

Secquard Applicatie Gebruikers Handleiding



DISCLAIMER	3
Uitleg	3
1 Het instellen van de applicatie	4
1.1 Het selecteren van standaarden	4
1.2 Client en domains	4
1.2.1 Clients	5
1.2.2 Domains	7
1.3 Het aanmaken van gebruikers	9
1.4 Het definiëren van rollen	10
1.5 Het selecteren en/of aanpassen van profielen	11
2 Het gebruik van de applicatie	14
2.1 Dashboard	14
2.1.1 Standards	15
2.1.2 Hardening	17
2.1.3 Security patches	18
2.1.4 Vulnerabilities	19
2.1.5 Antivirus	21
2.1.6 Administrators	22

DISCLAIMER

De Secquard applicatie biedt onder voorbehoud van fouten een zo volledig mogelijk overzicht van een aantal onderwerpen van alle aangesloten systemen: Hardening, patching & vulnerabilities, anti-virus en active directory. Wij willen u er op wijzen dat niet alle instellingen automatisch controleerbaar zijn en daardoor niet meegenomen worden in de applicatie.

Uitleg

In deze handleiding bespreken wij een aantal stappen die u zo snel mogelijk op weg helpen met de Secquard applicatie. Deze handleiding sluit aan op de installatie handleiding, en gaat er daarom vanuit dat de stappen die daarin worden beschreven reeds zijn doorlopen. Voor een uitgebreid overzicht van alle pagina's van de Secquard applicatie kunt u gebruik maken van de Secquard referentie handleiding.

1 Het instellen van de applicatie

Voordat u de applicatie echt goed kunt gebruiken raden wij aan om de volgende stappen zorgvuldig te doorlopen.

1.1 Het selecteren van standaarden

De kans is aanwezig dat u Secquard gebruikt om uw compliance met een of meerdere standaarden wilt aantonen. Om de compliance met uw gewenste standaard(en) weer te geven, doorloopt u de volgende stappen:

Ga naar het menu: Options -> Update Standards. Hier kunt u standaarden toevoegen en updaten. Wanneer u op update klikt, zal de standaard worden toegevoegd of geüpdatet.

STANDARD	CURRENT	LATEST VERSION	
ISO 17799:2005 Automated controls	0	1	
CIS Controls V7.1	0	2	
CIS Critical Security Controls	0	4	update
BIC V3.0 (2019)	0	1	update
ISO/IEC 27002:2013 (Automated controls)	0	1	update
NIST 800-53 rev4	0	1	update
Quick Scan	0	1	update
E2A Quick Scan	0	2	update
ISO 27002:2005	0	1	update
NEN 7510-2:2017	0	2	update
UK Cyber Essentials	0	1	update
PCI DSS 3.0	0	3	update
NIST 800-171	0	2	update
BIR	0	1	update
COBIT 5	0	2	update
BIO 1.04	0	3	update

Om de standaard daad werkelijk te activeren gaat u via het menu: Accounts -> Clients -> EDIT activeren, en daarna terugvinden in het dashboard. Zie ook de volgende paragraaf.

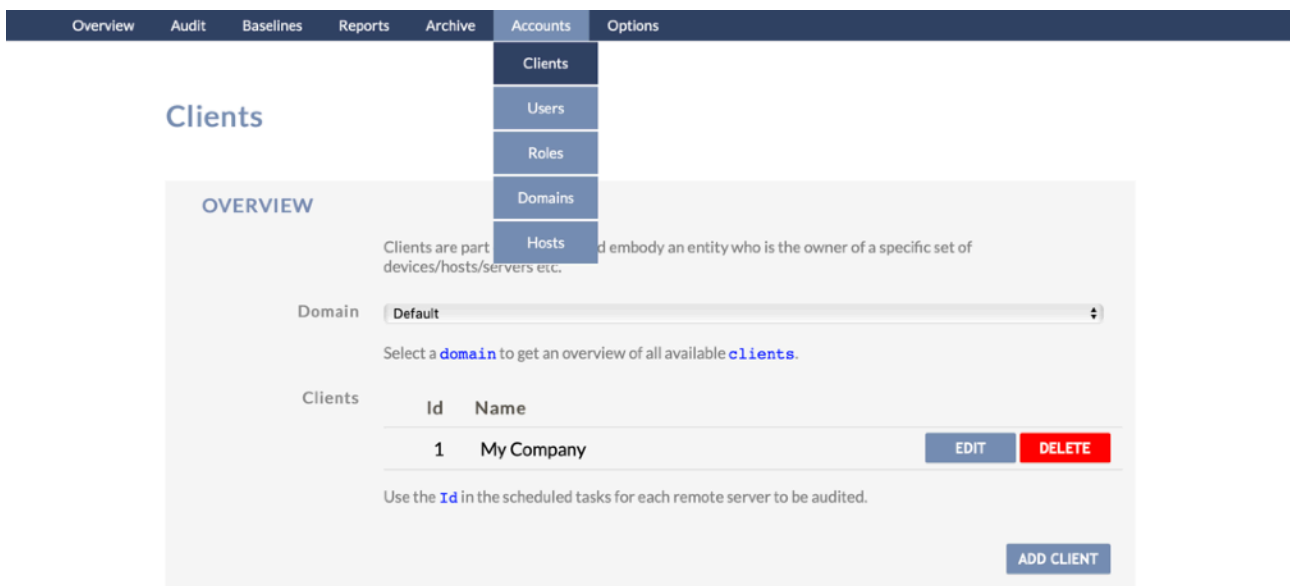
1.2 Client en domains

Voor veel gebruikers van de Secquard applicatie is het niet noodzakelijk om clients en/of domains aan te maken, maar voor sommige organisaties kan dit een zeer handig optie zijn. Clients zijn groepen van systemen en domains zijn groepen van clients. U kunt er bijvoorbeeld voor kiezen om uw Linux en Windows machines onder verschillende clients te verdelen en deze weer onder te brengen in een productie- en een testdomein. Voor MSP's (managed services providers) kan het handig zijn om systemen van iedere klant in

een eigen client in te delen. Of en hoe u van deze functionaliteit gebruik maakt, laten wij graag aan u over.

