Capture Security Appliance

Getting Started Guide

SONICWALL®

Contents

1

Introduction

Welcome to the *SonicWall Capture Security Appliance Getting Started Guide*. This guide provides the information you need to deploy your Capture Security Appliance (CSa) in your network, configure the initial settings, and prepare it to start analyzing suspicious files from your firewalls, Email Security systems and API connectors.

This *Getting Started Guide* supports the following SonicWall Capture Security Appliance:

- CSa 1000

2

Technical Overview

The Capture Security Appliance provides the same Real-Time Deep Memory Inspection (RTDMI™) technology used by the SonicWallCapture Advanced Threat Protection (Capture ATP) cloud service to protect your network from malware. RTDMI does the following:

- Proactively detects and blocks unknown mass-market malware via deep memory inspection in real time
- Detects and blocks malware that does not exhibit any malicious behavior and hides its weaponry via custom encryption
- Forces malware to “reveal” its weaponry into memory
- Identifies and mitigates sophisticated attacks where weaponry is exposed for less than 100 nanoseconds

One benefit of the Capture Security Appliance is that it brings the power of RTDMI into an appliance form factor to serve customers who, due to geographical, regulatory or organizational requirements, cannot send files to the cloud for ATP analysis.

Benefits of the Capture Security Appliance:

- Memory-based inspection with RTDMI
- Multi-stage analysis with reputation check, static analysis and dynamic analysis
- API access for threat analysis
- Broad file type support
- Block until verdict support
- High-security effectiveness
- Reporting
- Role-Based access

You can connect the Capture Security Appliance to a supported SonicWall firewall and/or SonicWall Email Security appliance, or to an API Connector.

Because the Capture Security Appliance is IP addressable, it does not need to be connected directly to a firewall or Email Security appliance in order to process files. You can connect an API Connector to the CSa and pass files to it for analysis, run scripts that generate reports, and use other features via API. Refer to https://github.com/sonicwall for resources describing how to use the Capture ATP API.

To utilize the Capture Security Appliance with a connected firewall, the firewall must be able to ping and communicate via UDP port 2259. Email Security and API scripts need to be able to ping and access the Capture Security Appliance via HTTPS. As long as the firewalls ,Email Security or API Connector can ping the CSa, it is operational.

The Capture Security Appliance operates in one-arm mode. Traffic does not pass through it and the CSa does not sniff files from the network. Files must be sent to the CSa by the supported sources (firewall, Email Security or API).

The current capabilities of the Capture Security Appliance include:

- Analysis:
    - Global Verdict Lookup – SHA256 reputation lookup is performed before proceeding to static and dynamic analysis.
    - RTDMI Static & Dynamic Analysis
    - Whitelist / Blacklist
- User Role Management – Ability to create various roles (such as security analyst, network engineer) and control what the various roles can see, access and edit.
- Scheduled Reporting & Alerts – Ability to create scheduled reports for groups of file sources on a schedule.
- Security Dashboard – Provides a quick glance at file activity.
- Configuration Backup & Management – Provides safe upgrade/downgrade operations.
- API Access – Provides access for file analysis.

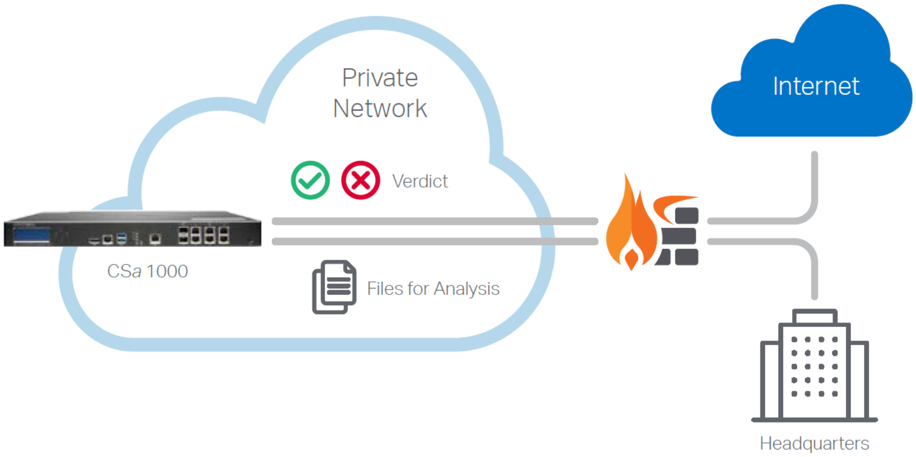
Deployment Examples

There are three primary deployments for the Capture Security Appliance:

- **Single Office/Single Location**

  The CSa can be deployed anywhere on the network. It must be reachable via an IP address, and SonicWall firewalls connected to it must be able to access it via UDP on port 2259.

  Firewalls and Email Security systems can send suspicious files to the CSa for analysis within the local network, rather than using the SonicWall Capture ATP cloud service.

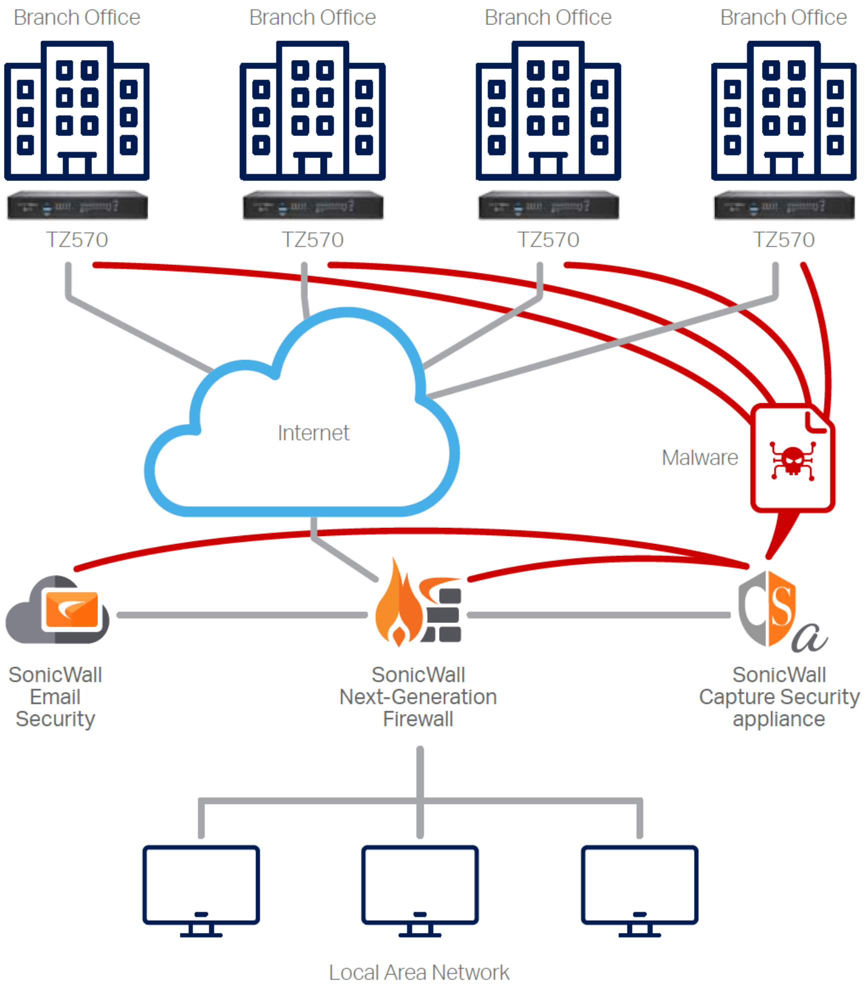


- **Distributed Enterprise / Multiple Locations**

  Multiple offices or branches can share access to a single CSa device, deployed either in the headquarters data center or in a remote data center accessible by all devices.

