# Secure Mobile Access 10.2

# NetExtender Feature Guide

SONICWALL®

# Contents

1

# NetExtender Feature Overview

**Topics:**

- Document Scope

## Document Scope

This document provides a brief overview of the SonicWall SMA 10.2.1 NetExtender features, concepts, and how to configure and manage them.

**Topics:**

- What is NetExtender
- Benefits of using NetExtender
- NetExtender Concepts
- Supported Platforms
- Feature Support in NetExtender

## What is NetExtender

SonicWall NetExtender is a transparent software application that enables the remote users to securely connect to the remote network. With NetExtender, remote users can securely run any application on the remote network. Users can upload and download files, mount network drives, and access resources in the same way as if they were on the local network. The NetExtender connection uses a Point-to-Point Protocol (PPP) connection.

## Benefits of using NetExtender

NetExtender provides remote users with full access to the protected internal network. The experience is virtually identical to that of using a traditional IPSec VPN clients, but NetExtender does not require any manual client installation. Instead, the stand-alone NetExtender client is automatically installed on the PC of a remote user by an HTML5 control when using the Edge or Firefox. On Linux systems, supported browsers use Java controls to automatically install NetExtender from the Virtual Office portal.

The NetExtender Windows client also has a custom-dialer that allows it to be launched from the Windows Network Connections menu. This custom-dialer allows NetExtender to be connected before the Windows domain login. The NetExtender Windows client also supports a single active connection, and displays real-time throughput and data compression ratios in the client.

After installation, NetExtender automatically launches and connects a virtual adapter for SSL-secure NetExtender point-to-point access to permitted hosts and subnets on the internal network.

# NetExtender Concepts

The following sections describes the advanced concepts of SonicWall NetExtender

- Stand-Alone Client
- Installing NetExtender through Microsoft Installer - Pre-filling the Server and Domain Fields
- NetExtender support Network logon (PreLogon)
- Multiple Ranges and Routes
- IP Address User Segmentation
- Client Routes
- External Authentication Methods
- Point to Point Server IP Address
- Tunnel All Mode
- Proxy Configuration
- About SMA Connect Agent
- Supported Operating Systems for Connect Agent

## Stand-Alone Client

Secure Mobile Access provides a stand-alone NetExtender application. NetExtender is a browser-installed lightweight application that provides comprehensive remote access without requiring users to manually download and install the application. The first time a user launches NetExtender, the NetExtender stand-alone client is automatically installed on the user's PC. The installer creates a profile based on the user's login information. The installer window then closes and automatically launches NetExtender. If the user has a legacy version of NetExtender installed, the installer first uninstalls the old NetExtender and installs the new version.

After the NetExtender stand-alone client has been installed, Windows users can launch NetExtender from their PC's **Start** > **Programs** menu and configure NetExtender to launch when Windows boots.

NetExtender can establish a VPN session before the user logs into the Windows domain. Users can click **Switch User** on the Windows login screen and click the blue computer icon that appears at the right bottom of the screen to view the dialup connection list, and then can select NetExtender to connect.

On Linux systems, the installer creates a desktop shortcut in `/usr/share/NetExtender`. This can be dragged to the shortcut bar in environments like Gnome and KDE.

NetExtender is officially supported on the following client platforms

- Fedora core 36+ or Red Hat Enterprise Linux 8.x+
- Ubuntu 20.04+
- OpenSUSE 15.4+ or CentOS 8.x+
- Windows 11/10

NetExtender might work properly on other Linux distributions, but they are not officially supported by SonicWall.

## Installing NetExtender through Microsoft Installer - Pre-filling the Server and Domain Fields

Installing NetExtender through Microsoft Installer (MSI) now supports the use of default profile settings during the installation process where the default server and default domain can be pre-filled along with additional options that control whether the server and domain fields can be edited by a standard user. This feature is designed specifically for administrators who want their default servers and domains pre-set during the installation process.

***To set the default server and domain during the NetExtender Installation with Microsoft Installer:***

1. On the **Default Profile Setting** page, enter the **IP address of the Default Server** in the appropriate fieldand the location of the **Default Domain** in the second field.
2. Disable **Allow connections to other profiles** to prevent users from connecting to other profiles. This setting disables the Server and Domain fields for editing on the login page of NetExtender.
3. Enable this option to allow those connections. If this option is not enabled, users are not able to add or delete profiles on the NetExtender properties page.

## NetExtender support Network logon (PreLogon)

ⓘ | **NOTE:** Network Logon support is available from SMA 10.2.1.9 onwards.

Users always log in to their Windows accounts before connecting a VPN tunnel. But in a typical scenario, a VPN tunnel (NetExtender) is required to allow the user to log in for the first time or after a password reset. Network Logon (PreLogon) is a feature that allows users to establish a VPN tunnel (NetExtender) before they can log on to their Windows accounts.

To enable Network Logon (PreLogon) and more information, see Enabling Network Logon (PreLogon) feature on NetExtender section.

## Multiple Ranges and Routes

The Network administrators can use the multiple range and route support of NetExtender to easily segment groups and users, without configuring firewall rules to govern access. This user segmentation allows granular control of access to the network, allows users to access the necessary resources, and restricts access to the sensitive resources to only those who require them.

For networks that do not require segmentation, client addresses and routes can be configured globally.

## IP Address User Segmentation

Administrators can configure separate NetExtender IP address ranges for users and groups. These settings are configured on the **Users** > **Local users** and **Users** > **Local groups** pages. A **NetExtender** tab has been added to the **Edit User** and **Edit Group** windows.

When configuring multiple user and group NetExtender IP address ranges, it is important to know how the SMA appliance assigns IP addresses. When assigning an IP address to a NetExtender client, the SMA appliance uses the following hierarchy of ranges:

- An IP address from the range defined in the user's local profile.
- An IP addRess from the range defined in the group profile to which the user belongs.
- An IP address from the global NetExtender range.

To reserve a single IP address for an individual user, enter the same IP address in both the **Client Address Range Begin** and **Client Address Range End** fields on the **NetExtender** tab of the **Edit Group** window.

## Client Routes

NetExtender client routes are used to allow and deny access to various network resources. You can configure the client routes at the user and group level. NetExtender client routes are also configured on the **Edit User** and **Edit Group** windows. The segmentation of client routes is fully customizable allowing administrator to specify any possible permutations of user, group, and global routes. For example, only group routes, only user routes, group and global routes, user, group, and global routes, and so on. This segmentation is controlled by **Add Global NetExtender Client routes** and **Add Group NetExtender Client routes**.

## External Authentication Methods

Networks that use an external authentication server are not configured with local user names on the SMA appliance. In such cases, when a user is successfully authenticated, a local user account is created when the **Add Global NetExtender Client routes** and **Add Group NetExtender Client routes** settings are enabled.

## Point to Point Server IP Address

In Secure Mobile Access, the PPP server IP address is 192.0.2.1 for all connecting clients. This IP address is transparent to both the remote users connecting to the internal network and to the internal network hosts communicating with remote NetExtender clients. Because the PPP server IP address is independent from the NetExtender address pool, all IP addresses in the global NetExtender address pool are used for NetExtender clients.

## Tunnel All Mode

Tunnel All mode routes all traffic to and from the remote user over the Secure Mobile Access NetExtender tunnel including traffic to the remote users local network. This accomplished by adding the following routes to all remote clients' route table.

**TUNNEL ALL MODE: ROUTES TO BE ADDED TO REMOTE CLIENT'S ROUTE TABLE**

| IP Address | Subnet Mask |
|---|---|
| 0.0.0.0 | 0.0.0.0 |
| 0.0.0.0 | 128.0.0.0 |
| 128.0.0.0 | 128.0.0.0 |

NetExtender also adds routes for the local networks of all connected Network Connections. These routes are configured with higher metrics than any existing routes to force traffic destined for the local network over the Secure Mobile Access tunnel instead. For example, if a remote user is has the IP address 10.0.67.64 on the 10.0.*.* network, the route 10.0.0.0/255.255.0.0 is added to route traffic through the Secure Mobile Access tunnel.

Tunnel All mode is configured at the global, group, and user levels.

## Proxy Configuration

SMA appliances support NetExtender sessions using proxy configurations. Currently, only HTTPS proxy is supported. When launching NetExtender from the Web portal, if your browser is already configured for proxy access, NetExtender automatically inherits the proxy settings. The proxy settings can also be manually configured in the NetExtender client preferences. NetExtender can automatically detect proxy settings for proxy servers that support the Web Proxy Auto Discovery (WPAD) Protocol.

NetExtender provides three options for configuring proxy settings:

- **Automatically detect settings** - To use this setting, the proxy server must support Web Proxy Auto Discovery Protocol (WPAD) that can push the proxy settings script to the client automatically.
- **Use automatic configuration script** - If you know the location of the proxy settings script, you can select this option and provide the URL of the script.
- **Use proxy server** - You can use this option to specify the IP address and port of the proxy server. Optionally, you can enter an IP address or domain in the **BypassProxy** field to allow direct connections to those addresses and bypass the proxy server. If required, you can enter a user name and password for the proxy server. If the proxy server requires a username and password, but you do not specify them, a NetExtender pop-up window prompts you to enter them when you first connect.

When NetExtender connects using proxy settings, it establishes an HTTPS connection to the proxy server instead of connecting to the SMA server directly. The proxy server then forwards traffic to the SMA server. All traffic is encrypted by SSL with the certificate negotiated by NetExtender, of which the proxy server has no knowledge. The connecting process is identical for proxy and non-proxy users.

## About SMA Connect Agent

The Browser Plug-ins (NPAPI) are used to launch native applications such as NetExtender, EPC and so on. For security reasons, popular browsers block theses Plug-ins. The Chrome and Edge browsers, for example, has disabled all NPAPI Plug-ins. As such, the ease-of-use ability of launching directly from the browser is no longer functional, and a new method for seamless launching is necessary.

There is another application to launch that opens a specific Scheme URL. There are some Schemes already defined in the Windows/macOS, such as *mailto*. The SMA Connect Agent uses the Scheme URL to replace the Browser Plug-ins. The SMA Connect Agent is like a bridge that receives the Scheme URL requests and launches the specific native application.

To launch the Citrix Workspace through a Citrix bookmark, you must first install the SMA Connect Agent.

## Supported Operating Systems for Connect Agent

The SMA Connect Agent supports Windows and Mac operating systems.

# Supported Platforms

**Topics:**

- NetExtender Client Versions
- Supported Clients
- Supported SonicWall Appliances

## NetExtender Client Versions

The NetExtender client versions include the following:

| Description | Version |
|---|---|
| NetExtender for Windows 10/11 64 bit MSI/EXE | 10.2.337 |
| NetExtender for Windows 10 32-bit MSI/EXE | 10.2.337 |
| NetExtender for 32-bit Linux TGZ | 10.2.850 |
| NetExtender for 64-bit Linux TGZ | 10.2.850 |
| NetExtender for 32-bit Linux RPM | 10.2.850 |
| NetExtender for 64-bit Linux RPM | 10.2.850 |

## Supported Clients

NetExtender 10.2.337 is supported on computers running the following Windows versions:

- Windows 11/10 with the latest patches.

