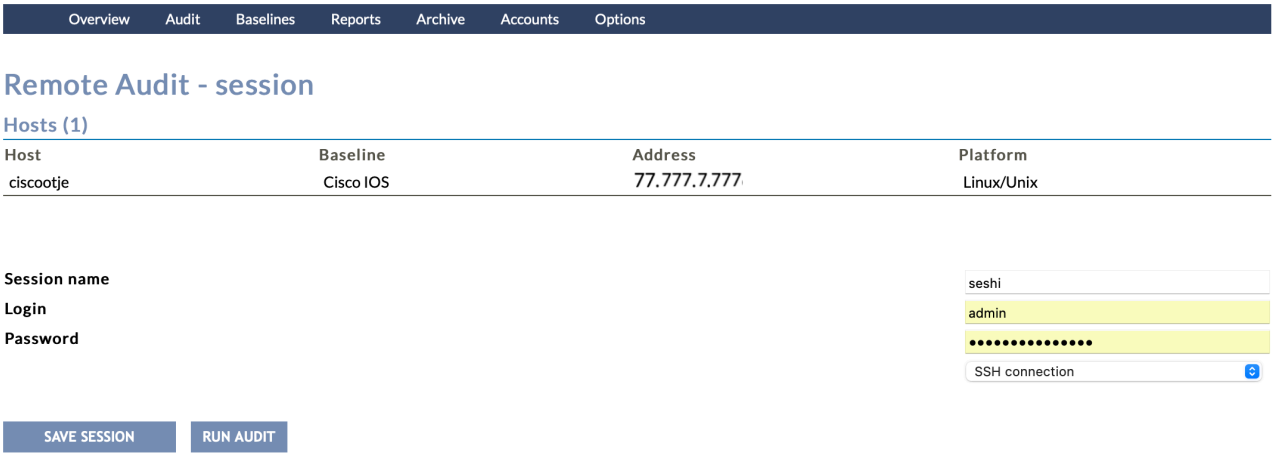


Daarna kunt u terug naar het menu: Audit -> Remote audit -> NEW SESSION.

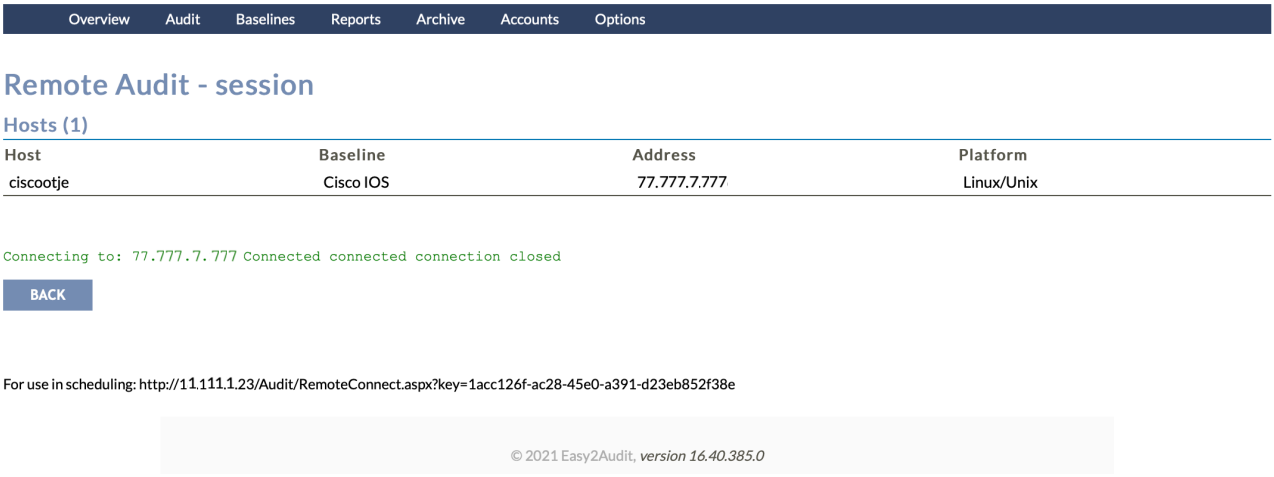
Hier kunt u het device aanvinken en klikken op CREATE SESSION.



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

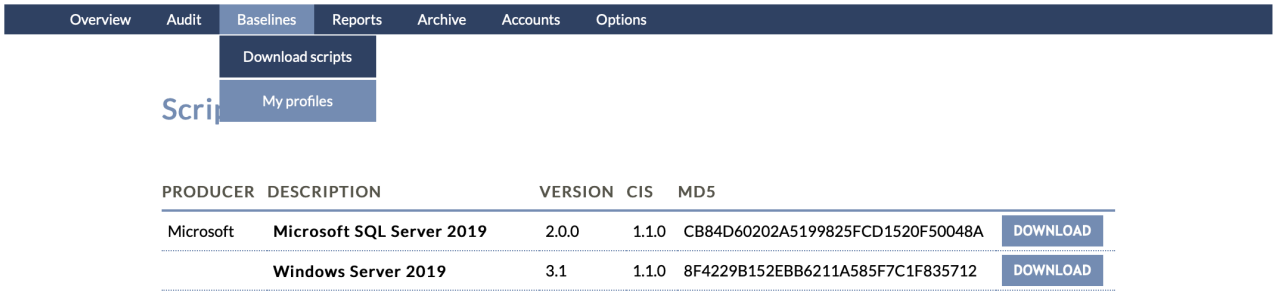


Wacht even tot de audit klaar is. Als deze goed is verlopen zult u onderstaande melding zien. Daaronder verschijnt direct een URL voor het automatisch inplannen. Voor meer informatie over het automatisch inplannen van remote edits, kunt u terecht bij de Secquard tool suite (menu: Options -> Downloads -> download tool suite).

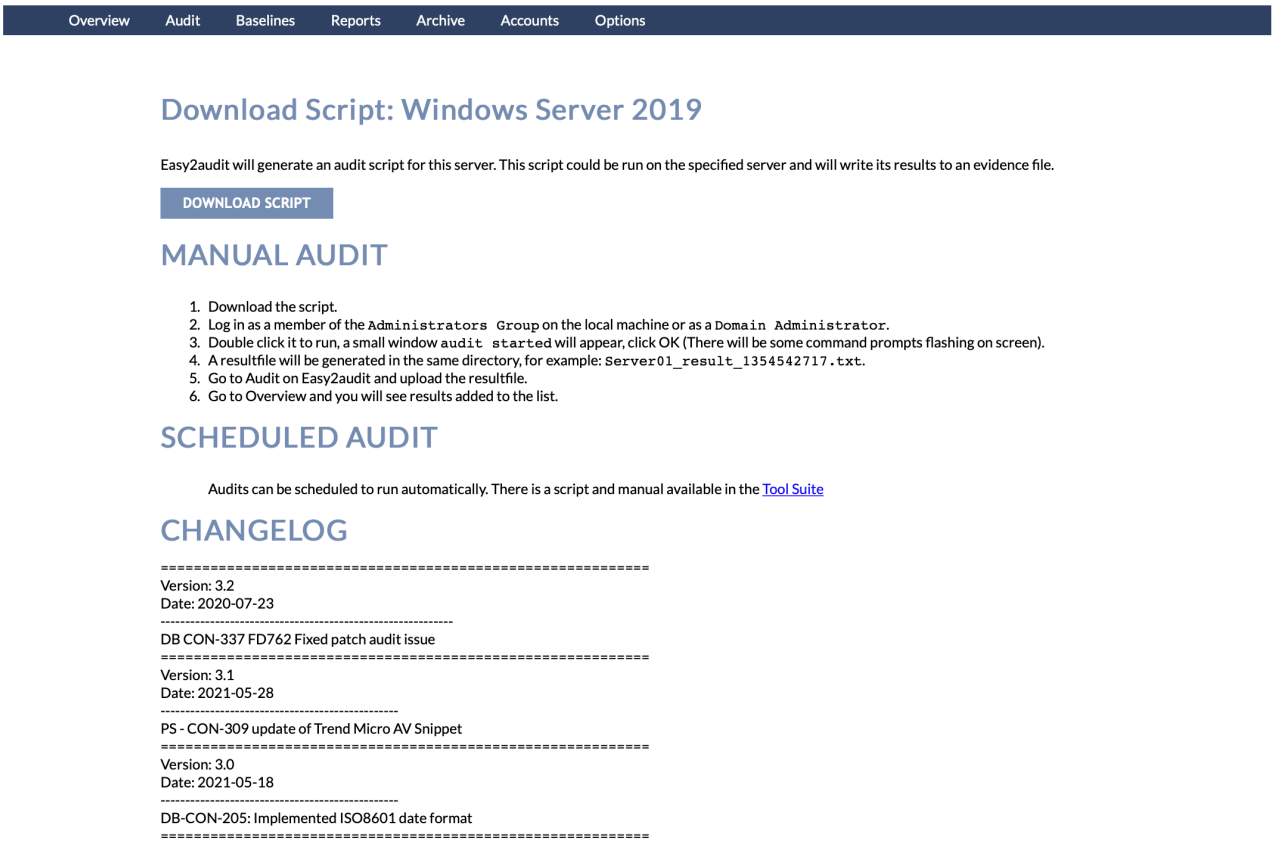


Menu: Baselines -> Download scripts

Op deze pagina kunt u scripts downloaden. Als het script dat u nodig hebt hier niet bij staat, ga dan naar het menu: Options -> Update Baselines en klik op update bij de gewenste baseline. Als u nu terugkeert naar Baselines -> Download scripts, zal het script hier getoond worden.