1.2.1 Clients

Via het menu: Accounts -> Clients krijgt u een overzicht van uw huidige clients. 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.



Overview Audit Baselines Reports Archive Accounts Options

Clients

Users

Roles

Domains

Hosts

Clients

OVERVIEW

Clients are part of an account and embody an entity who is the owner of a specific set of devices/hosts/servers etc.

Domain:

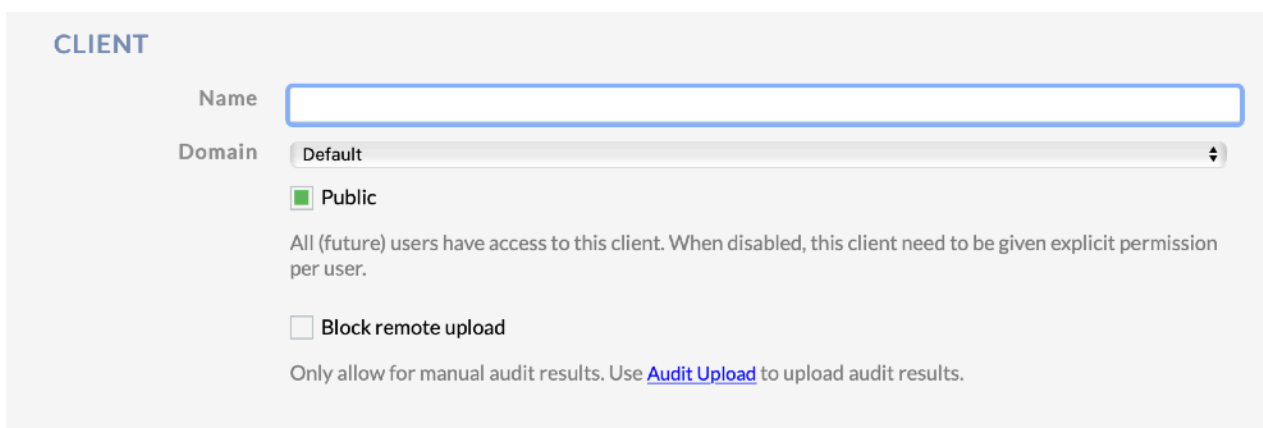
Select a **domain** to get an overview of all available **clients**.

Clients	Id	Name		
	1	My Company	EDIT	DELETE

Use the **Id** in the scheduled tasks for each remote server to be audited.

ADD CLIENT

Via EDIT of ADD CLIENT kunt u een bestaande client aanpassen of een nieuwe 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.



CLIENT

Name:

Domain:

Public

All (future) users have access to this client. When disabled, this client need to be given explicit permission per user.

Block remote upload

Only allow for manual audit results. Use [Audit Upload](#) to upload audit results.

Als we verder naar onder scrollen kunnen we door middel van vinkjes aangeven welke standaarden moeten worden meegenomen voor deze client. Mist u een standaard? Zie vorige paragraaf.

STANDARD

Select the **standard(s)** which should be influenced by the devices related to this **client**.

- Available NEN 7511-1
 ISO 27002:2013

Het onderdeel actions is bij de installatie van de applicatie behandeld.

ACTIONS

Scheduler <http://18.192.8.23/Process?key=6c34031-8447-4b>

Use this **URL** to perform one or more of the given actions. The **URL** could be used in scheduled tasks for example.

Actions Close period

All results will be archived into a freshly generated **Archive** and the period could be considered as *closed*.

Send Management report

Fill in one or more email addresses, these will receive the generated Management Report.

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.

PATCHES

Specify when patches should be accounted for when certain types of patches become available.

Critical

Critical patches require a swift response, these patches fix something which most likely makes the device vulnerable for attackers. So keep the threshold low (for example 7 days maximum).

Security

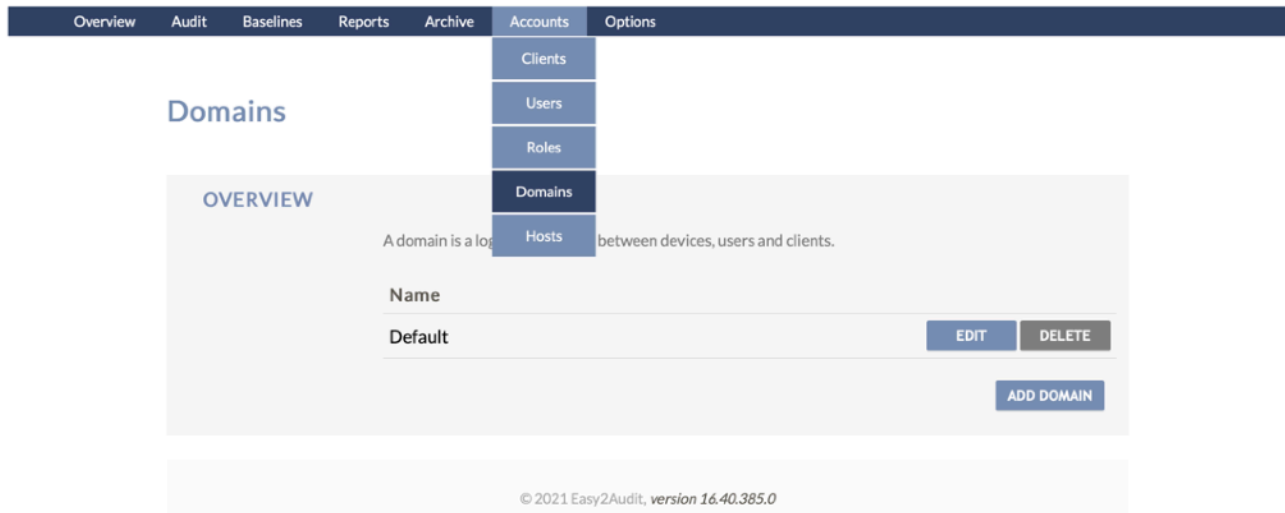
Security patches should be applied as soon as possible - but could be given a bit more slack regarding installation date then critical patches - so keep the threshold low to medium (for example 30 days). Most vendors have a patch release once a month.

