SonicWall® Secure Mobile Access 10.0.0.0

Release Notes

May 2019

These release notes provide information about the SonicWall® Secure Mobile Access 10.0.0.0 release.

Topics:

About SonicWall SMA 10.0.0.0

SonicWall SMA 10.0.0.0 is a new feature release that includes a number of known issues. Refer to the New Features, and Known Issues sections for additional information. This release supports all the features and resolved issues from previous SMA 9.0 releases. For more information see the previous release notes on MySonicWall.

Supported Platforms

SonicWall SMA 10.0.0.0 is supported on the following SonicWall appliances:

- SMA 200
- SMA 400
- SMA 500v for ESXi
- SMA 500v for Hyper-V

The SonicWall SMA 500v for ESXi is supported for deployment on VMware ESXi 5.0 and higher.

For additional information, see Feature Support by Platform and Client Versions Released with 10.0.0.0.

New Features

Secure Mobile Access 10.0 release several new features including:

- Two-factor Authentication and One-time Password Support for HTTP Posting to ISP URLs and SMS Integration
- Custom Ports for HTTPS
- Deprecation of the VirtualAssist/VirtualMeeting Features
- Downloading Files and Folders using HTML5 File Share Applets
- End Point Control Improvements
- Enhancement of Syslog Documentation for NetExtender Users, Assigned IP Addresses, and Data Traffic or Usage
- Hyper-V Support
- Restful API - Phase 1 Support
- Single Sign-on Functionality Included in NetExtender for Mapping Network Drives using Batch Scripts for Non-domain PCs
- Support for Gen 7 Hardware
- UX/UI Improvements

Two-factor Authentication and One-time Password Support for HTTP Posting to ISP URLs and SMS Integration

SMA currently supports sending One-time Passwords (OTP) through SMTP. Although most cellular carriers support the translation of mail to a Short Message Service (SMS) text, in some countries, this is not an option and SMA must integrate with third-party SMS gateway providers such as Twilio, Nexmo, and Clickatell through their REST APIs to send outgoing SMA messages from one mobile number to others around the globe.

SMA now provides an option to configure which HTTP status codes the gateway would send after accepting a message for delivery.

Services include:

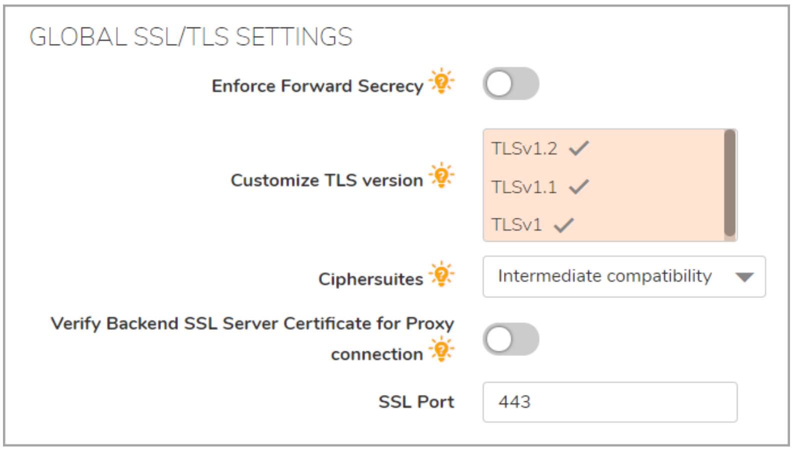
- **SMS Gateway Configuratio**n - SMA should be able to reliably identify whether an SMS Gateway provider has accepted a message for delivery so that it can notify the administrator and end-user (in case of failures).
- **Authentication Server Configuration** - The authentication module would facilitate optionally sending OTP through SMS along with mail.
- **SMS Gateway Selection** - Choose a gateway between pre-configured SMS gateway configurations.
- **Phone Attributes for Local Users** - Configure phone attributes for locally authenticated users.

