Capture Security Appliance

Administration Guide

SONICWALL®

Contents

1

Introduction

This administration guide provides configuration information for the SonicWall® Capture Security Appliance.

Technical Overview - Capture ATP

To combat evasive and targeted malware, sandbox analysis is required to discover and stop unknown threats. SonicWall Capture Advanced Threat Protection (Capture ATP) is a cloud-based service that provides this type of file analysis.

Traditional network security technology detects known threats but cannot detect advanced threats like custom malware and zero-day exploits. To better detect unknown threats, security professionals are deploying advanced threat detection technologies, such as sandboxes, that analyze the behavior of suspicious files and uncover hidden malware. However, some organizations and agencies cannot send grey-listed files to cloud-based sandboxes for analysis and many on-premises sandboxing technologies are expensive and are prone to evasion tactics.

SonicWall Capture ATP uses a combination of reputation-based checks, static file analysis and SonicWall's patented Real-Time Deep Memory Inspection™ (RTDMI) engine for dynamic analysis to ensure that it provides not only the best possible detection rate of malicious files, but also does this efficiently, in the shortest possible time. The SonicWall ecosystem of security products, already fully integrated with the cloud-delivered Capture ATP analysis, is able to enforce inline security with features such as **Block Until Verdict**.

Technical Overview - Capture Security Appliance

The SonicWall Capture Security Appliance™ (CSa) brings Capture ATP and sandboxing malware analysis to on-premises deployment scenarios for customers with compliance and policy restrictions against sending files to cloud analysis, or who prefer that all of their data remain inside their organization. With many attack types only revealing their weaponry within memory, a memory-based approach is required to detect and stop attacks before they reach endpoints. Furthermore, cloud-based sandboxing engines can introduce latency while an on-premise solution can provide better performance.

The SonicWall Capture Security Appliance is an on-premises sandbox for SonicWall next-generation firewalls that enables you to inspect suspicious files within your data center using fast and accurate memory-based analysis to provide a strong layer of defense against advanced and targeted threats.

The Capture Security Appliance can analyze suspicious files coming from other SonicWall products to provide rapid, high accuracy detection of previously unseen threats, while the customer retains custody of their files. Additionally, the REST API functionality on the CSa opens up the benefits of this highly effective file analysis capability to threat intelligence teams, third-party security systems and any software stack that can integrate with published APIs.

To protect against the increasing dangers of unknown, zero-day threats, the Capture Security Appliance detects and optionally blocks unknown threats at the gateway until verdict. Equipped with Real-Time Deep Memory Inspection (RTDMI), the CSa can detect and stop attacks embedded in a wide range of file types by forcing malware to reveal its weaponry into memory.

The same capabilities available with the cloud-based SonicWall Capture ATP are supported when SonicWall firewalls and other products are connected to a Capture Security Appliance.

Capture Security Appliance Key Features

- Reputation & Global Verdict lookup (configurable)
- Static analysis & dynamic analysis with RTDMI
- Broad file type analysis
- Per-Source Rate Limiting
- Allow List/Block List on hash/domain
- Configurable scheduled reporting
- Logging & alerting
- Role-based administration (Pre-Configured roles)
- Management over HTTPS on a dedicated management interface or via the WAN network interface
- False positive & false negative reporting with automatic whitelist/blacklist
- Closed Network Operation
- REST API for device management and for file analysis
- Hardened OS with Secure Boot and chain of trust for anti-tampering

More details about certain features are provided in the next topics.

RTDMI

SonicWall’s patent-pending Real-Time Deep Memory Inspection (RTDMI) file analysis engine is a novel method of analyzing suspicious files by monitoring the behavior of an application in memory. RTDMI can see through any obfuscation or encryption techniques that modern malware might deploy to evade network and sandbox analysis, yielding extremely high accuracy detection of attacks borne by documents, executables, archive files and a variety of other file types.

Real-Time Protection and Block Until Verdict

The combination of reputation and global intelligence checks, static analysis and RTDMI technology operate in concert to deliver results quickly enough to enable technologies like **Block Until Verdict** in SonicWall products. This capability allows for a file inspection policy on the firewall to prevent suspicious files from being downloaded by the end-user until the full inspection is completed and a verdict is reached by the Capture Security Appliance.

Broad File Type Analysis

The SonicWall Capture Security Appliance supports analysis for a broad range of file types, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including Windows, Android, and multi-browser environments. Administrators can customize protection by selecting or excluding files to be sent for analysis, including by file type, file size, sender, recipient and protocol. In addition, administrators can manually submit files to the appliance for analysis.

PDF & MS Office File Detection

The PDF and MS Office capabilities defense against phishing emails containing these files.

The Capture Security Appliance analyzes documents dynamically via proprietary exploit detection technology along with static forms of inspection with the ability to detect many malicious document categories, including:

- Malicious Flash-based MS Office documents
- Dynamic Data Exchange (DDE) based exploits and malware inside Office files
- MS Office and PDF files containing malicious executables
- PDF documents containing MS Office malware
- Malevolent shellcode-based files
- Macro-based malicious files
- Malicious multi-layer files
- PDF documents with “JavaScript infectors”
- JavaScript-based exploits in PDF documents
- Files leading to phishing and malware hosting websites
- “Phishing style” malicious PDF documents leading to both phishing and malware hosting websites

Range of Allowed Input Devices

SonicWall firewalls, Email Security systems and a variety of API Connectors are supported.

Reporting, Analysis, Logging and Alerts

The Capture Security Appliance provides reports that detail the analysis results for files sent to the appliance including session information, operating system information and activity, network activity and a copy of the original file (based on privacy settings).

The CSa provides an insight into files submitted from all sources with an easy to navigate dashboard and file analysis history, providing an insight into the frequency, sources, verdicts and other insights around files submitted for analysis.

Reporting capabilities provide a global view into the ATP protection across the organization, with ability to schedule regular reports configured based on different roles.

Log alerts provide notification of suspicious files sent to the CSa and file analysis and verdict results.

User Roles and Administration

Administrators can grant granular access to the CSa to a variety of roles with the ability to restrict access to any part of the CSa web management interface.

Different user roles provide security and flexibility. For example:

- Security analysts can have access to the scanning history with ability to modify the whitelist/blacklist, allowed devices and report any suspected false positives or false negatives, but cannot make network configuration changes or upgrade firmware.
- Network-level administrators can be granted access to the operational configuration of the appliance while being restricted, for confidentiality reasons, from seeing the submitted files and their sources.

Deployment Options

SonicWall CSa deployment is quick and straightforward, requiring configuration of basic networking, reporting and allowed device access to get started. For initial setup and information about deployment options, refer to the *Capture Security Appliance Getting Started Guide*, available on https://www.sonicwall.com/support/technical-documentation.

The CSa is built to be IP-addressable and can therefore be deployed anywhere as long as it is reachable by devices that submit files for analysis.

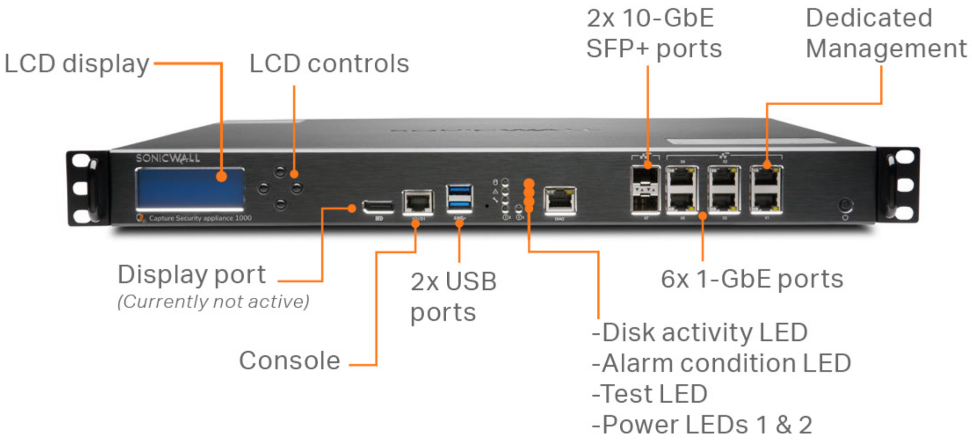
REST API Gateway

The Capture Security Appliance provides a REST API interface that can be used by API Connectors to submit files for analysis and query results by threat intelligence teams via their own scripts, web-portal integrations and other security products.

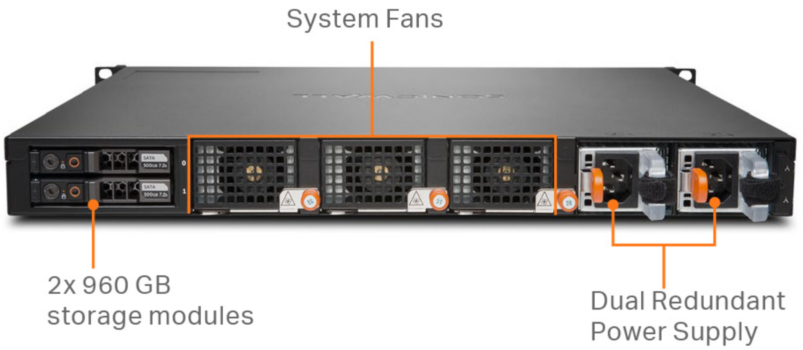
Instructions on how to get started with API scripting for the CSa and code samples are available at https://github.com/sonicwall. Details of the management and file submission APIs can be found in the user interface of the appliance.

CSa Hardware Overview

FRONT PANEL



REAR PANEL



The CSa includes two RAID disks that contain appliance data, as well as internal storage for the OS and maintenance.

The *Capture Security Appliance Getting Started Guide* also provides hardware information for the CSa.

ⓘ | **NOTE:** Console port serial settings: 115200/8/1/N/N

Essential Steps in Configuring the CSa

For details on setting up the CSa, go to https://www.sonicwall.com/support/technical-documentation and search for:

- *Capture Security Appliance Getting Started Guide*

Basic steps for configuring a CSa are summarized below:

1. Change default password — see Configuring Users
2. Set up networking (critical, does not operate otherwise) — see Network Configuration
3. Register & License (critical, does not operate otherwise) — see Registration / Licensing
4. Update Firmware (highly recommended) — see Firmware Management
5. Add allowed devices (critical, does not operate otherwise) — see Allowed Devices
6. Add users and set up roles — see Configuring Users
7. Set up reporting — see Reporting

2

Dashboard Overview

The two dashboards present subscreens summarizing CSa system status:

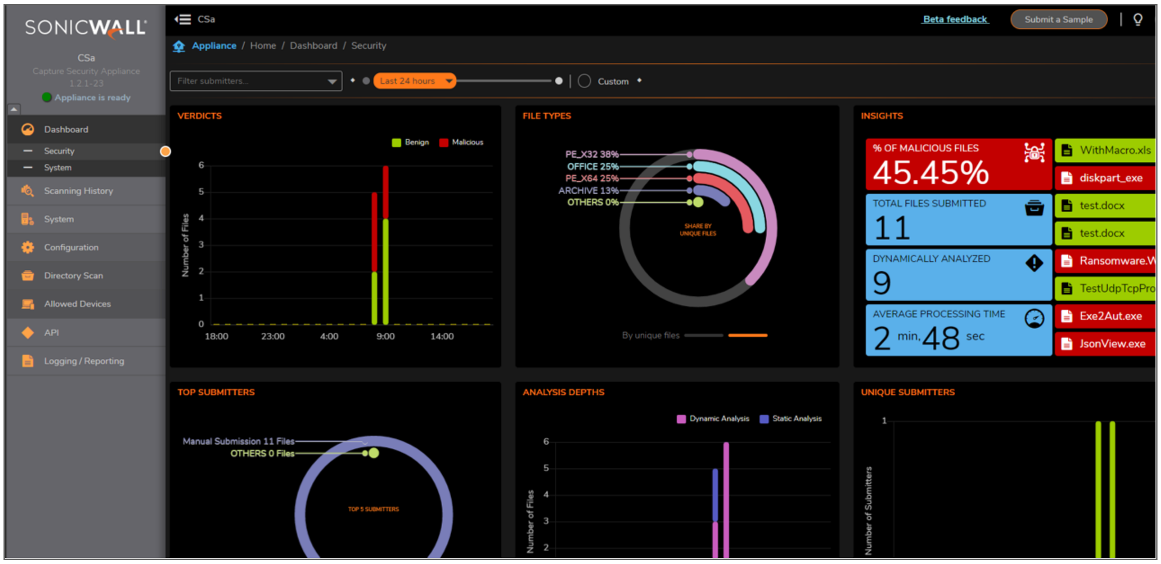
- Dashboard Overview
- Dashboard Overview

Security Dashboard

The **Security** dashboard provides an overview of the files submitted to the CSa, their origin, verdict, scan depth, and patterns over time. Filters set at the upper left of the display allow focus on specific file submitters, or time periods, including custom dates and times.

Security:

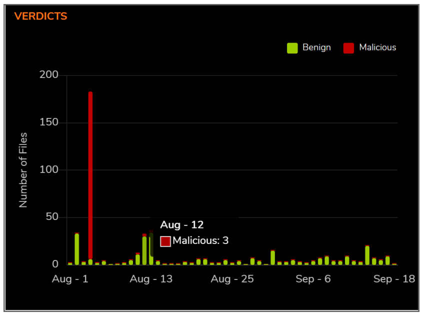
- Verdicts
- File Types
- Insights
- Top Submitters
- Analysis Depths
- Attack Origins
- Unique Submitters
- Files by Submitters



Verdicts

The **Verdicts** display summarizes the outcome of sandbox decisions made on files over the defined period from the specified sources.

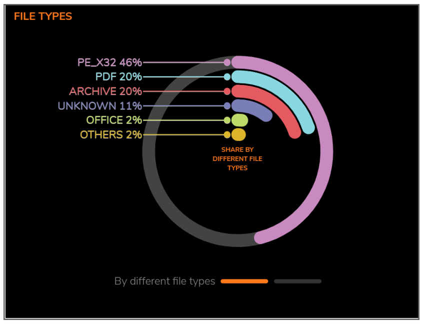
ⓘ | **NOTE:** Hover your mouse over a bar to get specific **Benign** and **Malicious** numbers.



File Types

In this instance, all the traffic to the sandbox falls into six groups.

ⓘ | **NOTE:** Click the bars at the bottom of the display to show the percentage of files of a particular type, or the percentage of unique files falling into each group.

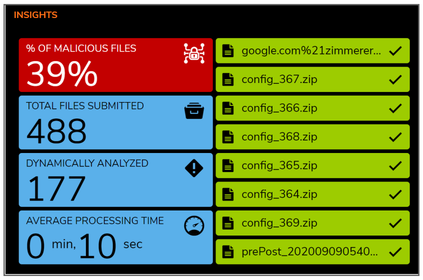


Insights

The **Insights** panel highlights sandbox operations over the defined period.

Dynamically Analyzed tells how many files the sandbox detonates.

Click any panel in this display for further data organized for analysis. The files shown here are the last files submitted in the currently selected time period. The statistics shown represent the time period currently selected.



INSIGHTS

% OF MALICIOUS FILES
39%

TOTAL FILES SUBMITTED
488

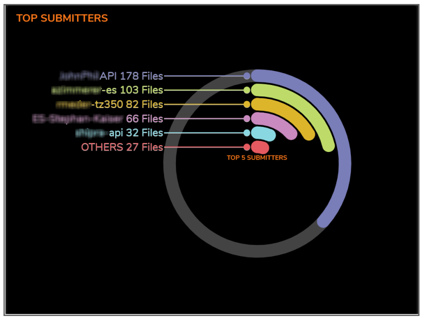
DYNAMICALLY ANALYZED
177

AVERAGE PROCESSING TIME
0 min, 10 sec

- google.com%21zimmerer... ✓
- config_367.zip ✓
- config_366.zip ✓
- config_368.zip ✓
- config_365.zip ✓
- config_364.zip ✓
- config_369.zip ✓
- prePost_202009090540... ✓

Top Submitters

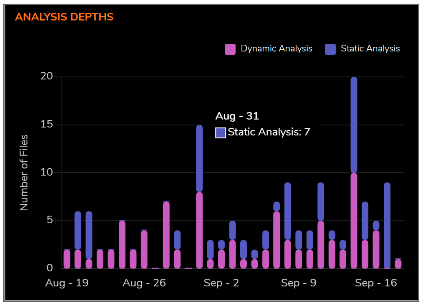
This display shows the top five sources of submitted files.



Analysis Depths

This display contrasts the number of files requiring Static Analysis (pattern checking, signature comparison) as opposed to Dynamic Analysis (execution).

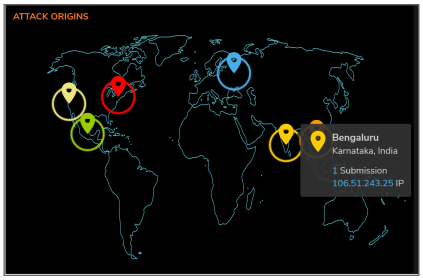
ⓘ | **NOTE:** Hover over the bars to view specific numbers.



Attack Origins

This maps the source locations of the files sent to the sandbox. These are the locations of the submitters.

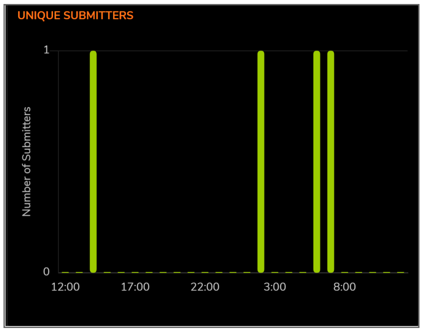
ⓘ | **NOTE:** Hover over the marker for details on source geo-location, number of submissions, and IP address.



Unique Submitters

This table shows the number of unique sources of files for analysis across a particular time horizon.

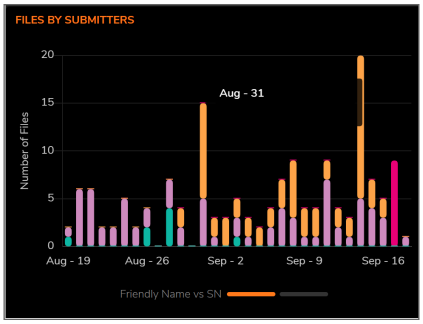
ⓘ | **NOTE:** Hover over the bar to reveal specific numbers.



Files by Submitters

This display shows patterns in submissions among firewalls, email security systems, and API sources. This display is useful in determining whether the volume of files is coming from a single submitter, or is gradually split.

ⓘ | **NOTE:** Hover over a line segment for details on the submission source.

