



# SonicWall Secure Mobile Access 10.2.1

## Release Notes

These release notes provide information about the SonicWall Secure Mobile Access (SMA) 10.2.1 release.

### Versions:

- [Version 10.2.1.14](#)
- [Version 10.2.1.13](#)
- [Version 10.2.1.12](#)
- [Version 10.2.1.11](#)
- [Version 10.2.1.10](#)
- [Version 10.2.1.9](#)
- [Version 10.2.1.8](#)
- [Version 10.2.1.7](#)
- [Version 10.2.1.6](#)
- [Version 10.2.1.5](#)
- [Version 10.2.1.4](#)
- [Version 10.2.1.3](#)
- [Version 10.2.1.2](#)
- [Version 10.2.1.1](#)
- [Version 10.2.1](#)

## Version 10.2.1.14

November 2024

## About Secure Mobile Access

Secure Mobile Access (SMA) provides scalable, secure mobile access for your enterprise while blocking untrusted applications, WiFi pirates, and 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 ESXi, Microsoft Hyper-V, Amazon Web Services (AWS), Azure, and KVM.

## Compatibility and Installation Notes

- Most popular browsers are supported, but Google Chrome is preferred for the real-time graphics display on the dashboard.
- A MySonicWall account is required.
- SMA 10.2.1.14 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 (Web Application Firewall) Threats, Authentications, VPN Accesses, Bookmark Access, Active devices and Users on a 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.

SonicWall SMA 10.2.1.14 is supported on the following SonicWall appliances:

- SMA 200/400
- SMA 210/410
- SMA 500v for ESXi
  - Supported for deployment on ESXi 6.0 and higher
- SMA 500v for HyperV
  - Supported for deployment on Hyper-V server version 2016 and 2019
- SMA 500v for AWS
- SMA 500v for Azure
- SMA 500v for KVM

## What's New

- This release provides the fixes for previously reported issues and security improvements.

## Resolved Issues

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

| Issue ID | Issue Description  |
|----------|--|
| SMA-5466 | Using the "Message authenticator" attribute is recommended, but user authentication fails. |
| SMA-5536 | Path traversal issue.  |
| SMA-5537 | Heap-based buffer overflow issue.  |
| SMA-5538 | Stack-based buffer overflow issue.   |
| SMA-5539 | Authentication bypass using an Alternate Path or Channel.                                  |
| SMA-5540 | Insecure randomness.   |
| SMA-5567 | Stack based buffer overflow issue.   |

## Known Issues

Not Applicable.

## Additional References

Not Applicable.

## Version 10.2.1.13

August 2024

## About Secure Mobile Access

Secure Mobile Access (SMA) provides scalable, secure mobile access for your enterprise while blocking untrusted applications, WiFi pirates, and 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 ESXi, Microsoft Hyper-V, Amazon Web Services (AWS), Azure, and KVM.

## Compatibility and Installation Notes

- Most popular browsers are supported, but Google Chrome is preferred for the real-time graphics display on the dashboard.

- A MySonicWall account is required.
- SMA 10.2.1.14 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 (Web Application Firewall) Threats, Authentications, VPN Accesses, Bookmark Access, Active devices and Users on a 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.

SonicWall SMA 10.2.1.14 is supported on the following SonicWall appliances:

- SMA 200/400
- SMA 210/410
- SMA 500v for ESXi
  - Supported for deployment on ESXi 6.0 and higher
- SMA 500v for HyperV
  - Supported for deployment on Hyper-V server version 2016 and 2019
- SMA 500v for AWS
- SMA 500v for Azure
- SMA 500v for KVM

## What's New

- Added an option in portal to restrict the access. The portal only allows the NetExtender/Mobile Connect to access.
- This release provides the fixes for previously reported issues.

## Resolved Issues

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

| Issue ID | Issue Description  |
|----------|--|
| SMA-4939 | Routing mode is no longer an option in the user interface of the SMA 500v in Azure/AWS platform.   |
| SMA-4970 | Unable to delete the old certificates not used anywhere are shown as a pending state.              |
| SMA-5168 | Unable to boot after the upgrade from 10.2.1.10/11 to 10.2.1.12, and it fails on Hyper-V platform. |

# Known Issues

Not Applicable.

# Additional References

SMA-5463, SMA-5398, SMA-5374, SMA-5339, SMA-5201, SMA-5199, SMA-5186, SMA-5063, SMA-5047, SMA-5020, SMA-5019, SMA-5007, SMA-4998, SMA-4989, SMA-4988, SMA-4960, SMA-4937, SMA-4936, SMA-4934, SMA-4932, SMA-4903, SMA-4858, SMA-4842.

# Version 10.2.1.12

April 2024

# About Secure Mobile Access

Secure Mobile Access (SMA) provides scalable, secure mobile access for your enterprise while blocking untrusted applications, WiFi pirates, and 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 ESXi, Microsoft Hyper-V, Amazon Web Services (AWS), Azure, and KVM.

# Compatibility and Installation Notes

- Most popular browsers are supported, but Google Chrome is preferred for the real-time graphics display on the dashboard.
- A MySonicWall account is required.
- SMA 10.2.1.12 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 (Web Application Firewall) Threats, Authentications, VPN Accesses, Bookmark Access, Active devices and Users on a 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.

SonicWall SMA 10.2.1.12 is supported on the following SonicWall appliances:

- SMA 200/400
- SMA 210/410
- SMA 500v for ESXi
  - Supported for deployment on ESXi 6.0 and higher
- SMA 500v for HyperV
  - Supported for deployment on Hyper-V server version 2016 and 2019
- SMA 500v for AWS
- SMA 500v for Azure
- SMA 500v for KVM

## What's New

This release provides the following new feature.

Blocking Source IP Address for Continuous Login Failures is introduced in Secure Mobile Access 10.2.1.12 onwards:

Block Source IP Address for Continuous Login Failures is a default-enabled feature that blocks IP addresses and will not be allowed to access the appliance.

For more information, refer to the section *Blocking Source IP Address for Continuous Login Failures* in the *SMA100 10.2 Administration Guide*.