  Files can be sent to the CSa directly over the internet or over VPN.

  You can use either SonicWall GMS or the cloud-based NSM centralized management solutions for rapid configuration of multiple SonicWall systems to point to the CSa.



- **REST API Gateway**

  The Capture Security Appliance has a REST API interface that can be used 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 along with code samples are available at https://github.com/sonicwall.

4

Prerequisites for CSa Deployment

The following SonicWall appliances and versions are supported in a Capture Security Appliance deployment:

- Capture Security Appliance running 1.2.0 or newer
- Firewalls running SonicOS/X 7.0.0 or newer
- Firewalls running SonicOS 6.5.4.6 or newer
- Email Security running 10.0.6 or newer

Additional prerequisites include:

- MySonicWall account
- Intelligence Updates license for the CSa
- REST API license for the CSa, if using REST API from an API Connector
- Capture ATP license on firewalls and Email Security

5

High-Level Task List

The following are the steps for a successful deployment of your Capture Security Appliance:

1. Physically connect the CSa to your network device and management computer
2. Log into the CSa
3. Change the admin account password (highly recommended)
4. Set up networking (critical, will not operate otherwise)

   After this step, you can manage your CSa from either the X0 or the WAN interface. Using X0 allows management traffic to be on a separate subnet, while using the WAN interface allows you to manage the CSa from a remote location via the internet.
5. Register and license your CSa (critical, will not operate otherwise)
6. Update firmware on your CSa (highly recommended)
7. Add allowed devices and other sources that can send files for analysis to the CSa (critical, will not operate otherwise)

These tasks are described in this *Getting Started Guide*.

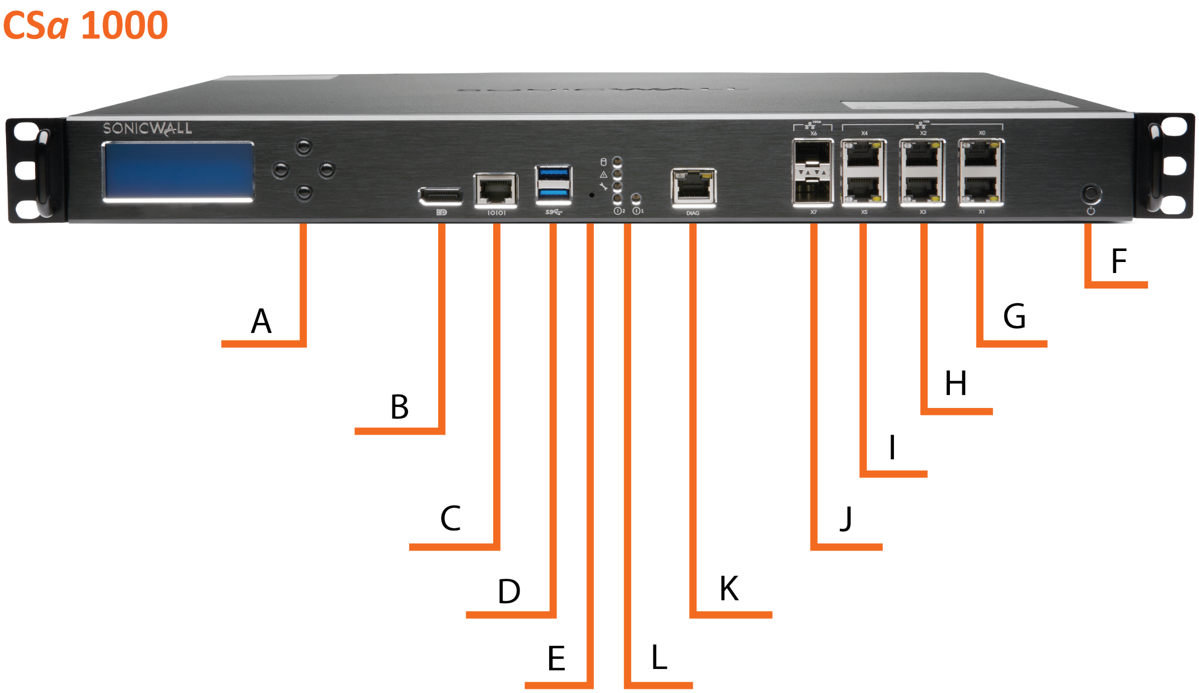
For information about additional configuration of your Capture Security Appliance and configuring your firewalls, Email Security system or API Connectors to use your CSa, refer to the Related Documents for Additional Configuration section.

6

Hardware Overview

This section describes the hardware components of the CSa 1000 appliance.

FRONT PANEL ILLUSTRATION

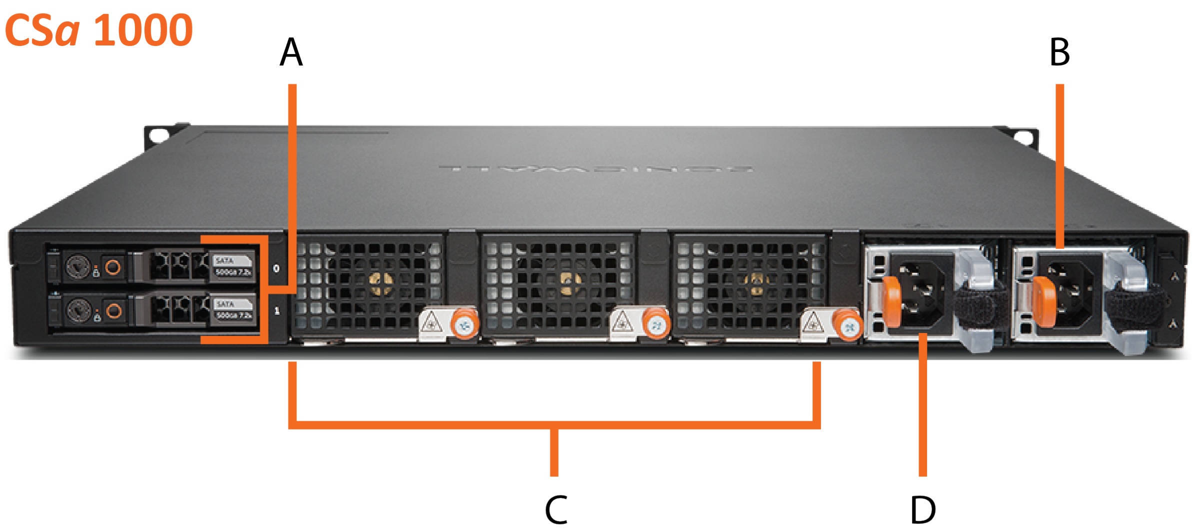


FRONT PANEL COMPONENT DESCRIPTIONS

Item	Description
A	LCD controls
B	Display port - Disabled
C	Console port for serial connection Settings are: Speed=115200, Data bits=8, Stop bits=1, Parity=None, Flow control=None
D	USB ports

