

Secquard Applicatie Referentie Handleiding



Uitleg	4
Inlogscherm	4
Menu	5
Menu: Overview -> Dashboard	6
Menu: Overview -> Servers	17
Menu: Overview -> Inventory	18
Menu: Audit -> Upload audit result file	19
Menu: Audit -> Upload Active Directory	20
Menu: Audit -> Remote Audit	21
Menu: Baselines -> Download scripts	24
Menu: Baselines -> My profiles	25
Menu: Reports -> Reports	27
Menu: Reports -> Audit Log	27
Menu: Archive -> Reset Current Audit	28
Menu: Archive -> Create New Archive	28
Menu: Archive -> Archives	29
Menu: Accounts -> Clients	30
Menu: Accounts -> Users	32
Menu: Accounts -> Roles	33
Menu: Accounts -> Domains	34
Menu: Accounts -> Hosts	36
Menu: Options -> Updates	37
Menu: Options -> Update Baselines	37
Menu: Options -> Update Standards	38
Menu: Options -> Downloads	39
Menu: Options -> Maintenance	40
Menu: Options -> Setup	41

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.**

Inlogschermb

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-schermb. 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 heeft 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.

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	
		Hosts	Level	Hosts	Level	Hosts	Variance
Baselines	1						
Windows Server 2019		1	24.4%	1	24.4%	0	0%

Security Patches

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

Vulnerabilities

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

Anti-virus

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

Administrators

Hosts	2	Current			Previous audit			Differ		
		Enterprise	Domain	Users	Enterprise	Domain	Users	Enterprise	Domain	Users
Domains	1									
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%.

Overview Audit Baselines Reports Archive Accounts Options

client baseline archive
 My Company Windows Server 2019 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 Bedrijfsseisen 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 36%
 - ✚09.04 Toegangsbeheersing voor informatiesystemen en informatie 41%
- ✚10 Cryptografie 27%
- ✚12 Beveiliging bedrijfsvoering 8%
- ✚13 Communicatiebeveiliging 14%
- ✚14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen 15%
- ✚18 Naleving 23%

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.

Standard	BIO 1.04		
Control	Beheer van gebruikerswachtwoorden		
Description	De toewijzing van wachtwoorden behoort met een formeel beheerproces te worden beheerst.		
Compliance	36%	<div style="width: 36%; height: 10px; background-color: green; border: 1px solid black;"></div>	<div style="width: 64%; height: 10px; background-color: red; border: 1px solid black;"></div>
	BASELINE	COMPLIANCE	FAILED
	Windows Server 2019	36.5% <div style="width: 36.5%; height: 10px; background-color: green; border: 1px solid black;"></div>	108 control(s)
			MAPPING show control(s)

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)

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.

Standard	BIO 1.04	
Control	Beheer van speciale bevoegdheden	
Baseline	Windows Server 2019	
	MAPPED BASELINE CONTROL	
	01.01.01	(L1) Ensure Enforce password history is set to 24 or more password(s)
	01.01.02	(L1) Ensure Maximum password age is set to 60 or fewer days, but not 0
	01.01.03	(L1) Ensure Minimum password age is set to 1 or more day(s)
	01.01.04	(L1) Ensure Minimum password length is set to 14 or more character(s)

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%.

Hardening

Hosts	Baselines	Current		Previous audit		Realization	
Hosts	Baselines	Hosts	Level	Hosts	Level	Hosts	Variance
1	1	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. 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.

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

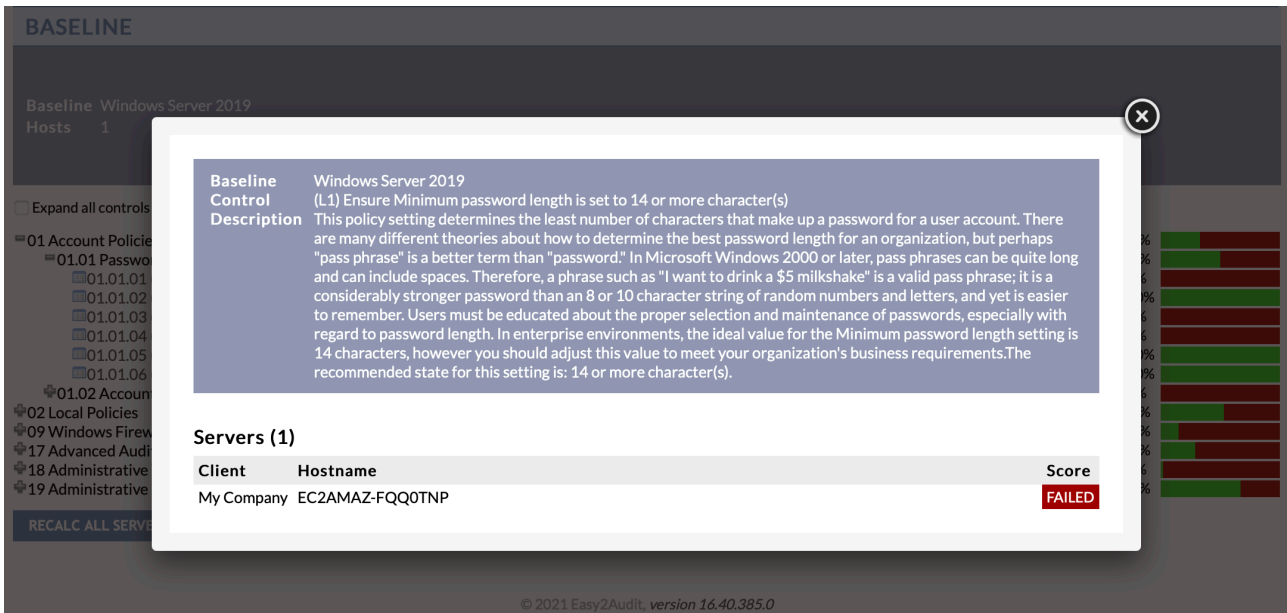
33%	<div style="width: 33%; height: 10px; background: linear-gradient(to right, green, red);"></div>
50%	<div style="width: 50%; height: 10px; background: linear-gradient(to right, green, red);"></div>
0%	<div style="width: 0%; height: 10px; background: linear-gradient(to right, green, red);"></div>
100%	<div style="width: 100%; height: 10px; background: linear-gradient(to right, green, red);"></div>
0%	<div style="width: 0%; height: 10px; background: linear-gradient(to right, green, red);"></div>
100%	<div style="width: 100%; height: 10px; background: linear-gradient(to right, green, red);"></div>
100%	<div style="width: 100%; height: 10px; background: linear-gradient(to right, green, red);"></div>
0%	<div style="width: 0%; height: 10px; background: linear-gradient(to right, green, red);"></div>
53%	<div style="width: 53%; height: 10px; background: linear-gradient(to right, green, red);"></div>
15%	<div style="width: 15%; height: 10px; background: linear-gradient(to right, green, red);"></div>
29%	<div style="width: 29%; height: 10px; background: linear-gradient(to right, green, red);"></div>
2%	<div style="width: 2%; height: 10px; background: linear-gradient(to right, green, red);"></div>
67%	<div style="width: 67%; height: 10px; background: linear-gradient(to right, green, red);"></div>

RECALC ALL SERVERS

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.



The screenshot shows the Secquard interface with a pop-up window for a baseline control. The pop-up contains the following information:

- 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).

Below the description, a table lists the servers affected by this control:

Servers (1)		
Client	Hostname	Score
My Company	EC2AMAZ-FQQ0TNP	FAILED

The background interface shows a sidebar with a tree view of controls, including '01 Account Policies', '02 Local Policies', '09 Windows Firewall', '17 Advanced Audit', '18 Administrative', and '19 Administrative'. A 'RECALC ALL SERVERS' button is visible at the bottom left of the sidebar.

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 weergegeven.

Security Patches

Hosts	1	Current			Previous audit			Realization		
		Hosts	Compliant	NOT Compliant	Hosts	Compliant	NOT Compliant	Hosts	Compliant	NOT Compliant
Baselines	1									
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.

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).

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

PATCHES (1 SERVERS)

HOST	BASELINE	LAST UPLOAD	IMPORTANT PATCHES	CRITICAL PATCHES	PATCH AGE
EC2AMAZ-FQQTNP	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 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.

« 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

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	Current					Previous audit					Realization										
		Total		CVE's			Affected		Total		CVE's			Affected		Total		CVE's			Affected	
		hosts		C	H	M	hosts		hosts	C	H	M	hosts	C	H	M	hosts	C	H	M	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
baseline

My Company
Windows Server 2019

VULNERABILITIES

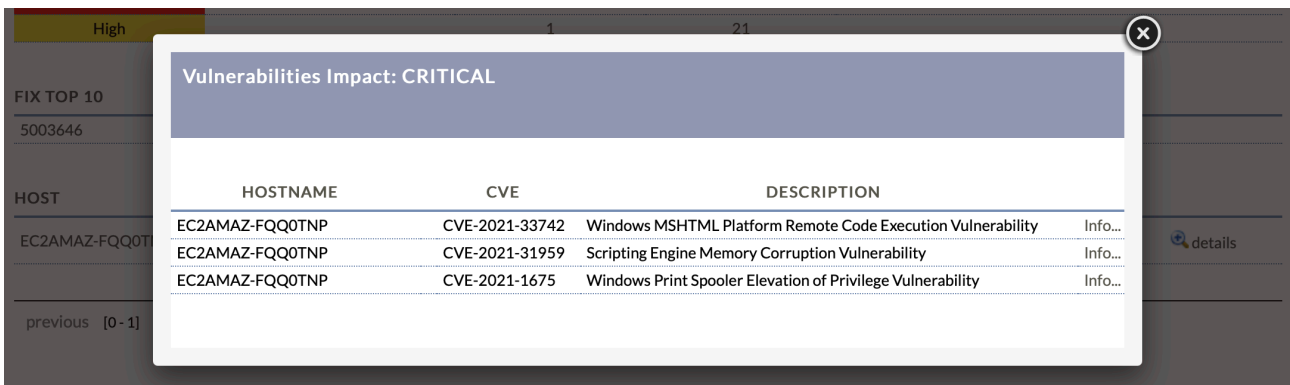
IMPACT	HOSTS	VULNERABILITIES
Critical	1	3
High	1	21

