SonicWall®

Getting Started with Management, Reports, and Analytics

SONICWALL®

Contents

1

CSC Overview

SonicWall® Capture Security Center (CSC) is a Web-based application that centralizes management, reporting, and analytics for the SonicWall family of network security appliance and web services. This cloud solution automates the steps to set up an appliance and offers robust reporting and management tools.

IMPORTANT: Before using this document, you need to enable the CSC Management, Reporting or Analytics as described in the *Capture Security Center Help*. This includes setting up your MySonicWall account and profile, registering the firewall, enabling Zero Touch Deployment, if desired, and licensing the service.

If you haven't completed all those tasks, return to Capture Security Center portal and click on Help  . Follow the directions in the section called "Management, Reports, and Analytics." Then return to this document to get started with these services.

This *Getting Started* document helps you rapidly deploy one or more firewalls and to quickly configure necessary protection to get started. It covers the basic management functionality, as well as options for live and scheduled reporting options.

Topics:

System Requirements

Your security infrastructure must meet certain minimum requirements for the following:

Supported Browsers

Since SonicWall is a cloud service, you only need access to a Web browser and an Internet connection to access Capture Security Center. The following browsers are supported:

Browser Supported	Notes
Google Chrome (latest version)	This is the preferred browser for the real-time graphics display on the Dashboard.
Apple Safari (latest version)	

Browser Supported	Notes
Microsoft Edge (latest version)	
Mozilla Firefox (latest version)	

My SonicWall Account

To login into the Capture Security Center and access licensing information, you must have an active MySonicWall account. Your MySonicWall credentials are also used to log into Capture Security Center.

To take advantage of Zero-Touch Deployment, you much also Enable Zero Touch on your MySonicWall account profile. Refer to Prerequisites for information on how to set up an account.

Firewall Types and Firmware

The following firewall models can be managed by the Management, Reports, and Analytics services.

	Management	Reporting	Analytics
Entry Level Firewalls	SOHO-W TZ Series NSv 10-100	TZ Series NSv 10-100	TZ Series NSv 10-100
Mid Range Firewalls	NSA 2500-6600 NSa 2650-6650 NSv 200-400	NSA 2500-6600 NSa 2650-6650 NSv 200-400	NSA 2500-6600 NSa 2650-6650 NSv 200-400
High-End Firewalls	SuperMassive 9000 12K Series NSa 9250-9650 NSv 800-1600	Planned for future releases	Planned for future releases
Zero Touch Deployment	SOHO-W with firmware 6.5.2 or later TZ Series, NSA Series, NSa Series with firmware 6.5.1.1 or later Not supported for SOHO, NSv Series or SuperMassive Series		

Additional requirements include the following:

- Each firewall needs to be licensed with the Comprehensive/Advanced Gateway Security Suite (CGSS/AGSS).
- The firewalls in the configuration must not be associated with a Cloud GMS 1.0 implementation.
- The firewalls in the configuration must be a part of a group.
- Each firewall must have HTTPS management enabled.

IMPORTANT: For manually added firewalls, if a firewall is behind a NAT device, then the HTTPS management port must be opened for the cloud services to communicate with the firewall. This does not apply to firewalls that use Zero-Touch Deployment.

Interface Conventions

When acquiring devices for management and reporting, the **Status** option (viewable on the **HOME**, **MANAGE**, **REPORTS**, **ANALYTICS**, and **NOTIFICATIONS** views) uses colored icons to indicate the various states of the devices being monitored and managed.

Status Icon	Definition
	Indicates that a process is in progress. In some instances, specific details are provided: for example, **Requesting Licenses**.
	Indicates that a process has completed successfully. May provide the message **Success** or something with more detail like **Device parameters set up in Cloud Capture Security Center complete**.
	Indicates that a task is in process or pending the completion of another task. The message **Pending** is usually displayed, as well.
	Indicates a potential issue. Messages provide additional detail to help you resolve the issue.
	Indicates an error. Additional information may be provided via an information icon. Click the icon or mouse over it to see the message:  For example, **Gateway Firewall is not available in CSC**.

