

Secure Mobile Access 100 Cloud Management and Reporting

Getting Started Guide

SONICWALL®

Contents

About This Guide	1
Preparing Accounts and Tenants	2
Configuring the SMA Appliance	6
Monitoring	9
Dashboard	9
Analytics	10
Alerts	10
Threats	11
WAF Threats	12
Activities	13
Appliances	14
Status	14
Appliances	15
Reports	19
Generating a Report	19
Scheduling a Report	19
E-mailing a Report	20
Downloading a Report	21
Jobs	21
Other Monitoring Resources	22
Logging Out	23
SonicWall Support	24
About This Document	25

About This Guide

This document describes how to get started with the a cloud instance of SonicWall® Secure Mobile Access (SMA) 100. The features supported by this release include single sign-on from the Capture Security Center, a Dashboard for monitoring status and views for Alerts, Threats, WAF Threats, and Access. You can also monitor our device registration and active devices.

① **IMPORTANT:** SMA Cloud Management and Reporting 2.0 is supported for SMA 100 series beginning with version 10.2.1 or later.

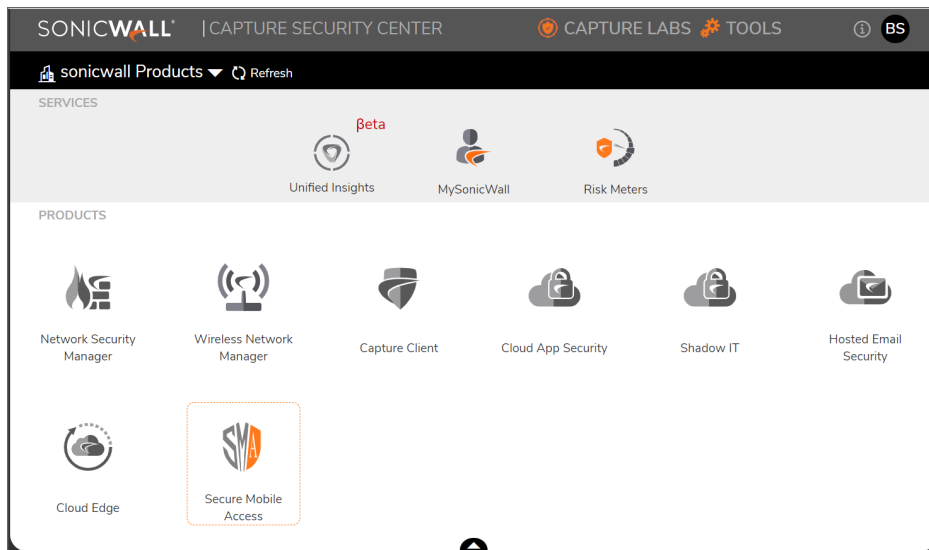
Topics:

- [Preparing Accounts and Tenants](#)
- [Configuring the SMA Appliance](#)
- [Monitoring](#)
- [Logging Out](#)

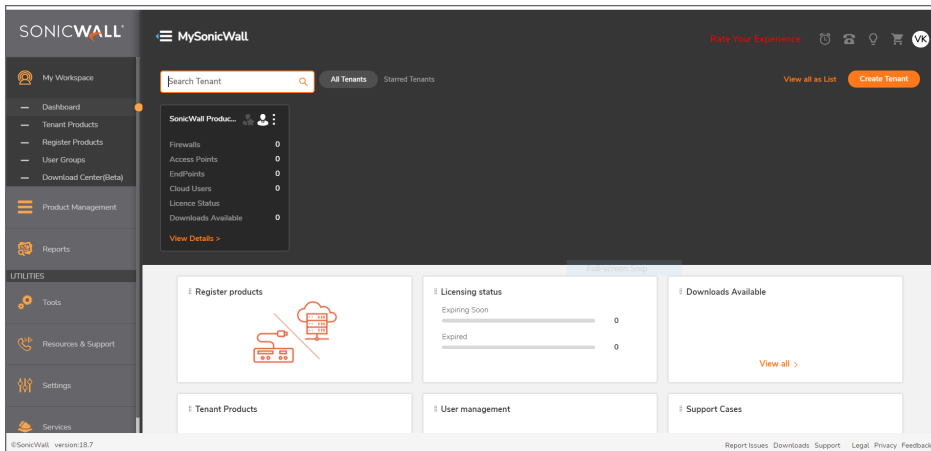
Preparing Accounts and Tenants

Before setting up SMA, you need to access MySonicWall to register your appliance, activate your license, and creating tenants.

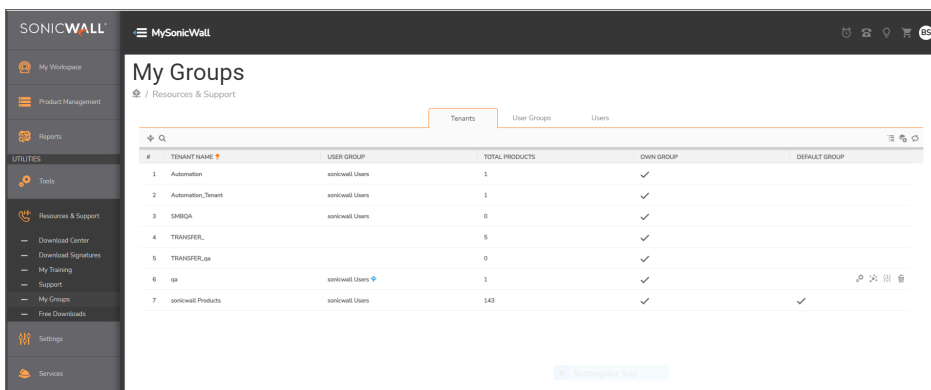
1. Navigate to [Capture Security Center](#).
2. Log in with your MySonicWall credentials.



3. Click on the **MySonicWall** tile.
MySonicWall page is displayed.



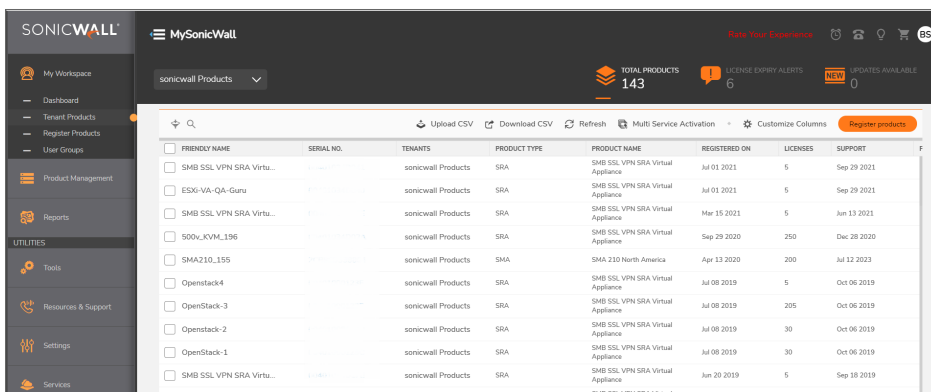
4. Navigate to **Resources & Support > My Groups**.