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

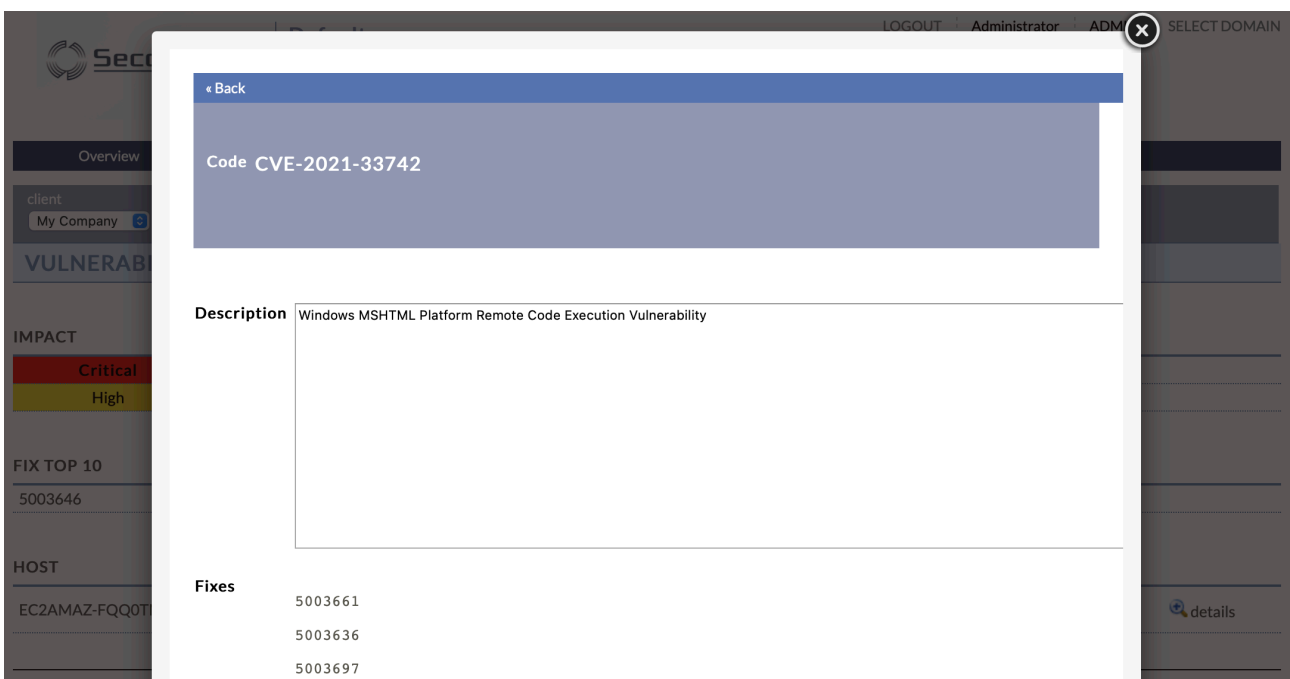
HOST	BASELINE	LAST UPLOAD	CRITICAL	HIGH	MEDIUM	LOW	NONE	STATUS
EC2AMAZ-FQQ0TNP	Windows Server 2019	2021-07-21T10:45:51.443Z	3	21	0	0	0	24 found details

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		baseline						
My Company		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).

Anti-virus

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

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 .

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](#)

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

Menu: Overview -> Servers

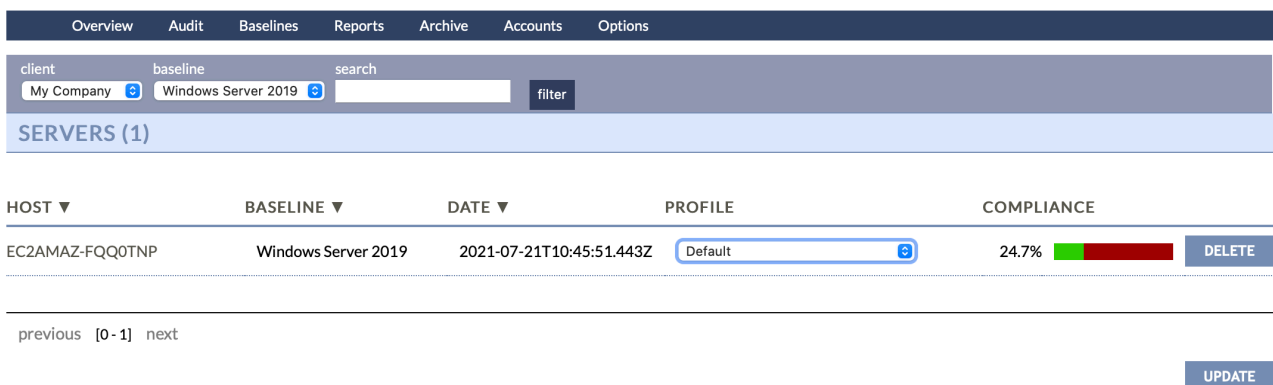
Wanneer we boven in het menu onze muis op Overview houden, kunnen wij in het dropdown menu “Servers” selecteren. Dit brengt ons naar onderstaande pagina.

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.

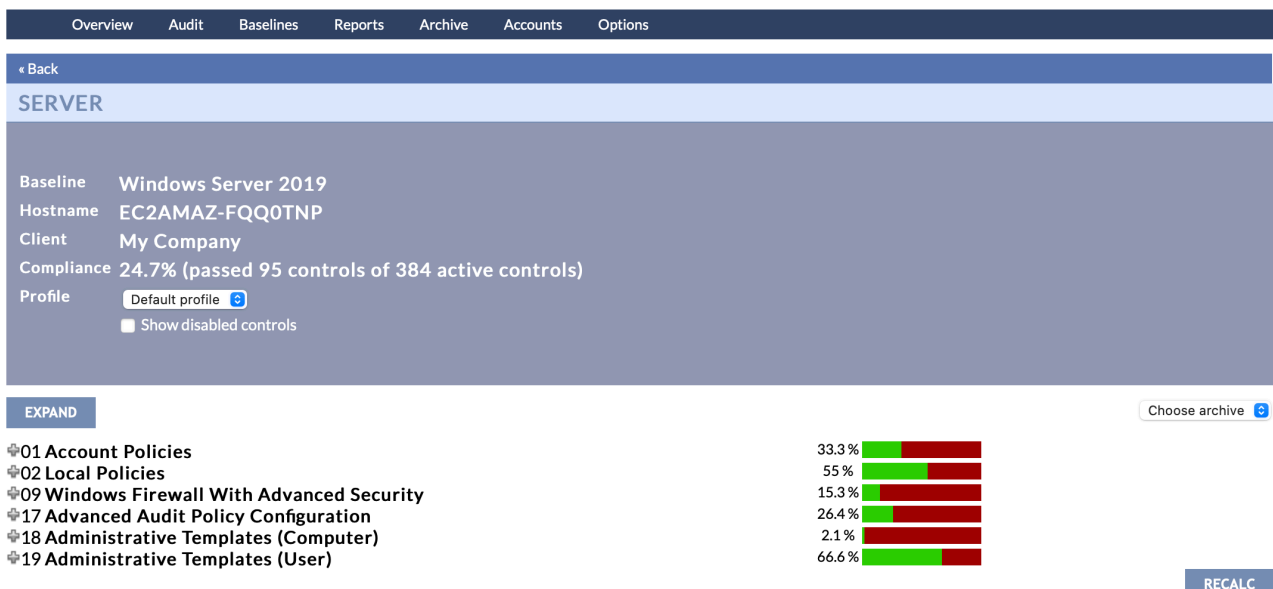


HOST	BASELINE	DATE	PROFILE	COMPLIANCE	
EC2AMAZ-FQQ0TNP	Windows Server 2019	2021-07-21T10:45:51.443Z	Default	24.7%	DELETE

previous [0 - 1] next

UPDATE

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.



EXPAND

Choose archive

01 Account Policies	33.3%
02 Local Policies	55%
09 Windows Firewall With Advanced Security	15.3%
17 Advanced Audit Policy Configuration	26.4%
18 Administrative Templates (Computer)	2.1%
19 Administrative Templates (User)	66.6%

RECALC

Menu: Overview -> Inventory

Het inventory overzicht laat per server een aantal kenmerken zien, het operating system (OS), een aantal hardware specificaties (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.