NetExtender 10.2.850 is supported on computers running the following Linux versions:

- Ubuntu 20.04+.
- Fedora Core 36+ or Red Hat Enterprise Linux 8.x+.
- OpenSUSE 15.4+ or CentOS 8.x+.

ⓘ **NOTE:** Always on VPN and SND are available with NetExtender MSI client for Windows, but not with NetExtender for Linux.

## Supported SonicWall Appliances

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

SonicWall firewalls runningSonicOS 7.0, including the following platforms:

- TZ670, TZ570, TZ570W, TZ570P running SonicOS 7.0
- NSv 270, NSv 470, and NSv 870 running SonicOS 7.0
- NSsp 15700 running SonicOS 7.0

SonicWall firewalls running SonicOS 6.5, including the NSa, TZ, SOHO, and SuperMassive series platforms:

- NSa 2600-6600
- NSa 2650-9650
- TZ300-TZ600, TZ300W-TZ500W, TZ300P, TZ600P, TZ350, TZ350W
- SOHO W, SOHO 250, SOHO 250W
- SuperMassive 9200-9600

Secure Mobile Access (SMA) 100 Series appliances running 9.0 or higher:

- SMA 200/400
- SMA 210/410
- SMA 500v for ESXi (on ESXi 6.0 and higher)
- SMA 500v for Hyper-V (on Hyper-V 2016 and 2019)
- SMA 500v for AWS
- SMA 500v for Azure
- SMA 500v for KVM

# Feature Support in NetExtender

### FEATURE SUPPORT ON NETEXTENDER FOR WINDOWS AND NETEXTENDER FOR LINUX

| Feature | Supported by NetExtender for Windows | Supported by NetExtender for Linux |
|---|---|---|
| Tunneling | Yes | Yes |
| Certificate Authentication | Yes | No |
| SAML Authentication | Yes | Yes |
| TLSv1.3 Support | No | Yes |
| Always On VPN | Yes | No |
| Endpoint Control | Yes | Yes |
| Personal Device Authorization | Yes | Yes |
| Auto Reconnect | Yes | Yes |
| Credential Cache | Yes | Yes |
| Post Connection Script | Yes | Yes |
| Network Logon (PreLogon) | Yes | No |

### FEATURE SUPPORT ON SMA 100 AND SONICWALL FIREWALLS

| Feature | Supported on SMA 100 | Supported on Firewalls |
|---|---|---|
| Always On VPN | Yes | No |
| SAML Authentication | Yes | Yes |
| One-Time Password Method Switching | Yes | Yes |
| Post Connection Script | Yes | No |
| Endpoint Control | Yes | No |
| Personal Device Authorization | Yes | No |
| DHCP IP Pool | Yes | Yes |
| Network Logon (PreLogon) | Yes | Yes |

ⓘ **NOTE:** The features listed above in the Feature Support on SMA 100 and SonicWall Firewalls table are supported only when using NetExtender with the SMA 100 Series.

2

# Configuring NetExtender

This section explains how to configure SonicWall NetExtender.

**Topics:**

- User Prerequisites
- User Configuration Tasks

## User Prerequisites

This section describes the user Prerequisites for Windows clients and Linux clients for installing NetExtender.

### For Windows Clients

Windows clients must meet the following prerequisites to use NetExtender:

| | |
|---|---|
| Platform | Windows 11/10 |
| Browsers | Mozilla Firefox 103.0 and higher<br>Google Chrome 104.0 and higher |

To initially install the NetExtender client, the user must be logged into the PC with administrative privileges.

If the SMA gateway uses a self-signed SSL certificate for HTTPS authentication, it is necessary to install the certificate before establishing a NetExtender connection. If you are unsure if the certificate is self-signed or generated by a trusted root Certificate Authority, SonicWall recommends that you import the certificate. The easiest way to import the certificate is to click Import Certificate on the Virtual Office home page.

When using the network logon method from the Windows login screen, NetExtender uses System Store for certificate-based authentication. When the user is already logged in to Windows, NetExtender uses the User Store for certificate-based authentication. A user who wants to use the network logon method when certificate authentication is also enabled should import his user certificate into the System Store as well as into the User Store.

## For Linux Clients

Linux 32-bit or 64-bit clients are supported for NetExtender when running one of the following distributions (32-bit or 64-bit):

- Linux Fedora Core 36 or higher, Ubuntu 20.04 or higher, or OpenSUSE 10.3 or higher, Red Hat Enterprise Linux 8.x and higher, and CentOS 8.x and higher

The NetExtender client has been known to work on other distributions as well, but these are not officially supported.

ⓘ **NOTE:** Open source Java Virtual Machines (VMs) are not currently supported. If you do not have Java 1.5 or higher, you can use the command-line interface version of NetExtender.

# User Configuration Tasks

SonicWall NetExtender is a software application that enables remote users to securely connect to the remote network. With NetExtender, remote users can virtually join the remote network. Users can mount network drives, upload and download files, and access resources in the same way as if they were on the local network.

The following sections describe how to use NetExtender on the various supported platforms:

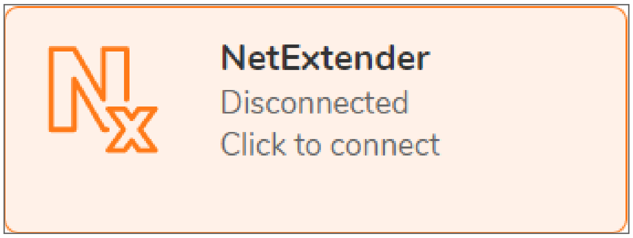
| | |
|---|---|
| Windows Platform Installation | Installing NetExtender on Windows<br>Enabling Network Logon (PreLogon) feature on NetExtender |
| Windows Platform Usage | Launching NetExtender Directly from Computer<br>Installing NetExtender with Microsoft Installer |
| Configuring NetExtender Properties | Configuring Connection Profiles Settings<br>Configuring Settings<br>Connection Scripts Settings<br>Configuring Proxy Settings<br>Configuring Log Settings<br>Configuring Acceleration Settings<br>Configuring Packet Capture Settings<br>Configuring Languages Settings<br>Configuring Protocol |
| Linux Platform | Installing NetExtender on Linux<br>Using NetExtender on Linux |

# Installing NetExtender on Windows

The procedure for installing NetExtender is same for all supported browsers on Windows platform.

***To install and launch NetExtender for the first time:***

1. Log in to the Workplace portal.
2. Click **NetExtender**.



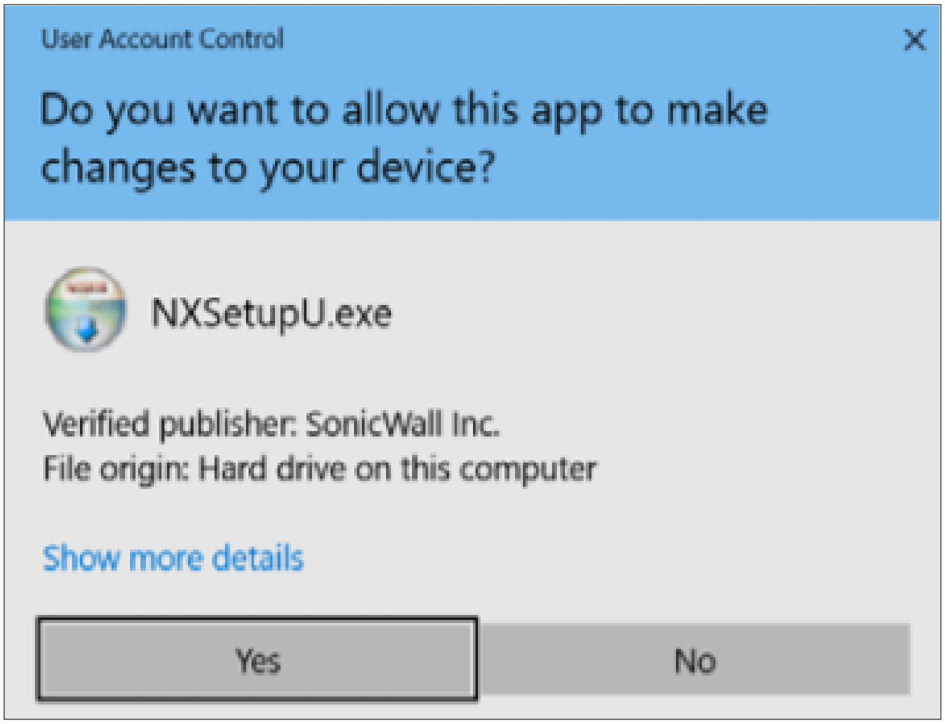
NetExtender
Disconnected
Click to connect

The prompt is displayed asking you to download the SMA Connect Agent.

3. Download and install the SMA Connect Agent and allow SMA Connect agent to launch NetExtender from your browser.

ⓘ **NOTE:** If the SMA Connect Agent is already installed, click Installed to ensure that you don't see the prompt again or click Continue to skip the prompt.

The NetExtender is downloaded automatically and the NetExtender installer launches.



User Account Control

Do you want to allow this app to make changes to your device?

NXSetupU.exe

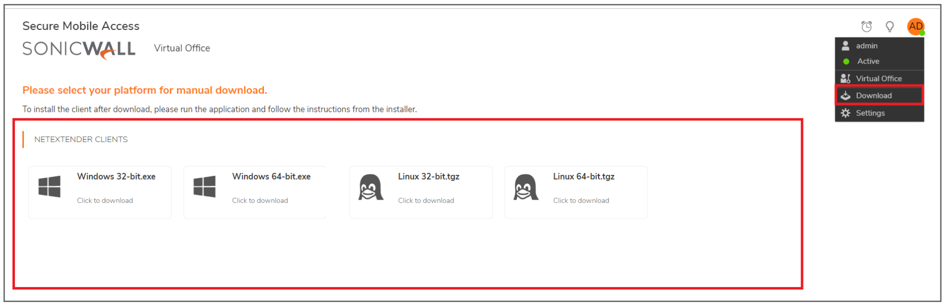
Verified publisher: SonicWall Inc.
File origin: Hard drive on this computer

4. In the **User Account Control** prompt, click **Yes** to run the NetExtender installer.

   NetExtender is connected.

   > ⓘ **NOTE:** If you see error connecting to NetExtender, click **Reconnect**, and skip to enter the user credentials step.

5. Optionally, if you do not see the prompt, the NexExtender client has not downloaded automatically. Continue executing the next steps to download and install the NetExtender manually.



Please select your platform for manual download.

To install the client after download, please run the application and follow the instructions from the installer.

   a. Click the User icon at the upper-right corner of the page.

   b. Click **Downloads**.

   c. Select your platform for manual download and click **Save File**.

      The file is saved in your `Downloads` folder.

6. Navigate to your `Downloads` folder and double-click **NXSetupU.exe** to run the installer.

   The User Account Control message ***Do you want to allow the following program to make changes to this computer?*** is displays.