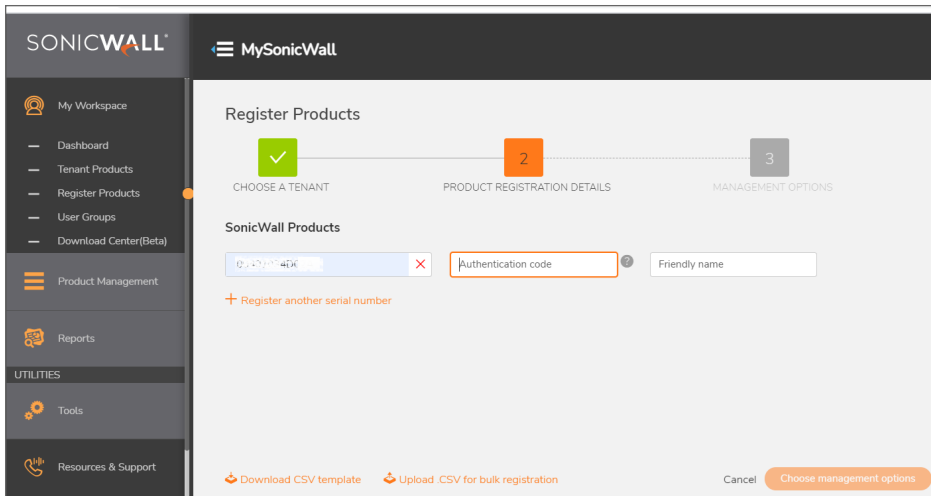
5. Create the Tenants needed for your environment.

For more information on how to create Tenants, click  (Help) icon.

6. Navigate to **My Workspace > Tenant Products**.



7. Click on **Register Products** to register new SMA products under a specific tenant.



8. Provide the information requested by the registration wizard:

- Tenant name
- Serial number
- Authentication code for the SMA product
- Friendly name for the SMA product

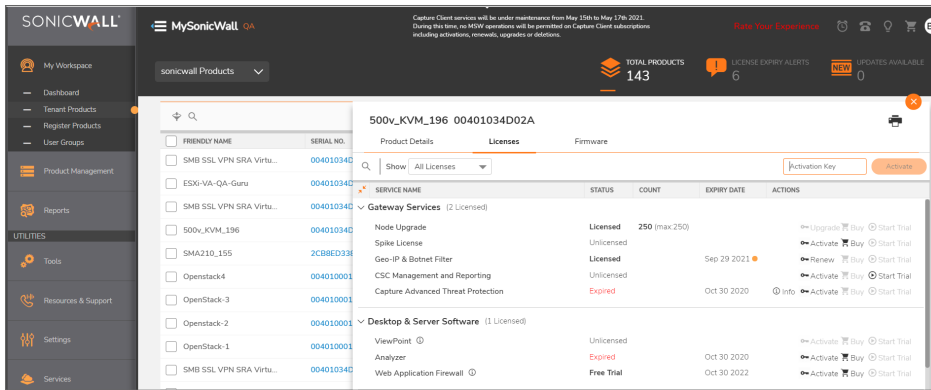
9. Verify that the appliance is registered under the selected tenant.

FRIENDLY NAME	SERIAL NO.	TENANTS	PRODUCT TYPE	PRODUCT NAME	REGISTERED	ACTIONS
<input type="checkbox"/> SMA500v_Hyperv_112	00401034D319	tenant-2	SMA	SMB SSL VPN SRA Virtual Appliance	Aug 22 2019	• • •
<input type="checkbox"/> SMA500v_Azure	00401034D312	tenant-1	SMA	SMB SSL VPN SRA Virtual Appliance	Aug 07 2019	• • •
<input type="checkbox"/> SMA_GMS_119	00401035A586	Sonicwall Products	GMS SOFTWARE	GMS Software License	Apr 10 2019	• • •
<input type="checkbox"/> SMA_ANALYZER	0040103650F2	Sonicwall Products	ANALYZER SOFTWARE	SonicWall Analyzer Software	Apr 09 2019	• • •
<input type="checkbox"/> SMA500_Hyperv_111	00401034D202	tenant-1	SMA	SMB SSL VPN SRA Virtual Appliance	Mar 12 2019	• • •
<input type="checkbox"/> SMA410_158	2CB8ED3388A4	tenant-1	SMA	SMA 410 North America	Feb 28 2019	• • •
<input type="checkbox"/> SMA 210 North America	2CB8ED338804	Sonicwall Products	SMA	SMA 210 North America	Feb 28 2019	• • •
<input type="checkbox"/> SMA210_154	2CB8ED338808	tenant-1	SMA	SMA 210 North America	Feb 28 2019	• • •
<input type="checkbox"/> SMA500v_AWS_188	00401034D1FE	tenant-2	SMA	SMB SSL VPN SRA Virtual Appliance	Feb 22 2019	• • •
<input type="checkbox"/> SMA400_190	18B169093148	tenant-1	SMA	SMA 400 North America	Sep 28 2018	• • •

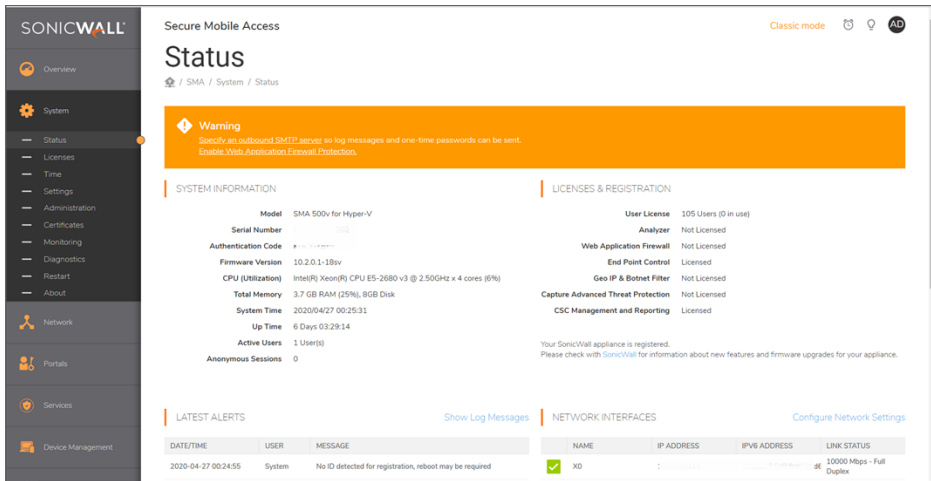
10. Click on the **Activate service** key for the serial number you want to enable.

11. Under **Gateway Services**, find **CSC Management and Reporting** and click on **Activate** and provide activation key.

① **NOTE:** A free trial for SMA Cloud Dashboard and Reporting is available, and you can click on **Start Trial** to activate it. A one-year subscription license is also available.



12. Log into the appliance you updated.
13. Navigate to **System > Status**.
14. Verify that **CSC Management and Reporting** shows as Licensed.