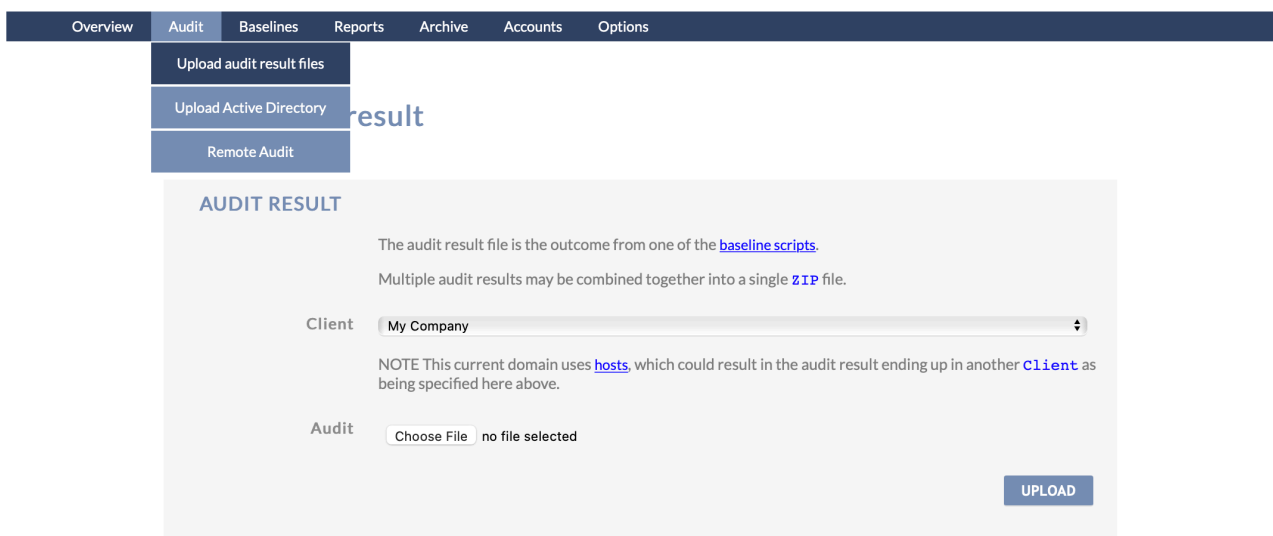
Overview Audit Baselines Reports Archive Accounts Options			
client Dashboard Baseline			
My Servers Windows Server 2019			
Inventory			
Hosts	OS	System	Anti-virus
EC2AMAZ-FQQ0TNP Windows Server 2019 Installed software [hide]	OS Name: Microsoft Windows Server 2019 Datacenter C:\Windows\Device\Harddisk0\Partition1 Os Version: 10.0.17763 Service Pack: 0.0 Microsoft SQL Server 2017 (64-bit) Microsoft SQL Server 2017 (64-bit) SQL Server 2017 Client Tools Extensions SQL Server 2017 Database Engine Shared SQL Server 2017 Shared Management Objects SQL Server 2017 XEvent SQL Server 2017 Client Tools Extensions Microsoft VSS Writer for SQL Server 2017 SQL Server 2017 Database Engine Services SQL Server 2017 Batch Parser Microsoft SQL Server 2017 Setup (English) Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29913 AWS PV Drivers Azure Data Studio SQL Server 2017 Shared Management Objects SQL Server Management Studio for Analysis Services Microsoft SQL Server 2017 RsFx Driver Microsoft ODBC Driver 13 for SQL Server SQL Server 2017 Database Engine Shared SQL Server Management Studio for Reporting Services Microsoft MPI (10.0.12498.5) Microsoft ODBC Driver 17 for SQL Server SQL Server 2017 Connection Info SQL Server 2017 Shared Management Objects Extensions Microsoft Analysis Services OLE DB Provider SQL Server 2017 Common Files Microsoft OLE DB Driver for SQL Server Microsoft SQL Server 2012 Native Client SQL Server 2017 Client Tools SQL Server 2017 Connection Info SQL Server 2017 XEvent SQL Server Management Studio Microsoft Visual Studio Tools for Applications 2017 x64 Hosting Support Easy2Audit SQL Server 2017 Common Files SQL Server 2017 DMF SQL Server 2017 Client Tools aws-cfn-bootstrap SSMS Post Install Tasks SQL Server 2017 Full text search	Avail. Memory: 3958372 BIOS Version: Xen - 0 Type: x64 DeviceID: C: 59% Free	Windows Defender 1.1.18300.4 Anti Virus build 1.343.1348.0 Running

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.



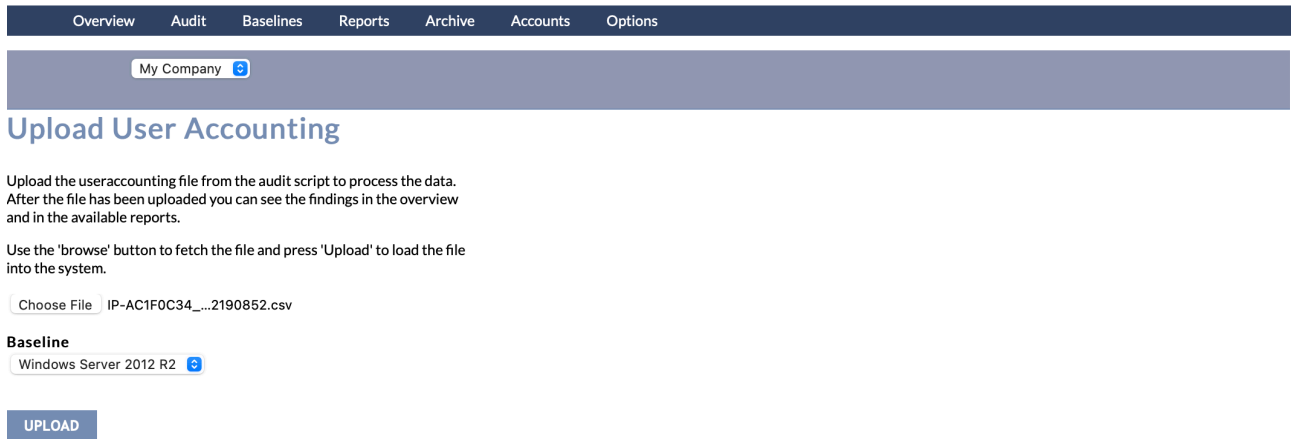
The screenshot shows the 'Audit' menu in the Secquard interface. The 'Upload audit result files' option is selected, leading to the 'AUDIT RESULT' page. The page contains the following elements:

- Navigation Bar:** Overview, Audit (selected), Baselines, Reports, Archive, Accounts, Options.
- Sub-menu:** Upload audit result files (selected), Upload Active Directory, Remote Audit.
- Section Header:** AUDIT RESULT
- Text:** The audit result file is the outcome from one of the [baseline scripts](#). Multiple audit results may be combined together into a single [ZIP](#) file.
- Client:** A dropdown menu showing 'My Company'.
- Note:** NOTE This current domain uses [hosts](#), which could result in the audit result ending up in another [Client](#) as being specified here above.
- Audit:** A 'Choose File' button and the text 'no file selected'.
- Button:** A blue 'UPLOAD' button.

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.



Overview Audit Baselines Reports Archive Accounts Options

My Company

Upload User Accounting

Upload the useraccounting file from the audit script to process the data. After the file has been uploaded you can see the findings in the overview and in the available reports.

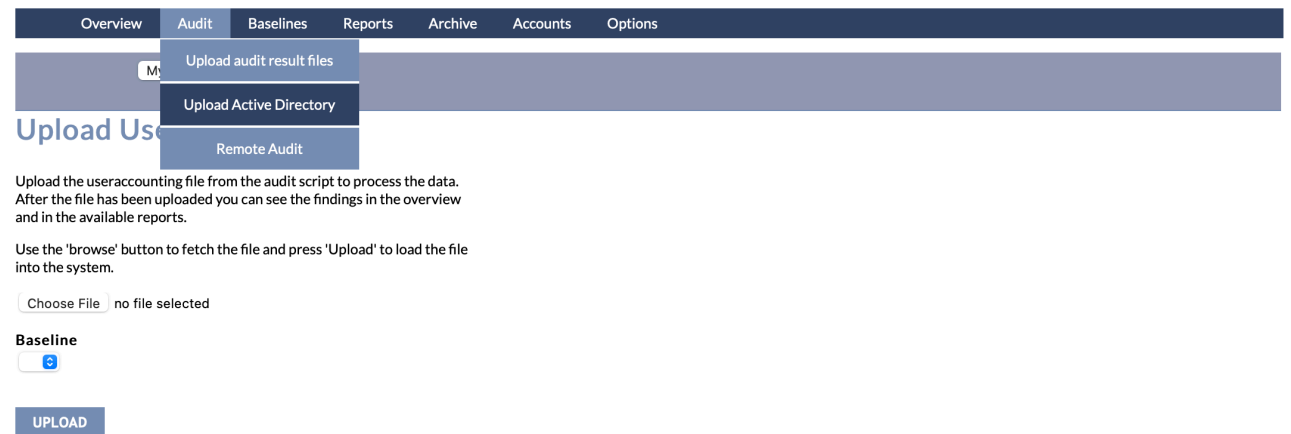
Use the 'browse' button to fetch the file and press 'Upload' to load the file into the system.

Choose File IP-AC1F0C34_...2190852.csv

Baseline

Windows Server 2012 R2

UPLOAD



Overview Audit Baselines Reports Archive Accounts Options

My Company

Upload User Accounting

Upload the useraccounting file from the audit script to process the data. After the file has been uploaded you can see the findings in the overview and in the available reports.

Use the 'browse' button to fetch the file and press 'Upload' to load the file into the system.

Choose File no file selected

Baseline

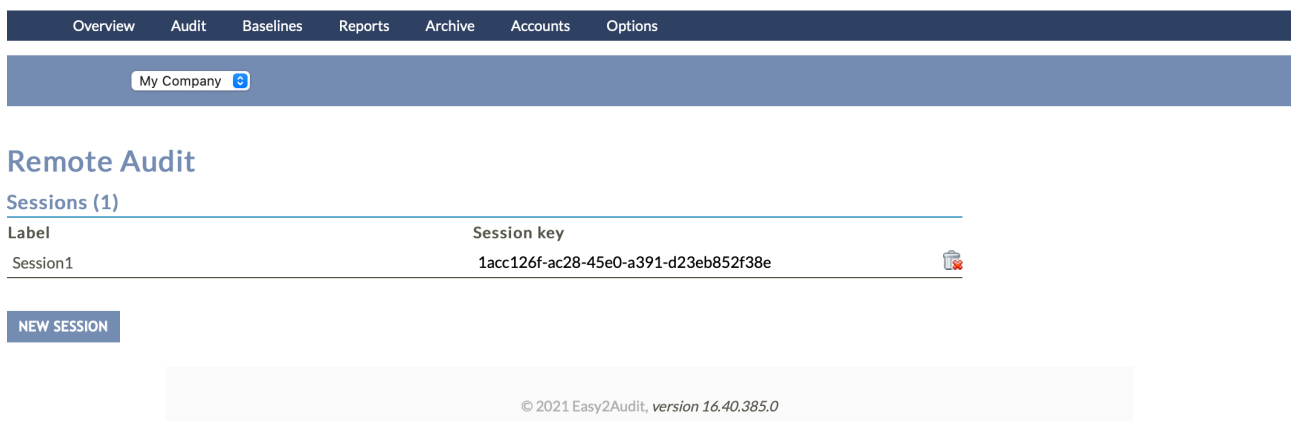
Windows Server 2012 R2

UPLOAD

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.