7. Click **Yes**.

   The SonicWall NetExtender Setup wizard is launched. The Welcome screen recommends that you close all other applications before starting the setup to avoid the need to restart your computer after the installation. When ready to proceed, click **Next**.

8. In the License Agreement screen, read the agreement, select **I accept the terms of the License Agreement** and then click **Next**.

9. Optionally you can change the **Destination Folder** field click **Browse** and click **Next**.

10. Select or clear the shortcut options checkboxes that you require. The following options are selected by default:

    - Create a shortcut on StartMenu.
    - Create a shortcut on QuickLaunch bar.
    - Create a shortcut on Desktop.

11. Click **Install**.

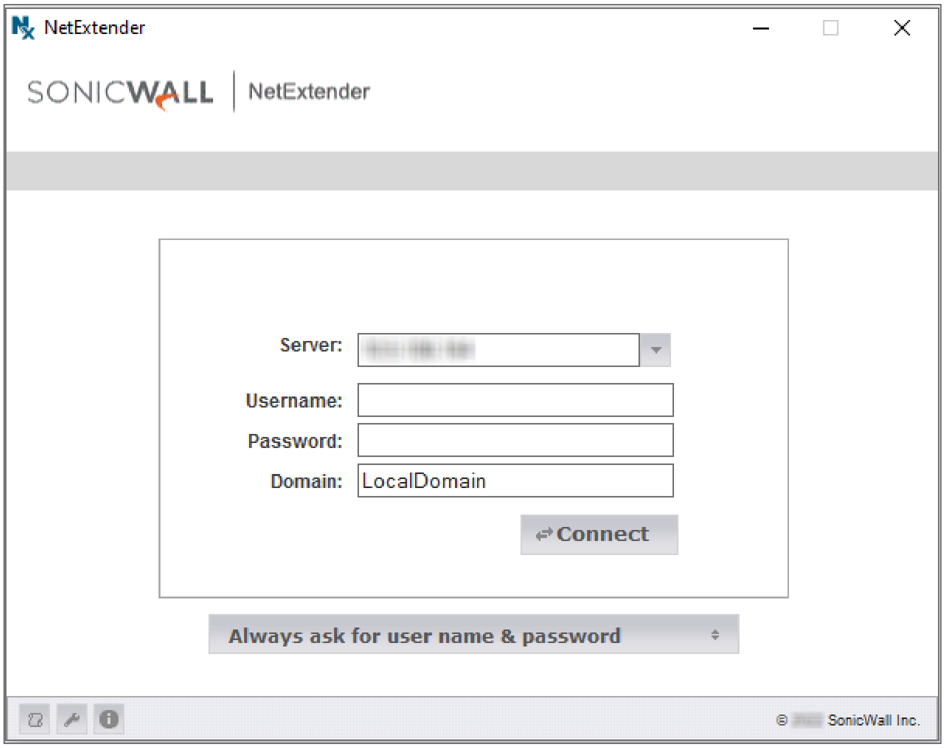
12. If a **Windows Security** dialog box displays ***Would you like to install this device software?***, click **Install**.

13. Optionally, you can select the **Run SonicWall NetExtender** check boxto launch NetExtender immediately after installation.

14. Click **Finish**.

15. After launching NetExtender, type the IP address or FQDN of the SMA appliance in the **Server** field.

    ⓘ **TIP:** This is the same server that you point your browser to when accessing the portal page to download NetExtender.



Server: [redacted]

Username:

Password:

Domain: LocalDomain

Always ask for user name & password

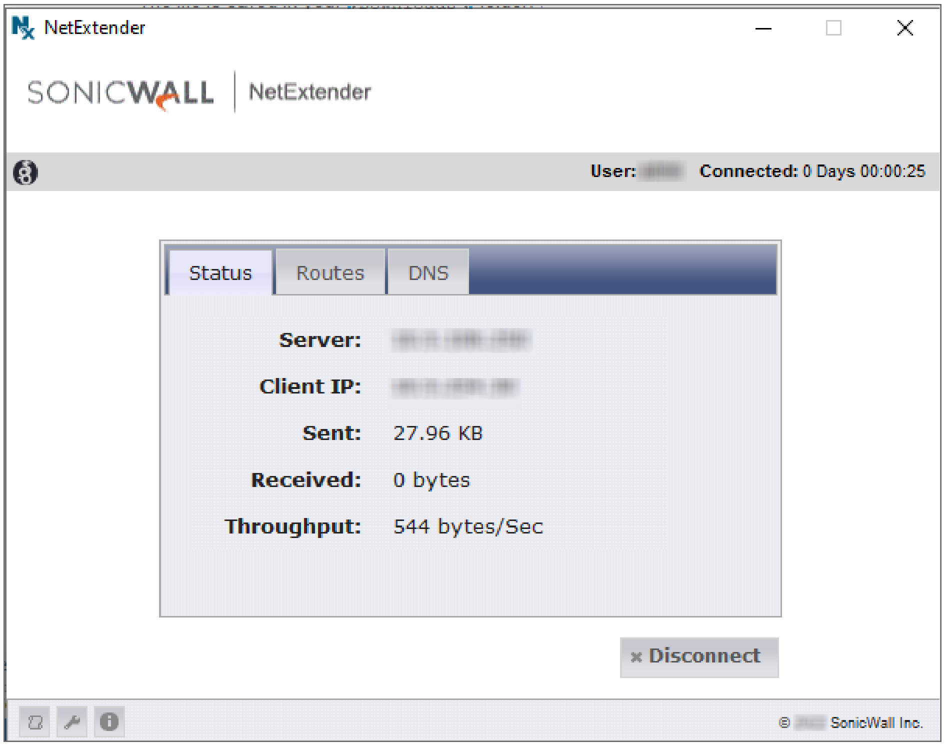
16. Enter the **Username** and **Password**.

17. In the **Domain** field, type in the domain.

    ⓘ **NOTE:** This is the same domain shown in the Domain field of the login page when you access the portal in your browser.

18. Click **Connect**

    NetExtender takes a few seconds to connect to the server and verify your credentials. The NetExtender status window displays, indicating that NetExtender successfully connected. The NetExtender icon is displayed in the task bar.



User: [redacted] Connected: 0 Days 00:00:25

Server: [redacted]

Client IP: [redacted]

Sent: 27.96 KB

Received: 0 bytes

Throughput: 544 bytes/Sec

© [redacted] SonicWall Inc.

| Field | Description |
|---|---|
| Server | Indicates the name of the server to which the NetExtender client is connected. |
| Client IP | Indicates the IP address assigned to the NetExtender client. |
| Sent | Indicates the amount of traffic the NetExtender client has transmitted since initial connection. |
| Received | Indicates the amount of traffic the NetExtender client has received since initial connection. |
| Throughput | Indicates the current NetExtender throughput rate. |

19. (Optional) To disconnect NetExtender, click **Disconnect**.

    ⓘ **TIP:** Closing the window (clicking the **x** icon in the upper right corner of the window) does not close the NetExtender session, but minimizes it to the system tray for continued operation.

# Enabling Network Logon (PreLogon) feature on NetExtender

**Perquisites:**

- NetExtender must be installed and enabled for Network Logon.

The Network Logon feature is a default enabled feature. This Network Logon feature will be enabled by default during NetExtender (NXsetupU.exe) and (MSI installer) installation.

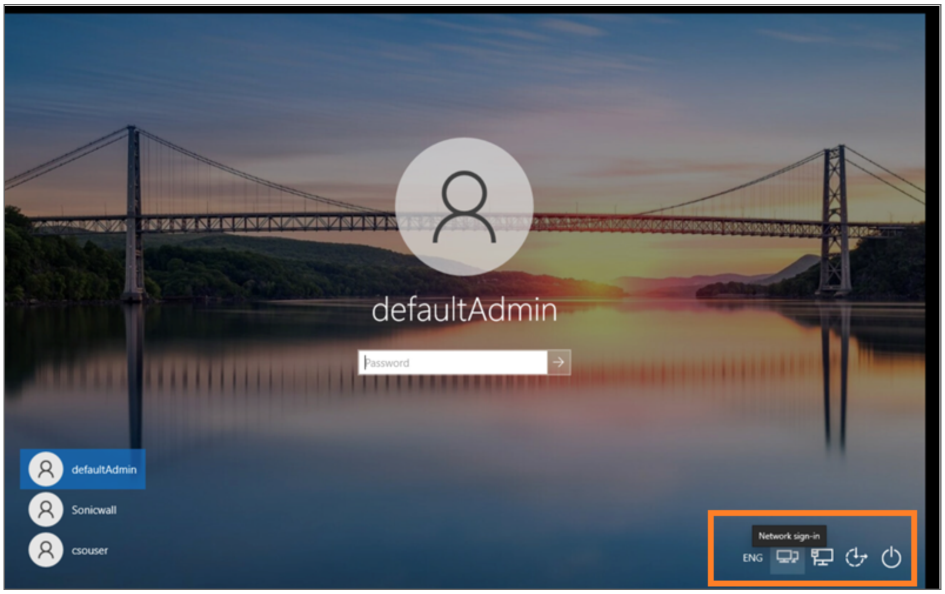
ⓘ **NOTE:** The Network Logon is a default, so if you update NetExtender from auto-update or upgraded, the Network Logon will be installed by default.

## Launching VPN Connection using Network Logon

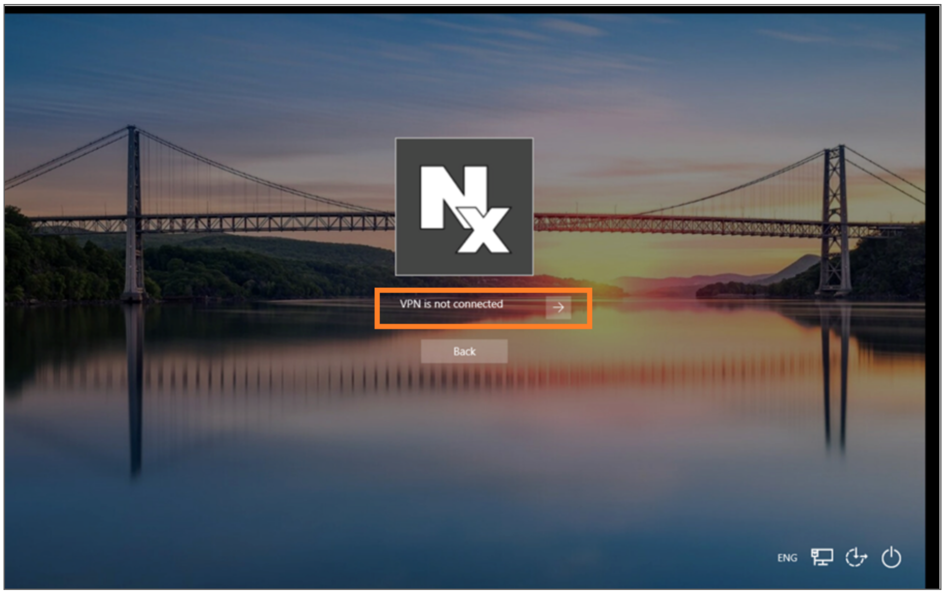
This section provides information on connecting to the VPN tunnel using Network Logon before log on to Windows accounts.