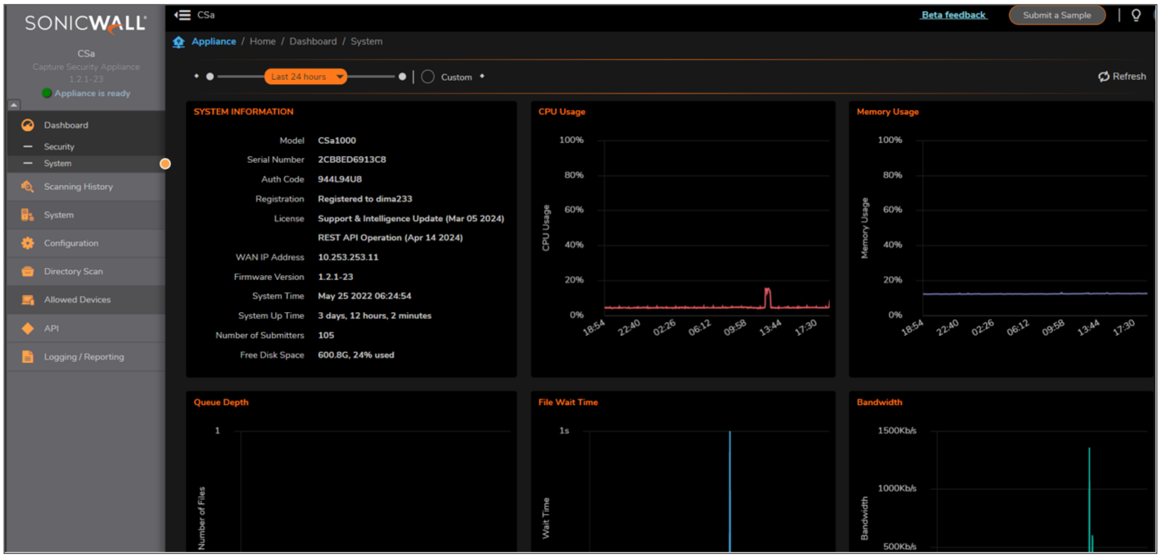


System Dashboard

The **System** dashboard is concerned with the health of the device. This page presents key information on device utilization, licensing status, firmware version, up time, disk space utilization, and so on.

System:

- System Information
- Memory Usage
- CPU Usage
- Queue Depth
- File Wait Time
- Bandwidth



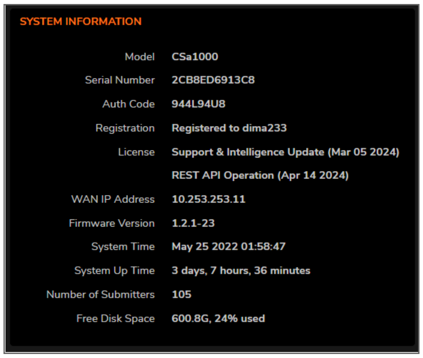
SYSTEM INFORMATION

Model	CSa1000
Serial Number	2CB8ED6913C8
Auth Code	944L94U8
Registration	Registered to dima233
License	Support & Intelligence Update (Mar 05 2024) REST API Operation (Apr 14 2024)
WAN IP Address	10.253.253.11
Firmware Version	1.2.1-23
System Time	May 25 2022 06:24:54
System Up Time	3 days, 12 hours, 2 minutes
Number of Submitters	105
Free Disk Space	600.8G, 24% used

The **System** dashboard allows filtering by source of submissions, time scale and reporting period, including custom dates and times. The results of filtering are displayed across all of the sub-screens.

System Information

This display presents basic system status information.



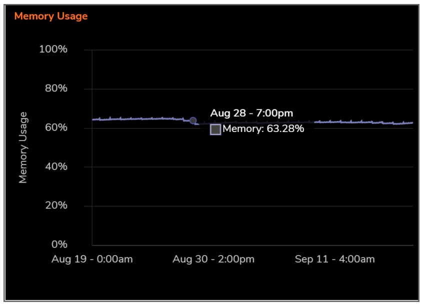
SYSTEM INFORMATION

Model	CSa1000
Serial Number	2CB8ED6913C8
Auth Code	944L94U8
Registration	Registered to dima233
License	Support & Intelligence Update (Mar 05 2024) REST API Operation (Apr 14 2024)
WAN IP Address	10.253.253.11
Firmware Version	1.2.1-23
System Time	May 25 2022 01:58:47
System Up Time	3 days, 7 hours, 36 minutes
Number of Submitters	105
Free Disk Space	600.8G, 24% used

Memory Usage

This display shows the percentage memory utilization over time by the CSa.

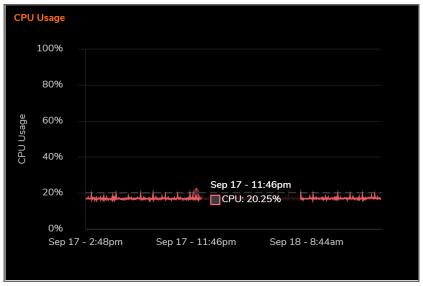
ⓘ | **NOTE:** Hover over the line to get specific numbers.



CPU Usage

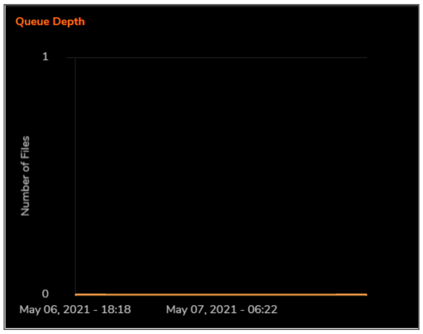
This display shows patterns in CPU utilization over time.

ⓘ | **NOTE:** Hover over the utilization line to get specific times and percentage utilization numbers.



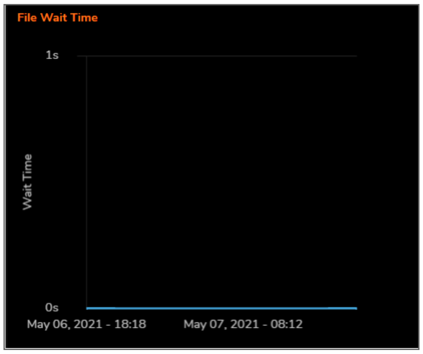
Queue Depth

This display shows the queue depth.



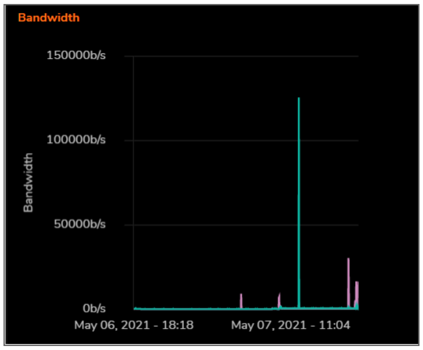
File Wait Time

This display shows the file wait time.



Bandwidth

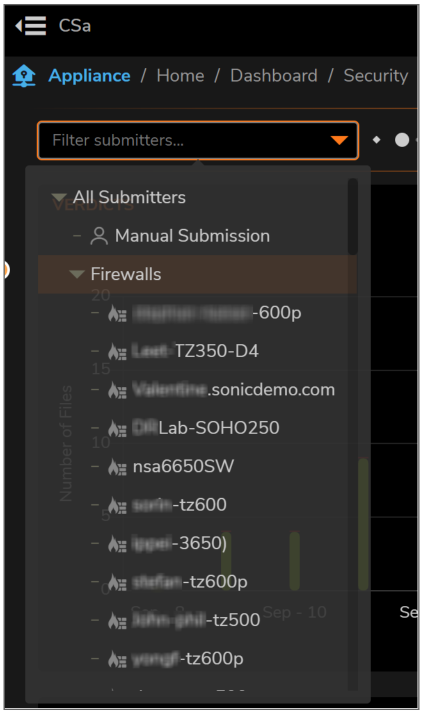
This display shows the bandwidth.



Filter by Source of Submission

All dashboards can be filtered by the source of submission. Source can be either individual devices or device classes such as firewalls or API sources. This allows selection of the sources of sandbox operations. For example, only the results of submissions from firewalls as opposed to email servers may be displayed. This filtering is applied across of the sub-displays on the **Security Dashboard**.

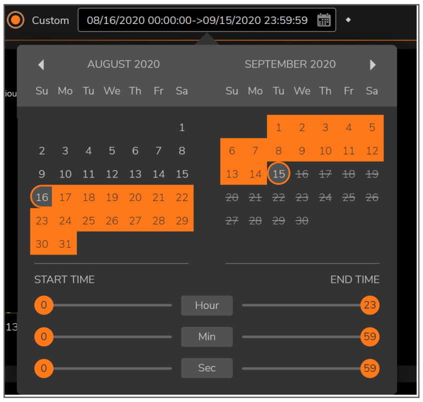
Setting up Filter by Source



Filter by Custom Period

Click **Custom** to define a specific period by which to filter.

Setting Custom Period

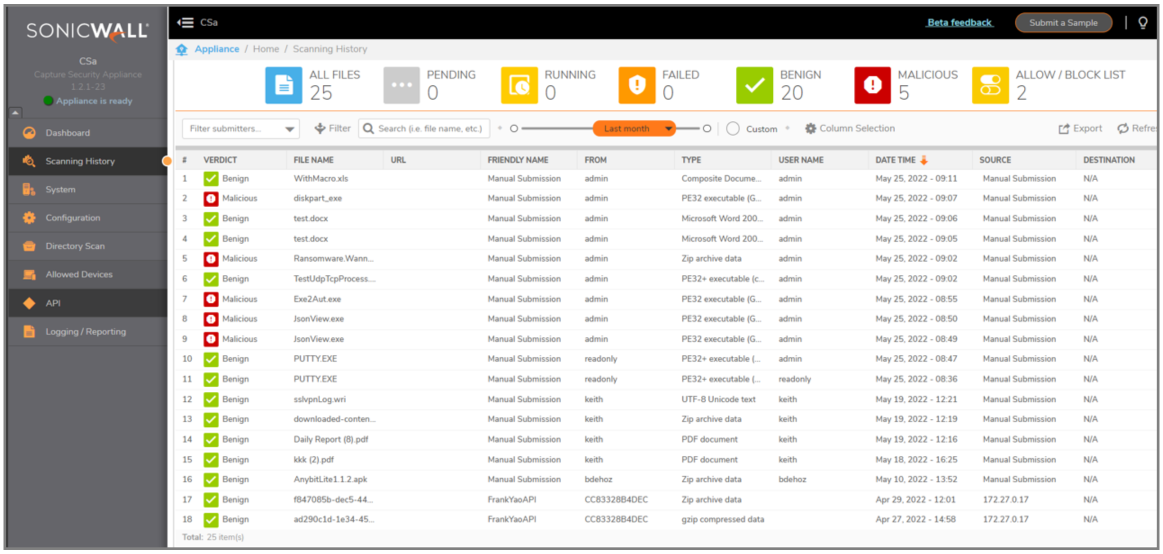

Custom 08/16/2020 00:00:00->09/15/2020 23:59:59

3

Scanning History

Here you can search and filter reports on sandbox operations based on existing file names or submission sources.

Filtering Reports

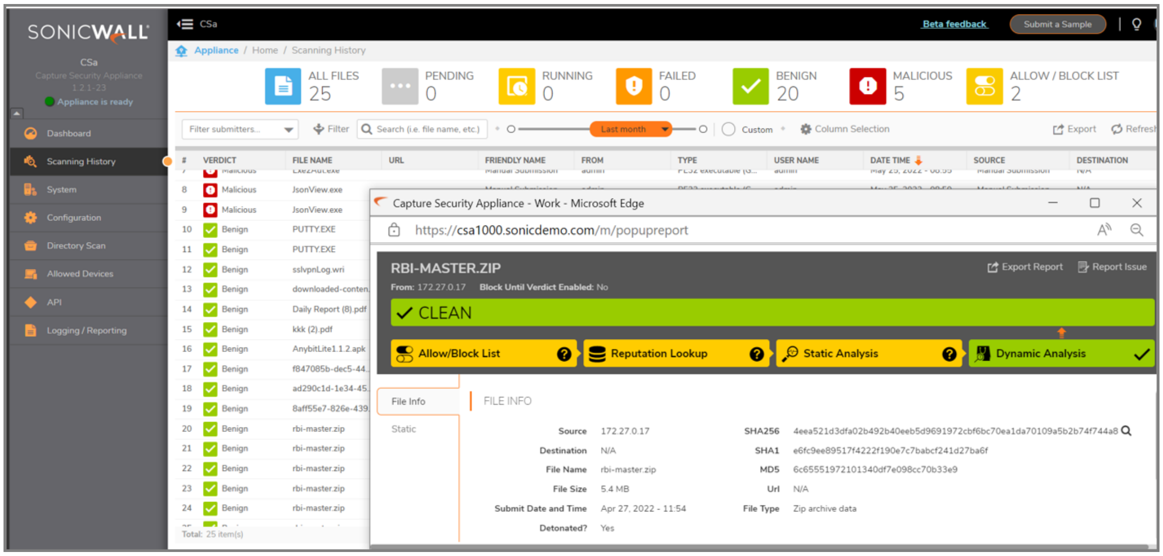


#	VERDICT	FILE NAME	URL	FRIENDLY NAME	FROM	TYPE	USER NAME	DATE TIME	SOURCE	DESTINATION
1	✓ Benign	WithMacro.xls		Manual Submission	admin	Composite Docume...	admin	May 25, 2022 - 09:11	Manual Submission	N/A
2	! Malicious	diskpart_exe		Manual Submission	admin	PE32 executable (G...	admin	May 25, 2022 - 09:07	Manual Submission	N/A
3	✓ Benign	test.docx		Manual Submission	admin	Microsoft Word 200...	admin	May 25, 2022 - 09:06	Manual Submission	N/A
4	✓ Benign	test.docx		Manual Submission	admin	Microsoft Word 200...	admin	May 25, 2022 - 09:05	Manual Submission	N/A
5	! Malicious	Ransomware.Wann...		Manual Submission	admin	Zip archive data	admin	May 25, 2022 - 09:02	Manual Submission	N/A
6	✓ Benign	TestUdpTcpProcess....		Manual Submission	admin	PE32+ executable (c...	admin	May 25, 2022 - 09:02	Manual Submission	N/A
7	! Malicious	Exe2Aut.exe		Manual Submission	admin	PE32 executable (G...	admin	May 25, 2022 - 08:55	Manual Submission	N/A
8	! Malicious	JsonView.exe		Manual Submission	admin	PE32 executable (G...	admin	May 25, 2022 - 08:50	Manual Submission	N/A
9	! Malicious	JsonView.exe		Manual Submission	admin	PE32 executable (G...	admin	May 25, 2022 - 08:49	Manual Submission	N/A
10	✓ Benign	PUTTY.EXE		Manual Submission	readonly	PE32+ executable (...	admin	May 25, 2022 - 08:47	Manual Submission	N/A
11	✓ Benign	PUTTY.EXE		Manual Submission	readonly	PE32+ executable (...	readonly	May 25, 2022 - 08:36	Manual Submission	N/A
12	✓ Benign	sslvpnLog.wri		Manual Submission	keith	UTF-8 Unicode text	keith	May 19, 2022 - 12:21	Manual Submission	N/A
13	✓ Benign	downloaded-conten...		Manual Submission	keith	Zip archive data	keith	May 19, 2022 - 12:19	Manual Submission	N/A
14	✓ Benign	Daily Report (8).pdf		Manual Submission	keith	PDF document	keith	May 19, 2022 - 12:16	Manual Submission	N/A
15	✓ Benign	kkk (2).pdf		Manual Submission	keith	PDF document	keith	May 18, 2022 - 16:25	Manual Submission	N/A
16	✓ Benign	AnybitLite1.1.2.apk		Manual Submission	bdehoz	Zip archive data	bdehoz	May 10, 2022 - 13:52	Manual Submission	N/A
17	✓ Benign	f847085b-dec5-44...		FrankYaoAPI	CC83328B4DEC	Zip archive data		Apr 29, 2022 - 12:01	172.27.0.17	N/A
18	✓ Benign	ad290c1d-1e34-45...		FrankYaoAPI	CC83328B4DEC	gzip compressed data		Apr 27, 2022 - 14:58	172.27.0.17	N/A

Total: 25 item(s)

To view and export reports:

1. Double click on a report row and a report summary appears.
2. Click **Export** to download the report to your PC.



#	VERDICT	FILE NAME
8	Malicious	JsonView.exe
9	Malicious	JsonView.exe
10	Benign	PUTTY.EXE
11	Benign	PUTTY.EXE
12	Benign	sslvpnLog.wri
13	Benign	downloaded-conten...
14	Benign	Daily Report (8).pdf
15	Benign	kkk (2).pdf
16	Benign	AnybitLite1.1.2.apk
17	Benign	f847085b-dec5-44...
18	Benign	ad290c1d-1e34-45...
19	Benign	8aff55e7-826e-439...
20	Benign	rbi-master.zip
21	Benign	rbi-master.zip
22	Benign	rbi-master.zip
23	Benign	rbi-master.zip
24	Benign	rbi-master.zip

Total: 25 item(s)

RBI-MASTER.ZIP

From: 172.27.0.17 **Block Until Verdict Enabled:** No

✓ CLEAN

FILE INFO

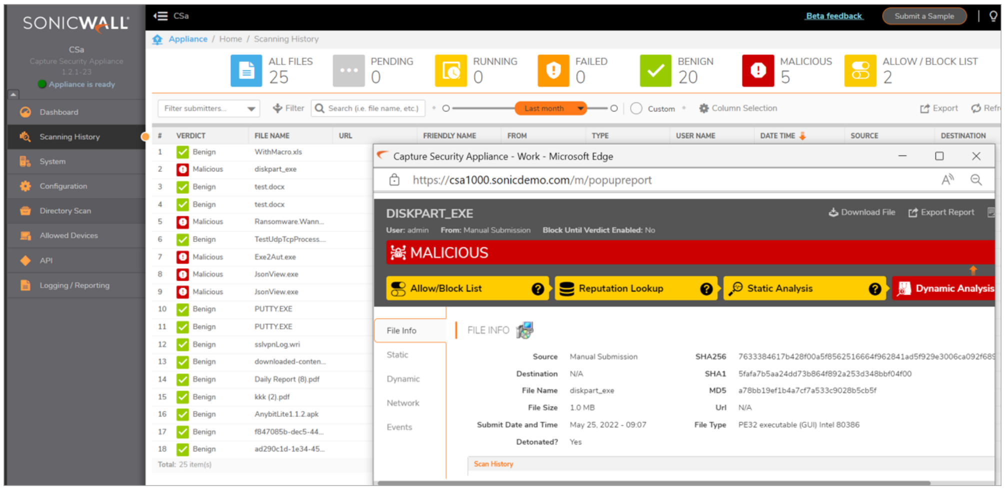
Source	172.27.0.17	**SHA256**	4eea521d3dfa02b492b40eeb5d9691972cbf6bc70ea1da70109a5b2b74f744a8
Destination	N/A	**SHA1**	e6fc9ee89517f4222f190e7c7babcf241d27ba6f
File Name	rbi-master.zip	**MD5**	6c65551972101340df7e098cc70b33e9
File Size	5.4 MB	**Url**	N/A
Submit Date and Time	Apr 27, 2022 - 11:54	**File Type**	Zip archive data
Detonated?	Yes		

3. Click **Report Issue** to report false positives.

Reading Report Summaries

The green color indicates a benign verdict, red, a malicious verdict. Amber indicates a black or whitelist decision. The heading of the report summary indicates at which stage the verdict was made.

