SonicWall Secure Mobile Access 1000 Series 12.4 Release Notes

These release notes provide information about the SonicWall Secure Mobile Access (SMA) 1000 series version 12.4 release.

Versions:

12.4.3

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.

Central Management Server (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:

- 12.4.1 + latest hotfixes -> 12.4.3
- 12.4.2 + latest hotfixes -> 12.4.3
- 12.1.0 + latest hotfixes -> 12.4.3

ⓘ | **IMPORTANT:**

- It is recommended to upgrade to 12.4.3 from 12.4.2 with latest hotfixes.

For more information on supported platforms, clients, servers, IT infrastructure, and online services, refer to *SMA 1000 12.4 Administration Guide*.

Be sure to review the following Knowledge Base article for information on the SMA 1000 Series, and CMS.

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

ⓘ | **NOTE:** Any 12.4.x client can connect to version 12.4.3 as we support backward or forward compatibility. However, an older client may not support newer features like exclusion, and customers must upgrade to version 12.4.3 of the client to access them.

What's New

Secure Mobile Access (SMA) 12.4.3 includes these new features:

- **Access Request Logging**
  Admin can limit the types of access requests that are saved with User Sessions.
- **Always On VPN Enhancements**
  Following new options are available to admin under Always On VPN section:
  - **Allow user to disconnect**- Controls whether a user is allowed to disconnect from the VPN.
  - **Restrict network access when VPN is not Connected**- Allows admin to control whether user is allowed to access internet when the VPN is disconnected.

- **Cached Credentials Enhancements**

  Two new options are available under Cache Credential section:

  - **Username only**- Only username will be cached.
  - **Disabled**- Credential caching will be disabled.

- **Cisco Duo Security Multi-factor Authentication Server**

  In addition to using SAML and RADIUS protocols to integrate with Cisco Duo Security Multi-factor server for user authentication, administrators can now utilize Auth API integration to provide Multi-factor authentication using Cisco Duo Security Multi-factor server. A new Authentication server called Cisco Duo Security Multi-factor Authentication server is now available for that.

  Unlike RADIUS authentication, this authentication server allows users to choose their preferred second-factor authentication method to complete authentication process.

- **CMS Alerts Logging**

  Information about all alerts such as high CPU usage, disk usage, and so on is now sent to Syslog when configured.

- **Copying Resources Groups**

  Rather than creating a new resource group from scratch, you can save time by making a copy of an existing group and changing some parameters to fit the new group.

- **Device VPN Enhancements**

  The **Device VPN Communities** (under **Services > Network Tunnel Service**) has two

  additional check boxes that allows users to bypass entering VPN credentials for User VPN, when the client machine is powered on or restarts in secure network. Also, if Device VPN is enabled, **Allow user to disconnect**

  option takes precedence over **Always On VPN** configuration. Below are the two Device VPN options:

  - **Allow user to disconnect**
  - **Do not connect in secure network**

- **Dynamic Form SSO Improvements**

  New login experience is provided where admin can choose SSO or login behavior based on the resource application.

  - New option **Login experience** is available to configure how the user will be automatically logged in.
  - New login detection method **Status code** is added.

- **Exclusions**

  - Allows tunnel configurations with redirect-all and wildcard domain exclusions.
  - Connect Tunnel clients are capable of excluding the traffic on the fly.

- **Global Overrides in AMC**

  The **Enable accounting records** value for realms can now be overridden when set to different options accordingly under **Global Overrides**.

- **Global Policy Settings in CMS**

  The Global Policy settings and enabled options are introduced in the Resource Groups and Exclusions.

- **Managing Administrator Account Settings**

  The following options are available for administrators under the **System Configuration > General Settings > Administrators > Authentication > Advance** section.

  - **Password Policy** settings help to set strong password complexity settings for the primary administrator account.
  - **Account lockout** settings for administrators when there are multiple failed login attempts.
  - **Session timeout** settings for administrators to configure the session inactivity timeout.
  - **Concurrent Session** settings for administrators to configure the concurrent session to limit the number of sessions and admins that can be logged in to AMC.

- **RSA Authentication Manager as Authentication server**

  RSA Authentication Manager can now be integrated using superior SecurID Authentication API. This is an improvement over the older SDK integration, now termed Legacy, which was cumbersome and error-prone. Additionally, this new authentication server simplifies deployment by eliminating the DNS requirements that were necessary with SDK integration.