Item	Description
E	Reset button
F	Power button
G	X0/X1 - 1 Gigabit interfaces X0 is a Dedicated Management interface X1 can be configured as a WAN interface and used for WAN management
H	X2/X3 - 1 Gigabit interfaces Can be configured as a WAN interface / WAN management
I	X4/X5 - 1 Gigabit interfaces Can be configured as a WAN interface / WAN management
J	X6/X7 - 10G interface Can be configured as a WAN interface / WAN management SFP+ ports - Disabled
K	Diagnostics port - For future use
L	LED indicators – Top to bottom: • Hard disk drive activity • Alarm condition: • Solid Color 1 (Amber)- FIPS errors • Blinking Color 2 (Red)- Approaching non operational state or in non operational state • Slow Blink: DISK > 75% Licenses will expire in 60 days • Medium Blink: Disk > 85% Licenses will expire in 30 days • Fast Blink: Disk >95% Licenses will expire in 15 days • Solid Color - Non operational or degraded operation - Requires immediate attention Disk full, overwriting old files Licenses expired (Most Important) • Test: Off - All fine Blinking - Non-operational state On - In a mode where the user can interact • Power 1 & 2: Blue = Operating correctly Yellow = Unconnected power supply or failure

BACK PANEL ILLUSTRATION



BACK PANEL COMPONENT DESCRIPTIONS

Item	Descriptions
A	Hard drives (2 x 960GB storage modules, RAID)
B	Primary power supply
C	Fans (3)
D	Redundant power supply

In addition to the two RAID disks that contain the appliance data, the CSa1000 also has internal storage used for the operating system and maintenance which is not accessible or serviceable by users.

7

Connect and Power On

This section describes the initial physical setup of your Capture Security Appliance .

To connect and power on your Capture Security Appliance:

1. Install the appliance into a rack with your other networking equipment. The Capture Security Appliance is designed to be mounted in a standard 19-inch rack mount cabinet. Follow the instructions provided in the rack mounting kit shipped with the appliance.
2. Using a standard Ethernet cable, connect the CSa WAN (typically X1) interface to a switch that provides access to the internet.

   This is how the CSa will access licensing services, update servers and access reputation checks. The WAN interface is also used for data transfer from your firewalls, Email Security system and API Connectors. After completing the initial setup, you can use this interface to manage the device.
3. Using the provided Ethernet cable, connect X0 to your management computer. You can use this interface for initial setup and device management by using your browser to access the web management interface.

   ⓘ | **NOTE:** To access the CSa at its default IP address of 192.168.168.168, your computer must be configured with an address on the 192.168.168.x/24 subnet, such as 192.168.168.100.
4. Optionally connect the RJ45 connector of the provided serial console cable to the Console port on the CSa. Connect the DB-9 connector to a serial port on your network device.

   This step is optional because CSa management is not supported from the command line interface (CLI) via the console. The console is only used if the CSa cannot boot up normally or must be put into maintenance mode (SafeMode) for system recovery.
5. Using the provided power cords, connect both the primary and redundant power supplies to an appropriate AC power source (120V). The Power LEDs turn blue and the Test LED blinks until the CSa comes up.

   ⓘ | **NOTE:** To disconnect AC power, both power cords must be removed.

You are now ready to log into your Capture Security Appliance, change the admin password and perform the initial setup. Continue to:

- Change the Administrator Password
- Initial Setup Using Web Management

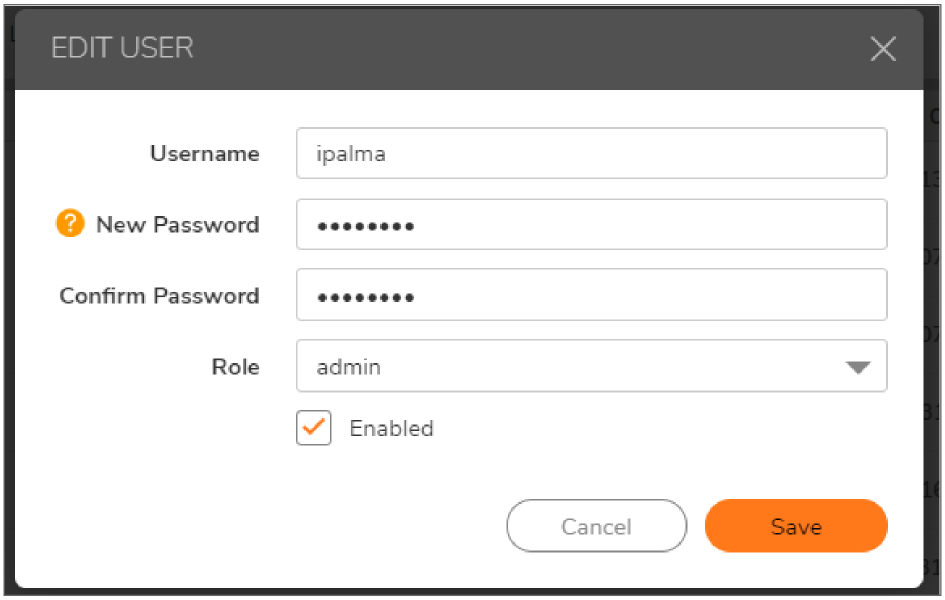
8

Change the Administrator Password

For security, SonicWall recommends that you change the password for the administrator account as the first step of the initial setup of your Capture Security Appliance.

To change the administrator password:

1. Log into the CSa web management interface as the administrator using the default credentials, ***admin / password***.
2. Navigate to the **Configuration > User Management** page.
3. Select the three-dotted menu (...) on the right of the user list to open the **Edit User** dialog.



EDIT USER

Username: ipalma

New Password: ••••••••

Confirm Password: ••••••••

Role: admin

☑ Enabled

4. Type the new password into both the **New Password** and **Confirm Password** fields.
5. Click **Save**.

Continue to Initial Setup Using Web Management.