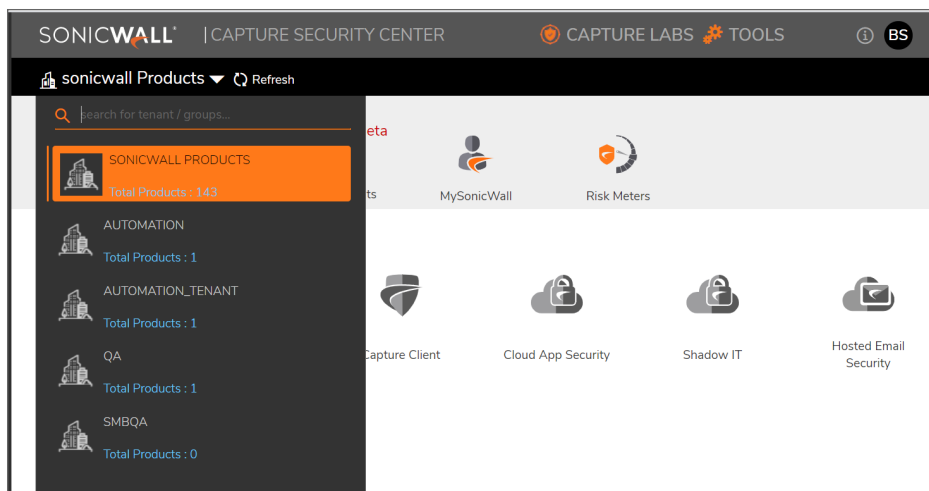
The SMA tile on Capture Security Center also reflects the activated state (not grayed out).

Configuring the SMA Appliance

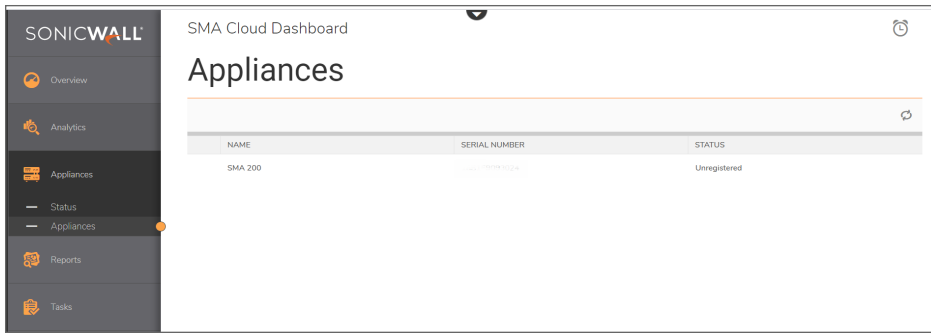
The next step is to configure the SMA appliance for operation after all the MySonicWall configuration is complete.

To configure the SMA appliance:

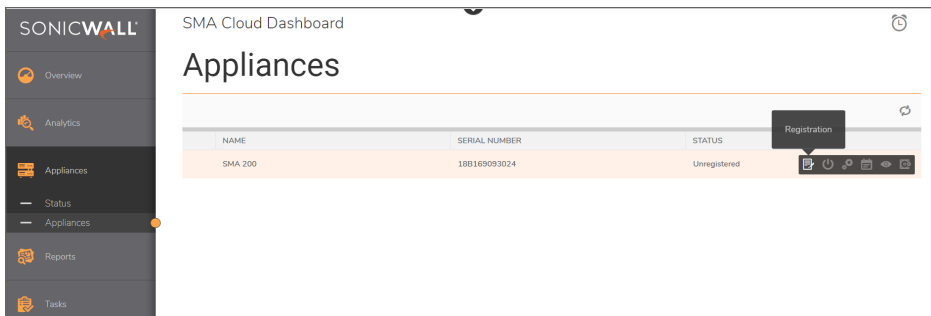
1. Click the down arrow  at the top of the MySonicWall page to return to the Capture Security Center portal.
2. Select the tenant and click on the **Secure Mobile Access** tile.



3. In the left pane, select **Appliances > Appliances**.
All the appliances with its serial number and registration status are displayed.

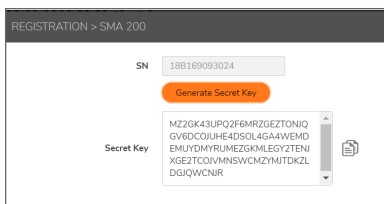


4. Hover over the appliance from the list that you want to update and click **Registration** icon.

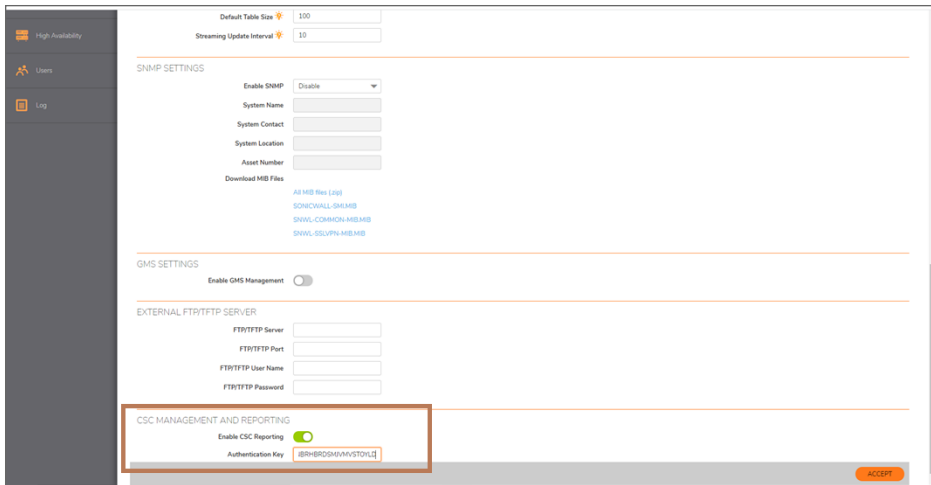


The **Registration** pop-up screen is displayed.

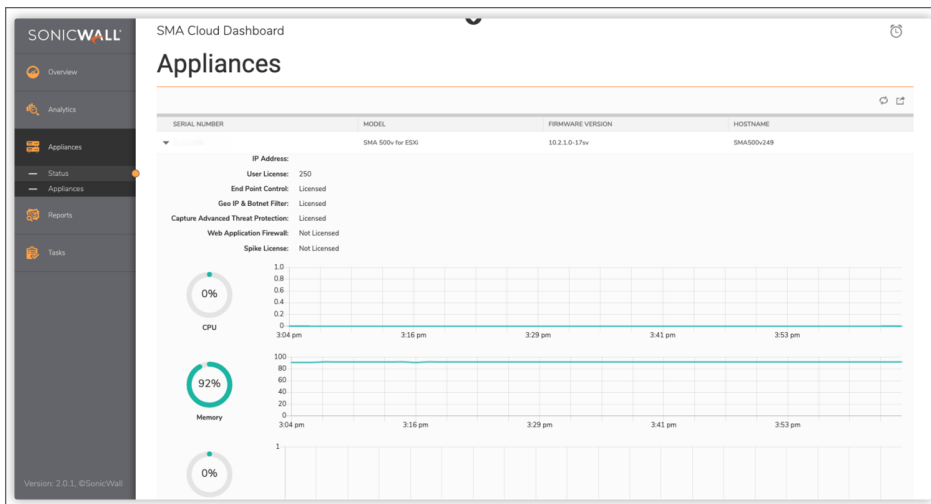
5. Click on **Generate Secret Key**.
6. Copy the **Secret Key** and keep it somewhere to paste into the SMA 100 appliance later.