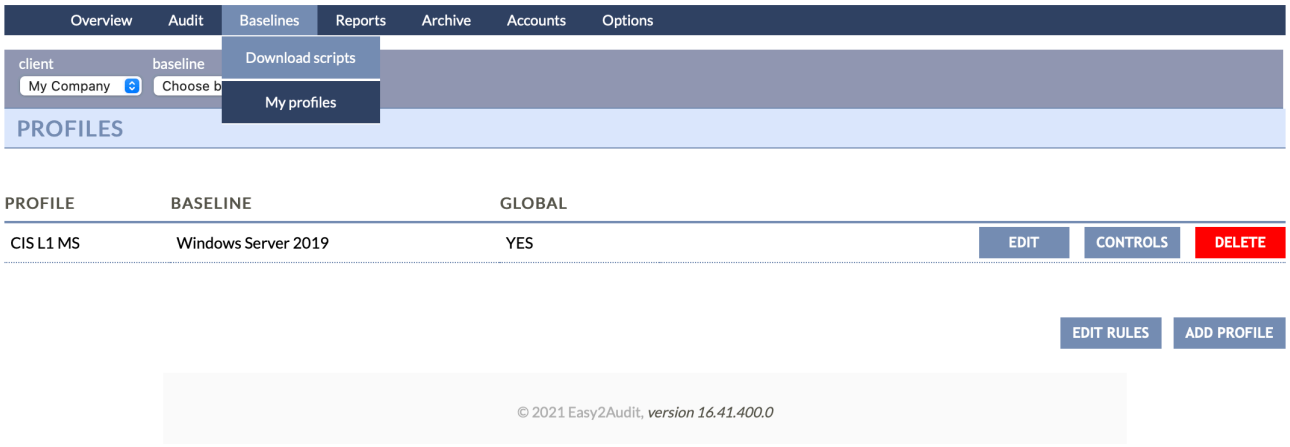


Als u op download klikt, komt u op onderstaande pagina, waar u via de DOWNLOAD SCRIPT knop uw script download. Instructies voor het runnen voor het script worden daarnaast in 6 stappen beschreven. U kunt ervoor kiezen om audits automatisch uit te voeren, instructies daarvoor vindt u via de link naar de Tool Suite. Tenslotte vindt u een changelog, waar u de laatste aanpassingen aan het script kunt teruglezen.

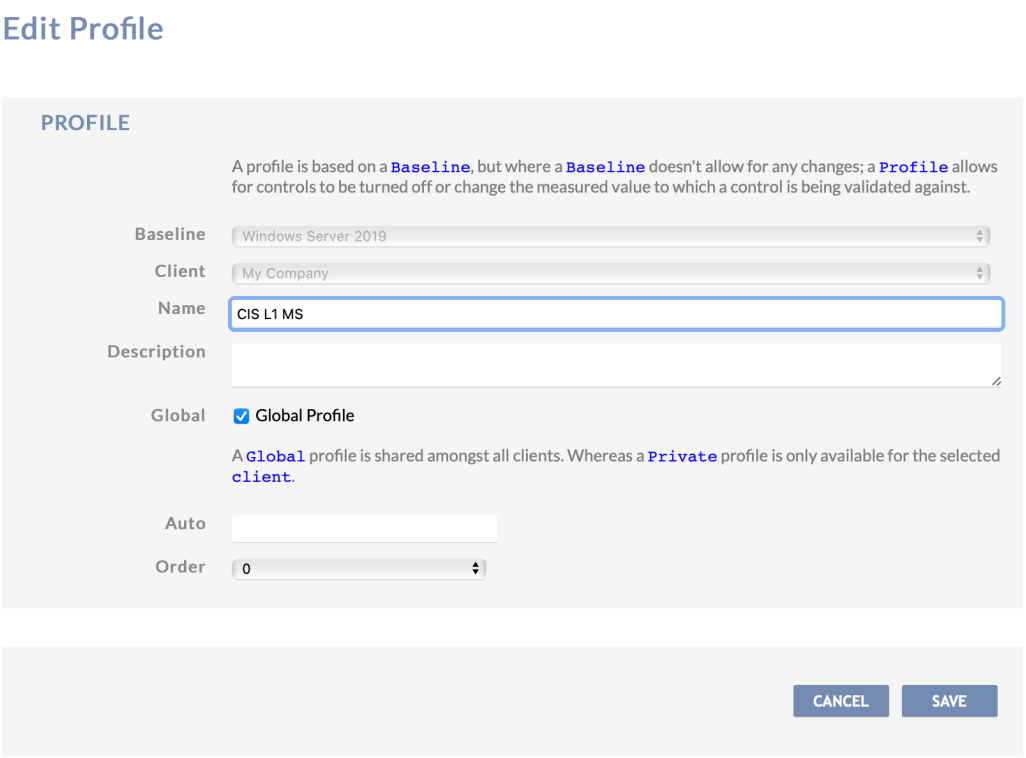


Menu: Baselines -> My profiles

Op deze pagina vindt u uw profielen. Een profiel is een set met regels die ervoor zorgen dat bepaalde controls wel of niet worden meegenomen in een audit.
Standaard worden alle controls van een systeem meegenomen in audits. Met een CIS L(evel)1 profiel worden sommige controls niet meegenomen. Dit kan voor een hogere score zorgen dan wanneer u geen profiel toepast. Het is belangrijk dat u de juiste profielen kiest voor de juiste systemen.

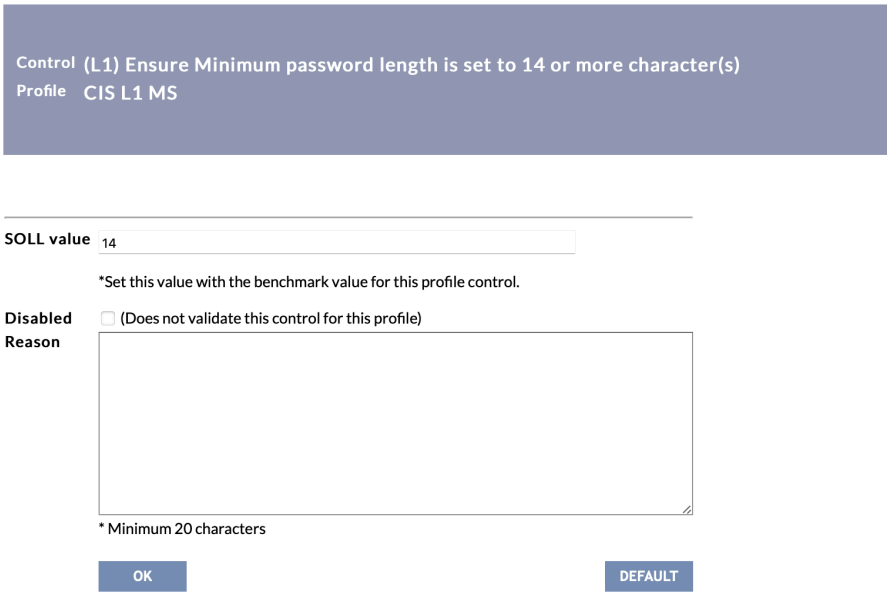


Als u op de EDIT knop drukt, kunt u verschillende parameters van uw profiel aanpassen. Zoals u hieronder kunt zien past u op eenvoudige wijze de naam van het profiel, en de omschrijving aan. Daarnaast kunt u aan en uitzetten of het profiel wordt gedeeld onder alle clients. Auto en order kunt u gebruiken om automatisch profielen toe te kennen. Deze functionaliteit is nog wat te ingewikkeld in gebruik om hier uit te leggen, maar zal later versimpeld worden.



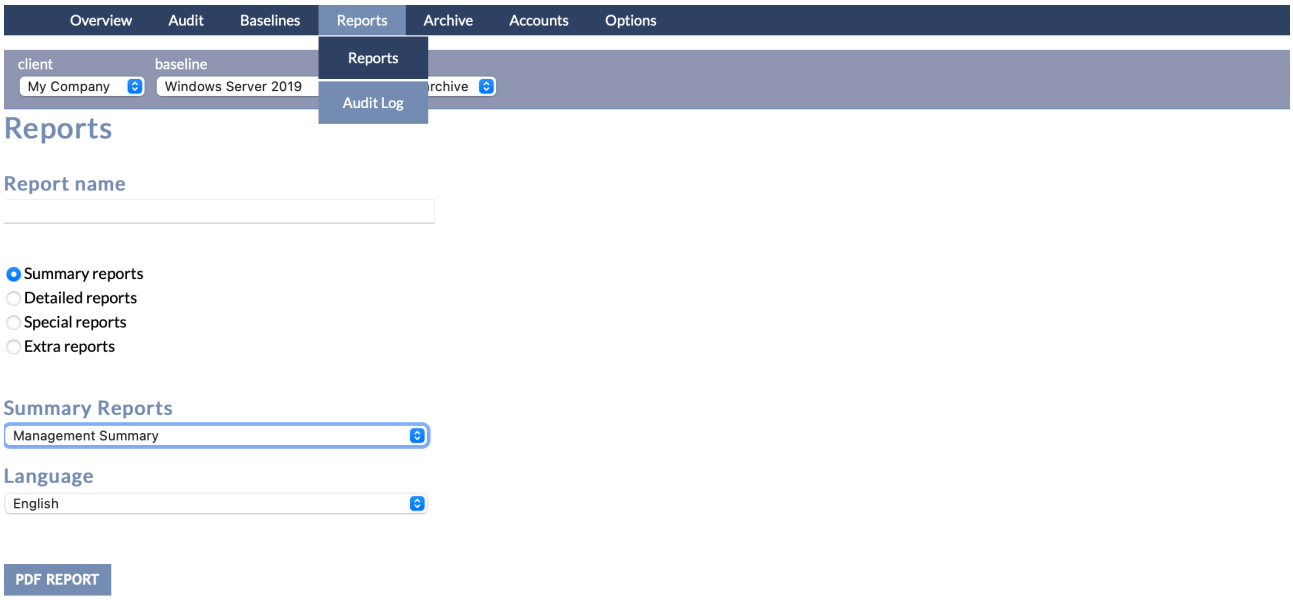
Via CONTROLS vindt u een overzicht van alle opgenomen controls van het profiel. Zoals u hieronder kunt zien, kunt u op de plusjes klikken om de hoofdstukken uit te klappen. U kunt hier ook profielen importeren via IMPORT, bijvoorbeeld nadat u een profiel heeft gedownload via het menu: Options -> Downloads -> DOWNLOAD PROFILE. Als u wijzigingen heeft doorgevoerd aan een profiel kunt u deze ook exporteren via de EXPORT KNOP, zodat u deze later weer kunt importeren. De RECALC knop zorgt ervoor dat uw compliance scores opnieuw worden berekend.