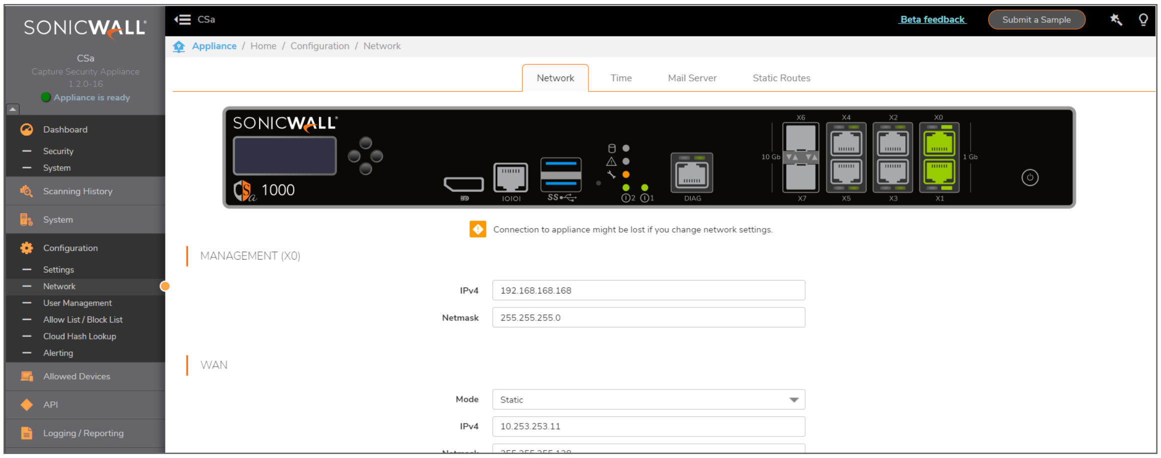
Initial Setup Using Web Management

This section describes how to configure network settings on your Capture Security Appliance, including time zone and mail server settings.

If you haven't already changed the password for the administrator account, SonicWall strongly recommends that you do that right away. (Refer to Change the Administrator Password for instructions.)

To perform initial CSa setup using the web management interface:

1. Point your browser to https://192.168.168.168, the default LAN (X0) IP address.
2. Log into the CSa using the admin account credentials (default: **admin/password**).
3. Navigate to the **Configuration > Network** page.



Connection to appliance might be lost if you change network settings.

MANAGEMENT (X0)

IPv4 192.168.168.168

Netmask 255.255.255.0

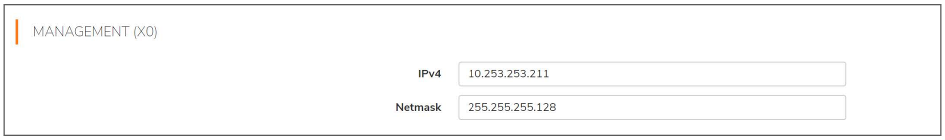
WAN

Mode Static

IPv4 10.253.253.11

Netmask 255.255.255.128

4. Configure the following settings on the **Network** screen:
   - In the **MANAGEMENT (X0)** section, optionally change the IP address of the X0 interface. Set the **IPv4** field to an address on your local management subnet. The default is 192.168.168.168. Change the **Netmask** field as needed for your subnet. The default is 255.255.255.0.

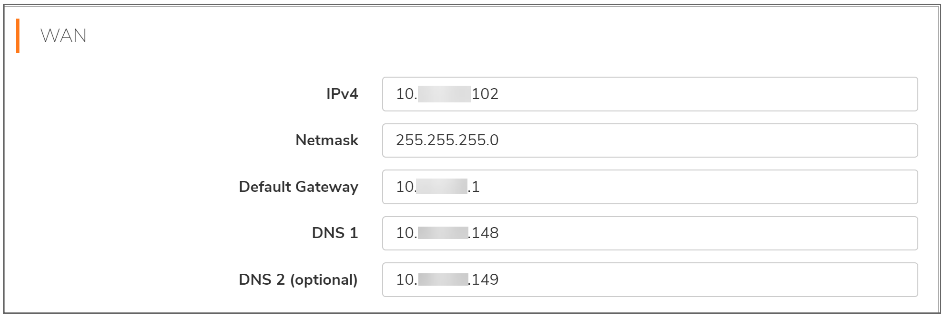


MANAGEMENT (X0)

IPv4 10.253.253.211

Netmask 255.255.255.128

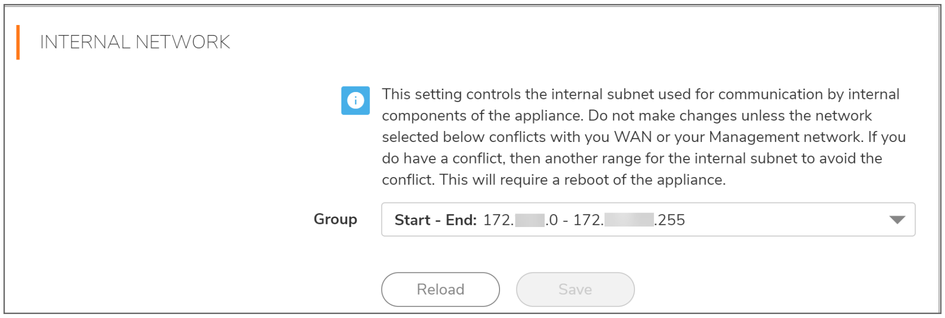
- In the **WAN** section, configure the following settings:
  - **IPv4** – This is the IP address of the WAN interface. Select DHCP addressing if your DHCP server will provide an address, or enter a static IP address on your network. Any interface except X0 can be selected as the WAN/Management interface, including the 10GbE X6/7 ports.



WAN

IPv4	10.[redacted]102
Netmask	255.255.255.0
Default Gateway	10.[redacted].1
DNS 1	10.[redacted].148
DNS 2 (optional)	10.[redacted].149

  - **Netmask** – Enter the netmask for your network in a format such as 255.255.255.0 or 255.255.255.128.
  - **Default Gateway** – Enter the IP address of your gateway device, such as your perimeter firewall.
  - **DNS 1** – Enter the IP address of your primary DNS server.
  - **DNS 2 (Optional)** – Optionally enter the IP address of a secondary DNS server.
- In the **INTERNAL NETWORK** section, optionally select a different subnet. The Internal Network is used for internal communications among the components of the Capture Security Appliance. The default is 172.24.0.0 – 172.31.255.255.

