SonicWall® SMA 100 Cloud Management and Reporting 1.0

Release Notes

November 2020

These release notes provide information about the SonicWall® SMA 100 Cloud Management and Reporting 1.0 release.

Topics:

About SMA 100 Cloud Management and Reporting 1.0

SMA 100 Cloud Management and Reporting 1.0 is the initial release of Cloud Management and Reporting for SMA 100 Series appliances running SMA 10.2.0.1 or higher. SMA 100 Cloud Management and Reporting provides integration with SonicWall Capture Security Center (CSC). SMA 100 Series appliances have been compatible with CSC starting from SonicWall SMA 10.2.0.1.

SMA 100 Cloud Management and Reporting provides a cloud dashboard that displays the overall status of all the registered SMA 100 Series appliances. The dashboard has sliders to choose the Time Period and displays the counts of Alerts, Threats, WAF Threats, Authentications, VPN Clients, Bookmark accesses, a map showing the active SMA devices and users, and a list of threats types with counts and percentages.

Using SMA 100 Cloud Management and Reporting is easy:

- Use your MySonicWall credentials to log into Capture Security Center at https://cloud.sonicwall.com.
- Click the **Secure Mobile Access** tile to view the SMA Cloud Dashboard, complete registration, and enable cloud management.

For more information about licensing and integrating with SMA 100 Cloud Management and Reporting, refer to the *SMA 100 Cloud Management and Reporting Getting Started Guide*, available on the SonicWall Technical Documentation portal here.

Supported Platforms

SMA 100 Cloud Management and Reporting 1.0 is supported on the following SonicWall SMA appliances running SMA 10.2.0.1 or newer firmware:

- SMA 200/400
- SMA 210/410
- SMA 500v for ESXi

  SonicWall SMA 500v for ESXi is supported for deployment on VMware ESXi 5.0 and higher.
- SMA 500v for Hyper-V

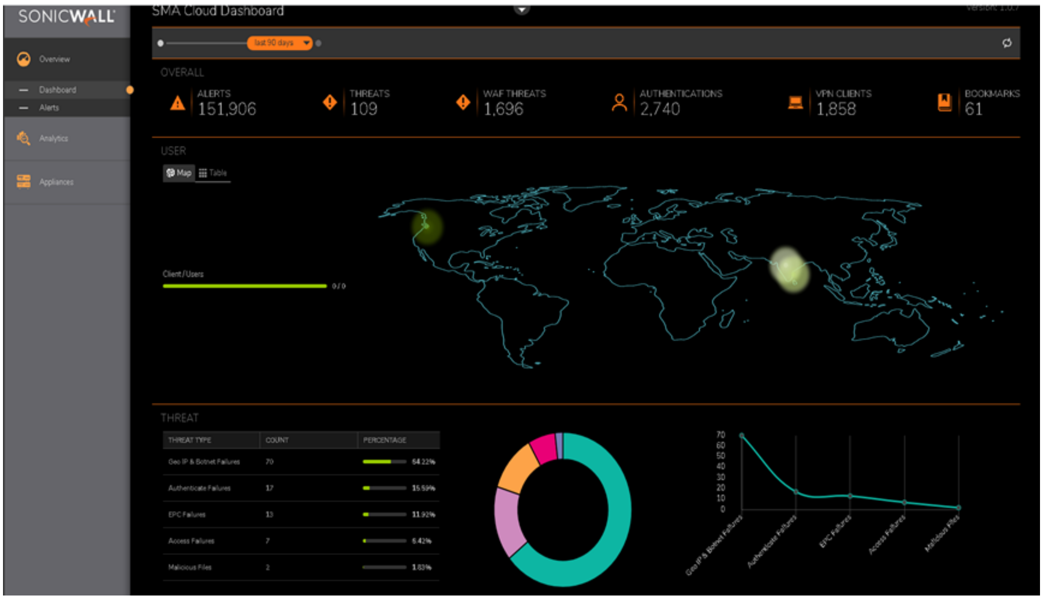
  SonicWall SMA 500v for Hyper-V is supported for deployment on Hyper-V Server 2016 and 2019.
- SMA 500v for AWS
- SMA 500v for Azure

Key Features

SMA 100 Cloud Management and Reporting 1.0 introduces the key features described in this section.