***To launch a VPN connection using Network Logon:***

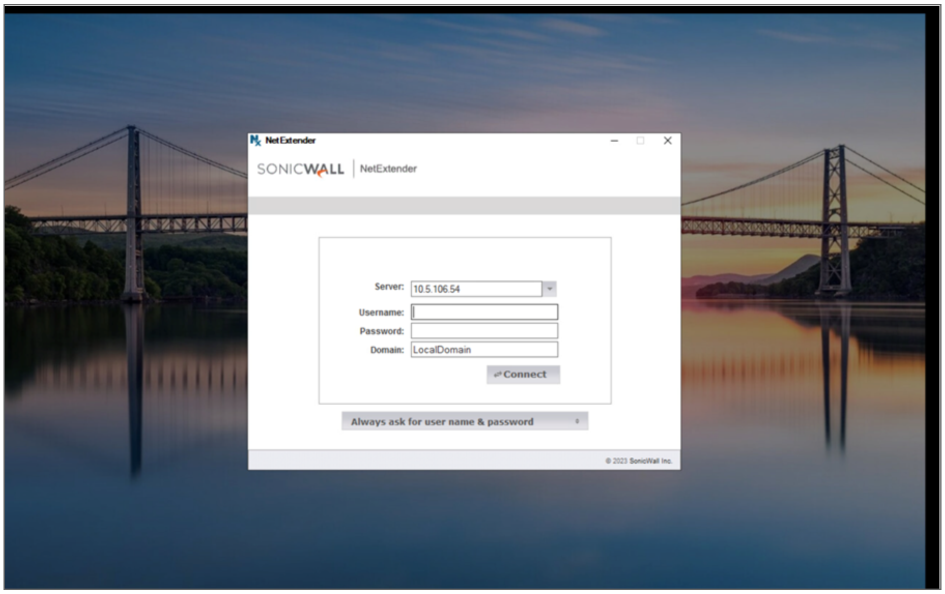
1. Select the **Network sign-in** icon.



2. **VPN is not connected** user interface displays, click the Arrow icon.



3. NetExtender user interface pop-up displays. Enter the details such as **Server**, **Username**, **Password**, and **Domain**.



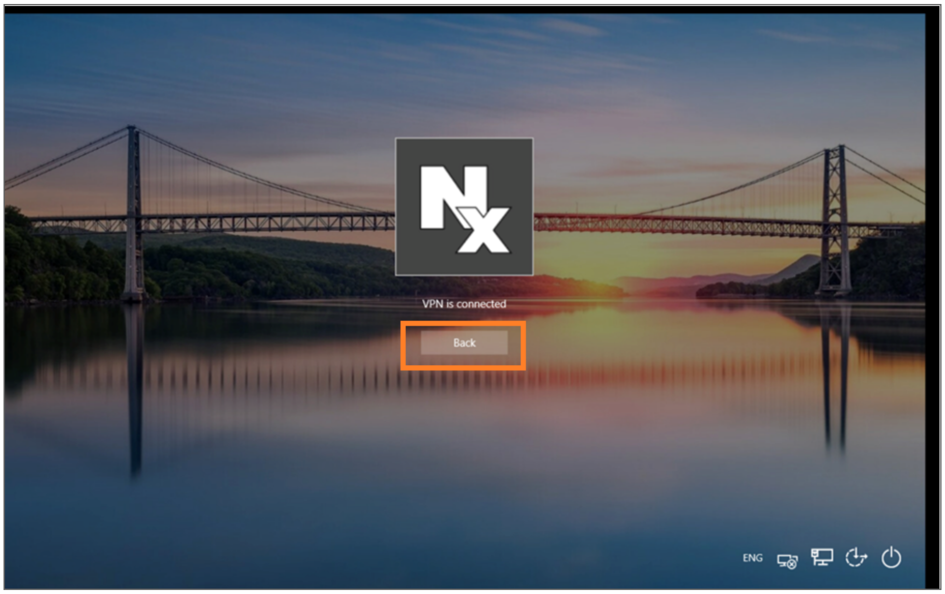
Server: 10.5.106.54

Username:

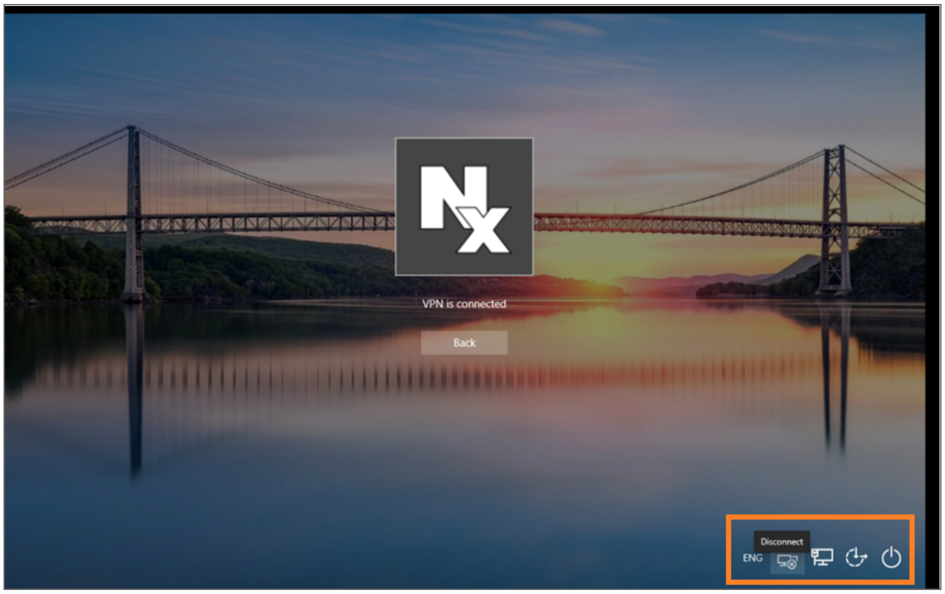
Password:

Domain: LocalDomain

4. Click **Connect** to establish the VPN connection. Once it is successfully connected, **VPN is connected** user interface displays.



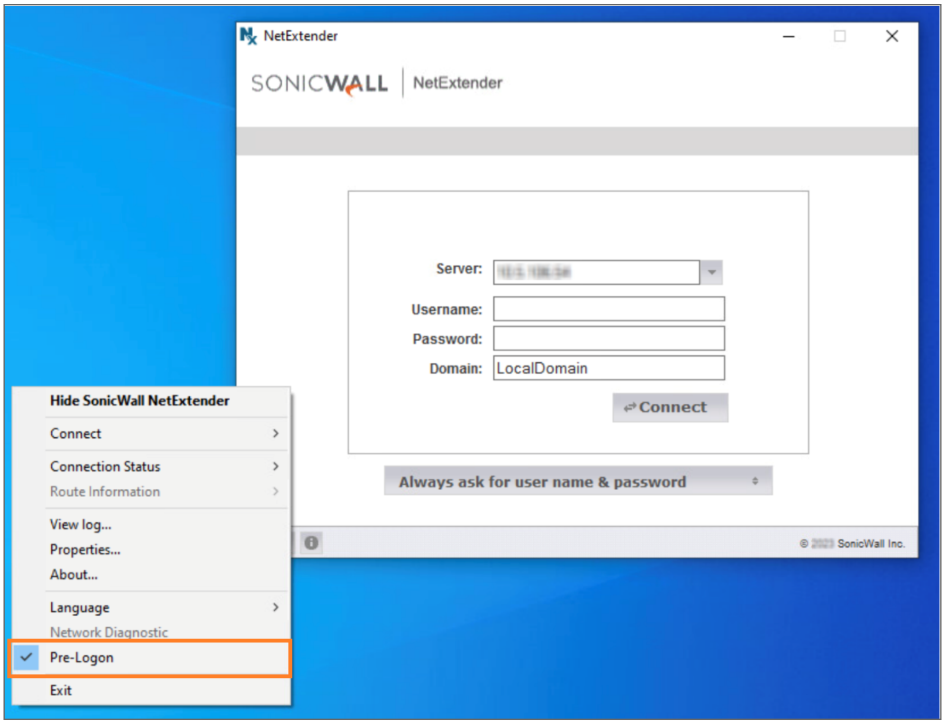
5. Click **Back** and proceeds with your windows credentials to login Windows user session.
6. If you want to disconnect your VPN at this stage, Click the **disconnect** icon to disconnect the VPN.



ⓘ **NOTE:** Network logon feature does not support EPC, NetExtender Upgrade, and SAML Authentication but once the Windows user logs in, VPN session is restarted with existing session and invokes all the functionality that was skipped earlier. Then NetExtender is re-established as per the new policy.

*To disable Network Logon (Pre-Logon):*

1. After the user logs on to Windows user session, Right-click on the NetExtender user interface pop-up display.
2. Uncheck the **Pre-Logon** option to disable the Network logon feature.



# Launching NetExtender Directly from Computer

After the first access and installation of NetExtender, you can launch NetExtender directly from your computer without first navigating to the Secure Mobile Access portal.

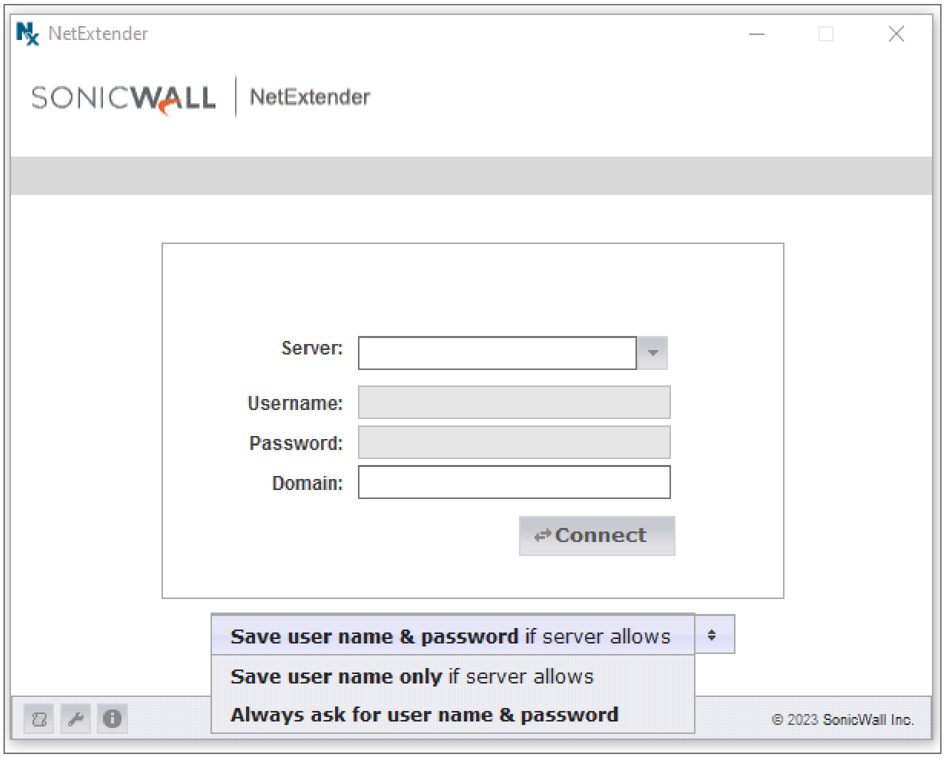
*To launch NetExtender:*

1. Navigate to **Start** > **All Programs**.
2. Select the SonicWall NetExtender folder, and then click **SonicWall NetExtender**.