7. Log into the SMA 100 appliance.
8. Navigate to **System > Administration**.
9. Scroll down to **CSC MANAGEMENT AND REPORTING** group.



10. Enable the **Enable CSC Reporting** option.
11. Paste the authentication key into the **Authentication Key** field.
12. Click **Accept**.
13. Return to the **Appliance > Registration** page on the SMA Cloud.
14. Verify that the registration status for the appliance you updated changed from **Registered** to **Online**.
Once the SMA 100 appliance is online, it is ready to send logging information to the SMA Cloud dashboard. The image below is an example of what you can see about the appliance when you navigate to **Appliance > Status**.



You can expand the appliance entry by clicking on the arrowhead by the appliance. You can see details about the appliance like IP address, firmware version and user licenses. You can also see whether the enhanced features have been licensed or not. In addition, system metrics such as CPU, memory, and users are tracked. This data is plotted on a graph so you can see the performance over time.

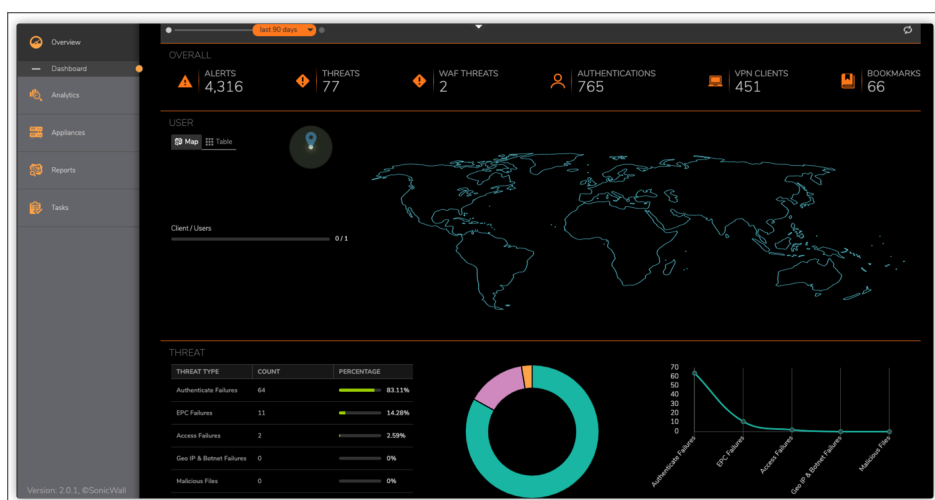
Monitoring

SMA Cloud provides several ways to monitor the performance of your devices. These include:

- [Dashboard](#)
- [Analytics](#)
- [Appliances](#)
- [Reports](#)
- [Jobs](#)
- [Other Monitoring Resources](#)

Dashboard

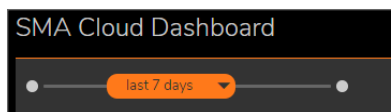
You can use the Dashboard (**Overview > Dashboard**) to monitor basic appliance operation. Across the top of the Dashboard you can see the number of Alerts, Threats, WAF Threats, Authentications, VPN Clients and Bookmarks.



It also shows a graphical representation of where your users are distributed on the map and provides a summary of the threat information at the bottom.

On the Dashboard, you can toggle between the map view and a user table. Just click your preference under the **User** heading.

By default, the SMA Cloud Dashboard displays the appliance data for the last 7 days. You can set the period for the charts by using the sliding bar at the top.



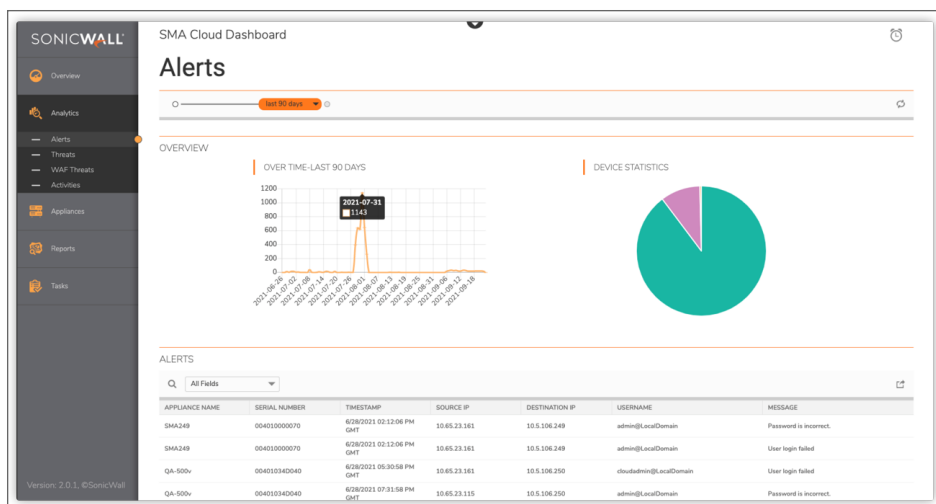
Analytics

The Analytics commands offer several way to drill down on specific activities.

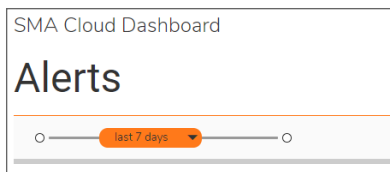
- Alerts
- Threats
- WAF Threats
- Activities

Alerts

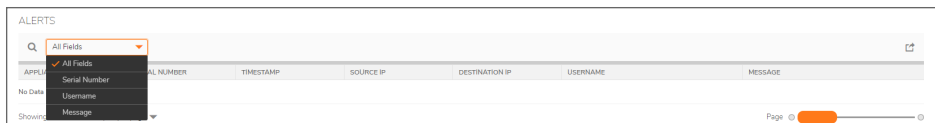
You can use the Dashboard (**Analysis > Alerts**) to monitor the respective alerts for all the SMA appliances.



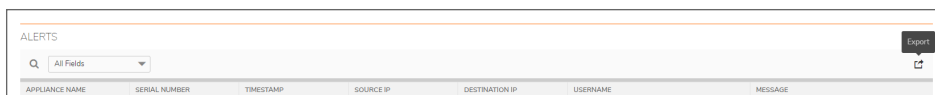
By default, the SMA Cloud Dashboard displays the alerts for the last 7 days. You can set the period for the charts by using the sliding bar at the top.



You can filter the alerts based on the appliance serial number, user name, or message.

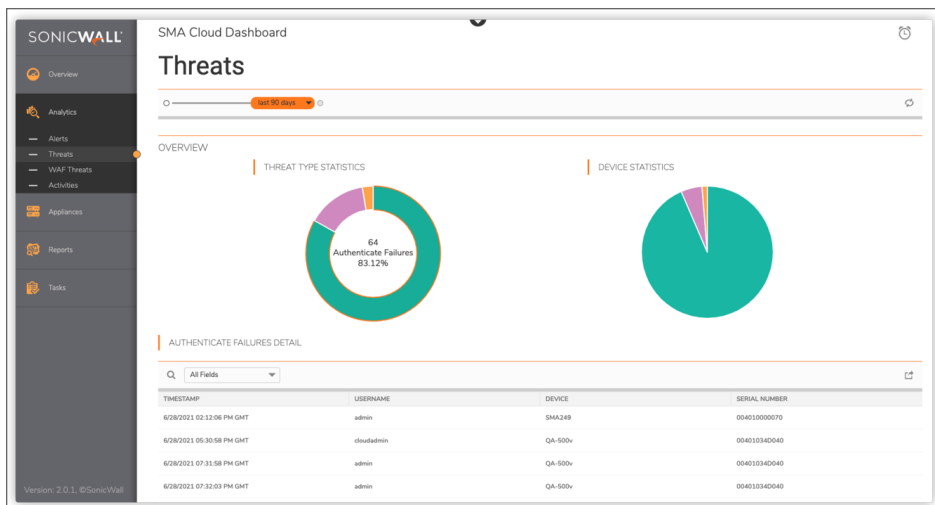


Click the **Export** icon to export the alerts to csv format.