Deep Report for Malicious File



ALL FILES 25 | PENDING 0 | RUNNING 0 | FAILED 0 | BENIGN 20 | MALICIOUS 5 | ALLOW / BLOCK LIST 2

#	VERDICT	FILE NAME	URL	FRIENDLY NAME	FROM	TYPE	USER NAME	DATE TIME	SOURCE	DESTINATION
1	Benign	WithMacro.xls								
2	Malicious	diskpart_exe								
3	Benign	test.docx								
4	Benign	test.docx								
5	Malicious	Ransomware.Wann...								
6	Benign	TestUdpTcpProcess....								
7	Malicious	Exe2Aut.exe								
8	Malicious	JsonView.exe								
9	Malicious	JsonView.exe								
10	Benign	PUTTY.EXE								
11	Benign	PUTTY.EXE								
12	Benign	sslvpnLog.wri								
13	Benign	downloaded-conten...								
14	Benign	Daily Report (8).pdf								
15	Benign	kkk (2).pdf								
16	Benign	AnybitLite1.1.2.apk								
17	Benign	f847085b-dec5-44...								
18	Benign	ad290c1d-1e34-45...								

Total: 25 item(s)

Capture Security Appliance - Work - Microsoft Edge

https://csa1000.sonicdemo.com/m/popupreport

DISKPART_EXE

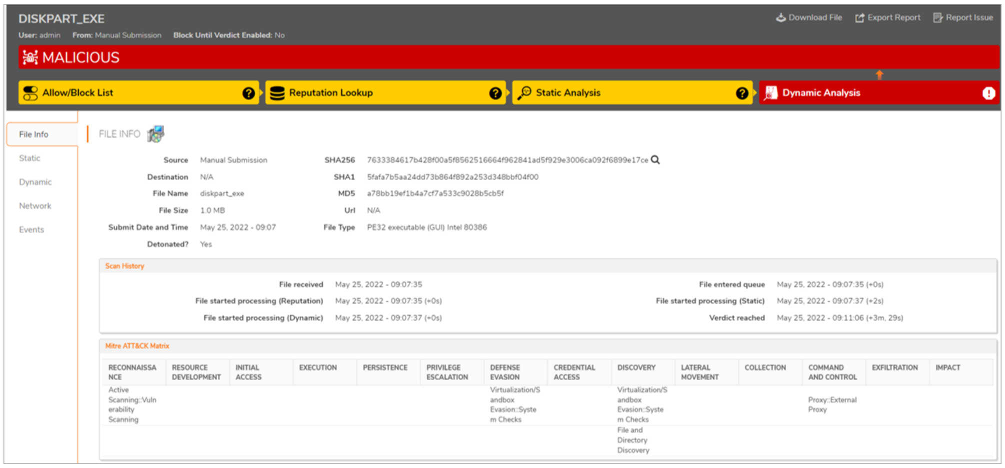
User: admin **From:** Manual Submission **Block Until Verdict Enabled:** No

MALICIOUS

FILE INFO

Source	Manual Submission	SHA256	7633384617b428f00a5f8562516664f962841ad5f929e3006ca092f689
Destination	N/A	SHA1	5fafa7b5aa24dd73b864f892a253d348bbf04f00
File Name	diskpart_exe	MD5	a78bb19ef1b4a7cf7a533c9028b5cb5f
File Size	1.0 MB	Url	N/A
Submit Date and Time	May 25, 2022 - 09:07	File Type	PE32 executable (GUI) Intel 80386
Detonated?	Yes		

Scan History



DISKPART_EXE

User: admin **From:** Manual Submission **Block Until Verdict Enabled:** No

MALICIOUS

FILE INFO

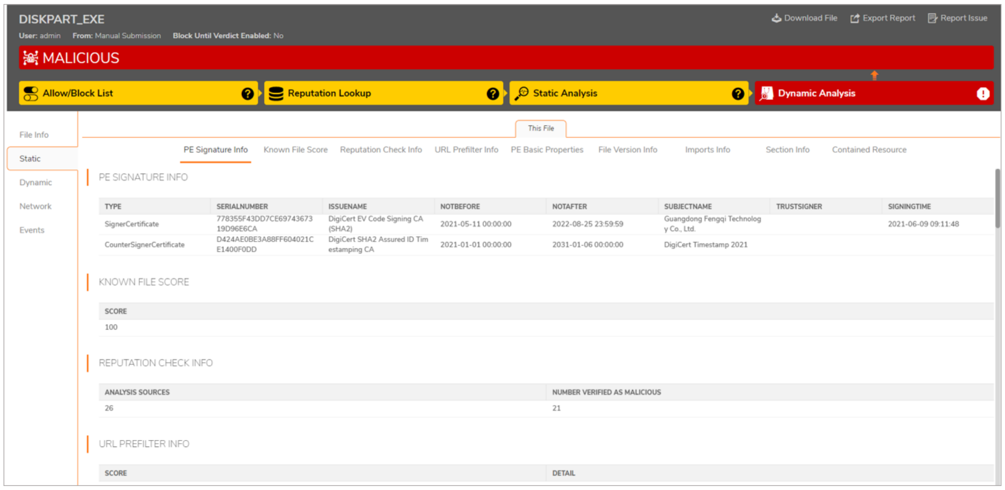
Source	Manual Submission	SHA256	7633384617b428f00a5f8562516664f962841ad5f929e3006ca092f6899e17ce
Destination	N/A	SHA1	5fafa7b5aa24dd73b864f892a253d348bbf04f00
File Name	diskpart_exe	MD5	a78bb19ef1b4a7cf7a533c9028b5cb5f
File Size	1.0 MB	Url	N/A
Submit Date and Time	May 25, 2022 - 09:07	File Type	PE32 executable (GUI) Intel 80386
Detonated?	Yes		

Scan History

File received	May 25, 2022 - 09:07:35	File entered queue	May 25, 2022 - 09:07:35 (+0s)
File started processing (Reputation)	May 25, 2022 - 09:07:35 (+0s)	File started processing (Static)	May 25, 2022 - 09:07:37 (+2s)
File started processing (Dynamic)	May 25, 2022 - 09:07:37 (+0s)	Verdict reached	May 25, 2022 - 09:11:06 (+3m, 29s)

Mitre ATT&CK Matrix

RECONNAISSANCE	RESOURCE DEVELOPMENT	INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND AND CONTROL	EXFILTRATION	IMPACT
Active Scanning::Vulnerability Scanning						Virtualization/Sandbox Evasion::System Checks		Virtualization/Sandbox Evasion::System Checks			Proxy::External Proxy		
								File and Directory Discovery					



DISKPART_EXE

User: admin **From:** Manual Submission **Block Until Verdict Enabled:** No

PE SIGNATURE INFO

TYPE	SERIALNUMBER	ISSUENAME	NOTBEFORE	NOTAFTER	SUBJECTNAME	TRUSTSIGNER	SIGNINGTIME
SignerCertificate	778355F43DD7CE69743673 19D96E6CA	DigiCert EV Code Signing CA (SHA2)	2021-05-11 00:00:00	2022-08-25 23:59:59	Guangdong Fengqi Technolog y Co., Ltd.		2021-06-09 09:11:48
CounterSignerCertificate	D424AE0BE3A88FF604021C E1400F0DD	DigiCert SHA2 Assured ID Tim estamping CA	2021-01-01 00:00:00	2031-01-06 00:00:00	DigiCert Timestamp 2021		

KNOWN FILE SCORE

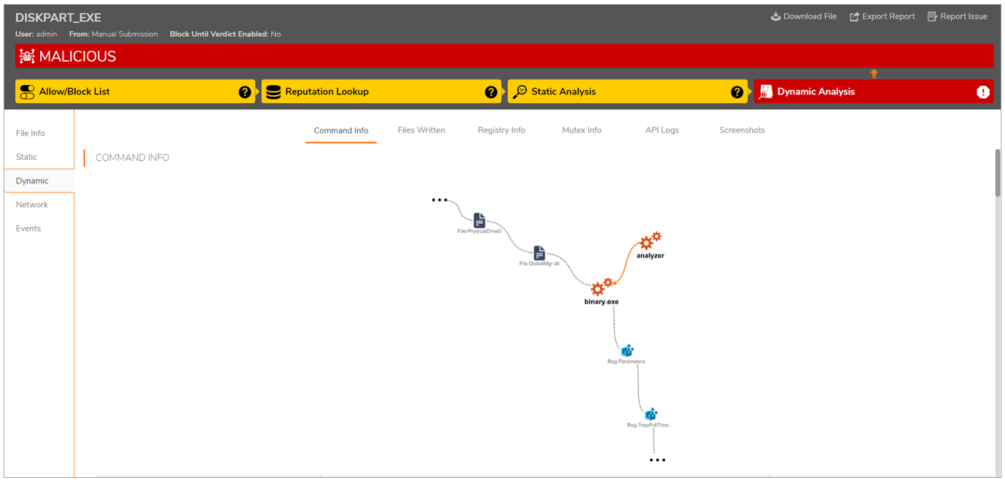
SCORE
100

REPUTATION CHECK INFO

ANALYSIS SOURCES	NUMBER VERIFIED AS MALICIOUS
26	21

URL PREFILTER INFO

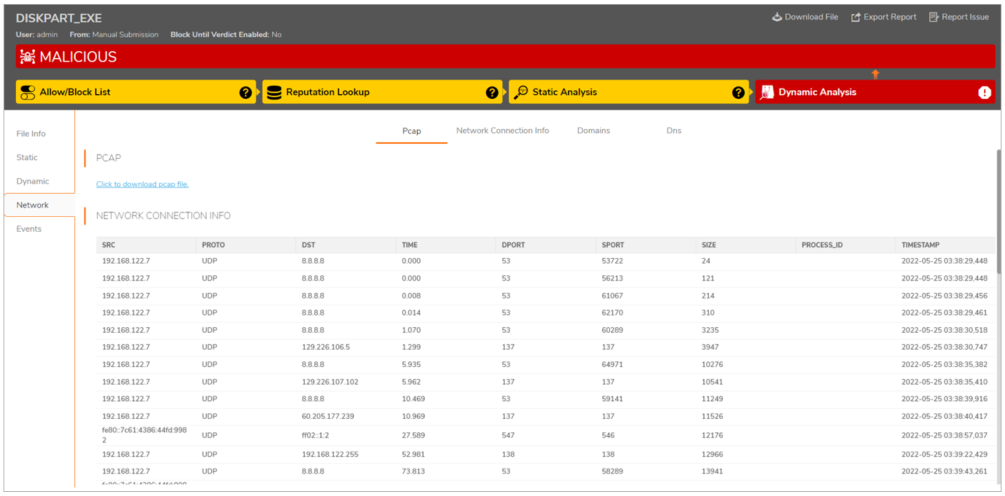
SCORE	DETAIL



DISKPART_EXE

User: admin **From:** Manual Submission **Block Until Verdict Enabled:** No

COMMAND INFO



DISKPART_EXE

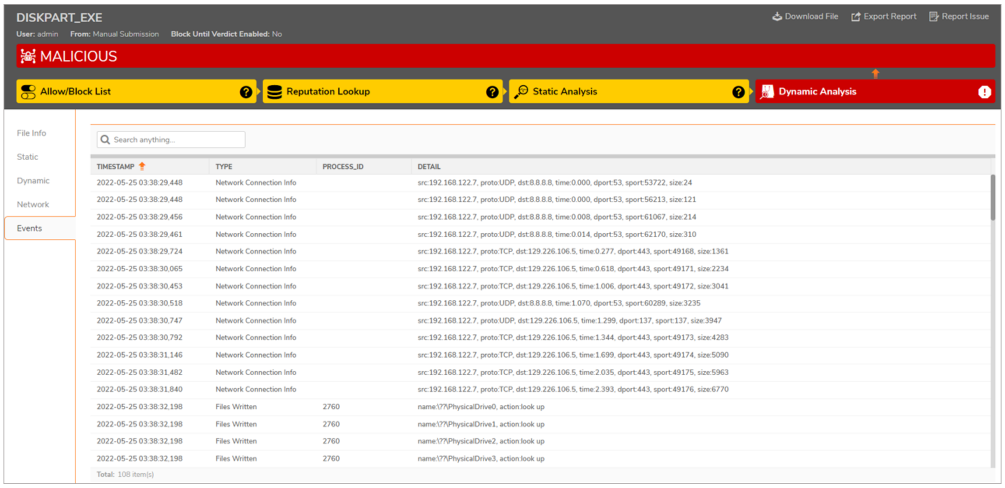
User: admin **From:** Manual Submission **Block Until Verdict Enabled:** No

PCAP

Click to download pcap file.

NETWORK CONNECTION INFO

SRC	PROTO	DST	TIME	DPORT	SPORT	SIZE	PROCESS_ID	TIMESTAMP
192.168.122.7	UDP	8.8.8.8	0.000	53	53722	24		2022-05-25 03:38:29,448
192.168.122.7	UDP	8.8.8.8	0.000	53	56213	121		2022-05-25 03:38:29,448
192.168.122.7	UDP	8.8.8.8	0.008	53	61067	214		2022-05-25 03:38:29,456
192.168.122.7	UDP	8.8.8.8	0.014	53	62170	310		2022-05-25 03:38:29,461
192.168.122.7	UDP	8.8.8.8	1.070	53	60289	3235		2022-05-25 03:38:30,518
192.168.122.7	UDP	129.226.106.5	1.299	137	137	3947		2022-05-25 03:38:30,747
192.168.122.7	UDP	8.8.8.8	5.935	53	64971	10276		2022-05-25 03:38:35,382
192.168.122.7	UDP	129.226.107.102	5.962	137	137	10541		2022-05-25 03:38:35,410
192.168.122.7	UDP	8.8.8.8	10.469	53	59141	11249		2022-05-25 03:38:39,916
192.168.122.7	UDP	60.205.177.239	10.969	137	137	11526		2022-05-25 03:38:40,417
fe80::7c61:4386:44fd:998 2	UDP	ff02::1:2	27.589	547	546	12176		2022-05-25 03:38:57,037
192.168.122.7	UDP	192.168.122.255	52.981	138	138	12966		2022-05-25 03:39:22,429
192.168.122.7	UDP	8.8.8.8	73.813	53	58289	13941		2022-05-25 03:39:43,261



DISKPART_EXE

User: admin **From:** Manual Submission **Block Until Verdict Enabled:** No

TIMESTAMP	TYPE	PROCESS_ID	DETAIL
2022-05-25 03:38:29,448	Network Connection Info		src:192.168.122.7, proto:UDP, dst:8.8.8.8, time:0.000, dport:53, sport:53722, size:24
2022-05-25 03:38:29,448	Network Connection Info		src:192.168.122.7, proto:UDP, dst:8.8.8.8, time:0.000, dport:53, sport:56213, size:121
2022-05-25 03:38:29,456	Network Connection Info		src:192.168.122.7, proto:UDP, dst:8.8.8.8, time:0.008, dport:53, sport:61067, size:214
2022-05-25 03:38:29,461	Network Connection Info		src:192.168.122.7, proto:UDP, dst:8.8.8.8, time:0.014, dport:53, sport:62170, size:310
2022-05-25 03:38:29,724	Network Connection Info		src:192.168.122.7, proto:TCP, dst:129.226.106.5, time:0.277, dport:443, sport:49168, size:1361
2022-05-25 03:38:30,065	Network Connection Info		src:192.168.122.7, proto:TCP, dst:129.226.106.5, time:0.618, dport:443, sport:49171, size:2234
2022-05-25 03:38:30,453	Network Connection Info		src:192.168.122.7, proto:TCP, dst:129.226.106.5, time:1.006, dport:443, sport:49172, size:3041
2022-05-25 03:38:30,518	Network Connection Info		src:192.168.122.7, proto:UDP, dst:8.8.8.8, time:1.070, dport:53, sport:60289, size:3235
2022-05-25 03:38:30,747	Network Connection Info		src:192.168.122.7, proto:UDP, dst:129.226.106.5, time:1.299, dport:137, sport:137, size:3947
2022-05-25 03:38:30,792	Network Connection Info		src:192.168.122.7, proto:TCP, dst:129.226.106.5, time:1.344, dport:443, sport:49173, size:4283
2022-05-25 03:38:31,146	Network Connection Info		src:192.168.122.7, proto:TCP, dst:129.226.106.5, time:1.699, dport:443, sport:49174, size:5090
2022-05-25 03:38:31,482	Network Connection Info		src:192.168.122.7, proto:TCP, dst:129.226.106.5, time:2.035, dport:443, sport:49175, size:5963
2022-05-25 03:38:31,840	Network Connection Info		src:192.168.122.7, proto:TCP, dst:129.226.106.5, time:2.393, dport:443, sport:49176, size:6770
2022-05-25 03:38:32,198	Files Written	2760	name:\??\PhysicalDrive0, action:look up
2022-05-25 03:38:32,198	Files Written	2760	name:\??\PhysicalDrive1, action:look up
2022-05-25 03:38:32,198	Files Written	2760	name:\??\PhysicalDrive2, action:look up
2022-05-25 03:38:32,198	Files Written	2760	name:\??\PhysicalDrive3, action:look up

Total: 108 item(s)

4

System

The **System** section of the CSa local web management interface includes support for system utilities:

- Registration / Licensing
- Firmware Management
- Configuration Backup
- Restart / Shutdown

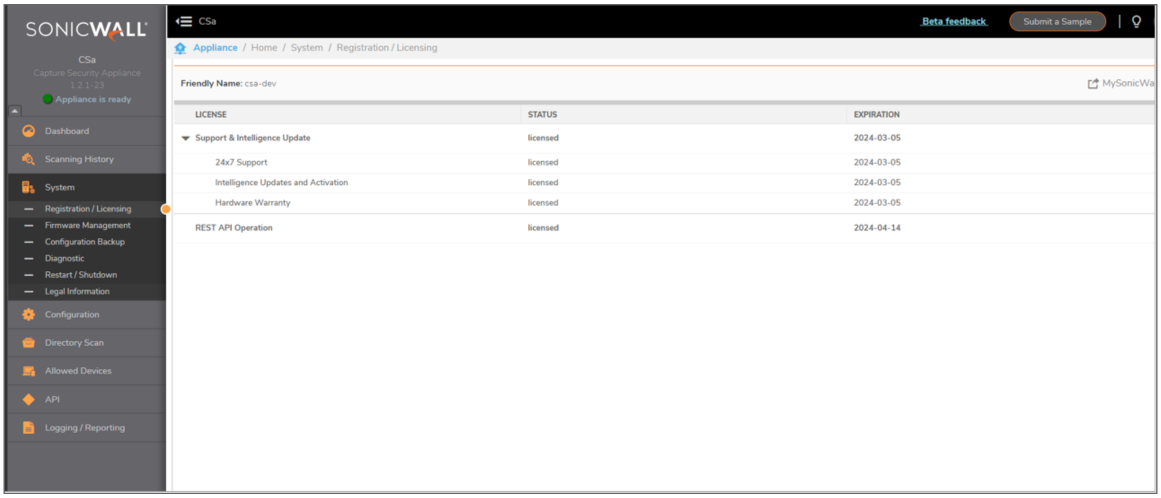
Registration / Licensing

Unless registration is complete, as shown below, you are prompted to provide license identification.

Licensing is mandatory in order for the device to operate.

The CSa must be registered at MySonicWall first, and then the administrator enters their MySonicWall account credentials into the CSa web management interface so that the appliance can synchronize with the license server.