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

SAVE

1.2.2 Domains

Via het menu: Accounts -> Domains kunt u domeinen toevoegen of aanpassen. Binnen een domein kunt u meerdere clients hebben, binnen die clients kun u verschillende hosts hebben (systemen).



The screenshot shows the 'Accounts' menu with 'Domains' selected. The 'OVERVIEW' section contains a description: 'A domain is a logical relationship between devices, users and clients.' Below this is a table with one row: 'Name' with the value 'Default'. To the right of the 'Default' value are 'EDIT' and 'DELETE' buttons. At the bottom right of the overview section is an 'ADD DOMAIN' button. The footer of the page reads '© 2021 Easy2Audit, version 16.40.385.0'.

Wanneer u op EDIT of ADD DOMAIN klikt, 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 critical en security patches geïnstalleerd dienen te zijn om als compliant beschouwd te worden. Als u zowel bij domains als clients een beleid heeft, is dat van clients leidend.

Add Domain

DOMAIN

Name

The domain name, once saved it cannot be changed.

Hosttable Use hosttable

[Hosttables](#) are used to enforce a specific host to be mapped against a specific client and group in this domain.

Vulnerabilities Process Patch and CVE information

Processing Patches and CVE information could be a relative heavy operation, when this kind of information is not required disabling the processing will speed up calculations.

Maximum Failed Audits Saved

The amount of audit results - which failed during processing - to be saved on the server, so they could be investigated manually.

PATCHES

Specify when patches should be accounted for when certain types of patches become available.

Critical

Critical patches require a swift response, these patches fix something which most likely makes the device vulnerable for attackers. So keep the threshold low (for example 7 days maximum).

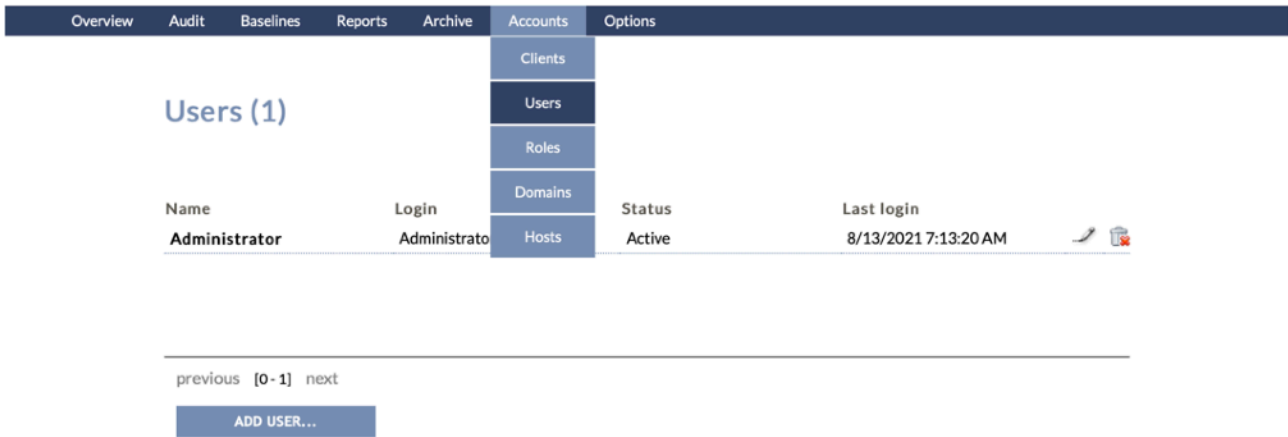
Security

Security patches should be applied as soon as possible - but could be given a bit more slack regarding installation date then critical patches - so keep the threshold low to medium (for example 30 days). Most vendors have a patch release once a month.

1.3 Het aanmaken van gebruikers

Via het menu Menu: Accounts -> Users

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



The screenshot shows the 'Accounts' menu with sub-items: Clients, Users, Roles, Domains, and Hosts. The 'Users' sub-item is selected, displaying a table with one user: Administrator. The table has columns for Name, Login, Status, and Last login. Below the table are navigation links 'previous [0-1] next' and an 'ADD USER...' button.

Name	Login	Status	Last login
Administrator	Administrato	Active	8/13/2021 7:13:20 AM

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.

Add user

User Name*


Login*

Password*

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.

Edit user

Full Name
Login
Password
Domain admin No 
Administrator full administrator for the application