Overview Audit Baselines Reports Archive Accounts Options

My Company

Remote Audit

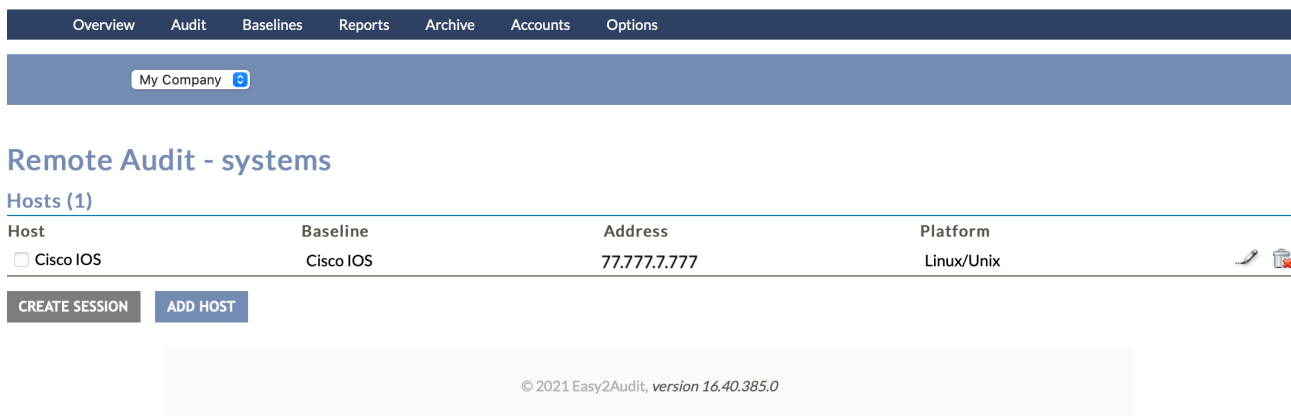
Sessions (1)

Label	Session key
Session1	1acc126f-ac28-45e0-a391-d23eb852f38e

NEW SESSION

© 2021 Easy2Audit, version 16.40.385.0

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.



Overview Audit Baselines Reports Archive Accounts Options

My Company

Remote Audit - systems

Hosts (1)

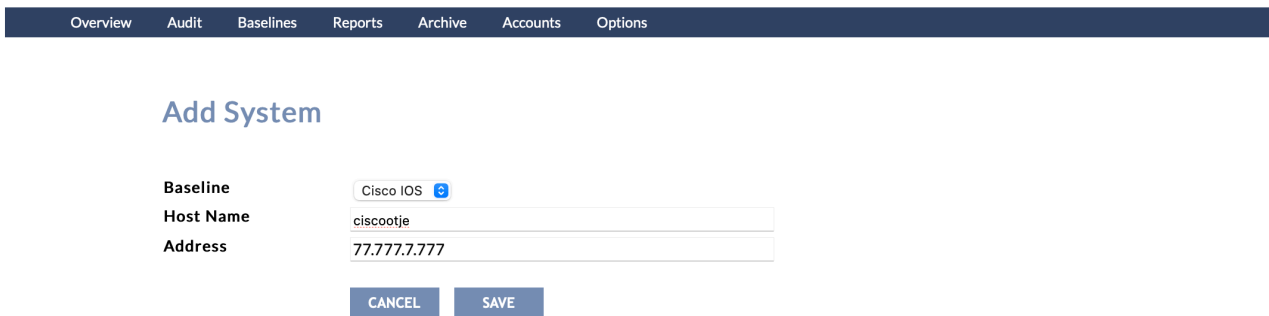
Host	Baseline	Address	Platform
<input type="checkbox"/> Cisco IOS	Cisco IOS	77.777.7.777	Linux/Unix

CREATE SESSION ADD HOST

© 2021 Easy2Audit, version 16.40.385.0

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.



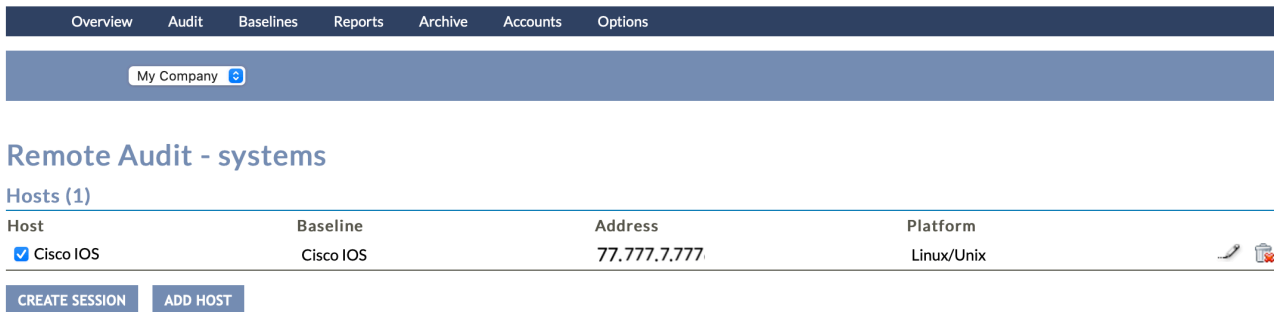
The screenshot shows the 'Add System' form with the following fields and values:

- Baseline: Cisco IOS
- Host Name: ciscootje
- Address: 77.777.7.777

Buttons: CANCEL, SAVE

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

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

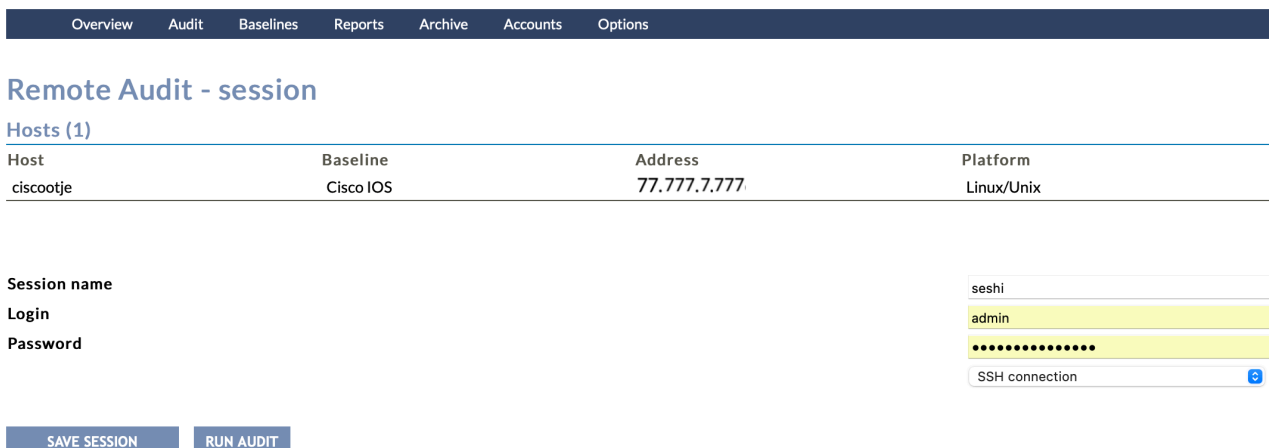


The screenshot shows the 'Remote Audit - systems' page with a table of hosts:

Host	Baseline	Address	Platform
<input checked="" type="checkbox"/> Cisco IOS	Cisco IOS	77.777.7.777	Linux/Unix

Buttons: CREATE SESSION, ADD HOST

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



The screenshot shows the 'Remote Audit - session' page with the following fields and values:

- Session name: seshi
- Login: admin
- Password: [Redacted]
- SSH connection: SSH connection

Buttons: SAVE SESSION, 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).

Overview Audit Baselines Reports Archive Accounts Options

Remote Audit - session

Hosts (1)

Host	Baseline	Address	Platform
ciscootje	Cisco IOS	77.777.7.777	Linux/Unix

Connecting to: 77.777.7.777 Connected connected connection closed

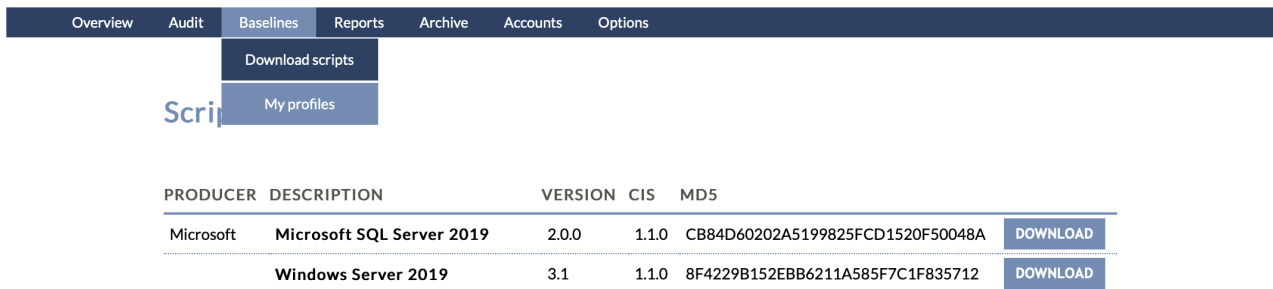
BACK

For use in scheduling: <http://11.111.1.23/Audit/RemoteConnect.aspx?key=1acc126f-ac28-45e0-a391-d23eb852f38e>

© 2021 Easy2Audit, version 16.40.385.0

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.



PRODUCER	DESCRIPTION	VERSION	CIS	MD5	
Microsoft	Microsoft SQL Server 2019	2.0.0	1.1.0	CB84D60202A5199825FCD1520F50048A	DOWNLOAD
	Windows Server 2019	3.1	1.1.0	8F4229B152EBB6211A585F7C1F835712	DOWNLOAD

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.



Download Script: Windows Server 2019

Easy2audit will generate an audit script for this server. This script could be run on the specified server and will write its results to an evidence file.

[DOWNLOAD SCRIPT](#)

MANUAL AUDIT

1. Download the script.
2. Log in as a member of the Administrators Group on the local machine or as a Domain Administrator.
3. Double click it to run, a small window audit started will appear, click OK (There will be some command prompts flashing on screen).
4. A resultfile will be generated in the same directory, for example: Server01_result_1354542717.txt.
5. Go to Audit on Easy2audit and upload the resultfile.
6. Go to Overview and you will see results added to the list.