   The NetExtender login window is displayed.
3. To display a list of recent SMA servers you have connected to, click the arrow.
4. Enter your username and password.
5. The last domain you connected to is displayed in the **Domain** field.

   ⓘ **NOTE:** The NetExtender client reports an error message if the provided domain is invalid when you attempt to connect. Note that the domain names are case-sensitive.

6. The drop-down menu at the bottom of the window provides three options for remembering your username and password:
   - Save user name only if server allows
   - Save user name and password if server allows
   - Always ask for user name & password


NetExtender
SONICWALL
NetExtender
Server:
Username:
Password:
Domain:
Connect
Save user name & password if server allows
Save user name only if server allows
Always ask for user name & password
© 2023 SonicWall Inc.

> ⓘ **TIP:** Having NetExtender save your user name and password can be a security risk and should not be enabled if there is a chance that other people could use your computer to access sensitive information on the network.

## Installing NetExtender with Microsoft Installer

Installing NetExtender through Microsoft Installer (MSI) supports the use of default profile settings during the installation process where the default server and default domain can be pre-filled along with additional options that control whether the server and domain fields can be edited by a standard user. This feature is designed specifically for administrators who want their default servers and domains pre-set during the installation process.

***To set the default server and domain during the NetExtender Installation with Microsoft Installer:***

1. On the **Default Profile Setting** page, enter the IP address of the **Default Server** and the location of the domain in **Default Domain**.
2. Disable **Allow connections to other profiles** to prevent users from connecting to other profiles.

   This setting disables the **Server** and **Domain** fields for editing on the login page of NetExtender.

# Configuring NetExtender Properties

NetExtender Properties feature helps you to manage the options including settings, log, languages, and so on.

**Topics:**

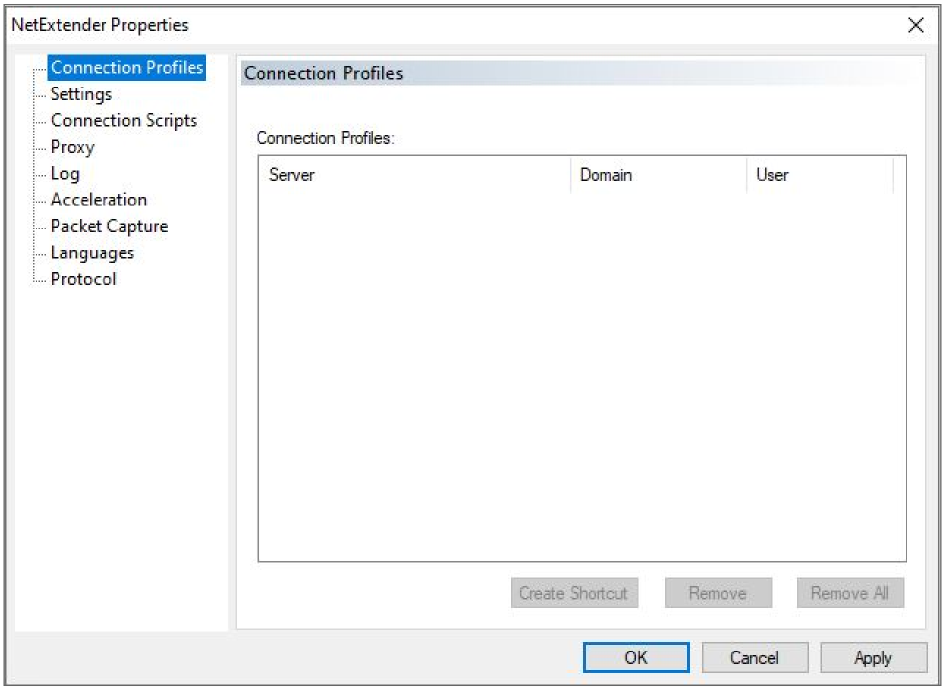
- Configuring Connection Profile Settings
- Configuring Settings
- Connection Scripts Settings
- Configuring Proxy Settings
- Configuring Log Settings
- Configuring Acceleration Settings
- Configuring Packet Capture Settings
- Configuring Languages Settings
- Configuring Protocol

# Configuring Connection Profile Settings

The **Connection Profiles** tab displays the Secure Mobile Access connection profiles you have used, including the IP address of the SMA server, the domain, and the username.

*__To manage the connection profiles settings:__*

1. Click to view the **NetExtender Properties** window and then click **Connection Profiles**.



2. Click **Create Shortcut** to create a shortcut on your desktop that launches NetExtender with the specified profile.
3. Click **Remove** to delete a profile.

   Or

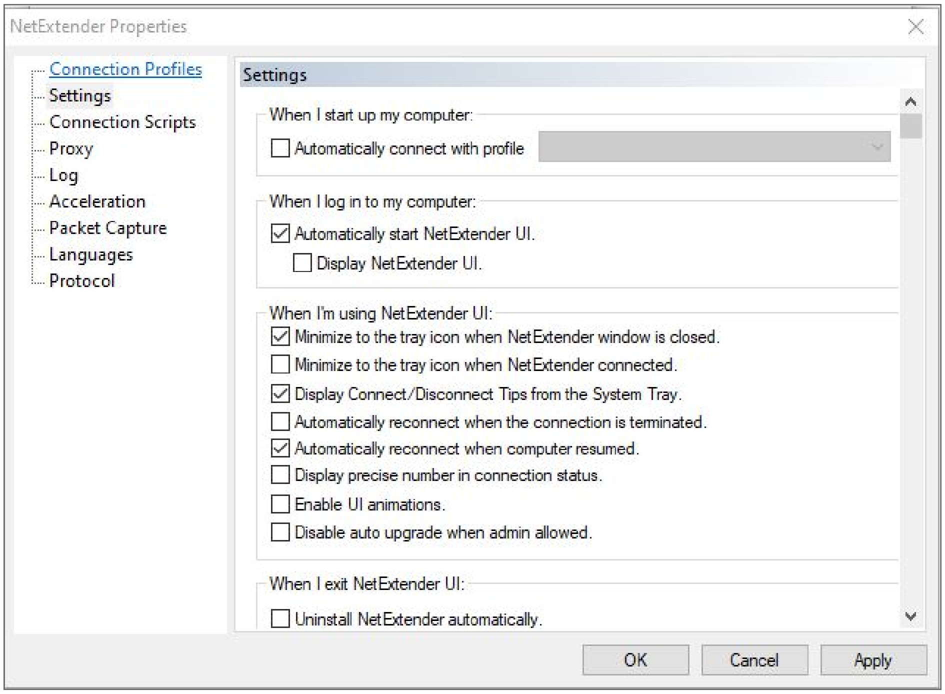
   Click **Remove All** to delete all the connection profiles.
4. Click **Apply** to save your changes.

## Configuring Settings

The **Settings** tab allows you to customize the behavior of NetExtender.

### *To manage the settings option:*

1. Click 🔧 to view the **NetExtender Properties** window and then click **Settings**.



Settings

When I start up my computer:

☐ Automatically connect with profile

When I log in to my computer:

☑ Automatically start NetExtender UI.

☐ Display NetExtender UI.

When I'm using NetExtender UI:

☑ Minimize to the tray icon when NetExtender window is closed.

☐ Minimize to the tray icon when NetExtender connected.

☑ Display Connect/Disconnect Tips from the System Tray.

☐ Automatically reconnect when the connection is terminated.

☑ Automatically reconnect when computer resumed.

☐ Display precise number in connection status.

☐ Enable UI animations.

☐ Disable auto upgrade when admin allowed.

When I exit NetExtender UI:

☐ Uninstall NetExtender automatically.

2. Enable the required settings.

| Setting | Description |
|---|---|
| **Automatically connect with profile** | NetExtender connects to a specific profile when starting up the computer device. |
| **Automatically start NetExtender UI** | NetExtender launches when you log in to your computer device. |
| **Display NetExtender UI** | Displays NetExtender login window |
| **Minimize to the tray icon when NetExtender window is closed** | Enable the NetExtender icon display in the system tray.<br>ⓘ **NOTE:** If this option is not selected, you can only access the NetExtender UI through Window's program menu. |
| **Minimize to the tray icon when NetExtender connected** | NetExtender icon display in the system tray when you are connected. |
| **Display Connect/Disconnect Tips from the System Tray** | NetExtender display tips when you hover the mouse pointer over the NetExtender icon. |
| **Automatically reconnect when the connection is terminated** | NetExtender attempts to reconnect when it loses connection. |
| **Automatically reconnect when computer resumed** | NetExtender reconnects when the computer resumes from a sleep or a locked mode. |
| **Display precise number in connection status** | Displays precise byte value information in the connection status. |
| **Enable UI animations** | Enables the sliding animation effects in the UI. |
| **Disable auto upgrade when admin allowed** | Eanbles auto upgrades |
| **Uninstall NetExtender automatically** | NetExtender uninstalls every time you end a session |
| **Disconnect an active connection** | NetExtender logs out of all of your SSL VPN sessions when you exit a NetExtender session. |

| Setting | Description |
|---|---|
| **Uninstall EPC Agent automatically** | End Point Control Agent gets uninstalled when NetExtender is uninstalled from the system. |

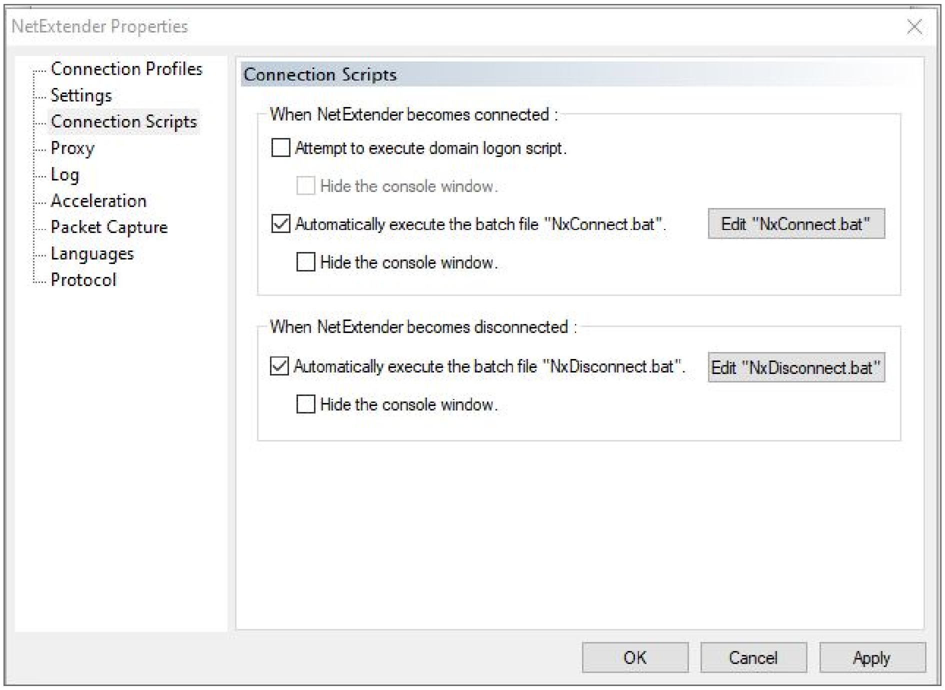
3. Click **OK** to save your changes.