Access
 Default



Clients
 My Company

✓ Choose a role...
 Administrator
 Auditor
 Demo
 Support
 Viewer

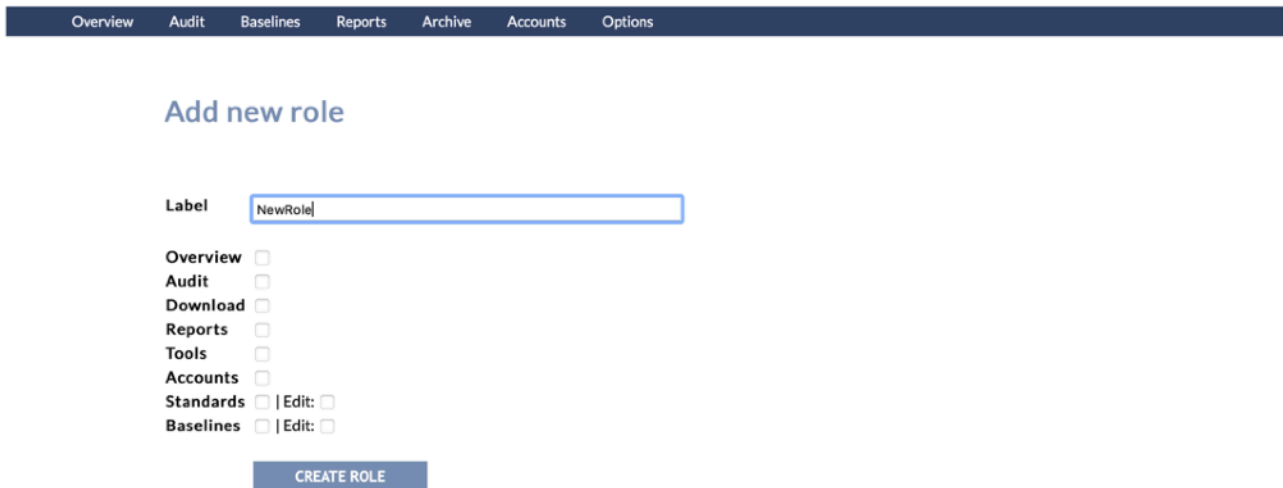
1.4 Het definiëren van rollen

Om zo veilig mogelijk gebruik te maken van de Secquard applicatie raden wij u aan om rollen te creëren voor (groepen van) gebruikers. Door de rechten van iedere rol te beperken tot het strikt noodzakelijke, kunt u misbruik voorkomen. Zorg er wel voor dat u per gebruiker de juiste rol toekent, zodat deze ook niet te weinig rechten heeft om zijn/haar taken juist uit te voeren.

Ga naar het menu: Accounts -> Roles om de rollen te definiëren. U kunt nieuwe rollen toevoegen via de ADD NEW ROLE knop, of bestaande rollen wijzigen (potloodje) of verwijderen (prullenbakje).

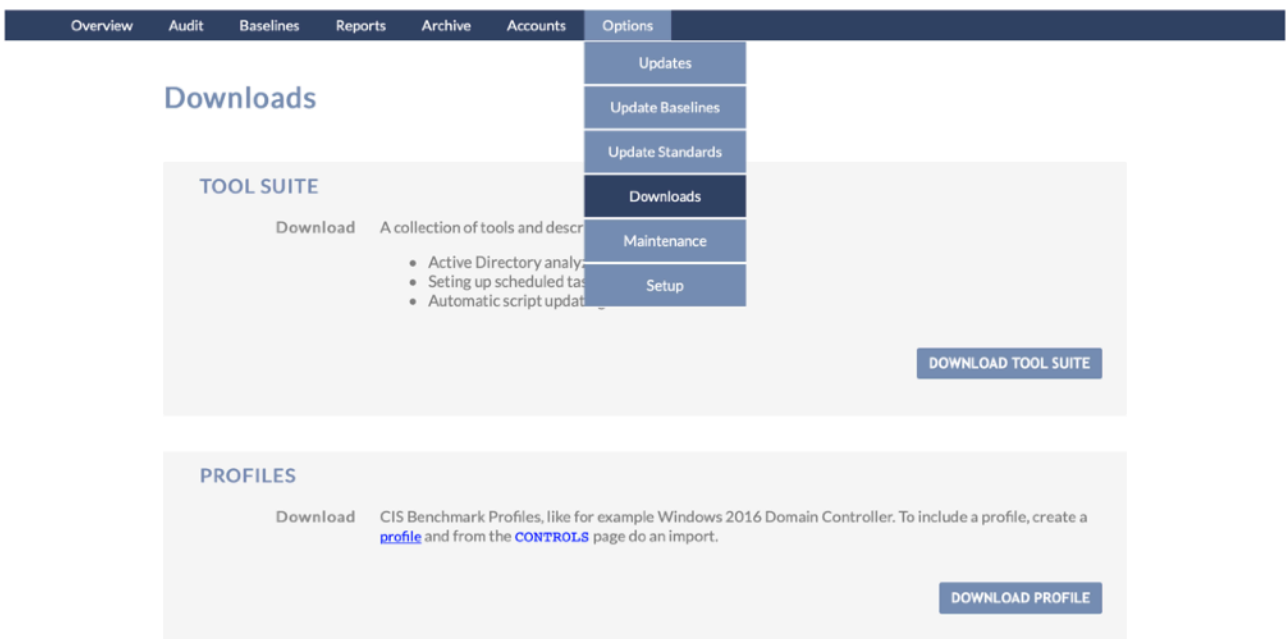
Overview		Audit		Baselines		Reports		Archive		Accounts		Options	
										Clients			
										Users			
										Roles			
										Domains			
										Hosts			
Roles													
Description													
Administrator												 	
Auditor												 	
Demo												 	
Support												 	
Viewer												 	
<input type="button" value="ADD NEW ROLE"/>													

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.

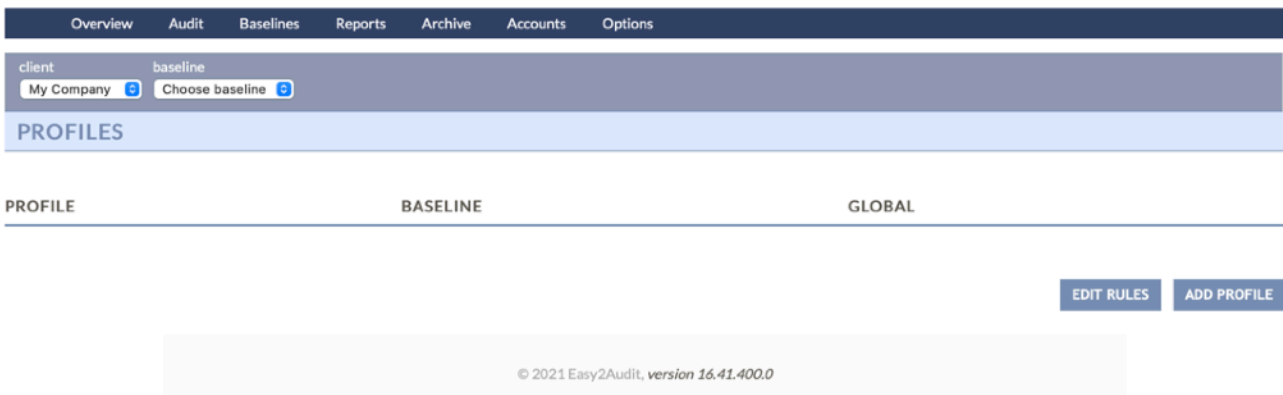


1.5 Het selecteren en/of aanpassen van profielen

In de Secquard applicatie kunt u ervoor kiezen om profielen te gebruiken. Een profiel is een set met regels die ervoor zorgen dat bepaalde controls wel of niet worden meegenomen in een audit. Standaard worden in de Secquard applicatie alle beschikbare controls van een systeem meegenomen in audits. Met een CIS L1 (level 1) profiel bijvoorbeeld worden minder controls meegenomen dan met een CIS L2 profiel. Dit kan voor een hogere score zorgen met dezelfde instellingen. Het is belangrijk dat u de juiste profielen kiest voor de juiste systemen. Ga naar het menu: Options -> Downloads en klik op DOWNLOAD PROFILE om de profielen te downloaden.