SCHEDULED AUDIT

Audits can be scheduled to run automatically. There is a script and manual available in the [Tool Suite](#)

CHANGELOG

```

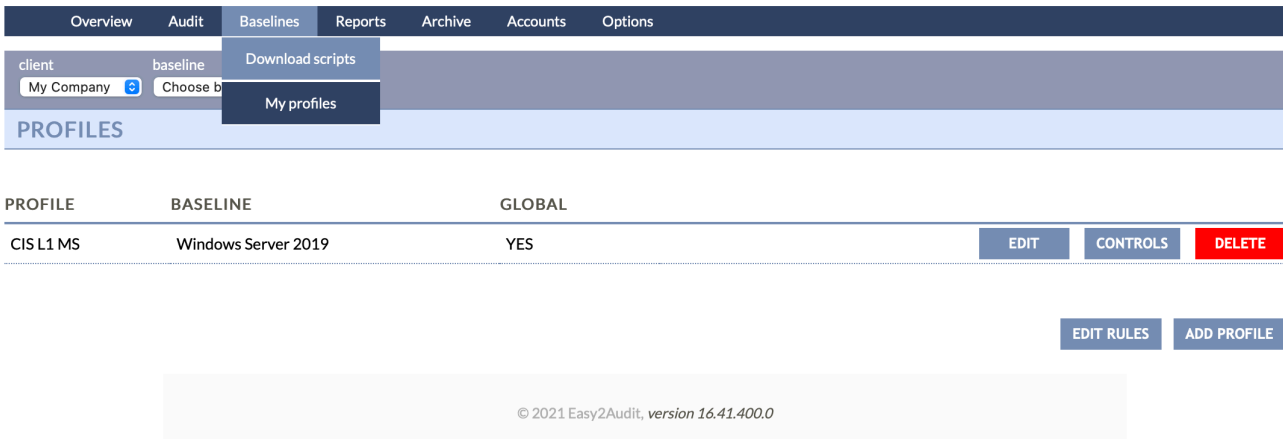
=====
Version: 3.2
Date: 2020-07-23
-----
DB CON-337 FD762 Fixed patch audit issue
=====
Version: 3.1
Date: 2021-05-28
-----
PS - CON-309 update of Trend Micro AV Snippet
=====
Version: 3.0
Date: 2021-05-18
-----
DB-CON-205: Implemented ISO8601 date format
=====

```


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(level)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.



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

[EDIT RULES](#)
[ADD PROFILE](#)

© 2021 Easy2Audit, version 16.41.400.0

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.

Edit 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:

[CANCEL](#)
[SAVE](#)

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.

← Back

PROFILE

Baseline **Windows Server 2019**
 Profile **CIS L1 MS**

- + **01 Account Policies**
 - + **01.01 Password Policy**

01.01.01 (L1) Ensure Enforce password history is set to 24 or more password(s)	24	↕
01.01.02 (L1) Ensure Maximum password age is set to 60 or fewer days, but not 0	5184000	↕
01.01.03 (L1) Ensure Minimum password age is set to 1 or more day(s)	86400	↕
01.01.04 (L1) Ensure Minimum password length is set to 14 or more character(s)	14	↕
01.01.05 (L1) Ensure Password must meet complexity requirements is set to Enabled	1	↕
01.01.06 (L1) Ensure Store passwords using reversible encryption is set to Disabled	0	↕
 - + **01.02 Account Lockout Policy**
- + **02 Local Policies**
- + **09 Windows Firewall With Advanced Security**
- + **17 Advanced Audit Policy Configuration**
- + **18 Administrative Templates (Computer)**
- + **19 Administrative Templates (User)**

IMPORT
EXPORT
RECALC

© 2021 Easy2Audit, version 16.40.385.0

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.

Control (L1) Ensure Minimum password length is set to 14 or more character(s)
 Profile **CIS L1 MS**

SOLL value

*Set this value with the benchmark value for this profile control.

Disabled (Does not validate this control for this profile)

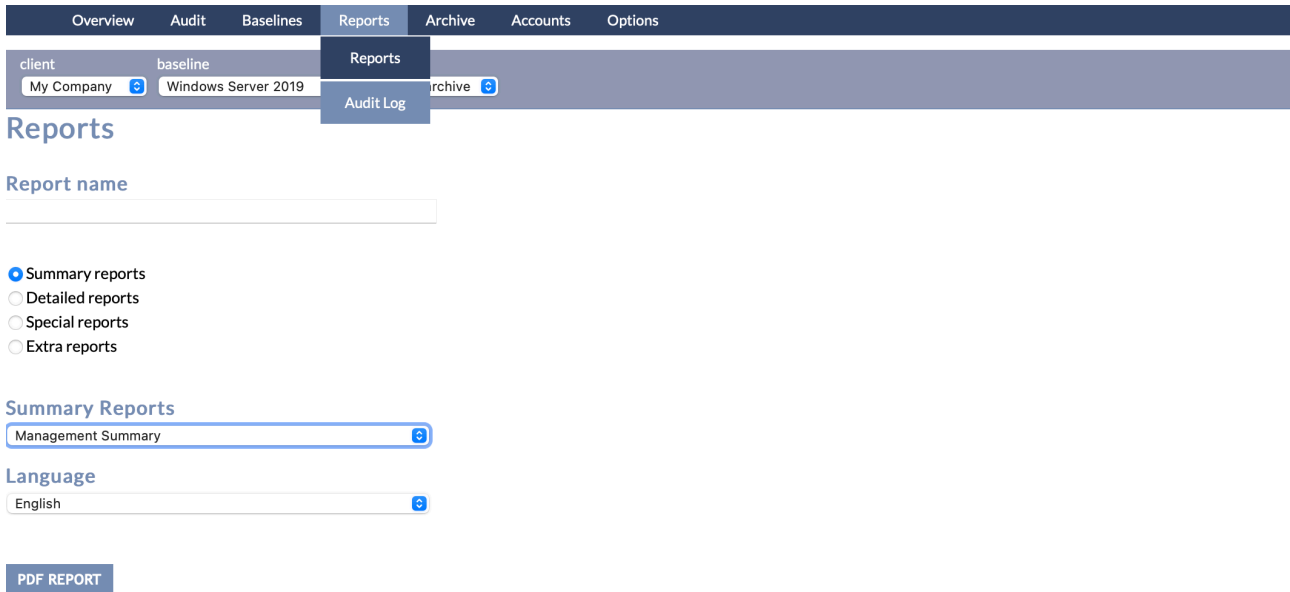
Reason

* Minimum 20 characters

OK
DEFAULT

Menu: Reports -> Reports

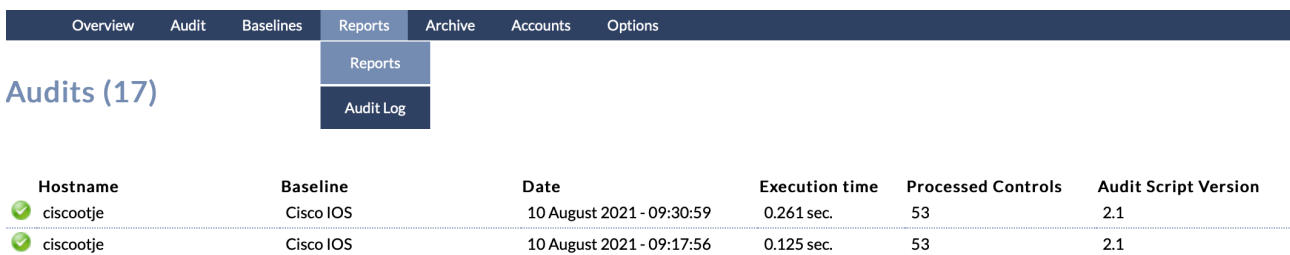
Via de reports pagina kunt u verschillende rapportages downloaden. U kunt kiezen voor samenvattingen, gedetailleerde rapporten, speciale rapporten en extra rapporten. Via de dropdown keuze-menu's daarna kunt u uw selectie verder specificeren voordat u uw rapport downloadt.



The screenshot shows the 'Reports' menu in the Secquard interface. The navigation bar includes 'Overview', 'Audit', 'Baselines', 'Reports', 'Archive', 'Accounts', and 'Options'. The 'Reports' dropdown menu is open, showing 'Reports' and 'Audit Log'. Below the menu, there are filters for 'client' (My Company) and 'baseline' (Windows Server 2019). The 'Reports' section has a 'Report name' input field and radio buttons for 'Summary reports' (selected), 'Detailed reports', 'Special reports', and 'Extra reports'. Under 'Summary Reports', there is a dropdown menu set to 'Management Summary'. The 'Language' dropdown is set to 'English'. A 'PDF REPORT' button is visible at the bottom.

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.

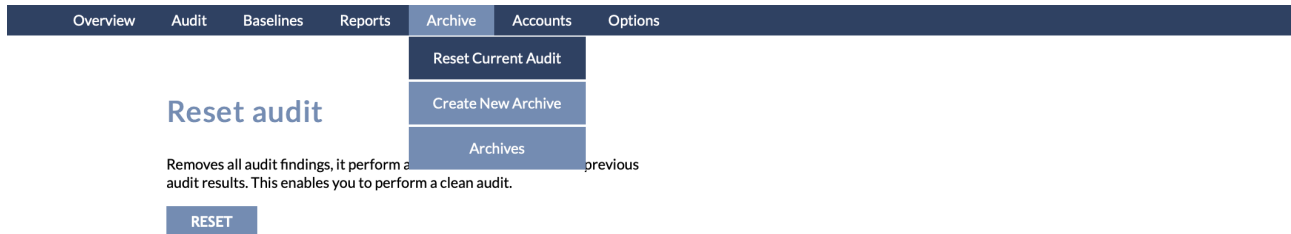


The screenshot shows the 'Audit Log' page in the Secquard interface. The navigation bar is the same as in the previous screenshot. The 'Audit Log' dropdown menu is open. The page title is 'Audits (17)'. Below the title is a table with the following columns: Hostname, Baseline, Date, Execution time, Processed Controls, and Audit Script Version. The table contains two rows of audit data.

