



Capture Security Center

User Guide

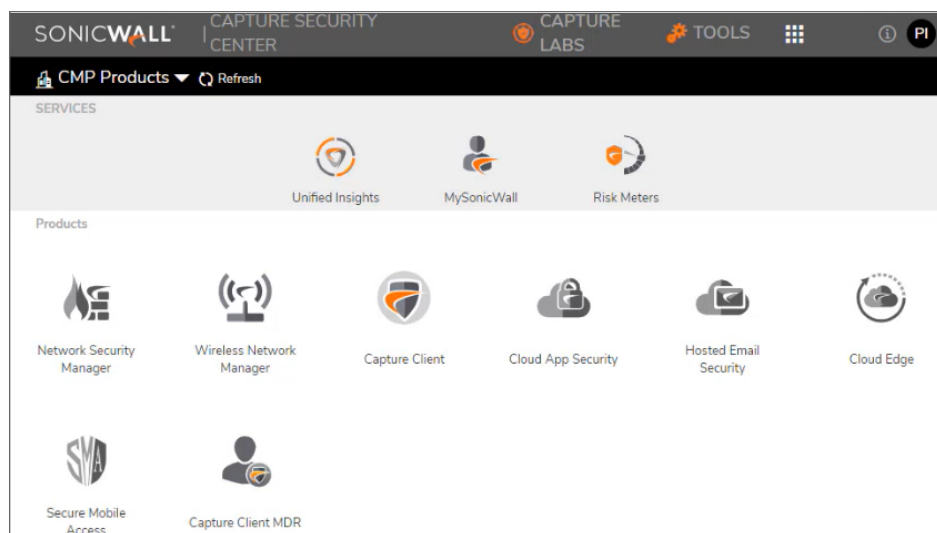
SONICWALL[®]

Contents

Overview	3
User Profile	4
Tenant Selector	4
Services	5
Products	5
Product Status	6
Products Tiles	7
Using Unified Insights	9
Using the Unified Insights Dashboard	9
Customizing Widgets on the Unified Insights Dashboard	10
Grouping Data on Widgets on the Unified Insights Dashboard	11
Moving Widgets on the Unified Insights Dashboard	11
Adding Widgets to the Unified Insights Dashboard	12
Removing Widgets from the Unified Insights Dashboard	12
Saving the Layout of Unified Insights Dashboard	13
Exporting the Unified Insights Dashboard as a Report	13
Generating Capture Security Center Reports	13
Creating Unified Insights Reports	14
Downloading Unified Insights Reports	19
Deleting Unified Insights Reports	20
Using Risk Meters	21
Navigating the Risk Meter Views	21
Risk Meters View	22
Personalized Tenant-Level Threat Data	23
Defense Layers	23
DEFCON and Shield Levels	24
What-If Analysis	26
Threat Metric	27
Third-Party Configuration	28
Worldwide Attacks View	29
Threat Metrics View	30
Security News View	31
SonicWall Support	32
About This Document	33

Overview

The landing page for SonicWall Capture Security Center acts as a single access point for the cloud services and products you can license from SonicWall Inc..



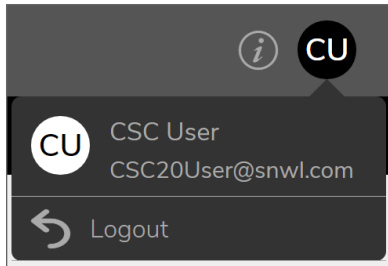
Capture Security Center has been designed to improve the user experience and access to SonicWall services and products. The key improvement is the ability to open different applications to different tabs or windows. This enables cross-product data reviews for easier incident response. The Capture Security Center interface is divided into these segments:

- [User Profile](#)
- [Tenant Selector](#)
- [Services](#)
- [Products](#)

User Profile

The gray bar, or segment, at the top of the screen contains the **Information** link and **User Profile** options. Click the **Information** link and a new tab opens displaying *SonicWall Capture Security Center Information*.

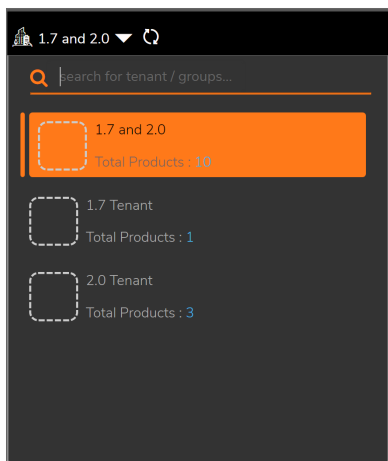
Click the **User Profile** link to see the full name and the user ID of the user logged in. The **Logout** option is also listed here. Click **Logout** to exit the program.



IMPORTANT: When you select **Logout** from the Capture Security Center curtain, the user will be logged out of all tabs and products opened by that user.

Tenant Selector




The black bar, or segment, towards the top of the screen displays the **Tenant Selector**.



Click the down arrow to see the list of tenants and select the one whose data you want to view. The tenant selection is preserved and applied to your next **Services** or **Products** selection. Click the **Refresh** icon if you made changes to your tenant list and need to update it in this view.

Services

The applications that appear in the **Services** segment are services that apply to all SonicWall products. These cross-product services are currently available through the Capture Security Center. Click the tile to access the service.

