

SonicWall® Secure Mobile Access 10.2.0.3 Release Notes

November 2020

These release notes provide information about the SonicWall® Secure Mobile Access 10.2.0.3 release.

Topics:

- [About SonicWall SMA 10.2.0.3](#)
- [Supported Platforms](#)
- [Resolved Issues](#)
- [Known Issues](#)
- [Feature Support by Platform](#)
- [Client Versions Released with 10.2.0.3](#)
- [Product Licensing](#)
- [Upgrading Information](#)
- [SonicWall Support](#)

About SonicWall SMA 10.2.0.3

SonicWall SMA 10.2.0.3 updates NetExtender clients for Windows and Linux, updates SMA Connect Agent clients for Windows and macOS, and fixes a number of known issues found in previous releases. Refer to the [Client Versions Released with 10.2.0.3](#) and [Resolved Issues](#) sections for additional information. This release supports all the features and resolved issues from previous SMA 10.2 releases. For more information see the previous release notes on MySonicWall.

SMA 10.2.0.3 is compatible with Capture Security Center (CSC). CSC provides a cloud dashboard that displays the overall status of all the registered SMA appliances. The dashboard has sliders to choose the Time Period, Count of Alerts, Threats, WAF Threats, Authentications, VPN Accesses, Bookmark Access, Active devices and Users on Map, and Threats categories.

- Use your MySonicWall credentials to log into CSC at <https://cloud.sonicwall.com>.
- Click the **SMA** tile to view the SMA Dashboard, complete registration, and enable cloud management.

Supported Platforms

NOTE: SMA 10.2.0.3 is compatible with Capture Security Center (CSC).

SonicWall SMA 10.2.0.3 is supported on the following SonicWall appliances:

- SMA 200/400
- SMA 210/410
- SMA 500v for ESXi (The SonicWall SMA 500v for ESXi is supported for deployment on VMware ESXi 5.0 and higher)
- SMA 500v for Hyper-V (The SonicWall SMA 500v for Hyper-V is supported for deployment on Hyper-V Server version—2016 and 2019)
- SMA 500v for AWS
- SMA 500v for Azure

For additional information, see [Feature Support by Platform](#) and [Client Versions Released with 10.2.0.3](#).

Resolved Issues

This section provides a list of resolved issues in this release.

Resolved Issue	Issue ID
The NetExtender client address range appears exhausted.	SMA-1960
Using Native RDP, the Copy\Paste function and the local drive redirection with loopback IP are not functioning as expected.	SMA-1959
The SMA https web server could be susceptible to vulnerability.	SMA-1958
Geo-IP shows the SMA appliance location as being off the map.	SMA-1957
When in Contemporary Mode, enabling SNMPv3 does not function as expected.	SMA-1956
When configured from Contemporary Mode, the client route is missing for NetExtender.	SMA-1955
Boot Error. Respawnns too quickly during reboot, upgrade, or VM move.	SMA-1953
Bookmarks are limited when using the web user interface.	SMA-1952
Twillo returns an SMS template error message.	SMA-1951
At Windows log on, NetExtender offers no possibility of choosing how to send the OTP.	SMA-1950
Web HTTPS bookmarks fail to allow form-based fields. Returns a BadSSOFormsField error message.	SMA-1949
HTML5/Native RDP connections drop.	SMA-1947
When in Contemporary Mode, users are unable to add any bookmarks to a user's account .	SMA-1946
The NetExtender Client Version 10.2.816 selects disk the GUID as the unique identifier. When the system reboots, the line order changes and is recognized as a new device.	SMA-1945
NetExtender is unable to create a connection profile as expected.	SMA-1943
Unable to access Netapp Share through a CIFS bookmark.	SMA-1942
RDP bookmarks do not function as expected with the HTML5 access type.	SMA-1941
When using Android versions of Mobile Connect, a "Server Certificate Validation Error" appears.	SMA-1940
The OWA website does not accept input as expected.	SMA-1939