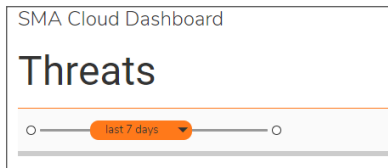


Threats

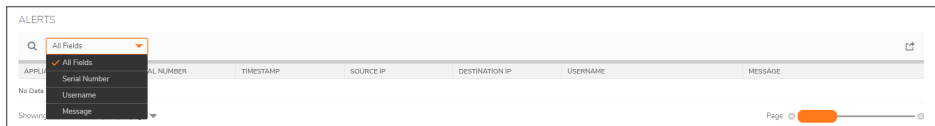
Navigate to **Analytics > Threat** to see an overview of the various threats. Select one of the items in the Overview chart to see the detail in the lower half of the table.



By default, the SMA Cloud Dashboard displays threats detected for the last 7 days. You can set the period for the charts by using the sliding bar at the top.



You can filter the threats based on the appliance serial number, user name, or device.

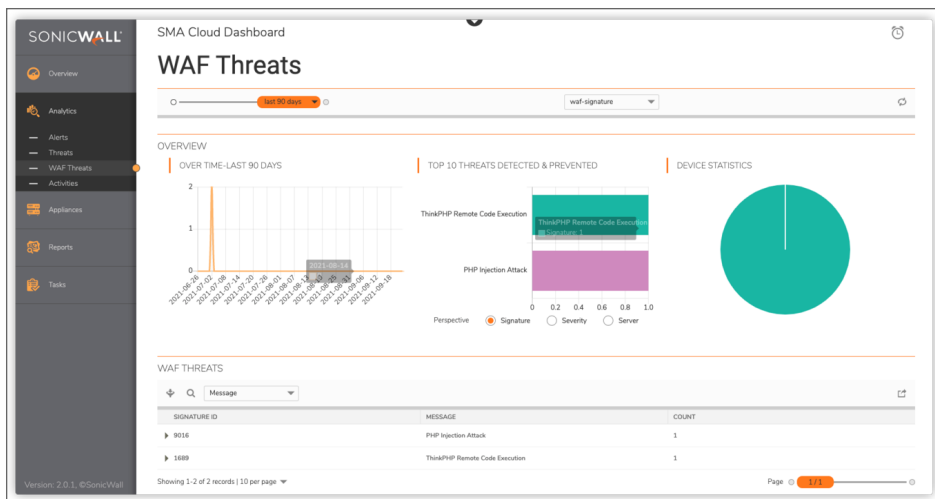


Click the **Export** icon to export the threat details to csv format.

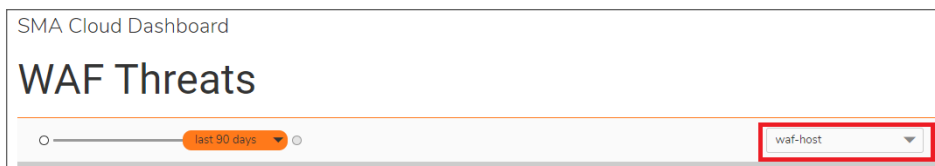


WAF Threats

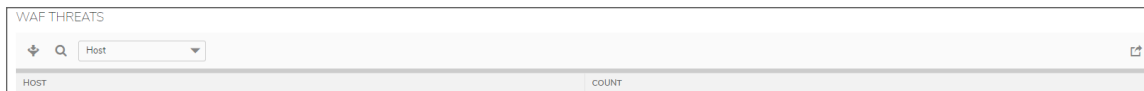
Navigate to **Analytics > WAF Threats** to view the WAF threat logging. . Click the arrowhead to expand the entry and see more detail. Click it again to hide the extra data.



By default, the SMA Cloud Dashboard displays the WAF Threats detected for the last 90 days. You can set the period for the charts by using the sliding bar at the top. Also, you can filter to sort by selecting the field names.

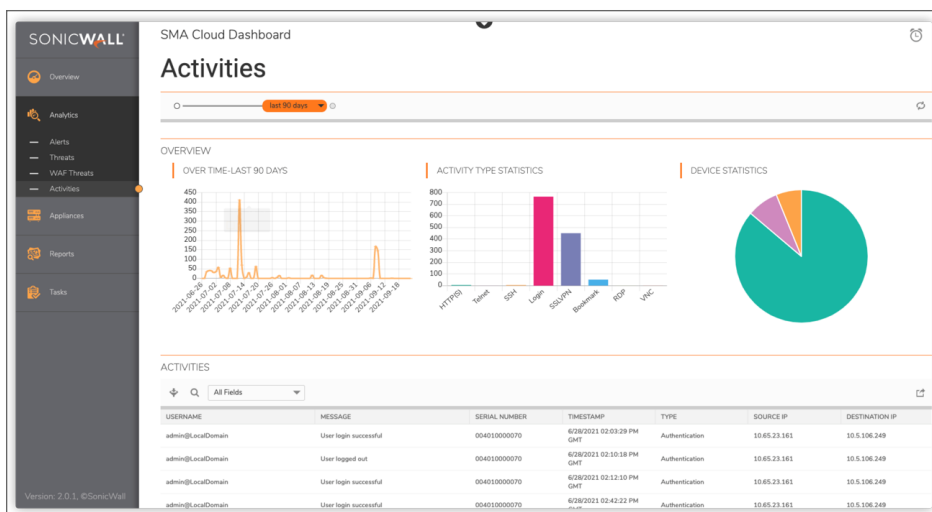


Click the **Export** icon to export the WAF Threat details to csv format.



Activities

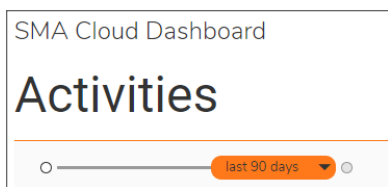
Navigate to **Analytics > Activities** to view the details of user activities.



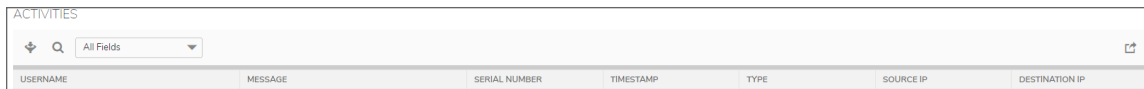
You can see details on the **Activities** page by clicking on option on the Dashboard page as well:

- Click on **VPN Clients** on the Dashboard to view VPN client logging.
- Click on **Bookmarks** on the Dashboard to view bookmarks.