## Connection Scripts Settings

Secure Mobile Access provides users with the ability to run batch file scripts when NetExtender connects and disconnects. The scripts can be used to map or disconnect network drives and printers, launch applications, or open files or websites.

***To manage the connection scripts options:***

1. Click to view the **NetExtender Properties** window and then click **Connection Scripts**.



Connection Scripts

When NetExtender becomes connected :

☐ Attempt to execute domain logon script.

☐ Hide the console window.

☑ Automatically execute the batch file "NxConnect.bat".

☐ Hide the console window.

When NetExtender becomes disconnected :

☑ Automatically execute the batch file "NxDisconnect.bat".

☐ Hide the console window.

2. Enable the required settings.

| Settings | Description |
|---|---|
| **Attempt to execute domain logon script** | Enabling this setting, allows the NetExtender to contact the domain controller and execute the login script.<br>ⓘ **NOTE:** Enabling this feature might cause connection delays while remote client’s printers and drives are mapped. Make sure the domain controller and any machines in the logon script are accessible through NetExtender routes. |
| **Hide the console window** | Enable to close the DOS console window while the script runs. |
| **Automatically execute the batch file “NxConnect.bat”** | Enabling this setting, runs the script when NetExtender connects. |
| **Automatically execute the batch file “NxDisconnect.bat.** | Enabling this setting, runs the script when NetExtender disconnects. |

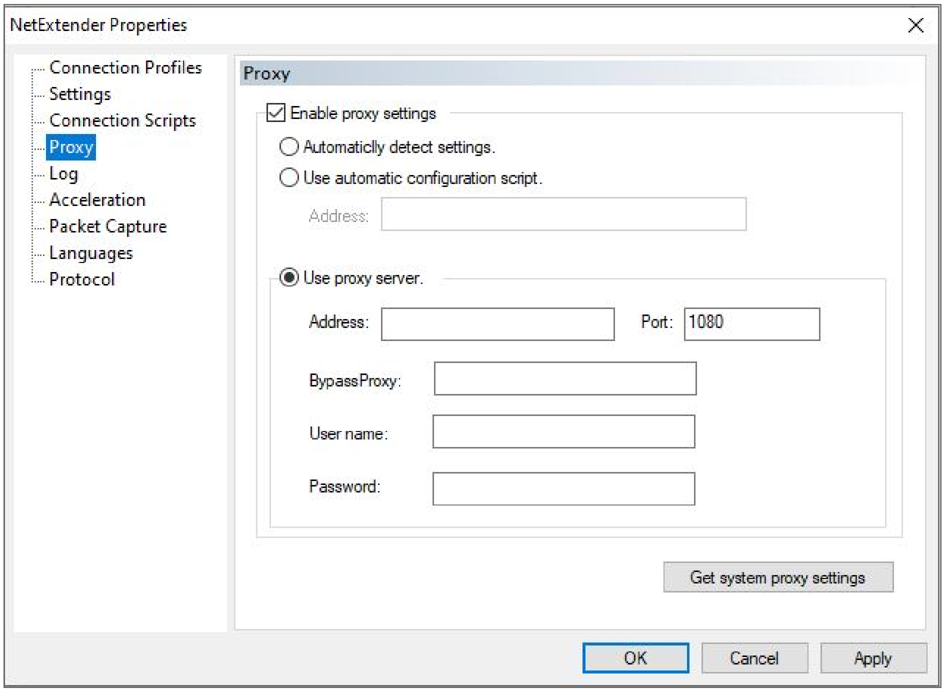
3. Click **OK** to save your changes.

## Configuring Proxy Settings

Secure Mobile Access supports NetExtender sessions using proxy configurations. Currently, only HTTPS proxy is supported. When launching NetExtender from the Web portal, if your browser is already configured for proxy access, NetExtender automatically inherits the proxy settings.

*To manage the proxy settings options:*

1. Click to view the **NetExtender Properties** window and then click **Proxy**.



☑ Enable proxy settings

○ Automaticly detect settings.

○ Use automatic configuration script.

Address:

● Use proxy server.

Address: Port: 1080

BypassProxy:

User name:

Password:

2. Select **Enable proxy settings**.

3. Select the required settings.

| Setting | Description |
|---|---|
| **Automatically detect settings** | To use this setting, the proxy server must support Web Proxy Auto Discovery Protocol (WPAD)) that can push the proxy settings script to the client automatically. |
| **Use automatic configuration script** | If you know the location of the proxy settings script, select this option and enter the URL of the scrip in the Address field. |
| **Use proxy server** | Select this option to enter the Address and Port of the proxy server. |
| **BypassProxy** | Enter an IP address or domain in the **BypassProxy** field to allow direct connections to those addresses that bypass the proxy server. If required, enter **User name** and **Password** for the proxy server.<br>ⓘ \| **NOTE:** If you have not entered the **User name** and **Password**, then **Properties** window is displayed, and you might need to enter the **User name** and **Password** when you connect for first time. |

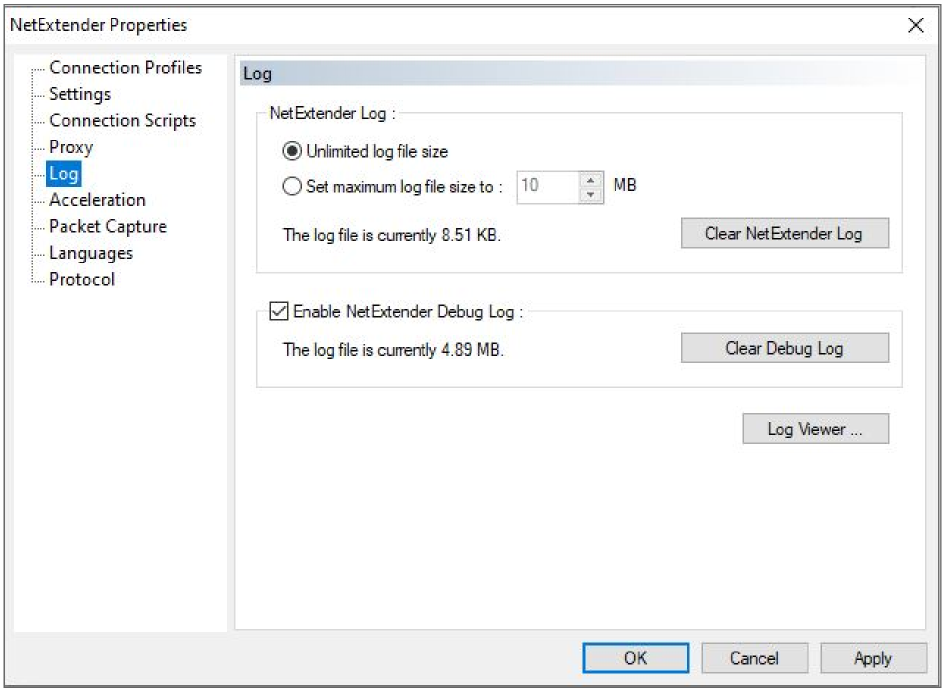
4. Click **Apply** to save your changes.

# Configuring Log Settings

The Log tab provides the basic control over the NetExtender Log and Debug Log.

***To manage the Log options:***

1. Click to view the **NetExtender Properties** window and then click **Log**.



NetExtender Properties

Log

NetExtender Log :

● Unlimited log file size

○ Set maximum log file size to : 10 MB

The log file is currently 8.51 KB.

☑ Enable NetExtender Debug Log :

The log file is currently 4.89 MB.

2. Select the required settings.

| Settings | Description |
|---|---|
| **Unlimited log file size** | Enable to establish the size of the NetExtender Log |
| **Set maximum log file size to** | To set a maximum size, use the adjoining arrows. |
| **Clear NetExtender Log** | To clear the NetExtender Log |
| **Clear Debug Log** | To clear the debug log.<br>ⓘ **NOTE:** Select **Enable NetExtender Log** to enable **Clear Debug Log**. |
| **Log Viewer** | To view the current NetExtender log. |

3. Click **OK** to save the changes.

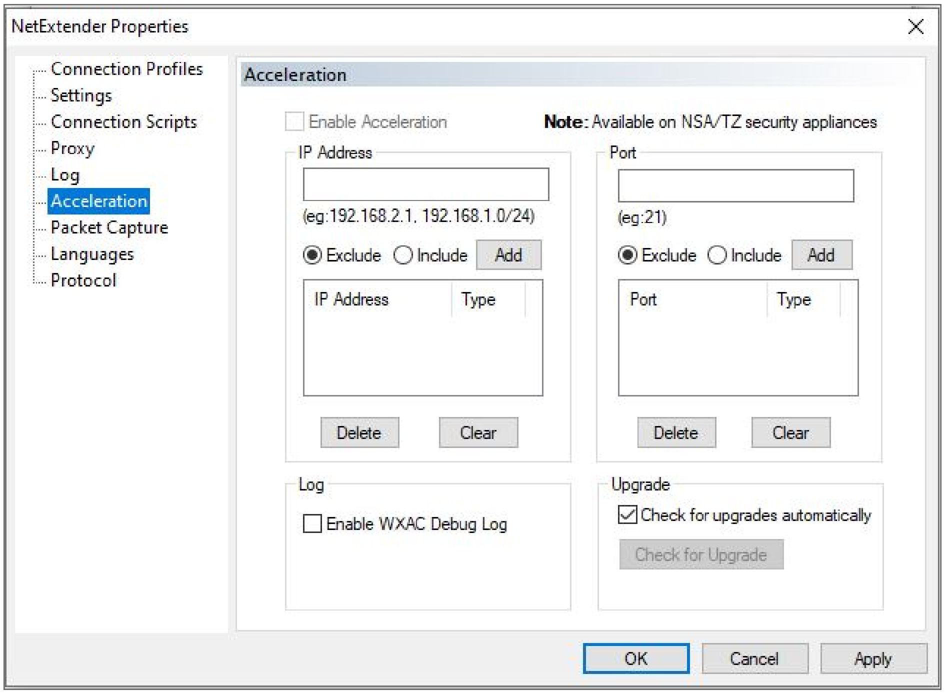
# Configuring Acceleration Settings

The Acceleration Settings tab allows you to accelerate IP and port to ensure high performance.