- **Dashboard**

  The **Overview > Dashboard** page displays the overall status of all registered SMA devices with a geographic and tabulated view of global SMA 100 Series appliance deployments.



OVERALL

ALERTS 151,906
THREATS 109
WAF THREATS 1,696
AUTHENTICATIONS 2,740
VPN CLIENTS 1,858
BOOKMARKS 61

THREAT

THREAT TYPE	COUNT	PERCENTAGE
Geo IP & Botnet Failures	70	64.22%
Authenticate Failures	17	15.59%
EPC Failures	13	11.92%
Access Failures	7	6.42%
Malicious Files	2	1.83%

  You can adjust the time period by using the Slider at the top of the page.

  In the **OVERALL** section below the time period slider, the counts of Alerts, Threats, WAF Threats, Authentications, VPN Client accesses, and Bookmark accesses are displayed.

  Active devices and users are displayed on the map in the **USER** section.

  Threats categories and counts are displayed in the **THREAT** section.

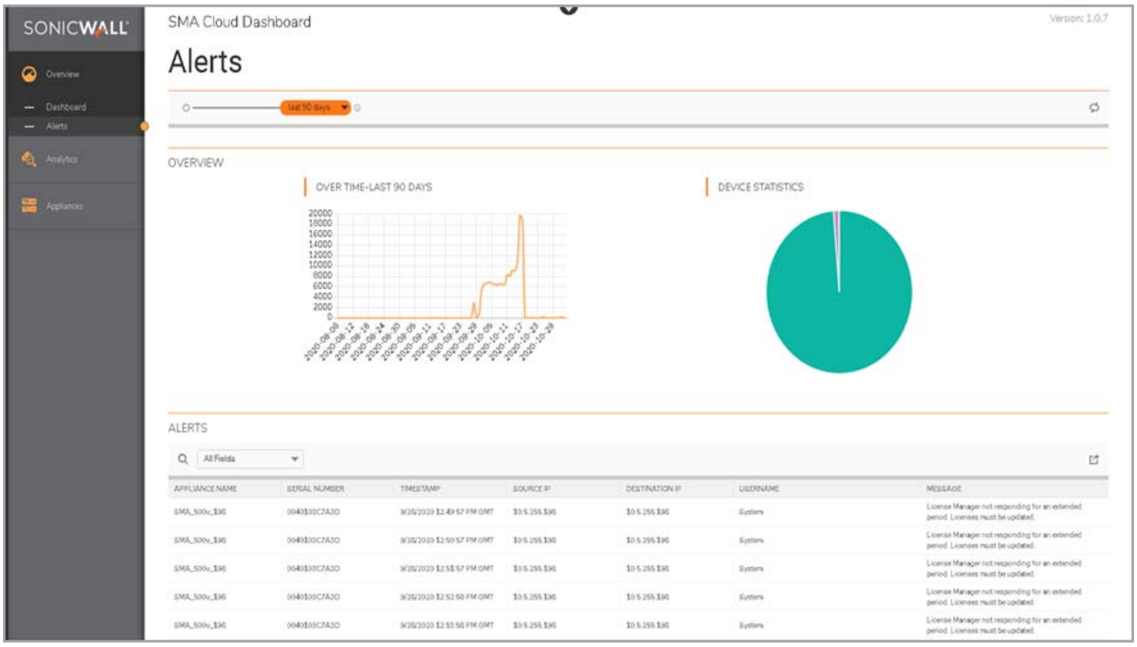
  You can perform the following actions on this page:

  - Click on the counts number to navigate to the detailed page for each category.

- Click a user on the map to show the detailed information for the active user.
- Click the device on the map to show the detailed device information page.
- Click the donut diagram to show the threats detail.