Custom Ports for HTTPS

There are two places where administrators can set custom ports for HTTPS:

- **Global Level Setting** - You can set a global custom port on the **System > Administration** page. The global setting is applied to all portals when they have not been edited on their own **Settings** page.

See the new option, **SSL Port**, in the **Global SSL/TLS Settings** section. The default port number is set at 443, but you can edit that port number to a customized one meant for all portals.



GLOBAL SSL/TLS SETTINGS

Enforce Forward Secrecy: ○

Customize TLS version: TLSv1.2 ✓ TLSv1.1 ✓ TLSv1 ✓

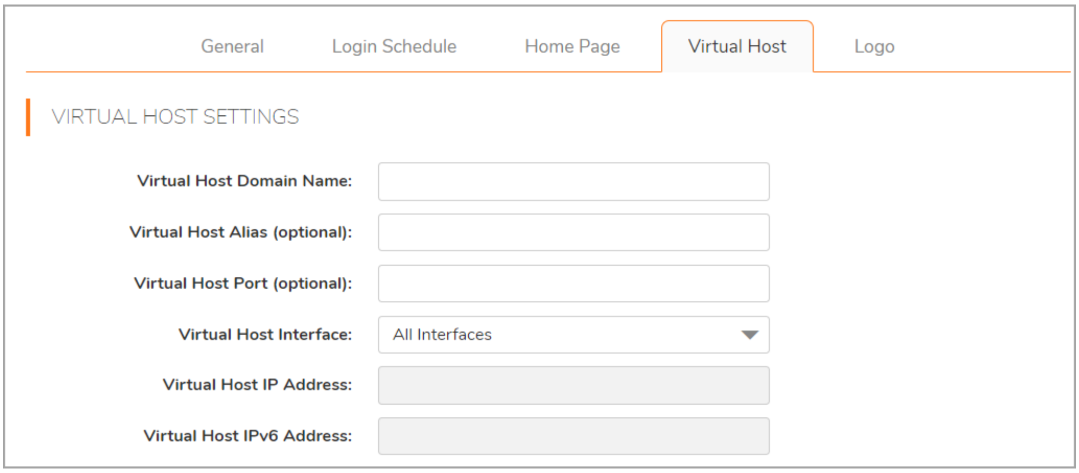
Ciphersuites: Intermediate compatibility

Verify Backend SSL Server Certificate for Proxy connection: ○

SSL Port: 443

- **Portal Level Setting** - You can add or edit custom ports on the **Portals > Portals | Add Portal** (include normal portal and web application) and **Edit Portal** pages. Overwrite the global settings or leave them blank to inherit the global settings.

  When adding a normal portal, the key to setting custom ports is through the **Virtual Host Port (optional)** on the **Virtual Host** tab. You can leave this space blank to use the global settings or edit a legal value for this portal.



VIRTUAL HOST SETTINGS

Virtual Host Domain Name:

Virtual Host Alias (optional):

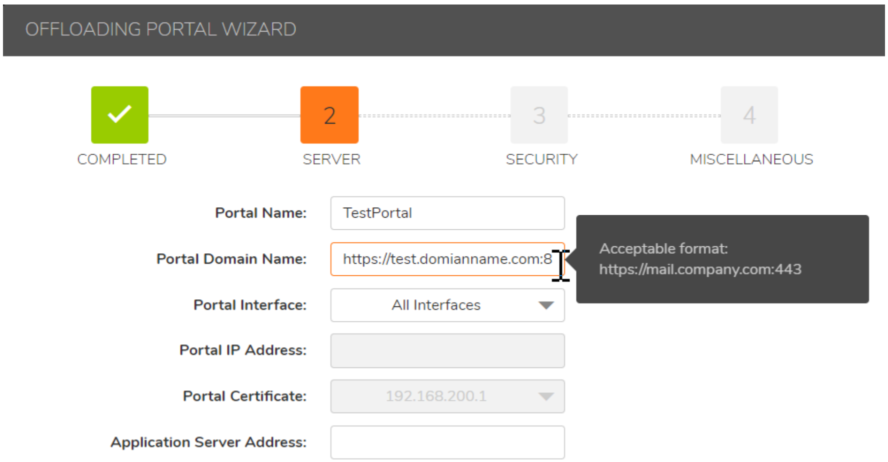
Virtual Host Port (optional):