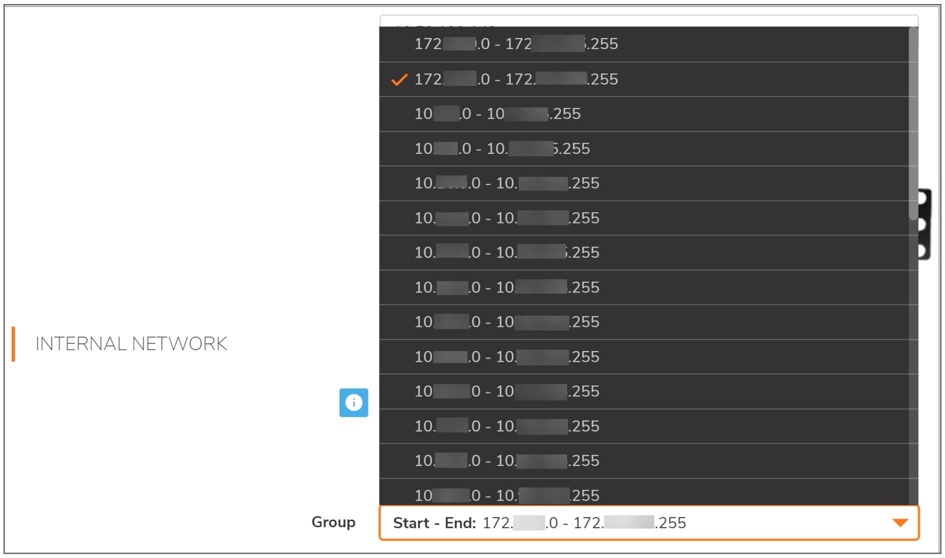


INTERNAL NETWORK

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.

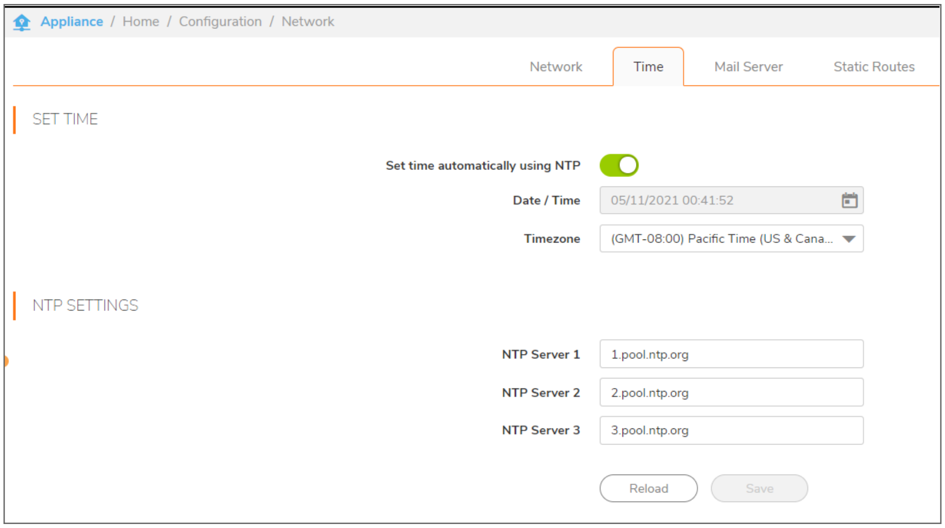
Group: Start - End: 172.[redacted].0 - 172.[redacted].255

If the default subnet overlaps with the CSa WAN or LAN (X0) subnets, you must select a different subnet for the Internal Network from the **Group** list.


INTERNAL NETWORK
172[redacted].0 - 172[redacted].255
✓ 172.[redacted].0 - 172.[redacted].255
10[redacted].0 - 10[redacted].255
10[redacted].0 - 10.[redacted].255
10.[redacted].0 - 10.[redacted].255
10.[redacted].0 - 10.[redacted].255
10.[redacted].0 - 10.[redacted].255
10.[redacted].0 - 10[redacted].255
10[redacted].0 - 10[redacted].255
10[redacted].0 - 10.[redacted].255
10[redacted]0 - 10[redacted].255
10.[redacted].0 - 10.[redacted].255
10.[redacted].0 - 10.[redacted].255
10[redacted]0 - 10.[redacted].255

Group: Start - End: 172.[redacted].0 - 172.[redacted].255

5. On the **Time** screen, select your timezone and optionally enter IP addresses for **NTP Server 1**, **2** and **3**.



Set time automatically using NTP: On

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

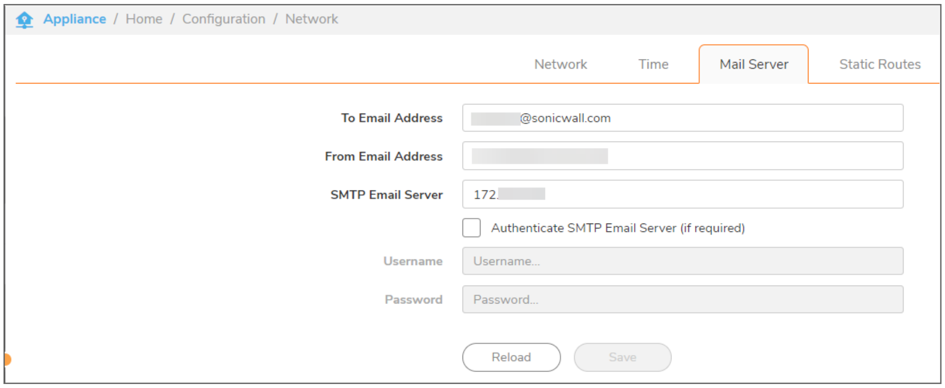
Timezone: (GMT-08:00) Pacific Time (US & Cana...

NTP Server 1: 1.pool.ntp.org

NTP Server 2: 2.pool.ntp.org

NTP Server 3: 3.pool.ntp.org

6. On the **Mail Server** screen, optionally add your mail server settings. SonicWall recommends configuring a mail server.



To Email Address: [redacted]@sonicwall.com

From Email Address: [redacted]

SMTP Email Server: 172.[redacted]

□ Authenticate SMTP Email Server (if required)

Username: Username...

Password: Password...

7. Click **Save** to save your changes.

8. Test connectivity from your management computer by pinging the appliance WAN IP that you just saved, and by accessing it via HTTPS in your browser.

ⓘ **NOTE:** The Management (X0) interface is only used for managing the Capture Security Appliance, while the WAN interface is for data transfer. Therefore, all firewalls, Email Security systems and API Connectors should connect to the CSa WAN interface.
You can manage the CSa on either the X0 or WAN interface.

You are now ready to register your Capture Security Appliance. Proceed to the Register and License section.

