

SonicWall NetExtender Windows 10.3.2 Release Notes

These release notes provide information about the SonicWall NetExtender Windows 10.3.2 release.

Versions:

- [Version 10.3.2](#)
- [Version 10.3.1](#)
- [Version 10.3.0](#)

Version 10.3.2

April 2025

About NetExtender Windows

NetExtender Windows is a transparent software application for Windows users that enables remote users to securely connect to the remote network accessed through a SonicWall appliance. With NetExtender Windows, remote users can securely run any application on the remote network. Users can upload and download files, mount network drives, and access resources as if they were on the local network.

This release supports all the features and contains all the issues resolved in previous NetExtender Windows releases. For more information, see the last release notes on MySonicWall at <https://mysonicwall.com>.

Compatibility and Installation Notes

- Most popular browsers are supported, but prefers Google Chrome for the real-time graphics display on the Dashboard.
- A [MySonicWall](#) account is required.

Supported Platforms

NetExtender Windows Client Versions

The following is a list of NetExtender Windows client versions that are available in this release.

Version	Description
10.3.2	NetExtender for Windows 10 32-bit MSI/EXE
10.3.2	NetExtender for Windows 10/11 64-bit MSI/EXE
10.3.2	NetExtender for Windows 11/10 ARM64-bit

Supported Client Platforms

NetExtender Windows 10.3.2 supports computers running the following versions:

- Windows 10/11.

Supported SonicWall Appliances

SonicWall appliances receive NetExtender Windows connections from remote clients. The following appliances are supported:

- SonicWall firewalls running SonicOS 8 and higher, including the following platforms:
 - TZ80 and NSa2800 running SonicOS 8
- SonicWall firewalls running SonicOS 7 and higher, including the following platforms:
 - TZ270, TZ270W, TZ370, TZ370W, TZ470, and TZ470W running SonicOS 7
 - TZ570, TZ570W, TZ570P, and TZ670 running SonicOS 7
 - NSa2700, NSa3700, NSa4700, NSa5700, and NSa6700 running SonicOS 7
 - NSv270, NSv470, and NSv870 running SonicOS 7
 - NSsp10700, NSsp11700, NSsp13700, and NSsp15700 running SonicOS 7
- SonicWall firewalls running SonicOS 6.5.4.7 and higher, including the TZ, NSa, SOHO, and SuperMassive (SM) series platforms:
 - TZ300, TZ300W, TZ300P, TZ350, TZ350W, TZ400, TZ400W, TZ500, TZ500W, TZ600, TZ600P
 - NSa2600, NSa3600, NSa4600, NSa5600, and NSa6600
 - NSa2650, NSa3650, NSa4650, NSa5650, NSa6650, NSa9250, NSa9450, and NSa9650
 - SOHOW, SOHO250, and SOHO250W
 - SM9200, SM9250, SM9400, SM9450, SM9600, and SM9650
- SonicWall virtual firewalls running all releases of SonicOS 6.5.4.4v, including the following NSv series platforms:
 - NSv 10, 25, 50, 100, 200, 300, 400, 800, 1600
- SonicWall firewall running all releases of SonicOS 5.9.2.8-11o and 5.9.2.14-13o, including the following platform:
 - SOHO

- Secure Mobile Access (SMA) 100 Series appliances running SMA 10.2.1 or higher:
 - SMA200, SMA210, SMA400, SMA410
 - SMA500v for ESXi (on ESXi 6.0 and higher)
 - SMA500v for Hyper-V (on Hyper-V 2019 and 2022)
 - SMA500v for AWS
 - SMA500v for Azure
 - SMA500v for KVM

Supported Firewall Firmware Version

- GEN 5 (SOHO only) - 5.9.2.8-11o / 5.9.2.14-13o
- GEN 6/6.5 - 6.5.4.13-105n / 6.5.4.15-117n
- GEN 7 - 7.0.1-5161 / 7.1.1-7058 / 7.1.2-7019 / 7.1.3-7015
- GEN 8 - 8.0.0-8035 / 8.0.1-8017

① | **NOTE:** SonicWall recommends using the latest GEN 7 and GEN 8 firmware for optimal performance.

