SonicWall® Secure Mobile Access 10.2.0.2

Release Notes

July 2020

These release notes provide information about the SonicWall® Secure Mobile Access 10.2.0.2 release.

Topics:

About SonicWall SMA 10.2.0.2

SonicWall SMA 10.2.0.2 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 10.2.0.2 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 10.2.0.2 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 10.2.0.2 is compatible with Capture Security Center (CSC).

SonicWall SMA 10.2.0.2 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 10.2.0.2.

Resolved Issues

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

Resolved Issue	Issue ID
Custom Active Directory attributes are displayed instead of the bookmark name. Occurs when the Virtual Office Portal is viewed in Contemporary Mode, after configuring custom AD attributes and a new bookmark.	SMA-1173
NetExtender client logs are not populated with log messages. User status details are sometimes not shown in the client. Occurs with NetExtender version 10.0.0.297.	SMA-1275
SMA for Hyper-V can reboot randomly, sometimes after a few hours.	SMA-1425
SAML Authentication can have errors when using a custom port or through port 443.	SMA-1429
The option for whether to allow editing of bookmarks is missing when creating a new bookmark. If the bookmark is saved and then edited, the option appears and can be configured. If the bookmark is not edited, then users can always edit the bookmark. Occurs when using SMA Contemporary Mode, but not with Classic Mode.	SMA-1436
VoIP does not work on an SMA for Azure because it does not know the original IP address of the endpoint. Occurs when the SMA for Azure is running in NAT Mode and cannot parse traffic from the LAN back to the SMA client.	SMA-1459
The correct certificate is not pushed for an offloaded portal.	SMA-1474
The SAML certificate is not shown in the SMA management interface, but attempting to import it shows that a duplicate certificate exists. Occurs after importing configuration settings that were exported from another unit, such as an SMA for Azure.	SMA-1475
The Device ID becomes jumbled and automatic device approval/registration fails.	SMA-1476
Chromebook users get the error, “Your device is not supported for this feature” when clicking on an RDP HTML5 bookmark. Occurs when using SMA Contemporary Mode, but not with Classic Mode.	SMA-1478

Resolved Issue	Issue ID
SMS authentication does not work in some cases when the portal is in Contemporary Mode. Occurs when Two-Factor authentication is enabled and • the user changes from SMS to Email during login for receiving a temporary password; no password is generated. • the user changes from Email to SMS during login for receiving a temporary password; login screen error prevents entering the generated password.	SMA-1480
A shared Single Sign-On domain, such as a bookmark link to an offloaded web application portal, does not work in Contemporary Mode.	SMA-1481
Video redirect and audio recording/playback does not work with HTML5 / Native RDP access. There is no setting in the configuration dialog that allows RDP camera forwarding.	SMA-1482
Portal login succeeds with a user name that is different from the CN in the client certificate. Occurs when using Contemporary Mode, but not in Classic Mode.	SMA-1491
When logging in using One-Time Password via Email, the second page to enter the temporary password does not appear. Instead, the login page is refreshed. Occurs when using Contemporary Mode, but not in Classic Mode.	SMA-1495
The RADIUS code page does not load in Classic Mode, and errors out in Contemporary Mode. Occurs when using the Starling App for RADIUS authentication.	SMA-1498

Known Issues

The following is a list of issues known to exist at the time of the SMA 10.2.0.2 release.

Known Issue	Issue ID
Malicious files are not displayed in the Capture ATP reports.	SMA-772
Browser-based SSH connection does not work to establish connection to the SMA 500v for AWS appliance.	SMA-878
A Duo PUSH script does not work in the Contemporary Mode web interface, but works fine in Classic Mode.	SMA-1087
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
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
User sessions are all displayed with “(On Active)” appended to the username in the Users > Status page. **Workaround**: Restart the SMA.	SMA-1529

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 10.2.0.2

Topics:

NetExtender Client Versions

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

Description	Version
NetExtender Linux RPM 32-Bit	10.2.816
NetExtender Linux RPM 64-Bit	10.2.816
NetExtender Linux TGZ 32-Bit	10.2.816

Description	Version
NetExtender Linux TGZ 64-Bit	10.2.816
NetExtender Windows	10.2.300

SMA Connect Agent Versions

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

Description	Version
SMA Connect Agent Windows	1.1.31
SMA Connect Agent macOS	1.1.31

Product Licensing

The SonicWall Secure Mobile Access 10.2.0.2 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.

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: 7/14/20

232-005359-00 Rev A