10

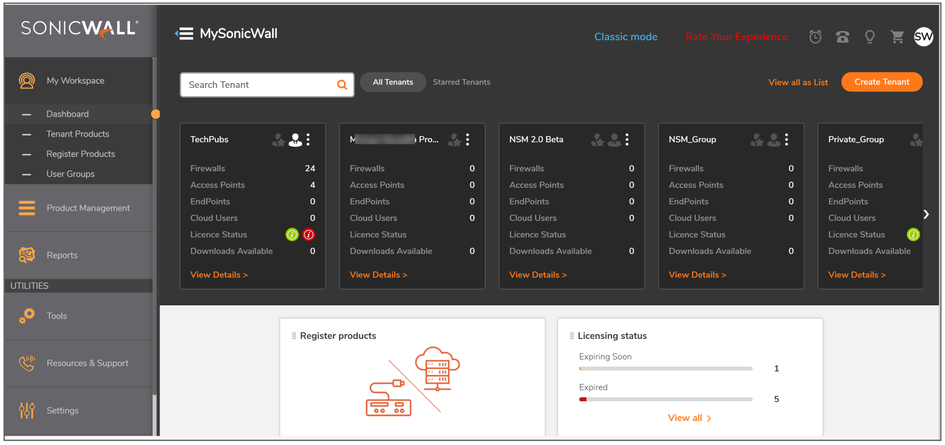
Register and License

Registration and licensing is a critical step in the initial setup of your Capture Security Appliance. Without it, the CSa will not perform file analysis, nor can you update its firmware.

If you do not yet have a MySonicWall account, you can easily create one as described in Creating a MySonicWall Account.

To register and license your CSa:

1. Log into your MySonicWall account at https://www.mysonicwall.com.
2. On the **My Workspace > Dashboard** page, select the **Tenant** for your CSa.



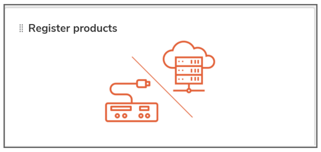
	TechPubs	M[redacted] Pro...	NSM 2.0 Beta	NSM_Group	Private_Group
Firewalls	24	0	0	0	
Access Points	4	0	0	0	
EndPoints	0	0	0	0	
Cloud Users	0	0	0	0	
Licence Status	ⓘ ⓘ				ⓘ
Downloads Available	0	0	0	0	
	View Details >	View Details >	View Details >	View Details >	View Details >

Licensing status

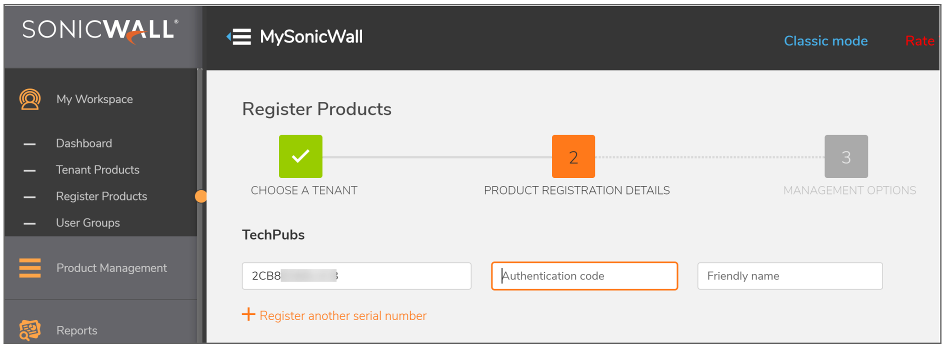
Expiring Soon	1
Expired	5

View all >

3. Click the **Register products** button.



4. On the **Register Products** page, enter the serial number, authentication code and friendly name of your CSa into the indicated fields and then click **Register**.



Register Products

CHOOSE A TENANT — PRODUCT REGISTRATION DETAILS — MANAGEMENT OPTIONS

TechPubs

2CB8[redacted] | Authentication code | Friendly name

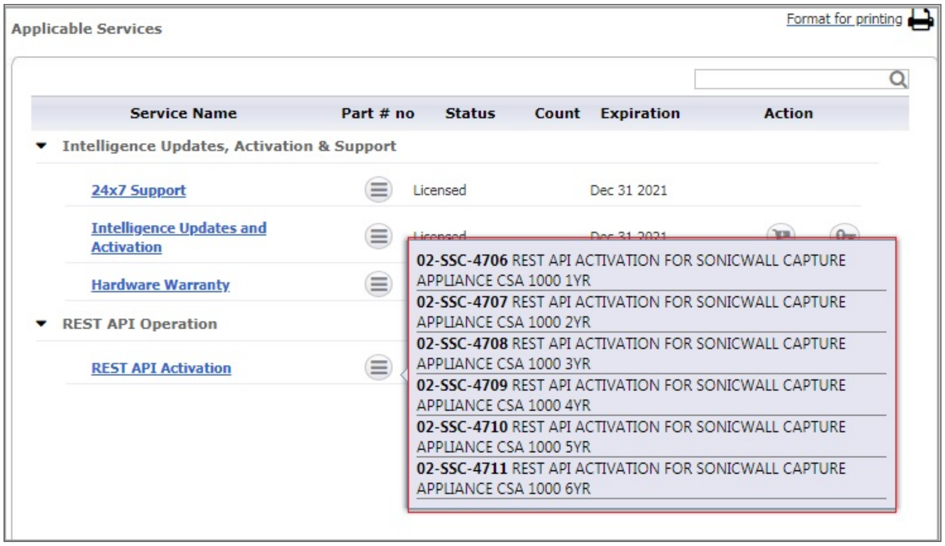
+ Register another serial number

MySonicWall indicates successful registration.

The Intelligence Updates license is activated.

5. Optionally activate a REST API license for your Capture Security Appliance.

   You need a separate license to use an API Connector with the CSa, the REST API ACTIVATION FOR SONICWALL CAPTURE APPLIANCE license. License SKUs are available starting at 1 year and up to 6 years in one-year increments.



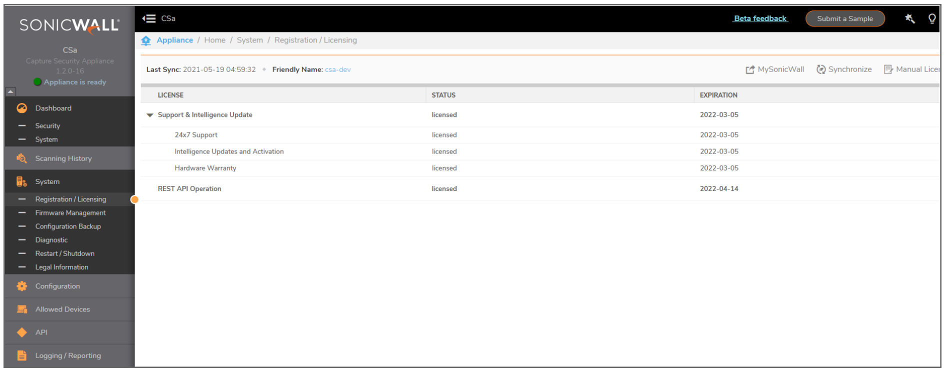
Applicable Services

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

6. Log into your CSa and navigate to the **System > Registration/Licensing** page.

7. On the **Registration/Licensing** screen, click the **Synchronize with License Server** button.



Last Sync: 2021-05-19 04:59:32 • **Friendly Name:** csa-dev

LICENSE	STATUS	EXPIRATION
Support & Intelligence Update	licensed	2022-03-05
24x7 Support	licensed	2022-03-05
Intelligence Updates and Activation	licensed	2022-03-05
Hardware Warranty	licensed	2022-03-05
REST API Operation	licensed	2022-04-14

The CSa pulls licensing information from the SonicWall License Server and is then fully registered and licensed.