Supported Firmware SMA Versions

- SMA 100 10.2.1.13
- SMA 100 10.2.1.14

① | **NOTE:** SonicWall recommends using the latest NetExtender Windows with the latest SMA 100 Series firmware for optimal performance.

What's New

This release provides the latest NetExtender Windows version with the latest version of the SMA 100 Series and fixes for previously reported issues.

Resolved Issues

Issue ID	Issue Description
NX-18	Improper privilege management vulnerability.
NX-21	NetExtender - 10.3.0/10.3.1 got an error as the SSLVPN tunnel failed to set DNS
NX-23	Failed to get the AD Login Script.
NX-27	Local privilege escalation vulnerability.

Issue ID	Issue Description
NX-30	Ability to fully edit a profile when the SSLVPN Server is unreachable or the client is offline.
NX-31	NetExtender arbitrary file overwrite vulnerability.
NX-35	Displays a security alert when the FQDN for the SSLVPN server does not match the CN in the server certificate.
NX-38	Netextender with AOV connections gets dropped frequently and requires manual reconnecting.
NX-54	The owner field that records the Windows user account in the connection .json is case-sensitive.

Known Issues

Not Applicable.

Additional Reference

Not Applicable.

Version 10.3.1

January 2025

About NetExtender Windows

NetExtender Windows is a transparent software application for Windows users that enables remote users to securely connect to the remote network accessed through a SonicWall appliance. With NetExtender Windows, remote users can securely run any application on the remote network. Users can upload and download files, mount network drives, and access resources as if they were on the local network.

This release supports all the features and contains all the issues resolved in previous NetExtender Windows releases. For more information, see the last release notes on MySonicWall at <https://mysonicwall.com>.

Compatibility and Installation Notes

- Most popular browsers are supported, but prefers Google Chrome for the real-time graphics display on the Dashboard.
- A [MySonicWall](#) account is required.

Supported Platforms

NetExtender Windows Client Versions

The following is a list of NetExtender Windows client versions that are available in this release.

Version	Description
10.3.2	NetExtender for Windows 10 32-bit MSI/EXE
10.3.2	NetExtender for Windows 10/11 64-bit MSI/EXE
10.3.2	NetExtender for Windows 11/10 ARM64-bit

Supported Client Platforms

NetExtender Windows 10.3.2 supports computers running the following versions:

- Windows 10/11.

Supported SonicWall Appliances

SonicWall appliances receive NetExtender Windows connections from remote clients. The following appliances are supported:

- SonicWall firewalls running SonicOS 8 and higher, including the following platforms:
 - TZ80 running SonicOS 8
- SonicWall firewalls running SonicOS 7 and higher, including the following platforms:
 - TZ270, TZ270W, TZ370, TZ370W, TZ470, and TZ470W running SonicOS 7
 - TZ570, TZ570W, TZZ570P, and TZ670 running SonicOS 7
 - NSa2700, NSa3700, NSa4700, NSa5700, and NSa6700 running SonicOS 7
 - NSv270, NSv470, and NSv870 running SonicOS 7
 - NSsp10700, NSsp11700, NSsp13700, and NSsp15700 running SonicOS 7