LICENSING INFORMATION

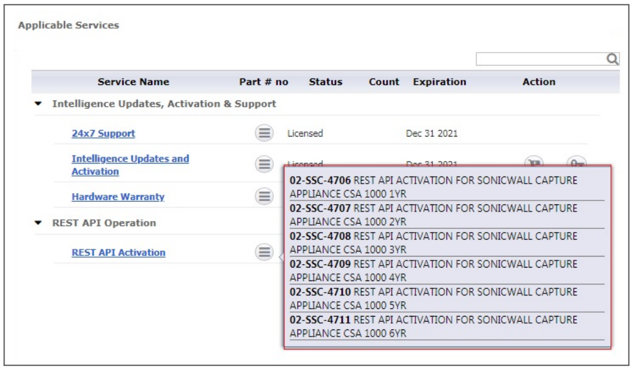


Friendly Name: csa-dev

LICENSE	STATUS	EXPIRATION
Support & Intelligence Update	licensed	2024-03-05
24x7 Support	licensed	2024-03-05
Intelligence Updates and Activation	licensed	2024-03-05
Hardware Warranty	licensed	2024-03-05
REST API Operation	licensed	2024-04-14

REST API OPERATION LICENSING

ⓘ **NOTE:** REST API Operations require a separate Standalone API license. There are six variations available a MySonicWall.


Applicable Services

Service Name	Part # no	Status	Count	Expiration	Action
Intelligence Updates, Activation & Support					
24x7 Support		Licensed		Dec 31 2021	
Intelligence Updates and Activation		Licensed		Dec 31 2021	
Hardware Warranty					
REST API Operation					
REST API Activation					

02-SSC-4706 REST API ACTIVATION FOR SONICWALL CAPTURE APPLIANCE CSA 1000 1YR
02-SSC-4707 REST API ACTIVATION FOR SONICWALL CAPTURE APPLIANCE CSA 1000 2YR
02-SSC-4708 REST API ACTIVATION FOR SONICWALL CAPTURE APPLIANCE CSA 1000 3YR
02-SSC-4709 REST API ACTIVATION FOR SONICWALL CAPTURE APPLIANCE CSA 1000 4YR
02-SSC-4710 REST API ACTIVATION FOR SONICWALL CAPTURE APPLIANCE CSA 1000 5YR
02-SSC-4711 REST API ACTIVATION FOR SONICWALL CAPTURE APPLIANCE CSA 1000 6YR

Firmware Management

This screen displays the current firmware level and supports easy upgrade or downgrade.

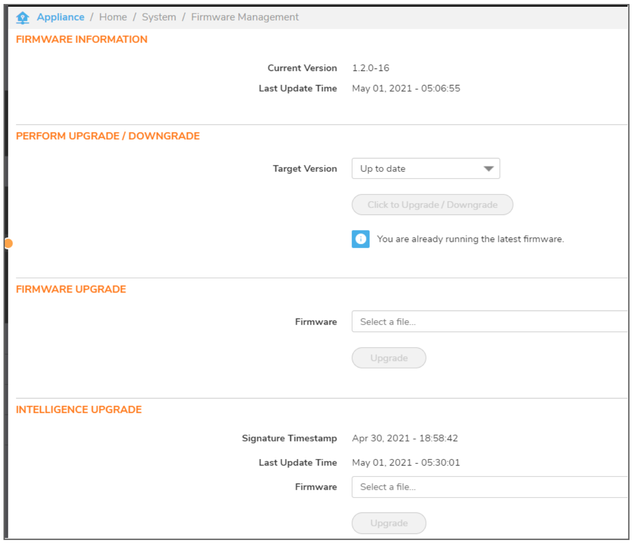
Upgrade / Downgrade Firmware

In the **Firmware Information** section, you can see the current software version running on your appliance. You can upgrade to a newer version, or downgrade your version by selecting the firmware version from the **Target Version** and then clicking, **Click to Upgrade/Downgrade**.

In the **Firmware Upgrade** section, you can manually upgrade firmware when you are working on a closed network environment.

In the **Intelligence Upgrade** section, you can manually upgrade intelligence when you are working on a closed network environment.

ⓘ | **NOTE:** Do not navigate away from this page until the firmware upgrade is completed.


Appliance / Home / System / Firmware Management

FIRMWARE INFORMATION

Current Version 1.2.0-16

Last Update Time May 01, 2021 - 05:06:55

PERFORM UPGRADE / DOWNGRADE

Target Version Up to date

Click to Upgrade / Downgrade

You are already running the latest firmware.

FIRMWARE UPGRADE

Firmware Select a file...

INTELLIGENCE UPGRADE

Signature Timestamp Apr 30, 2021 - 18:58:42

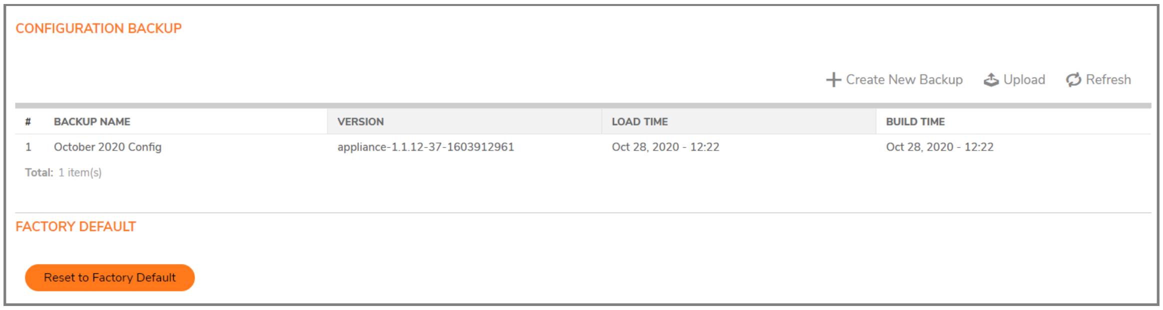
Last Update Time May 01, 2021 - 05:30:01

Firmware Select a file...

Configuration Backup

This function allows you to backup the complete configuration settings of the CSa for ease of replication to another CSa or to support recovery.

Backing Up Configurations



#	BACKUP NAME	VERSION	LOAD TIME	BUILD TIME
1	October 2020 Config	appliance-1.1.12-37-1603912961	Oct 28, 2020 - 12:22	Oct 28, 2020 - 12:22

Total: 1 item(s)

Create New Backup

To create a new configuration backup:

1. Click **+Create New Backup**.
2. Enter a **Backup Name** for in the **Name** field to backup your current configuration.

Upload Configuration

To upload a configuration backup:

1. Click **Upload**.
2. Select the configuration file.

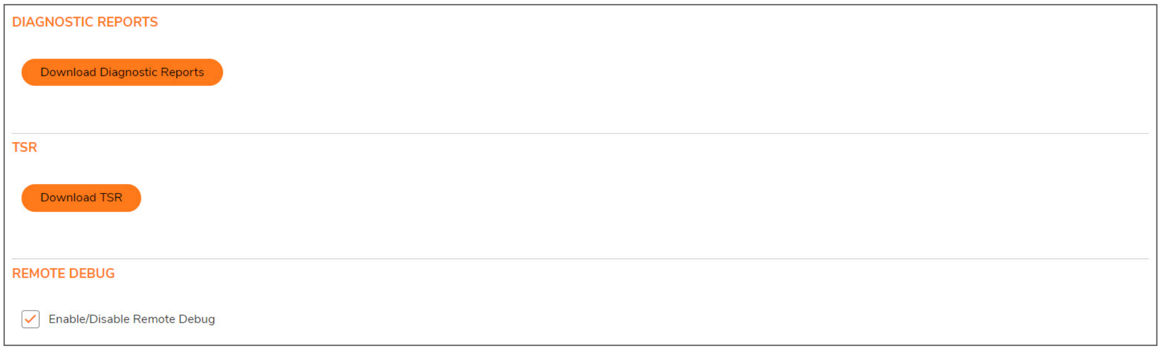
Factory Default

To reset your system to its factory default settings:

1. Click **Reset to Factory Default** to restore all settings back to their factory default settings.

Diagnostic

This screen allows you to **Download Diagnostic Reports** for later review or **Download TSR**, a Tech Support Report (TSR) to send to SonicWall Technical Support. The TSR collects diagnostic information from your system and compiles it into a report that the SonicWall Tech Support can use to debug and troubleshoot any system issues. This report includes diagnostic commands, log files, and optionally, a full system snapshot. The TSR also captures the system's current running configuration. You can also use **Remote Debug** to enable or disable a remote debugging mechanism.



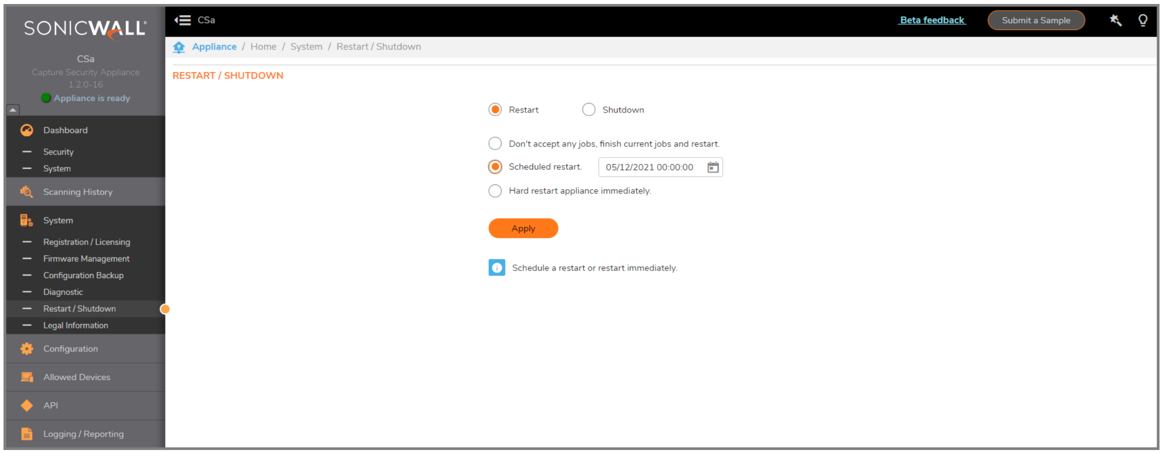
☑ Enable/Disable Remote Debug

Restart / Shutdown

The **Restart / Shutdown** display panel supports several operations:

- **Restart** - this executes a warm restart of CSa firmware without powering down the hardware
- **Shutdown** - this ends all software processes and powers down the appliance
- **Graceful but immediate restart** - this initiates a reset as soon as current jobs are complete
- **Graceful but immediate shutdown** - the appliance shuts down after completing current jobs
- **Immediate hard restart** - the system powers down completely and then restarts

Resetting and Shutting Down the Appliance



RESTART / SHUTDOWN

● Restart ○ Shutdown

○ Don't accept any jobs, finish current jobs and restart.

● Scheduled restart. 05/12/2021 00:00:00

○ Hard restart appliance immediately.

Schedule a restart or restart immediately.

Restart

You can chose the conditions around either restarting or shutting down your appliance.

To restart the appliance at a specific date or time:

1. Click **Restart.**
2. Click **Scheduled restart** and indicate an orderly restart at a predetermined date and time.
3. Click **Apply**.

Graceful but Immediate Restart

To gracefully shut down and restart the appliance once current processes have completed:

1. Click **Restart.**
2. Click **Don't accept any jobs....**
3. Click **Apply**.

Immediate Hard Restart

To hard restart the appliance immediately:

1. Click **Restart.**
2. Click on **Hard restart appliance immediately**.
3. Click **Apply**

Shutdown

To shut down the appliance at a specific date or time:

1. Click **Shutdown**.
2. Click **Scheduled shutdown** and indicate an orderly shutdown at a predetermined date and time.
3. Click **Apply**.

Graceful but Immediate Shutdown

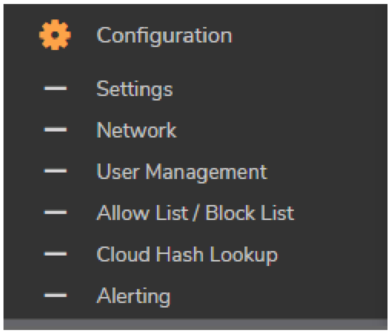
To gracefully shut down the appliance once current processes have completed:

1. Click **Shutdown**.
2. Click on **Don't accept any jobs....**
3. Click **Apply**.

5

Configuration

Configuration Pages



Topics:

- Settings
- Network
- User Management
- Allow List/Block List
- Cloud Hash Lookup
- Alerting

Settings

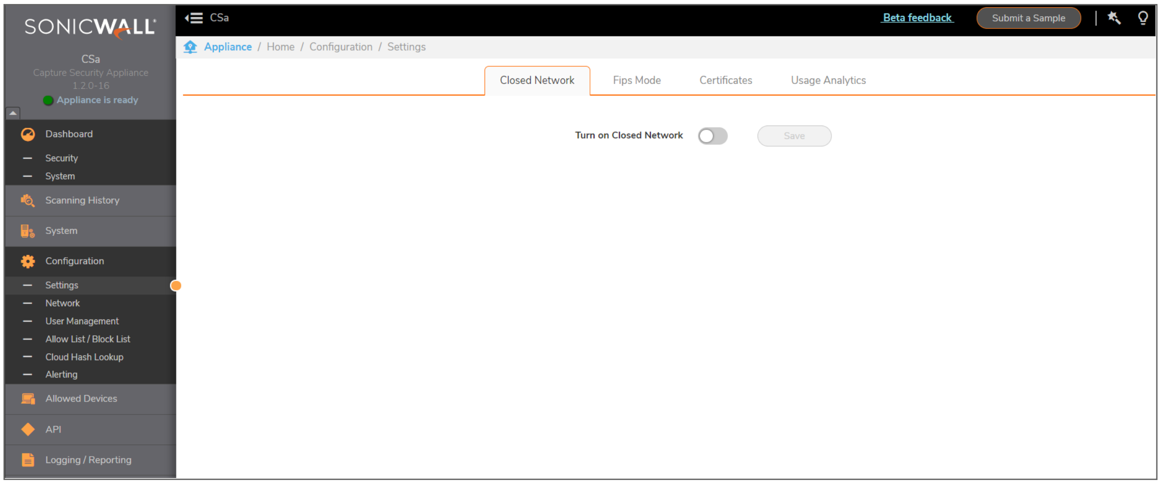
Topics:

- Closed Network
- Fips Mode
- Active-Active Clustering
- Certificates
- Usage Analytics

Closed Network

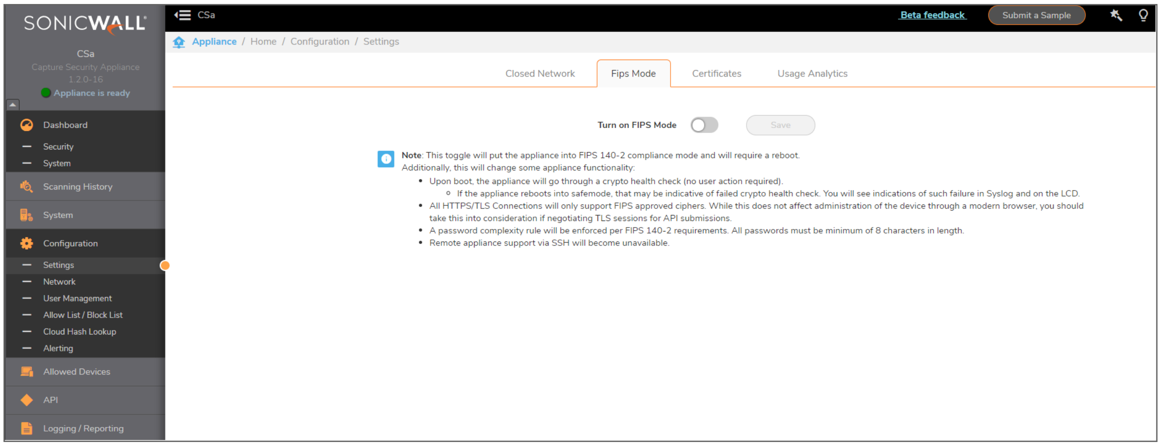
This configuration screen allows you to work on the appliance in an environment without the requirement of a network or internet. Enabling this mode will require that licensing, firmware update and intelligence updates be done manually. While firmware updates may occur once a quarter, intelligence updates, which are critical to accurate operation of the device, may occur as frequently as once per day. It is the responsibility of the administrator to manually update all CSas under management in a timely manner.

ⓘ | **NOTE:** All firmware and intelligence updates are cryptographically unique to every device.



Fips Mode

This configuration screen allows your to put the appliance into FIPS 140-2 compliance mode and would require a reboot.



Note: This toggle will put the appliance into FIPS 140-2 compliance mode and will require a reboot.
Additionally, this will change some appliance functionality:

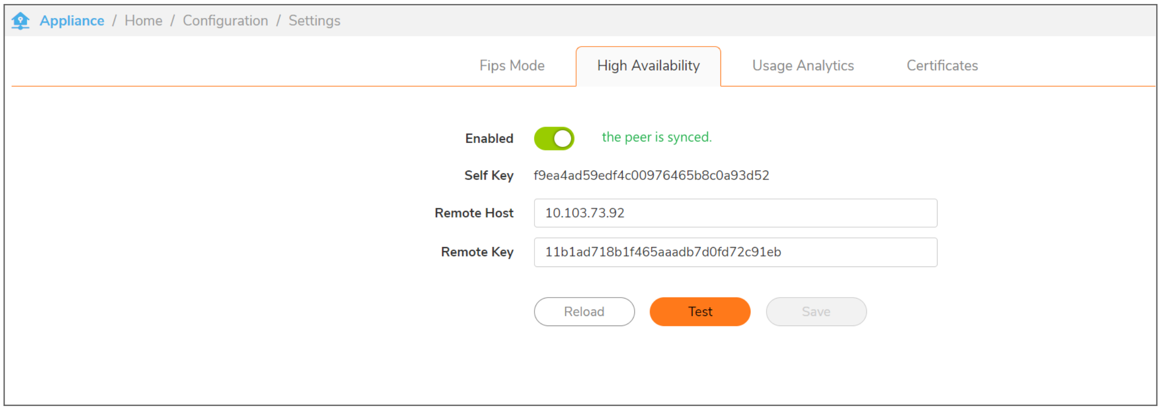
- Upon boot, the appliance will go through a crypto health check (no user action required).
  - If the appliance reboots into safemode, that may be indicative of failed crypto health check. You will see indications of such failure in Syslog and on the LCD.
- All HTTPS/TLS Connections will only support FIPS approved ciphers. While this does not affect administration of the device through a modern browser, you should take this into consideration if negotiating TLS sessions for API submissions.
- A password complexity rule will be enforced per FIPS 140-2 requirements. All passwords must be minimum of 8 characters in length.
- Remote appliance support via SSH will become unavailable.

Active-Active Clustering

Active-Active clustering features high-available and scalability for users, applicable for CSA1000 and CSA2500. User can setup at most two CSa clusters. User can submit files to any of the cluster. The reporting data and configuration data will be sync between the two clustes via API. In each cluster, there is a primary node and several secondary nodes. All nodes share the same database and storages. The primary node can offload traffic to the secondary nodes.

To enable Active-Active clustering:

1. Navigate to **Configuration>settings>High Availability.**
2. Now in the **Remote Host** section enter the IP address of the instance which you want to pair.
3. And under **Remote Key** section enter the **Self Key** of the other instance which you want pair then click on **Test** and then **Save** tab, you will notice the Active-Active cluster is now enabled.



Enabled the peer is synced.