Guide Conventions

The following text conventions are used in this guide:

Convention	Use
Bold text	Used in procedures to identify elements in the user interface like dialog boxes, windows, screen names, messages, and buttons. Also used for file names and text or values you are being instructed to select or type into the interface.
Menu divider | Menu item > Menu item	Indicates a multiple step menu choice on the user interface. For example, **System Setup | Users, Groups & Organizations > Users** means find the menu or section divider **System Setup** first, select **Users, Groups & Organizations**, and then select **Users**.
`Computer code`	Indicates sample code or text to be typed at a command line.
`<Computer code italic>`	Represents a variable name when used in command line instructions within the angle brackets. The variable name and angle brackets need to be replaced with an actual value. For example in the segment `serialnumber=<your serial number>`, replace the variable and brackets with the serial number from your device: serialnumber=C0AEA0000011.
Italic	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence, such as the first instance of a significant term or concept.

2

Prerequisites

Prior to configuring and deploying the SonicWall cloud services, you need to create or validate your MySonicWall account. 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, support, or software specific to your security solution. To take advantage of Zero-Touch Deployment, you need to enable it on your MySonicWall account.

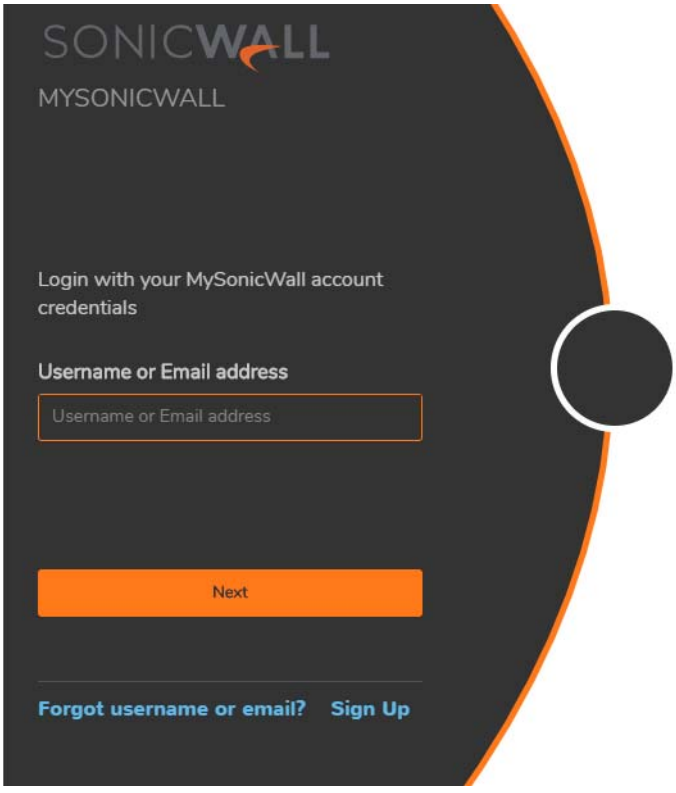
If you already have a MySonicWall account skip to Licensing Cloud Services.

Creating a MySonicWall Account

To create a new MySonicWall account from any computer:

1 Navigate to https://www.mysonicwall.com.

2 In the login screen, click the **Sign Up**.



3 Enter your email address and choose a password that meets the security requirements.

4 Select from the drop-down menu how you want to use two-factor authentication.

5 Finish CAPTCHA and click on **Continue** to go the **Company** page.

6 Fill your company information and click **Continue**.

7 On the **YOUR INFO** page, fill in your details and select your preferences.

8 Click **Continue** to go to the **EXTRAS** page.

9 Select whether you want to add additional contacts to be notified for contract renewals.

10 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**.

11 Select whether you want to add tax information.

> **NOTE:** This only applies to licensed partners or reseller.

12 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.**

13 Select whether you want to add your distributor information.

14 To set up the distributor information:

   a Input the **Distributor Name**.

   b Input the **Customer Number**.

   c Click **Add Distributor**.