Door op een potloodje te klikken kunt u per control wijzigen wat de SOLL-positie in uw profiel is. Dit is de positie waartegen getoetst wordt. in onderstaand voorbeeld kunt u de minimale wachtwoord lengte aanpassen. Als u een goede reden heeft om de standaard van 14 karakters te wijzigen, kunt u dit hier doen én toelichten.



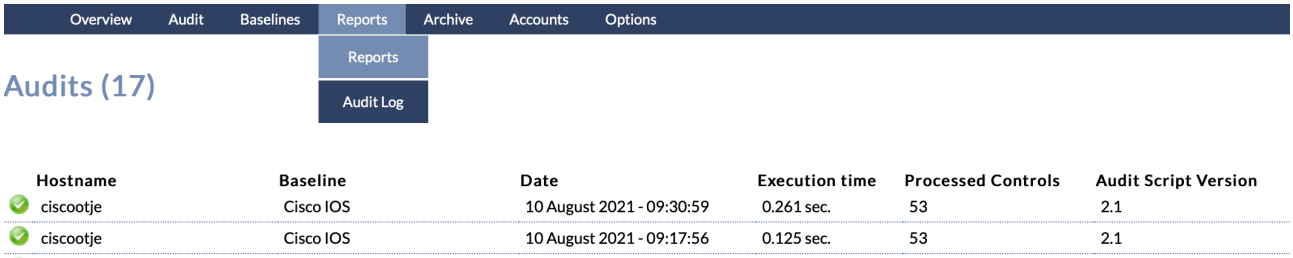
Menu: Reports -> Reports

Via de reports pagina kunt u verschillende rapportages downloaden. U kunt kiezen voor samenvattingen, gedetailleerde rapporten, speciale rapporten en extra rapporten. Via de dropdown keuze-menu's daarna kunt u uw selectie verder specificeren voordat u uw rapport downloadt.



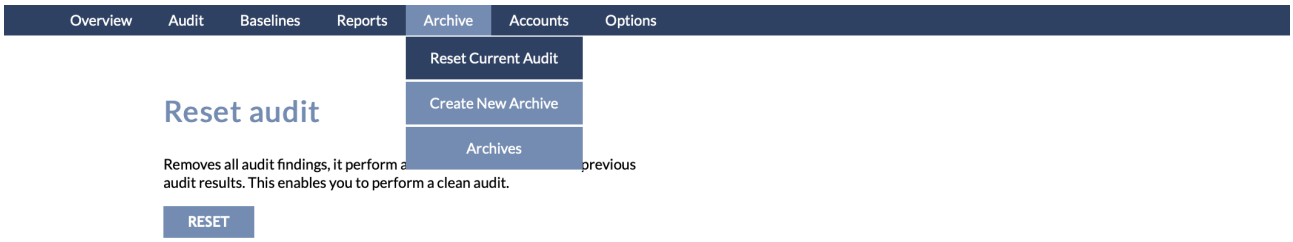
Menu: Reports -> Audit Log

Op deze pagina vindt u een overzicht van de uitgevoerde audits. Iedere audit is voorzien van informatie over de hostname, baseline, datum, hoe lang de audit duurde, hoeveel controls er zijn gecontroleerd en welke versie van het script (voor de specifieke baseline) is gebruikt.



Menu: Archive -> Reset Current Audit

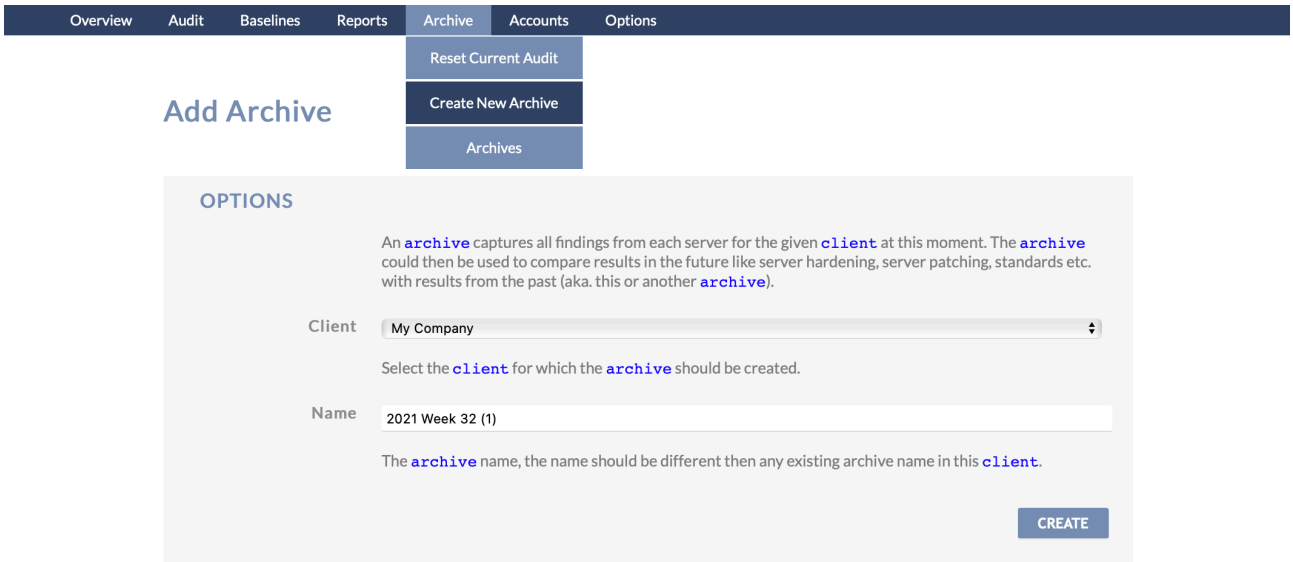
Via reset current audit kunt u alle huidige resultaten verwijderen, zodat u een ‘clean audit’ kunt uitvoeren.



Menu: Archive -> Create New Archive

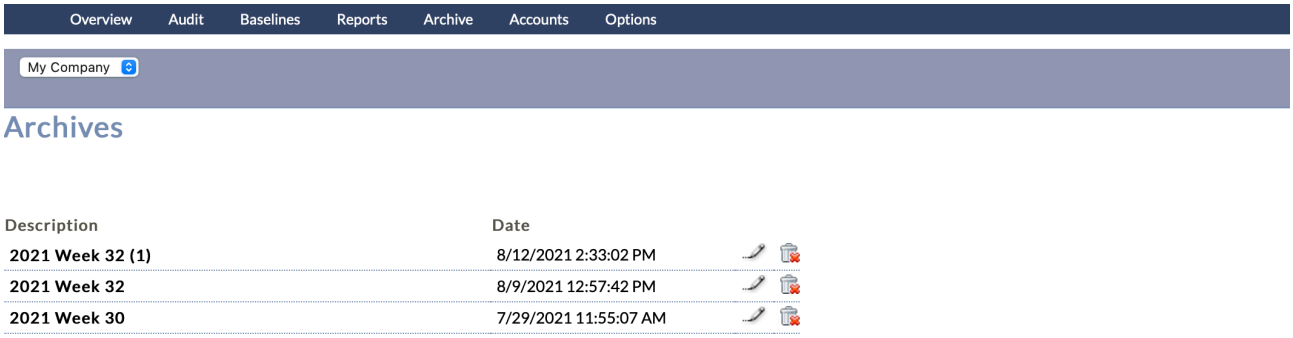
Create new archive kunt u gebruiken om handmatig een nieuw archief te creëren. Dit archief kunt u gebruiken om toekomstige audits mee te vergelijken. Ook zal deze automatisch worden meegenomen in de trendrapportage.

U kunt specificeren voor welke client u het archief wilt aanmaken en wat de naam voor dit archief moet zijn. Met de CREATE knop maakt u het archief daadwerkelijk aan.