Self Key f9ea4ad59edf4c00976465b8c0a93d52

Remote Host 10.103.73.92

Remote Key 11b1ad718b1f465aaadb7d0fd72c91eb

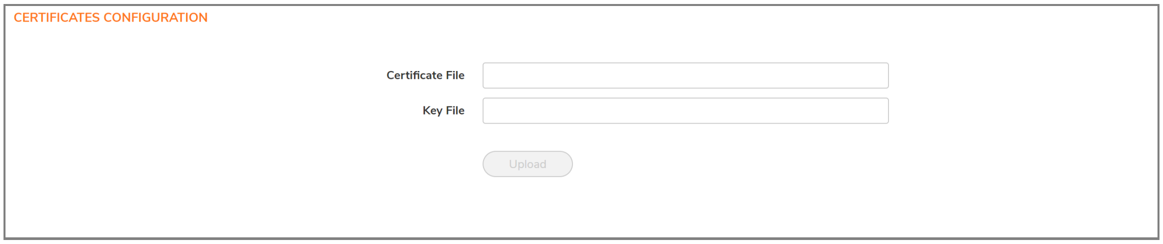
Certificates

At **Configuration > Settings > Certificates**, you can upload security certificates and key files.

Upload Certificate and Key Files

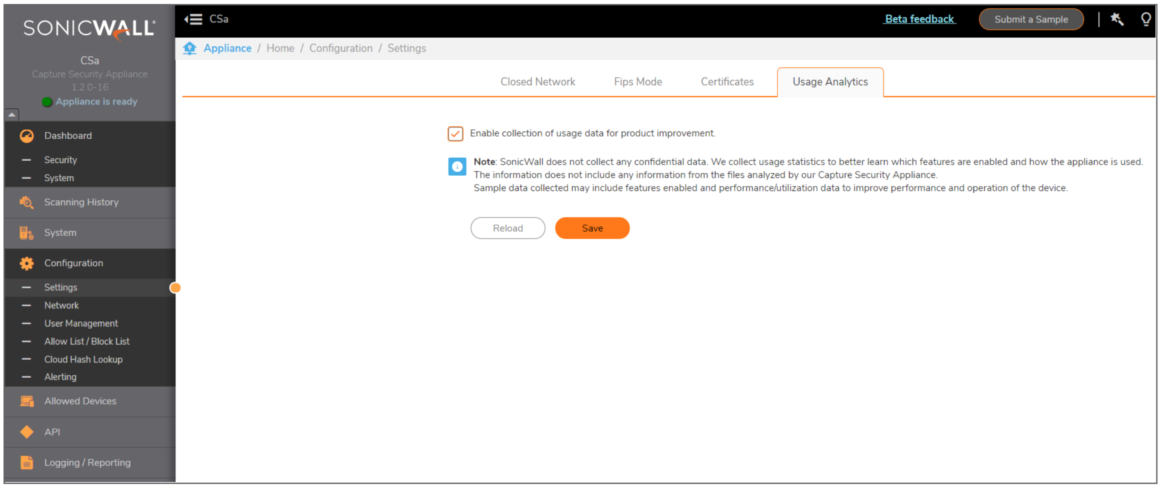
To configure Certificate and Key files:

1. Enter your certificate file name in the **Certificate File** field.
2. Enter your key file name in the **Key File** field.
3. Click **Upload**.



Usage Analytics

This configuration screen enables the collection of usage data for product improvement.



☑ Enable collection of usage data for product improvement.

Note: SonicWall does not collect any confidential data. We collect usage statistics to better learn which features are enabled and how the appliance is used. The information does not include any information from the files analyzed by our Capture Security Appliance. Sample data collected may include features enabled and performance/utilization data to improve performance and operation of the device.

Network

This panel allows access to five configuration screens arranged as tabs:

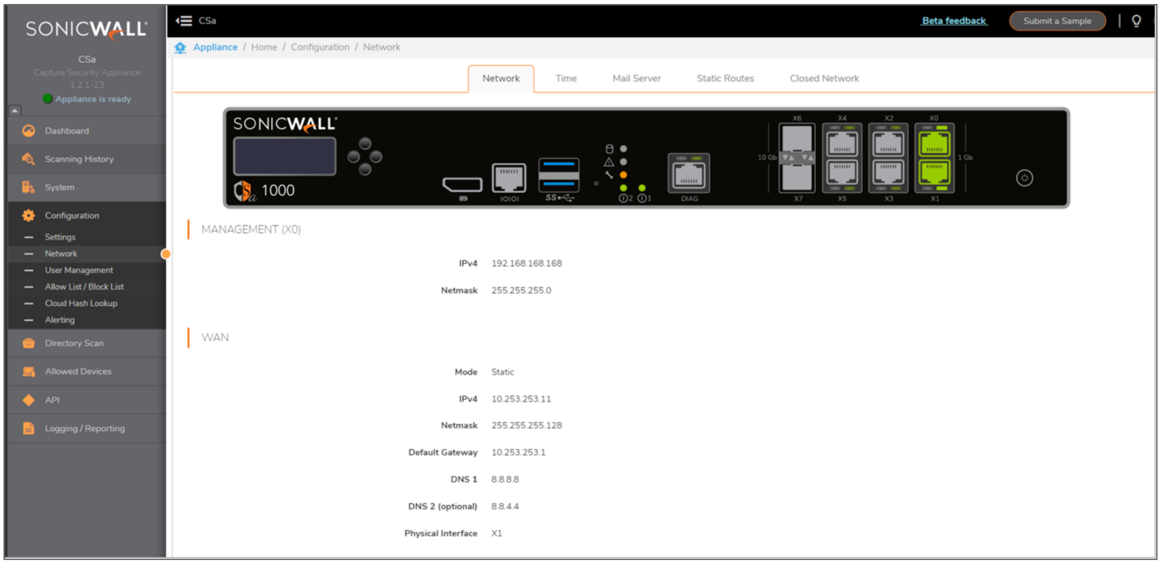
- Network Configuration
- Time
- Email Server Configuration
- Static Route Configuration

Network Configuration

The Network Configuration screen consists of three sections:

- **Management (X0)**
- **WAN (X1)**

- **Internal Network**



MANAGEMENT (X0)

IPv4	192.168.168.168
Netmask	255.255.255.0

WAN

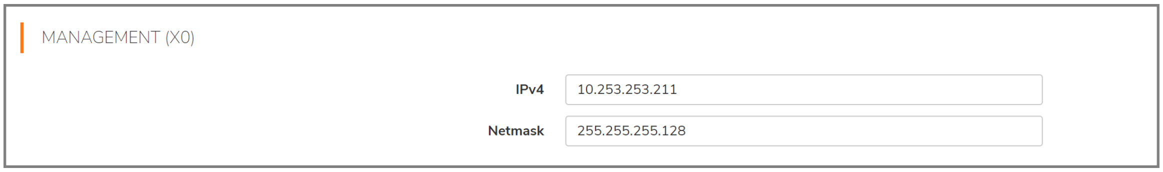
Mode	Static
IPv4	10.253.253.11
Netmask	255.255.255.128
Default Gateway	10.253.253.1
DNS 1	8.8.8.8
DNS 2 (optional)	8.8.4.4
Physical Interface	X1

The CSa can be set up for access through one of two methods. All Internet communication and management is performed through a single interface (WAN), or Internet communication is done through the WAN, but management and configuration is performed through a separate management network.

You can change the WAN interface by clicking on the required interface image, which will be highlighted in green color.

Management (X0) allows assignment of a local management IP address.

Management (X0)

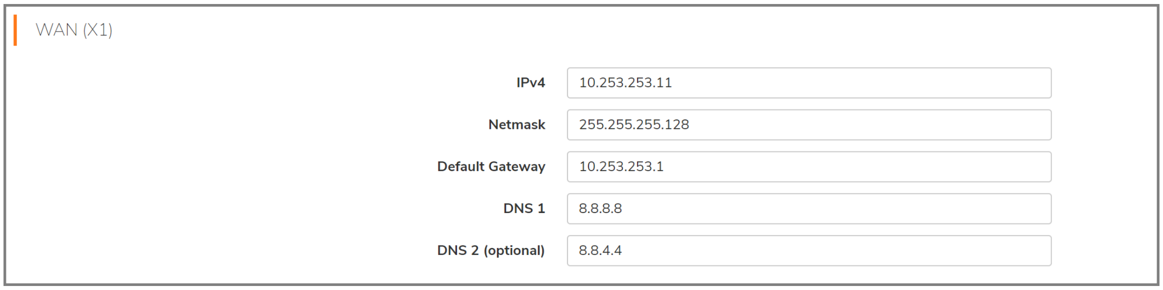


MANAGEMENT (X0)

IPv4	10.253.253.211
Netmask	255.255.255.128

WAN (X1) address and default gateway.

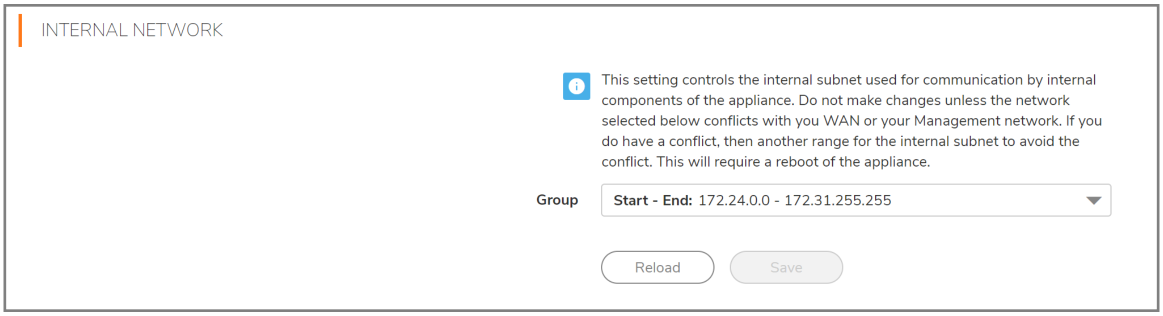
WAN (X1)



WAN (X1)

IPv4	10.253.253.11
Netmask	255.255.255.128
Default Gateway	10.253.253.1
DNS 1	8.8.8.8
DNS 2 (optional)	8.8.4.4

Internal Network



INTERNAL NETWORK

This setting controls the internal subnet used for communication by internal components of the appliance. Do not make changes unless the network selected below conflicts with you WAN or your Management network. If you do have a conflict, then another range for the internal subnet to avoid the conflict. This will require a reboot of the appliance.

Group: **Start - End:** 172.24.0.0 - 172.31.255.255

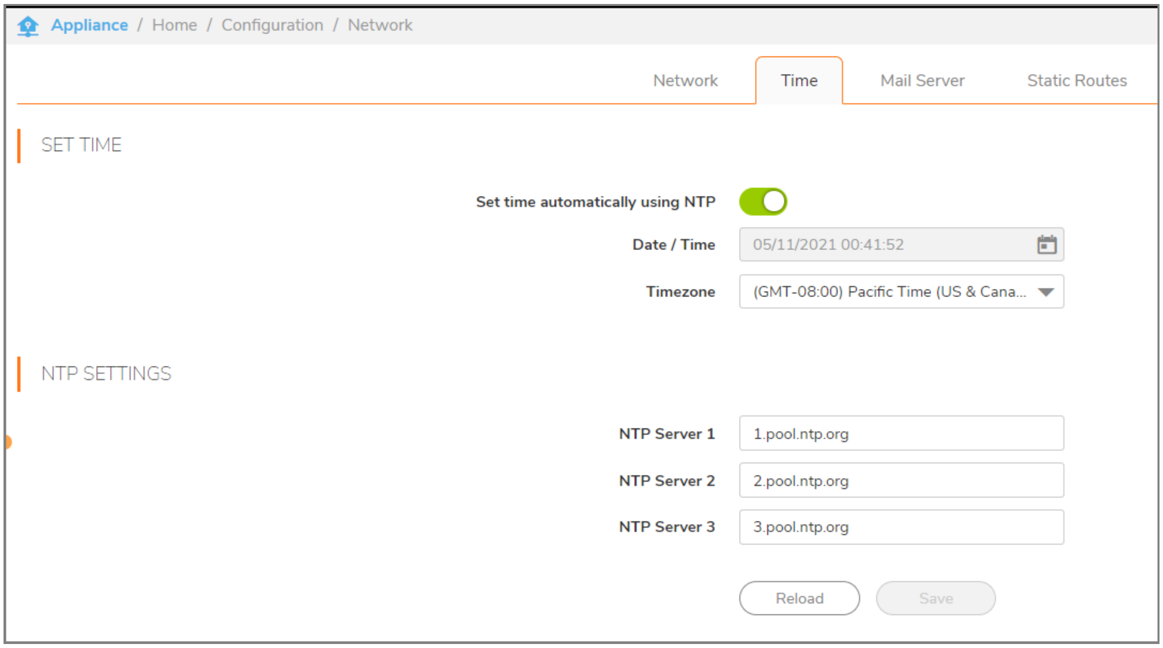
NOTE: The CSa uses internal subnets for communication among components. Occasionally, the internal network subnet might overlap with the network on which the CSa is deployed. In that case, you must select a different subnet that does not exist on your network. The Internal Network MUST NOT match or overlap with the IP addresses configured in the Management X0 and WAN X1 networks.

If you select a different address range in the Group field, a reboot of the CSa is required.

Time

This configuration screen allows the setting of the timezone location to the appliance as well as the assignment of **Network Time Protocol** (NTP) servers.

You can configure NTP servers to ensure reporting and other functions are properly synchronized. You are not required to reboot your system after changing NTP servers . Any newly submitted files are given new timestamps within the new NTP server system. The old timestamps remain with the previous files.



Appliance / Home / Configuration / Network

SET TIME

Set time automatically using NTP ●

Date / Time 05/11/2021 00:41:52

Timezone (GMT-08:00) Pacific Time (US & Cana...

NTP SETTINGS

NTP Server 1 1.pool.ntp.org

NTP Server 2 2.pool.ntp.org

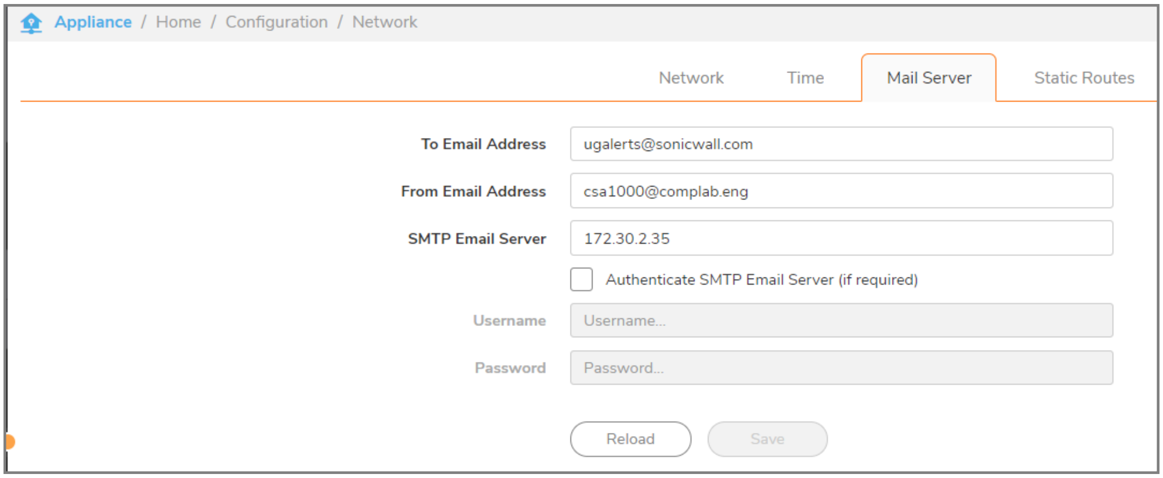
NTP Server 3 3.pool.ntp.org

Email Server Configuration

This configuration screen supports the assignment of an email server for Simple Mail Transfer Protocol functionality.

This configuration is highly recommended to support email alerts and reports.

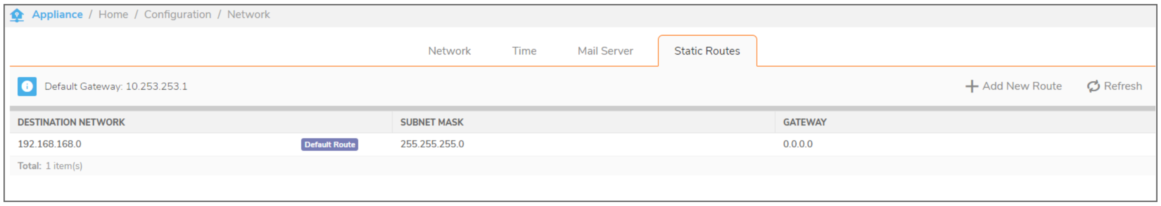
Configure Email Server



To Email Address	ugalerts@sonicwall.com
From Email Address	csa1000@complab.eng
SMTP Email Server	172.30.2.35
	□ Authenticate SMTP Email Server (if required)
Username	Username...
Password	Password...

Static Route Configuration

Static routes can be defined for the CSa. This is necessary when both the LAN and the WAN interfaces are configured and the device might not know which interface it should use for routing.



Default Gateway: 10.253.253.1

DESTINATION NETWORK		SUBNET MASK	GATEWAY
192.168.168.0	Default Route	255.255.255.0	0.0.0.0

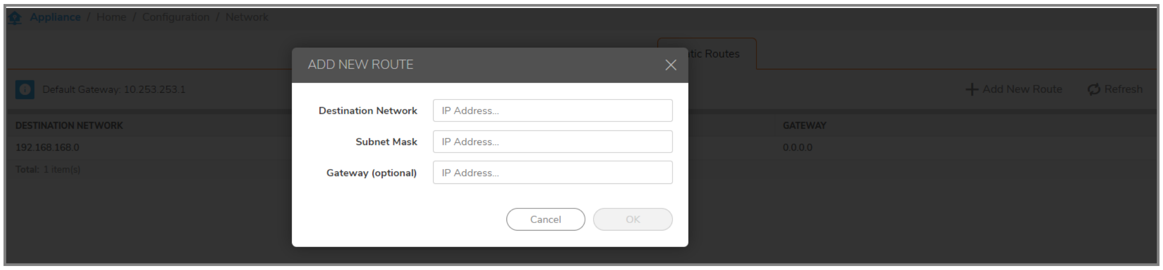
Total: 1 item(s)

Configuring Static Routes

To define the static routes for your configuration:

1. Click **+Add New Route**
2. Define the IP addresses of the **Destination Network**, the **Subnet Mask**, and optionally, the **Gateway**.

3. Click **OK** to save your settings.



Destination Network: IP Address...

Subnet Mask: IP Address...

Gateway (optional): IP Address...