Hostname	Baseline	Date	Execution time	Processed Controls	Audit Script Version
✓ ciscootje	Cisco IOS	10 August 2021 - 09:30:59	0.261 sec.	53	2.1
✓ ciscootje	Cisco IOS	10 August 2021 - 09:17:56	0.125 sec.	53	2.1

Menu: Archive -> Reset Current Audit

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

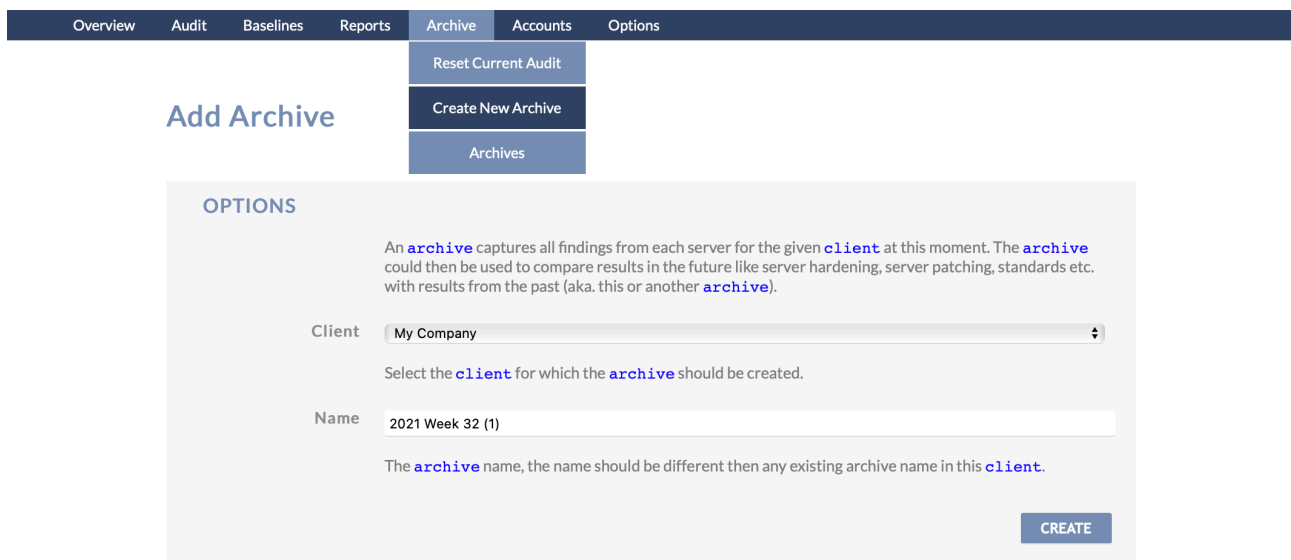


The screenshot shows the navigation menu with 'Archive' selected. A dropdown menu is open, showing 'Reset Current Audit', 'Create New Archive', and 'Archives'. The 'Reset Current Audit' option is highlighted. Below the menu, the text reads: 'Reset audit Removes all audit findings, it performs a clean audit. This enables you to perform a clean audit.' A 'RESET' button is visible at the bottom.

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.



The screenshot shows the 'Add Archive' form in the Archive section. The 'Create New Archive' option is highlighted in the dropdown menu. The form is titled 'OPTIONS' and contains the following fields and instructions:

- Client:** A dropdown menu with 'My Company' selected. Below it, the instruction reads: 'Select the client for which the archive should be created.'
- Name:** A text input field containing '2021 Week 32 (1)'. Below it, the instruction reads: 'The archive name, the name should be different then any existing archive name in this client.'

A 'CREATE' button is located at the bottom right of the form.

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.

Overview Audit Baselines Reports Archive Accounts Options

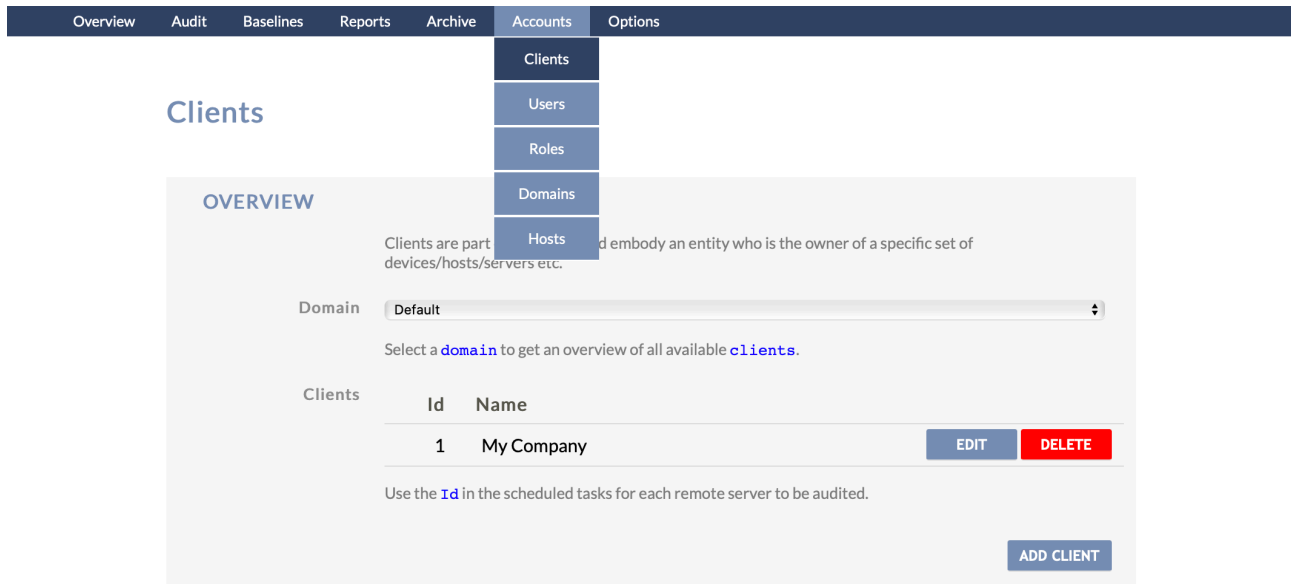
My Company

Archives

Description	Date	
2021 Week 32 (1)	8/12/2021 2:33:02 PM	 
2021 Week 32	8/9/2021 12:57:42 PM	 
2021 Week 30	7/29/2021 11:55:07 AM	 

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.



Overview | Audit | Baselines | Reports | Archive | **Accounts** | Options

Clients

Users
Roles
Domains
Hosts

OVERVIEW

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

Domain: Default

Select a [domain](#) to get an overview of all available [clients](#).

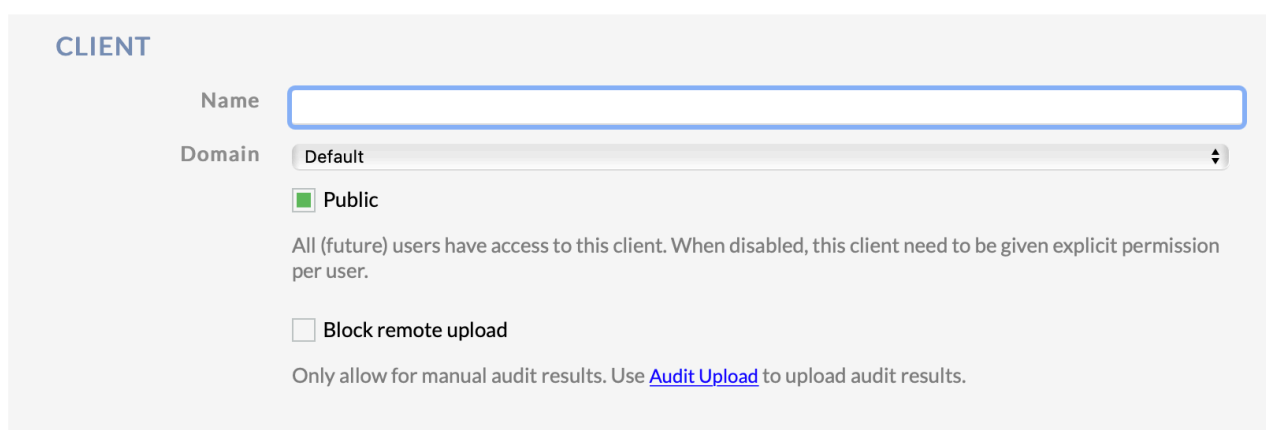
Id	Name	
1	My Company	EDIT DELETE

Use the [Id](#) in the scheduled tasks for each remote server to be audited.

[ADD CLIENT](#)

Via 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.

Add Client



CLIENT

Name:

Domain: Default

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. 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.

STANDARD

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

- Available NEN 7511-1
 ISO 27002:2013

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.

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.

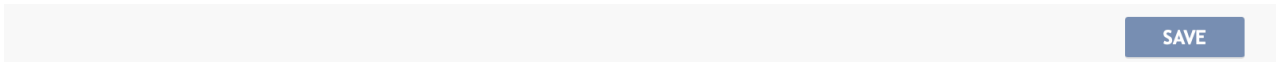
Critical

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

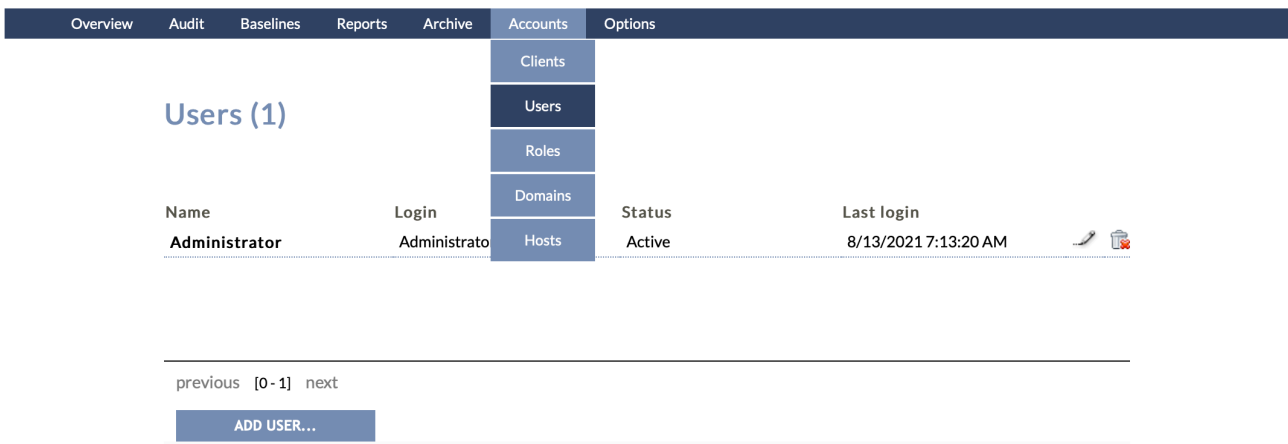
Security patches should be applied as soon as possible - but could be given a bit more slack regarding installation date then critical patches - so keep the threshold low to medium (for example 30 days). Most vendors have a patch release once a month.