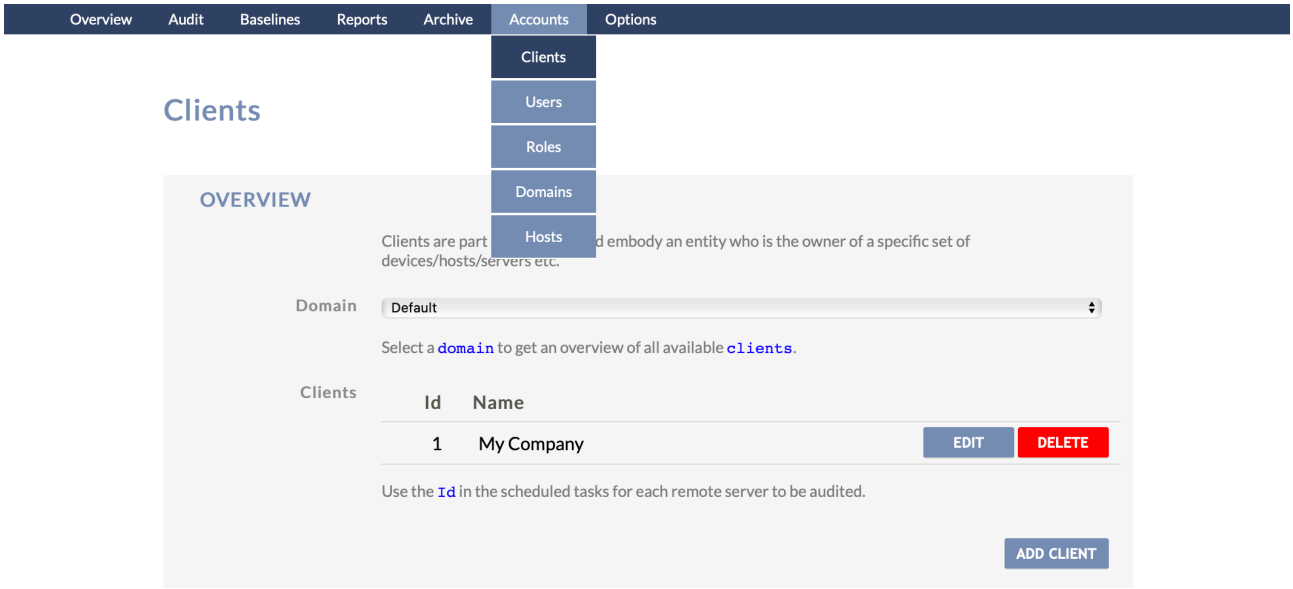
Menu: Archive -> Archives

Hier ziet u een overzicht van uw archieven met de daarbij behorende data. U kunt de namen van de archieven wijzigen met het potloodje en eventueel verwijderen met het prullenbakje.

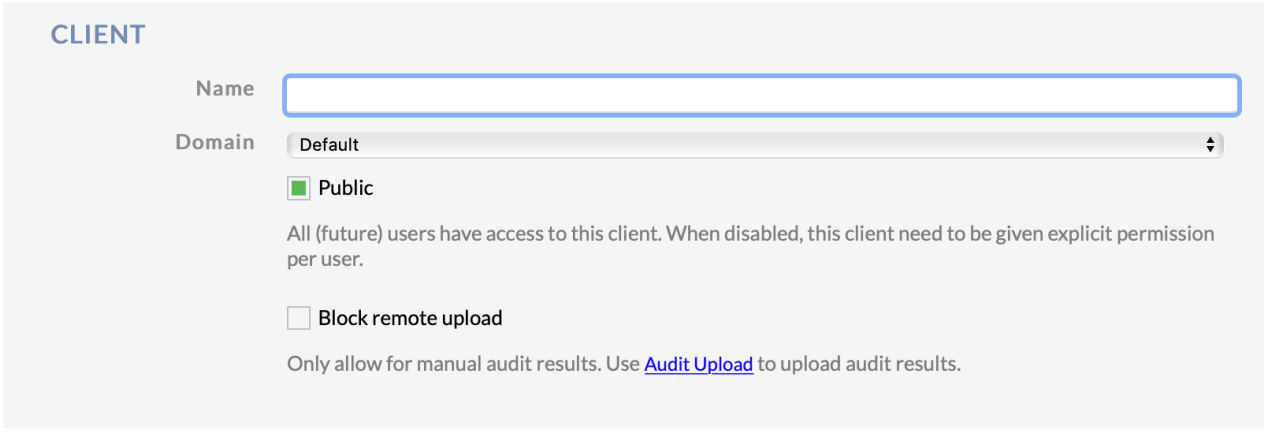


Menu: Accounts -> Clients

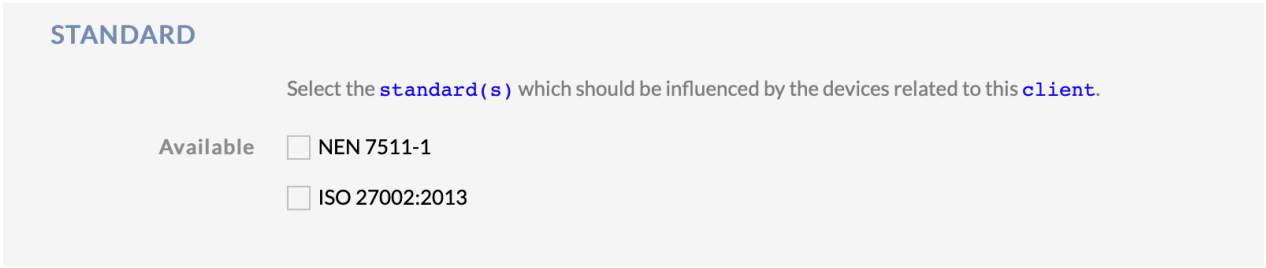
Via Accounts -> Clients krijgt u een overzicht van uw huidige clients. Een client is een groep systemen die binnen een domein (grotere groep) valt. U kunt uw clients per domein bekijken. Daarnaast kunt u via EDIT allerlei waarden aanpassen, deze komen overeen met de instellingen voor een nieuwe client aanmaken (zie ADD CLIENT hieronder). Via DELETE kunt u de client verwijderen.



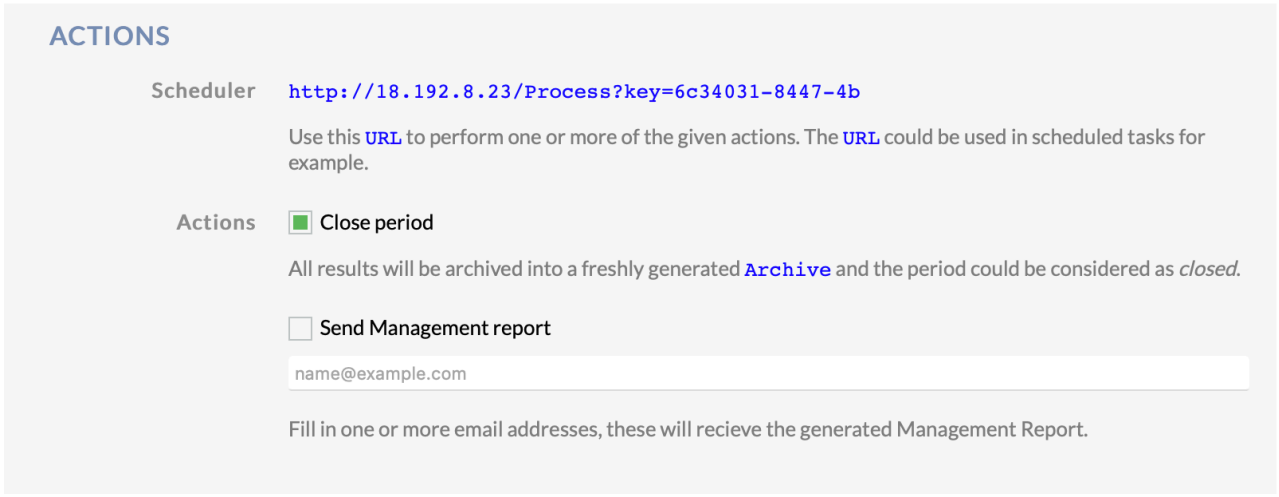
Via ADD CLIENT kunt u een nieuwe client toevoegen. Hier kunt u een flink aantal parameters instellen zoals hieronder beschreven. U kunt de client een naam geven en aangeven of deze client voor iedere user beschikbaar is. Voor uitzonderlijke gevallen kunt u het aangeven als audits alleen handmatig mogen worden uitgevoerd.



