Secure Mobile Access 10.2.1.2

WireGuard Feature Guide

SONICWALL®

Contents

1

Document Scope

This document describes how to configure and use the WireGuard Connector feature in SonicWall® Secure Mobile Access (SMA) 10.2.1.2.

ⓘ **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.

About WireGuard

WireGuard® is an extremely fast and simple VPN that utilizes state-of-the-art cryptography. Most users consider WireGuard a better choice over OpenVPN, as it is designed as a general purpose VPN that is appropriate for use in many different circumstances. WireGuard deploys cross-platform (Windows, macOS, BSD, iOS, and Android) on both embedded interfaces and super computers. Many regard it as the easiest and most secure VPN solution.

Guide Conventions

The following conventions are used in this guide:

CONVENTIONS USED IN THIS GUIDE

Convention	Use
Bold	Highlights field, button, and tab names. Also highlights window, dialog box, and screen names. Also used for file names and text or values you are being instructed to type into the interface.
Italic	Indicates the name of a technical manual, emphasis on certain words in a sentence, or the first instance of a significant term or concept.
Menu Item > Menu Item	Indicates a multiple step management interface menu choice. For example, **System > Status** means select the **Status** page under the **System** menu.

Browser Requirements

The following web browsers and operating systems support the Secure Mobile Access web-based management interface and the user portal, **Virtual Office**.

For information about certain limitations, see the *SMA10.2.1.2 Release Notes* available on MySonicWall.

Topics:

Browser Requirements for the Administrator

SECURE MOBILE ACCESS ADMINISTRATOR BROWSER REQUIREMENTS

Browser	Operating System
Edge (latest version)	• Windows 10
Mozilla Firefox (latest version)	• Windows 10 • Linux • macOS X
Google Chrome (latest version)	• Windows 10 • Linux • macOS X

To configure an SMA10.2.1.2 appliance using the Secure Mobile Access web-based management interface, an administrator must use a web browser with Java, JavaScript, ActiveX, cookies, pop-ups, TLS 1.2, and TLS 1.3 enabled.

Browser Requirements for the End User

The following is a list of Web browser and operating system support for various Secure Mobile Access protocols including NetExtender and various Application Proxy elements. Minimum browser version requirements are shown for Windows, Linux, and MacOS.

The following table provides specific browser requirements for the Secure Mobile Access End User Interface.

SECURE MOBILE ACCESS END USER BROWSER REQUIREMENTS

Browser	Operating System
Edge (latest version)	• Windows 10

Browser	Operating System
Mozilla Firefox (latest version)	• Windows 10 • Linux • macOS X
Google Chrome (latest version)	• Windows 10 • Linux • macOS X
Apple Safari (latest version)	• macOS X

2

Using WireGuard Connector

This chapter provides the information and steps for configuring WireGuard connector on the management interface and using it on the client.

ⓘ | **NOTE:** WireGuard supports both Windows and Linux.

- Configuring WireGuard
- Connecting WireGuard on NetExtender
- Viewing Connection Status

Configuring WireGuard

WireGuard can be configured on the **Services > Settings** page in the SonicWall Secure Mobile Access web-based management interface.

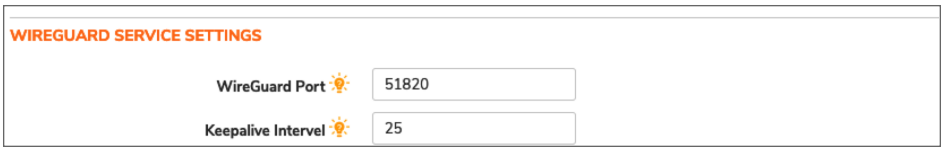
To enable WireGuard connector:

1. Go to **Settings** page under **Services** tab to view the various setting options.
2. In the **VPN Tunnel Type Setting** section select the **VPN Tunnel Type** as WireGuard.

ⓘ | **NOTE:** Wireguard can be connected on the client only if it is enabled in the management interface. Else, it will be connected to SSLVPN.

ⓘ | **NOTE:** You can make WireGuard as your first preference while connecting it on the client by moving it to the top, using the arrow symbol.