## Additional References

SMA-4993.

## Version 10.2.1.11

February 2024

## About Secure Mobile Access

Secure Mobile Access (SMA) provides scalable, secure mobile access for your enterprise while blocking untrusted applications, WiFi pirates, and 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.

## Compatibility and Installation Notes

- Most popular browsers are supported, but Google Chrome is preferred for the real-time graphics display on the dashboard.
- A MySonicWall account is required.
- SMA 10.2.1.11 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 (Web Application Firewall) Threats, Authentications, VPN Accesses, Bookmark Access, Active devices and Users on a 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.

SonicWall SMA 10.2.1.11 is supported on the following SonicWall appliances:

- SMA 200/400
- SMA 210/410
- SMA 500v for ESXi
  - Supported for deployment on VMware ESXi 6.0 and higher
- SMA 500v for HyperV
  - Supported for deployment on Hyper-V server version 2016 and 2019
- SMA 500v for AWS
- SMA 500v for Azure
- SMA 500v for KVM

## What's New

This release provides the fixes for previously reported issues.

## Resolved Issues

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

| Issue ID | Issue Description   |
|----------|---|
| SMA-3904 | No statistics in the WAF monitoring graph for connection count. |

| Issue ID | Issue Description   |
|----------|---|
| SMA-4716 | Device is unstable.   |
| SMA-4764 | The bookmarked page in Virtual Office is garbled after upgrading to 10.2.1.9.                                     |
| SMA-4789 | When adding a botnet policy in contemporary mode, if the name field contains a space, the policy cannot be saved. |
| SMA-4795 | NetExtender user failed to change its initial password due to server response error.                              |
| SMA-4802 | Key pair is not associated with authorized_keys when installing SMA 500v for AWS.                                 |
| SMA-4805 | SMA100 MFA Improper access control vulnerability.   |
| SMA-4820 | Unable to create a WAF rule with the operator field "Contains".   |
| SMA-4821 | Deleting an invalid syntax login policy fail to delete due to "Get user's setting failed".                        |
| SMA-4829 | Both full and partial imports makes the appliance inaccessible.   |
| SMA-4857 | When EPC fails, the custom messages are not displayed; instead, the default messages are displayed.               |

## Known Issues

Not Applicable.

## Additional References

Not Applicable.

## Version 10.2.1.10

November 2023

## About Secure Mobile Access

Secure Mobile Access (SMA) provides scalable, secure mobile access for your enterprise while blocking untrusted applications, WiFi pirates, and 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.



# Compatibility and Installation Notes

- Most popular browsers are supported, but Google Chrome is preferred for the real-time graphics display on the dashboard.
- A MySonicWall account is required.
- SMA 10.2.1.10 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 (Web Application Firewall) Threats, Authentications, VPN Accesses, Bookmark Access, Active devices and Users on a 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.

SonicWall SMA 10.2.1.10 is supported on the following SonicWall appliances:

- SMA 200/400
- SMA 210/410
- SMA 500v for ESXi
  - Supported for deployment on VMware ESXi 6.0 and higher
- SMA 500v for HyperV
  - Supported for deployment on Hyper-V server version 2016 and 2019
- SMA 500v for AWS
- SMA 500v for Azure
- SMA 500v for KVM

## What's New

This release provides the following new features, deprecated features, and fixes for previously reported issues.

### **New Features**

These features are introduced in Secure Mobile Access 10.2.1.10 onwards:

- Customize DNS Settings for the SMA Appliance using Azure/AWS Platform
- Customize a Default gateway for the SMA Appliance using Azure/AWS Platform
- Enabling Lockout for Source IP Address.

For more information, refer to the section *New features* in the *SMA100 10.2 Administration Guide*.

### **Deprecated Features**

This feature is deprecated in Secure Mobile Access 10.2.1.10 onwards:

- Deprecate Legacy User Interface (UI).

For more information, refer to the section *Deprecated features* in the *SMA100 10.2 Administration Guide*.

## Resolved Issues

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

| Issue ID | Issue Description   |
|----------|---|
| SMA-4120 | Outdated client-side java script libraries (Jquery) need to be upgraded in future releases.   |
| SMA-4187 | SMTP password visible in plain text (even with a Read-only account), it should be masked.   |
| SMA-4518 | Fails PCI scan issues from SYSNET.  |
| SMA-4557 | When the NTP server is enabled, the time is reset by a minute or two, resulting in TOTP connection failures.                                      |
| SMA-4596 | Path based issues.  |
| SMA-4597 | Unable to adjust DNS settings on SMA using Azure with or without custom settings.   |
| SMA-4620 | Duplicate device showing in device management, because of SMA-4499 issue.   |
| SMA-4625 | Login to Virtual Office portal and click in NetExtender to connect, DNS suffix is not pushed to client, direct NetExtender works.                 |
| SMA-4656 | SMA appliance is inaccessible due to post upgrade firmware from 10.2.1.7-50sv to 10.2.1.8-53sv on SMA 500v Azure platform.                        |
| SMA-4661 | SMA stops authenticating connection requests and when logging in to the web portal with ERROR = Socket Creation Failed.                           |
| SMA-4668 | Custom WAF rule cross side scripting causes reboot loop of the httpd process.   |
| SMA-4674 | Downloaded NetExtender installer cannot be validated. Ensure connecting to a trusted SSL VPN server and NAC agent issue.                          |
| SMA-4675 | Httpd process fails device rebooting 10.2.1.9 related to EasyAccess cannot import settings.   |
| SMA-4678 | OTP email does not include the subject line information even with [%] entered.  |
| SMA-4679 | EPC check fails with Virtual Office with Connect agent version 1.1.46 on SMA 10.2.1.9 version.  |
| SMA-4682 | Webshell on a SonicWall virtual SMA - malware analysis.   |
| SMA-4698 | Manual sending of event logs fails even if "Email Event Logs to" contains an email address within the email address field.                        |
| SMA-4705 | License sync fails after post upgrade from 10.2.1.0-17sv to 10.2.1.1-19sv on SMA 500v using KVM platform.   |
| SMA-4713 | After upgrade to 10.2.1.9 version, connection to <a href="https://soniclicense.global.sonicwall.com">soniclicense.global.sonicwall.com</a> fails. |

| Issue ID | Issue Description  |
|----------|--|
| SMA-4724 | Let's Encrypt certificate will not be renewed automatically.                             |
| SMA-4759 | Authenticated RCE.   |
| SMA-4783 | Duplication of AD user leading to MFA bypass in SMA100 appliances.                       |
| SMA-4761 | Unicode characters including Japanese/Chinese characters are garbled in the OTP message. |
| SMA-4784 | Unable to install and update EPC, sign certificate of EPC Agent has been expired.        |
| SMA-4787 | NetExtender Windows cannot validate OPSWAT package and fail to connect.                  |