By default, the SMA Cloud Dashboard displays the user activities of last 90 days. You can set the period for the charts by using the sliding bar at the top.



Click the **Export** icon to export the user activity details to csv format.



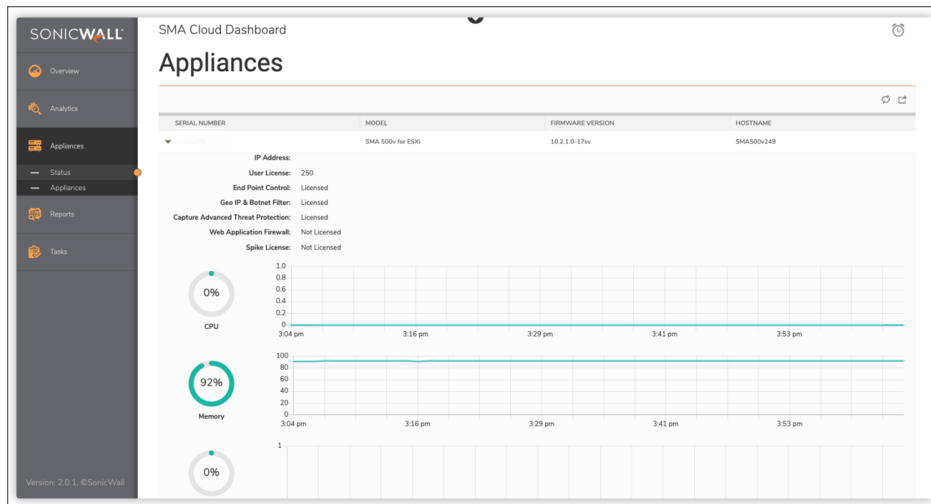
Appliances

The Appliances page lists all the online appliances of the Tenant. Also provides you the basic information and status of all the appliances. You can manage the appliances by hovering on the required appliance from the **Appliances > Appliances** page.

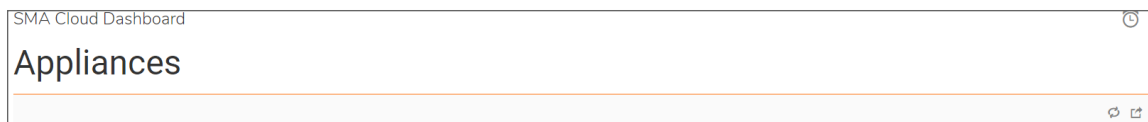
- [Status](#)
- [Appliances](#)

Status

Navigate to **Appliances > Status** to see the basic information and status of all the appliances. It also shows a graphical representation of appliance CPU and Memory.



Click the **Export** icon to export the appliance details to csv format.



Appliances

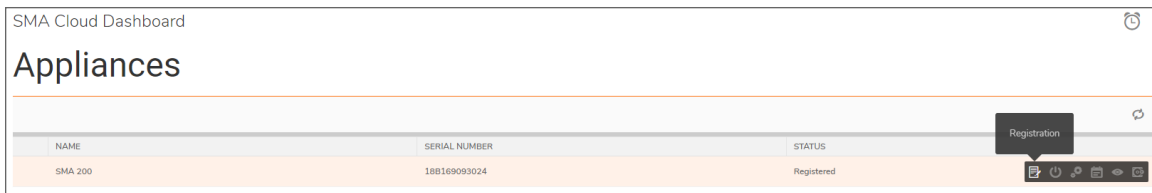
Navigate to **Appliances > Appliances** to view all the appliances and its registration status. You can also manage the appliances by hovering on the required appliance.

- [Registering an Appliance](#)
- [Rebooting an appliance](#)
- [Managing an Appliance](#)
- [Scheduling a backup](#)
- [View Settings](#)
- [Backup Settings](#)

Registering an Appliance

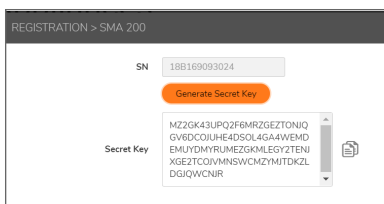
To register an appliance:

1. Navigate to **Appliances > Appliances** page.
The Appliances page lists all the appliances and its registration status.
2. Hover on the Appliance which you want to register and click **Register** icon.

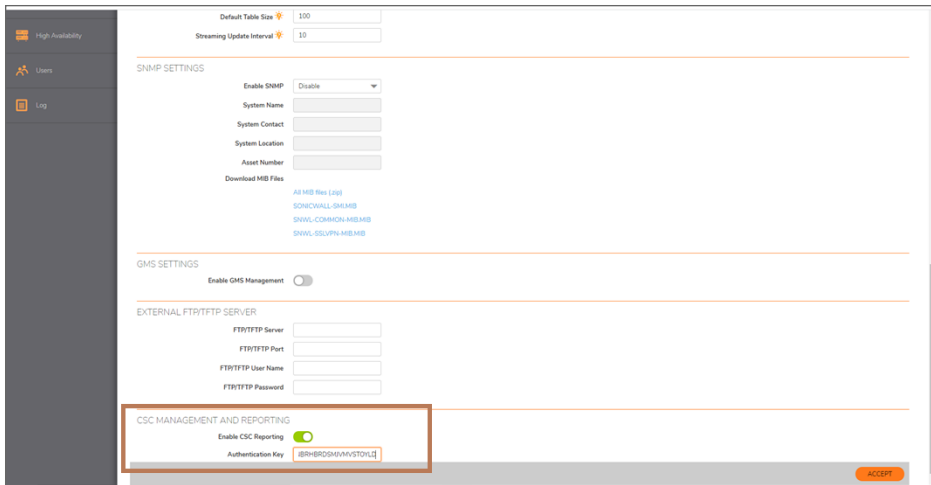


The **Registration** pop-up screen is displayed.

3. Click on **Generate Secret Key**.
4. Copy the **Secret Key** and keep it somewhere to paste into the SMA 100 appliance later.



5. Log into the SMA 100 appliance.
6. Navigate to **System > Administration**.
7. Scroll down to **CSC MANAGEMENT AND REPORTING** group.

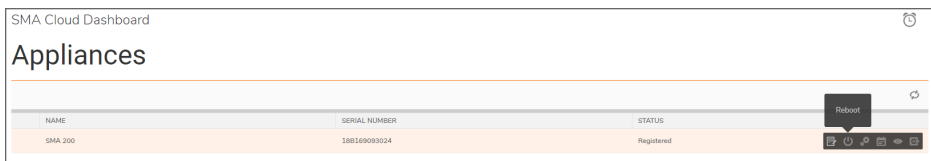


8. Enable the **Enable CSC Reporting** option.
9. Paste the authentication key into the **Authentication Key** field.
10. Click **Accept**.
11. Return to the **Appliance > Registration** page on the SMA Cloud.
12. Verify that the registration status for the appliance you updated changed from **Registered** to **Online**.

Rebooting an appliance

To reboot an appliance:

1. Navigate to **Appliances > Appliances** page.
The Appliances page lists all the appliances and its registration status.
2. Hover on the Appliance which you want to reboot and click **Reboot** icon.



A confirmation dialog appears, click **OK** to reboot the appliance.