- **Shell Access**

  The ability to disable shell access on the appliance is now available. This feature can be valuable in secure environments where shell access via serial console and SSH needs to be restricted or removed.

- **WorkPlace Enhancements**

  Following file explorer improvements are added:

  - A search option allowing users to locate files or folders by name.
  - The current user name is shown on the hamburger menu.
  - If the browser is closed while an upload is in progress, a confirmation message is displayed.
  - The reload icon has been relocated to the address bar.
  - Column sizes can be resized.

What's Deprecated

- Legacy SSO is deprecated and enhanced with Dynamic Single Sign On.
- The integration method for RSA Authentication Manager using CSDK has been deprecated, now referred to as RSA Authentication Manager Legacy. Additionally, the RSA Authentication Manager authentication server now supports integration using the superior SecureID Authentication API.

Discontinued Features

- Discontinued features in SMA 1000 12.4.1 onwards are:
  - vWorkspace
  - Fallback Servers
  - Application Control
- Discontinued features in SMA 1000 12.4.3 onwards are:
  - RSA ClearTrust Authentication Server
  - Modern Workplace
  - Cache Cleaner

NOTE: When upgrading the SMA version with discontinued features, it is mandatory to remove the existing configuration and then proceed with the upgrade.

Resolved Issues

Issue ID	Issue Description
SMA1000-7082	The SSL gateway dropped a large number of users, causing the policy server to crash.
SMA1000-7041	The appliance dropped all users due to a particular functionality issue with Device VPN access.
SMA1000-7038	RSA authentication failed due to incompatibility between the outdated RSA-AM version 8.2. and the newer RSA-SDK version 8.6.
SMA1000-7037	SND fails to detect when one of the hosts becomes unreachable.
SMA1000-6980	The appliance dropped all users in a specific case involving Device VPN access.
SMA1000-6964	The appliance crashes in a rare condition scenario when operating over IPv6.
SMA1000-6954	Eliminate less secure ciphers utilized in SSH connections.
SMA1000-6949	AAR Push logs are not functioning with SMA 1000 version 12.4.2, even with the latest hotfix applied.
SMA1000-6916	The appliance dropped users and restarted due to a particular functionality issue with DNS.
SMA1000-6869	Unable to add large number of address pools in the CMS.
SMA1000-6860	Let's encrypt renewal is creating a Certificate Signing Request (CSR) instead of renewing.
SMA1000-6837	The CMS reporting is not displaying certain appliances due to a database issue.
SMA1000-6766	The appliance database failed, and the storage failed to recover.
SMA1000-6667	SSL Tunnel with high-volume UDP application and slow tunnel performance is leading to users disconnections.

Issue ID	Issue Description
SMA1000-6666	Opening multiple RDP session simultaneously results in internal errors.
SMA1000-6663	Adding an exclusions under community breaks the URL shortcuts on the Workplace home page.
SMA1000-6662	Attributes associated with the Group Affinity based authentication server are not linked to the realm.
SMA1000-6653	The Workplace page displays an error when the default realm is disabled on the SMA managed appliance nodes.
SMA1000-6652	EPC Zone classification with Intune fails to calssify zones.
SMA1000-6651	The appliance experiences random reboots daily due to a race condition.
SMA1000-6650	Certificate authentication fails when connected to Connect Tunnel on MacOS platform.
SMA1000-6649	When VPN is not connected, the internet access is also restricted.
SMA1000-6595	Remove Cache Cleaner feature.
SMA1000-6392	The setting **Limit session length to credential lifetime** under **Configure Realm > Configure Community >Session Termination** is not working as expected.
SMA1000-6364	The appliance names in CMS user sessions display extra names.
SMA1000-6362	Uploads of files using file shares are limited to the size of the root partition.
SMA1000-6349	The Upgrade from SMA 1000 version 12.4.1 to SMA 1000 version 12.4.2 failing due to a corner case issue in the database restore process.
SMA1000-6319	The custom MTU value configured for interface via CLI reverts to default value after reboot.
SMA1000-6221	The upgrade failure is attributed to an encoding issue.
SMA1000-6189	The Spike license is automatically activated following the upgrade.
SMA1000-6185	Let's encrypt certificate chain builds with an expired R3 certificate.
SMA1000-6164	The Checkhosts tool fails when encountering DNS failures.
SMA1000-6132	Snapshot takes a longer duration when executed from AMC or SSH.
SMA1000-5959	German localization files are causing the upgrade fail.
SMA1000-5952	Log all alert events in the `management.log` file and send them to all configured syslog hosts.
SMA1000-5943	CMS and managed appliances display a blank screen when navigating to the TOTP users page.
SMA1000-5942	CMS is unable to map address pools for UK SMA appliances, but can map others.
SMA1000-5939	CMS displays a blank screen when navigating to configure community and is unable to create communities.
SMA1000-5927	Option to disable sending the "`X-Forwarded-For:`" header to backend servers.
SMA1000-5736	Unable to deselect or delete the old expired workplace certificate.
SMA1000-5681	Unable to connect to RDP resource using a third-party HTML5 based application when configured to access via reverse proxy.