- **Alerts View**

  The **Overview > Alerts** page displays all alerts that occurred on all the registered SMA devices.

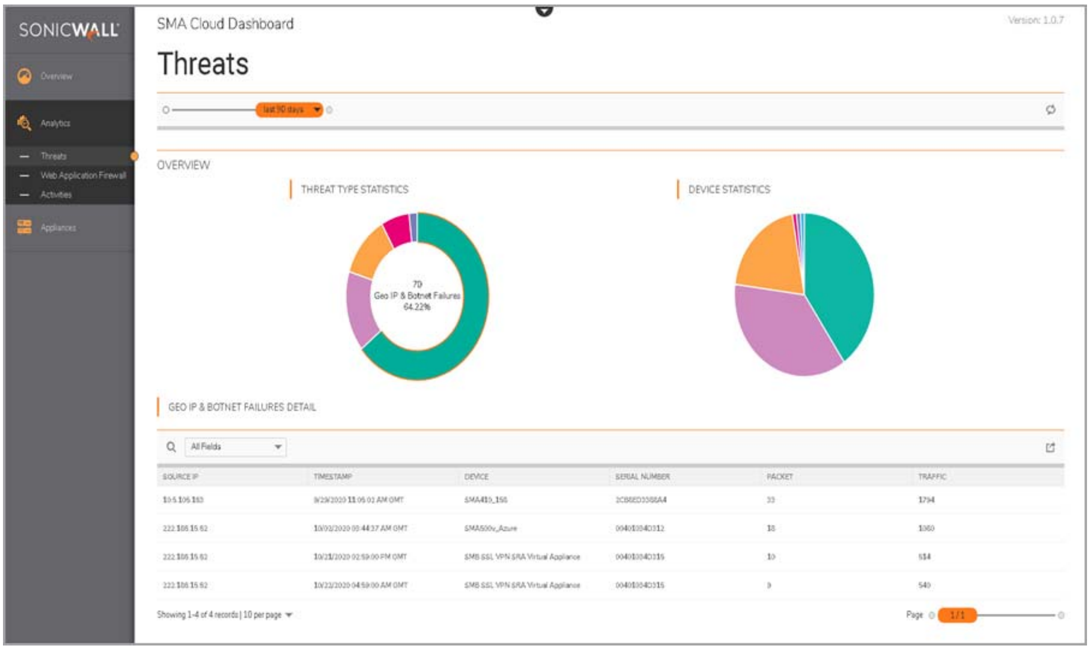


APPLIANCE NAME	SERIAL NUMBER	TIMESTAMP	SOURCE IP	DESTINATION IP	USERNAME	MESSAGE
SMA_500v_136	0040100C7A3D	9/28/2020 12:49:57 PM GMT	10.5.255.136	10.5.255.136	System	License Manager not responding for an extended period. Licenses must be updated.
SMA_500v_136	0040100C7A3D	9/28/2020 12:50:57 PM GMT	10.5.255.136	10.5.255.136	System	License Manager not responding for an extended period. Licenses must be updated.
SMA_500v_136	0040100C7A3D	9/28/2020 12:51:57 PM GMT	10.5.255.136	10.5.255.136	System	License Manager not responding for an extended period. Licenses must be updated.
SMA_500v_136	0040100C7A3D	9/28/2020 12:52:58 PM GMT	10.5.255.136	10.5.255.136	System	License Manager not responding for an extended period. Licenses must be updated.
SMA_500v_136	0040100C7A3D	9/28/2020 12:53:58 PM GMT	10.5.255.136	10.5.255.136	System	License Manager not responding for an extended period. Licenses must be updated.

  You can adjust the time period by using the Slider at the top of the page. This page also provides a Search function and a Field selection list above the table. You can click the Download button at the top right corner of the table to save the Alerts report in CSV format.

- **Threats View**

  The **Analytics > Threats** page displays all threats that occurred on all the registered SMA devices. Threat analytics for WAF, Capture ATP, EPC, GEO IP and BOTNET filtering are provided.