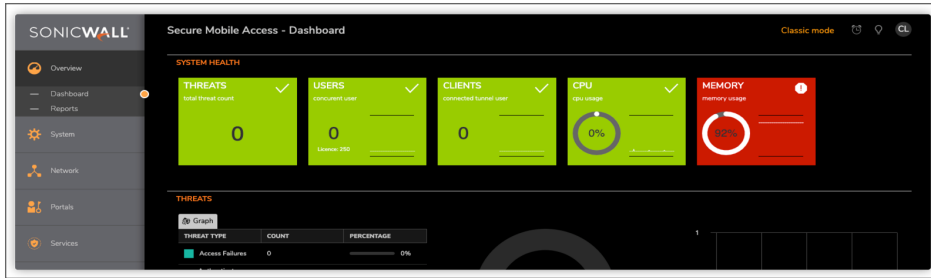
Managing an Appliance

To manage an appliance:

1. Navigate to **Appliances > Appliances** page.
The Appliances page lists all the appliances and its registration status.
2. Hover on the Appliance which you want to manage and click **Manage Appliance** icon.



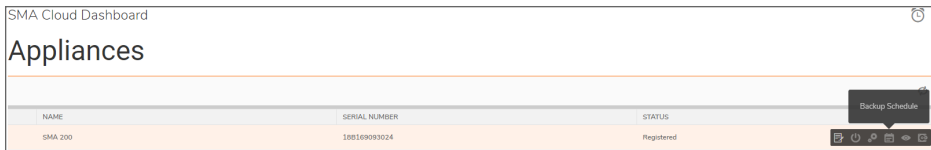
This will navigate you to the SMA appliance where you can manage the appliance configuration.



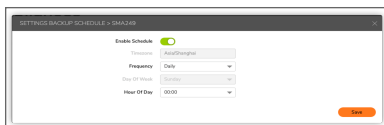
Scheduling a backup

To configure the scheduler to generate backup configuration:

1. Navigate to **Appliances > Appliances** page.
The Appliances page lists all the appliances and its registration status.
2. Hover on the Appliance which you want to manage and click **Backup Schedule** icon.



The **Settings Backup Schedule** dialog is displayed.



Select the frequency and time-line for the appliance backup and click **Save**.

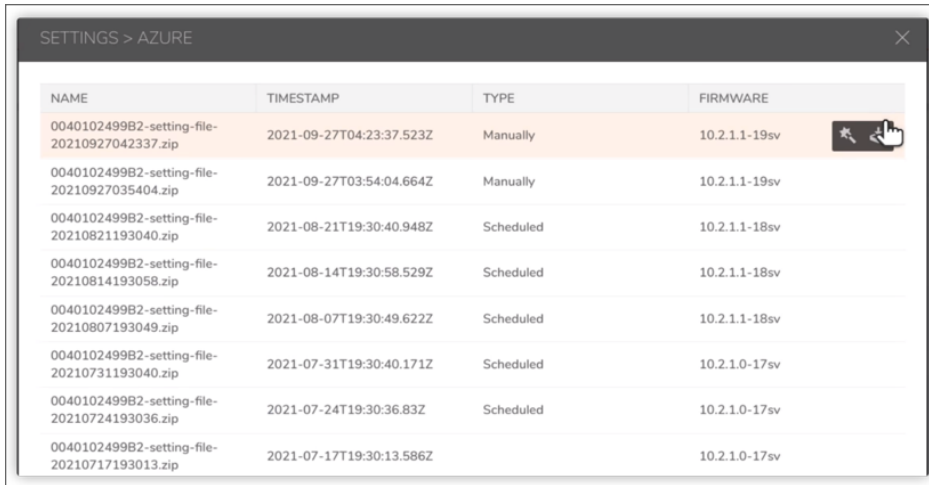
View Settings

To view the available configuration of an appliance:

1. Navigate to **Appliances > Appliances** page.
The Appliances page lists all the appliances and its registration status.
2. Hover on the Appliance which you want to manage and click **View Settings** icon.



The Appliance configuration settings are displayed.

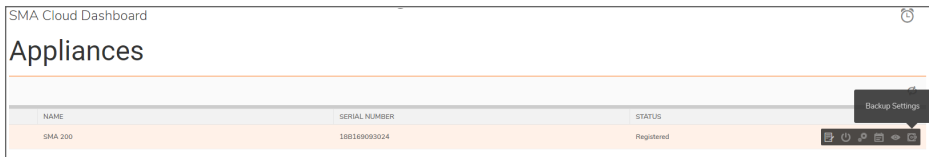


Hover on the settings and click  if you want to deploy back the configuration to SMA appliance.

Backup Settings

To generate configuration and to backup settings:

1. Navigate to **Appliances > Appliances** page.
The Appliances page lists all the appliances and its registration status.
2. Hover on the Appliance which you want to generate configuration and click **Backup Settings** icon.



Reports

You can use the (**Reports > Reports**) to view, generate, schedule, and e-mail the reports for all the SMA appliances.

Generating a Report

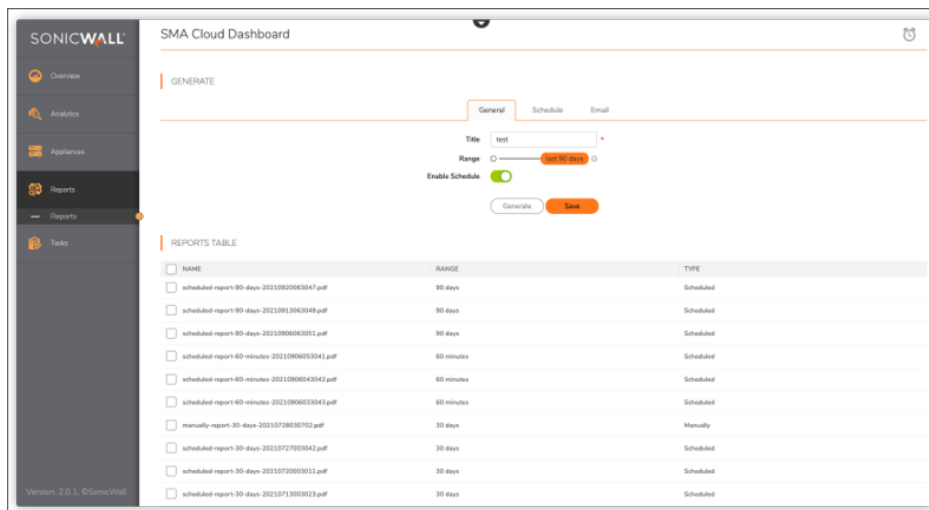
To Generate a report:

1. Navigate to **Reports > Reports** page.
2. Click **General** tab.
3. In the **Title** field, enter the title of the report.
4. Select the Range from the **Range** Sliding bar.
5. Click **Enable Schedule** and select **Generate** to generate the report.

Or

Click **Save** to generate the report later.

The Report is generated and displayed in the **Reports Table**.



Scheduling a Report

To schedule a report:

1. Navigate to **Reports > Reports** page.
2. Click **Schedule** tab.

① | **NOTE:** The **Timezone** field is set based on your location.