## Additional References

SMA-4702

## Version 10.2.1.9

August 2023

## 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.

## Compatibility and Installation Notes

- Most popular browsers are supported, but Google Chrome is preferred for the real-time graphics display on the Dashboard.
- A MySonicWall account is required.
- SMA 10.2.1.9 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 (Web Application Firewall) Threats, Authentications, VPN Accesses, Bookmark Access, Active devices and Users on a 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.

SonicWall SMA 10.2.1.9 is supported on the following SonicWall appliances:

- SMA 200/400
- SMA 210/410
- SMA 500v for ESXi
  - Supported for deployment on VMware ESXi 6.0 and higher
- SMA 500v for HyperV
  - Supported for deployment on Hyper-V server version 2016 and 2019
- SMA 500v for AWS
- SMA 500v for Azure
- SMA 500v for KVM

## What's New

This release provides fixes for previously reported issues.

## Resolved Issues

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

| Issue ID | Issue Description   |
|----------|---|
| SMA-3108 | PCI scanning detected that the SMA is using commonly used prime numbers.                          |
| SMA-3414 | High memory utilization causing the device to reboot.   |
| SMA-3704 | SMA 500V on AWS platform starts correctly and then goes to offline within an hour.                |
| SMA-3712 | The device reboots when the memory utilization reached 98%.                                       |
| SMA-3798 | After the device logged off for an external user, a local user is created that cannot be deleted. |
| SMA-3867 | DHCP leases the same IP for multiple client requests.   |
| SMA-3889 | Unable to delete the local users.   |
| SMA-3947 | Unknown error is displayed when the email settings is sent.                                       |
| SMA-3967 | Certificate page is not displayed on the contemporary mode.                                       |
| SMA-3971 | Bookmarked websites are not displayed properly.   |
| SMA-4018 | Mobile Connect, MacOS, WireGuard, Connect Tunnel are not working for Mac pro devices.             |

| Issue ID | Issue Description  |
|----------|--|
| SMA-4035 | https://device IP/_api/_v1/doc.json shows an vulnerability.  |
| SMA-4039 | Issues with the user account name character limit.   |
| SMA-4047 | Duo authentication fails on the Netextender with the custom port.  |
| SMA-4096 | Login fails in the Contemporary Mode when using a client certificate containing the string "&".                    |
| SMA-4116 | Unable to update the EPC version.  |
| SMA-4117 | Option to disable case sensitive user names.   |
| SMA-4130 | Images are not loading over HTTPS bookmarks.   |
| SMA-4154 | The source IP address in the log shows an IP address unrelated to the session.                                     |
| SMA-4191 | Japanese UI issue: iPerf > iPref.  |
| SMA-4236 | Client certificate EPC check fails on browsers with macOS, but works with Mobile Connect.                          |
| SMA-4329 | GEO-IP shows countries are colored but doesn't work with Contemporary Mode.  |
| SMA-4352 | PHP Injection Attack -single user issue after post upgrade to 10.2.1.7.  |
| SMA-4482 | SMA 400 running build 10.2.1.7-50sv - False Positive case - Serial # 18B1694D3E10.                                 |
| SMA-4515 | Device gets rebooted with Virtual Office if it is configured with the custom port.                                 |
| SMA-4529 | Internal Server Error is displayed during accessing the GUI after starting 10.2.1.7-50sv.jp with factory defaults. |
| SMA-4615 | Unable to access website through portal after post upgrade to 10.2.1.8 due to prevented WAF.                       |

## Known Issues

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

| Issue ID | Issue Description   |
|----------|---|
| SMA-4491 | Safe mode option is removed for ESXi-VA from both UI as well as CLI in the upgrade build. |

## Additional Reference

This section provides a list of additional reference in this release.

| Issue ID | Issue Description   |
|----------|---|
| SMA-4349 | WAF report is not printed correctly from Japanese firmware. |
| SMA-4012 | High memory utilization.                                    |

# Version 10.2.1.8

May 2023

## 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.

## Compatibility and Installation Notes

- Most popular browsers are supported, but Google Chrome is preferred for the real-time graphics display on the Dashboard.
- A MySonicWall account is required.
- SMA 10.2.1.8 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 (Web Application Firewall) Threats, Authentications, VPN Accesses, Bookmark Access, Active devices and Users on a 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.

SonicWall SMA 10.2.1.8 is supported on the following SonicWall appliances:

- SMA 200/400
- SMA 210/410
- SMA 500v for ESXi
  - Supported for deployment on VMware ESXi 6.0 and higher
- SMA 500v for HyperV
  - Supported for deployment on Hyper-V server version 2016 and 2019
- SMA 500v for AWS
- SMA 500v for Azure
- SMA 500v for KVM

## What's New

This release provides security enhancements and fixes for previously reported issues.

## Resolved Issues

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

| Issue ID | Issue Description   |
|----------|---|
| SMA-4401 | Security hardening.   |
| SMA-4471 | If Geo-IP policy is configured to block all traffic to USA, EPC (OPSWAT library) updates are not working. |

## Version 10.2.1.7

March 2023

## 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.

# Compatibility and Installation Notes

- Most popular browsers are supported, but Google Chrome is preferred for the real-time graphics display on the Dashboard.
- A MySonicWall account is required.
- SMA 10.2.1.7 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 (Web Application Firewall) Threats, Authentications, VPN Accesses, Bookmark Access, Active devices and Users on a 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.