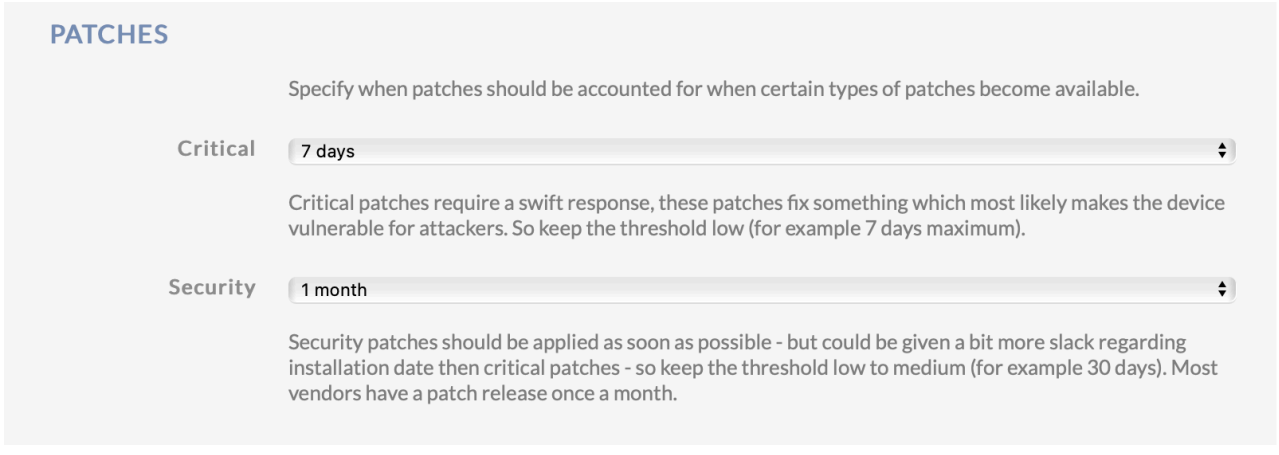
Als we verder naar onder scrollen kunnen we door middel van vinkjes aangeven welke standaarden moeten worden meegenomen voor deze client. Als u standaarden wilt zien die hier niet bij staan kunt u deze toevoegen via het menu: Options -> Update Standards. Als u hier op update klikt bij een standaard zal deze in onderstaand overzicht verschijnen.



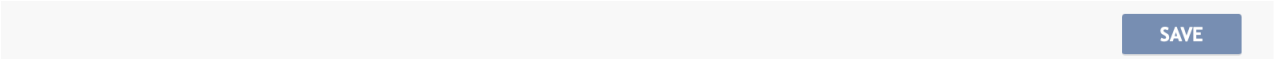
Onder het kopje actions vindt u een URL dat u kunt gebruiken om de taken die eronder staan geautomatiseerd uit te voeren: Het afsluiten van een periode, hiermee wordt een archief aangemaakt, en het sturen van een management rapportage naar één of meerdere email adressen. Als u meer email adressen wilt gebruiken, scheidt deze dan met een ; Voorbeeld: person1@company.com; person2@company.com.



Bij patches kunt u uw patchbeleid aangeven. Vul in binnen hoeveel tijd kritische en security patches geïnstalleerd moeten zijn om als compliant beschouwd te worden.

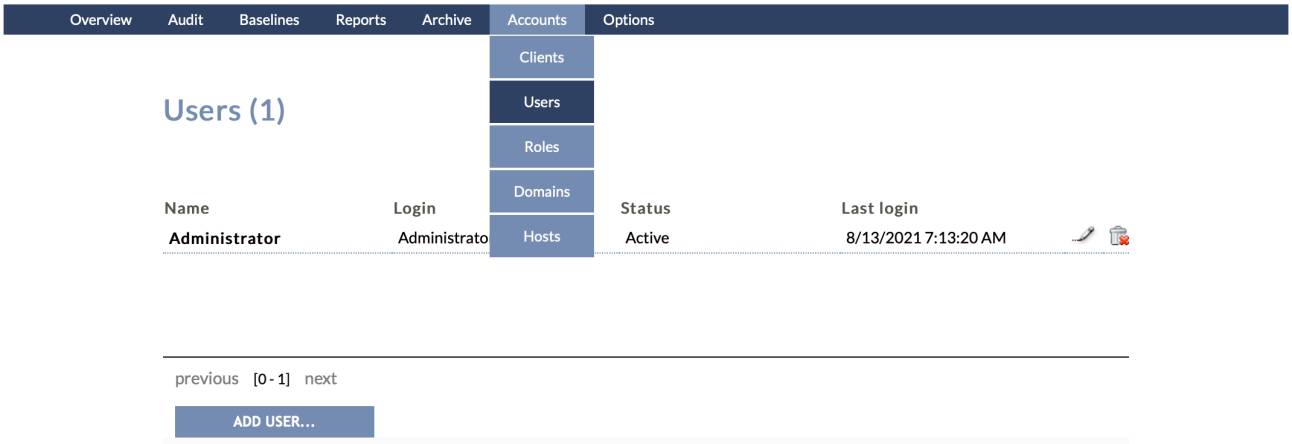


Als laatst op deze pagina: de SAVE knop. Waarmee u bovenstaande instellingen opslaat.

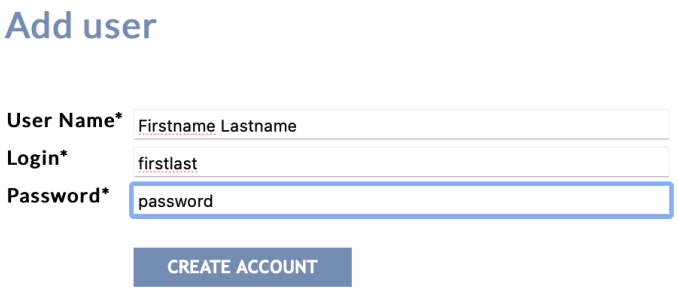


Menu: Accounts -> Users

In dit onderdeel van het menu kunt u gebruikers aan de applicatie toevoegen, aanpassen en verwijderen, en hen rechten toekennen.

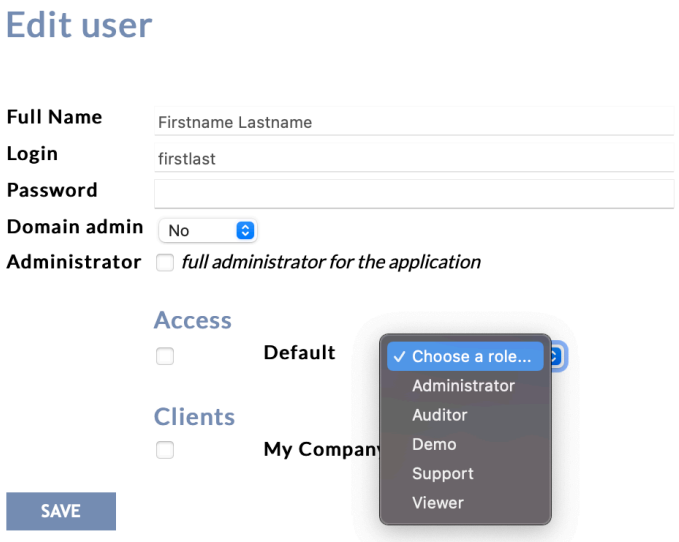


Het aanmaken van een gebruiker is heel eenvoudig. Klik op ADD USER… Vul een voor- en achternaam in, een gewenste gebruikersnaam en een wachtwoord. Klik op CREATE ACCOUNT.



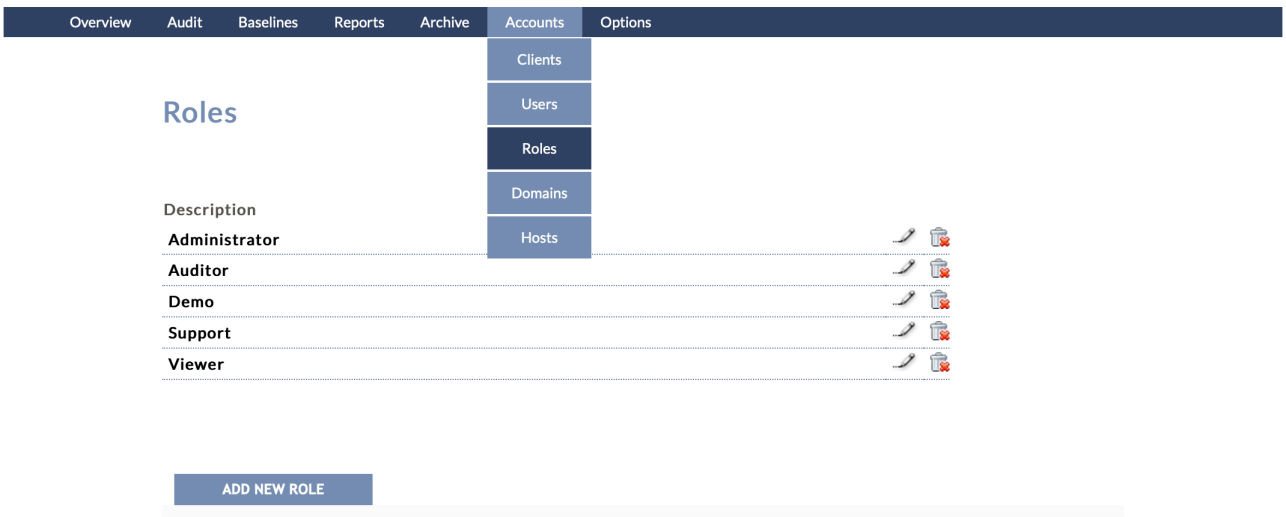
Daarna komt u automatisch op de edit user pagina. U kunt deze pagina ook bereiken door op het potloodje naast een gebruiker te klikken in het gebruikersoverzicht (menu: Accounts -> Users).

Hier kunt u aanpassingen maken aan de naam en gebruikersnaam van de user. Daarnaast kunt u aangeven of de gebruiker beheerder is van een domein of van de applicatie. Ook kunt u een rol toekennen per domein en aangeven of de gebruiker toegang heeft tot clients (die niet gekenmerkt zijn als public).