User Management

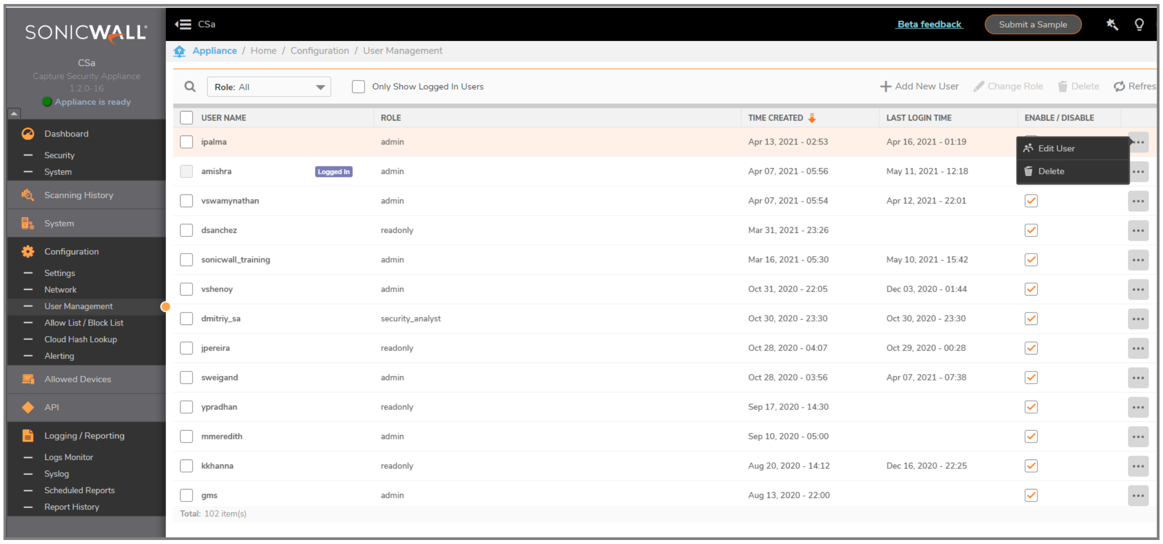
The User Management page includes the following tab:

- Configuring Users

Configuring Users

Configuration > Users allows for the defining of user's roles, as well as adding and deleting them.

Setting Up Users

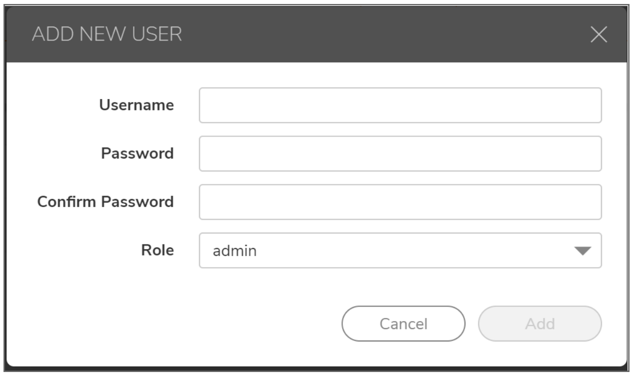


USER NAME	ROLE	TIME CREATED	LAST LOGIN TIME	ENABLE / DISABLE
ipalma	admin	Apr 13, 2021 - 02:53	Apr 16, 2021 - 01:19	
amishra	admin	Apr 07, 2021 - 05:56	May 11, 2021 - 12:18	
vswamynathan	admin	Apr 07, 2021 - 05:54	Apr 12, 2021 - 22:01	☑
dsanchez	readonly	Mar 31, 2021 - 23:26		☑
sonicwall_training	admin	Mar 16, 2021 - 05:30	May 10, 2021 - 15:42	☑
vshenoy	admin	Oct 31, 2020 - 22:05	Dec 03, 2020 - 01:44	☑
dmitriy_sa	security_analyst	Oct 30, 2020 - 23:30	Oct 30, 2020 - 23:30	☑
jpereira	readonly	Oct 28, 2020 - 04:07	Oct 29, 2020 - 00:28	☑
sweigand	admin	Oct 28, 2020 - 03:56	Apr 07, 2021 - 07:38	☑
ypradhan	readonly	Sep 17, 2020 - 14:30		☑
mmeredith	admin	Sep 10, 2020 - 05:00		☑
kkhanna	readonly	Aug 20, 2020 - 14:12	Dec 16, 2020 - 22:25	☑
gms	admin	Aug 13, 2020 - 22:00		☑

Total: 102 item(s)

To add a new user and password:

1. Click **+Add New User** to define passwords as shown in the **Add New User** dialog that follows.



Username	
Password	
Confirm Password	
Role	admin

2. Enter a **Username**, **Password**, **Confirm Password**, and **Role** intended for this user.
3. Click **Add**.

ⓘ **NOTE:** You can edit the user information and password by selecting the three-dotted menu (...) on the right of the user list to open the **Edit User** dialog.

Allow List/Block List

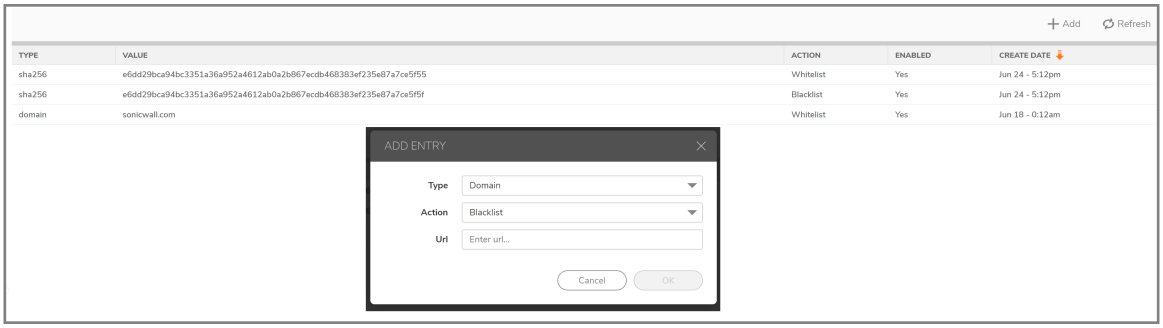
This page allows you to define URLs as either **Allowed** or **Blocked**.

Typical **Allow** entries include material from trusted sources such as Microsoft and Google.

To add Allow List or Block List entries:

1. Navigate to the **Configuration > Allow List/Block List** page.

   ALLOW LISTING AND BLOCK LISTING



TYPE	VALUE	ACTION	ENABLED	CREATE DATE
sha256	e6dd29bca94bc3351a36a952a4612ab0a2b867ecdb468383ef235e87a7ce5f55	Whitelist	Yes	Jun 24 - 5:12pm
sha256	e6dd29bca94bc3351a36a952a4612ab0a2b867ecdb468383ef235e87a7ce5f5f	Blacklist	Yes	Jun 24 - 5:12pm
domain	sonicwall.com	Whitelist	Yes	Jun 18 - 0:12am

Type	Domain
Action	Blacklist
Url	Enter url...

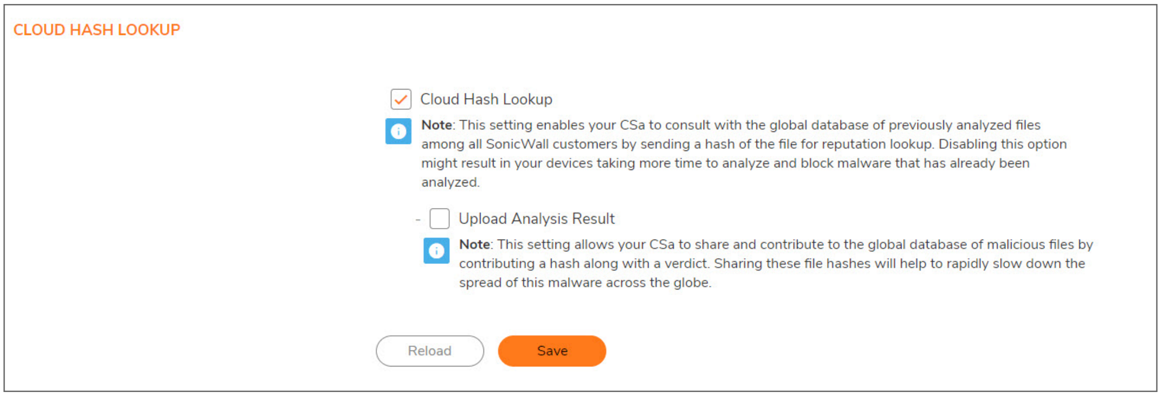
2. Click **+Add**.

   Allow Listing and **Block Listing** entries can be indicated by **Domain**, **MD5.** and **Sha256.**

Cloud Hash Lookup

SonicWall uses **Cloud Hash Lookup** as a way of looking up previously analyzed file results using data hashes, MD5, SHA1, and SHA256, as reputation lookup. This option is enabled by default. Disabling the option could result in your devices taking more time to analyze and block malware that has previously been analyzed.

Enabling **Upload Analysis Result** allows your CSa to share and contribute to the global database of malicious files by contributing a hash along with a verdict. Sharing file hashes helps to rapidly slow the spread of malware across the globe.



CLOUD HASH LOOKUP

☑ Cloud Hash Lookup

Note: This setting enables your CSa to consult with the global database of previously analyzed files among all SonicWall customers by sending a hash of the file for reputation lookup. Disabling this option might result in your devices taking more time to analyze and block malware that has already been analyzed.

□ Upload Analysis Result

Note: This setting allows your CSa to share and contribute to the global database of malicious files by contributing a hash along with a verdict. Sharing these file hashes will help to rapidly slow down the spread of this malware across the globe.

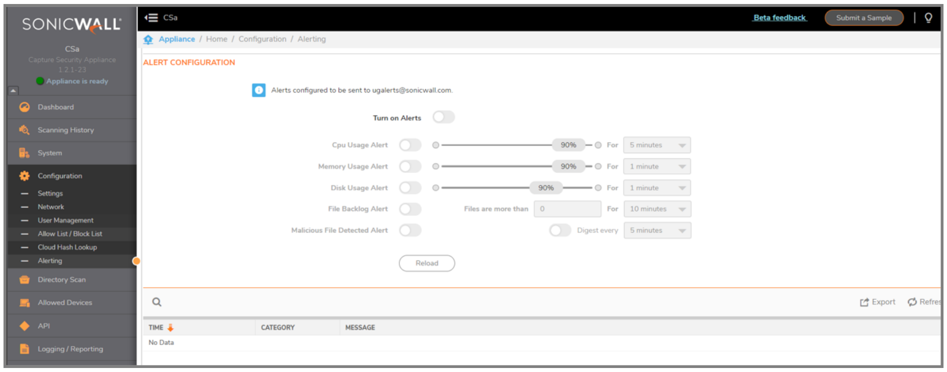
Alerting

The **Configuration > Alerting** page allows you to turn on and configure alerts for system capacity utilization.

Alert Configuration

After configuring your mail server (see **Configuration > Network | Mail Server**), you can turn on and enable the following alerts:

- CPU Usage
- Memory Usage
- Disk Usage
- File Backlog
- Malicious File Detected



ALERT CONFIGURATION

Alerts configured to be sent to ugalerts@sonicwall.com.

Turn on Alerts

Cpu Usage Alert 90% For 5 minutes

Memory Usage Alert 90% For 1 minute

Disk Usage Alert 90% For 1 minute

File Backlog Alert Files are more than 0 For 10 minutes

Malicious File Detected Alert Digest every 5 minutes

TIME	CATEGORY	MESSAGE
No Data		

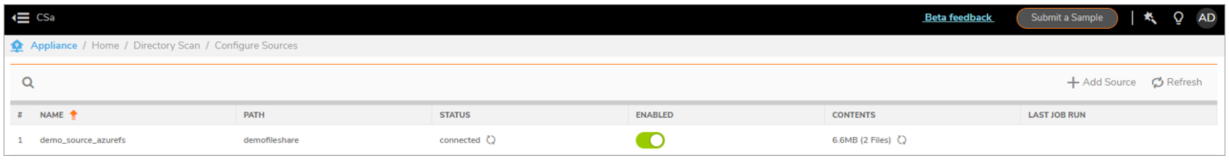
6

Directory Scan

The Directory scanner extends the Threat Analysis capability of CSa to file shares on-premise and in the cloud. The file share types supported in this release are AzureFS, AWS S3, and SMBv3.

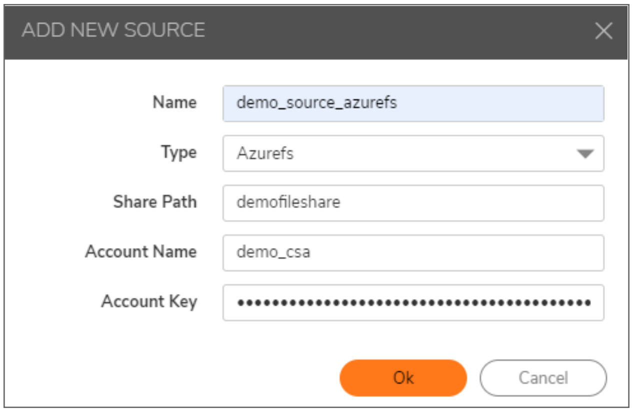
Source/Remote Share Configuration

Navigate to **Directory Scan>Configure Sources** and click on **Add Source**.



#	NAME	PATH	STATUS	ENABLED	CONTENTS	LAST JOB RUN
1	demo_source_azurefs	demofileshare	connected	●	6.6MB (2 Files)	

Now enter the fields in **ADD NEW SOURCE** window with a Name of your choice, Type (select from AzureFS, AWSS3 or SMBv3), and Share parameters and authentication credentials associated with the share type, as described in the following section e.g:



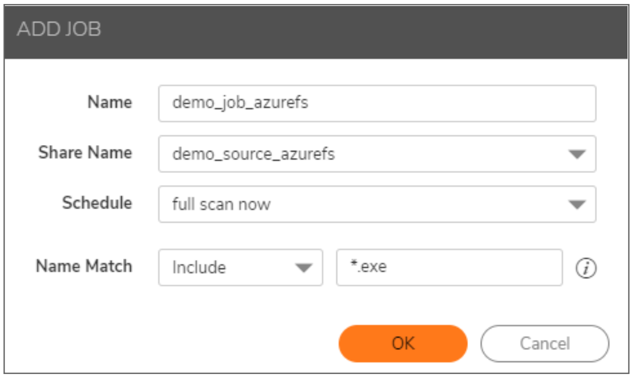
Name	demo_source_azurefs
Type	Azurefs
Share Path	demofileshare
Account Name	demo_csa
Account Key	••

Parameters required for each Share Type:

- Azure File Share
    - Authentication Credentials
        - Account Name (Name of the Storage Account)
        - Account Key (Secret Access key found on the Azure Portal under Storage Account Name-> Security+Networking -> Access Keys)
    - Share Parameters
        - Share Path (Name of the File Share under the Storage Account)
- AWS S3
    - Authentication Credentials (found or can be created on the AWS management Console in the IAM section)
        - Access Key ID
        - Secret Access Key
    - Share Parameters
        - Bucket Name
        - Folder (/ indicates all or /folder name in bucket)
- SMBv3
    - Authentication Credentials
        - Username
        - Password
    - Share Parameters
        - Server Name
        - Share Path

Job/Scan Configuration

Navigate to **Directory Scan>Scan Jobs** and click on **Add Job**. Now enter a job name of choice, select share configured in previous section to scan, a schedule of choice (now, later, or on a recurring interval of daily, weekly or monthly) and optionally an include or exclude filter to select files to match by filename pattern e.g *.doc, *.exe, etc.)



ADD JOB

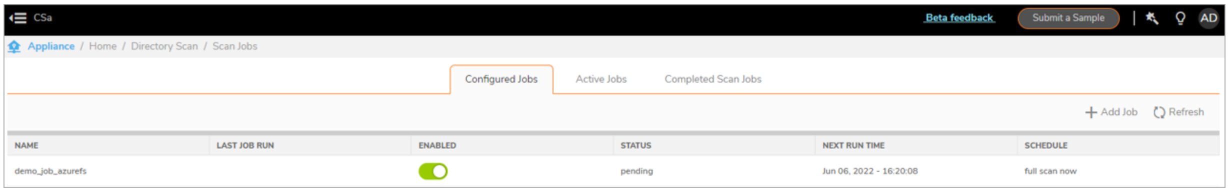
Name: demo_job_azurefs

Share Name: demo_source_azurefs

Schedule: full scan now

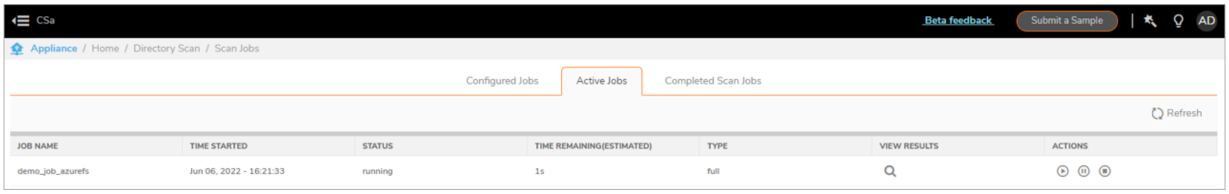
Name Match: Include *.exe

Now you can view the created job status, run time and job Schedule in the **Configured Jobs** section.



NAME	LAST JOB RUN	ENABLED	STATUS	NEXT RUN TIME	SCHEDULE
demo_job_azurefs		●	pending	Jun 06, 2022 - 16:20:08	full scan now

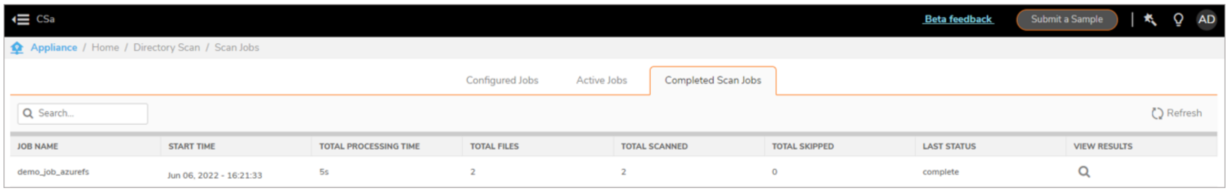
When a job is ready to run and it's active, you will be able to view to the job under the **Active Jobs** section. Here, you will also find the ability to pause, cancel or resume the job to control its progress, as indicated by radio buttons.



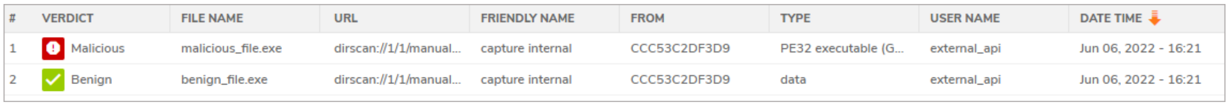
JOB NAME	TIME STARTED	STATUS	TIME REMAINING(ESTIMATED)	TYPE	VIEW RESULTS	ACTIONS
demo_job_azurefs	Jun 06, 2022 - 16:21:33	running	1s	full	🔍	▶ ⏸ ⏹

When a job is completed, you can view its summary in the **Completed Scan Jobs** section, as depicted below. Click on the **View results** magnifier icon.

For more details on the scan results and deep reports of the verdicts for the files scanned see Deep Report for Malicious File.



