SonicWall™ Secure Mobile Access 12.0.1

Release Notes

April 2017

These release notes provide information about the SonicWall™ Secure Mobile Access (SMA) 12.0.1 release.

About Secure Mobile Access

Secure Mobile Access (SMA) provides scalable, secure mobile access for your enterprise while blocking untrusted applications, WiFi pirates and mobile malware. SMA appliances provide a single gateway and a common user experience across all platforms, including managed and unmanaged devices. Traffic is encrypted using Secure Sockets Layer (SSL) to protect it from unauthorized users.

Supported Platforms

The SMA 12.0.1 release is supported on the following SMA 1000 series appliances:

- EX9000
- EX7000
- EX6000
- SMA 6200
- SMA 7200
- SMA 8200v (ESX/Hyper-V)

Client systems running version 12.0.1 client software can be used with SonicWall SMA appliances running one of the following firmware versions:

- 11.4.0
- 10.7.2

New Features

The focus of Secure Mobile Access 12.0.1 was the rebranding of the firmware and the interface as a SonicWall product. The look and feel of the user interface has been updated to a more modern appearance. Several issues were also resolved in this release; refer to Resolved Issues for more information about them.

SMA 12.0.1 also has the capability to re-image a physical appliance with any of the supported firmware versions. It is the equivalent of a full factory reset. All files and settings are permanently overwritten. You may want to use this capability if you are adding a new SMA appliance to environment running a prior version since SonicWall is shipping all new devices with version 12.0.1.

Deprecated Features

Old Aventail MIBs for SNMP have been discontinued.

Resolved Issues

The following is a list of resolved issues addressed in this release.

AMC

Resolved issue	Issue ID
Struts is vulnerable to certain kinds of attacks.	185183
AMC doesn't show IP address(es) in SAN list. Occurs when a SAN self-signed certificate is created in AMC and it is expanded to view details.	183206

Connect Tunnel

Resolved issue	Issue ID
Cipher set does not include the most secure ciphers. Occurs on Macintosh Connect Tunnel 11.4.0-325.	184014

Linux

Resolved issue	Issue ID
SMA-6200 and 7200 LCD panel and buttons are not working. Occurs when appliance was updated to SMA 12.0.1.	183236

Provisioning

Resolved issue	Issue ID
Agents provisioning through Java fails due to the end of support for NPAPI plugin. Occurs when using Firefox 52 browser.	184638

Known Issues

This section describes the known issues in this release.

AMC

Known issue	Issue ID
NTP fails to synchronize appliance timings with the NTP server. Occurs when we disable and enable NTP service in the AMC.	185976

Central Management

Known issue	Issue ID
The CMS overwrites authentication settings on the SMA appliance during policy synchronization. Occurs when Central User Licensing is disabled at the CMS, and "Each node has its own authentication server" is enabled.	178437
The critical and warning alerts for the event “Permanent/Temporary communication loss” on managed appliances have the same default values. As a result, only the warning alert is raised and the critical alert is NEVER raised. This prevents an SNMP trap from being raised by the CMS. Occurs when one of the managed appliances is rebooted or when the Eth0 interface is shutdown and an alert is generated.	177622
Managed appliances cannot be upgraded from the CMS. Occurs when trying to upgrade managed appliances from 11.4 to 12.0.	177593
FQDN resources cannot be disabled from the Central Management Service (CMS). Occurs when using web applications such as Jira and Confluence with Central Management Service (CMS) with Global Traffic Management (GTO).	177152

Connect Tunnel

Known issue	Issue ID
Not able to access WP using IPv4 address . Occurs when CT is connected using IPv6.	186156
Connect Tunnel becomes unresponsive after upgrading to Window 10 client version. Occurs when Connect Tunnel is pre installed.	183102
Connect Tunnel Service (CTS) cannot establish a tunnel. Occurs when "Device Authorization" is configured, and CTS is started.	178422

EPC

Known issue	Issue ID
The Client Certificate zone classification is successful with the ROOT CA certification, but it should not prompt for zone classification with ROOT CA. Occurs on Extra Web and Connect Tunnel on Windows.	185870

HTML5 Clients

Known issue	Issue ID
Text cannot be copied and pasted to or from remote computers. Occurs when using the HTML5 clients in the Chrome, Edge, or Firefox browsers.	177501

User Database

Known issue	Issue ID
The appliance loses all the user bookmarks; the bookmarks table is empty. Occurs on configuring Citrix, VMware and vWorkspace agents in AMC.	186114

Virutal Appliance

Known issue	Issue ID
The ESXI virtual appliance cannot be upgraded. Occurs when trying to upgrade an ESXI virtual appliance from 10.7.2 to 12.0 directly.	176950

Workplace

Known issue	Issue ID
When opting to install the CacheCleanerContrlClass add-on in WP home page, user is prompted to stay or leave the page. Occurs when user already has the older CC add-on installed in IE.	183102
SSH and Telnet HTML5 clients display an error message. Occurs when trying to use SSH or Telnet in Windows IE10.	178045
The French (Belgium) keyboard replaces the English (United states) keyboard and vice versa. Occurs when trying to select the English or French keyboards in WorkPlace.	177333

Upgrading Information

For information about upgrading an E-Class SMA appliance to version 12.0.x from an earlier release, be sure to consult the appropriate *SMA Upgrade Guide*, available on https://www.mysonicwall.com/.

Product Licensing

SonicWall SMA or E-Class SMA appliances must be registered on MySonicWall to enable full functionality and the benefits of SonicWall security services, firmware updates, and technical support.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid support 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://support.sonicwall.com.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- Download software
- View video tutorials
- Collaborate with peers and experts in user forums
- Get licensing assistance
- Access MySonicWall
- Learn about SonicWall professional services
- Register for training and certification

To contact SonicWall Support, visit https://support.sonicwall.com/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: 4/27/17

232-003884-00 Rev A