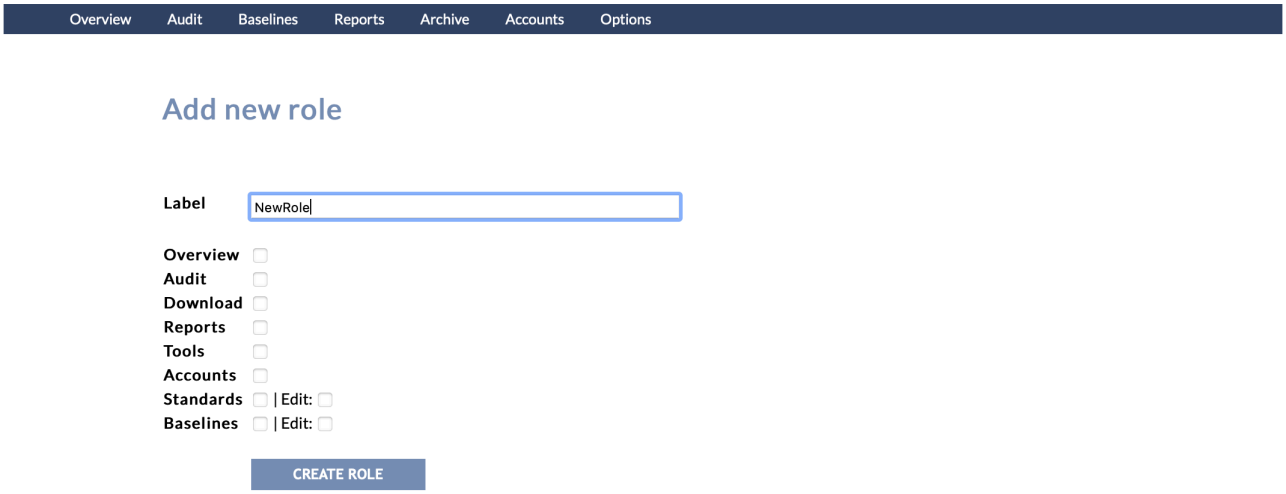


Menu: Accounts -> Roles

Onder roles kunt u de rollen definiëren die u aan uw users kunt toekennen (zie hierboven). U kunt nieuwe rollen toevoegen via de ADD NEW ROLE knop, of bestaande rollen wijzigen (potloodje) of verwijderen (prullenbakje).

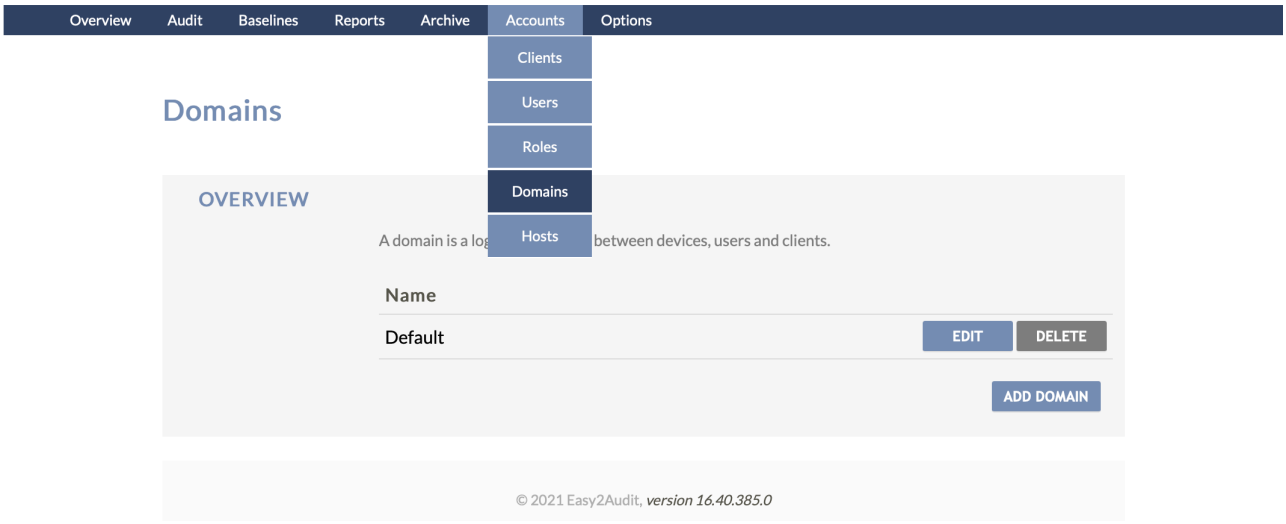


Als we een nieuwe rol aanmaken (of een bestaande rol wijzigen), kunnen we deze een naam geven, en aanvinken welke elementen van de applicatie in het menu getoond worden aan gebruikers met deze rol.



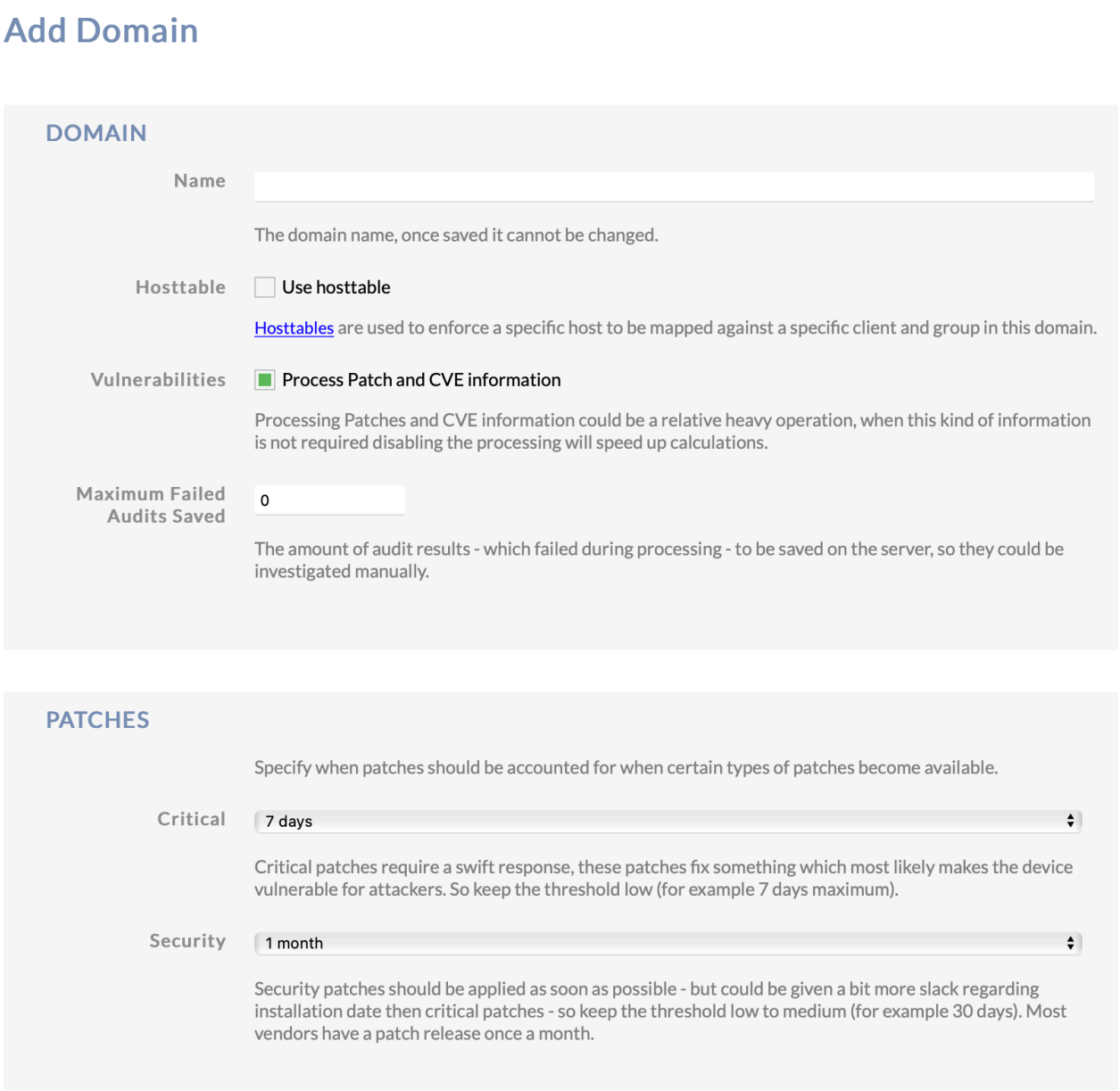
Menu: Accounts -> Domains

Hier kunt u domeinen toevoegen of aanpassen. Binnen een domein kunt u meerdere clients hebben, binnen die clients heeft u de hosts (systemen).



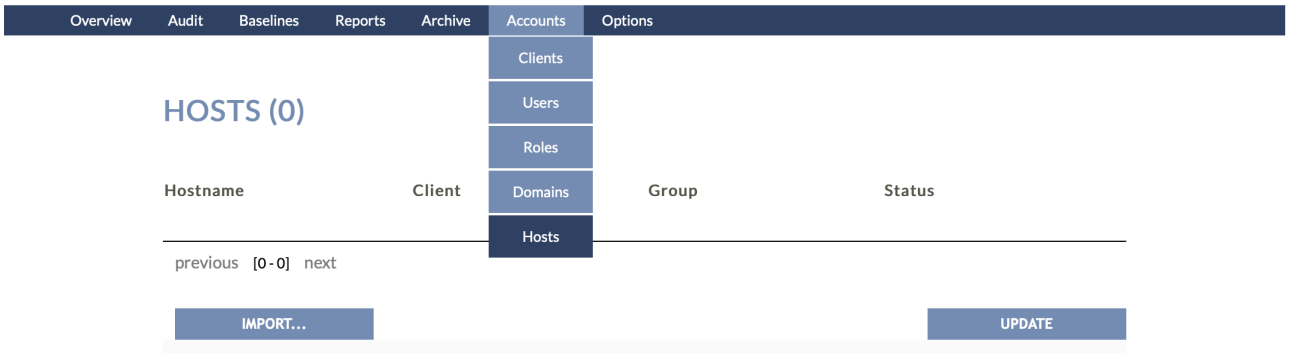
Wanneer u op EDIT of ADD DOMAIN klikt komt u in een volgend scherm. Hier kunt u een naam toevoegen of wijzigen en aangeven of u gebruikt wil maken van een host table (als dit zo is, dan weet u hiervan). U kunt kiezen om vulnerabilities wel of niet mee te nemen in audits en het maximaal aantal gefaalde audits dat bewaard wordt.