Virtual Host Interface: All Interfaces

Virtual Host IP Address:

Virtual Host IPv6 Address:

When adding an offloading portal using the Offloading Portal Wizard,, the key to setting custom ports is through the **Portal Domain Name**. You can edit that domain using `https://test.domainname.com` to inherit the global settings, or use `https://test.domainname.com:8443` to use 8443 as the custom port for the offloading portal.



OFFLOADING PORTAL WIZARD

Portal Name:	TestPortal
Portal Domain Name:	https://test.domianname.com:8
Portal Interface:	All Interfaces
Portal IP Address:	
Portal Certificate:	192.168.200.1
Application Server Address:	

Acceptable format:
https://mail.company.com:443

When editing a portal, the key to setting custom ports is through the **Virtual Host Port (optional)** on the **Virtual Host** tab. You can leave this space blank to use global settings or edit a legal value for this portal.

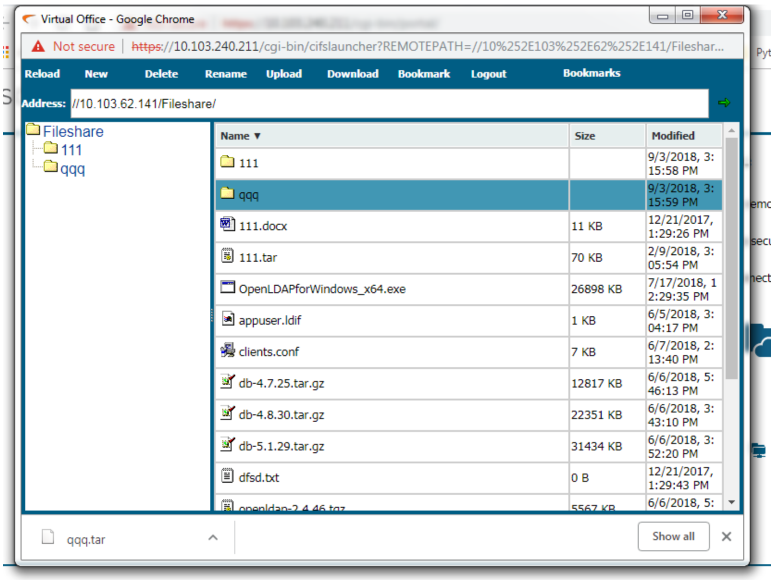
Deprecation of the VirtualAssist/VirtualMeeting Features

All VirtualAssist and VirtualMeeting configurations have been removed from SMA 10.0, including client binaries, license information in the TSR, and the Status page.

Downloading Files and Folders using HTML5 File Share Applets

You can download multiple files and folders in one tar ball, or download them one by one by selecting them and clicking the Download link located at the top of the file share window.

Download a single file and save it as a tar ball

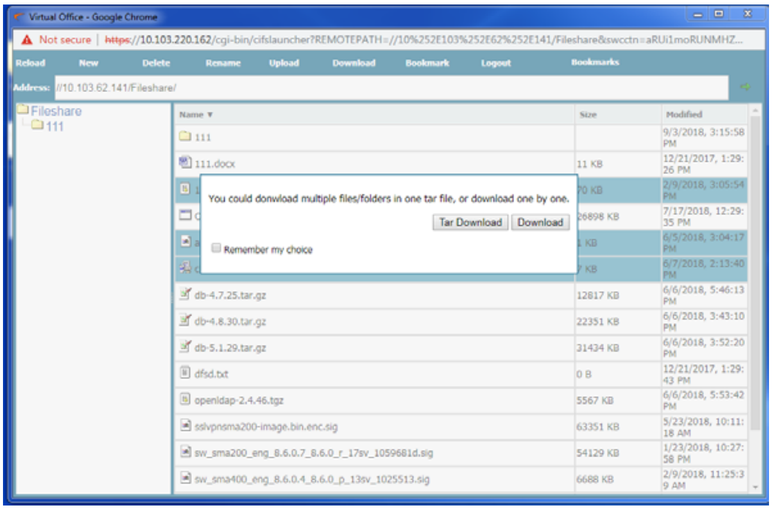


https://10.103.240.211/cgi-bin/cifslauncher?REMOTEPATH=//10%252E103%252E62%252E141/Fileshar...