Ga vervolgens naar het menu: Baselines -> My profiles. Klik op ADD PROFILE om een profiel toe te voegen.



Kies een baseline uit voor het profiel dat u wilt gebruiken en geef het een herkenbare naam, bijvoorbeeld: Windows Server 2019 CIS L1. Geef aan of u het profiel wilt delen onder alle clients. Druk op SAVE om de instellingen op te slaan.

Add Profile

PROFILE

A profile is based on a **Baseline**, but where a **Baseline** doesn't allow for any changes; a **Profile** allows for controls to be turned off or change the measured value to which a control is being validated against.

Baseline

Client

Name

Description

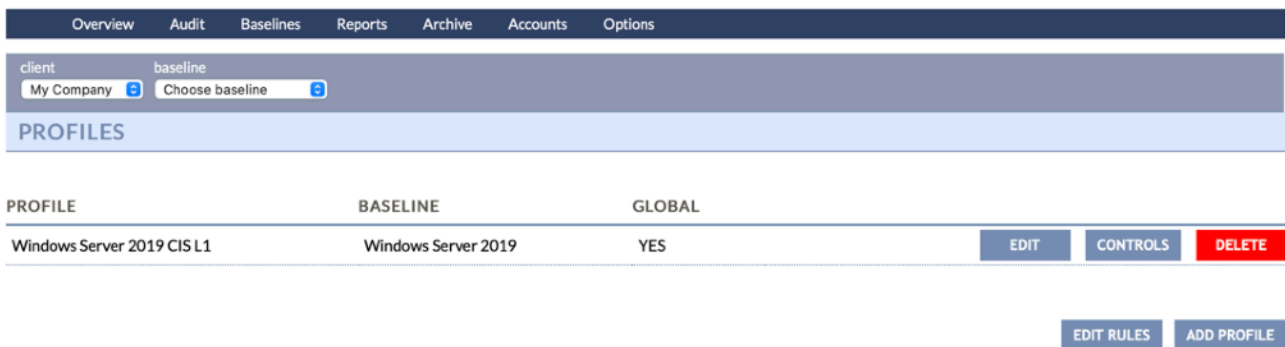
Global Global Profile

A **Global** profile is shared amongst all clients. Whereas a **Private** profile is only available for the selected **client**.

Auto

Order

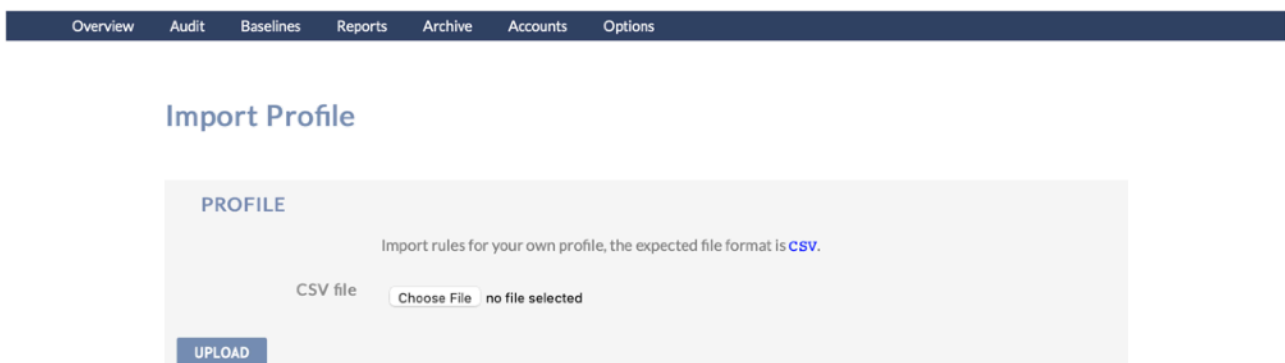
U keert nu terug naar het overzicht My profiles.



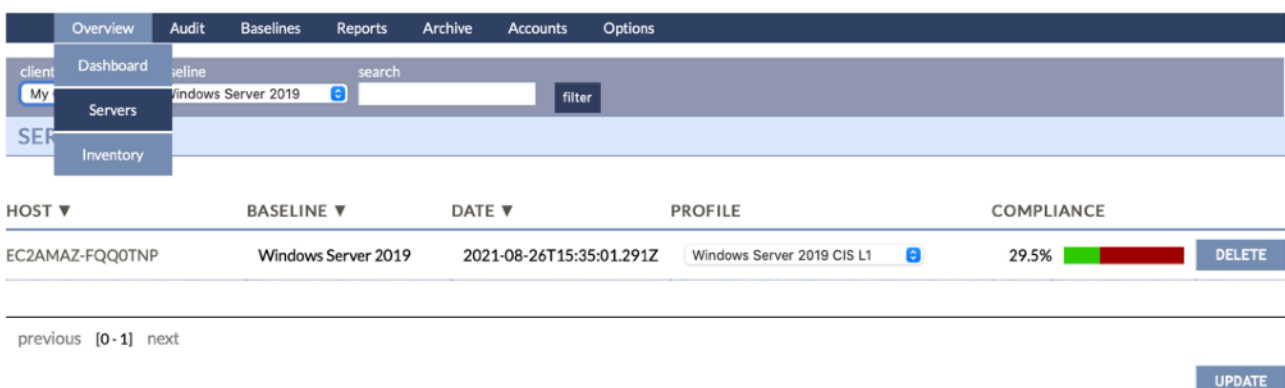
PROFILE	BASELINE	GLOBAL	
Windows Server 2019 CIS L1	Windows Server 2019	YES	EDIT CONTROLS DELETE


Klik op CONTROLS. U 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. Importeer hier het juiste profiel via IMPORT.