3. In the **WireGuard Service Settings** section enter the **WireGuard Port** and **Keepalive Interval** information.



ⓘ | **NOTE:** The configured port must be opened in firewall for UDP protocol.

4. Click **Accept** to save the setting.

Connecting WireGuard on NetExtender

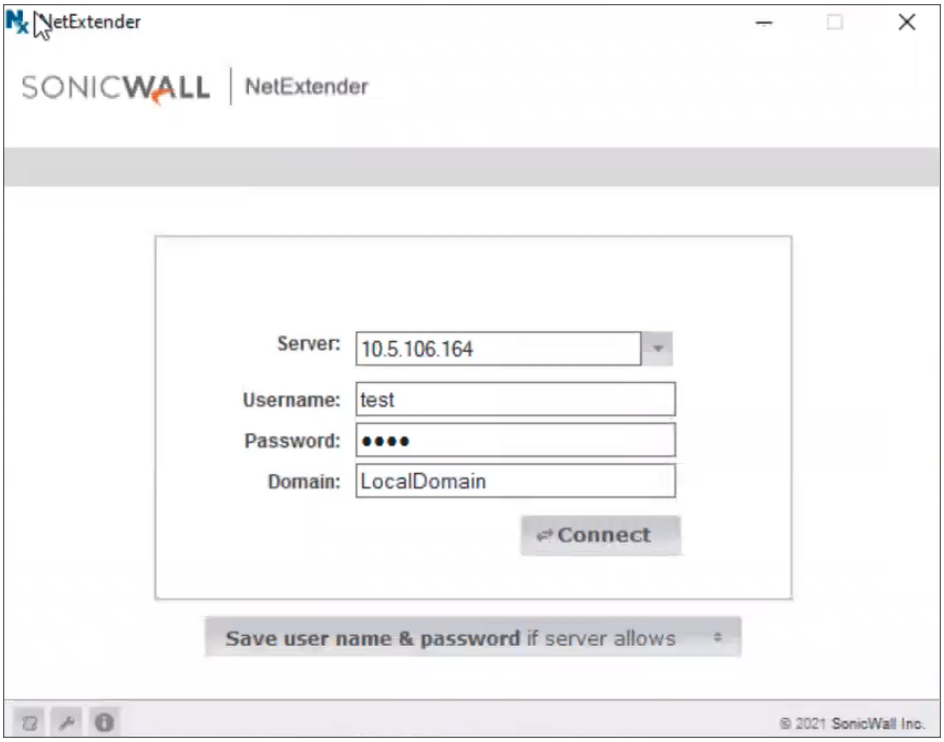
This section describes the steps to connect WireGuard connector on NetExtender client on Windows or Linux system.

Choosing Tunnel Protocol

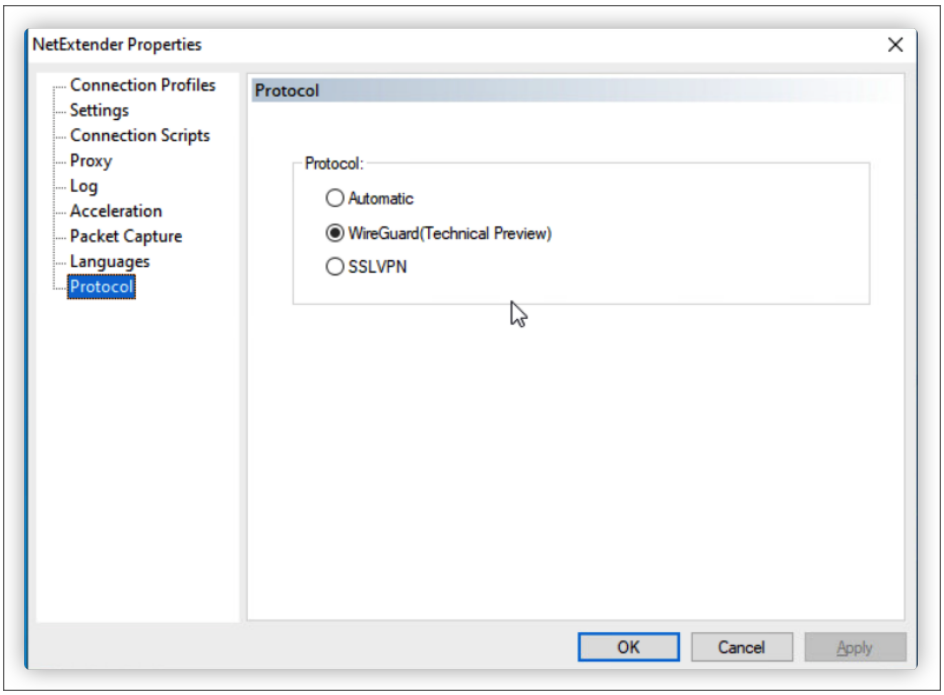
Before connecting WireGuard on the NetExtender client, you need to first select the tunnel protocol.