15 Click **Finish**.

16 Check your email address 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.

Enabling Zero Touch

Zero-Touch Deployment allows firewalls to be automatically acquired by your network infrastructure with minimal user intervention. It pushes policies, performs firmware upgrades and synchronizes licenses. You must opt in for Zero-Touch Deployment by setting it up in your MySonicWall profile.

To set up Zero Touch:

1 Login to your MySonicWall account.

2 Navigate to **Reports > Registered Products**.

3 Click on a product's serial number.

4 In the PRODUCT DETAILS page, under Active Support, toggle **Enable Zero Touch** switch.

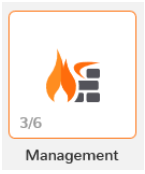
3

Licensing Cloud Services

Capture Security Center Cloud Services are offered in several different packages. Each package offers different features to meet your needs.

Licensing Packages

SonicWall offers several licensing packages for the management, reporting, and analytics web applications.

Package	Description	CSC Tile
Basic Management	Provides basic firewall management at the unit level. Is automatically included when purchasing the Capture Security Center for your firewall.	
Management	Includes a more robust set of management features including group management, inheritance, work flows and others.	
Management and Reporting	Combines full management with a reporting subscription. The reporting includes status reports, Live Monitor, dashboards, and the ability to download or schedule reports.	 
Analytics	Adds additional data collection, analysis, and drill down capability. Also includes the license for Cloud App Security (CAS). This product can be added to any level of Management service.	 

Registering your Appliance

Before starting this section, be sure to have the serial number and the authentication code. You can get that from a label on the firewall or on the box it came in. If you are not using Zero-Touch Deployment, you can log into the firewall and find the data on the following page: **Current Status | System Status** page on the **MONITOR** view.

To register the appliance:

1 Navigate to https://cloud.sonicwall.com.

2 Login with your MySonicWall credentials to get to the **Capture Security Center**.

3 Select the **MySonicWall** tile.

4 On the MySonicWall **Dashboard**, click on the Add Product icon.

5 Enter the serial number or activation key and click **Confirm**.

6 Enter a **Friendly name** and the **Authentication code**.

7 Select the **Tenant Name** from the drop-down menu.

8 Click **Register**.

> **NOTE:** The unit must be manually added if Zero Touch Deployment is not enabled. If it is enabled, the unit automatically added and acquisition begins as soon as the unit is powered on.

9 Navigate back to the Capture Security Center by clicking the down arrow at the top of the screen:

10 Click the **Licensing** tile.

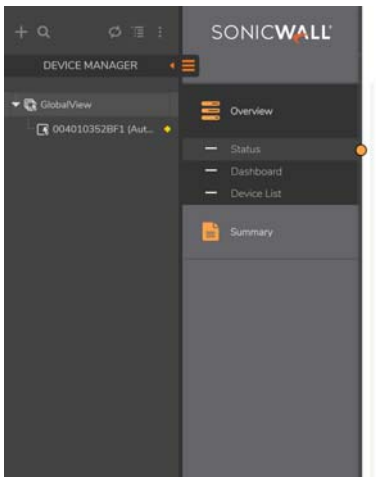
11 Click the **Try** button next to the firewall you are setting up.

Wait for a few seconds until you see the green confirmation at the bottom of the screen.

