SonicWall Secure Mobile Access 1000 Series 12.4 Release Notes

These release notes provide information about the SonicWall Secure Mobile Access (SMA) 1000 series v12.4.1 release.

Versions:

- 12.4.1

12.4.1

June 2021

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/Transport Layer Security (SSL/TLS) to protect it from unauthorized users.

SMA is available as a physical appliance or as a virtual appliance running on VMWare ESXi, Microsoft Hyper-V, Amazon Web Services (AWS), Azure, and KVM.

CMS can be run on VMWare ESXi, Microsoft Hyper-V, Amazon Web Services (AWS), Azure, and KVM.

Supported Platforms

The SMA 12.4 release is supported on the following SMA 1000 series appliances:

- SMA 6200 series (SMA 6200 and SMA 6210)
- SMA 7200 series (SMA 7200 and SMA 7210)
- SMA 8200v (ESXi/Hyper-V/AWS/Azure/KVM)
- Central Management Server (CMS) (ESXi/Hyper-V/AWS/Azure/KVM)

ⓘ | **NOTE:** SMA 12.4 is not supported on EX6000, EX7000, and EX9000 appliances.

Supported Firmware Levels

Client systems running version 12.4 client software can be used with SonicWall SMA appliances running one of the following firmware versions:

- 12.4.0 + latest hotfixes -> 12.4.1
- 12.1.0 + latest hotfixes -> 12.4.1
- 12.3.0 + latest hotfixes -> 12.4.0 + Latest HF -> 12.4.1

ⓘ | **IMPORTANT:** To upgrade from Secure Mobile Access 12.3, you must upgrade to version 12.4.0 first, then upgrade to 12.4.1.

ⓘ | **IMPORTANT:** You can directly upgrade to 12.4.1 from SMA 12.1.0, and 12.4.0 versions.

For more information on supported platforms, clients, servers, IT infrastructure, and online services, refer to *Administration Guide*.

Additional References

- https://www.sonicwall.com/support/knowledge-base/sma-1000-series-and-cms-general-faq/200317200026571/
- https://www.sonicwall.com/support/knowledge-base/sma-1000-series-support-matrix/170919113911935/

What's New

SonicWall Secure Mobile Access (SMA) 12.4.1 includes these new features:

- **Support to Let's Encrypt certificates**.

  Let’s Encrypt is a certificate authority that is Public, Free, API-driven, and Trusted by browsers/clients. Integrating Let's Encrypt certificate with SMA enhances the security and eases the deployment process. Also, Integration with Let's Encrypt allows administrators to obtain appliance certificate from Let's Encrypt CA and manage them automatically.
- **Support to Microsoft Intune**.

  Microsoft Intune is a Microsoft cloud-based management solution for mobile device and operating system management. It aims to provide Unified Endpoint Management of both corporate and BYOD devices in a way that protects corporate data. Integrating Microsoft Intune with SMA helps administrators to enable more robust policy decisions based on intune's device state attributes.
- **Support to KVM hypervisor**.

  KVM, or Kernel based Virtual Machine is a software module that allows Linux to operate as a hypervisor. QEMU, or Quick Emulator, allows guest operating systems to run on the KVM hypervisor and supports virtualization where applications executing in the user space can achieve near native speeds through full virtualization or paravirtualization.
- **WorkPlace enhancements**.
  - Audio and Video recording for RDP shortcuts and bookmarks is supported.
  - The Modern WorkPlace is now on par with the legacy WorkPlace. All the agents that are supported in legacy WorkPlace are supported in Modern WorkPlace.
  - To avoid multiple pop up windows, bookmarks are now launched in a new tab.

    - For enhanced user experience, following are the File Explorer improvements implemented in the current release.
        - Folder can be downloaded as a zip file.
        - You can cut, copy, and paste the files and folders.
- **Device VPN enhancements**.

  Secure Hosts for secure network detection can now be configured under community level and you can configure up to three secure hosts.
- **Connect Tunnel enhancements**.