Service	Description
 Unified Insights	<p>Unified Insights is our single pane of glass for Unified Security Operations, including aggregated dashboards, customizable layouts, and simplified reporting.</p> <p>Select the Unified Insights tile to access the Unified Insights dashboard, providing aggregated dashboards, customizable layouts, and simplified reporting. For more information about using the Unified Insights dashboard, refer to Using the Unified Insights Dashboard.</p>
 MySonicWall	<p>MySonicWall provides direct access to your MySonicWall account without having to log in through another interface. It shows the products and services from SonicWall that you are entitled to. You can register devices, manage your licenses and software, order or renew services, download software and firmware, and access SonicWall support.</p> <p>Select the MySonicWall tile to open your MySonicWall account. The service opens in a new tab, and you can see the products and services from SonicWall that you are entitled to. You can register devices, manage your licenses and software, order or renew services, download software and firmware, and access SonicWall support. Click the Help icon to get specific information about MySonicWall services and options.</p>
 Risk Meters	<p>Risk Meters is an entry point for several risk and threat metrics reports. The Risk Meters view offers a customized risk assessment of your environment; a view of live, world-wide attacks; a summary of the Capture Lab Threat Metrics; and security news items.</p> <p>Select the Risk Meters tile to access tools you can use to assess immediate threat risks and take defensive action with customizable threat data and risk scoring for your entire network infrastructure. Risk Meters are customizable to specific requirements of your network like the security resources presently in operation and the threats your network faces today. For more information on how to navigate and use Risk Meters, refer to Using Risk Meters.</p>

Products

The **Products** segment lists the cloud-based products you can use to manage your security solution. Tiles represent the products; the brightly colored tiles are the products that you have licensed. The faded tiles are products that are not currently licensed for your environment.

Topics:

- [Product Status](#)
- [Products Tiles](#)

Product Status

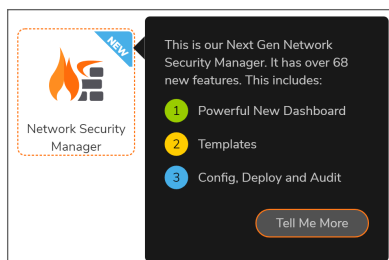
In addition to listing the tiles in the **Products** section, some tiles may display additional indicators.

Topics:

- [New Tag](#)
- [Alert Tag](#)
- [Beta Tag](#)

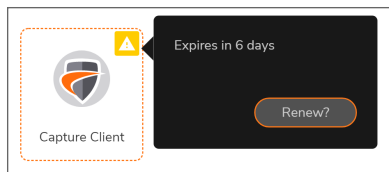
New Tag

The **NEW** tag indicates when a new tile has been added to the products list. If you mouse over the **NEW** tag, a brief introduction pops up and you can click on a link to get more information.



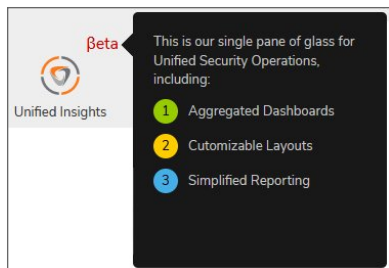
Alert Tag

The **Alert** tag indicates that your license is about to expire. It tells how many days are left and provides a link for renewing. The **Renew?** link takes you directly to MySonicWall to initiate the renewal.



Beta Tag



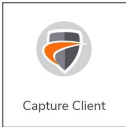

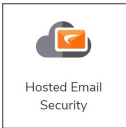
The **BETA** tag indicates that the product is an open Beta release available for testing and feedback.






- ① **NOTE:** For this Beta release of Capture Security Center, these features are not yet supported:
- simplified reporting

Products Tiles

These cloud products can be accessed through Capture Security Center.

Product	Description
	Network Security Manager is a web-based application that centralizes management, reporting, and analytics for the SonicWallfamily of network security appliances. This cloud solution automates the steps to set up an appliance and offers robust reporting and management tools.
	SonicWall Secure Wireless delivers exceptional wireless speed while securing your network and data against encrypted attacks. It includes 8.02.11ac Wave 2 support, 4x4 MU-MIMO, 2.5 GbE port for multi-gigabit wireless performance, three radios including a dedicated security radio, wireless signal and analysis tools, and indoor/outdoor options.
	Capture Client is a unified end point protection platform offering multiple protection capabilities. These include security enforcement, Capture ATP, certificate management, continuous behavioral monitoring, and unique rollback capabilities.
	Cloud App Security solution delivers out-of-band scanning of traffic to sanctioned and unsanctioned SaaS applications using APIs and traffic log analysis. It includes CASB-like functionalities, such as visibility, advanced threat protection, data loss prevention (DLP) and compliance.
	Hosted Email Security deploys a multi-layer solution dedicated to combating emerging threats that attach through email. It can help protect your organization from outside attacks with effective virus, zombie, phishing and spam blocker by leveraging multiple-threat detection techniques. It can also help you better understand email usage, archive for compliance, efficiently perform e-discovery, and audit all mailboxes and access controls to prevent violations.

Product	Description
 <p data-bbox="224 363 289 380">Cloud Edge</p>	<p data-bbox="337 262 1425 363">Cloud Edge is built to respond to the anytime, anywhere business world, whether on-prem or in the cloud. It delivers simple network-as-a-service for site-to-site and hybrid cloud connectivity with Zero-Trust and Least Privilege security as one integrated offering.</p>
 <p data-bbox="224 493 289 510">Secure Mobile Access</p>	<p data-bbox="337 409 1425 510">Secure Mobile Access secures your infrastructure while empowering your workforce. The Secure Mobile Access (SMA) series offers complete security for remote access to corporate resources hosted on-premises, in cloud, and in hybrid datacenters.</p>
 <p data-bbox="224 640 289 657">Capture Client MDR</p>	<p data-bbox="337 556 1425 623">Capture Client MDR combines our unified endpoint protection platform with 24x7 managed detection and response services that includes alert monitoring, investigation, and threat migration.</p>