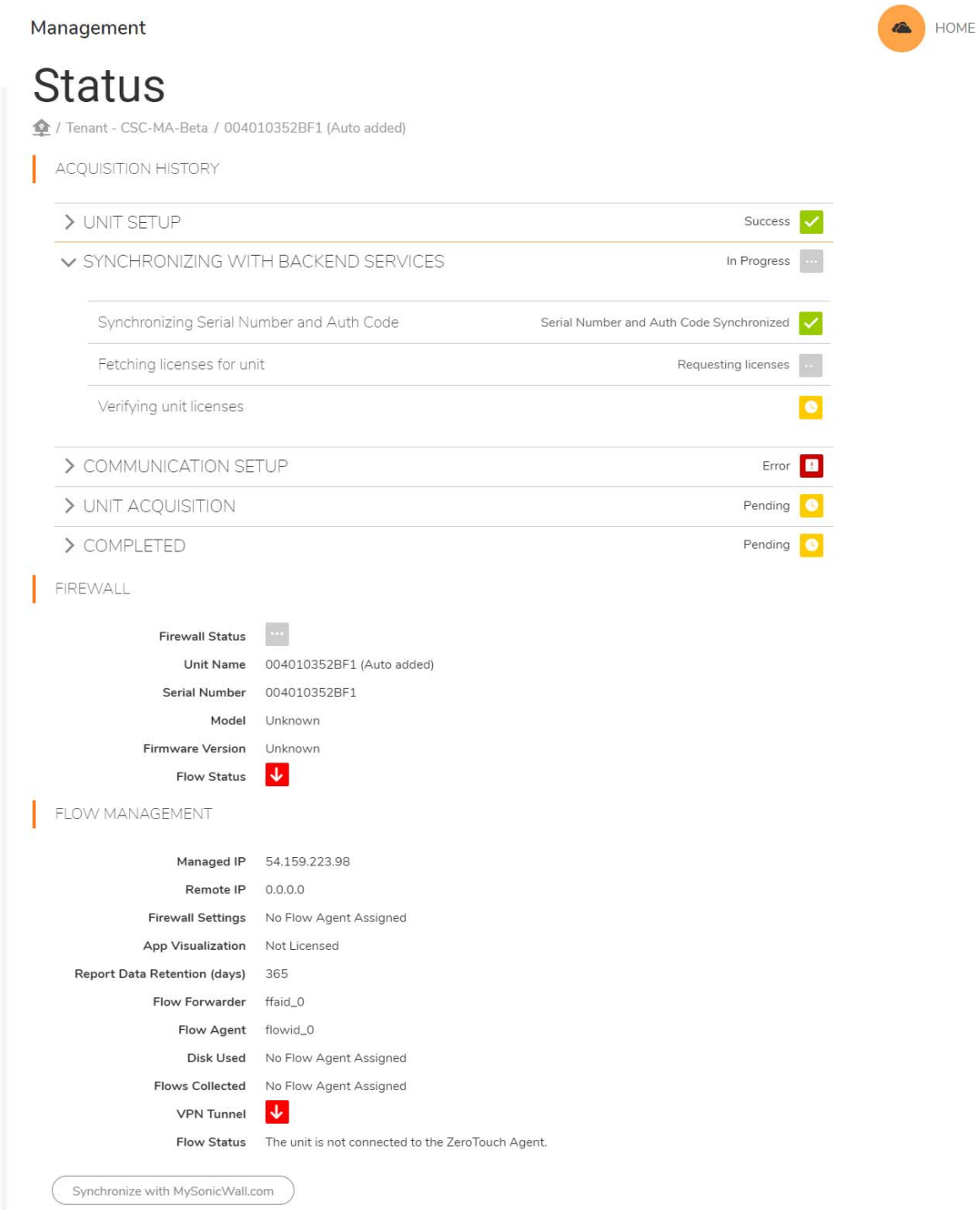
> **NOTE:** If you get a red error message, take the appropriate corrective action and try again.

12 Navigate back to the Capture Security Center by clicking the down arrow at the top of the screen:

13 Click on the **Management** tile. The Status window appears but no firewall is listed when you log in the first time.



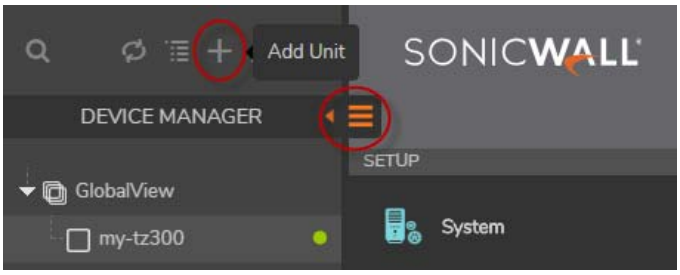
If Zero Touch Deployment is enabled, the firewall is added to Capture Security Center, and the system automatically acquires the firewall so long as it has power applied. The following figure shows the progression of a firewall acquisition. For more information about the other sections of this option, refer to *SonicWall **HOME** Administration*.