Address: //10.103.62.141/Fileshare/

Name ▼	Size	Modified
111		9/3/2018, 3: 15:58 PM
qqq		9/3/2018, 3: 15:59 PM
111.docx	11 KB	12/21/2017, 1:29:26 PM
111.tar	70 KB	2/9/2018, 3: 05:54 PM
OpenLDAPforWindows_x64.exe	26898 KB	7/17/2018, 1 2:29:35 PM
appuser.ldif	1 KB	6/5/2018, 3: 04:17 PM
clients.conf	7 KB	6/7/2018, 2: 13:40 PM
db-4.7.25.tar.gz	12817 KB	6/6/2018, 5: 46:13 PM
db-4.8.30.tar.gz	22351 KB	6/6/2018, 3: 43:10 PM
db-5.1.29.tar.gz	31434 KB	6/6/2018, 3: 52:20 PM
dfsd.txt	0 B	12/21/2017, 1:29:43 PM
openldap-2.4.46.tgz	5567 KB	6/6/2018, 5:

Download multiple files and save them as a tar ball



Virtual Office - Google Chrome
Not secure | https://10.103.220.162/cgi-bin/cifslauncher?REMOTEPATH=//10%252E103%252E62%252E141/Fileshare&swcctn=aRUi1moRUNMHZ...
Reload
New
Delete
Rename
Upload
Download
Bookmark
Logout
Bookmarks
Fileshare
111

Address: //10.103.62.141/Fileshare/

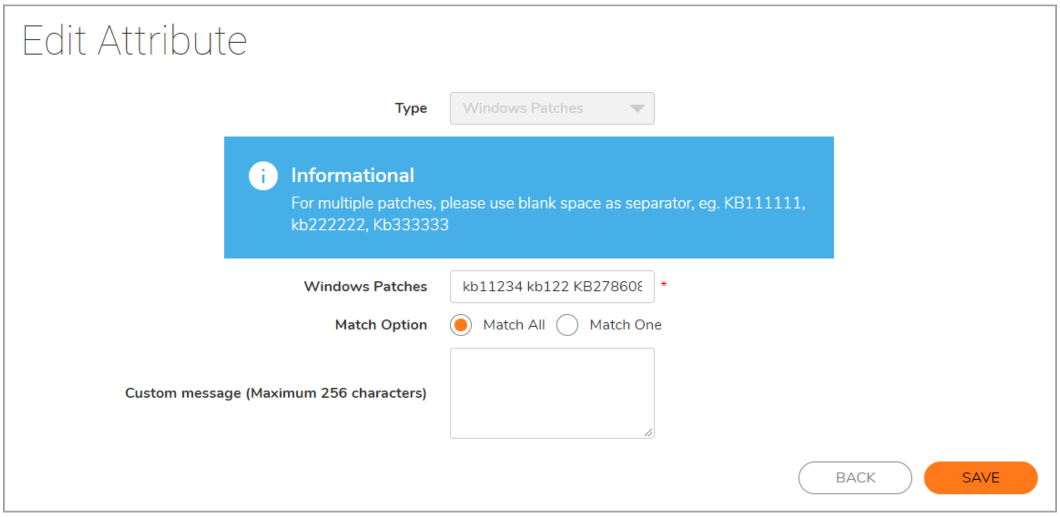
Name ▾	Size	Modified
111		9/3/2018, 3:15:58 PM
111.docx	11 KB	12/21/2017, 1:29:26 PM
1	70 KB	2/9/2018, 3:05:54 PM
c	26898 KB	7/17/2018, 12:29:35 PM
a	1 KB	6/5/2018, 3:04:17 PM
c	7 KB	6/7/2018, 2:13:40 PM
db-4.7.25.tar.gz	12817 KB	6/6/2018, 5:46:13 PM
db-4.8.30.tar.gz	22351 KB	6/6/2018, 3:43:10 PM
db-5.1.29.tar.gz	31434 KB	6/6/2018, 3:52:20 PM
dfsd.txt	0 B	12/21/2017, 1:29:43 PM
openldap-2.4.46.tgz	5567 KB	6/6/2018, 5:53:42 PM
sslvpnsma200-image.bin.enc.sig	63351 KB	5/23/2018, 10:11:18 AM
sw_sma200_eng_8.6.0.7_8.6.0_r_17sv_1059681d.sig	54129 KB	1/23/2018, 10:27:58 PM
sw_sma400_eng_8.6.0.4_8.6.0_p_13sv_1025513.sig	6688 KB	2/9/2018, 11:25:39 AM