Eronder kunt u voor het domein aangeven binnen hoeveel dagen uw critica en security patches geïnstalleerd dienen te zijn om als compliant beschouwd te worden.



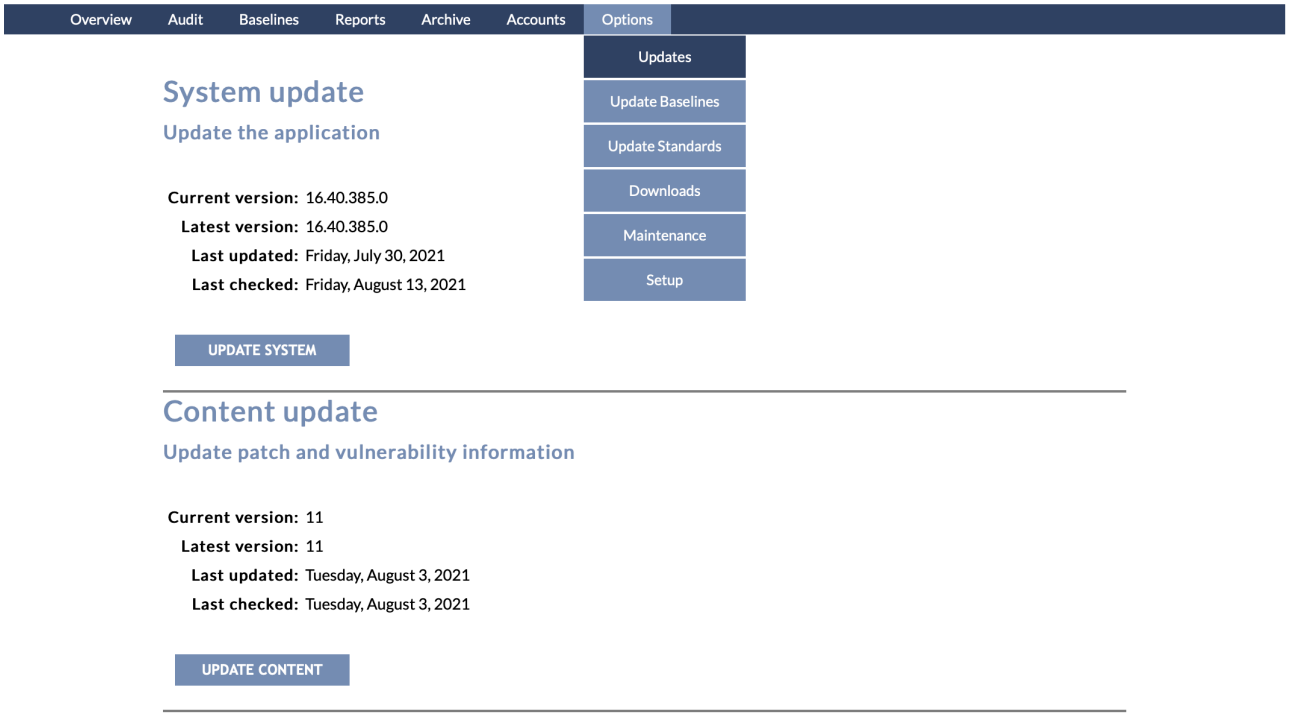
Menu: Accounts -> Hosts

Hier verschijnen uw hosts wanneer u gebruik maakt van een host table.



Menu: Options -> Updates

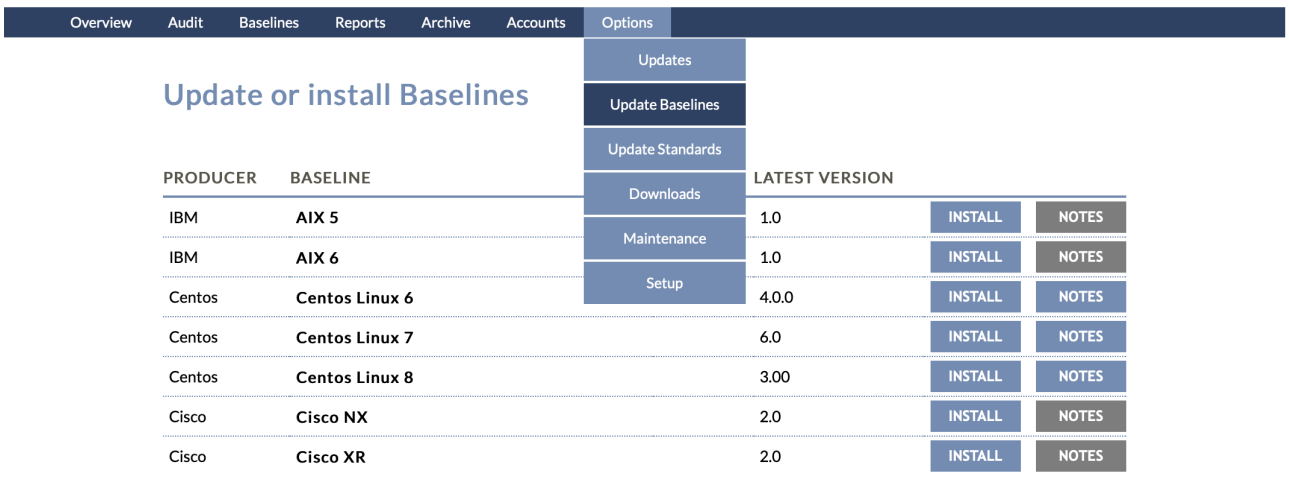
Op deze pagina kunt u zien of uw applicatie en uw content up-to-date zijn. Als dit niet het geval is kunt u hier gebruikmaken van de UPDATE SYSTEM en de UPDATE CONTENT knoppen.



Menu: Options -> Update Baselines

Hier vindt u een lijst met baselines die u kunt updaten of installeren door op de INSTALL knop te drukken. Als u dit heeft gedaan vindt u de bijbehorende scripts onder het menu: Baselines -> Download Scripts.

Via de NOTES knop kunt u notities bekijken die bij de baselines zijn gemaakt.



Menu: Options -> Update Standards

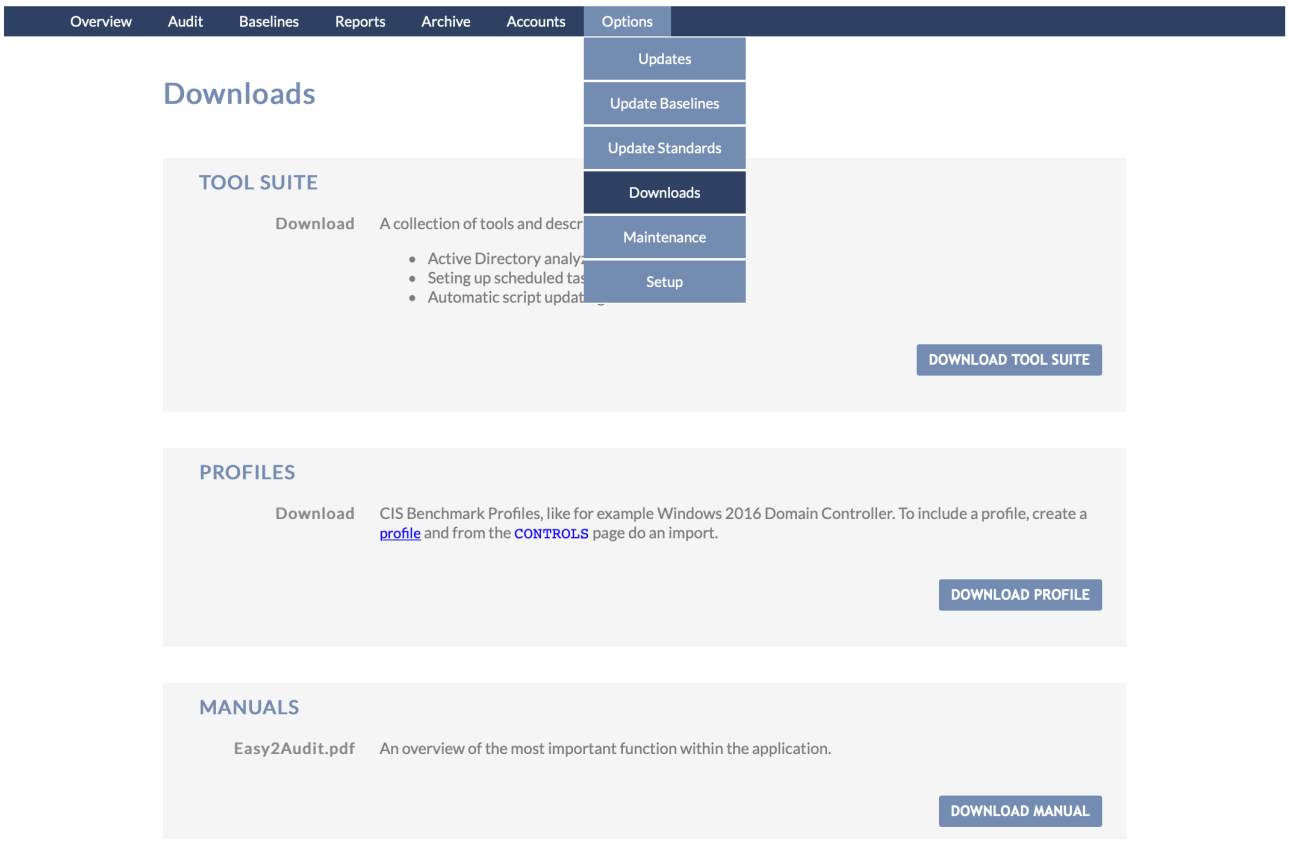
Hier kunt u standaarden toevoegen en updaten. Wanneer u op update klikt, zal de standaard worden toegevoegd. U kunt deze dan via het menu: Accounts -> Clients -> EDIT activeren, en daarna terugvinden in het dashboard.