To manually add the appliance:

1 In the **DEVICE MANAGER** pane, click on the **Expand** option:

2 Select **Add unit**.



NOTE: If the **DEVICE MANAGER** pane is not visible, click on the orange options icon to expand the view.

3 Enter the following data in the popup window:

- Unit Name
- Serial Number
- IP Address
- Login Name
- Password

NOTE: You can expand the advanced section if you want to acquire the device without giving the IP address. This requires you to configure the firewall to point to **cloud.sonicwall.com**.

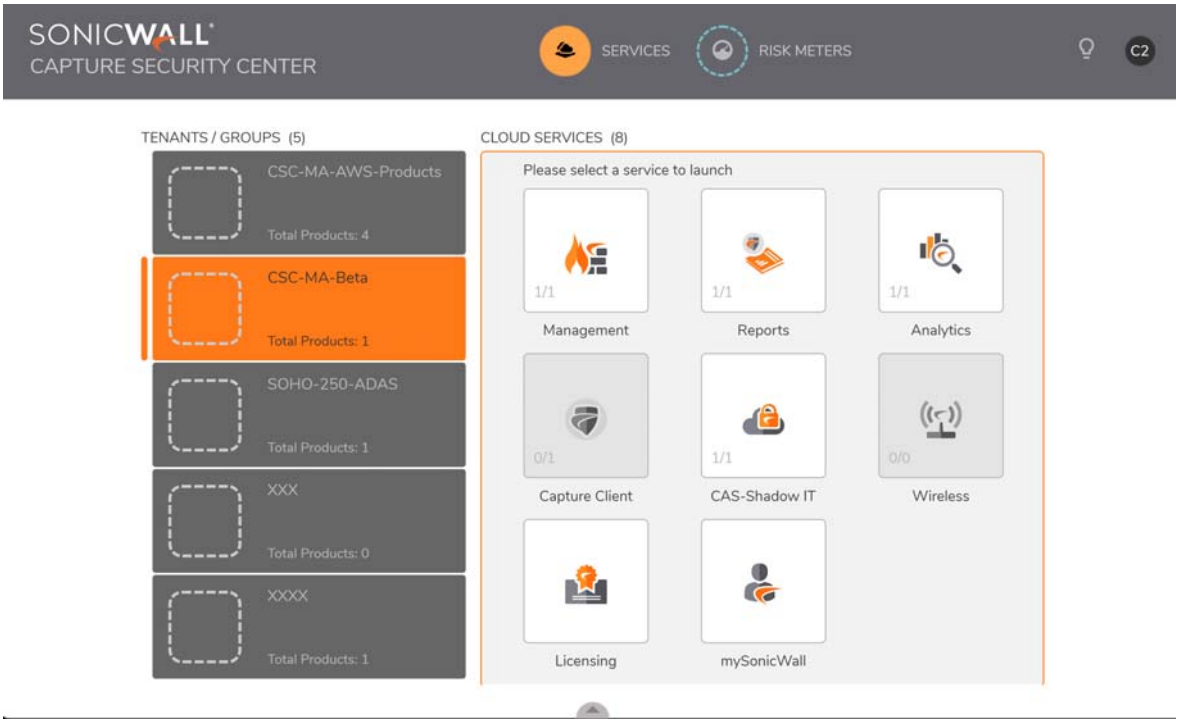
4 Wait for the firewall to get fully acquired. This may take about two to four minutes. Some of the data may take up to 10 minutes to become visible.

You can monitor the acquisition on the **Status** window. Simply expand each of the sections to see the completed steps. When finished, the status shows all green and the firewall status shows a green up arrow. Some of the data on the Dashboard and other summary reports may take up to 15 minutes to appear.

Navigation

You can use the Capture Security Center to navigate between the web service offerings. On the **SERVICES** view, which is the default shown in the following figure, you can see quickly which services are active by looking at the tiles. The active services are white and selectable, and the disabled services are grayed out. Click on a tile to access that service.