ⓘ | **NOTE:** Acceleration is supported only on Gen6.

***To manage the Acceleration settings:***

1. Click  to view the **NetExtender Properties** window and then click **Acceleration**.



NetExtender Properties

- Connection Profiles
- Settings
- Connection Scripts
- Proxy
- Log
- Acceleration
- Packet Capture
- Languages
- Protocol

Acceleration

□ Enable Acceleration **Note:** Available on NSA/TZ security appliances

IP Address
(eg:192.168.2.1, 192.168.1.0/24)
● Exclude ○ Include Add

| IP Address | Type |
|---|---|

Delete Clear

Port
(eg:21)
● Exclude ○ Include Add

| Port | Type |
|---|---|

Delete Clear

Log
□ Enable WXAC Debug Log

Upgrade
☑ Check for upgrades automatically
Check for Upgrade

OK Cancel Apply

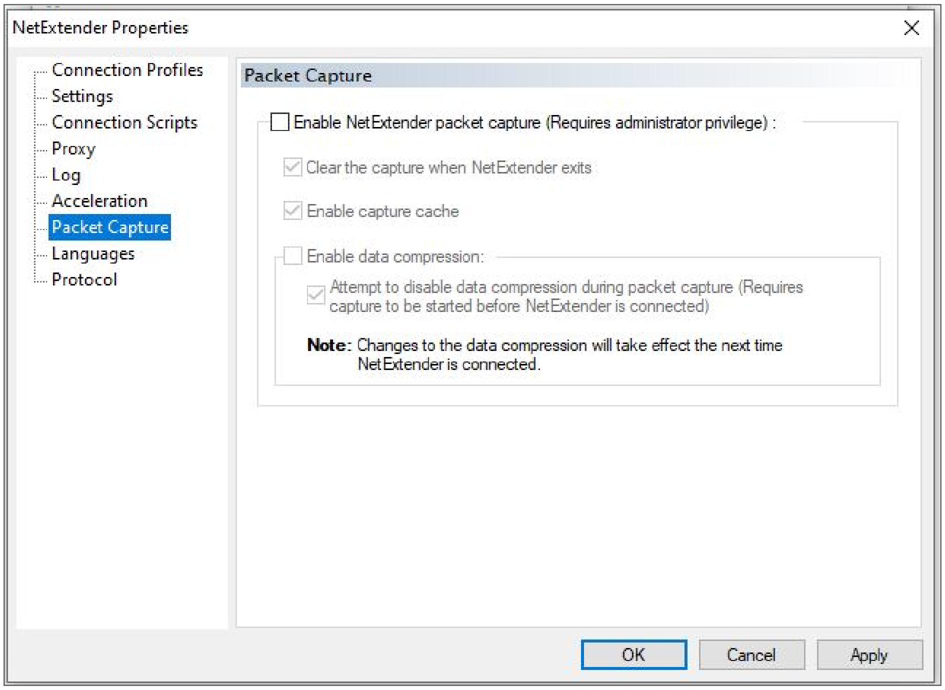
2. Select **Enable Acceleration** to enable the IP Address acceleration and enter the IP address. You can include or exclude the IP Address as required.
3. Specify the Port number and select **Check for upgrades** automatically to enable upgrades. You can include or exclude the Ports as required.
4. Optionally, you can select the **Enable WXAC Debug log** checkbox, if required.
5. Click **OK** to save your changes.

## Configuring Packet Capture Settings

The **Packet Capture** tab allows you to enable and disable packet capture and data compression on NetExtender. You must have Administrator privileges to change packet capture settings.

***To manage the Packet Capture settings:***

1. Click to view the **NetExtender Properties** window and then click **Packet Capture**.



Packet Capture

□ Enable NetExtender packet capture (Requires administrator privilege) :

☑ Clear the capture when NetExtender exits

☑ Enable capture cache

□ Enable data compression:

☑ Attempt to disable data compression during packet capture (Requires capture to be started before NetExtender is connected)

**Note:** Changes to the data compression will take effect the next time NetExtender is connected.

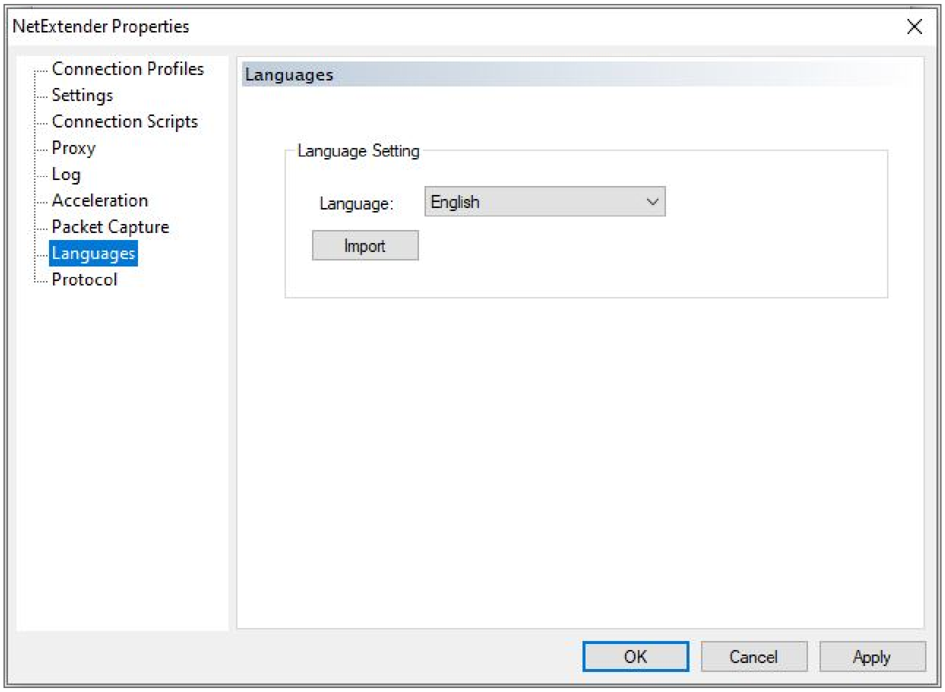
2. To enable packet capture, select **Enable NetExtender packet capture**.
3. Select **Clear the capture when NetExtender exits** to clear all captured packet data when NetExtender exits.
4. Select **Enable capture cache** to clear all captured packet data when NetExtender exits.
5. Select **Enable data compression** to enable data compression of captured packets.
6. Select **Attempt to disable data compression during packet capture**.if packet capture is enabled when NetExtender connects and you want to disable data compression immediately.
7. Click **OK** to save the changes.

# Configuring Languages Settings

The **Languages** tab allows you to define your language settings and import other packs on NetExtender.

***To manage the Language settings:***

1. Click 🔧 to view the **NetExtender Properties** window and then click **Advanced**.



Language: English

2. The **Language** drop-down list allows you to select the available languages on NetExtender.

   ⓘ | **NOTE:** The default language is English. After you select a language from the drop-down list, click **OK**.

3. Restart NetExtender for the new language to be applied.

4. Click **Import** to upload a new language pack to NetExtender.

   The languages packs must be in the .ZIP format. Select the language pack you want to import.

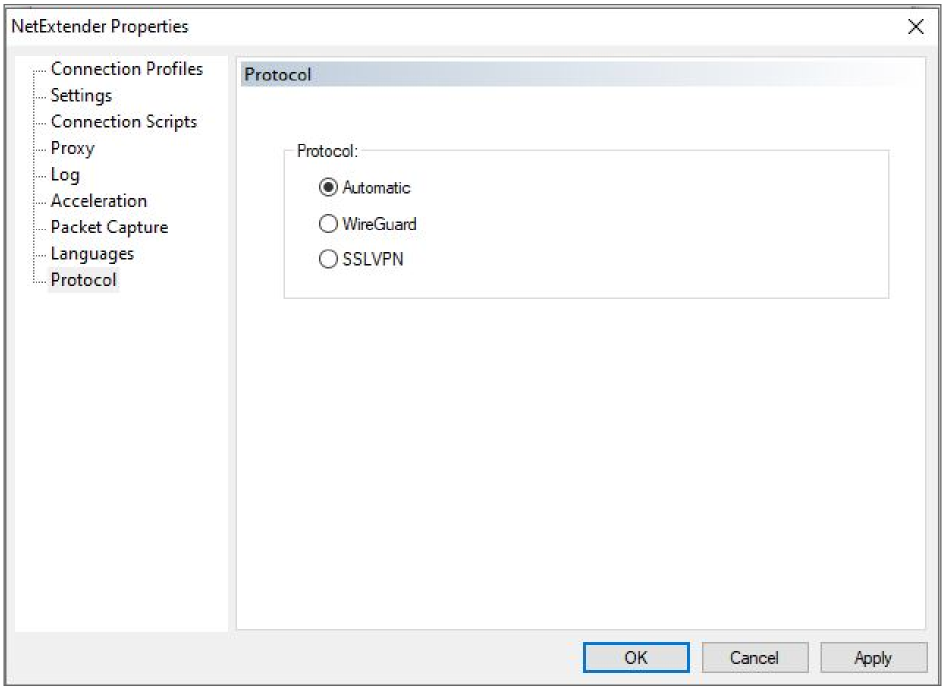
5. Click **Open**.

   After the import, the language displays in the Language drop-down list.

6. Click **OK** to save your changes.

# Configuring Protocol

Within the **NetExtender Properties** dialog box, click the **Protocol** heading in the menu on the left panel. The available options allow you to select your protocol on NetExtender.



Protocol:

● Automatic

○ WireGuard

○ SSLVPN

***To configure Protocol:***

1. 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.
2. Click **OK**.