Using Unified Insights

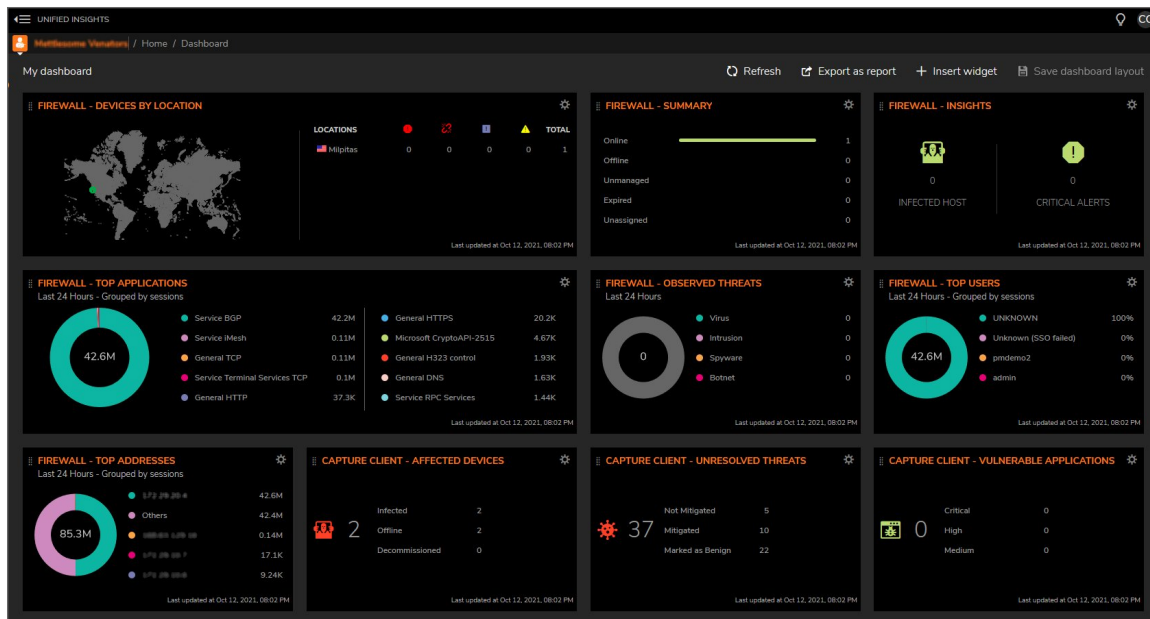
Select the **Unified Insights** tile to access the **Unified Insights** Dashboard and Reports, providing aggregated dashboards, customizable layouts, and simplified reporting.

Topics:

- [Using the Unified Insights Dashboard](#)
- [Generating Capture Security Center Reports](#)

Using the Unified Insights Dashboard

The **Unified Insights** Dashboard provides you with our single pane of glass for Unified Security Operations, including aggregated dashboards, customizable layouts, and simplified reporting.



In its default configuration, the **Unified Insights** Dashboard provides you with summary information about firewalls managed by the tenant and Capture Client activity.

To manually refresh the data displayed on the **Unified Insights** Dashboard, click **Refresh** at the upper right of the Dashboard.

Each of the widgets on the **Unified Insights** Dashboard can be customized and widgets can be rearranged, added, or removed.

Topics:

- [Customizing Widgets on the Unified Insights Dashboard](#)
- [Grouping Data on Widgets on the Unified Insights Dashboard](#)
- [Moving Widgets on the Unified Insights Dashboard](#)
- [Adding Widgets to the Unified Insights Dashboard](#)
- [Removing Widgets from the Unified Insights Dashboard](#)
- [Saving the Layout of Unified Insights Dashboard](#)
- [Exporting the Unified Insights Dashboard as a Report](#)

Customizing Widgets on the Unified Insights Dashboard

You can customize what data appears for a widget on the **Unified Insights** Dashboard.

You can also replace a widget with a different widget in its place without having to perform the separate steps of removing a widget and then adding a new one.

To customize a widget:

1. Click the gear icon located at the top right of the widget.
2. Select **Edit/Replace Widget**. The **Edit/Replace Widget** dialog displays.
3. You can select from these types of widgets:
 - **Firewall**
 - **Capture Client**
 - **Wireless**

The tab associated with the current widget will automatically be displayed. If you are replacing the widget, click the tab for the type of widget you want to add.

4. For the widget, you can specify:
 - **Scope:** Some widget types allow you to specify either **All groups** or **Root Group**.
 - **Widget:** Select the type of widget you want.
 - **Title:** Enter the title you want displayed for the widget. **NOTE:** This a required field.
 - **Time Frame:** Select the time frame for which you want the data to be displayed:

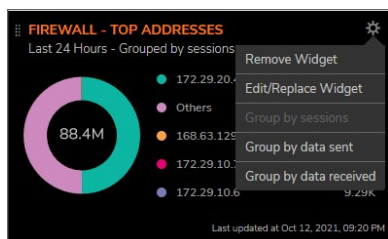
- **Last 24 Hours**
 - **Last 7 Days**
 - **Last 30 Days**
- **Refresh Rate (in seconds):** Enter how often you want the data updated.
5. After you have set all of the options for the widget, click **Save**.

Grouping Data on Widgets on the Unified Insights Dashboard

Some widgets, particularly those that display "top" data for a category, such as a **Top Users** or **Top Addresses**, allow you to group the data displayed in different ways.

To group the data displayed by a widget:

1. Click the gear icon located at the top right of the widget.
2. From the dropdown menu that appears, select the type of grouping you want for the data displayed by the widget.



NOTE: The available ways to group the data depends on the type of the widget and the kind of data that it displays.

Moving Widgets on the Unified Insights Dashboard

You can change the location of the widgets on the **Unified Insights** Dashboard to best meet your own needs.

To move a widget:

1. Hover over the icon at the top left of the widget until it becomes a cursors with four arrows.
2. Click and drag the widget to the location on the Dashboard where you want the widget to be displayed. Other widgets, depending on the size of the widget you are moving, will adjust their positions to fill in any empty space on the Dashboard.

After you have moved all of the widget to their desired locations, you may want to [save the layout of the dashboard](#).

Adding Widgets to the Unified Insights Dashboard

You can add widgets to the **Unified Insights** Dashboard.