Windows:

1. Open the **NetExtender Client** on your Windows system.



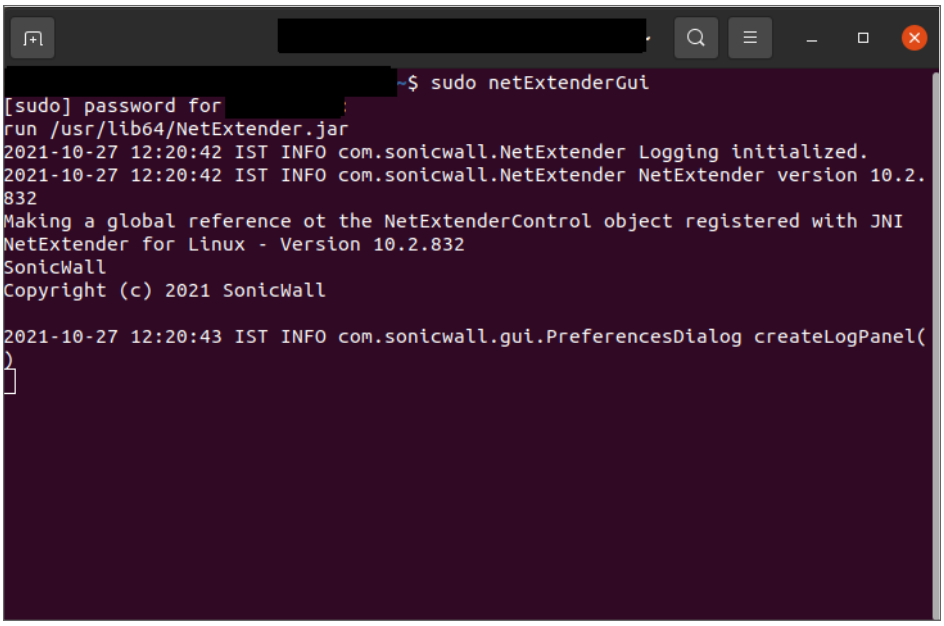
2. Click on **NetExtender Properties** button at the bottom and select **Protocol**.