JOB NAME	START TIME	TOTAL PROCESSING TIME	TOTAL FILES	TOTAL SCANNED	TOTAL SKIPPED	LAST STATUS	VIEW RESULTS
demo_job_azurefs	Jun 06, 2022 - 16:21:33	5s	2	2	0	complete	🔍



#	VERDICT	FILE NAME	URL	FRIENDLY NAME	FROM	TYPE	USER NAME	DATE TIME
1	Malicious	malicious_file.exe	dirscan://1/1/manual...	capture internal	CCC53C2DF3D9	PE32 executable (G...	external_api	Jun 06, 2022 - 16:21
2	✓ Benign	benign_file.exe	dirscan://1/1/manual...	capture internal	CCC53C2DF3D9	data	external_api	Jun 06, 2022 - 16:21

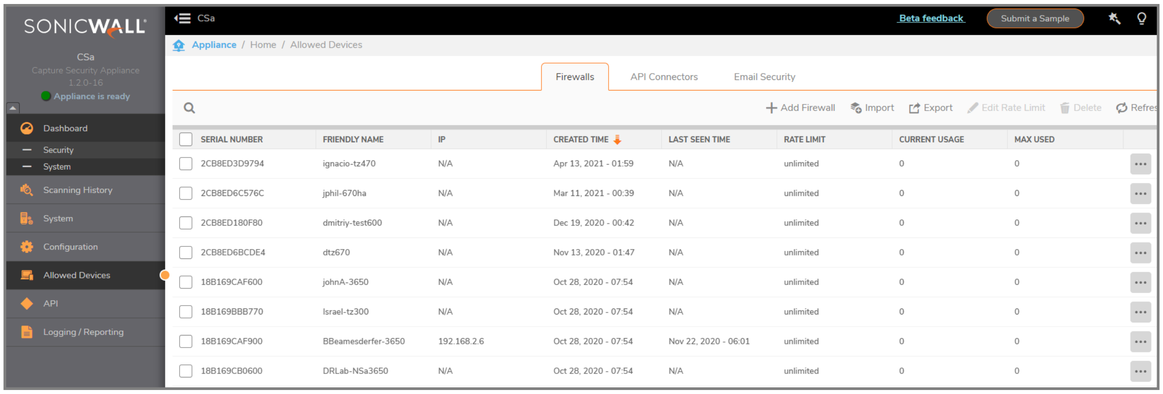
6

Allowed Devices

These screens allow the configuration of the devices that can contribute files for testing. For each, **Firewalls**, **API Connectors**, and **Email Security** servers, dialog boxes support recall of scanning history, and configuration of new source devices.

Firewalls

For adding a single device, click **+Add Firewall** to open the **Add New Firewall** dialog. For multiple devices, click **Import** to open the **Import Firewalls From File** dialog.



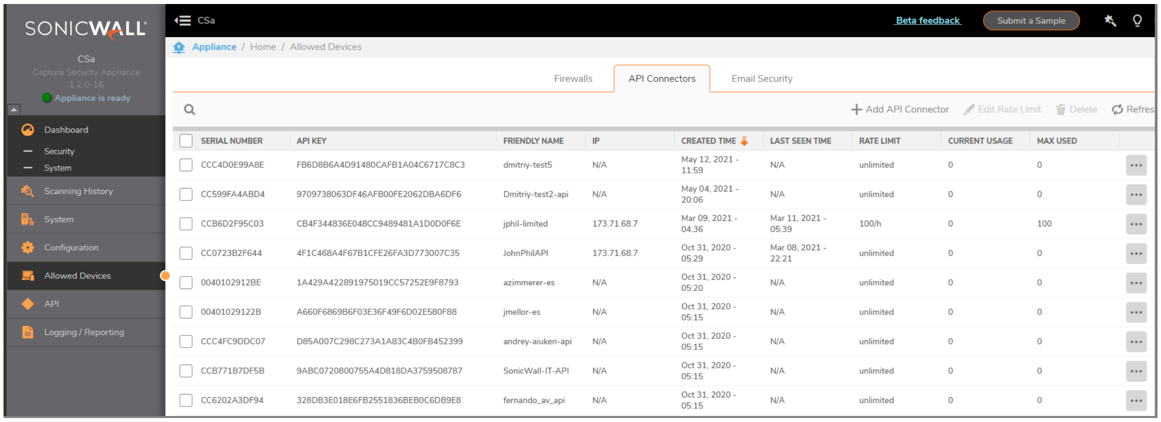
SERIAL NUMBER	FRIENDLY NAME	IP	CREATED TIME	LAST SEEN TIME	RATE LIMIT	CURRENT USAGE	MAX USED
2CB8ED3D9794	ignacio-tz470	N/A	Apr 13, 2021 - 01:59	N/A	unlimited	0	0
2CB8ED6C576C	jphil-670ha	N/A	Mar 11, 2021 - 00:39	N/A	unlimited	0	0
2CB8ED180F80	dmitriy-test600	N/A	Dec 19, 2020 - 00:42	N/A	unlimited	0	0
2CB8ED6BCDE4	dtz670	N/A	Nov 13, 2020 - 01:47	N/A	unlimited	0	0
18B169CAF600	johnA-3650	N/A	Oct 28, 2020 - 07:54	N/A	unlimited	0	0
18B169BBB770	Israel-tz300	N/A	Oct 28, 2020 - 07:54	N/A	unlimited	0	0
18B169CAF900	BBeamesderfer-3650	192.168.2.6	Oct 28, 2020 - 07:54	Nov 22, 2020 - 06:01	unlimited	0	0
18B169CB0600	DRLab-NSa3650	N/A	Oct 28, 2020 - 07:54	N/A	unlimited	0	0

For **Firewalls**, the additional allowed device is registered on MySonicWall, and its serial number and friendly name are added here.

NOTE: To add firewalls in a High Availability pair to the allowed list, enter the serial numbers and friendly names of both units into the **Firewalls** list, with each unit on its own line.

API Connectors

Click **+Add API Key** to open the **Add New API Connector** dialog.

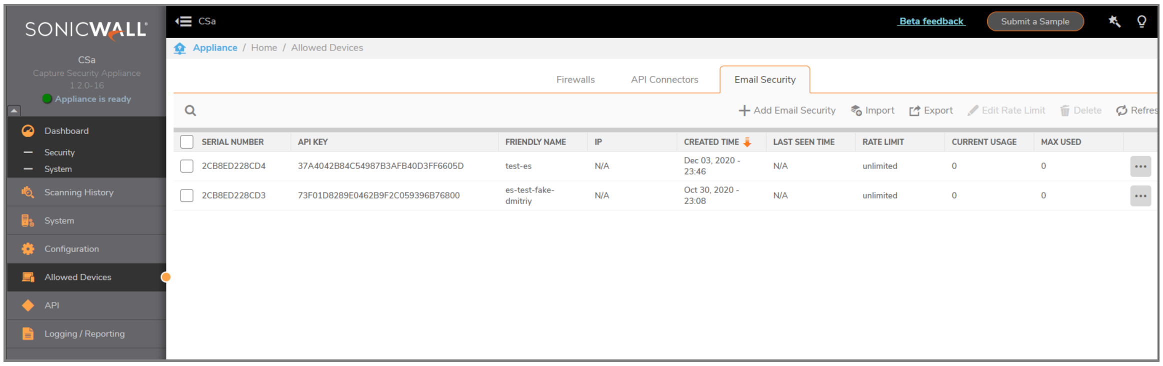


□	SERIAL NUMBER	API KEY	FRIENDLY NAME	IP	CREATED TIME	LAST SEEN TIME	RATE LIMIT	CURRENT USAGE	MAX USED	
□	CCC4D0E99A8E	FB6D8B6A4D91480CAFB1A04C6717C8C3	dmitriy-test5	N/A	May 12, 2021 - 11:59	N/A	unlimited	0	0	•••
□	CC599FA4ABD4	9709738063DF46AFB00FE2062DBA6DF6	Dmitriy-test2-api	N/A	May 04, 2021 - 20:06	N/A	unlimited	0	0	•••
□	CCB6D2F95C03	CB4F344836E048CC9489481A1D0D0F6E	jphil-limited	173.71.68.7	Mar 09, 2021 - 04:36	Mar 11, 2021 - 05:39	100/h	0	100	•••
□	CC0723B2F644	4F1C468A4F67B1CFE26FA3D773007C35	JohnPhilAPI	173.71.68.7	Oct 31, 2020 - 05:29	Mar 08, 2021 - 22:21	unlimited	0	0	•••
□	0040102912BE	1A429A422891975019CC57252E9F8793	azimmerer-es	N/A	Oct 31, 2020 - 05:20	N/A	unlimited	0	0	•••
□	00401029122B	A660F6869B6F03E36F49F6D02E580F88	jmellor-es	N/A	Oct 31, 2020 - 05:15	N/A	unlimited	0	0	•••
□	CCC4FC9DDC07	D85A007C298C273A1A83C4B0FB452399	andrey-aiuken-api	N/A	Oct 31, 2020 - 05:15	N/A	unlimited	0	0	•••
□	CCB771B7DF5B	9ABC0720800755A4D818DA3759508787	SonicWall-IT-API	N/A	Oct 31, 2020 - 05:15	N/A	unlimited	0	0	•••
□	CC6202A3DF94	328DB3E018E6FB2551836BEB0C6DB9E8	fernando_av_api	N/A	Oct 31, 2020 - 05:15	N/A	unlimited	0	0	•••

To add an API connector, the serial number and friendly name of the file source are added here and an **API Key** is generated.

Email Security

For adding a single device, click **+Add Email Security** to open the **Add New Email Security** dialog. For multiple devices, click **Import** to open the **Import Email Security Devices From File** dialog.

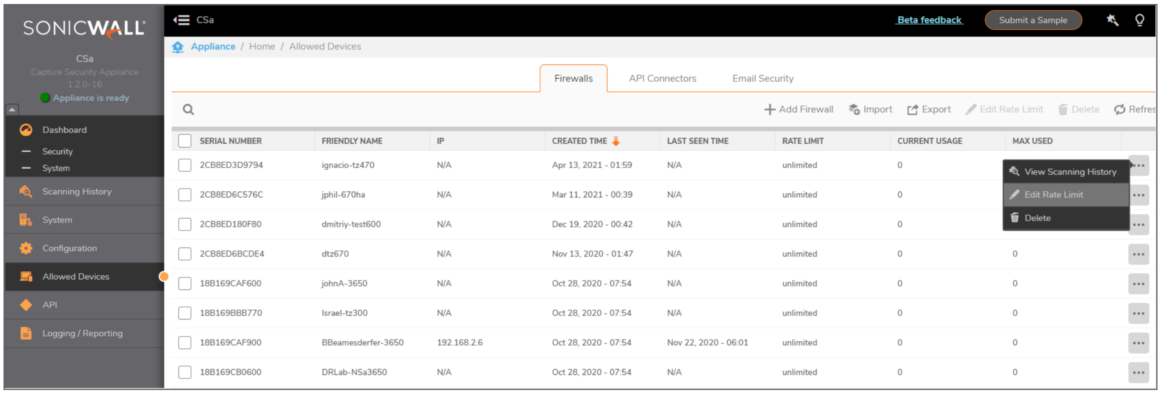


□	SERIAL NUMBER	API KEY	FRIENDLY NAME	IP	CREATED TIME	LAST SEEN TIME	RATE LIMIT	CURRENT USAGE	MAX USED	
□	2CB8ED228CD4	37A4042B84C54987B3AFB40D3FF6605D	test-es	N/A	Dec 03, 2020 - 23:46	N/A	unlimited	0	0	•••
□	2CB8ED228CD3	73F01D8289E0462B9F2C059396B76800	es-test-fake-dmitriy	N/A	Oct 30, 2020 - 23:08	N/A	unlimited	0	0	•••

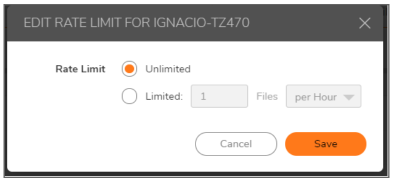
Email security file sources are registered by friendly name and serial number at MySonicWall and connected as allowed devices to the CSa here.

Rate Limit

Select the three-dotted menu (...) on the right of the device list to open the **Edit Rate Limit** dialog. You can also provide the rate limit when you add a new device.



	SERIAL NUMBER	FRIENDLY NAME	IP	CREATED TIME	LAST SEEN TIME	RATE LIMIT	CURRENT USAGE	MAX USED
□	2CB8ED3D9794	ignacio-tz470	N/A	Apr 13, 2021 - 01:59	N/A	unlimited	0	
□	2CB8ED6C576C	jphil-670ha	N/A	Mar 11, 2021 - 00:39	N/A	unlimited	0	
□	2CB8ED180F80	dmitriy-test600	N/A	Dec 19, 2020 - 00:42	N/A	unlimited	0	
□	2CB8ED6BCDE4	dtz670	N/A	Nov 13, 2020 - 01:47	N/A	unlimited	0	0
□	18B169CAF600	johnA-3650	N/A	Oct 28, 2020 - 07:54	N/A	unlimited	0	0
□	18B169BBB770	Israel-tz300	N/A	Oct 28, 2020 - 07:54	N/A	unlimited	0	0
□	18B169CAF900	BBeamesderfer-3650	192.168.2.6	Oct 28, 2020 - 07:54	Nov 22, 2020 - 06:01	unlimited	0	0
□	18B169CB0600	DRLab-NSa3650	N/A	Oct 28, 2020 - 07:54	N/A	unlimited	0	0



EDIT RATE LIMIT FOR IGNACIO-TZ470

Rate Limit ● Unlimited

○ Limited: 1 Files per Hour

7

API

The CSa supports two types of APIs to programmatically access the appliance:

- Service API for file submission and analysis
- Management API for device configuration

The API pages contain the API reference, which can also be used to interact with the appliance to see requests and response codes. Additional code samples on using the Capture API can be found at https://github.com/sonicwall.

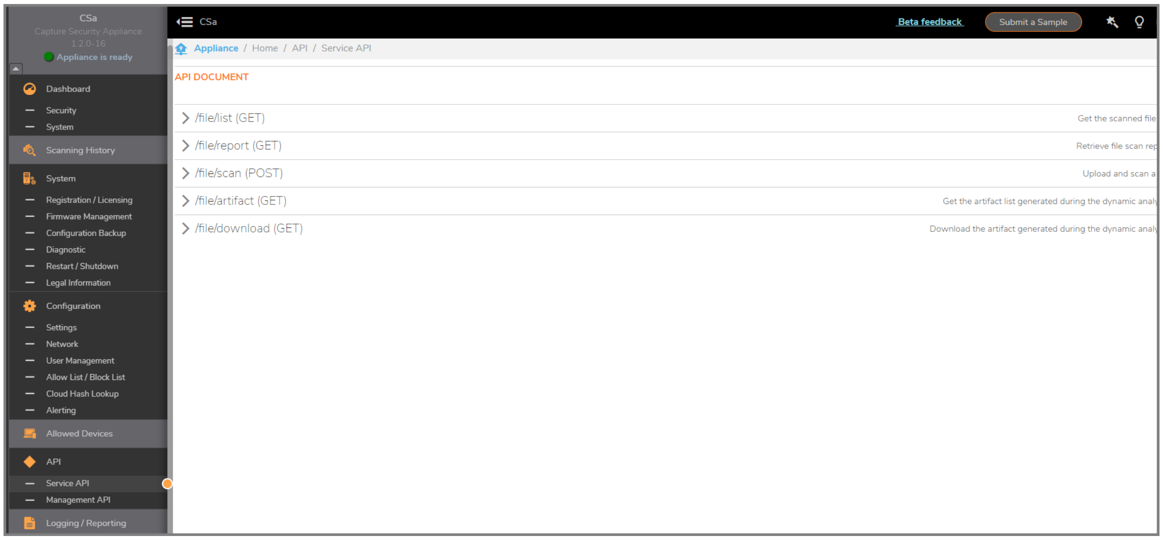
Sample Use Cases:

- Service API: A webserver used to receive files can be programmed to submit all files to the CSa for analysis before making them available inside the organization. For example, an insurance company or a local government can add such protection before any files make it inside their network.
- Service API: A security analyst with a large number of files gathered in the field can write a script to submit all the files to the CSa for analysis to get a verdict on which files are malicious and which are benign.
- Management API: An MSSP on boarding device can automatically add devices to the CSa "Allowed Devices" list as soon as a customer or a device are added to their inventory system.

To get a list of APIs, use the > symbol to compress the display. Available APIs appear.

Topics:

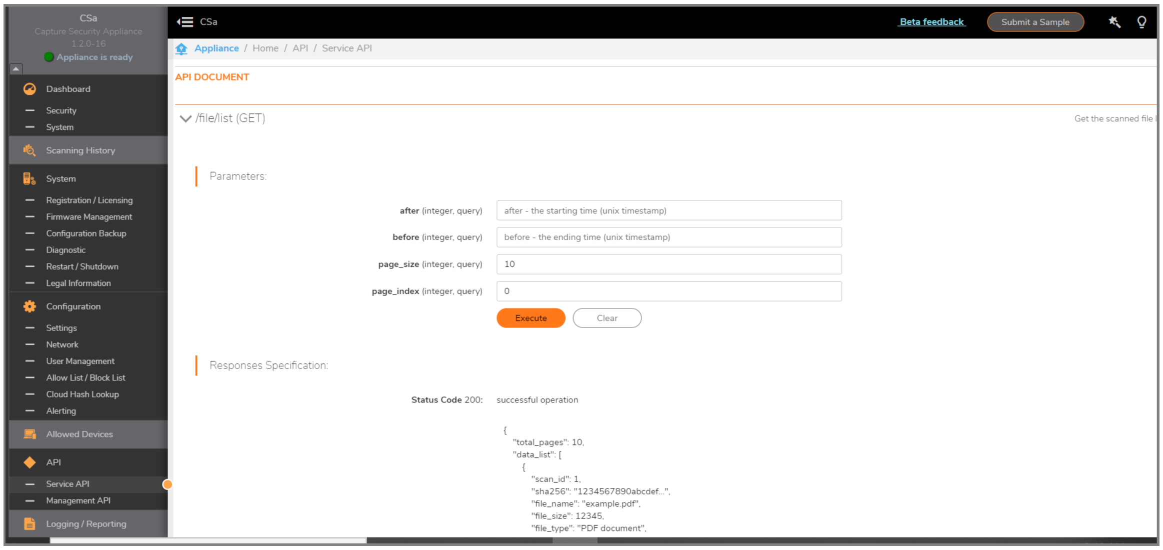
Service API



API DOCUMENT

- /file/list (GET) — Get the scanned file
- /file/report (GET) — Retrieve file scan rep
- /file/scan (POST) — Upload and scan a
- /file/artifact (GET) — Get the artifact list generated during the dynamic analy
- /file/download (GET) — Download the artifact generated during the dynamic analy

API Operation



API DOCUMENT

/file/list (GET) — Get the scanned file

Parameters:

after (integer, query): after - the starting time (unix timestamp)

before (integer, query): before - the ending time (unix timestamp)

page_size (integer, query): 10

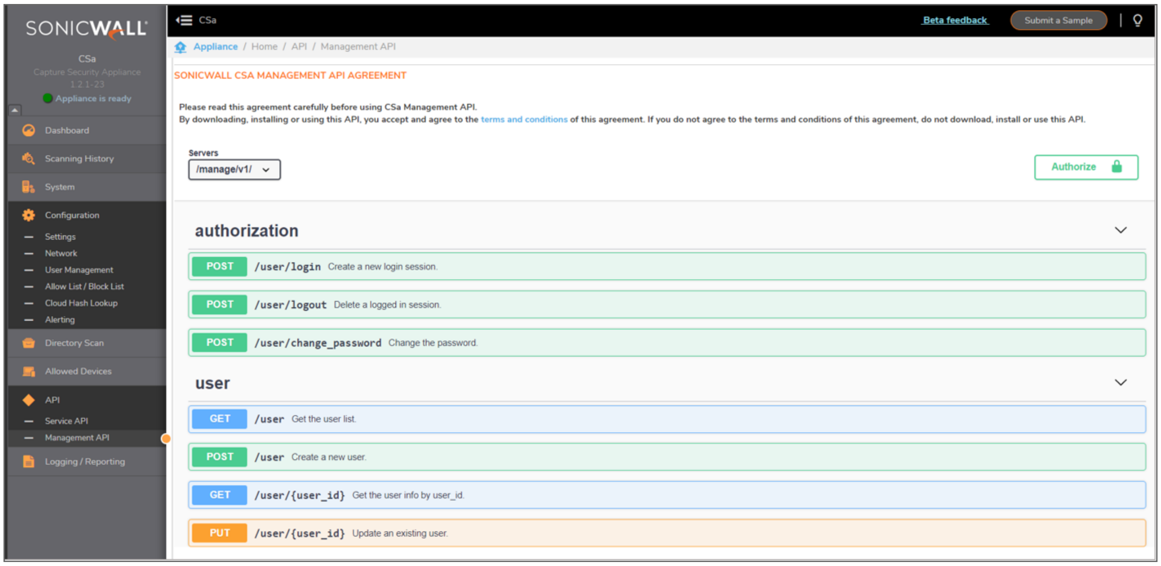
page_index (integer, query): 0

Responses Specification:

Status Code 200: successful operation

```
{
   "total_pages": 10,
   "data_list": [
      {
         "scan_id": 1,
         "sha256": "1234567890abcdef...",
         "file_name": "example.pdf",
         "file_size": 12345,
         "file_type": "PDF document",
```

Management API



SONICWALL CSA MANAGEMENT API AGREEMENT

Please read this agreement carefully before using CSa Management API.
By downloading, installing or using this API, you accept and agree to the terms and conditions of this agreement. If you do not agree to the terms and conditions of this agreement, do not download, install or use this API.