To add a widget:

1. Click **Insert widget** on the upper right of the Dashboard. The **New Widget** dialog displays.
2. You can select from these types of widgets:
 - **Firewall**
 - **Capture Client**
 - **Wireless**
3. For the widget, you can specify:
 - **Scope:** Some widget types allow you to specify either **All groups** or **Root Group**.
 - **Widget:** Select the type of widget you want.
 - **Title:** Enter the title you want displayed for the widget. **NOTE:** This a required field.
 - **Time Frame:** Select the time frame for which you want the data to be displayed:
 - **Last 24 Hours**
 - **Last 7 Days**
 - **Refresh Rate (in seconds):** Enter how often you want the data updated.
4. After you have set all of the options for widget, click **Save**.
 - ① **NOTE:** The new widget will be added to the Dashboard in the first empty location where it will fit. You can move the new widget to new a location on the Dashboard. Refer to [Moving Widgets on the Unified Insights Dashboard](#) for more information.
5. Click **Save Dashboard Layout** to save the updated Dashboard configuration.

Removing Widgets from the Unified Insights Dashboard

You can remove widgets from the **Unified Insights** Dashboard if you are not interested in the data it provides or to make room for other widgets.

To remove a widget:

1. Click the gear icon located at the top right of the widget.
2. Select **Remove Widget**.
3. When prompted, select **Proceed** to remove the widget from the Dashboard.
4. Click **Save Dashboard Layout** to save the updated Dashboard configuration.

① | **NOTE:** Removing a widget from the **Unified Insights** Dashboard does not delete it from the system, but makes it no longer visible on the Dashboard. You can **add the widget** again at any time.

Saving the Layout of Unified Insights Dashboard

You can save your layout of the **Unified Insights** Dashboard.

To save your dashboard layout:

1. Click **Save dashboard layout** at the top right of the **Unified Insights** Dashboard.
A status message will be displayed when the layout has been successfully saved.

① | **NOTE:** The saved layout is associated with the user who saved it.

Exporting the Unified Insights Dashboard as a Report

You can export a snapshot of the current **Unified Insights** Dashboard data as a report in PDF format.

The report consists of two pages:

- a graphical title page
- a page containing an image of the **Unified Insights** Dashboard at the time at which the report was generated.

To export the dashboard as a report:

1. Click **Export as report** at the upper right of the Dashboard.
2. A status message displays, informing you to wait until the report has been generated.
3. After the report has been generated, it will be available to you to open or save. (The immediate actions available to you will depend on which web browser you are using.)

Generating Capture Security Center Reports

Select the **Unified Insights** tile to access the **Unified Insights** Reports, providing access to simplified reporting.

To refresh the list of available reports, click **Refresh** in the upper right area of the page.

Topics:

- [Creating Unified Insights Reports](#)
- [Downloading Unified Insights Reports](#)
- [Deleting Unified Insights Reports](#)

Creating Unified Insights Reports

Existing reports for the devices managed by your tenant will automatically be imported into the Unified Insights Reports list.

You can create new Unified Insights reports for:

- [Creating Unified Insights Reports for Firewalls](#)
- [Creating Unified Insights Reports for Capture Client](#)
- [Creating Unified Insights Reports for Wireless Devices](#)

Creating Unified Insights Reports for Firewalls

Create Report Task

Firewall | Capture Client | Wireless

CONFIGURATION

Report Name:

Report Description:

Scope: Advanced | All groups

Report Type: On-demand Report Scheduled Report

Frequency: Time:

Delivery Type: Archive Email

Share via Email:

CONTENT Select All

<input checked="" type="radio"/> Flow Report	<input type="checkbox"/> Live Reports	<input type="checkbox"/> Applications
<input type="radio"/> Management Report	<input type="checkbox"/> Users	<input type="checkbox"/> Sources
	<input type="checkbox"/> Destinations	<input type="checkbox"/> Viruses
	<input type="checkbox"/> Intrusions	<input type="checkbox"/> Spyware
	<input type="checkbox"/> Source Locations	<input type="checkbox"/> Destination Locations
	<input type="checkbox"/> Web Categories	<input type="checkbox"/> Botnet
	<input type="checkbox"/> Blocked	<input type="checkbox"/> Threats
	<input type="checkbox"/> Source VPN	<input type="checkbox"/> Destination VPN

Cancel Save

To create an Unified Insights report:

1. Select the **Unified Insights** tile.
2. Select **Reports** on the left navigation pane.
3. Click **Create Report Task** in the upper right area of the page.
4. In the **Report Name** field, enter a name for the report. This is the name that will be displayed in the list of reports.
5. In the **Report Description** field, enter an optional description for the report.

6. From the **Scope** list, for the specified tenant, select:
 - **All groups** to include devices from all groups in the report.
 - **Root Group** to include only devices from the Root Group in the report.To select other groups or devices, use Network Security Manager.
7. For **Report Type**, select:
 - **Scheduled Report**
 - From the **Frequency** list, select:
 - **Daily**
 - **Weekly**
 - **Monthly**
 - From the **Time** list, select the one-hour time period during which the report should be generated.
 - From the **Scheduled On** list:
 - If you selected **Weekly** from the **Frequency** list, select the day of the week on which you want the report to be run.
 - If you selected **Monthly** from the **Frequency** list, select the numbered day of the month on which you want the report to be run.
8. For **Delivery Type**, select:
 - **Archive** to save the report.
 - **Email** to send the report by email.
 - In the **Share via Email** field, enter the email address(es) to where you want the report to be sent.
 - In the **Email subject** field, enter the Subject line for the email message that will include the report.
 - In the **Email body** field, enter the content for the body of the email message that will include the report.
9. Click **Select All** to generate all of the reports, or select the specific type of reports you want generated for this report task:
 - Select **Flow Report** to generate the flow reports, then select the flow reports you want generated.
 - ① | **NOTE:** Flow Reports are only available with Network Security Manager Advanced licenses.
 - Users
 - Destinations
 - Intrusions
 - Source Locations
 - Web Categories
 - Blocked
 - Source VPN
 - Applications
 - Sources
 - Viruses

- Spyware
 - Destination Locations
 - Botnet
 - Threats
 - Destination VPN
- Select **Management Report** to generate reports for:
 - **Expiring Reports**
 - **Expiring Reports (Free Trial)**
 - **Expired Reports**
 - **Firewall Inventory**

10. Click **Save**.

Creating Unified Insights Reports for Capture Client

NOTE: Capture Client reports are archived for a maximum of 5 days.