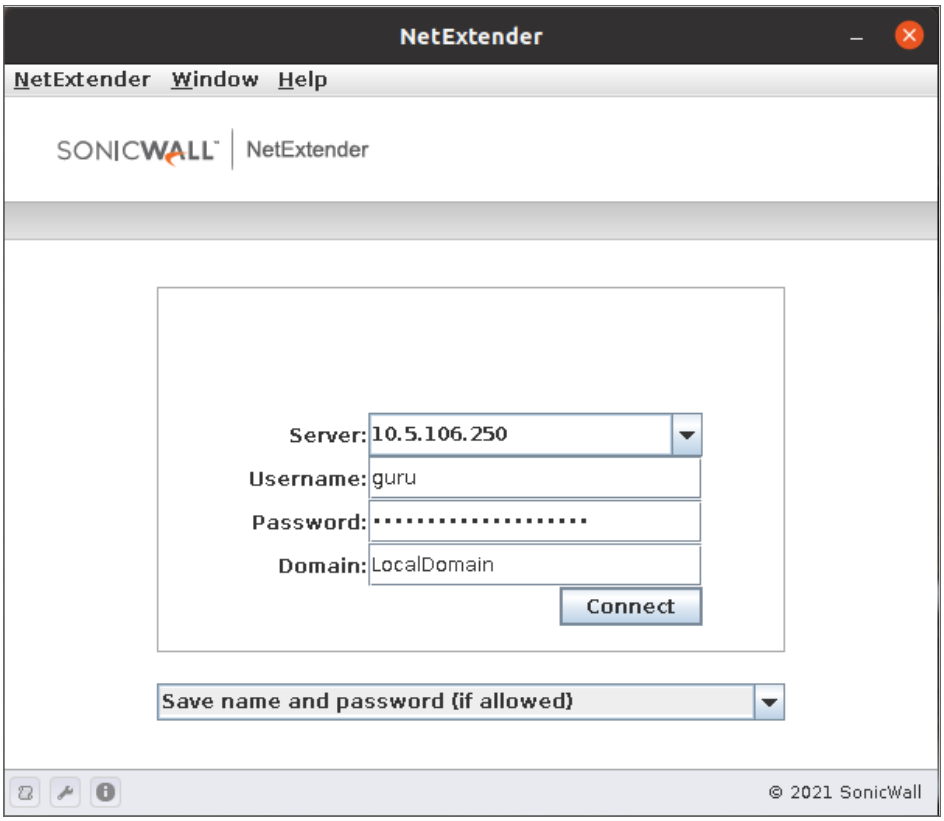


3. You can select from the following three protocol options:
    - **Automatic:** Connects to the tunnel that you have selected as your first preference on the management interface.
    - **WireGuard:** Connects to WireGuard tunnel. If WireGuard is not enabled, or fail to connect, it will return back to login page.
    - **SSLVPN:** Connects to SSLVPN tunnel.
4. Click **OK**.

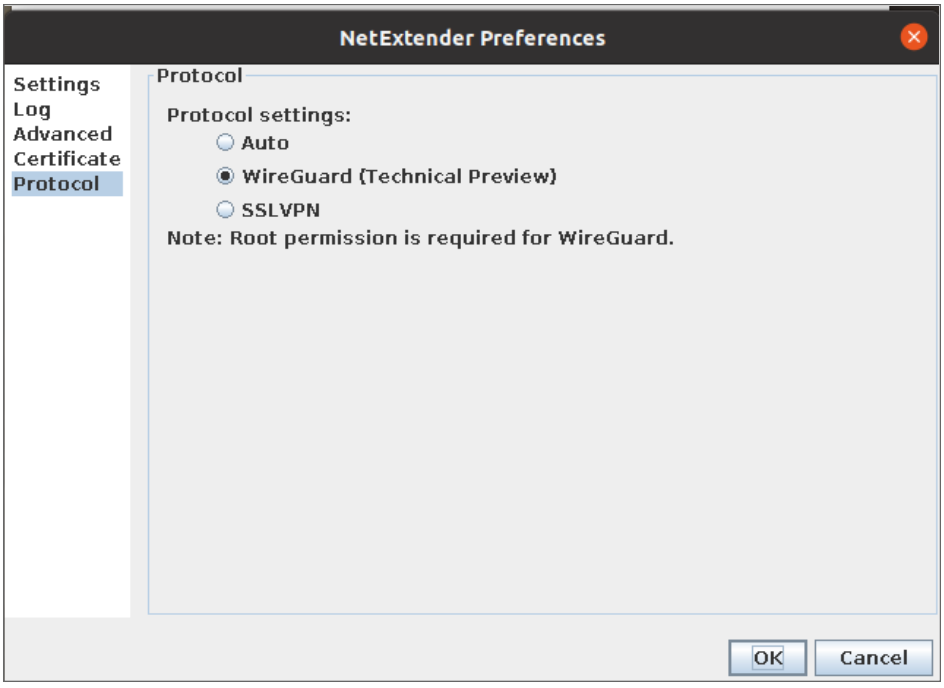
Linux:

1. Open the **NetExtender Client** on your Linux system with command prompt using sudo command.





2. Click on **NetExtender Prefernces** button at the bottom and select **Protocol**.



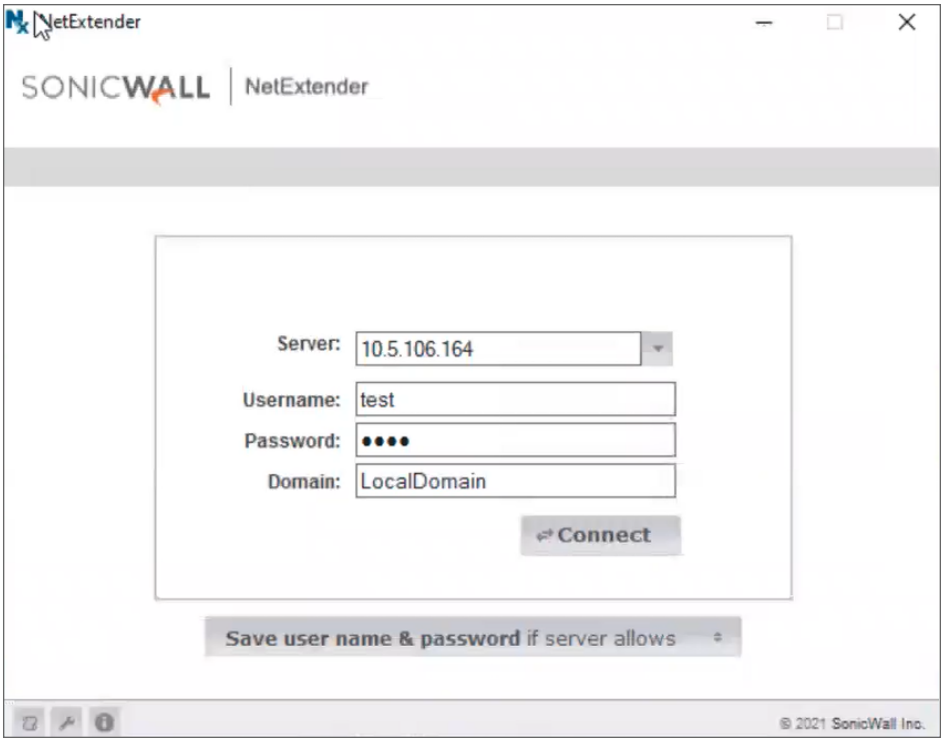
3. You can select from the following three protocol options:
    - **Automatic:** Connects to the tunnel that you have selected as your first preference on the management interface.
    - **WireGuard:** Connects to WireGuard tunnel. If WireGuard is not enabled, or fail to connect, it will return back to login page.
    - **SSLVPN:** Connects to SSLVPN tunnel.
4. Click **OK**.

Connecting to WireGuard Tunnel

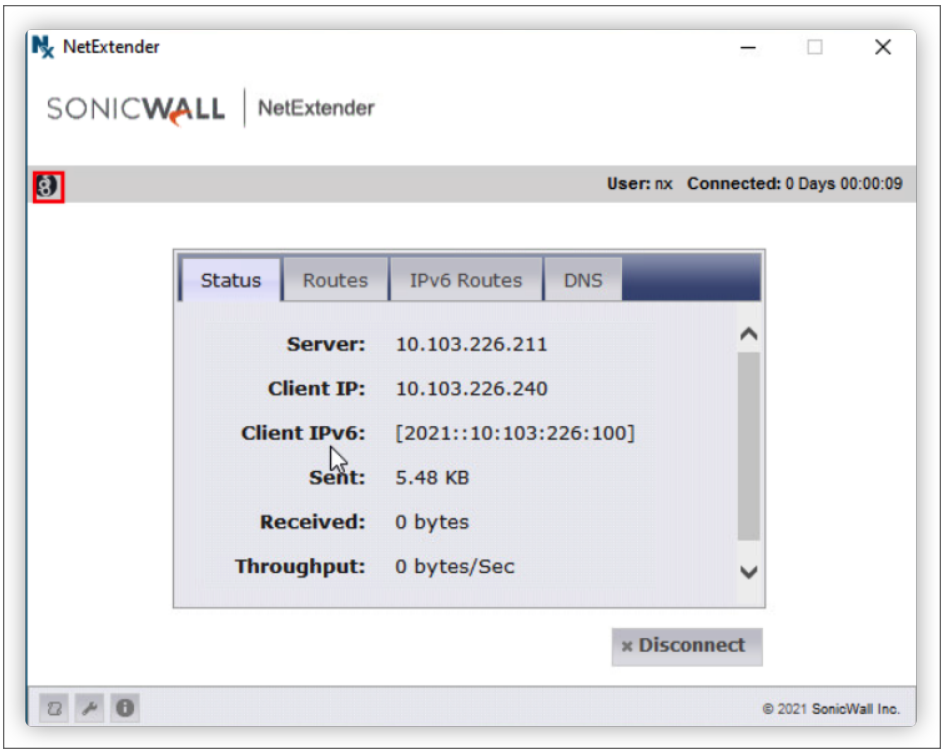
After selecting the protocol as WireGuard, you can connect NetExtender client using the following steps:

Windows:

1. On the home page of NetExtender, enter the details such as **Server**, **Username**, **Password** and **Domain**. Click **Connect**.



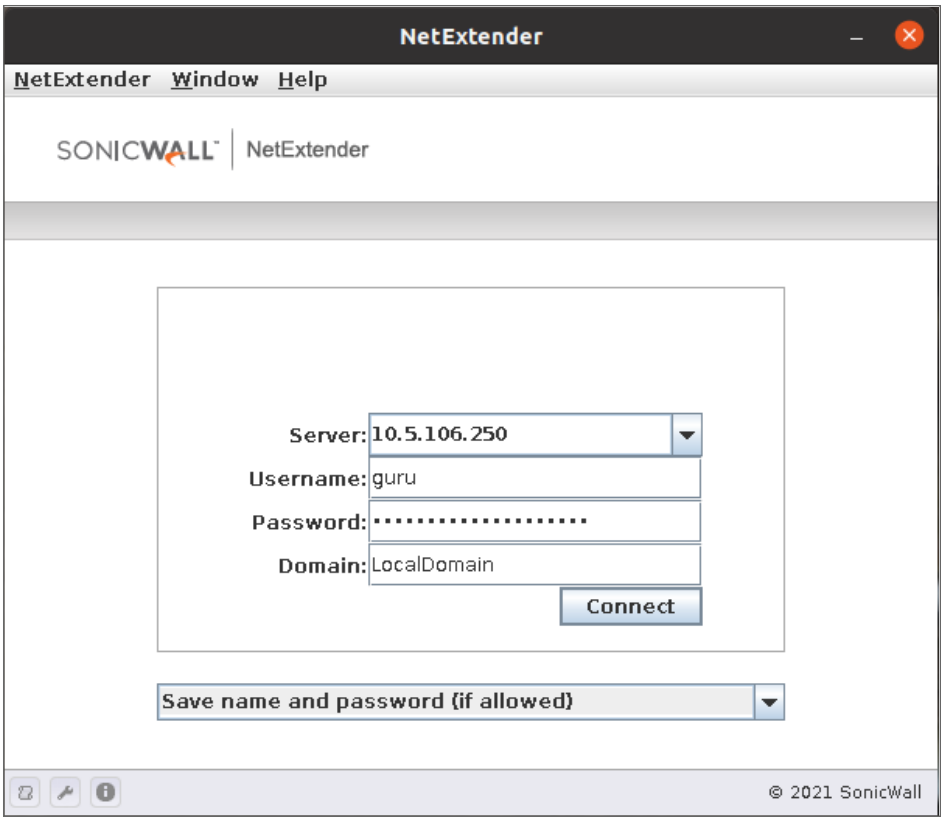
2. Once it is successfully connected, the **Status** page displays the connection information.