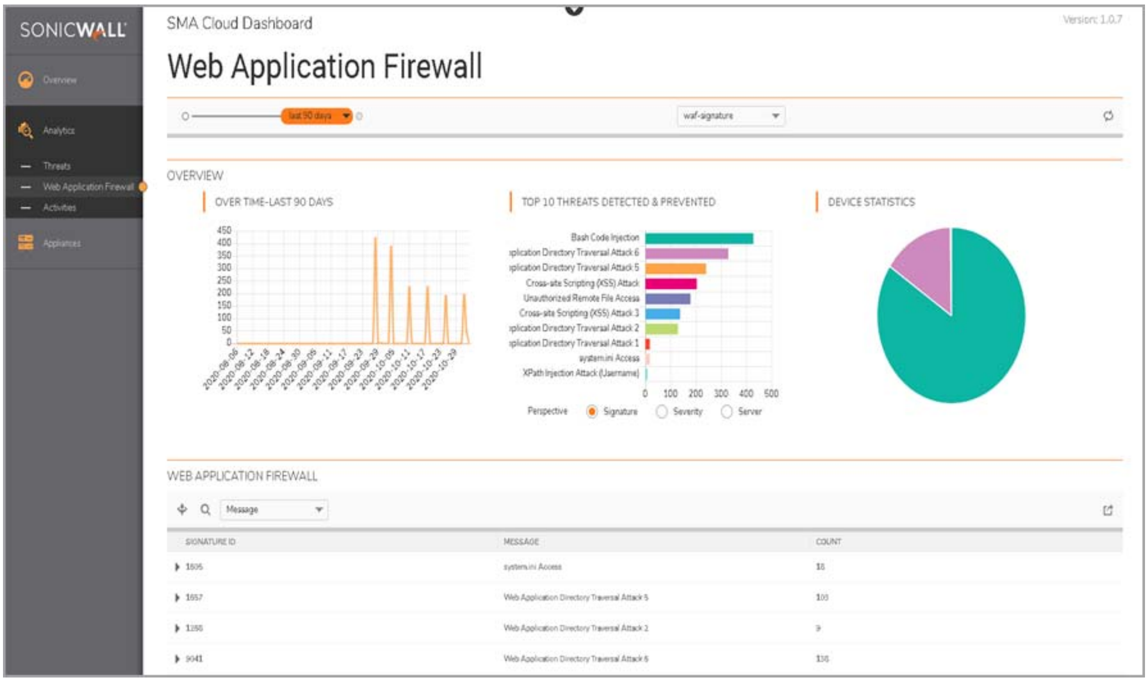
SOURCE IP	TIMESTAMP	DEVICE	SERIAL NUMBER	PACKET	TRAFFIC
10.5.105.183	9/29/2020 11:05:01 AM GMT	SMA410_156	2CB8ED3388A4	33	1794
222.186.15.62	10/02/2020 03:44:37 AM GMT	SMA500v_Azure	0040100400312	18	1060
222.186.15.63	10/21/2020 02:59:00 PM GMT	SMB SSL VPN SRA Virtual Appliance	004010040315	10	514
222.186.15.62	10/22/2020 04:59:00 AM GMT	SMB SSL VPN SRA Virtual Appliance	004010040315	9	540

Showing 1-4 of 4 records | 10 per page

You can adjust the time period by using the Slider at the top of the page. This page also provides a Search function and a Field selection list above the table. You can click the Download button at the top right corner of the table to save the Threats report in CSV format.

- **Web Application Firewall View**

  The **Analytics > Web Application Firewall** page displays all Web Application Firewall threats that occurred on all the registered SMA devices.