  The enhancements include support for Apple Silicon Mac, Surface Pro X, and parity with Legacy Connect Tunnel.
- **Tunnel Exclusions**

  Resource Exclusion List feature is enhanced and renamed as Tunnel Exclusions from 12.4.1 version onwards. Tunnel Exclusion excludes host names, IP addresses, subnets, IP ranges, or domains from being redirected to the appliance.
- **Manage SSH settings from CMS**

  For CMS Administrators, it is difficult to authorize keys when configuring on multiple appliances. To overcome this scenario, SMA is enhanced to manage the SSH settings centrally from CMS. You can configure SSH once in CMS and use the same to access SSH in all the managed appliances and CMS after successful completion of Policy Synchronization.
- **Support for User Groups in SAML IdP Authentication**

  SMA and CMS is enhanced to support SAML authentication for Administrators. Also, SMA is enhanced to support group membership details over SAML authentication and users without on-premise Active Directory can now have group level management.
- **Improved SAML Authentication server configuration experience**

  AMC now allows administrators to import/export SAML configuration as metadata files. SAML Authentication Server configuration page is redesigned which removes complexity involved in manually configuring SAML authentication servers.
- **CMS Address Pool enhancements**.

  CMS Address Pool is enhanced and each managed appliance can now:
    - Have a unique address pool
    - Share an address pool configuration with one or more other appliances
    - Use a default address pool

What's Deprecated

- Legacy WorkPlace and Connect Tunnel Service
- Support for ActiveX and Internet Explorer
- Support for Windows 7

Resolved Issues

Issue ID	Issue Description
SMA1000-3898	Disable/Stop all web proxying and enable only Tunnel service for user access.
SMA1000-3814	Random Connect Tunnel connections stalls at identifying when connecting to an appliance.
SMA1000-3772	CRADestinationData AUTO_INCREMENT is getting into automatic error recovery mode.
SMA1000-3747	Connect Tunnel connection timeout if ACL have unresolvable hostnames.
SMA1000-3723	Support Audio, Microphone and Camera redirection with RDP Personal Bookmarks.
SMA1000-3721	Citrix Workspace 2012 agent update should be controlled by Administrator.
SMA1000-3639	Vulnerability CVE-2021-3156.
SMA1000-3596	Secure Client Initiated Renegotiation, DOS vulnerabilities.
SMA1000-3512	OWA attachments with larger size fails with Dynamic SSO enabled.
SMA1000-3466	CMS: Alert emails are not sent with SMTP issues reported.
SMA1000-3444	High severity CVE in all versions of OpenSSL -- CVE-2020-1971
SMA1000-3433	User Sessions are not displayed in CMS.
SMA1000-3394	Connect Tunnel client does not auto update to 12.4 on macOS Big Sur.
SMA1000-3393	SMTP Test button fails with unknown error when deploying a virtual machine.
SMA1000-3371	Limitations in adding the default search domain.
SMA1000-3365	Null pointer exception is displayed while editing a user/group that is not set to Any realm.
SMA1000-3361	UI/UX improvements for Connect Tunnel icon.
SMA1000-3342	Appliance removed from CMS holds its entries of appliance and user sessions.
SMA1000-3275	Appliance crashes when uninstalling the client.
SMA1000-3228	License count cache mishandles actual count query results.
SMA1000-3218	Connect Tunnel update fails when clients do not have administrative rights on their local systems.
SMA1000-3214	OCSP failure due to missing HTTP host header entry when multiple backend virtual host server exists.
SMA1000-3046	Unable to view user sessions on CMS and synchronize all the managed appliances simultaneously.
SMA1000-2852	The graphs on CMS and the managed appliance shows the same shape but shows different peak bandwidth.
SMA1000-2633	Javascript library vulnerability CVE-2020-11022 (workplace/clients)
SMA1000-2490	12.4.0 upgrade fails on a single CMS managed SMA node.
SMA1000-2390	Unable to upgrade from 12.3 to 12.4 version.
SMA1000-2133	Log message enhancements in kern.log file.
SMA1000-2109	Local recording device option is not available in remote desktop session.

Issue ID	Issue Description
SMA1000-1986	Hostnames should not contain underscore and a maximum of 63 characters is allowed.
SMA1000-1202	Challenges in clearing the logs who do not have SSH access to the device. To overcome this scenario, options such as clear logs, reset logs, delete all snapshots, delete recent snapshots are added in the user interface as well as API.

Known Issues

Issue ID	Issue Description
SMA1000-3918	Unable to create LE certificate when CMS eth0 is not reachable from MA.
SMA1000-4063	Connect Tunnel does not connect with 142 resource exclusion with RANL but DNS resolution fails.

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 - June 2021
Software Version - 12.4
232-005695-00 Rev A

Copyright © 2021 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall 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 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 reserves the right to make changes to specifications and product descriptions at any time without notice. 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.