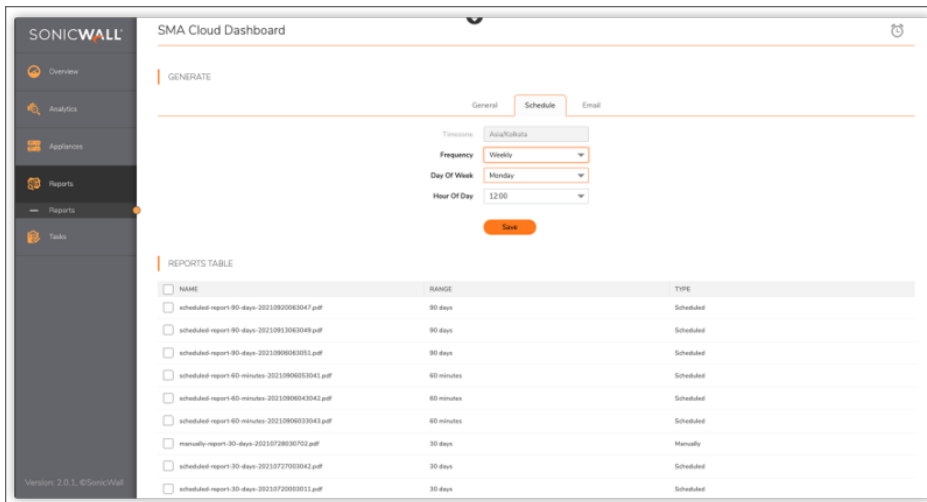
3. In the **Frequency** field, select **Daily** if you wish to generate the report everyday.

OR

Select **Weekly** if you wish to generate the report every week and select the day on which you want to generate the report.

4. In the **Hour of Day** field, select the time to generate the report.

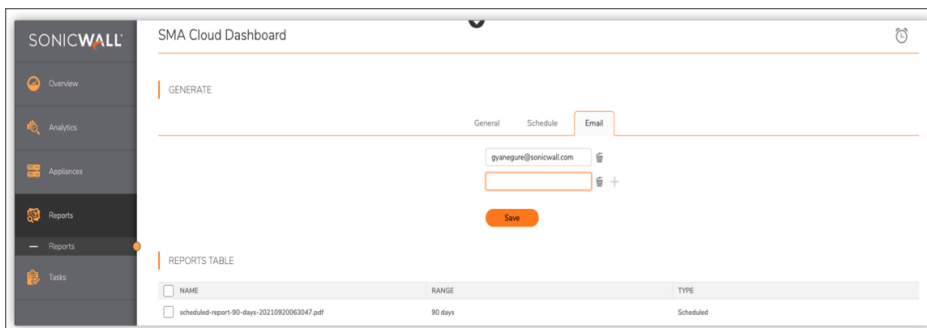
5. Click **Save**.



E-mailing a Report

To e-mail a report automatically:

1. Navigate to **Reports > Reports** page.
2. Click **Email** tab.
3. Enter the e-mail address for which you want to share the report.
You can add multiple e-mail address by clicking on **+** icon.
4. Click **Save**.



Downloading a Report

To download a report:

1. Navigate to **Reports > Reports** page.
2. Under the **Reports Table**, hover on the report which you want to download and click **Download** icon.



REPORTS TABLE

<input type="checkbox"/> NAME	RANGE	TYPE	Download Report
<input type="checkbox"/> manually-report-60-minutes-20210928060133.pdf	60 minutes	Manually	

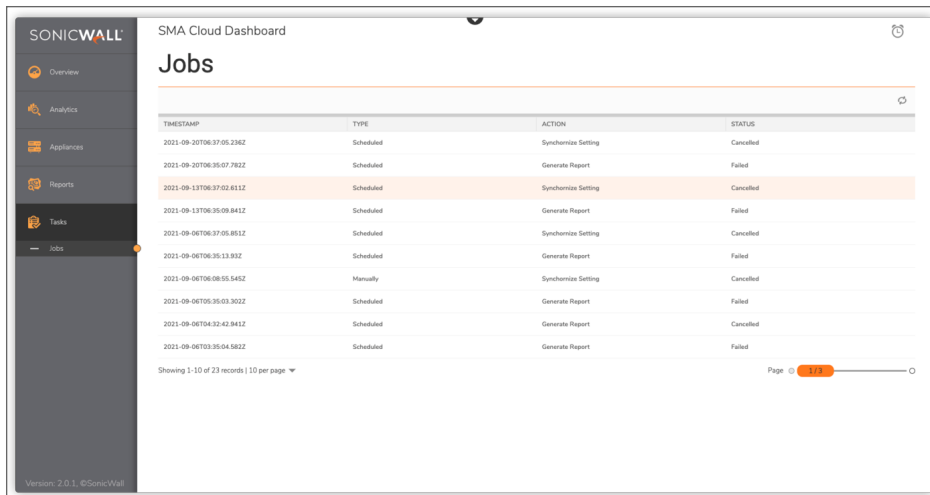
Download Selected Reports

To download multiple reports, select the check box of the reports which you want to download and click **Download Selected Reports** button.

The reports are downloaded in PDF format.

Jobs

Navigate to **Tasks > Jobs** to view the job status in the system.



SMA Cloud Dashboard

Jobs

TIMESTAMP	TYPE	ACTION	STATUS
2021-09-20T06:37:05.236Z	Scheduled	Synchronize Setting	Cancelled
2021-09-20T06:35:07.782Z	Scheduled	Generate Report	Failed
2021-09-13T06:37:02.611Z	Scheduled	Synchronize Setting	Cancelled
2021-09-13T06:35:09.841Z	Scheduled	Generate Report	Failed
2021-09-06T06:37:05.851Z	Scheduled	Synchronize Setting	Cancelled
2021-09-06T06:35:13.93Z	Scheduled	Generate Report	Failed
2021-09-06T06:08:55.145Z	Manually	Synchronize Setting	Cancelled
2021-09-06T05:35:03.302Z	Scheduled	Generate Report	Failed
2021-09-06T04:32:42.941Z	Scheduled	Generate Report	Cancelled
2021-09-06T03:35:04.582Z	Scheduled	Generate Report	Failed

Showing 1-10 of 23 records | 10 per page

Page 0 / 3 / 3

Other Monitoring Resources

Aside from the reporting and monitoring tools provided in SMA 100, you can use the dashboards on MySonicWall and Capture Security Center.

To access MySonicWall's Dashboard, click on the **MySonicWall** tile. When it first opens, MySonicWall defaults to the **Dashboard on My Workspace**. From here you can find a quick status of your various tenants and see summaries about products, licensing status and downloads. Select **View Details** on a tenant tile to see product details for that tenant. Click the **Help** icon in upper right corner to learn more about what MySonicWall has to offer.

By selecting **Risk Meters** on the Capture Security Center, you can see data that can help you assess the risk to your network security. Based on licensing and product information provided by MySonicWall, you can see what is working well and what areas may need attention. Click on **DEFCON** or **SHIELD LEVEL** to see the Risk Meters details. Click on the **Help** icon on the main Capture Security Center page to learn more about information on the Risk Meter.

Logging Out

To log out of Cloud SMA and CSC:

1. Click the down arrow at the top of the Cloud SMA page to return to the Capture Security Center portal.
2. On the CSC page, click on the user initials in the top, right-hand corner and select **Logout**.

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

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.

Secure Mobile Access 100 Cloud Management and Reporting Getting Started Guide
Updated - May 2022
232-005399-01 Rev A

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