SIGNATURE ID	MESSAGE	COUNT
1505	system.ini Access	18
1657	Web Application Directory Traversal Attack 5	103
1156	Web Application Directory Traversal Attack 2	9
9041	Web Application Directory Traversal Attack 6	138

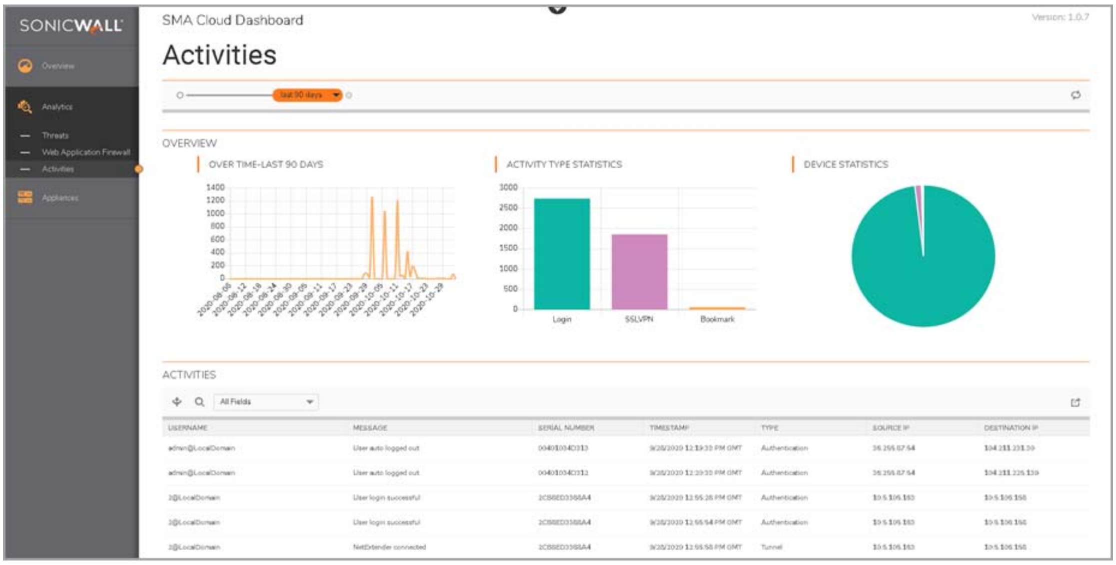
You can adjust the time period by using the Slider at the top of the page. This page also provides a Search function and a Message selection list above the table. You can click the Download button at the top right corner of the table to save the Web Application Firewall report in CSV format.

Under **TOP 10 THREATS**, you can select one of the following as the **Perspective**:

  - **Signature**
  - **Severity**
  - **Server**

- **Activities View**

  The **Analytics > Activities** page displays information about logins and network access events that occurred on all the registered SMA devices.