Issue ID	Issue Description
SMA1000-5629	Wildcard Exclusions does not work as expected with Redirect All Mode.
SMA1000-5580	An admin with only monitoring permission is unable to reset and unlock the TOTP data of a user in CMS and managed appliance.
SMA1000-5257	Support Network Logon on x86 and ARM64 devices.
SMA1000-3305	Support for more secure Let's Encrypt GTO certificates should be added.

Known Issues

No additional known issues

Additional References

SMA1000-6761, SMA1000-5786, SMA1000-5697, SMA1000-5695, SMA1000-5693, SMA1000-5692, SMA1000-5691, SMA1000-5690, SMA1000-5689, SMA1000-5688, SMA1000-5682, SMA1000-5679, SMA1000-5678, SMA1000-5675, SMA1000-5669, SMA1000-5661, SMA1000-5656, SMA1000-5651, SMA1000-5650, SMA1000-5648, SMA1000-5647, and SMA1000-5645.

12.4.2

July 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.

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 and above + latest hotfixes -> 12.4.2
- 12.1 + latest hotfixes -> 12.4.2

IMPORTANT: To upgrade from Secure Mobile Access 12.3, you must upgrade to version 12.4.0 first, then upgrade to 12.4.2.

IMPORTANT: You can directly upgrade to 12.4.2 from SMA 12.1 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) 12.4.2 includes these new features:

- **Support multiple policies with CMS and shared licensing**
  - Support CMS-based configuration of appliance-specific authentication servers.
  - Allow realms and access rules to be mapped to individual appliances.
  - Support more than one GTO service, and assign GTO services to one or more appliances.
  - Map GTO resources (WorkPlace sites, host-mapped resources) to one or more GTO services.
- **API Keys for Management API Access**
  You can use API keys that allow use of the Management API without embedding user credentials in a script. API keys can be used to provide access to scripts when two-factor authentication is required for AMC access.
- **Improved troubleshooting with logs in a CMS environment**
- **Connect Tunnel Enhancements**
  - Connect Tunnel for MacOS does not require Java Runtime.
  - Connect Tuneel for Windows supports Network Logon.

- **Web Application Profile option to disable URL translations**
    - Under Web Application Profile, you can disable URL translation for URL resources with split Domain Name System (DNS) approach. When configuring a URL resource, if both the resource's Fully Qualified Doamain Name (FQDN) and the appliance's FQDN for that resource are the same, then there is no need for translation. In such cases, you can disable the URL translation to improve the system performance.
    - Under **Content translation**, select the **Enable Content translation** checkbox and other Web proxy service to translate.
- **Allow Outlook Web App, Active Sync and Outlook Anywhere on same appliance-FQDN**
- **Using Global Overrides**
  Provide the ability to easily override community-specific settings to make it easier to troubleshoot issues. Global overrides are recommended to be used only during troubleshooting. Use it to override the following community settings:
    - ESP Mode
    - Software Updates
    - Limit session length to credential lifetime
- **Simplified SMS Gateway Service configuration**
- **API JSON Schema should use a public standard**
- **Host Connectivity Testing**
  You can test all the resource hosts or URLs for connectivity. This feature helps to secure the system and verifies certificates of internal systems.
- **Import mapped accounts from CSV file**
    - You can import the mapped accounts for users and groups via CSV file at once.
- **SAML Enhancements**
    - AMC displays the SAML IdP Endpoint URLs in the IdP Configuration page and also provides an option to copy those URLs.
    - Import of SAML metadata file on SAML Service Provider Resource configuration page.
    - View and Import buttons for certificates on SAML Service Provider Resource configuration page.
- **Configuring ICMP**
  From 12.4.2 onwards in AMC/CMC you can enable ICMP for internal only or external only or both interfaces.
- **Managing Snapshots**
    - You can select one or more saved snapshots and delete or download them.
- **Support DHCP for internal and external interfaces**

- **Managing saved captures**
    - You can select one or more saved captures and delete or download them.
        - When multiple captures are selected, the **Delete** option is enabled.
        - When a single capture is selected, both the **Download** and the **Delete** options are enabled.