You can also click on the **RISK METERS** view to see a summary of the data coming into the SonicWall Capture Labs. It provides a three-page view of the worldwide attacks: world-wide attacks over the last 24 hours, Capture Labs threat metrics, and Security News.



Moving between Services

You can move easily between services on the Capture Security Center. Click on a tile to activate a service and click on the down arrow at the top, , to return to Capture Security Center. Clicking the up arrow at the bottom of Capture Security Center, , allows you to return to the most recently accessed service.

Management

Management offers two top level navigation items.

Views	Function
MANAGE	The **MANAGE** view provides commands grouped by function. The functions include: **SETUP**, **SYSTEM**, and **SECURITY** for the device selected. The commands under each function can be expanded for additional options. These commands can be used to manage your appliances. When you initially select **MANAGE**, the default view is the **Setup| System > Status**.
CONSOLE	The **CONSOLE** view provides commands grouped by function. The functions include: **WORKFLOW**, **TOOLS**, **SYSTEM SETUP**, and **HELP** for the device selected. The commands under each function can be expanded for additional options. These commands can be used to manage your appliances. When you initially select **MANAGE**, the default view is the **Tools | View Log**.

Reports

Reports offers two top level navigation items.

Views	Function
HOME	The **HOME** view provides an **Overview** and **Summary** of the device selected. You can expand each of these options for more details. When you initially select **HOME**, the default view is the **Overview > Dashboard**.
REPORTS	The **REPORTS** view provides the options for **Overview**, **Details**, and **Scheduled Reports** for the device selected. You can expand each of those options for more details.

Refer to *SonicWall **HOME** Administration* and *SonicWall **REPORTS** Administration* for more information.

Analytics

The **ANALYTICS** view provides the options for **Overview**, **All Traffic**, **Web Activities**, **Blocked** and **Threats**. You can expand each of those options for more details. When you initially select **ANALYTICS**, the default view is the **Overview > Status**.

Refer to *SonicWall **ANALYTICS** Administration* for more information.

Notifications

The **NOTIFICATIONS** view covers important alerts and notifications. It shows you firmware details like the number of firewalls configured in Capture Security Center and flow reporting license details. You can synchronize Notifications with your MySonicWall account.

4

Operations Review

The Management, Reports, and Analytics offer many different features for monitoring and managing your security infrastructure. A few key features are highlighted here.

Topics:

Dashboard

The Dashboard provides a visual status of the security infrastructure. You can quickly see whether you have issues and where to focus to resolve them.