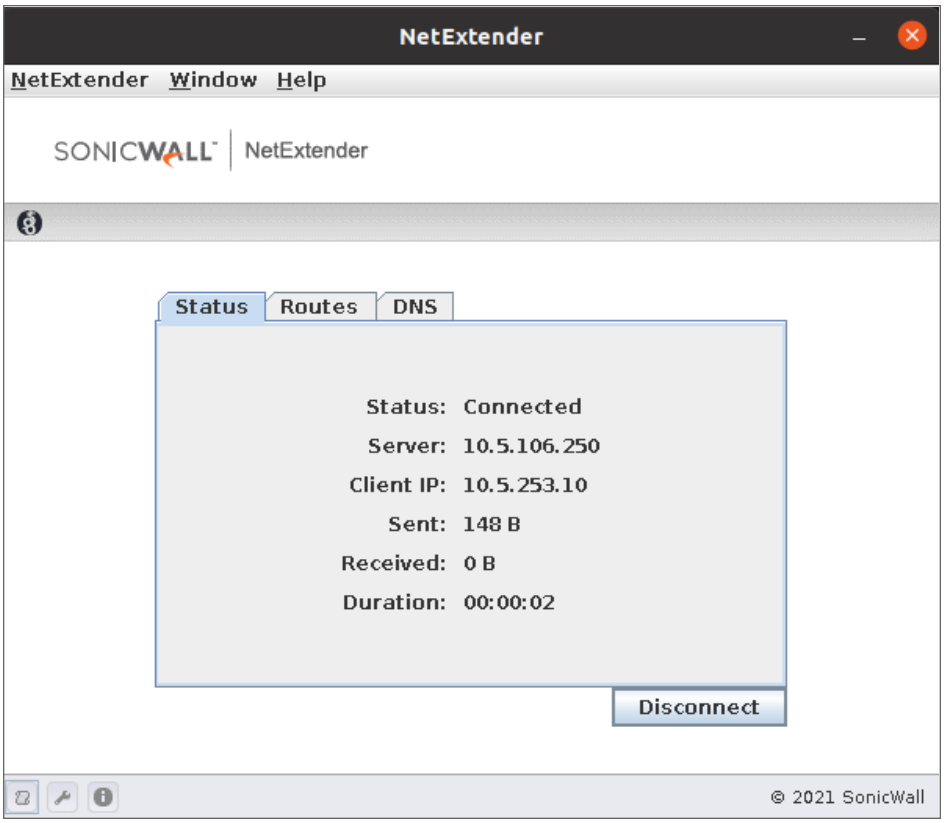
NOTE: You can check the symbol at the top left of the page to confirm if the client is connected through WireGuard or SSLVPN.

Linux:

1. On the home page of NetExtender, enter the details such as **Server**, **Username**, **Password** and **Domain**. Click **Connect**.



2. Once it is successfully connected, the **Status** page displays the connection information.



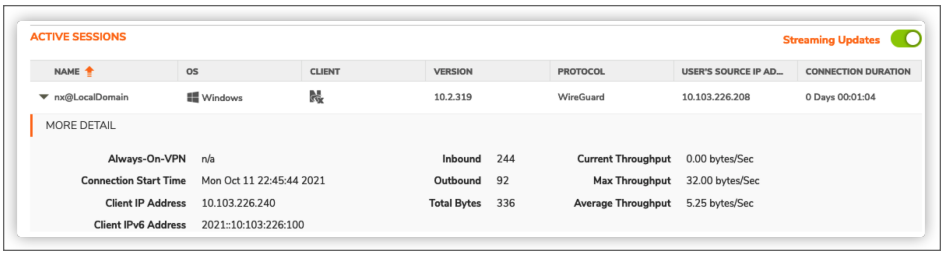
NOTE: You can check the symbol at the top left of the page to confirm if the client is connected through WireGuard or SSLVPN.

Viewing Connection Status

After NetExtender client successfully establishes connection using Wireguard protocol you can view the status of the connection on the **Clients > Status** page on the management interface

To view connection status:

1. Go to **Status** page under **Clients** tab to view the **Active Sessions** page. This page displays all the connection information such as **Usename**, **OS**, **Client**, **Version**, **Protocol**, **User's source IP address** and **Connection duration**.



2. You can view more details about the connection by expanding the data using the arrow symbol next to the Username.

3

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- View video tutorials
- Access https://mysonicwall.com
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

About This Document

NOTE: A NOTE icon indicates supporting information.

IMPORTANT: An IMPORTANT icon indicates supporting information.

TIP: A TIP icon indicates helpful information.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

Secure Mobile Access WireGuard Feature Guide
Updated - November 2021
Software Version - 10.2.1.2
232-005777-00 Rev A

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/end-user-product-agreements/.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035