SonicWall® Secure Mobile Access 10.2.0.0

Release Notes

February 2020

These release notes provide information about the SonicWall® Secure Mobile Access 10.2 release.

Topics:

About SonicWall SMA 10.2

SonicWall SMA 10.2 is a feature release that includes new features and fixes a number of known issues found in previous releases. Refer to the New Features and Resolved Issues sections for additional information. This release supports all the features and resolved issues from previous SMA 10.0 releases. For more information see the previous release notes on MySonicWall.

SMA 10.2 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 is compatible with Capture Security Center (CSC).

SonicWall SMA 10.2 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 HyperV (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.

New Features

Secure Mobile Access 10.2 adds the following new features:

- Transport Layer Security TLS 1.3 Support
- Hosting of SMA Virtual Appliance on Public Cloud Environment—AWS and Azure
- Option to Deny Mobile App Binding when Login is Attempted from any External Network
- Reuse of Mobile App Binding Text Code
- Flexibility to Choose Two-Factor Authentication Method for NetExtender Login
- Generating Certificates Using Let's Encrypt
- SMA Dashboard Enhancements
- SAML 2.0 Authentication
- “Use user-mapped address” support for Active Directory Groups/Users
- Restful API - Phase 2 Support

Transport Layer Security TLS 1.3 Support

SMA has been enhanced to support the latest secured protocol version TLS 1.3 for both incoming and outgoing connections.

ⓘ **NOTE:** TLS 1.3 is supported on NetExtender for Linux but not on NetExtender for Windows.

Hosting of SMA Virtual Appliance on Public Cloud Environment—AWS and Azure

Users can now launch their own instances of SMA 500v in public cloud environment—AWS and Azure. The hosted 500v supports the same features as a data center-hosted 500v.

For information on installing and configuring SMA 500v instance for AWS and Azure, see the *SMA 500v Getting Started Guide for AWS and SMA 500v Getting Started Guide for Azure* available at the Technical Documentation portal: https://www.sonicwall.com/support/technical-documentation/.

Option to Deny Mobile App Binding when Login is Attempted from any External Network

If the administrator has enabled **Mobile App** option for Time-based One Time Password (TOTP) Two Factor Authentication and has specified networks such as corporate network to bind the mobile App during **Virtual Office** login, users will see the mobile-binding QR code only when login is attempted from any of the networks specified by the administrator.

Reuse of Mobile App Binding Text Code

If an administrator enables **Allow Sharing TOTP key** option for an SMA appliance, the mobile app binding text code for binding a mobile app with a user account can be reused when binding mobile app with other user accounts, thereby OTP generated in a single mobile-app account can be used for authentication during login of all the users that shared binding key.

Flexibility to Choose Two-Factor Authentication Method for NetExtender Login

User can now choose the required OTP Authentication method: **Email**, **SMS**, or **Mobile APP** for NetExtender login authentication if the administrator enables **One-Time Password** in **Login Policies**.

ⓘ **NOTE:** This feature is supported on NetExtender for Windows but not on NetExtender for Linux.

Generating Certificates Using Let's Encrypt

Let's Encrypt is a non-profit certificate authority run by Internet Security Research Group that provides X.509 certificates for Transport Layer Security encryption at no charge.

This feature enables administrators to generate a valid public certificate trusted by most browsers for different portals. Certificate is generated quickly, and administrator can use it in the portal.

SMA Dashboard Enhancements

The **Overview > Dashboard** page displays the overview of system health—total threat count, current & historic graph for CPU, memory, concurrent users, connected tunnel users, current users and application locational info, and threat summary.

SAML 2.0 Authentication

Security Assertion Markup Language (SAML) is a standard protocol used by web browsers to enable Single Sign-On (SSO) through secure tokens.

SAML eliminates the need for passwords during sign-in by implementing a secure method of passing user authentications and authorizations between the identity provider and service providers. When a user logs into a SAML enabled application, the service provider requests authorization from the appropriate identity provider. The identity provider authenticates the user's credentials and then returns the authorization for the user to the service provider, and the user is now able to use the application.

SAML 2.0 specifies a Web Browser SSO Profile that involves exchanging information among an identity provider (IDP), a service provider (SP), and a principal (user) on a web browser. SMA100 works as a Service Provider (SP); Microsoft Azure Active Directory and onelogin server work as Identity Providers.

"Use user-mapped address" support for Active Directory Groups/Users

Administrators can configure NetExtender client address pool to "Use user-mapped address" for Active Directory Group, Radius Group, and User.

Restful API - Phase 2 Support

Restful API phase 2 includes mainly the Management APIs and Report APIs:

- With Management APIs, the front-end developers can query, add, modify and delete SMA appliance management configuration data.
- With Report APIs, the front-end developers can query current active users, sessions and system status.

Resolved Issues

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

Resolved Issue	Issue ID
Unable to import appliance settings from a previously-saved configuration file to an HA-paired appliance.	SMA-666
Customized logos on portals are not displayed properly in the contemporary mode.	SMA-757
In some cases, the SMA appliance stops responding, resulting in: preventing administrator-login; logs out an active administrator.	SMA-976
NetExtender login fails with incorrect username/password message. This issue repeats every 8 days after it is temporarily fixed by restarting the appliance.	SMA-1010

Known Issues

The following is a list of issues known to exist at the time of the SMA 10.2 release.

Known Issue	Issue ID
Error message: *SSL-VPN clock is out of sync with Active Directory* is not displayed during Active-Directory user login even when there is no clock synchronization between the appliance and the domain controller.	SMA-514
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
When **Enable Hit Counters** option is enabled for the custom rules generated on the **WAF > Rules** page, an error message is displayed.	SMA-908
In SMA 500v Hyper-V High-Availably configuration setup, if the primary appliance is restarted from the management interface, the failover does not work.	SMA-939
When the SMA appliance is configured with IPv6 address/gateway, the user location in the dashboard is shown as out of map.	SMA-950
When the active MobileConnect sessions are disconnected using the **DISCONECT ALL option** on the **Clients > Status** page, the **Status** page continues to show the MobileConnect sessions as active, though the sessions are terminated. This is a UI error.	SMA-956
Although **Enforce login uniqueness** is enabled and enforcement method is set as **Confirm logout of existing session** for a portal, when the same user attempts login from another browser, the login is granted without terminating the existing session.	SMA-970

Feature Support by Platform

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

The SonicWall SonicWall SMA/SRA 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

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	10.2.813
NetExtender Linux RPM 64-Bit	10.2.813
NetExtender Linux TGZ 32-Bit	10.2.813
NetExtender Linux TGZ 64-Bit	10.2.813
NetExtender Windows	10.2.292

SMA Connect Agent Versions

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

Description	Version
SMA Connect Agent Windows	1.1.27
SMA Connect Agent macOS	1.1.22

Product Licensing

The SonicWall Secure Mobile Access 10.2.0.0 firmware provides user-based licensing on SonicWall SMA/SRA 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 and to customers who have trial versions.

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 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: 2/18/20

232-005199-00 Rev A