You could donwload multiple files/folders in one tar file, or download one by one.

□ Remember my choice

End Point Control Improvements

Windows Patch inspection has been added to the End Point Control profile to confirm important software patches have been installed. To do this, you can add Windows patch numbers on SMA's **End Point Control > Device Profiles** page. Use a space to separate multiple patches. Windows Patch inspections are only supported on NetExtender Windows clients.



Edit Attribute

Type: Windows Patches

Informational

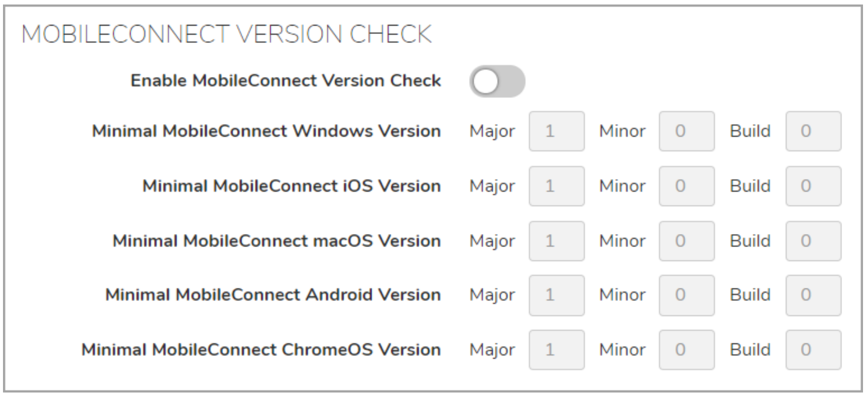
For multiple patches, please use blank space as separator, eg. KB111111, kb222222, Kb333333

Windows Patches: kb11234 kb122 KB27860E *

Match Option: ● Match All ○ Match One

Custom message (Maximum 256 characters):

You can also enable the new Mobile Connect Version Inspection on the **Clients > Advanced Settings** page.