Resolved Issue	Issue ID
Outlook does not function correctly when it is connected to the Offloaded Exchange 2016 Application (basic authentication).	SMA-1938
Unable to change the Active Directory (AD) password before expiration.	SMA-1936
RDP bookmark credentials are in clear text on the connect agent logs.	SMA-1934
Cannot change the options of the NetExtender Traffic Log Settings.	SMA-1933
The EPC is unable to detect the Operating System version of a Windows 10 Virtual machine on the KVM host.	SMA-1932
Verify that a partial domain name (DN) in the subject to %AD:cn% does not function as expected.	SMA-1893
The NetExtender client address range appears exhausted.	SMA-1789
AOV with OTP is generating multiple user-sessions and multiple OTP's.	SMA-1641
An RSA AM PIN change results in a "PIN Rejected" error message even after the server had accepted the PIN.	SMA-1609
Enabling "Allow Password Changes" in the Contemporary Mode user interface, reverts back to the disabled state after clicking Submit .	SMA-1606
User sessions are all displayed with "(On Active)" appended to the username in the Users > Status page. Workaround: Restart the SMA.	SMA-1529
Duo MFA requires a piece of code to execute for authentication in Contemporary Mode.	SMA-1401
A Duo PUSH script does not work in the Contemporary Mode web interface, but works fine in Classic Mode.	SMA-1087

Known Issues

The following is a list of issues known to exist at the time of the SMA 10.2.0.3 release.

Known Issue	Issue ID
Browser-based SSH connection does not work to establish connection to the SMA 500v for AWS appliance.	SMA-878
Malicious files are not displayed in the Capture ATP reports.	SMA-772
In the 10.2.0.3 build, duo authentication in Classic mode does not function as expected, however, when in Contemporary Mode it does.	SMA-1963
Enabling Allow Password Changes reverts back to the disabled state after clicking Submit. Occurs when creating a RADIUS domain in Contemporary Mode . Workaround: Use Classic Mode.	SMA-1513
Avast Premium anti-virus is not available under the EPC profile and the EPC check fails. Occurs after updating the Avast anti-virus package to the latest updates, which changes its name to Avast Premium.	SMA-1244

Feature Support by Platform

Although all SonicWall SMA appliances support major Secure Mobile Access features, not all features are supported on all SonicWall SMA appliances.

The SonicWall SonicWall SMA appliances share most major Secure Mobile Access features, including:

- Virtual Office
- NetExtender
- Application Offloading
- Web Application Firewall
- Geo-IP
- Botnet
- End Point Control
- Load Balancing

Features Not Supported on SonicWall SMA 200/210

The following features are supported on the SonicWall SMA 400/410, but not on the SonicWall SMA 200/210:

- Application profiling
- High Availability

Features Not Supported on SonicWall SMA 500v for AWS and Azure

- High Availability

Client Versions Released with 10.2.0.3

Topics:

- [NetExtender Client Versions](#)
- [SMA Connect Agent Versions](#)

NetExtender Client Versions

The following is a list of NetExtender client versions introduced in this release.

Description	Version
NetExtender Linux RPM 32-Bit	10.2.817
NetExtender Linux RPM 64-Bit	10.2.817
NetExtender Linux TGZ 32-Bit	10.2.817

Description	Version
NetExtender Linux TGZ 64-Bit	10.2.817
NetExtender Windows	10.2.302

SMA Connect Agent Versions

The following is a list of SMA Connect Agent versions supported in this release.

Description	Version
SMA Connect Agent Windows	1.1.33
SMA Connect Agent macOS	1.1.33

Product Licensing

The SonicWall Secure Mobile Access 10.2.0.3 firmware provides user-based licensing on SonicWall SMA 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 Secure Mobile Access 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 appliance:

- 1 Log in 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.
- 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>.

Copyright © 2020 SonicWall Inc. All rights reserved.

This product is protected by U.S. and international copyright and intellectual property laws. SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

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: 11/10/20

232-005514-00 Rev A