Klik op Choose File en navigeer naar uw downloads folder. Navigeer nu naar profiles en naar de map die het juiste OS weergeeft. In ons geval is dit Windows Server 2019. Hier kiest u het gewenste profiel. Wij kiezen voor een CIS L1 (level 1) MS (member server). Klik vervolgens op UPLOAD en daarna op CONTINUE en daarna op RECALC om compliance scores opnieuw te berekenen.



Als u nu naar het menu: Overview -> Servers gaat kunt u bij uw gekozen baseline het geïnstalleerde profiel selecteren. Klik daarna op UPDATE. En navigeer terug naar het algemeen dashboard. Hier zult u zien dat uw coulance score is aangepast aan het profiel dat u heeft geïnstalleerd.



HOST	BASELINE	DATE	PROFILE	COMPLIANCE	
EC2AMAZ-FQ0TNP	Windows Server 2019	2021-08-26T15:35:01.291Z	Windows Server 2019 CIS L1	29.5%	 DELETE

2 Het gebruik van de applicatie

Als u bovenstaande hoofdstukken heeft doorlopen is alles gereed voor gebruik. Daarover in dit hoofdstuk wat meer informatie. Een uitgebreid overzicht van alle pagina's van de Secquard applicatie kunt u vinden in de Secquard referentie handleiding. In het huidige hoofdstuk bieden wij u een snel overzicht van belangrijke overzichten.

2.1 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. Ook kunt u bovenaan de pagina filters instellen voor clients en baselines, en een archief selecteren om de huidige audit scores mee te vergelijken.

Overview Audit Baselines Reports Archive Accounts Options													
client		baseline		archive									
My Company		Windows Server 2019		2021 Week 32									
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		Current				Previous audit			Realization				
Baselines 1		Hosts	Level			Hosts	Level		Hosts	Variance			
Windows Server 2019		1	24.4%			1	24.4%			0	0%		
Security Patches													
Hosts 1		Current				Previous audit			Realization				
Baselines 1		NOT			NOT			NOT					
		Hosts	Compliant	Compliant		Hosts	Compliant	Compliant		Hosts	Compliant	Compliant	
Windows Server 2019		1	1			1	1			0	0	0	
Vulnerabilities													
Hosts 1		Current				Previous audit			Realization				
Baselines 1		Total	CVE's			Affected	Total	CVE's			Affected		
		hosts	C	H	M	hosts	hosts	C	H	M	hosts		
Windows Server 2019		1	3	21		1	1	3	21		0		
Anti-virus													
Hosts 1		Current				Previous audit			Realization				
Baselines 1		NOT			NOT			NOT					
		Compliant	Compliant	Installed		Compliant	Compliant	Installed		Compliant	Compliant	Installed	
Windows Server 2019		1				1				1			
Administrators													
Hosts 2		Current				Previous audit			Differ				
Domains 1		Enterprise	Domain		Users	Enterprise	Domain		Users	Enterprise	Domain		
Windows 2012 R2 - patched		1	1		828	1	1		828	1	828		

2.1.1 Standards

Onder standards staan standaards die u zelf heeft uitgekozen. 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.

Overview Audit Baselines Reports Archive Accounts Options

client: My Company | baseline: Windows Server 2019 | archive: 2021 Week 32

Standards

Hosts	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%	

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.

Overview Audit Baselines Reports Archive Accounts Options

Standard: BIO 1.04
Client: My Company
Compliance: 26.38%
301 of 1141 successfully passed

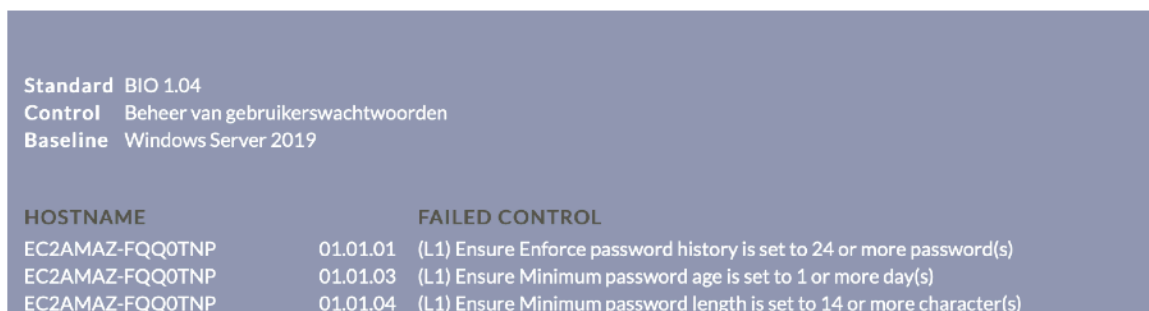
- ✚ 08 Beheer van bedrijfsmiddelen 28%
- ✚ 09 Toegangsbeveiliging 34%
 - ✚ 09.01 Bedrijfsbeheer ten aanzien van toegangsbeheersing 30%
 - ✚ 09.02 Beheer van toegangsrechten van gebruikers 33%
 - 09.02.01 Registratie en afmelden van gebruikers 28%
 - 09.02.02 Gebruikers toegang verlenen 36%
 - 09.02.03 Beheer van speciale bevoegdheden 36%
 - 09.02.04 Beheer van gebruikerswachtwoorden 36%
 - 09.02.05 Beoordeling van toegangsrechten van gebruikers 36%
 - 09.02.06 Blokkering van toegangsrechten 36%
 - ✚ 09.03 Verantwoordelijkheden van gebruikers 41%
 - ✚ 09.04 Toegangsbeheersing voor informatiesystemen en informatie 27%
- ✚ 10 Cryptografie 8%
- ✚ 12 Beveiliging bedrijfsvoering 14%
- ✚ 13 Communicatiebeveiliging 15%
- ✚ 14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen 23%
- ✚ 18 Naleving

RECALC

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.