To create an Unified Insights report:

1. Select the **Unified Insights** tile.
2. Select **Reports** on the left navigation pane.
3. Click **Create Report Task** in the upper right area of the page.
4. In the **Report Name** field, enter a name for the report. This is the name that will be displayed in the list of reports.
5. The **Scope** displays the name of the current tenant for which the reports will be generated.

6. For **Report Type**, select:
 - **On-demand Report**
 - From the **Interval** list, select:
 - **Last Week**
 - **Last 15 days**
 - **Last 30 days**
 - **Scheduled Report**
 - From the **Frequency** list, select:
 - **Daily**
 - **Weekly**
 - **Monthly**
 - From the **Time** list, select the one-hour time period during which the report should be generated.
 - From the **Scheduled On** list:
 - If you selected **Weekly** from the **Frequency** list, select the day of the week on which you want the report to be run.
 - If you selected **Monthly** from the **Frequency** list, select the numbered day of the month on which you want the report to be run.
7. For **Delivery Type**, select:
 - **Archive** to save the report.
 - **Email** to send the report by email.
 - In the **Share via Email** field, enter the email address(es) to where you want the report to be sent.
8. Click **Select All** to generate all of the reports, or select the specific type of reports you want generated for this report task:
 - **Threats**
 - **Basic**
 - **Detailed**
 - **Threat-History**
 - **Threat-List**
 - **Capture ATP Events**
 - **Basic**
 - **ATP-History**
 - **ATP-List**
 - **Devices**
 - **Basic**
 - **Device-History**
 - **Device-List**

- **Activities**
 - **Basic**
 - **Detailed**
- **Web Protection**
 - **Basic**
 - **Detailed**
- **Applications**
 - **Basic**
 - **Risky-Device-List**
 - **Risky-App-List**
- **Tenants**
 - **Basic**
 - **Tenant-List**

9. Click **Save**.

Creating Unified Insights Reports for Wireless Devices

To create an Unified Insights report:

1. Select the **Unified Insights** tile.
2. Select **Reports** on the left navigation pane.
3. Click **Create Report Task** in the upper right area of the page.
4. In the **Report Name** field, enter a name for the report. This is the name that will be displayed in the list of reports.
5. The **Scope** displays the name of the current tenant for which the reports will be generated.

6. For **Report Type**, select:
 - **On-demand Report**
 - From the **Interval** list, select:
 - **Day**
 - **Week**
 - **Month**
 - **Scheduled Report**
 - From the **Frequency** list, select:
 - **Daily**
 - **Weekly**
 - From the **Time** list, select the one-hour time period during which the report should be generated.
 - From the **Scheduled On** list:
 - If you selected **Weekly** from the **Frequency** list, select the day of the week on which you want the report to be run.
 - If you selected **Monthly** from the **Frequency** list, select the numbered day of the month on which you want the report to be run.
7. In the **Share via Email** field, enter the email address(es) to where you want the report to be sent.
8. Click **Select All** to generate all of the reports, or select the specific type of reports you want generated for this report task:
 - Executive Summary
 - Recommendations
 - Statistics
 - Inventory
 - Security (Client Security Service Details)
 - Topology
9. Click **Save**.

Downloading Unified Insights Reports

To download a single report:

1. Select the **Unified Insights** tile.
2. Select **Reports** on the left navigation pane.
3. Click the three dots (...) on the far right of the line for the report in the list.
4. Click **Download**.

A status message is displayed that indicates whether the download of the report was successful.

Deleting Unified Insights Reports

You can delete reports and report tasks when you no longer need them.

① | **NOTE:** Reports generated for Capture Client cannot be manually deleted. They will be automatically deleted.

To delete a report or report task:

1. Select the **Unified Insights** tile.
2. Select **Reports** on the left navigation pane.
3. Select the report(s) you want to delete by selecting the checkbox to the left of the name of the report.
① | **TIP:** To delete all of the reports, select the checkbox at the top of the list.
4. Click **Delete** at the top right of the page. A confirmation dialog displays.
5. Click **Proceed** to delete the selected reports.

Using Risk Meters

Clicking on **Risk Meters** opens a new tab for the Risk Meter Dashboard provided by Capture Security Center. Risk Meters provides visibility into the active or missing layers of your defense and the resulting risk. Customizable threat data like this provides a very specific defense layer: your real-time, graphics-assisted analysis. Security teams can see potential security gaps, recognize incoming attacks, and monitor all possible threat vectors. **Risk Meters** also includes access to three additional pages of related risk and attack data.

Topics:

- [Navigating the Risk Meter Views](#)
- [Risk Meters View](#)
- [Worldwide Attacks View](#)
- [Threat Metrics View](#)
- [Security News View](#)

Navigating the Risk Meter Views

Each of the **Risk Meter** views can be seen by clicking on the gray bars at the bottom of the window. The bar for the active screen turns orange so you can see where you are relative to the sequence of information presented.



A help icon appears on each of the Capture Security Center views:

Help Icon



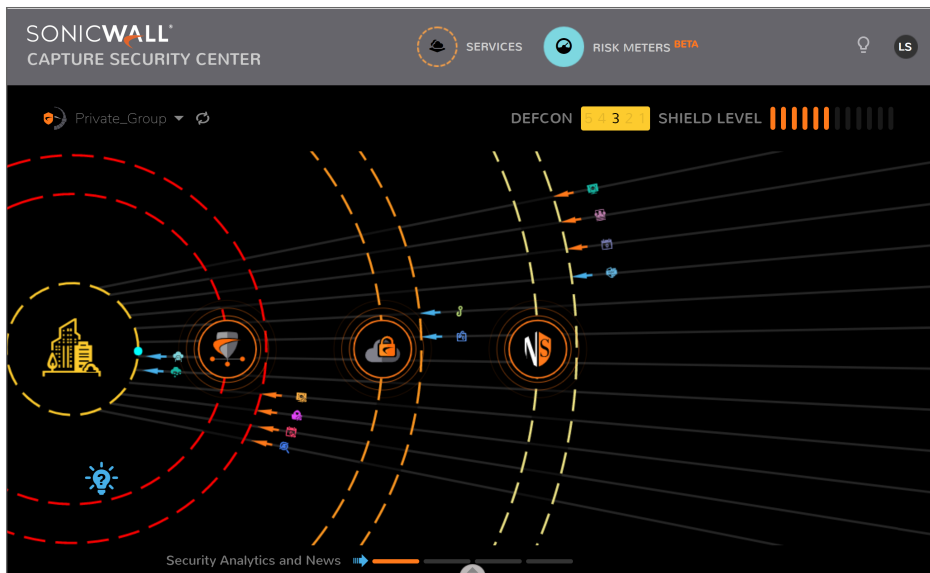
Help Icon expanded



Click on the help icon to show the circular menu. The circular menu provides additional links to other valuable resources. If the help icon or the menu is blocking something, just drag it anywhere on the screen. Click on the X to close the circular menu.

Risk Meters View

Risk Meters provides visibility into the active or missing layers of your defense and the resulting risk. Using Defense Layer Visualization, you can see the impact of active and inactive layers across your infrastructure, allowing you to see at a glance where you may have potential gaps or attack penetration points.

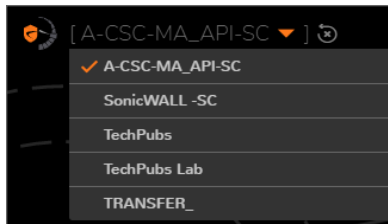


Topics:

- [Personalized Tenant-Level Threat Data](#)
- [Defense Layers](#)
- [DEFCON and Shield Levels](#)
- [What-If Analysis](#)
- [Threat Metrics View](#)
- [Third-Party Configuration](#)

Personalized Tenant-Level Threat Data

Individualized threat metrics at the tenant level allows you to restrict the focus of incoming attacks to a specific environment. The name of the tenant or group being shown is displayed in the top left corner of the **Risk Meters**. To change the tenant or group, click the drop-down list and select a new tenant.



Defense Layers

Three defense layers are currently shown on the Risk Meters.

IMPORTANT: A defense layer in the Risk Meter represents that a particular technology is licensed for use, but it does not indicate whether the layer has been configured in the best possible way to protect you from all threats.



Network Security Analytics and WAF (Web App Firewall) layer accounts for 55% of the overall protection strength and includes threat metrics for:

- Malware
- Intrusion
- Zero-Day Threats
- Web App Attacks



CAS (Shadow IT and SaaS Security) and Email accounts for 12% of the overall protection strength.

It includes threat metrics for:

- Phishing
- Malicious Attachments
- Malware on the Cloud
- Cloud Data Loss



Endpoint Security accounts for 33% of the overall protection strength and includes threat metrics for:

- Endpoint Malware
- Endpoint Exploits
- Zero-Day Endpoint Threats
- Ransomware that needed to be rolled back

Defense layers that are licensed in MySonicWall have the appropriate risk meter shields enabled automatically. The threat vectors that correspond to those defense layers show as being blocked and provide tenant level threat statistics where applicable. If a product does not support tenant level statics, averaged data based on active product customers is used instead. Tenant data is represented by the orange arrows and averages from global data is represented by the blue arrows.

DEFCON and Shield Levels

In the top right corner of the **Risk Meters**, you can see a **DEFCON** (defense readiness condition) score and the **SHIELD LEVEL**.



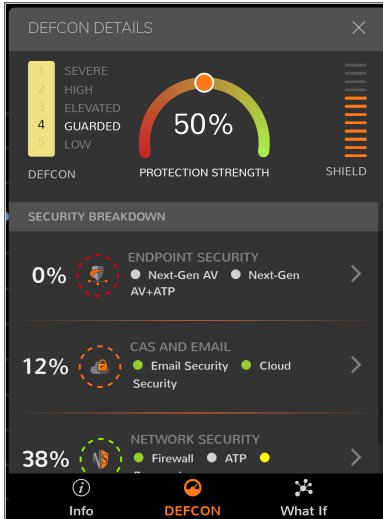
The **DEFCON** score indicates what risk level you face based on your defense layers. They range from 1, which indicates the highest risk (SEVERE), to 5, which is the lowest risk (LOW). Product layers are weighted differently based on the level of protection they provide. For example, firewalls without Capture ATP are less effective than firewalls with Capture ATP.

The **SHIELD LEVEL** indicates how many security measures are in place to protect the infrastructure from threats. The shields are represented by orange bars in the upper right corner. Shields are enabled by default based on the active SonicWall product licenses.

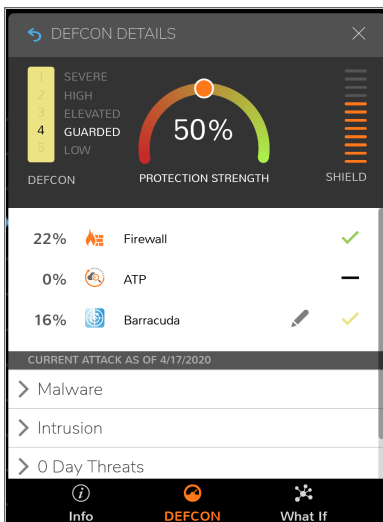
You can drill down to get more data about the details behind the security breakdown.

To see the DEFCON DETAILS:

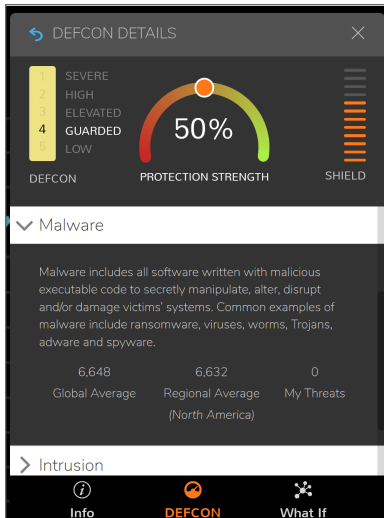
1. Click on either **DEFCON** or **SHEILD LEVEL**. This displays the **DEFCON DETAILS**, including the speedometer. The speedometer represents the cumulative protection level offered by all the licensed SonicWall products.