SonicWall SMA 10.2.1.7 is supported on the following SonicWall appliances:

- SMA 200/400
- SMA 210/410
- SMA 500v for ESXi
  - Supported for deployment on VMware ESXi 6.0 and higher
- SMA 500v for HyperV
  - Supported for deployment on Hyper-V server version 2016 and 2019
- SMA 500v for AWS
- SMA 500v for Azure
- SMA 500v for KVM

## What's New

### Security Enhancements

- **New firmware availability notification**  
Added the firmware upgrade notification on the System > licenses page of SMA100 to notify a newer firmware is available for upgrade. SonicWall recommends using the latest firmware version for highest level of security efficacy and optimal performance.  
For more information, refer to the section *New firmware availability notification* in the SMA100 10.2.1 Administration Guide.



- OpenSSL version upgrade

OpenSSL library is updated to the latest version 1.1.1t. This latest version fixes the OpenSSL vulnerability documented in CVE-2022-4304: A timing-based side channel exists in the OpenSSL RSA Decryption implementation.

For more information, refer to the section *OpenSSL version upgrade* in the SMA100 10.2.1 *Administration Guide*.

- Additional security enhancements
  - Enforce WAF to protect the SMA100 itself.
  - Warning on security configurations, includes enabling 2FA (Two-Factors Authentication), Password expiration, and WAF.
  - Disable user added custom scripts that run automatically after bootup while deploying SMA 500v in AWS or Azure environments.
 

① **NOTE:** Due to this security enforcement the user scripts deployed in SMA 500v will not function. Existing user scripts prior to upgrading version 10.2.1.7 will not function after this upgrade.
  - Additional security checks are done to verify the integrity of the firmware.
  - Restricted traffic - If a firmware integrity issue is detected, the SMA will restrict its own initiated outbound communications. This will not affect any user's VPN access to applications or any resource on the network.
  - In a corner case, the firmware integrity checks may result in a false positive situation and the SMA100 will restrict its own initiated outbound email/syslog communications. On further checks and analysis, the outbound email/syslog communication will be restored to the normal operation.

For more information, refer to the section *Additional security enhancements* in the SMA100 10.2.1 *Administration Guide*.

## Firmware Upgrade

Be sure to review the following Knowledge Base articles for information on the firmware upgrade on SMA100 Series.

- [How to Upgrade Firmware on SMA100 Series Appliances](#)
- [Additional SMA 100 Series 10.x and 9.x Firmware Updates Required](#)
- [Upgrade Path For SMA100 Series](#)
- [SMA 100 Series OpenSSL Library Update in 10.2.1.7](#)

## Resolved Issues

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

| Issue ID | Issue Description  |
|----------|--|
| SMA-3940 | Due to an internal SSH daemon configuration issue, PCI Scan test is showing this as an vulnerable. |
| SMA-4179 | CVE-2022-4304: A timing-based side channel exists in the Open SSL RSA Decryption implementation.   |

## Version 10.2.1.6

August 2022

## 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.

## Important

Be sure to review the following Knowledge Base article for information on the potential impact of the OpenSSL Infinite Loop on SonicWall products.

- [Security Notice: OpenSSL Infinite loop when parsing certificates CVE-2022-0778.](#)

## Compatibility and Installation Notes

- Most popular browsers are supported, but Google Chrome is preferred for the real-time graphics display on the Dashboard.
- A MySonicWall account is required.
- SMA 10.2.1.6 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 a 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.

SonicWall SMA 10.2.1.6 is supported on the following SonicWall appliances:

- SMA 200/400
- SMA 210/410
- SMA 500v for ESXi
  - Supported for deployment on VMware ESXi 6.0 and higher
- SMA 500v for HyperV
  - Supported for deployment on Hyper-V server version 2016 and 2019
- SMA 500v for AWS
- SMA 500v for Azure
- SMA 500v for KVM

| NetExtender Version   | Supported Firewall Firmware                      |
|---|--|
| NetExtender clients 10.2.331 for Windows10, 11 and 10.2.845 for Linux | GEN 6 – 6.4.5.9-93n GEN 7 – 7.0.1-5030 and above |

| NetExtender Version   | Supported SMA Firmware |
|---|------------------------|
| NetExtender clients 10.2.331 for Windows10, 11 and 10.2.845 for Linux | 10.2.1.6-37sv          |
|   | 10.2.1.5-34sv          |

## What's New

- Support for NetExtender 10.2.331 for Windows 10,11 and NetExtender 10.2.845 for Linux.

① **NOTE:** SonicWall recommends to use the latest NetExtender version with the latest version of SMA 100 Series firmware for optimal performance.

## Resolved Issues

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

| Issue ID | Issue Description   |
|----------|---|
| SMA-3437 | Geo-IP filter is not blocking the countries that were blocked.              |
| SMA-3518 | After rebooting, AWS deployment is unavailable and loses licenses.          |
| SMA-3521 | Netextender dialup is not displayed on Windows Login Screen.                |
| SMA-3551 | Wireguard tunnel does not disconnect even after reaching the session limit. |