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



Menu: Accounts -> Users

In dit onderdeel van het menu kunt u gebruikers aan de applicatie toevoegen, aanpassen en verwijderen, en hen rechten 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 is a pagination control '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*

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).

Edit user

Full Name
Login
Password
Domain admin 
Administrator *full administrator for the application*

Access
 Default











Clients
 My Company

SAVE

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

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).

Overview	Audit	Baselines	Reports	Archive	Accounts	Options
					Clients	
					Users	
					Roles	
					Domains	
					Hosts	
Roles						
Description						
Administrator						 
Auditor						 
Demo						 
Support						 
Viewer						 
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.

Add new role

Label

Overview
 Audit
 Download
 Reports
 Tools
 Accounts
 Standards | Edit:
 Baselines | Edit:

CREATE ROLE

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).

Accounts menu: Clients, Users, Roles, Domains, Hosts

Domains

OVERVIEW

A domain is a logical connection between devices, users and clients.

Name

Default EDIT DELETE

ADD DOMAIN

© 2021 Easy2Audit, version 16.40.385.0

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.

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

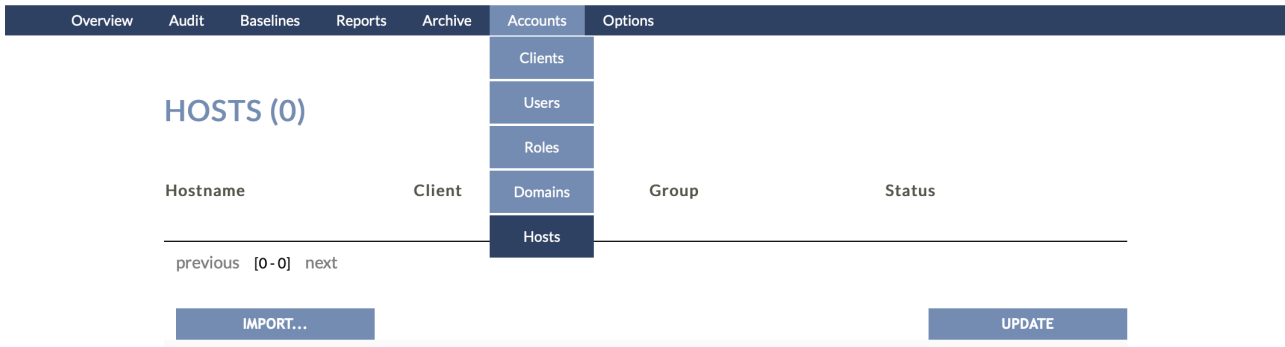
Critical patches require a swift response, these patches fix something which most likely makes the device vulnerable for attackers. So keep the threshold low (for example 7 days maximum).

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.

Menu: Accounts -> Hosts

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



The screenshot shows the 'Accounts' menu in the Secquard interface. The 'Accounts' menu is open, showing options: Clients, Users, Roles, Domains, and Hosts. The 'Hosts' option is selected. Below the menu, the 'HOSTS (0)' section is visible, showing a table with columns: Hostname, Client, Group, and Status. The table is currently empty. Below the table, there are navigation links: 'previous [0-0] next'. At the bottom, there are two buttons: 'IMPORT...' and 'UPDATE'.

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.

Overview	Audit	Baselines	Reports	Archive	Accounts	Options
						<ul style="list-style-type: none"> Updates Update Baselines Update Standards Downloads Maintenance Setup
<h3>System update</h3> <p>Update the application</p> <p>Current version: 16.40.385.0 Latest version: 16.40.385.0 Last updated: Friday, July 30, 2021 Last checked: Friday, August 13, 2021</p> <p>UPDATE SYSTEM</p>						
<h3>Content update</h3> <p>Update patch and vulnerability information</p> <p>Current version: 11 Latest version: 11 Last updated: Tuesday, August 3, 2021 Last checked: Tuesday, August 3, 2021</p> <p>UPDATE CONTENT</p>						

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.

Overview	Audit	Baselines	Reports	Archive	Accounts	Options																																								
						<ul style="list-style-type: none"> Updates Update Baselines Update Standards Downloads Maintenance Setup 																																								
<h3>Update or install Baselines</h3> <table border="1"> <thead> <tr> <th>PRODUCER</th> <th>BASELINE</th> <th>LATEST VERSION</th> <th>INSTALL</th> <th>NOTES</th> </tr> </thead> <tbody> <tr> <td>IBM</td> <td>AIX 5</td> <td>1.0</td> <td>INSTALL</td> <td>NOTES</td> </tr> <tr> <td>IBM</td> <td>AIX 6</td> <td>1.0</td> <td>INSTALL</td> <td>NOTES</td> </tr> <tr> <td>Centos</td> <td>Centos Linux 6</td> <td>4.0.0</td> <td>INSTALL</td> <td>NOTES</td> </tr> <tr> <td>Centos</td> <td>Centos Linux 7</td> <td>6.0</td> <td>INSTALL</td> <td>NOTES</td> </tr> <tr> <td>Centos</td> <td>Centos Linux 8</td> <td>3.00</td> <td>INSTALL</td> <td>NOTES</td> </tr> <tr> <td>Cisco</td> <td>Cisco NX</td> <td>2.0</td> <td>INSTALL</td> <td>NOTES</td> </tr> <tr> <td>Cisco</td> <td>Cisco XR</td> <td>2.0</td> <td>INSTALL</td> <td>NOTES</td> </tr> </tbody> </table>						PRODUCER	BASELINE	LATEST VERSION	INSTALL	NOTES	IBM	AIX 5	1.0	INSTALL	NOTES	IBM	AIX 6	1.0	INSTALL	NOTES	Centos	Centos Linux 6	4.0.0	INSTALL	NOTES	Centos	Centos Linux 7	6.0	INSTALL	NOTES	Centos	Centos Linux 8	3.00	INSTALL	NOTES	Cisco	Cisco NX	2.0	INSTALL	NOTES	Cisco	Cisco XR	2.0	INSTALL	NOTES	
PRODUCER	BASELINE	LATEST VERSION	INSTALL	NOTES																																										
IBM	AIX 5	1.0	INSTALL	NOTES																																										
IBM	AIX 6	1.0	INSTALL	NOTES																																										
Centos	Centos Linux 6	4.0.0	INSTALL	NOTES																																										
Centos	Centos Linux 7	6.0	INSTALL	NOTES																																										
Centos	Centos Linux 8	3.00	INSTALL	NOTES																																										
Cisco	Cisco NX	2.0	INSTALL	NOTES																																										
Cisco	Cisco XR	2.0	INSTALL	NOTES																																										

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.

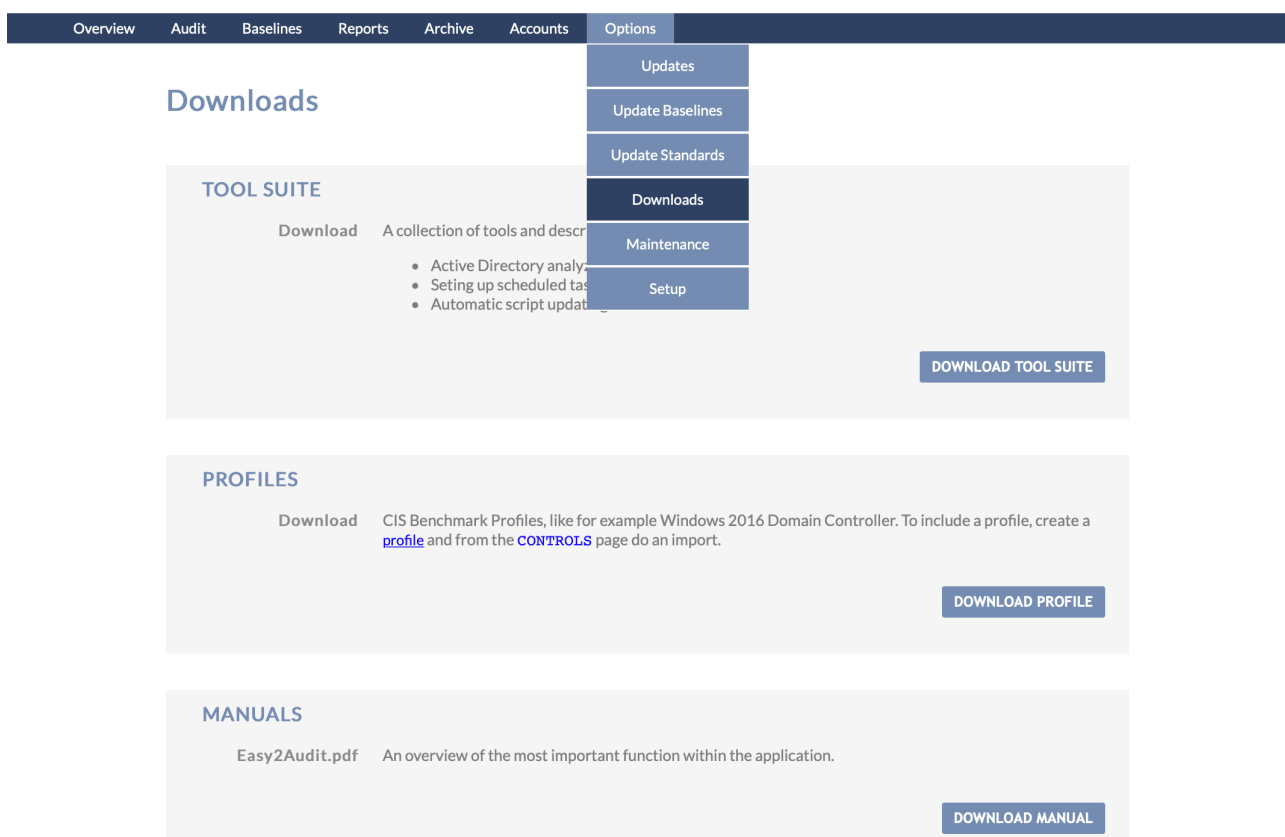
STANDARD	CURRENT	LATEST VERSION	
ISO 17799:2005 Automated controls	0	1	update
CIS Controls V7.1	0	2	update
CIS Critical Security Controls	0	4	update
BIC V3.0 (2019)	0	1	update
ISO/IEC 27002:2013 (Automated controls)	0	1	update
NIST 800-53 rev4	0	1	update
Quick Scan	0	1	update
E2A Quick Scan	0	2	update
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

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.