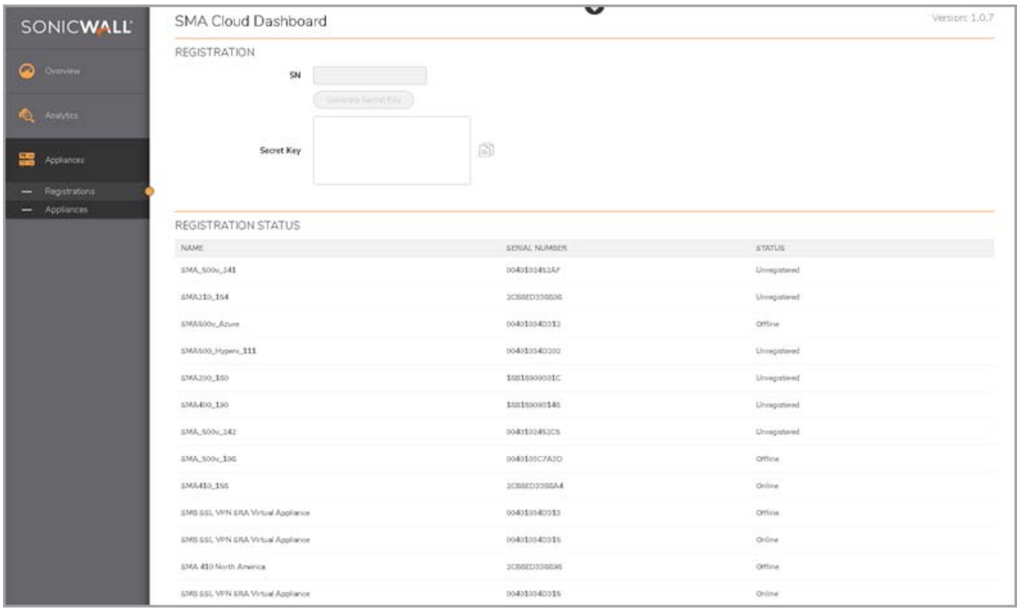


USERNAME	MESSAGE	SERIAL NUMBER	TIMESTAMP	TYPE	SOURCE IP	DESTINATION IP
admin@LocalDomain	User auto logged out	00401034D313	9/28/2020 12:19:33 PM GMT	Authentication	36.255.87.54	104.211.231.30
admin@LocalDomain	User auto logged out	00401034D312	9/28/2020 12:20:33 PM GMT	Authentication	36.255.87.54	104.211.225.139
2@LocalDomain	User login successful	2CB8ED3368A4	9/28/2020 12:55:28 PM GMT	Authentication	10.5.106.163	10.5.106.158
2@LocalDomain	User login successful	2CB8ED3368A4	9/28/2020 12:55:54 PM GMT	Authentication	10.5.106.163	10.5.106.158
2@LocalDomain	NetExtender connected	2CB8ED3368A4	9/28/2020 12:55:58 PM GMT	Tunnel	10.5.106.163	10.5.106.158

  You can view activity logs for tracking logins, SSL VPN sessions, and Bookmark sessions. Adjust the time period by using the Slider at the top of the page. This page also provides a Search function and a Field selection list above the table. You can click the Download button at the top right corner of the table to save the Activities report in CSV format.

- **Registrations View**

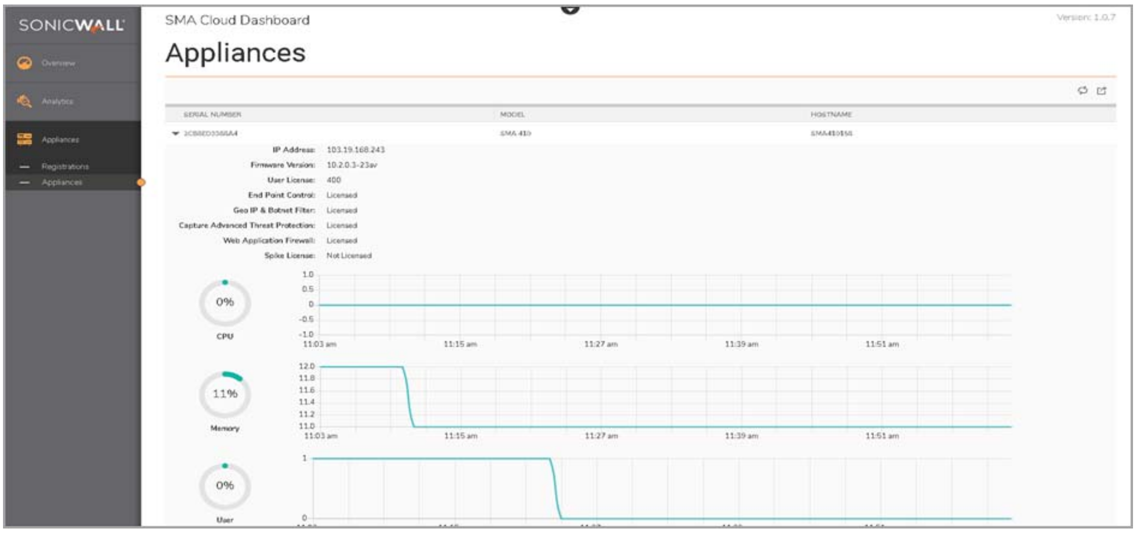
  The **Appliances > Registrations** page provides a way to view the status of all the SMA devices in the selected tenant and to generate registration keys for them.