- SonicWall firewalls running SonicOS 6.5.4.7 and higher, including the TZ, NSa, SOHO, and SuperMassive (SM) series platforms:
 - TZ300, TZ300W, TZ300P, TZ350, TZ350W, TZ400, TZ400W, TZ500, TZ500W, TZ600, TZ600P
 - NSa2600, NSa3600, NSa4600, NSa5600, and NSa6600
 - NSa2650, NSa3650, NSa4650, NSa5650, NSa6650, NSa9250, NSa9450, and NSa9650
 - SOHOW, SOHO250, and SOHO250W
 - SM9200, SM9250, SM9400, SM9450, SM9600, and SM9650
- SonicWall virtual firewalls running all releases of SonicOS 6.5.4.4v, including the following NSv series platforms:
 - NSv 10, 25, 50, 100, 200, 300, 400, 800, 1600
- SonicWall firewall running all releases of SonicOS 5.9.2.8-11o and 5.9.2.14-13o, including the following platform:
 - SOHO
- Secure Mobile Access (SMA) 100 Series appliances running SMA 10.2.1 or higher:
 - SMA200, SMA210, SMA400, SMA410
 - SMA500v for ESXi (on ESXi 6.0 and higher)
 - SMA500v for Hyper-V (on Hyper-V 2019 and 2022)
 - SMA500v for AWS
 - SMA500v for Azure
 - SMA500v for KVM

Supported Firewall Firmware Version

- GEN 5 (SOHO only) - 5.9.2.8-11o / 5.9.2.14-13o
- GEN 6/6.5 - 6.5.4.13-105n / 6.5.4.15-117n
- GEN 7 - 7.0.1-5161 / 7.1.1-7058 / 7.1.2-7019
- GEN 8 - 8.0.0-8035

① | **NOTE:** SonicWall recommends using the latest GEN 7 and GEN 8 firmware for optimal performance.

Supported Firmware SMA Versions

- SMA 100 10.2.1.13
- SMA 100 10.2.1.14

① | **NOTE:** SonicWall recommends using the latest NetExtender Windows with the latest SMA 100 Series firmware for optimal performance.

What's New

The NetExtender feature "Connect automatically with the default connection" only allows the VPN to connect following Windows logon. This behavior change prevents the VPN from connecting prior to Windows Logon, which could lead to unauthorized network access, especially for shared desktop/laptop computers.

This release provides the latest NetExtender Windows version with the latest version of the SMA 100 Series and fixes for previously reported issues.

Resolved Issues

Issue ID	Issue Description
SMA-5590	NetExtender Windows 10.3.0 client users could not connect when they upgraded to 10.2.1.13-72sv. The error message shows "Cannot get a response from the server."
SMA-5595	The behavior of EPC profiles varies depending on the version of NetExtender.
SMA-5602	NetExtender Windows 10.3.0 displays the MFA PIN code entry screen.
SMA-5603	NetExtender Windows 10.3.0 executable shows version 10.0.0.0 instead of 10.3.0, causing Qualys Scanning Platform to flag it as vulnerable.
SMA-5604	NetExtender Windows 10.3.0 shows an error message "Failed to log in to server" when the password contains German umlaut characters (ä, ö, ü). It works with NetExtender 10.2.341.
SMA-5635	NetExtender Windows 10.3.0 loses the connection profile. When users try to create a profile with the same name, NetExtender UI shows an error, "The connection has already existed."

Known Issues

Not Applicable.

Additional Reference

Not Applicable.

Version 10.3.0

November 2024

About NetExtender Windows

NetExtender Windows is a transparent software application for Windows users that enables remote users to securely connect to the remote network accessed through a SonicWall appliance. With NetExtender Windows, remote users can securely run any application on the remote network. Users can upload and download files, mount network drives, and access resources as if they were on the local network.

This release supports all the features and contains all the issues resolved in previous NetExtender Windows releases. For more information, see the last release notes on MySonicWall at <https://mysonicwall.com>.

Compatibility and Installation Notes

- Most popular browsers are supported, but prefers Google Chrome for the real-time graphics display on the Dashboard.
- A [MySonicWall](#) account is required.

Supported Platforms

NetExtender Windows Client Versions

The following is a list of NetExtender Windows client versions that are available in this release.

Version	Description
10.3.0	NetExtender for Windows 10 32-bit MSI/EXE
10.3.0	NetExtender for Windows 10/11 64-bit MSI/EXE
10.3.0	NetExtender for Windows 11/10 ARM64-bit

Supported Client Platforms

NetExtender Windows 10.3.0 supports computers running the following Windows versions:

- Windows 10/11.