MOBILECONNECT VERSION CHECK

Enable MobileConnect Version Check: off

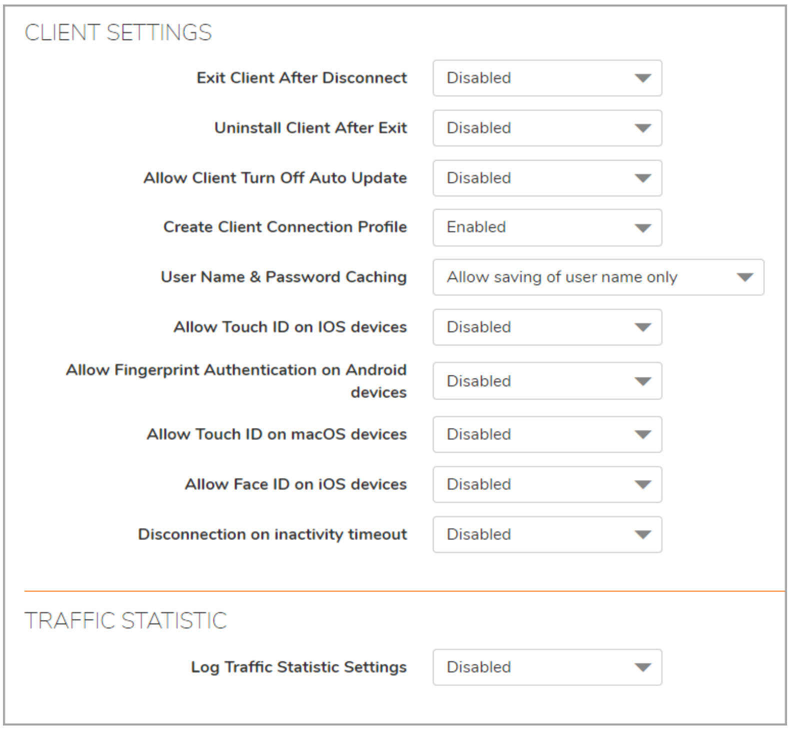
Minimal MobileConnect Windows Version	Major	1	Minor	0	Build	0
Minimal MobileConnect iOS Version	Major	1	Minor	0	Build	0
Minimal MobileConnect macOS Version	Major	1	Minor	0	Build	0
Minimal MobileConnect Android Version	Major	1	Minor	0	Build	0
Minimal MobileConnect ChromeOS Version	Major	1	Minor	0	Build	0

Enhancement of Syslog Documentation for NetExtender Users, Assigned IP Addresses, and Data Traffic or Usage

When you log in with NetExtender, you can specify that the logs reported to the syslog servers include the IP addresses assigned and the interval at which to log traffic statistics for date usage. There are additional messages that periodically document the data usage of each user in the network.

You can set Interval at which to log traffic statistics for data usage after logging in to SMA through an SMA client.

- **Global Level Setting** - Edit the interval in **Clients > Settings** or **Edit Global Policies** page. The global settings impact all users. You can find the **Log Traffic Statistic Interval** option in the **Traffic Statistic** section or on the **Clients** tab of **Edit Global Policies**. The default is **0** which means to never log the traffic statistic or set a positive number as the interval.



CLIENT SETTINGS

Exit Client After Disconnect	Disabled
Uninstall Client After Exit	Disabled
Allow Client Turn Off Auto Update	Disabled
Create Client Connection Profile	Enabled
User Name & Password Caching	Allow saving of user name only
Allow Touch ID on IOS devices	Disabled
Allow Fingerprint Authentication on Android devices	Disabled
Allow Touch ID on macOS devices	Disabled
Allow Face ID on iOS devices	Disabled
Disconnection on inactivity timeout	Disabled

TRAFFIC STATISTIC

Log Traffic Statistic Settings	Disabled

- **Group Level Settings** - You can edit the interval on the **Edit Group** page. The interval impacts the users in this group. Leaving it blank uses the global settings.
- **User Level Settings** - You can edit the interval on the **Edit User** page, which impacts only that specific user. Leaving it blank uses the group settings.

Hyper-V Support

SMA can now be deployed within a Hyper-V virtual environment. This feature is developed specifically to support the deployment of SMA 500v images installed on Microsoft Hyper-V platforms. Virtual machines for Hyper-V can be registered at MySonicWall, as well as license activation.

SMA 500v for Hyper-V shares serial numbers and authorization codes from SMA 500v for ESXi machines. All other SMA functionalities perform identically on the SMA 500v for Hyper-V virtual machines.

Restful API - Phase 1 Support

Using several dedicated Restful APIs, you can access an SMA 100 appliance. Using API's to log in to or from the appliance, you can also perform End Point Control checks, device profile checks, and so on.

- **Authentication API** - The Authentication API is set for your appliance. API consumers can refer to the API documentation and follow it step by step. It is also very convenient for external integration.
- **Threat API** - The Threat API reports threat information about your appliance, and includes varying information depending on the circumstances.
- **API Documentation** - The documentation for the API is tightly integrated with the actual implementation of the API to minimize the potential for the documentation and implementation to drift out of synch.