Standard	BIO 1.04	
Control	Beheer van gebruikerswachtwoorden	
Baseline	Windows Server 2019	
	HOSTNAME	FAILED CONTROL
	EC2AMAZ-FQQ0TNP	01.01.01 (L1) Ensure Enforce password history is set to 24 or more password(s)
	EC2AMAZ-FQQ0TNP	01.01.03 (L1) Ensure Minimum password age is set to 1 or more day(s)
	EC2AMAZ-FQQ0TNP	01.01.04 (L1) Ensure Minimum password length is set to 14 or more character(s)

2.1.2 Hardening

Onder het kopje hardening vindt u een overzicht van alle systemen. In de huidige audit (current) scoort dit systeem 24.4% compliance (ten opzichte van de CIS benchmark).

Hardening

Hosts	1	Current	Previous audit	Realization	
Baselines	1	Hosts	Level	Hosts	Variance
Windows Server 2019		1 24.4%	1 24.4%	0 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 uitgeklaapt door op het plusje te klikken.

client
baseline

My Company
Windows Server 2019

BASELINE

Baseline: Windows Server 2019
Hosts: 1

Expand all controls

- 01 Account Policies
 - 01.01 Password Policy
 - 01.01.01 (L1) Ensure Enforce password history is set to 24 or more password(s) 33%
 - 01.01.02 (L1) Ensure Maximum password age is set to 60 or fewer days, but not 0 50%
 - 01.01.03 (L1) Ensure Minimum password age is set to 1 or more day(s) 0%
 - 01.01.04 (L1) Ensure Minimum password length is set to 14 or more character(s) 100%
 - 01.01.05 (L1) Ensure Password must meet complexity requirements is set to Enabled 0%
 - 01.01.06 (L1) Ensure Store passwords using reversible encryption is set to Disabled 0%
 - 01.02 Account Lockout Policy 100%
- 02 Local Policies 0%
- 09 Windows Firewall With Advanced Security 53%
- 17 Advanced Audit Policy Configuration 15%
- 18 Administrative Templates (Computer) 29%
- 19 Administrative Templates (User) 2%

RECALC ALL SERVERS

Wanneer wij op een control klikken krijgen wij een pop-up, met een lijst van servers en of deze wel of niet compliant zijn.

Baseline: Windows Server 2019
Control: (L1) Ensure Minimum password length is set to 14 or more character(s)
Description: This policy setting determines the least number of characters that make up a password for a user account. There are many different theories about how to determine the best password length for an organization, but perhaps "pass phrase" is a better term than "password." In Microsoft Windows 2000 or later, pass phrases can be quite long and can include spaces. Therefore, a phrase such as "I want to drink a \$5 milkshake" is a valid pass phrase; it is a considerably stronger password than an 8 or 10 character string of random numbers and letters, and yet is easier to remember. Users must be educated about the proper selection and maintenance of passwords, especially with regard to password length. In enterprise environments, the ideal value for the Minimum password length setting is 14 characters, however you should adjust this value to meet your organization's business requirements. The recommended state for this setting is: 14 or more character(s).

Servers (1)

Client	Hostname	Score
My Company	EC2AMAZ-FQQ0TNP	FAILED

2.1.3 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.

Security Patches

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

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.

client: My Company | baseline: Windows Server 2019 | Status: All hosts | Host name: | filter

PATCHES (1 SERVERS)

HOST	BASELINE	LAST UPLOAD	IMPORTANT PATCHES	CRITICAL PATCHES	PATCH AGE	
EC2AMAZ-FQQ0TNP	Windows Server 2019	2021-07-21T10:45:51.443Z	Compliant	Compliant	42 days	details

previous [0-1] next

Wanneer we op de naam van de host klikken, of op details, komen we bij het volgende scherm. Hier zien we o.a. een lijst met geïnstalleerde patches.

« Back

PATCH INFORMATION

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

Patch Level: Compliant
 Patch age: 42 days
Last installed patch before audit date

Installed

890830 - Tuesday, June 8, 2021
 890830 - Tuesday, June 8, 2021
 5003778 - Tuesday, June 8, 2021
 890830 - Tuesday, May 11, 2021
 890830 - Tuesday, May 11, 2021
 890830 - Tuesday, April 13, 2021
 890830 - Tuesday, March 9, 2021
 890830 - Tuesday, March 9, 2021
 4589208 - Tuesday, March 9, 2021
 4577586 - Tuesday, February 16, 2021
 890830 - Tuesday, January 12, 2021
 4535680 - Tuesday, January 12, 2021

2.1.4 Vulnerabilities

Terug naar het dashboard, zien we bij de vulnerabilities hoeveel vulnerabilities (CVE's) er zijn gevonden op de volgende niveaus: Critical, High, en Medium.

Vulnerabilities

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

Wanneer we doorklikken door op de baseline te klikken komen we in het volgende scherm.

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. 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		