NAME	SERIAL NUMBER	STATUS
SMA_500v_141	0040102452AF	Unregistered
SMA310_154	2CB8ED336606	Unregistered
SMA500v_Azure	00401034D312	Offline
SMA500_Hyperv_111	00401034D302	Unregistered
SMA200_160	18816909001C	Unregistered
SMA400_190	18815909014B	Unregistered
SMA_500v_142	00401024 52C5	Unregistered
SMA_500v_196	0040100C7A3D	Offline
SMA410_156	2CB8ED3368A4	Online
SMB SSL VPN SRA Virtual Appliance	00401034D313	Offline
SMB SSL VPN SRA Virtual Appliance	00401034D315	Online
SMA 410 North America	2CB8ED336696	Offline
SMB SSL VPN SRA Virtual Appliance	00401034D316	Online

- **Appliances View**

  The **Appliances > Appliances** page displays details about all the registered SMA devices for monitoring SMA appliance vital stats, such as IP address, firmware version, licensing, CPU, memory, users and more.



SERIAL NUMBER	MODEL	HOSTNAME
[illegible]	SMA 410	SMA410158

IP Address: 103.19.168.243
Firmware Version: 10.2.0.3-23sv
User License: 400
End Point Control: Licensed
Geo IP & Botnet Filter: Licensed
Capture Advanced Threat Protection: Licensed
Web Application Firewall: Licensed
Spike License: Not Licensed

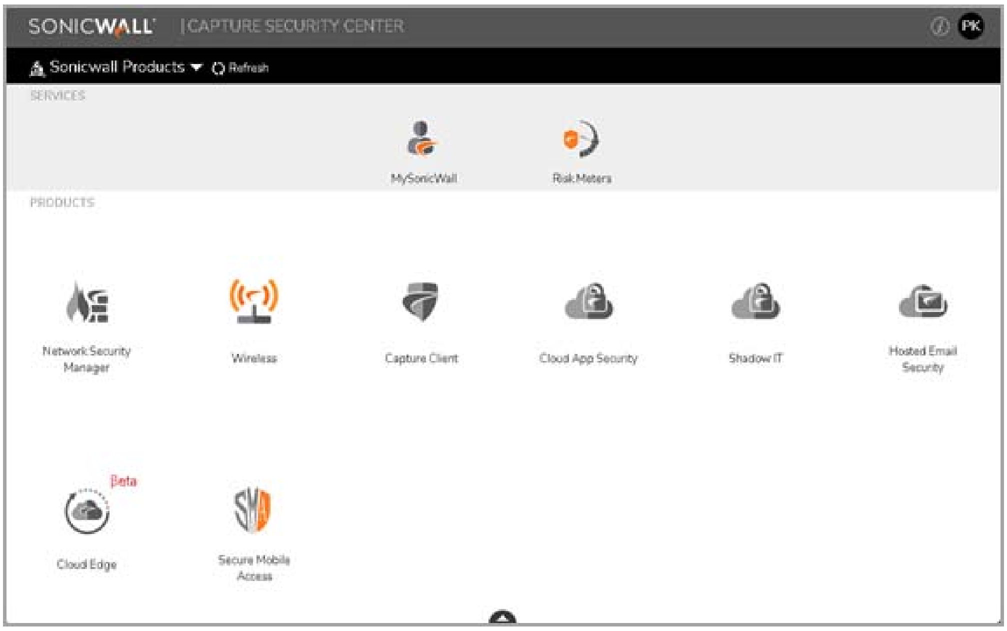
For each SMA device, the following information is displayed:

- Serial number
- Model
- Hostname
- Firmware version
- User license count
- End Point Control license status
- Geo IP & Botnet Filter license status
- Capture ATP license status
- Web Application Firewall license status
- Spike license status
- CPU usage, Memory usage, and User information and graphs

You can click the Download button at the top right corner of the page to save the Appliances report in CSV format.

- **Capture Security Center Integration**

  Once you log into SonicWall Capture Security Center, you can access SMA 100 Cloud Management and Reporting to view your SMA appliances using Single Sign-On, with no need to log in again.