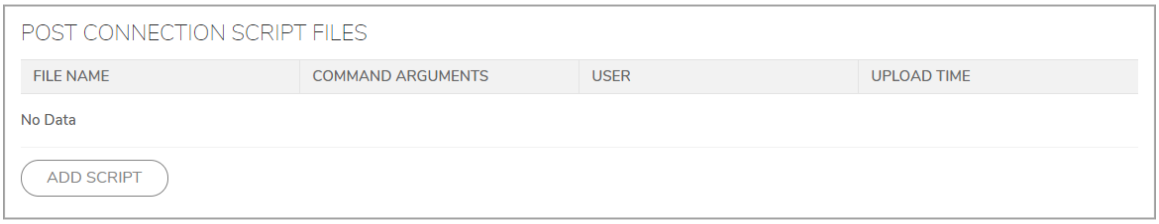
Single Sign-on Functionality Included in NetExtender for Mapping Network Drives using Batch Scripts for Non-domain PCs

This feature is supported only on Windows NetExtender clients and is based on feature post connect scripts with execution arguments added to each script. When the client executes a post-connection script, the arguments are executed together. Several special variables are defined, standing in for the runtime environment parameters, such as the client logon user name, the client logon domain, password, and so on.

In NetExtender Post Connection Scripts, you can use variables in batch scripts to map your network drives, depending on different levels of access. In Domain PCs, when the script is run as follows:

```
ECHO ON REM ============Map a network drive======================== net use z:
\\server\share /user:Domain%USERNAME%
```

This script does not prompt you for credentials and still maps the network drive successfully. But, in case of non-domain PCs, the variable %USERNAME% takes the username that is logged on to the machine and so authentication for mapping the network drive fails. Credentials are reprompted. See the **Clients > Advanced Settings | Post Connection Script Files** page.



POST CONNECTION SCRIPT FILES

FILE NAME	COMMAND ARGUMENTS	USER	UPLOAD TIME
No Data			

Support for Gen 7 Hardware

SMA provides support for Gen 7 Hardware with firmware and Safemode images for SMA210 and SMA410.

UX/UI Improvements

In the SMA 10.0 release, the SMA Management Console user interface style is being updated to a new SonicWall user interface appearance that not only provides a new look and feel, but employs improved navigation capabilities as well.

Known Issues

The following is a list of issues known to exist at the time of the SMA 10.0 release.

Authentication

Known Issue	Issue ID
The Active Directory Group search capability does not function as expected.	215849

Capture ATP

Known Issue	Issue ID
The option to close the file report window when in Contemporary mode is not present.	216023

Logs

Known Issue	Issue ID
Custom Favicons do not function as expected.	214796

SSL-VPN

Known Issue	Issue ID
Cannot create service policies using standard IP addresses.	216069
Cannot create service policies using IPv6 Deny.	216059
Cannot edit IPv6 service policies.	216055
The “Access type selection” option is no longer found in newly created VNC bookmarks.	216014
The copyright year of the SMA Connect Agent Windows Application needs to be updated.	215039
The Page Up/Down option should be enabled on the current window.	214527

WAF

Known Issue	Issue ID
The Hyper-V appliance crashes when the Web Application firewall has been enabled with the Auto Install Signatures option.	216267

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

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

- Application profiling
- High Availability

Client Versions Released with 10.0.0.0

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	10.0.807
NetExtender Linux RPM 64-Bit	10.0.807
NetExtender Linux TGZ 32-Bit	10.0.807
NetExtender Linux TGZ 64-Bit	10.0.807
NetExtender Windows	10.0.0.282

SMA Connect Agent Versions

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

Description	Version
SMA Connect Agent Windows	1.1.20
SMA Connect Agent MacOSX	1.1.18

Product Licensing

The SonicWall Secure Mobile Access 10.0.0.0 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 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: 5/13/19

232-004895-00 Rev A