| Issue ID | Issue Description   |
|----------|---|
| SMA-3607 | HTTP bookmark is not working  |
| SMA-3628 | The appliance becomes unresponsive randomly and the users get dropped.  |
| SMA-3637 | Upon upgrading from 10.2.0.9 to 10.2.1.4, adding Botnet, editing or deleting GeoIP policy displays error  |
| SMA-3652 | Manual upgrade of licensing text box is available in Hyper-v,Azure and AWS.   |
| SMA-3667 | An OTP error and alert email is sent to the administrator with no user information.   |
| SMA-3684 | Penetration test found low level risks while security settings were enabled on the SMA appliance.   |
| SMA-3688 | Appliance stops working after changing the portal settings.   |
| SMA-3692 | [Vulnerability] SonicWall SMA 100 Heap Buffer Overflow  |
| SMA-3701 | Not able to open and read files from the extracted .tar file.   |
| SMA-3714 | EPC check failed with NetExtender 10.2.324 windows version.   |
| SMA-3715 | EPC Windows 10 policy not working in SMA HyperV.  |
| SMA-3720 | Upon upgrading EPC, the NetExtender connection fails.   |
| SMA-3723 | SMA100 multiple out dated 3PL and version discloser vulnerability   |
| SMA-3727 | <b>Notify me when new firmware is available</b> option does not work.   |
| SMA-3728 | EPC check fails for Windows version   |
| SMA-3756 | Switching Windows users on one computer system creates a new profile with a blank user name, even if a profile is already created.  |
| SMA-3759 | SMA 10.2.1.5 version allows code injection into the header during requests.   |
| SMA-3766 | Warning message " <b>certificate chain too long. Do you want to proceed? Hostname for this server does not match hostname in certificate</b> " is displayed instead of indicating that the error is in the certificate. |
| SMA-3774 | Reports from the appliance is inaccurate.   |
| SMA-3775 | Wireguard NX clients do not obtain client routes from group level.  |
| SMA-3777 | Upon upgrading to Netextender 10.2.324, the Network Login feature on Windows is not available.  |
| SMA-3824 | EPC check fails on Windows 10 version.  |

## Additional Issues

SMA-3872

# Version 10.2.1.5

April 2022

## 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.

## Important

Be sure to review the following Knowledge Base article for information on the potential impact of the OpenSSL Infinite Loop on SonicWall products.

- [Security Notice: OpenSSL Infinite loop when parsing certificates CVE-2022-0778.](#)

## Compatibility and Installation Notes

- Most popular browsers are supported, but Google Chrome is preferred for the real-time graphics display on the Dashboard.
- A MySonicWall account is required.
- SMA 10.2.1.5 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 a 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.

SonicWall SMA 10.2.1.5 is supported on the following SonicWall appliances:

- SMA 200/400
- SMA 210/410
- SMA 500v for ESXi
  - Supported for deployment on VMware ESXi 6.0 and higher
- SMA 500v for HyperV
  - Supported for deployment on Hyper-V server version 2016 and 2019
- SMA 500v for AWS
- SMA 500v for Azure
- SMA 500v for KVM

| NetExtender Version   | Supported Firewall Firmware                          |
|---|--|
| NetExtender clients 10.2.324 for Windows10, 11 and 10.2.839 for Linux | GEN 6/6.5 – 6.4.5.9-93n GEN 7 – 7.0.1-5030 and above |

| NetExtender Version   | Supported SMA Firmware |
|---|------------------------|
| NetExtender clients 10.2.324 for Windows10, 11 and 10.2.839 for Linux | 10.2.1.5-34sv          |

## What's New

- Support for NetExtender 10.2.324 for Windows 10,11 and NetExtender 10.2.839 for Linux.

① **NOTE:** SonicWall recommends to use the latest NetExtender version with the latest version of SMA 100 Series firmware for optimal performance.

## Resolved Issues

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

| Issue ID | Issue Description  |
|----------|--|
| SMA-3141 | An ajax call gives unexpected 403 status for the http book mark is not working and getting sql injection attack. |
| SMA-3240 | Http resource stopped working after an upgrade to firmware 10.2.0.8 on both windows and macOS.                   |
| SMA-3390 | Geo-IP resolution is not working on the status pages as unknown.   |
| SMA-3392 | SMA assign opp-sited client IP address to a NetExtender randomly.  |
| SMA-3405 | Users are not able to access internal resources or internet intermittently with NetExtender.                     |

| Issue ID | Issue Description   |
|----------|---|
| SMA-3411 | User license cannot be released immediately, while disconnecting NetExtender connection.                        |
| SMA-3421 | Users get a message which says, failed to get WireGuard parameters.   |
| SMA-3432 | Werkzeug library and the python interpreter version disclosure vulnerability.                                   |
| SMA-3436 | EPC unable to detect windows defender on windows 7.   |
| SMA-3470 | Disable password reveal button on portal login in contemporary mode.  |
| SMA-3492 | Native bookmark authentication failure with password, works with pin for AzureAD joined computer.               |
| SMA-3501 | Internet traffic does not route via Internal proxy settings, it's ignored with the latest NetExtender 10.2.319. |
| SMA-3509 | SMA Connect Agent install fails, prompting to update though it's up to date.                                    |
| SMA-3522 | Post Auth Command Injection Vulnerability.  |
| SMA-3553 | Unable to access resources using WireGuard tunnel protocol.   |
| SMA-3559 | NetExtender with AOV does not re-connecting automatically when the system comes back from the hibernate/sleep.  |
| SMA-3568 | NetExtender windows client v10.2.322 buffer overflow.   |
| SMA-3573 | RDP bookmark automatically log in - disabled in contemporary mode.  |
| SMA-3582 | GUI is not properly localized in Japanese for 10.2.1.4.   |
| SMA-3599 | Idle timeout is not getting reset, when the WireGuard protocol is used.   |
| SMA-3606 | SMA100 OpenSSL CVE-2022-0778 DoS Vulnerability.   |
| SMA-3610 | NetExtender OpenSSL CVE-2022-0778 DoS Vulnerability.  |
| SMA-3640 | SMA/Overview/Reports is not getting downloaded with SMA500v.  |

## Known Issues

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

| Issue ID | Issue Description   |
|----------|---|
| SMA-3652 | Manual upgrade text box is available in Hyper-v, KVM, Azure, and AWS. |

# Version 10.2.1.4

January 2022

## 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.

## Compatibility and Installation Notes

- Most popular browsers are supported, but Google Chrome is preferred for the real-time graphics display on the Dashboard.
- A MySonicWall account is required.
- SMA 10.2.1.4 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 a 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.

SonicWall SMA 10.2.1.4 is supported on the following SonicWall appliances:



- SMA 200/400
- SMA 210/410
- SMA 500v for ESXi
  - Supported for deployment on VMware ESXi 6.0 and higher
- SMA 500v for HyperV
  - Supported for deployment on Hyper-V server version 2016 and 2019
- SMA 500v for AWS
- SMA 500v for Azure
- SMA 500v for KVM

| NetExtender Version   | Supported Firewall Firmware                |
|---|--|
| NetExtender clients 10.2.322 for Windows10, 11 and 10.2.835 for Linux | GEN 6/6.5 – 6.4.5.9-92n GEN 7 – 7.0.1-5030 |

| NetExtender Version   | Supported SMA Firmware |
|---|------------------------|
| NetExtender clients 10.2.322 for Windows10, 11 and 10.2.835 for Linux | 10.2.1.4-31sv          |

## What's New

- Support for NetExtender 10.2.322 for Windows 10,11 and NetExtender 10.2.835 for Linux.