- **Deleting saved configuration data stored on the appliance**
    - The options to **Delete**, **Restore** and **Export** saved configuration is enabled when a single configuration is selected.
    - When multiple configurations are selected, **Restore** and **Export** is graded out and **Delete** option is enabled.
- **Improved Network Traffic Filenames**
    - You can edit the filename with a user friendly name and save. This enables the support team users to easily understand about the capture that you share.
- **External URLs as remediate links on quarantine zone**
    - External URLs as remediate links on quarantine zone, when creating remediate links on quarantine zone, you can configure if the URL is hosted on external network.
- **Support for Windows 11 and MacOS Monterey**
- **Secure Endpoint Manager(SEM)**

  SEM is the client application responsible for evaluating EPC, launching agents and bookmarks. SEM registers a custom URL sceheme that gets invoked from browser for the specific tasks. SEM has two modules namely, Web Agent and Connect Agent.
    - Web Agent : This unified client is responsible for handling the following:
        - End point control: Perform the end point control checks.
        - Install and update Connect Tunnel.
        - Agent activation: Auto activate OnDemand Proxy and OnDemand Tunnel.
    - Connect Agent: This unified client is responsible for handling bookmarks from WorkPlace. This client also provides backward compatibility if someone accesses WorkPlace on prior 12.4 versions.

- **Splunk Integration**
  The SonicWallSMA1000 Splunk Add-on is integrated in the Splunk Server using the Splunk Common Information Model (CIM).
  The SonicWallSMA1000 Splunk Add-on uses the following collection methods to collect the logs:
    - Logs collected via syslog are:
        - Authentication
        - Change
        - Network sessions
        - Network Traffic
    - Logs collected via API polling is:
        - Performance
- **Device VPN endpoint enrollment**
    - Deploy client certificates on end devices for Device Tunnel authentication.
    - Get details of the list of enrolled device certificates such as device certificate subject DN, Device ID, Expiration date, and so on.
    - Revoke or delete enrolled device certificates.
- **Microsoft Intune**
  The SMA and Microsoft Intune integration is supported for MacOS based managed devices.
- **Dynamic SSO Profile for Microsoft RDWeb and Citrix XenApp**
  You can quickly configure Single Sign-On for Microsoft RDWeb and Citrix XenApp service by selecting **Microsoft Remote Desktop Web Client** and **Citrix XenApp** option respectively while creating a Dynamic Single Sign-On profile.
- **Web Security Headers**
  You have an option to enable the web proxy security headers that sets the HTTP Respons headers and provides protection from attacks. As an admin, you can enable security headers on workplace login pages for added security.

What's Deprecated

- Cache Cleaner functionality is no longer supported.
- Fallback server is no longer supported.
- Application Control, Application Zones, and Application Rules are no longer supported.
- Change default policy in setup wizard from "allow" to "deny": The **allow authenticated users access to all defined resources** option is removed and no longer supported.

Resolved Issues

Issue ID	Issue Description
SMA1000-2326	Connect Tunnel is supported for ARM Processor Based Architecture
SMA1000-2905	Managed Appliance supported with Single home to participate in GTO from 12.4.0
SMA1000-4225	Do not allow SSH to be enabled with no allowed hosts
SMA1000-4229	Able to select signatures updated and file system scanned on device profile, even if the settings were disabled.
SMA1000-4329	Linux vulnerability CVE-2021-33909 Sequoia
SMA1000-4347	CMS appliance list should include pool IP
SMA1000-4348	Add a duration to default alerts
SMA1000-4363	IP range is converted to a subnet and the last available address is blocked by treating it as a broadcast IP, resulting in a High Metric Value of 271
SMA1000-4391	AMC must normalize SND fingerprint in order for system to use it
SMA1000-4415	Add DNS authoritative server status to CMS dashboard
SMA1000-4430	Local user Group membership not working in ACL
SMA1000-4482	Post firmware upgrade the OD Portmap Application breaks and fails to work.
SMA1000-4500	The AD tree test connection and user & group browsing is not working when only AES ciphers is enabled in Backend Active Directory.
SMA1000-4501	Post firmware upgrade to 12.4.1 SMA6200 appliances restarts automatically with VMcores.
SMA1000-4503	Post firmware upgrade to 12.4.1, the AMC console does not display the username and password to login, however it is able to login into SMA console via CMS.
SMA1000-4522	Services should prefer time-valid certificates.
SMA1000-4577	Security headers are not sent and not observed in robots.txt
SMA1000-4580	WINS are enabled on Connect Tunnel even though not configured in AMC
SMA1000-4601	Misspelling in SMA 1000 Stop Network Capture dialog
SMA1000-4605	Post hotfix upgrade to 12.4.1 with security headers enabled, PKI authentication does not work.
SMA1000-4607	Cli commands to enable **connect automatically at windows logon** option.
SMA1000-4634	CT users fail SAML auth using OneLogin
SMA1000-4639	SEM crashes when accessing Citrix applications
SMA1000-4684	Initializing JitterEntropy failed (9): CATASTROPHIC installing 12.4.1 OVA on ESXi 7.0.2
SMA1000-4760	Provide clues in AMC SSL certificate selection UI
SMA1000-4799	Unregistered device log does not display any data,even EPC check for equipment ID failed.