The screenshot shows the 'Options' menu in the Secquard application. The 'Downloads' option is selected, opening a dropdown menu with the following items: Updates, Update Baselines, Update Standards, Downloads (highlighted), Maintenance, and Setup. Below the menu, the 'Downloads' section is visible, containing three main categories: TOOL SUITE, PROFILES, and MANUALS. Each category has a 'Download' link, a brief description, and a corresponding 'DOWNLOAD' button.

Downloads

TOOL SUITE

Download A collection of tools and descriptions for Active Directory analysis, setting up scheduled tasks, and automatic script updates.

- Active Directory analysis
- Setting up scheduled tasks
- Automatic script updates

DOWNLOAD TOOL SUITE

PROFILES

Download CIS Benchmark Profiles, like for example Windows 2016 Domain Controller. To include a profile, create a [profile](#) and from the **CONTROLS** page do an import.

DOWNLOAD PROFILE

MANUALS

Easy2Audit.pdf An overview of the most important function within the application.

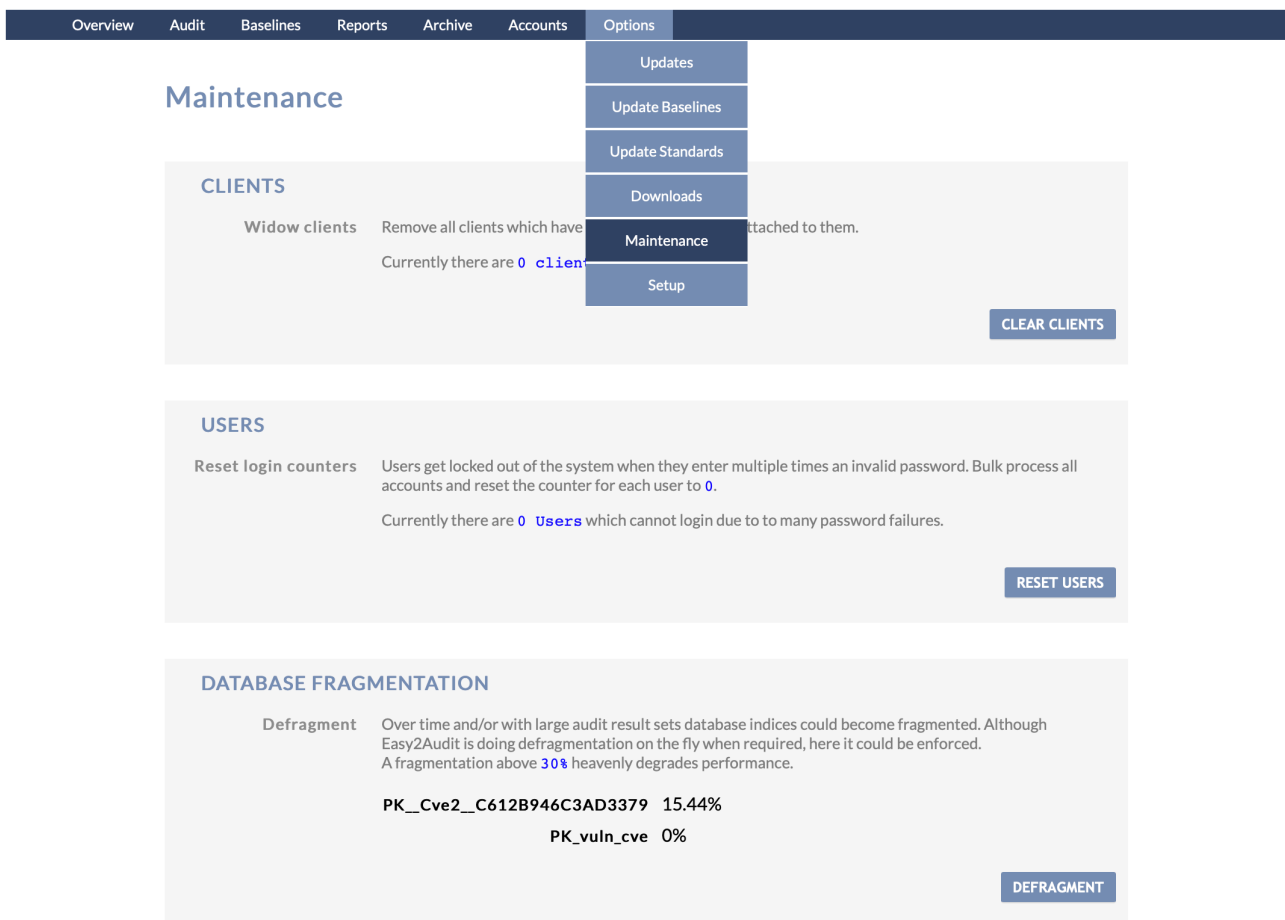
DOWNLOAD MANUAL

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.



The screenshot shows the 'Options' menu with 'Maintenance' selected. The 'Maintenance' dropdown menu is open, showing options: Updates, Update Baselines, Update Standards, Downloads, Maintenance (selected), and Setup. The main content area is titled 'Maintenance' and contains three sections: 'CLIENTS', 'USERS', and 'DATABASE FRAGMENTATION'.

CLIENTS

Widow clients Remove all clients which have no hosts/audits attached to them.
Currently there are 0 clients.

CLEAR CLIENTS

USERS

Reset login counters Users get locked out of the system when they enter multiple times an invalid password. Bulk process all accounts and reset the counter for each user to 0.
Currently there are 0 Users which cannot login due to too many password failures.

RESET USERS

DATABASE FRAGMENTATION

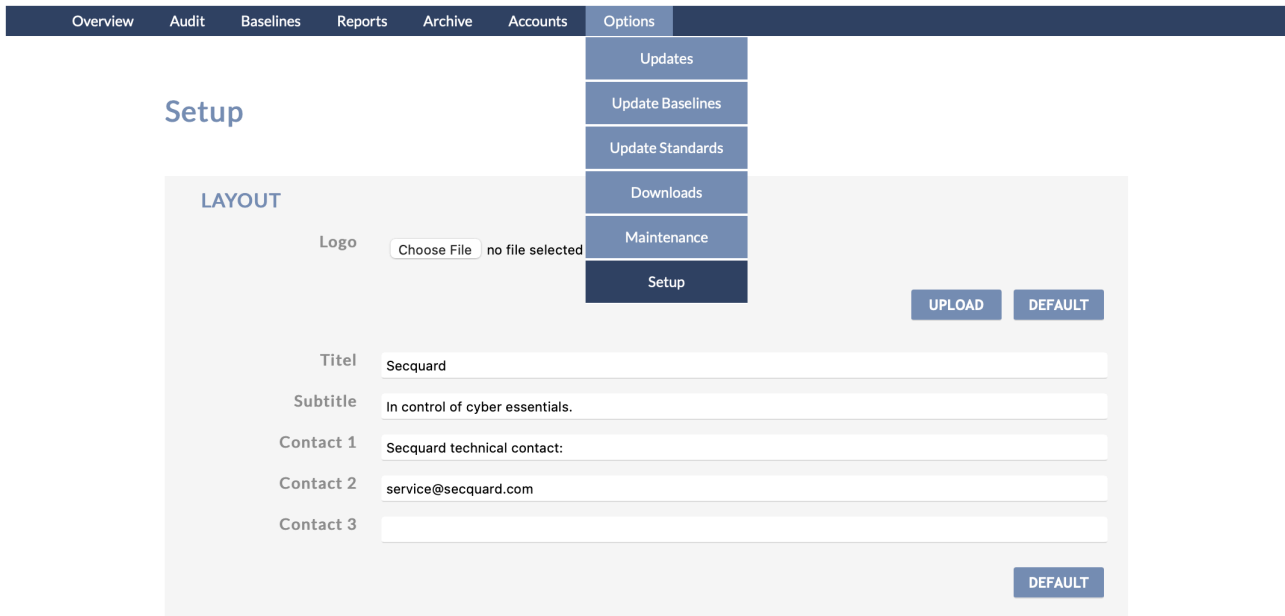
Defragment Over time and/or with large audit result sets database indices could become fragmented. Although Easy2Audit is doing defragmentation on the fly when required, here it could be enforced. A fragmentation above 30% heavily degrades performance.

PK_Cve2__C612B946C3AD3379	15.44%
PK_vuln_cve	0%

DEFRAGMENT

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.



Setup

LAYOUT

Logo no file selected

Titel

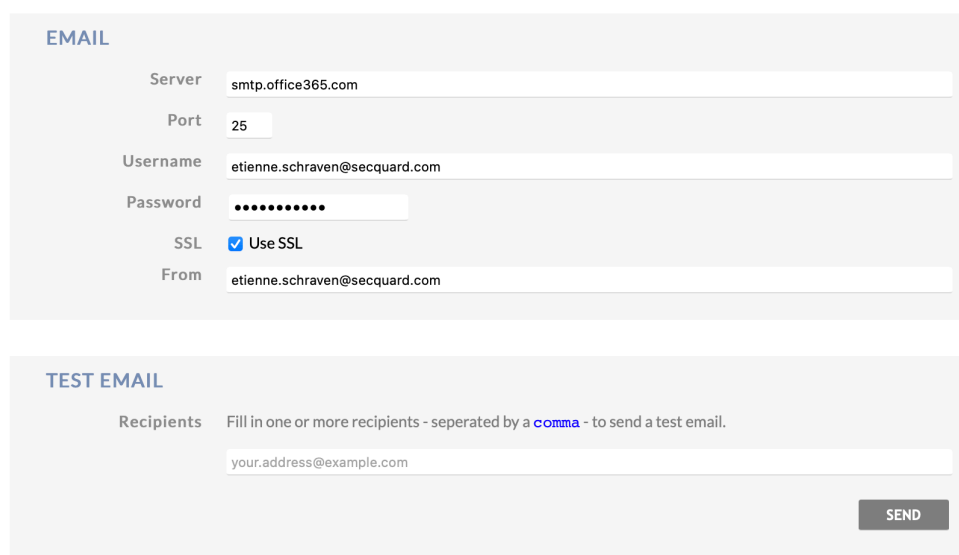
Subtitle

Contact 1

Contact 2

Contact 3

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



EMAIL

Server

Port

Username

Password

SSL Use SSL

From

TEST EMAIL

Recipients