**NOTE:** SonicWall recommends to use the latest NetExtender version with the latest version of SMA 100 Series firmware for optimal performance.

## Resolved Issues

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

| Issue ID | Issue Description  |
|----------|--|
| SMA-3361 | Unable to change password when user discretion is selected.  |
| SMA-3335 | NetExtender freezes while Initializing connection parameters status during the first time.                     |
| SMA-3227 | After upgrading to NetExtender 10.2.319, connection to Google related sites slows down or becomes unreachable. |
| SMA-3310 | DNS resolution does not work after using Net Extender Client version 10.2.319.                                 |
| SMA-3309 | No traffic passed on new NetExtender -10.2.319.  |
| SMA-3307 | Update needed for guest (Azure) agent due to failed backups.   |

| Issue ID | Issue Description   |
|----------|---|
| SMA-3291 | After upgrading to 10.2.1.2, post connection scripts are not working on Windows Operating System.<br><br>ⓘ   <b>NOTE:</b> This was a known issue until 10.2.1.3 versions, and is fixed in 10.2.1.4. |
| SMA-3284 | Get Domain Attempt Timeout with both Classic & Contemporary modes using UPN names.  |
| SMA-3282 | Duo is not working with Linux NX with WireGuard protocol.   |
| SMA-3262 | Time is displayed wrong on <b>SCHEDULED REBOOT</b> in <b>Internal Settings</b> page.  |
| SMA-3242 | Does not connect to VoIP communication after upgrading to 10.2.1.2 and 10.2.1.3   |
| SMA-3189 | Fails to launch Netextender from Virtual Office after upgrading to 10.2.1.1.  |
| SMA-3137 | Let's encrypt certificate is not auto-renewed.  |
| SMA-3126 | Cannot login to SAML and Dual user for Net Extender Client on Linux using CMD prompt.   |
| SMA-2893 | SND is detecting without entering OTP.  |

## Known Issues

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

| Issue ID | Issue Description   |
|----------|---|
| SMA-3411 | User license does not release immediately, while disconnecting NX connection. |

## Additional References

SMA-3428

## Version 10.2.1.3

December 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.

## Compatibility and Installation Notes

- Most popular browsers are supported, but Google Chrome is preferred for the real-time graphics display on the Dashboard.
- A MySonicWall account is required.
- SMA 10.2.1.3 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 a 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.

SonicWall SMA 10.2.1.3 is supported on the following SonicWall appliances:

- SMA 200/400
- SMA 210/410
- SMA 500v for ESXi
  - Supported for deployment on VMware ESXi 6.0 and higher
- SMA 500v for HyperV
  - Supported for deployment on Hyper-V server version 2016 and 2019
- SMA 500v for AWS
- SMA 500v for Azure
- SMA 500v for KVM

## What's New

- WireGuard Integration with SMA100 products. For information about this feature, see the *WireGuard Feature Guide* available on the Support portal at <https://www.sonicwall.com/support/technical-documentation/>.  
**NOTE:** WireGuard feature for SMA 10.2.1.3 is a Tech Preview build. The full support for WireGuard would be available from SMA 10.2.2 onwards.

## Resolved Issues

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

| Issue ID | Issue Description   |
|----------|---|
| SMA-3235 | Vulnerability: SMA100 multiple unauthenticated File Explorer Heap-based and Stack-based Buffer Overflows. |
| SMA-3233 | Vulnerability: SMA100 POST Auth RCE.  |
| SMA-3231 | Vulnerability: SMA100 getBookmarks Heap-based Buffer Overflow.  |
| SMA-3229 | The change password dialogue does not appear in contemporary mode, but it does in classic mode.           |
| SMA-3228 | DUO radius authentication broken for NetEx/MC users after 10.2.1.2 upgrade.                               |
| SMA-3217 | Vulnerability: Critical SMA100 unauthenticated stack-based buffer overflow.                               |
| SMA-3213 | Lets encrypt certificate is not working.  |
| SMA-3208 | Vulnerability: SMA100 Unauthenticated "Confused Deputy".  |
| SMA-3207 | Vulnerability: SMA100 Unauthenticated CPU exhaustion vulnerability.                                       |
| SMA-3206 | Vulnerability: SMA100 Unauthenticated file upload path traversal vulnerability                            |
| SMA-3204 | Vulnerability: SMA100 authenticated command injection vulnerability as Root.                              |
| SMA-3199 | Clicking on customer logo with user login redirecting to admin console.                                   |
| SMA-3138 | Error when connecting to SonicWall Firewall via SSHv2 bookmark with custom credentials.                   |
| SMA-3111 | Vulnerability: HTTP Host Head Value Reflections.  |
| SMA-1980 | Security Issue: SMA Agent/NetExtender do not assign an individual device ID.                              |

## Known Issues

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

| Issue ID | Issue Description   |
|----------|---|
| SMA-3282 | Duo is not working with Linux NX with wireguard protocol.   |
| SMA-3281 | The warning message "No country was selected" pops up when adding GeoIP policies on Geo IP & Botnet Filter > Policies page. |
| SMA-3262 | Time is wrong on SCHEDULED REBOOT on diag setting page.   |
| SMA-3249 | Linux NX error message is wrong for local password update with password complexity.   |

# Version 10.2.1.2

October 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.

## Compatibility and Installation Notes

- Most popular browsers are supported, but Google Chrome is preferred for the real-time graphics display on the Dashboard.
- A MySonicWall account is required.
- SMA 10.2.1.2 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 a 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.