Servers: /manage/v1/

authorization

- POST `/user/login` Create a new login session.
- POST `/user/logout` Delete a logged in session.
- POST `/user/change_password` Change the password.

user

- GET `/user` Get the user list.
- POST `/user` Create a new user.
- GET `/user/{user_id}` Get the user info by user_id.
- PUT `/user/{user_id}` Update an existing user.

8

Logging and Reporting

Topics:

- Logs Monitor
- Syslog
- Reporting

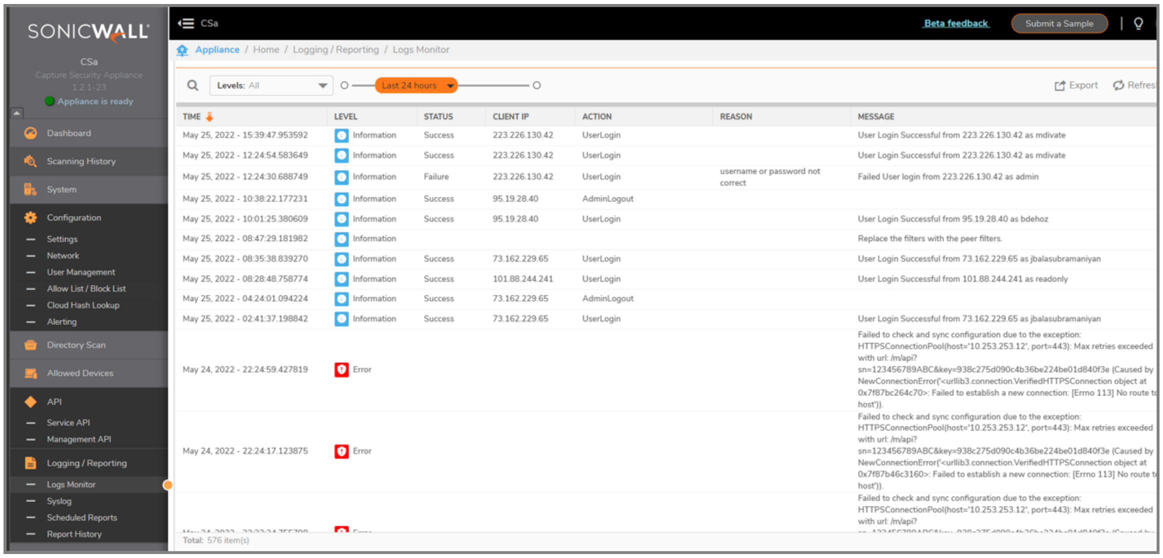
Logs Monitor

The **Logs Monitor** screen allows filtering of all events by **Levels**:

- **Critical**
- **Error**
- **Warning**
- **Information**
- **Debug**
- **Not set**

And by time period (slider):

- **Last 1 hour**
- **Last 24 hours**
- **Last week**
- **Last month**
- **All**



Appliance / Home / Logging / Reporting / Logs Monitor

Levels: All — Last 24 hours

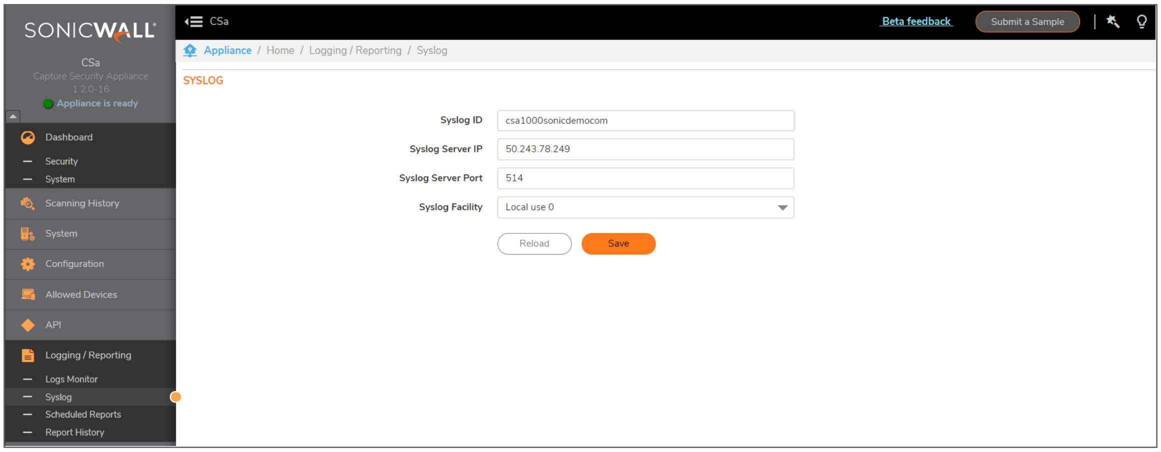
TIME	LEVEL	STATUS	CLIENT IP	ACTION	REASON	MESSAGE
May 25, 2022 - 15:39:47.953592	Information	Success	223.226.130.42	UserLogin		User Login Successful from 223.226.130.42 as mdivate
May 25, 2022 - 12:24:54.583649	Information	Success	223.226.130.42	UserLogin		User Login Successful from 223.226.130.42 as mdivate
May 25, 2022 - 12:24:30.688749	Information	Failure	223.226.130.42	UserLogin	username or password not correct	Failed User login from 223.226.130.42 as admin
May 25, 2022 - 10:38:22.177231	Information	Success	95.19.28.40	AdminLogout		
May 25, 2022 - 10:01:25.380609	Information	Success	95.19.28.40	UserLogin		User Login Successful from 95.19.28.40 as bdehoz
May 25, 2022 - 08:47:29.181982	Information					Replace the filters with the peer filters.
May 25, 2022 - 08:35:38.839270	Information	Success	73.162.229.65	UserLogin		User Login Successful from 73.162.229.65 as jbalasubramaniyan
May 25, 2022 - 08:28:48.758774	Information	Success	101.88.244.241	UserLogin		User Login Successful from 101.88.244.241 as readonly
May 25, 2022 - 04:24:01.094224	Information	Success	73.162.229.65	AdminLogout		
May 25, 2022 - 02:41:37.198842	Information	Success	73.162.229.65	UserLogin		User Login Successful from 73.162.229.65 as jbalasubramaniyan
May 24, 2022 - 22:24:59.427819	Error					Failed to check and sync configuration due to the exception: HTTPSConnectionPool(host='10.253.253.12', port=443): Max retries exceeded with url: /m/api?sn=123456789ABC&key=938c275d090c4b36be224be01d840f3e (Caused by NewConnectionError('<urllib3.connection.VerifiedHTTPSConnection object at 0x7f87bc264c70>: Failed to establish a new connection: [Errno 113] No route to host')).
May 24, 2022 - 22:24:17.123875	Error					Failed to check and sync configuration due to the exception: HTTPSConnectionPool(host='10.253.253.12', port=443): Max retries exceeded with url: /m/api?sn=123456789ABC&key=938c275d090c4b36be224be01d840f3e (Caused by NewConnectionError('<urllib3.connection.VerifiedHTTPSConnection object at 0x7f87b46c3160>: Failed to establish a new connection: [Errno 113] No route t host')).
						Failed to check and sync configuration due to the exception: HTTPSConnectionPool(host='10.253.253.12', port=443): Max retries exceeded with url: /m/api?

Total: 576 item(s)

After filtering log events, all table headings can be sorted by clicking the arrow next to each column heading. You can sort either ascending or descending for **Time**, **Level**, **Status**, **Client IP**, **Action**, **Reason**, or **Message**.

Syslog

The Syslog screen is used to send logging events.



Appliance / Home / Logging / Reporting / Syslog

SYSLOG

Syslog ID	csa1000sonicdemocom
Syslog Server IP	50.243.78.249
Syslog Server Port	514
Syslog Facility	Local use 0

Reload Save

Reporting

The Capture Security Appliance supports detailed scheduling and history of reports.

Reporting is split into two sections:

- Scheduling or configuration of the reports — Reports can be customized to report on specific appliances and sources and then sent to different recipients.

  See Scheduled Reports

- History of generated reports. Lists reports that have run and have been mailed. They can be rerun from this page or downloaded directly.

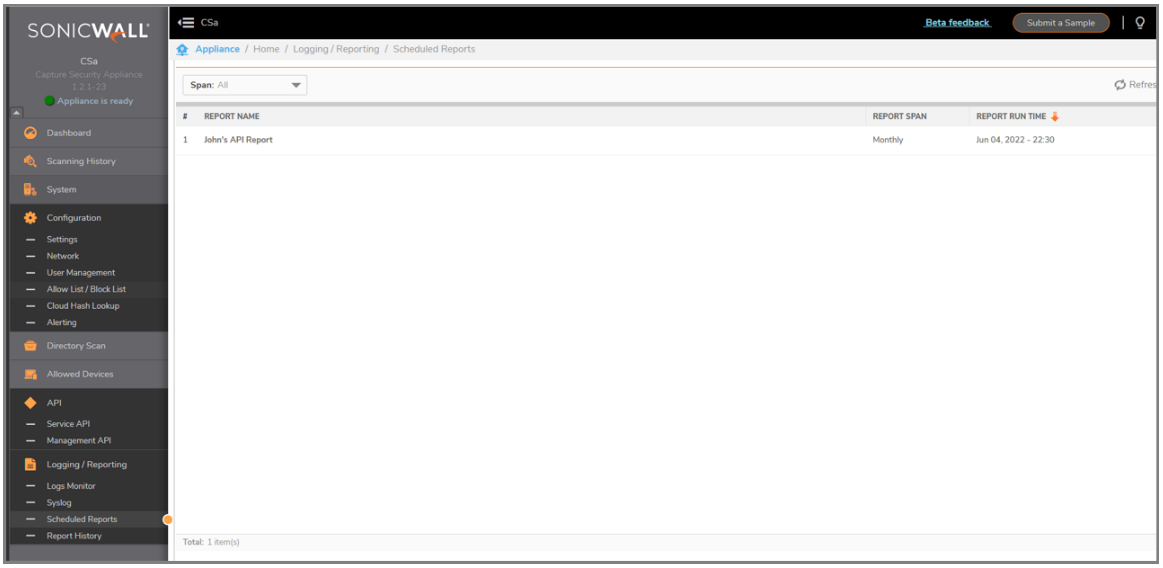
  See Report History

Scheduled Reports

On this screen records are scheduled and tracked.

ⓘ | **NOTE:** The filter box at the left allows reports to be displayed as **All**, **Weekly**, **Monthly**, or **Daily**.

Filtering Monthly Reports



Span: All

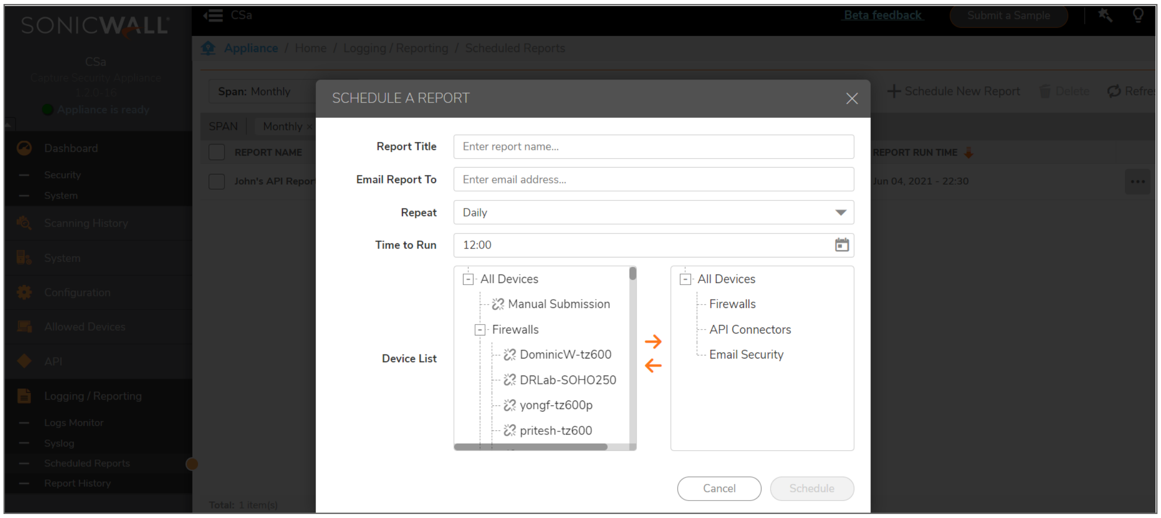
#	REPORT NAME	REPORT SPAN	REPORT RUN TIME
1	John's API Report	Monthly	Jun 04, 2022 - 22:30

Total: 1 item(s)

Scheduling Reports

Scheduling a New Report:

1. Click **+Schedule New Report.**
2. When the **Schedule A Report** dialog appears, fill it out.



SCHEDULE A REPORT

Report Title: Enter report name...

Email Report To: Enter email address...

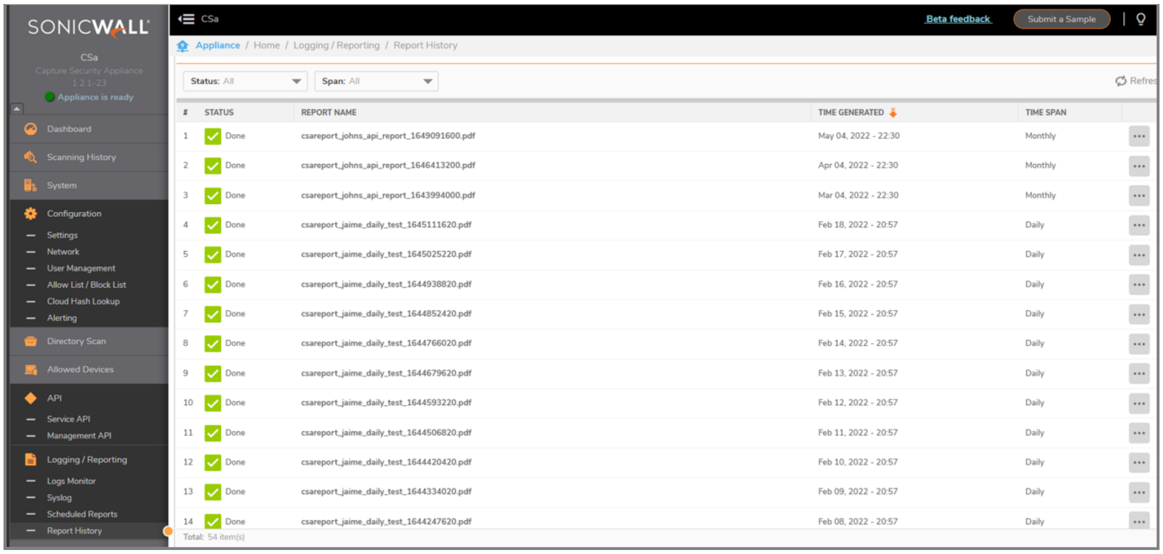
Repeat: Daily

Time to Run: 12:00

3. At the bottom of the dialog, move specific submissions sources, or categories (**Firewalls**, **API Connectors**, and **Email Security**) from the **Device List** to the list of devices on which reports are generated.
4. To complete, click **Schedule**.

Report History

Report History supports filtering reports based on **Status** (**All**, **Done**, **Failed**, and **In Progress**) and **Span** (**All**, **Weekly**, **Monthly**, **Daily**).



Status: All

Span: All

#	STATUS	REPORT NAME	TIME GENERATED	TIME SPAN
1	✓ Done	csareport_johns_api_report_1649091600.pdf	May 04, 2022 - 22:30	Monthly
2	✓ Done	csareport_johns_api_report_1646413200.pdf	Apr 04, 2022 - 22:30	Monthly
3	✓ Done	csareport_johns_api_report_1643994000.pdf	Mar 04, 2022 - 22:30	Monthly
4	✓ Done	csareport_jaime_daily_test_1645111620.pdf	Feb 18, 2022 - 20:57	Daily
5	✓ Done	csareport_jaime_daily_test_1645025220.pdf	Feb 17, 2022 - 20:57	Daily
6	✓ Done	csareport_jaime_daily_test_1644938820.pdf	Feb 16, 2022 - 20:57	Daily
7	✓ Done	csareport_jaime_daily_test_1644852420.pdf	Feb 15, 2022 - 20:57	Daily
8	✓ Done	csareport_jaime_daily_test_1644766020.pdf	Feb 14, 2022 - 20:57	Daily
9	✓ Done	csareport_jaime_daily_test_1644679620.pdf	Feb 13, 2022 - 20:57	Daily
10	✓ Done	csareport_jaime_daily_test_1644593220.pdf	Feb 12, 2022 - 20:57	Daily
11	✓ Done	csareport_jaime_daily_test_1644506820.pdf	Feb 11, 2022 - 20:57	Daily
12	✓ Done	csareport_jaime_daily_test_1644420420.pdf	Feb 10, 2022 - 20:57	Daily
13	✓ Done	csareport_jaime_daily_test_1644334020.pdf	Feb 09, 2022 - 20:57	Daily
14	✓ Done	csareport_jaime_daily_test_1644247620.pdf	Feb 08, 2022 - 20:57	Daily

Total: 54 item(s)

9

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- View video tutorials
- Access https://mysonicwall.com
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

About This Document

ⓘ | **NOTE:** A NOTE icon indicates supporting information.

ⓘ | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

ⓘ | **TIP:** A TIP icon indicates helpful information.

△ | **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

⚠ | **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

Capture Security Appliance Administration Guide
Updated - June 2022
232-005487-00 Rev D

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/end-user-product-agreements/.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to “SonicWall Inc.”, to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035