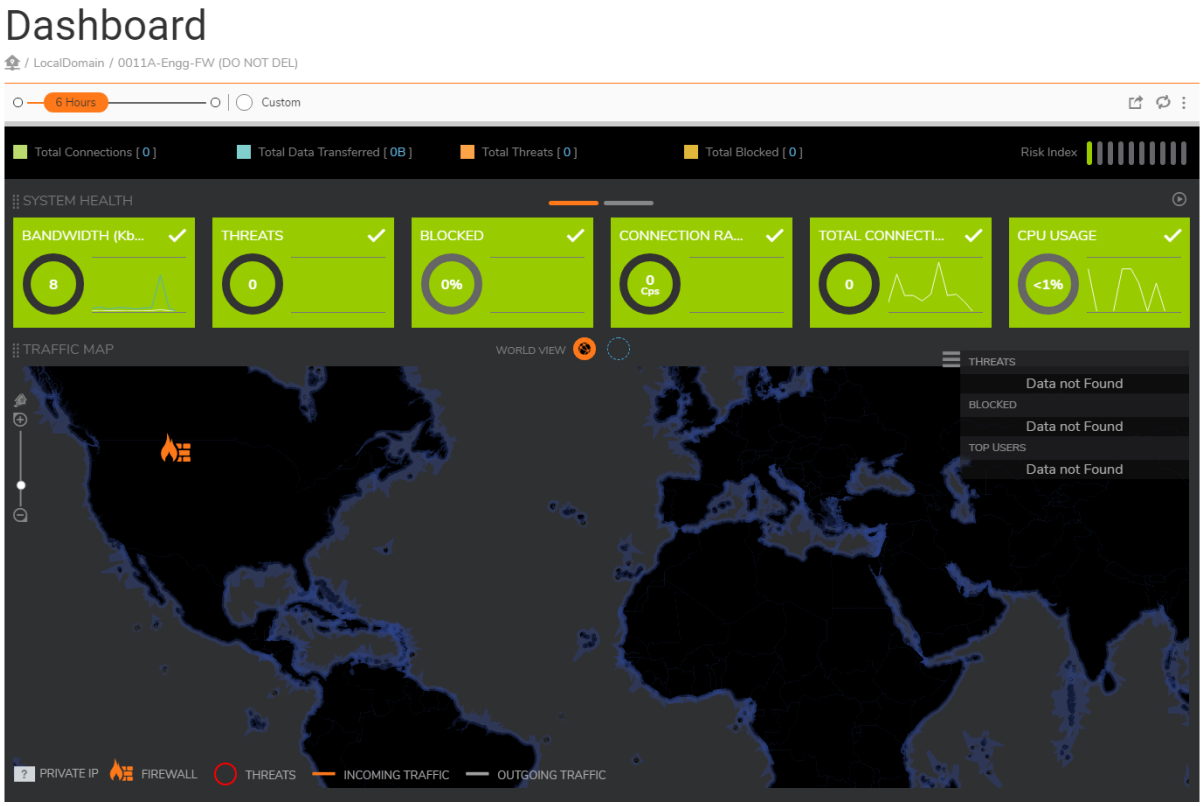
The Dashboard view can be customized by using the options above the map.

- Use the sliding bar to change the time interval displayed in the map.
- Use the **Custom** option to define a specific period to be covered.
- The bar graph in the upper right corner shows the risk index. A single green bar indicates very low risk. More bars and colors that progress towards red indicates higher risk.

The Dashboard has two views. You can toggle between views by clicking on the short orange lines above the map; they act the same as tabs.

- **SYSTEM HEALTH** shows the status of the appliance and includes BANDWIDTH, THREATS, BLOCKED, CONNECTION RATE, TOTAL CONNECTIONS, and CPU USAGE.
- **TOP ATTACKS** shows data about potential threats and includes TOP ATTACKER IP, TOP BOTNET IP, TOP ATTACK ORIGIN, TOP VIRUS, TOP SPYWARE, and TOP INTRUSIONS.

On the Dashboard, you can also toggle between **WORLD VIEW** and **GRID VIEW** to access **TRAFFIC MAP** or **TRAFFIC SUMMARY**.



Threats

You can get information about threats from a number of different displays throughout Management, Reports and Analytics. Any threat can be initially viewed on the Dashboard and from there you can drill down on a number of different options.

NOTE: The ability to drill down to specific details of an incident is dependent up on the licensing options you purchased. Having Management and Reporting with Analytics added on ensure the broadest access to information.

To get additional detail on a threat, you can double-click on the Threats tile on the Dashboard to see the details. Other options include:

- Navigate to **Home | Summary > Threats** to see top three threats based on what was detected or what was blocked.
- Navigate to **Reports | Details > Threats** to get a list view of all the threats detected. You can see the results in a grid-only view or chart view.

Network Topology

The Network Topology feature of Analytics and Management offers a topological view of your network infrastructure for monitoring and management. To view threats from a topological view, navigate to the **ANALYTICS** view in Analytics, and select **Overview > Network Topology**. You can then click on each of the devices to see its status.

In Management to see your devices in the topology view, navigate to the **MANAGE | SETUP > Network > Topology View**. You can click on any of the devices in the topology to see details about the device. You can also export the topology graph to a PDF file using Export/Download Options at the topology view.

NOTE: If the appliance hasn't been acquired properly and doesn't show an active green up arrow, the device does not appear in Network Topology.

5

SonicWall Support

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

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 video tutorials
- Access MySonicWall
- 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

Legend

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

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

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Getting Started with Management, Reports and Analytics
Updated - February 2019
232-004725-00 Rev A