SonicWall SMA 10.2.1.2 is supported on the following SonicWall appliances:

- SMA 200/400
- SMA 210/410
- SMA 500v for ESXi
  - Supported for deployment on VMware ESXi 6.0 and higher
- SMA 500v for HyperV
  - Supported for deployment on Hyper-V server version 2016 and 2019
- SMA 500v for AWS
- SMA 500v for Azure
- SMA 500v for KVM

## What's New

- WireGuard Integration with SMA100 products. For information about this feature, see the *WireGuard Feature Guide* available on the Support portal at <https://www.sonicwall.com/support/technical-documentation/>.

① **NOTE:** WireGuard feature for SMA 10.2.1.2 is a Tech Preview build. The full support for WireGuard would be available from SMA 10.2.2 onwards.

## Resolved Issues

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

| Issue ID | Issue Description  |
|----------|--|
| SMA-3121 | When users login through Virtual office, they get an error message only Contemporary UI after entering the SMS OTP.    |
| SMA-3112 | Get Domain Attempt Timeout when using contemporary mode after upgrading to 10.2.1.1.                                   |
| SMA-3057 | Button missing for install updates on Web Application Firewall > Status.   |
| SMA-3028 | Post upgrade to 10.2.1.1, NX/MC client version option/display is missing.  |
| SMA-3006 | AD users are getting an error stating "login failed - no suitable group found" when they login post upgrade 10.2.1.    |
| SMA-2978 | Self signed certificate error in Linux NX.   |
| SMA-2938 | When Device management is enabled, SMA connect agent crashes on Win7 only and the approval does not take place on SMA. |
| SMA-2935 | DUO radius authentication broken for NetEx/MC users after 10.2.1.x upgrade, Virtual office works.                      |
| SMA-2917 | GEO-IP Database not Syncing-errno 2.   |
| SMA-2904 | Need to add custom url for the custom logo.  |

# Known Issues

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

| Issue ID | Issue Description  |
|----------|--|
| SMA-3213 | Lets encrypt certificate is not working.   |
| SMA-3199 | Clicking on customer logo with user login redirecting to admin console.                  |
| SMA-3126 | Unable to login SAML user on Linux using Nx client launched with cmd.                    |
| SMA-2941 | Post upgrade to 10.2.1.0, EPC update fails when attribute is set to File System scanned. |

## Version 10.2.1.1

September 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.

## Compatibility and Installation Notes

- Most popular browsers are supported, but Google Chrome is preferred for the real-time graphics display on the Dashboard.
- A MySonicWall account is required.
- SMA 10.2.1.1 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 a 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.

SonicWall SMA 10.2.1.1 is supported on the following SonicWall appliances:

- SMA 200/400
- SMA 210/410
- SMA 500v for ESXi
  - Supported for deployment on VMware ESXi 6.0 and higher
- SMA 500v for HyperV
  - Supported for deployment on Hyper-V server version 2016 and 2019
- SMA 500v for AWS
- SMA 500v for Azure
- SMA 500v for KVM

## What's New

- Maintenance fixes provided for issues identified in Resolved Issues

## Resolved Issues

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

| Issue ID | Issue Description  |
|----------|--|
| SMA-1583 | Unable to obtain analytics data from the hypervisor (VMWare, HyperV, Azure, AWS, etc) that is running underneath each 500v instance. |
| SMA-2541 | EPC check is executed in the loop for aov session even though the EPC check is failed.   |
| SMA-2746 | Post upgrading to 10.2.1, CIFS File Share Bookmark does not work as intended.  |
| SMA-2836 | Get Domain Attempt Timeouts when trying to log in using contemporary mode.   |
| SMA-2846 | When a network change is detected, the NetExtender with Always On VPN enabled does not reconnect automatically.                      |
| SMA-2847 | Folder download fails when the name of the file in the folder contains un-ascii characters.  |
| SMA-2851 | Offloaded portal dropped due to HTTP DoS Settings.   |
| SMA-2854 | Unable to display the frame when "X-Frame-Options" is set to "sameorigin".   |
| SMA-2856 | Switching back to SMS OTP option in the latest UI always triggers OTP.   |
| SMA-2859 | When User discretion of OTP is enabled, the settings option in the user portal is not displayed.                                     |
| SMA-2861 | Unable to edit user created bookmark in contemporary mode.   |



| Issue ID | Issue Description   |
|----------|---|
| SMA-2866 | Resources are not available in the tab after successful authentication with Azure AD SSO.   |
| SMA-2867 | Post upgrading to 10.2.0.6, unable to load application offload portal.  |
| SMA-2892 | An error "Your password has expired" is displayed after upgrading to 10.2.1.0 with NX clients updated to 10.2.313 and unable to connect.  |
| SMA-2903 | SMA 500v on Azure displays high CPU and memory utilization.   |
| SMA-2905 | SAML authentication using OKTA fails when failover to backup SMA.   |
| SMA-2910 | Post upgrading to 10.2.1, the memory usage on the appliance remains at 92% constantly.  |
| SMA-2912 | Post upgrading SMA 500v ESXi with firmware to 10.2.1.0, appliance crashes.  |
| SMA-2913 | Post upgrading to 10.2.1.0, NetExtender client address range appears exhausted.   |
| SMA-2923 | SMTP password fails after restarting the appliance.   |
| SMA-2939 | When connecting to NetExtender, traffic is displayed as Appliance IP address instead of displaying IP address of the Net extender client. |
| SMA-2940 | Prompt to change password does not show up when two factor authentication (2FA) is enabled.   |
| SMA-2947 | Private IPs are displayed in public facing portal.  |
| SMA-2949 | Update Signature failed frequently with error message "Update Signature failed, error code 500".  |
| SMA-2950 | SMA Connect does not launch NetExtender with SAML Authentication.   |
| SMA-2951 | Backup system does not switch to primary role and unable to take ownership of the IP.   |
| SMA-2954 | Pcap and netstat results display communication as SMA IP instead of NX IP.  |
| SMA-2957 | Authenticated SMA100 Arbitrary Command Injection Vulnerability.   |
| SMA-2959 | Unauthenticated SMA100 Arbitrary File Delete Vulnerability.   |
| 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

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

| Issue ID | Issue Description  |
|----------|--|
| SMA-2496 | Login uniqueness with 'Confirm logout of existing session' does not work as intended.  |
| SMA-2904 | Unable to customize url for the custom logo in the SMA portal.   |
| SMA-2941 | EPC update fails when the attribute option is set to "File System Scanned" after upgrading the appliance to 10.2.10.   |
| SMA-3001 | Unable to log in using certificate domain after upgrading appliance from 9.0.0.10-28sv to 10.2.1.1-19sv.<br><br><b>Workaround:</b> <ul style="list-style-type: none"><li>• Disable the TLS 1.3 option</li><li>• Edit the domain and check the trusted CA certificate</li></ul> |

## 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/>.

## Version 10.2.1

June 2021

## Compatibility and Installation Notes

- Most popular browsers are supported, but Google Chrome is preferred for the real-time graphics display on the Dashboard.
- A MySonicWall account is required.