The next step is to upgrade firmware on your Capture Security Appliance. For instructions, continue to the Upgrade the Firmware section.

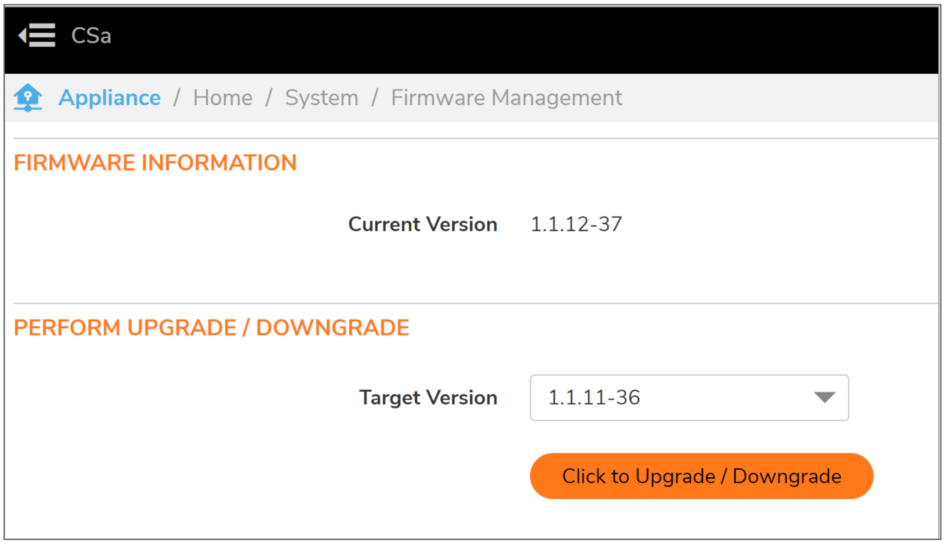
11

Upgrade the Firmware

SonicWall recommends running the latest firmware on your Capture Security Appliance. Your appliance must be registered and licensed in MySonicWall before you can update firmware on it.

To update firmware on your CSa:

1. Log into your CSa as an administrator.
2. Navigate to the **System > Firmware Management** page.


CSa
Appliance / Home / System / Firmware Management

FIRMWARE INFORMATION

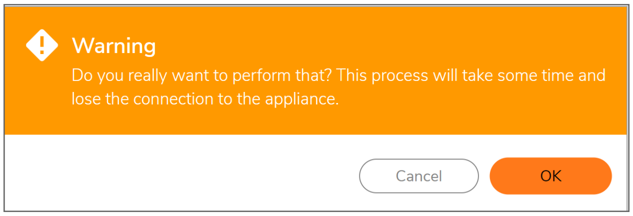
Current Version 1.1.12-37

PERFORM UPGRADE / DOWNGRADE

Target Version 1.1.11-36

Click to Upgrade / Downgrade

3. Select the desired version from the **Target Version** drop-down list.
4. Click the **Click to Upgrade / Downgrade** button.
5. In the Warning popup, click **OK**.



Warning

Do you really want to perform that? This process will take some time and lose the connection to the appliance.

The appliance loads the selected firmware and restarts. This may take a few minutes.

The next step is to configure your Capture Security Appliance to accept files for analysis from your firewalls and other systems. Proceed to Configure Allowed Devices.

12

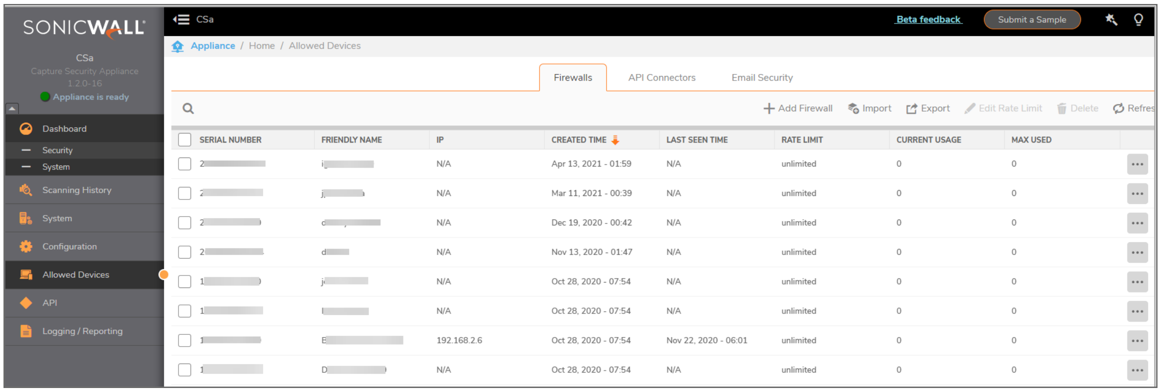
Configure Allowed Devices

Allowed devices are those firewalls, API Connectors, and Email Security systems from which the CSa will accept files for analysis. Configuring allowed devices is therefore a critical step in the initial setup of your Capture Security Appliance.

To begin the configuration, log into your CSa as the administrator and navigate to the **Configuration > Allowed Devices** page.

To add an allowed firewall:

1. 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.



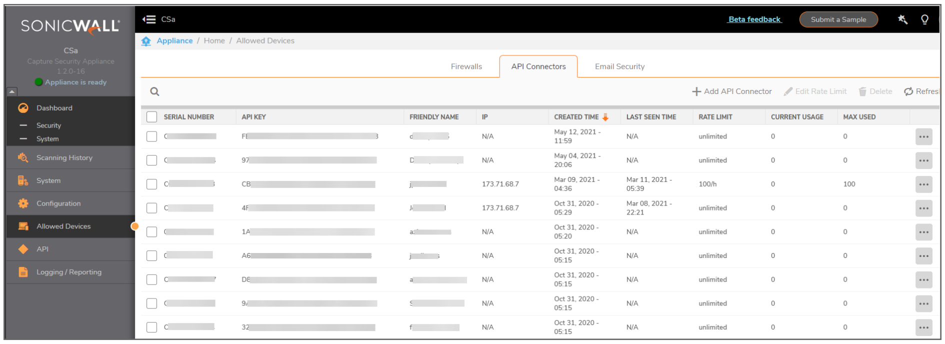
SERIAL NUMBER	FRIENDLY NAME	IP	CREATED TIME	LAST SEEN TIME	RATE LIMIT	CURRENT USAGE	MAX USED
[redacted]	[redacted]	N/A	Apr 13, 2021 - 01:59	N/A	unlimited	0	0
[redacted]	[redacted]	N/A	Mar 11, 2021 - 00:39	N/A	unlimited	0	0
[redacted]	[redacted]	N/A	Dec 19, 2020 - 00:42	N/A	unlimited	0	0
[redacted]	[redacted]	N/A	Nov 13, 2020 - 01:47	N/A	unlimited	0	0
[redacted]	[redacted]	N/A	Oct 28, 2020 - 07:54	N/A	unlimited	0	0
[redacted]	[redacted]	N/A	Oct 28, 2020 - 07:54	N/A	unlimited	0	0
[redacted]	[redacted]	192.168.2.6	Oct 28, 2020 - 07:54	Nov 22, 2020 - 06:01	unlimited	0	0
[redacted]	[redacted]	N/A	Oct 28, 2020 - 07:54	N/A	unlimited	0	0

ⓘ **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.

