SonicWall Secure Mobile Access 10.2.0.8

Release Notes

These release notes provide information about the SonicWall Secure Mobile Access (SMA) 10.2.0.8 release.

Versions:

Version 10.2.0.8

September 2021

About SonicWall SMA 10.2.0.8

SonicWall SMA 10.2.0.8 fixes a number of known issues found in previous releases. Refer to the Resolved Issues section for additional information. This release supports all the features and resolved issues from previous SMA 10.2 releases.

Knowledge Base Articles for Upgrading

ⓘ **IMPORTANT:** Be sure to review the following Knowledge Base articles before upgrading your SMA appliance.

- How To Upgrade Firmware On SMA 100 Series Appliances
- Aditional SMA 100 Series 10.X And 9.X Firmware Updates Required
- SMB SSL-VPN: Upgrading Firmware On SMA 500v Virtual Appliance

Compatibility and Installation Notes

ⓘ | **NOTE:** SMA 10.2.0.8 is compatible with Capture Security Center (CSC).

SonicWall SMA 10.2.0.8 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

SMA 10.2.0.8 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 cloud.sonicwall.com.
- Click the SMA tile to view the SMA Dashboard, complete registration, and enable cloud management.

For additional information, see Feature Support by Platform and Client Versions Released with 10.2.0.8.

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 and Load Balancing
- Web Application Firewall
- Geo IP and Botnet Filtering
- End Point Control
- Capture ATP
- CSC Management and Reporting

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 10.2.0.8

Topics:

NetExtender Client Versions

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

Description	Version
NetExtender Linux RPM 32-Bit	NetExtender.Linux-10.2.827-1.i686.rpm
NetExtender Linux RPM 64-Bit	NetExtender.Linux-10.2.827-1.x86.64.rpm
NetExtender Linux TGZ 32-Bit	NetExtender.Linux-10.2.827.x86.tgz
NetExtender Linux TGZ 64-Bit	NetExtender.Linux-10.2.827.x86_64.tgz
NetExtender Windows	NetExtender.Linux-10.2.314

SMA Connect Agent Versions

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

Description	Version
SMA Connect Agent Windows	1.1.37
SMA Connect Agent macOS	1.1.30

Product Licensing

The SonicWall Secure Mobile Access 10.2.0.8 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 upgrading information, refer to the Knowledge Base articles listed in Knowledge Base Articles for Upgrading.

ⓘ **NOTE:** SMA upgrades should be done sequentially. For example, on SMA appliances running SMA 8.6, first upgrade to firmware version 9.0.0.10 and then to 10.2.0.8.

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.

Upgrading a High Availability Pair

To upgrade firmware on an SMA HA Pair:

1. Upload the new SMA firmware on the active unit (node 1).
2. Boot the new firmware on active unit (node 1).
3. While node 1 is rebooting, the idle unit will become active (node 2).
4. Upload the new firmware on active unit (node 2).
5. Boot the new firmware on active unit (node 2).

After the two appliances are rebooted, the HA pair is fully updated with the new firmware.

About Client Upgrades

Normally, the client is upgraded automatically if there is a new client version included with the firmware.

NOTE: If the NetExtender client is installed with the Windows MSI installer, it will not be upgraded automatically.

Resolved Issues

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

Issue ID	Issue Description
SMA-2144	High Availability (HA) is not stable due to random fail-over events.
SMA-2184	Duo PUSH Proxy script does not work as intended.
SMA-2243	EPC update fails post upgrading to 10.2.0.5-29 version.
SMA-2344	SAML users are unable to log in to SMA 500v appliances.
SMA-2345	Unable to load Application Offload Portal post upgrading to 10.2.0.6 version.
SMA-2432	NetExtender RPM package does not contain " libNetExtenderEpc" files.
SMA-2435	File download fails when CIFS/SMB bookmark contains more than14 Japanese characters in file name.
SMA-2436	Post upgrading to 10.2.0.6-32 version, SMA 500v on Azure displays high CPU utilization at 100 percent.
SMA-2437	PCI scan fails and displays the following error "Insecure configuration of Cookie attributes" when "HTTP Only" for SRA cookies is enabled.
SMA-2438	Incorrect Spanish characters are displayed in HTTP Bookmarks.
SMA-2439	Unable to edit or delete device information when searched from the device list page.