Issue ID	Issue Description
SMA1000-4814	Worksplace takes abnormally longer time to load
SMA1000-4824	AMC should not redirect to IP address HTTP 1.0 request w/o host header
SMA1000-4845	Include the ForceAuthn = "true" parameter in the SAML Auth request made by the SMA
SMA1000-4876	Even when the SMA does not have any PKI auth server displays *OCSP:: Could not verify response* error message.
SMA1000-4910	`Favicon.ico` replace does not work with workplace style and displays an error.
SMA1000-4919	EPC Cookie Does Not Contain The "HTTPOnly" Attribute
SMA1000-4941	Application EPC check fails when process has custom extension
SMA1000-4967	Post upgrade to new version **Connect automatically at Windows logon** option is enabled.
SMA1000-5003	HTML5 RDP does not get disconnected even after the session is terminated with workplace
SMA1000-5079	CVE-2022-0847
SMA1000-5080	PS core found, trace to captcha lib(libgd)
SMA1000-5086	CT on MacOS displays an error message that cannot reach the Hostname/IP
SMA1000-5100	CVE-2022-0778 - OpenSSL BN_mod_sqrt DOS
SMA1000-5148	Allow control of whether an imported config overwrites existing CA certificates (RFE 4701)
SMA1000-5173	12.4.2:Tunnel connections are suddenly dropping and reconnecting
SMA1000-5174	12.4.2:Enable 10Gb connectivity over Internal and External Interface
SMA1000-5197	Certificate chain error occurs when connecting with Connect Tunnel in 12.4.1
SMA1000-5211	Equipment Identifier field is needed for user session no option to relate with user logged in from AMC
SMA1000-5267	Profile creation may take long without any progress indication to user
SMA1000-5272	Post upgrade from 12.3 to 12.4.1-02629 RDP function is not working.
SMA1000-5277	Access Rule when expanded gives extended error and no information is displayed.
SMA1000-5297	Windows CT - installer should not install credential provider by default, this is an advanced option
SMA1000-5305	12.4.2 Mac CT crashes during SND upon connecting to 12.1
SMA1000-5306	Mac CT thread/timing issue using 2FA prompts
SMA1000-5307	Mac CT - hangs when adding new configuration, or takes a long time
SMA1000-5319	On CMS GTO DNS delegations page, show all GTO services
SMA1000-5369	DynamicGroup AD group edit in Access control displays *up page not found* message
SMA1000-5382	Connect Tunnel crashes and fails to launch when user.config `Settings file` is corrupted

Issue ID	Issue Description
SMA1000-5404	Post upgrade from version-12.4.0-03189 to 12.4.1-02629 CMS fails to boot, it is in loop
SMA1000-5470	Redirect All mode with exclusions is not working as expected in MAC

Known Issues

Issue ID	Issue Description
SMA1000-5257	Support Network Logon on x86 and arm64 devices
SMA1000-5433	CMS Reports page displays incorrect user counts
SMA1000-5513	Test connection under Intune MDM settings works only for in-built admin account

Additional References

SMA1000-5034, SMA1000-4987, SMA1000-4903

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 Connect Tunnel 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.

Issue ID	Issue Description
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.
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 at https://sonicwall.com/pes.
- 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 for Release Notes
Updated - February 2024
Software Version - 12.4.3
232-005695-00 Rev C