  Click the **Secure Mobile Access** tile to enter SMA 100 Cloud Management and Reporting, or click the **MySonicWall** tile to access MySonicWall. Other tiles provide access to other SonicWall products.

Resolved Issues

The following is a list of resolved issues in the SMA 100 Cloud Management and Reporting 1.0 release.

Resolved Issue	Issue ID
Logs are updating after CSC management and license is expired.	SMA-1278
If re-authentication fails the Cloud Dashboard displays an error, but should allow three retries before resulting in an error.	SMA-1386
The Cloud Dashboard displays offline devices in the map.	SMA-1387
Export buttons do not always work. This is observed with the Activities log.	SMA-1448
No graph is generated for Activities Bookmark/SSLVPN in specific scenarios. If the number of devices is large, then the graph is not generated for a small number of Bookmark/SSLVPN logs. If the number of devices is small, then no logging graphs are generated.	SMA-1723

Product Licensing

SMA 100 Series customers running SMA 10.2.0.1 and higher firmware with an active Support license (8x5 or 24x7) have the **CSC Management and Reporting** link enabled by default in MySonicWall.

Activation of the **CSC Management and Reporting** service uses the following SKU:

02-SSC-6785 SONICWALL BOUNDLESS CYBERSECURITY SMA100 SERIES CLOUD MANAGMENT REPORTING ANALYTICS 1YR

Customers with SMA 100 Series appliance(s) registered on MySonicWall can use Cloud Management and Reporting and the SMA Cloud Dashboard by enabling the trial license:

- LSID7102 - SonicWall CSC Management for SMA 30 Days – 30 days free trial

SMA 100 Cloud Management and Reporting licenses are also available for purchase on MySonicWall.

Refer to the *SMA 100 Cloud Management and Reporting Getting Started Guide* for information about licensing SonicWall SMA 100 Cloud Management and Reporting.

The SonicWall SMA firmware provides user-based licensing on SMA 100 Series appliances. Licensing is controlled by the SonicWall license manager service, and you can add licenses through your MySonicWall account. Unregistered units support the default license allotment for their model, but the unit must be registered in order to activate additional licensing from MySonicWall.

License status is displayed in the SMA management interface, on the Licenses & Registration section of the **System > Status** page. The TSR, generated on the **System > Diagnostics** page, displays both the total licenses and active user licenses currently available on the appliance.

If a user attempts to log into the Virtual Office portal and no user licenses are available, the login page displays the error, “No more User Licenses available. Please contact your administrator.” The same error is displayed if a user launches the NetExtender client when all user licenses are in use. These login attempts are logged with a similar message in the log entries, displayed in the **Log > View** page.

To activate licensing for your SMA appliance:

1. Log into your SMA as **admin**, and navigate to the **System > Licenses** page.
2. Click the **Activate, Upgrade or Renew services** link. The MySonicWall login page is displayed.
3. Type your MySonicWall account credentials into the fields to log into MySonicWall. This must be the account to which the appliance is, or will be, registered. If the serial number is already registered through the MySonicWall web interface, you will still need to log in to update the license information on the appliance itself.

   MySonicWall automatically retrieves the serial number and authentication code.
4. Type a descriptive name for the appliance into the **Friendly Name** field, and then click **Submit**.
5. Click **Continue** after the registration confirmation is displayed.
6. Optionally upgrade or activate licenses for other services, such as for Cloud Management and Reporting.
7. After activation, view the **System > Licenses** page on the appliance to see a cached version of the active licenses.

Upgrading Information

For information about obtaining the latest firmware, upgrading the firmware image on your SonicWall appliance, and importing configuration settings from another appliance, see the *SonicWall SMA Upgrade Guide* available on the Support portal at https://www.sonicwall.com/support/technical-documentation.

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 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.

The information in this document is provided in connection with SonicWall Inc. 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 SonicWall 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 reserve the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc.. 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.

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/eupa.

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

Last updated: 11/5/20

232-005405-00 Rev A