- SMA 10.2.1 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 a 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.

SonicWall SMA 10.2.1 is supported on the following SonicWall appliances:

- SMA 200/400
- SMA 210/410
- SMA 500v for ESXi
  - Supported for deployment on VMware ESXi 6.0 and higher
- SMA 500v for HyperV
  - Supported for deployment on Hyper-V server version 2016 and 2019
- SMA 500v for AWS
- SMA 500v for Azure
- SMA 500v for KVM

## What's New

These features are introduced in Secure Mobile Access 10.2.1:

- **System Report**  
You are now able to generate functionality reports on System Information, System Status, Threats, Active Users, and Activities using all supported basic and advanced combinations. Reports can be scheduled on a daily, weekly, or monthly basis.
- **HTML5 SSH Key File Authentication Support**  
User names and passwords were previously the only authentication methods supported by HTML SSH. More and more SSH servers are now being used as key file authentication sites, especially within the cloud environment. SonicWall has added support for that Key File authentication method.
  - HTML5 SSH bookmarks support identity file authentication
  - HTML5 SSH features can save the identity file and user information in a browser's local storage
  - HTML5 SSH features can use the saved information to log in to an SSH server automatically

- **Migration Tool**

The ability to migrate configurations across SMA platforms has been developed allowing you to keep your key network configuration by mapping the source device interfaces to the destination device interfaces. This new tool disables the device/network-related features such as High Availability, and converts only the device-related feature configurations, such as *Policies* and so on. For any configuration migration scenarios, review the [SMA100: Configuration Migration Tool](#) Knowledge base article or reach out to Support for assistance.

- **SMA 500v on KVM**

SMA 500v for KVM allows you to run an SMA 500v appliance in a KVM environment while supporting most of the features available on physical SMA appliances.

- **Allowed Host Option in the Content Security Policy Header**

You can add an Allowed Host option in the Content Security Policy Header that supports third-party resources. You must access your appliance's internal settings to input the third-party URLs in the **Content Security Policy Settings**.

- **DUO Security Authentication Support for NetExtender and Mobile Connect Clients**

SMA supports **DUO Security Authentication** during user login. DUO Security Authentication login is supported for different clients such as web browsers and Mobile Connect clients in both Contemporary and Classic Modes.

- **Secure Hosts for Secure Network Detection**

When **Secure Network Detection** is enabled, using a new **Secure Hosts** setting, SMA can check whether or not an SSL certificate is trusted, thereby allowing you to add secure hosts for "always on" VPN connections. If a secure network is not detected, the client will connect to the VPN.

- **iPerf Integration**

iPerf can be integrated into SMA and used to measure and tune network performance. It produces standardized performance measurements on any network and can function as both client and server. It can also create data streams that measure the throughput between the end client machine and the SMA appliance in one or both directions as a backend resource host. iPerf output includes time-stamped reports of the amount of data transferred and the throughput measured.

You can learn more about these new features in the **New Features** section of the *Secure Mobile Access 10.2 Administration Guide*.

## Resolved Issues

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

| Issue ID | Issue Description  |
|----------|--|
| SMA-2587 | All logs are deleted on appliance reboot.                                      |
| SMA-2581 | Migration tool should be validated with a message from lower to higher models. |

| Issue ID | Issue Description  |
|----------|--|
| SMA-2566 | The appliance is consuming licenses in particular cases.   |
| SMA-2561 | Settings imported from an SRA 4600 do not allow login to SMA.  |
| SMA-2539 | The AlwaysOnVPN feature does not activate as expected for specific domains.                              |
| SMA-2393 | Daily log emails are not being sent as expected.   |
| SMA-2317 | The <b>System &gt; Settings</b> page needed for upgrades is blank and not functioning as expected.       |
| SMA-2268 | An End Point Control (EPC) inspection returned invalid equipment IDs including incorrect serial numbers. |
| SMA-1847 | SecureDNS causes Secure Network Detection (SND) to fail.   |
| SMA-1392 | DUO authentication with NetExtender on Linux client does not function as expected.                       |
| SMA-1187 | The "Allow password changes" feature is not functioning as expected.                                     |

## Known Issues

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

| Issue ID | Issue Description   |
|----------|---|
| SMA-2720 | In the new user interface, switching between authentication methods such as the SMS OTP (one time password) option and Use Mobile App or Use Email. Switching back to the SMS OTP option always triggers OTP. |
| SMA-2563 | Folder download does not function correctly when file names in the folder include non-ASCII characters.   |
| SMA-2496 | Login uniqueness with 'Confirm logout of existing session' does not function as expected.   |
| SMA-1962 | Unable to open Excel or Word files using SharePoint.  |

# 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.

The [Support Portal](#) enables you to:

- View [Knowledge Base](#) articles and [Technical Documentation](#)
- View and participate in the [Community Forum](#) discussions
- View [Video Tutorials](#)
- Access [MySonicWall](#)
- Learn about [SonicWall Professional Services](#)
- Review [SonicWall Support services and warranty information](#)
- Register at [SonicWall University](#) for training and certification

# About This Document

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **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 for the SMA 100 Series

Updated - November 2024

Software Version - 10.2.1.14

232-005681-00 Rev S

Copyright © 2024 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>.