2. Click on the arrows to drill down for more information. For example, clicking on **ENDPOINT SECURITY** for this system displays this:



3. Click on the arrow next to the threat type and to see more information about that threat. The following example shows the data for **Malware**. You may need to scroll down to see all the information. Click on the blue **Return** arrow in the upper left corner to exit the drill-down.



4. Click on the icons at the bottom for additional data:
 - The **Info** icon provides additional information about the data being displayed on the **Risk Meters**.
 - The **What If** icon shows what changes you could make to get 100% protection.

What-If Analysis

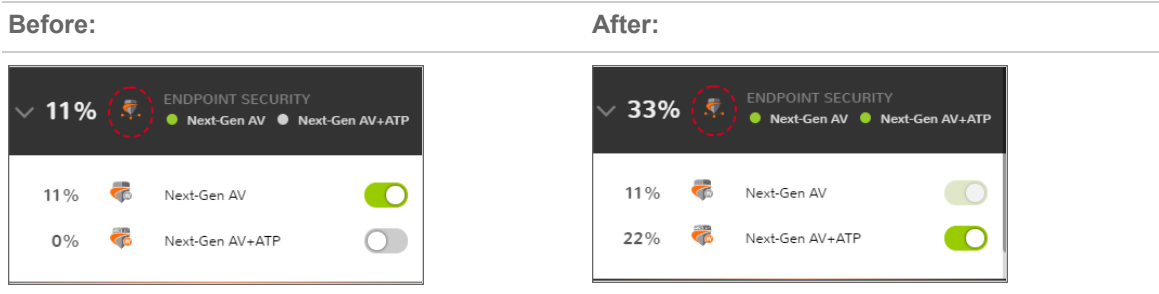
Capture Security Center users can look at how their **DEFCON** and **SHIELD** scores may be impacted using the What-If scenario simulations to turn on or off specific layers. Any change made here can be reset to return to the original **DEFCON** and **SHIELD** scores.

① **IMPORTANT:** All scoring using the **DEFCON** and **SHIELD** metrics are based only on the possibility of protection against the defined threat types and are no guarantees of actual risk posed to the organization.

To access and use the What-If analysis:

1. Click on either **DEFCON** or **SHIELD LEVEL**.
2. Click the **What If** icon at the bottom of the **DEFCON DETAILS** window.
3. Expand any of the options in the **SECURITY BREAKDOWN** section.

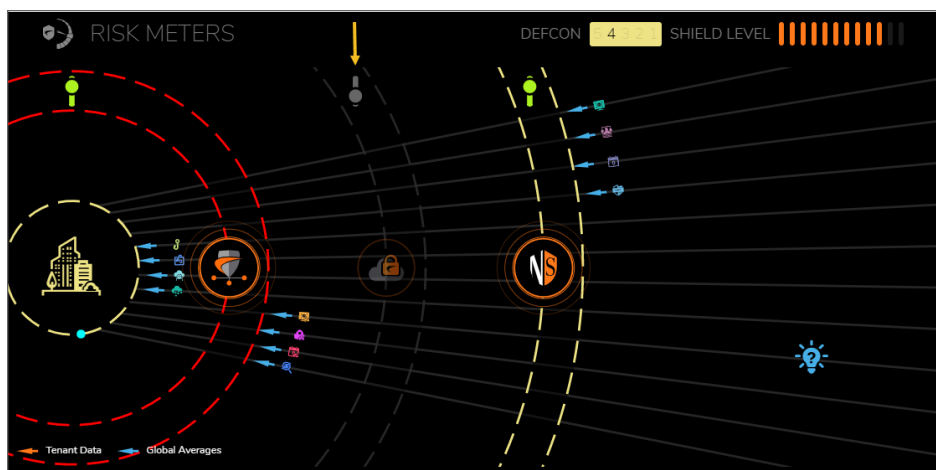
- Make changes to the options provided to see how your coverage changes. **ENDPOINT SECURITY** is shown as an example.



- Make other adjustments in the other layers, as desired.
- To restore the original scores, click the **DEFCON** icon at the bottom of the **DEFCON DETAILS** window.

Threat Metric

For each layer and the associated threat types that it protects against, Risk Meters gathers the individual volume of events (“My Threats”) as well as the Global average and Regional average volumes of events. Drill-down into each layer shows the comparison of these three metrics side by side, allowing you to review how much you are being targeted, compared to your peers in the region and across the globe. Additionally, this comparison also allows you to understand what kind of attacks may be targeting you, especially if you don’t have specific layers enabled.



The color of the arrow for each threat type indicates whether the metric provided is global averaged data or personalized tenant data. The blue arrows indicate Global Averages, which are calculated values showing the average per SonicWall customer. The orange arrow indicates tenant data, which represents data for the specified tenant. All metrics are calculated daily and show averages for the last 30 days.

① | **NOTE:** If a product does not support tenant-level statistics, averaged data is used instead.

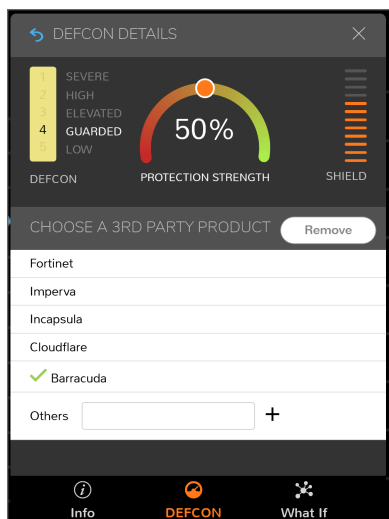
You can also get additional information on each of the individual threat vectors. Click on the icon for a threat vector and window pops up showing more information about that particular threat. Some descriptions are long so scroll down to access all the data.