2. Enter the Serial Number, Friendly Name and Rate Limit information.
3. Click **OK**.

To add an allowed API Connector:

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

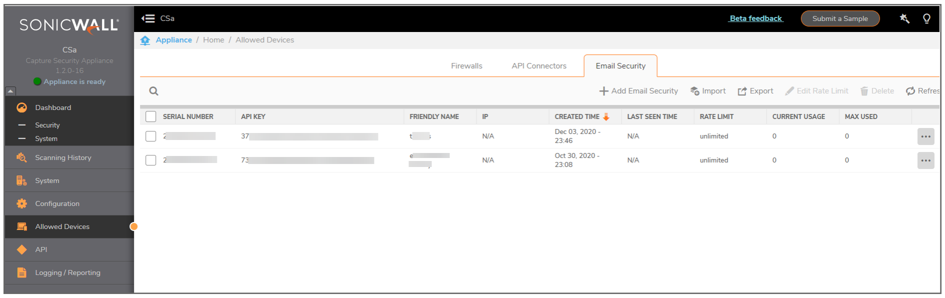


☐	SERIAL NUMBER	API KEY	FRIENDLY NAME	IP	CREATED TIME	LAST SEEN TIME	RATE LIMIT	CURRENT USAGE	MAX USED	
☐	[redacted]	[redacted]	[redacted]	N/A	May 12, 2021 - 11:59	N/A	unlimited	0	0	•••
☐	[redacted]	[redacted]	[redacted]	N/A	May 04, 2021 - 20:06	N/A	unlimited	0	0	•••
☐	[redacted]	[redacted]	[redacted]	173.71.68.7	Mar 09, 2021 - 04:36	Mar 11, 2021 - 05:39	100/h	0	100	•••
☐	[redacted]	[redacted]	[redacted]	173.71.68.7	Oct 31, 2020 - 05:29	Mar 08, 2021 - 22:21	unlimited	0	0	•••
☐	[redacted]	[redacted]	[redacted]	N/A	Oct 31, 2020 - 05:20	N/A	unlimited	0	0	•••
☐	[redacted]	[redacted]	[redacted]	N/A	Oct 31, 2020 - 05:15	N/A	unlimited	0	0	•••
☐	[redacted]	[redacted]	[redacted]	N/A	Oct 31, 2020 - 05:15	N/A	unlimited	0	0	•••
☐	[redacted]	[redacted]	[redacted]	N/A	Oct 31, 2020 - 05:15	N/A	unlimited	0	0	•••
☐	[redacted]	[redacted]	[redacted]	N/A	Oct 31, 2020 - 05:15	N/A	unlimited	0	0	•••

2. Enter the Friendly Name and Rate Limit information.
3. Click **OK**.

To add an allowed Email Security system:

1. 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	
☐	[redacted]	[redacted]	[redacted]	N/A	Dec 03, 2020 - 23:46	N/A	unlimited	0	0	•••
☐	[redacted]	[redacted]	[redacted]	N/A	Oct 30, 2020 - 23:08	N/A	unlimited	0	0	•••

2. Enter the Serial Number, Friendly Name and Rate Limit information.
3. Click **OK**.

This is the last step needed for initial setup of your Capture Security Appliance. You may also wish to configure users, user roles, reporting options and other settings, and you will need to connect and configure your firewalls and other devices to communicate with your CSa. These topics are covered in other SonicWall documentation, described in the Related Documents for Additional Configuration section.

13

Related Documents for Additional Configuration

For information about additional configuration of your Capture Security Appliance, such as configuring users and user roles, and setting up reporting, refer to the:

- *Capture Security Appliance Administration Guide*

Instructions for configuring your firewall to connect to and communicate with the Capture Security Appliance are available in the following SonicOS and SonicOSX documentation:

- *SonicOS/X 7 Capture ATP Administration Guide*
- *SonicOS 6.5 Security Configuration Administration Guide, under Capture ATP*

For information about configuring Email Security to use the Capture Security Appliance, refer to the:

- *Email Security 10.0 Administration Guide*

These administration guides are available on the SonicWall Technical Documentation portal at https://www.sonicwall.com/support/technical-documentation. Filter by product, document type and version, or use the Search field to locate these documents.

For information about using the Capture ATP API, go to https://github.com/sonicwall.

14

Creating a MySonicWall Account

You need to have a valid MySonicWall account to use Capture Security Appliance. A MySonicWall account is critical to receiving the full benefits from SonicWall security services, firmware updates, and technical support. MySonicWall is used to license your site and to activate or purchase licenses for other security services specific to your security solution.

To create a new MySonicWall account:

1. Navigate to https://mysonicwall.com.
2. In the login screen, click **Sign Up**.
3. Enter the email address you want associated with your MySonicWall account.
4. Create a password that meets the security requirements.
5. From the drop-down menu select how you want to use two-factor authentication.
6. Finish CAPTCHA and click on **Continue** to go the Company page.
7. Fill your company information and click **Continue**.
8. On the **YOUR INFO** page, complete the details and select your preferences.
9. Click **Continue** to go to the **EXTRAS** page.
10. Select whether you want to add additional contacts to be notified for contract renewals.
11. To set up additional contacts:
    a. Input the **First name**.
    b. Input the **Last name**.
    c. Add the **Email address** for that person
    d. Click **Add Contact**.
12. Select whether you want to add tax information.
13. If providing tax information:
    a. In the **Reseller for** field, select the state from the drop-down menu.
    b. Add your **Federal Tax ID**.
    c. Add the **Expiry (expiration) Date**.
    d. Enter the **Certificate ID**.
    e. Click on **ADD TAX ENTRY**.
14. Select whether you want to add your distributor information.

15. To set up the distributor information:

    a. Input the **Distributor Name**.
    b. Input the **Customer Number**.
    c. Click **Add Distributor**.

16. Click **Finish**.

17. Check your email for a verification code and enter it in the **Verification Code*** field. If you did not receive a code, contact Customer Support by clicking on the support link.

15

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 Getting Started Guide
Updated - June 2022
232-005486-00 Rev D

Copyright © 2022 SonicWall Inc. All rights reserved.

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