Issue ID	Issue Description
SMA-2445	Post upgrading to the latest firmware version, the following error "not a valid cookie domain name" is displayed in both classic mode and contemporary mode.
SMA-2446	Virtual Office bookmark does not forward passwords after DUO authentication in contemporary mode.
SMA-2448	FTP backup does not work as intended post upgrading to 10.2.0.6 version.
SMA-2449	Configured scheduled daily backup does not work as intended.
SMA-2458	RDP bookmark SSO fails for Local LDAP linked to Azure AD LDAP.
SMA-2462	SSO authentication does not work as intended for Citrix bookmark.
SMA-2530	Even after disabling HTTP and HTTPS of x1 interface, users are able to access management over X1 interface.
SMA-2533	Unable to send logs through email.
SMA-2535	Kaspersky EPC checks only version for all the attributes.
SMA-2548	In the DNS tab, all the DNS suffixes are not displayed when connecting to NetExtender.
SMA-2563	Folder download fails when the name of the file in the folder contains un-ascii characters.
SMA-2620	Backup system does not switch to primary role and unable to take ownership of the IP.
SMA-2636	Password timeout of OTP does not work as intended for Always-On-VPN.
SMA-2642	EPC checks fails for the equipment ID's and the serial number of users PC is displayed as "System Serial number" instead of displaying PC Serial number.
SMA-2647	Unable to import Settings and logging to SMA appliance fails.
SMA-2664	Offloaded portal dropped due to HTTP DoS Settings.
SMA-2690	SMA Connect does not launch NetExtender with SAML Authentication.
SMA-2707	Unable to display the frame when "X-Frame-Options" is set to "sameorigin".
SMA-2717	Post upgrading to 10.2.0.6 version, Macintosh web users are not able to open RDP native client bookmarks.
SMA-2720	Switching back to SMS OTP option in the latest UI always triggers OTP.
SMA-2727	When User discretion of OTP is enabled, the settings option in the user portal is not displayed.
SMA-2736	The Japanese characters on websites registered in bookmarks are distorted in 10.2.0.6 firmware version.
SMA-2741	Update Signature failed frequently with error message "Update Signature failed, error code 500".
SMA-2759	Resources are not available in the tab after successful authentication with Azure AD SSO.
SMA-2766	Unable to edit user created bookmark in contemporary mode.

Issue ID	Issue Description
SMA-2807	Issues with RADIUS Authentication when users try to log in using expired password.
SMA-2818	RADIUS Authentication with Challenge-Response does not work as intended in Contemporary Mode.
SMA-2819	Incorrect French characters are displayed in HTTP Bookmarks.
SMA-2821	Unable to access features of Application offloaded portal in few web browsers.
SMA-2822	SMA appliance experienced a power failure which cleared stored device IDs.
SMA-2823	Issues with translation in Application Offload Portal post upgrading to 10.2.0.6 version.
SMA-2825	While logging with NetExtender (MSI) for the first time, unreadable routes are displayed.
SMA-2876	When a network change is detected, the NetExtender with Always On VPN enabled does not reconnect automatically.
SMA-2934	Unauthenticated SMA100 Arbitrary File Delete Vulnerability.
SMA-2957	Authenticated SMA100 Arbitrary Command Injection Vulnerability.
SMA-2973	Private IPs are displayed in public facing portal.
SMA-3002	Net-SNMP package is vulnerable to insufficient check of NULL pointer (SNMP DoS).
SMA-3015	Local Privileged Escalation via Command Injection in HA.

Known Issues

Issue ID	Issue Description
SMA-2276	First user session is automatically logged out even when *Enforcement method* is set to "Confirm logout of Existing session".
SMA-2662	Settings backup fails through email when email address include "-" character.
SMA-2765	Calender Synchronization of Teams fails over SMA with or without WAF.
SMA-2893	Secure Network Detection (SND) is detected without even entering OTP.

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

NOTE: A NOTE icon indicates supporting information.

IMPORTANT: An IMPORTANT icon indicates supporting information.

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 Release Notes
Updated - September 2021
Software Version - 10.2.0.8
232-005755-00 Rev B

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