Supported SonicWall Appliances

SonicWall appliances receive NetExtender Windows connections from remote clients. The following appliances are supported:

- SonicWall firewalls running SonicOS 8 and higher, including the following platforms:
 - TZ80 running SonicOS 8
- SonicWall firewalls running SonicOS 7 and higher, including the following platforms:
 - TZ270, TZ270W, TZ370, TZ370W, TZ470, and TZ470W running SonicOS 7
 - TZ570, TZ570W, TZZ570P, and TZ670 running SonicOS 7
 - NSa2700, NSa3700, NSa4700, NSa5700, and NSa6700 running SonicOS 7
 - NSv270, NSv470, and NSv870 running SonicOS 7
 - NSsp10700, NSsp11700, NSsp13700, and NSsp15700 running SonicOS 7
- SonicWall firewalls running SonicOS 6.5.4.7 and higher, including the TZ, NSa, SOHO, and SuperMassive (SM) series platforms:
 - TZ300, TZ300W, TZ300P, TZ350, TZ350W, TZ400, TZ400W, TZ500, TZ500W, TZ600, TZ600P
 - NSa2600, NSa3600, NSa4600, NSa5600, and NSa6600
 - NSa2650, NSa3650, NSa4650, NSa5650, NSa6650, NSa9250, NSa9450, and NSa9650
 - SOHOW, SOHO250, and SOHO250W
 - SM9200, SM9250, SM9400, SM9450, SM9600, and SM9650
- SonicWall virtual firewalls running all releases of SonicOS 6.5.4.4v, including the following NSv series platforms:
 - NSv 10, 25, 50, 100, 200, 300, 400, 800, 1600
- SonicWall firewall running all releases of SonicOS 5.9.2.8-11o and 5.9.2.14-13o, including the following platform:
 - SOHO
- Secure Mobile Access (SMA) 100 Series appliances running SMA 10.2.1 or higher:
 - SMA200, SMA210, SMA400, SMA410
 - SMA500v for ESXi (on ESXi 6.0 and higher)
 - SMA500v for Hyper-V (on Hyper-V 2019 and 2022)
 - SMA500v for AWS
 - SMA500v for Azure
 - SMA500v for KVM

Supported Firewall Firmware Version

- GEN 5 (SOHO only) - 5.9.2.8-11o / 5.9.2.14-13o
- GEN 6/6.5 - 6.5.4.13-105n / 6.5.4.15-117n
- GEN 7 - 7.0.1-5161 / 7.1.1-7058 / 7.1.2-7019
- GEN 8 - 8.0.0-8035

① | **NOTE:** SonicWall recommends using the latest GEN 7 and GEN 8 firmware for optimal performance.

Supported Firmware SMA Versions

- SMA 100 10.2.1.12
- SMA 100 10.2.1.13

① | **NOTE:** SonicWall recommends using the latest NetExtender Windows with the latest SMA 100 Series firmware for optimal performance.

What's New

This release provides the latest NetExtender Windows version with the latest version of the SMA 100 Series, enhancements, new features, and fixes for previously reported issues.

- Supports TLS1.3 for NetExtender Windows Client.
- Supports ARM64 for NetExtender Windows Client.
- NetExtender supports authenticating with a smart card.
- Configuration for changing Maximum Transmission Unit (MTU) value for NetExtender Windows Client.
- Profile Management.
- NetExtender User Interface upgrade

Resolved Issues

Issue ID	Issue Description
SMA-4841	NetExtender is not detecting SND if it is already connected.
SMA-5499	NetExtender generates the error “server is not responding” after applying the 23H2 Windows update.
SMA-5006	Change NetExtender default browser to Chrome for SAML authentication.

Known Issues

Not Applicable.

Additional Reference

Not Applicable.

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.

SonicWall NetExtender Windows Release Notes

Updated - April 2025

Software Version - 10.3.2

232-006227-00 Rev B

Copyright © 2025 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>.