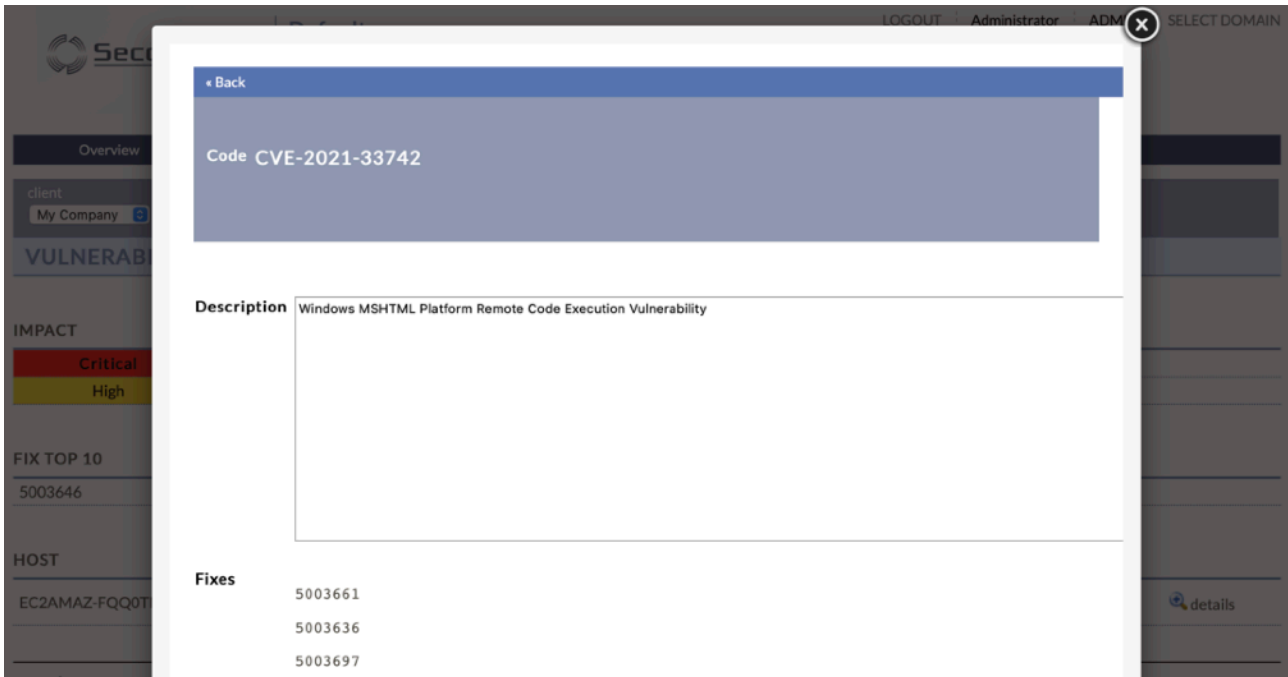
HOST	BASILINE	LAST UPLOAD	CRITICAL	HIGH	MEDIUM	LOW	NONE	STATUS	
EC2AMAZ-FQQ0TNP	Windows Server 2019	2021-07-21T10:45:51.443Z	3	21	0	0	0	24 found	details

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.

HOSTNAME	CVE	DESCRIPTION	Info...
EC2AMAZ-FQQ0TNP	CVE-2021-33742	Windows MSHTML Platform Remote Code Execution Vulnerability	Info...
EC2AMAZ-FQQ0TNP	CVE-2021-31959	Scripting Engine Memory Corruption Vulnerability	Info...
EC2AMAZ-FQQ0TNP	CVE-2021-1675	Windows Print Spooler Elevation of Privilege Vulnerability	Info...

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		baseline						
My Company		Windows Server 2019						
VULNERABILITIES								
IMPACT	HOSTS	VULNERABILITIES						
Critical	1	3						
High	1	21						
FIX TOP 10	HOSTS	CRITICAL	HIGH					
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

previous [0 - 1] next

2.1.5 Antivirus

Terug op het dashboard zien we het hoofdstuk anti-virus. Hier ziet u een overzicht van de baselines en daarbij behorende hosts, en hoeveel van deze hosts wel en niet compliant zijn.

Anti-virus

Hosts	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			1					

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.

client: My Company | baseline: Windows Server 2019 | Status: All hosts | | filter

ANTI VIRUS (1)

HOST	BASELINE	LAST UPLOAD	INSTALLED	ENGINE	DATABASE	
EC2AMAZ-FQQ0TNP	Windows Server 2019	2021-07-21T10:45:51.443Z	Installed	Compliant	Compliant	details

previous [0-1] next

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).

ANTI VIRUS INFORMATION

Server Windows Server 2019 : EC2AMAZ-FQQ0TNP
 Client My Company
 Av Level Compliant

Information

Windows Defender 1.1.18300.4
 Anti Virus build 1.343.1348.0
 Running

2.1.6 Administrators

Onder Administrators kunt u zien welke users onder uw active directory vallen. Door op de server te klikken komt u in een volgend scherm.

Administrators

	Hosts	Domains	Current			Previous audit			Delta		
			Enterprise	Domain	Users	Enterprise	Domain	Users	Enterprise	Domain	Users
Server 1	3	1	1	1	4						

Hier ziet u een overzicht van gebruikersgroepen die bepaalde kenmerken delen.

Overview
Audit
Baselines
Reports
Archive
Accounts
Options

Domain Users

Active Users (4)	100.0%	<div style="width: 100%; height: 10px; background-color: green;"></div>
Inactive Users (3)	75.0%	<div style="width: 75%; height: 10px; background-color: green;"></div>
Administrator Rights (2)	50.0%	<div style="width: 50%; height: 10px; background-color: green;"></div>
Domain Administrators (1)	25.0%	<div style="width: 25%; height: 10px; background-color: green;"></div>
Enterprise Administrators (1)	25.0%	<div style="width: 25%; height: 10px; background-color: green;"></div>
Password not required to logon (0)	0.0%	<div style="width: 0%; height: 10px; background-color: green;"></div>
Password never expire (2)	50.0%	<div style="width: 50%; height: 10px; background-color: green;"></div>
Not logged in over 90 days (1)	25.0%	<div style="width: 25%; height: 10px; background-color: green;"></div>
Password not changed over 90 days (0)	0.0%	<div style="width: 0%; height: 10px; background-color: green;"></div>
Invalid logon attempts greater than 3 (0)	0.0%	<div style="width: 0%; height: 10px; background-color: green;"></div>
Never Logged in (1)	25.0%	<div style="width: 25%; height: 10px; background-color: green;"></div>
No Specific Logon Profile (0)	0.0%	<div style="width: 0%; height: 10px; background-color: green;"></div>
Not restricted to specific workstation (0)	0.0%	<div style="width: 0%; height: 10px; background-color: green;"></div>
No Logon Script (0)	0.0%	<div style="width: 0%; height: 10px; background-color: green;"></div>
No Home directory (0)	0.0%	<div style="width: 0%; height: 10px; background-color: green;"></div>

EXPORT (XLS)
DELETE

© 2021 Easy2Audit, version 16.42.415.0

Wanneer u klikt op een kenmerk (zoals inactieve users) krijgt u een overzicht van alle daarbij behorende gebruikers.

Domain User Names

Server	Windows Server 2012 R2
Description	Inactive Users
Portion	75.0% <div style="width: 75%; height: 10px; background-color: green;"></div>
Users	3
Account Names	1. DefaultAccount 2. Guest 3. krbtgt