Third-Party Configuration

If you have not purchased a SonicWall license, but have a third-party product deployed to mitigate the threats that the SonicWall layer would protect against, you may identify the product and the **DEFCON** score and **SHIELD** levels are updated to consider the deployment of your third-party product. Note that this still shows a “0” count under the **My Threats** section for each threat type.

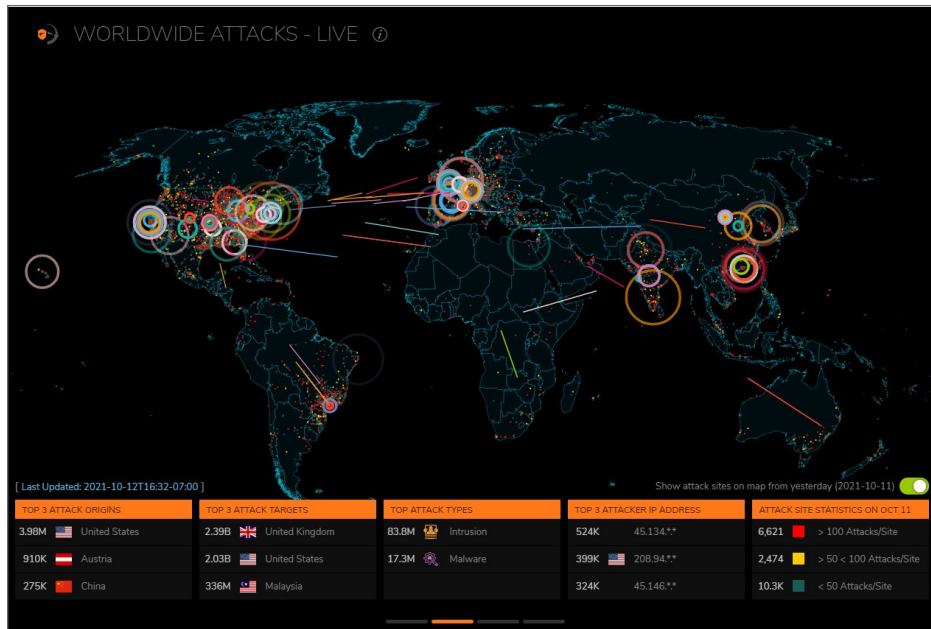
To access the third-party configuration:

1. Click on either **DEFCON** or **SHIELD LEVEL**.
2. Expand **ENDPOINT SECURITY**.
3. Click on the **Edit** icon.
4. Select one of the third-party products listed and click **Apply**. The following example shows a Barracuda device already added.



Worldwide Attacks View

WORLDWIDE ATTACKS shows a live view of active attacks being made across the world. It shows the rolling 24-hour attack statistics, updated every minute. You can see where the attacks originate from and where they hit.



The thickness of the line indicates relative volume: a thicker line means more attacks than a thinner line. You can also show the attack sites from the previous day (when the switch is slid to green). These are shown as red, yellow and green dots, depending on the number of attacks per site on that day.

Other top-trending information is also shown. Use the large gray/white dots under the table to navigate between options.

- Top 3 attack origins
- Top 3 attack targets
- Top attack types
- Top 3 attacker IP addresses
- Attack site statistics from yesterday

Threat Metrics View

CAPTURE LABS THREAT METRICS summarizes the type of attacks being made and how they are trending.

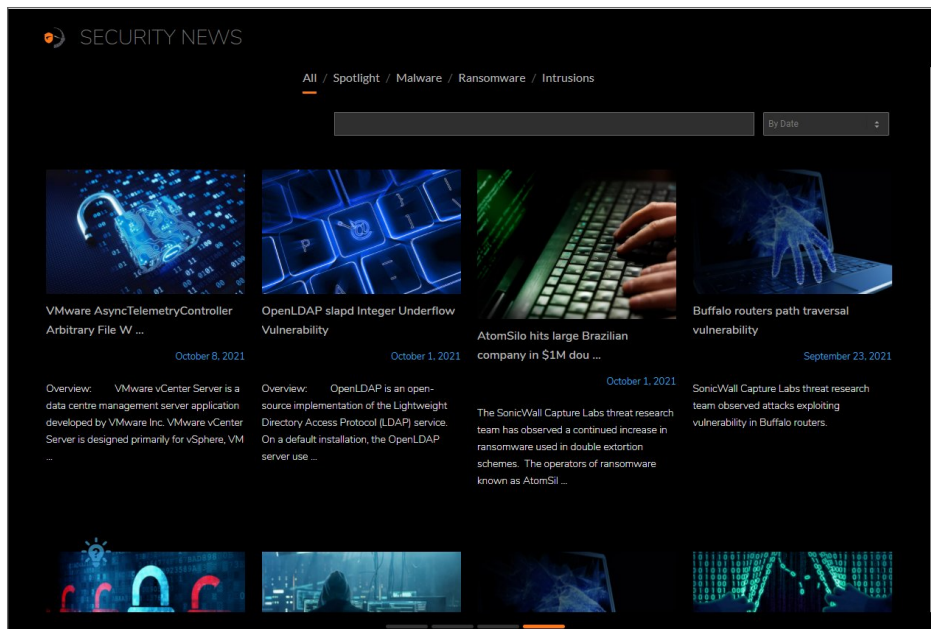


As you click on each threat type, the graph changes to show the details for that threat. It includes comparisons from current year to previous year, including a monthly break down. Top attack or target origins are also listed and graphed. By selecting the abbreviations on the right, you can filter the graph by region:

- **WW** (worldwide)
- **NAM** (North America)
- **EU** (Europe)
- **APJ** (Asia Pacific and Japan)

Security News View

SECURITY NEWS presents articles from the SonicWall Capture Labs Threat Research Team. These articles discuss the most recent vulnerabilities.



You can filter the articles by selecting one of the words at the top of the page, or you can search by topic or date using the search fields.

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 at <https://sonicwall.com/pes>.
- 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

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **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 Center User Guide
Updated - January 2024
232-005773-00 Rev C

Copyright © 2024 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