Menu: Options -> Downloads

Hier vindt u verschillende downloads. Als u op DOWNLOAD TOOL SUITE klikt downloadt u een zip met een collectie van tools en beschrijvingen voor active directory analyses, het opzetten van geplande taken (scheduled tasks), en het automatisch updaten van scripts.

Via de DOWNLOAD PROFILE knop downloadt u alle profielen, deze kunt u weer in de applicatie importeren, als u hier gebruik van wilt maken. Kijk hiervoor in het menu: Baselines -> My profiles.

Via DOWNLOAD MANUAL downloadt u een Secquard handleiding waar u snel mee aan de slag kunt.

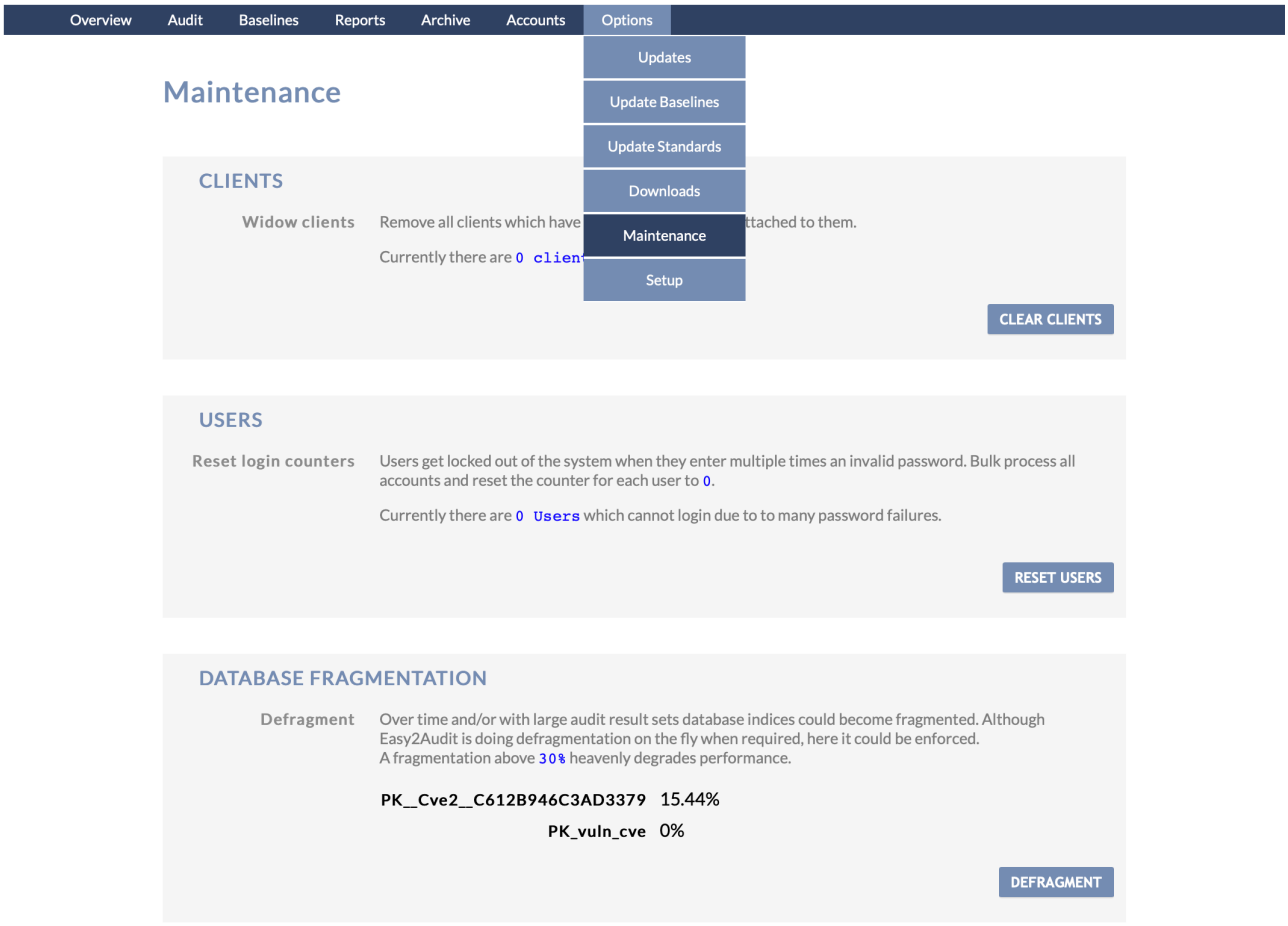


Menu: Options -> Maintenance

Op deze pagina kunt u een aantal onderhoudsinstellingen aanpassen. CLEAR CLIENTS zorgt ervoor dat alle clients zonder hosts/audits worden verwijderd.

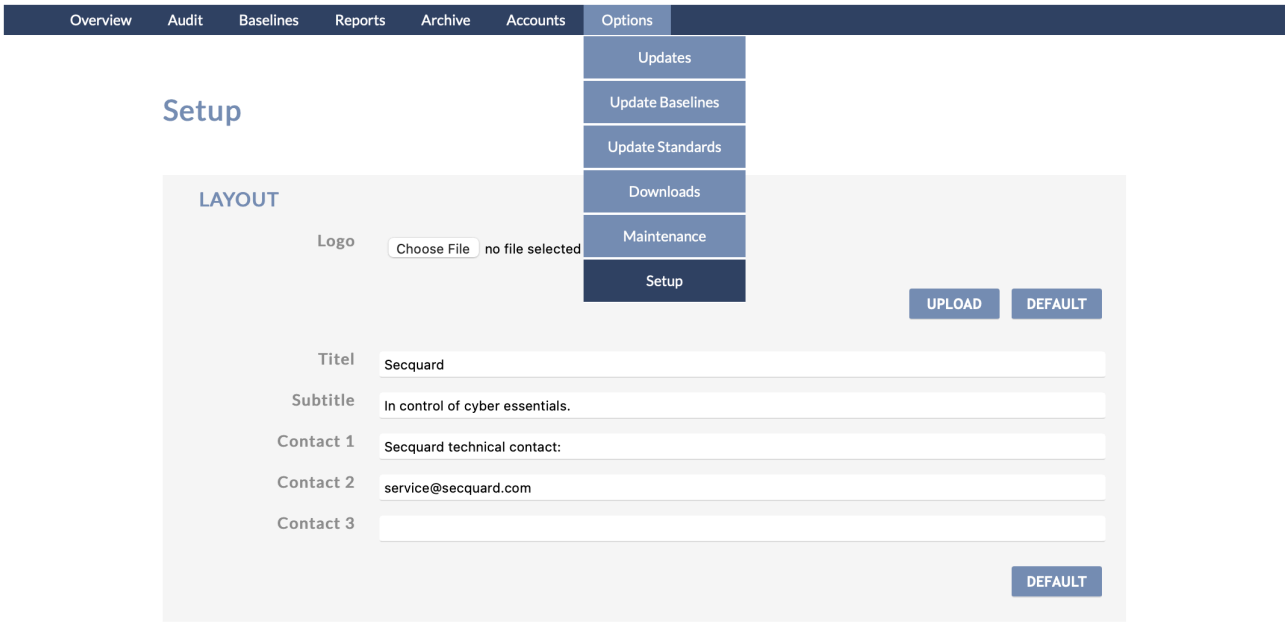
RESET USERS zorgt ervoor dat alle users die geen toegang meer hebben door het te vaak invoeren van een verkeerd wachtwoord weer kunnen proberen in te loggen in de applicatie.

Met de DEFRAGMENT knop, defragmenteert u de database.



Menu: Options -> Setup

Op deze pagina kunt u verschillende instellingen wijzigen. Zoals uw logo, de titel, subtitel en contactinformatie die worden weergegeven in de applicatie.



Daaronder kunt u een email server instellen. Als u niet weet hoe dit werkt, neem dan even contact op met uw systeembeheerder, hij of zij kan u hiermee verder helpen. U heeft deze instelling bijvoorbeeld nodig om geautomatiseerd management rapportages te versturen (zie voor meer informatie hierover