# Installing NetExtender on Linux

Secure Mobile Access supports NetExtender on Linux. To use NetExtender on your Linux system, your system must meet the following prerequisites:

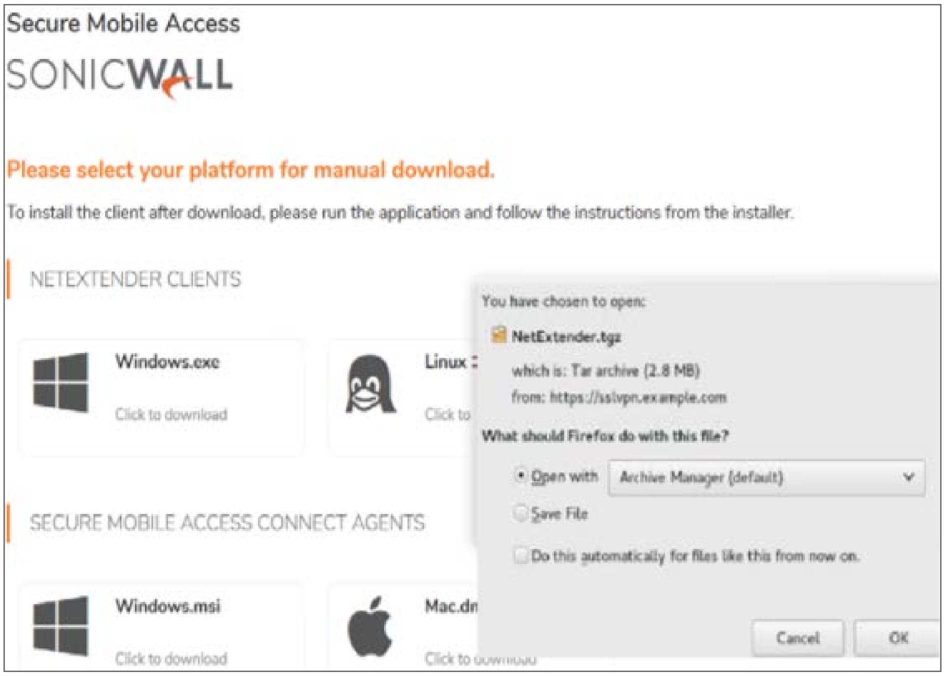
- i386-compatible distribution of Linux
- Linux Fedora Core 36 or later, Ubuntu 20.04 or later, or OpenSUSE 10.3 or later, Red Hat Enterprise Linux 8.x and later, and CentOS8.x and later

***To install NetExtender on your Linux system:***

1. Log in to the Workplace portal.
2. Click **NetExtender**.

A pop-up window indicates that you have chosen to open a `.tgz` file.

3. Click **OK** to save it to your default download directory.



Secure Mobile Access

SONICWALL

Please select your platform for manual download.

To install the client after download, please run the application and follow the instructions from the installer.

NETEXTENDER CLIENTS

Windows.exe

Click to download

Linux :

Click to

SECURE MOBILE ACCESS CONNECT AGENTS

Windows.msi

Click to download

Mac.dr

Click to download

You have chosen to open:

NetExtender.tgz

which is: Tar archive (2.8 MB)

from: https://sslvpn.example.com

What should Firefox do with this file?

● Open with [Archive Manager (default)]

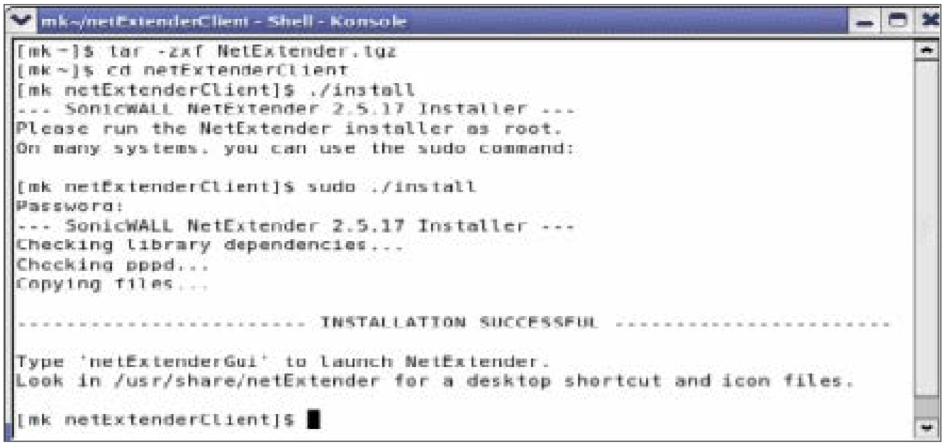
○ Save File

□ Do this automatically for files like this from now on.

Cancel OK

ⓘ **NOTE:** You must be logged in as root to install NetExtender, although many Linux systems allows the `sudo ./install` command to be used if you are not logged in as root.

4. To install NetExtender from the CLI, navigate to the directory where you saved the .tgz file and enter the `tar -zxf NetExtender.tgz` command.



mk~/netExtenderClient - Shell - Konsole

```
[mk ~]$ tar -zxf NetExtender.tgz
[mk ~]$ cd netExtenderClient
[mk netExtenderClient]$ ./install
--- SonicWALL NetExtender 2.5.17 Installer ---
Please run the NetExtender installer as root.
On many systems, you can use the sudo command:

[mk netExtenderClient]$ sudo ./install
Password:
--- SonicWALL NetExtender 2.5.17 Installer ---
Checking library dependencies...
Checking pppd...
Copying files...

----------------------- INSTALLATION SUCCESSFUL -----------------------

Type 'netExtenderGui' to launch NetExtender.
Look in /usr/share/netExtender for a desktop shortcut and icon files.

[mk netExtenderClient]$ █
```

5. Enter the `cd netExtenderClient/` command.

6. Enter `su -C “ ./install"` to install NetExtender.

7. Enter your system password.

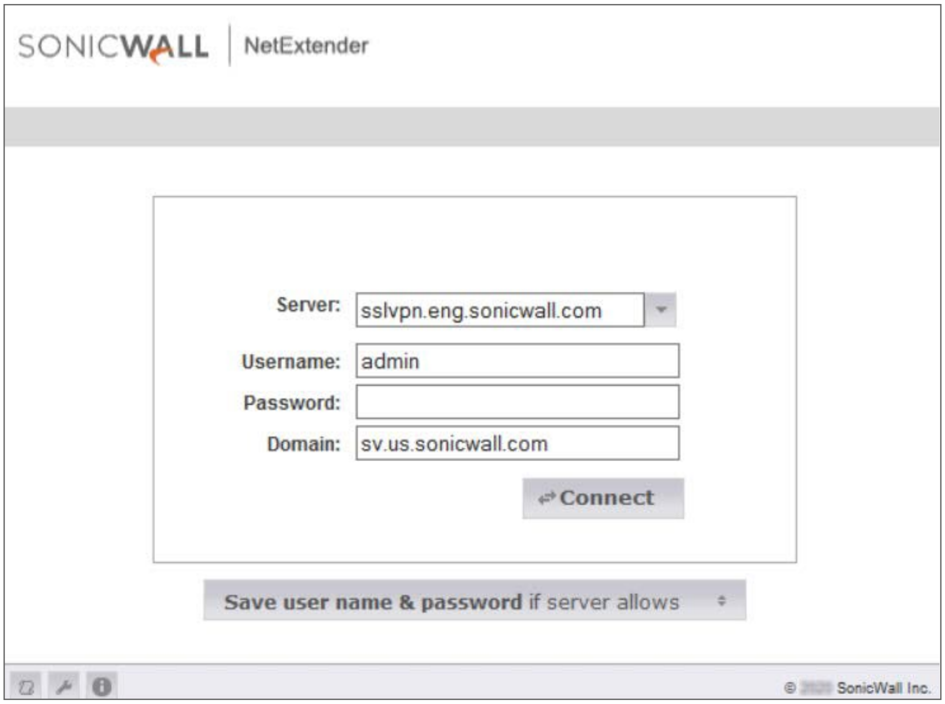
8. The installer asks if you want non-root users to be able to run NetExtender. Enter either **y** for yes or **n** for no.

   ⓘ | **NOTE:** To allow non-root users to run NetExtender, the installer sets PPPD to run as root. This could be considered a security risk.

# Using NetExtender on Linux

***To use NetExtender on a Linux computer:***

1. After NetExtender is installed, there are two methods to launch it:
   - Click the NetExtender icon in the Applications menu, under either the **Internet** or **Network** category.
   - Enter the `netExtenderGui` command.
2. The first time you connect, you must enter the SMA server name in the **Server** field.


SONICWALL | NetExtender
Connect
Save user name & password if server allows
© [redacted] SonicWall Inc.

Server: sslvpn.eng.sonicwall.com

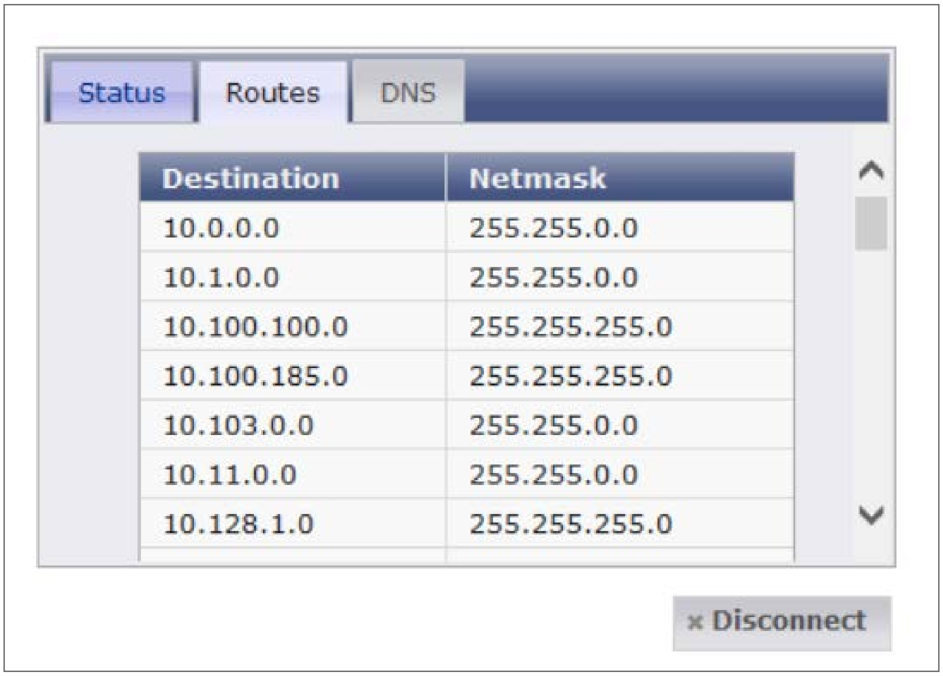
Username: admin

Password:

Domain: sv.us.sonicwall.com

3. Enter your username and password.
4. The first time you connect, you must enter the **Domain name**.

   ⓘ | **NOTE:** The domain name is case-sensitive. NetExtender remembers the domain name in the future.
5. To view the NetExtender routes, select the **Routes** tab in the main **NetExtender** window.



| Destination | Netmask |
|---|---|
| 10.0.0.0 | 255.255.0.0 |
| 10.1.0.0 | 255.255.0.0 |
| 10.100.100.0 | 255.255.255.0 |
| 10.100.185.0 | 255.255.255.0 |
| 10.103.0.0 | 255.255.0.0 |
| 10.11.0.0 | 255.255.0.0 |
| 10.128.1.0 | 255.255.255.0 |

6. To view the NetExtender DNS server information, select the **DNS** tab in the main **NetExtender** window.

3

# Using NetExtender

This chapter describes how to use NetExtender on the various supported platforms:

- Viewing the NetExtender Log
- Disconnecting NetExtender
- Upgrading NetExtender
- Changing Passwords
- Authentication Methods
- Uninstalling NetExtender
- Verifying NetExtender operation from the System Tray
- Using the NetExtender Command Line Interface

## Viewing the NetExtender Log

The NetExtender log displays information on NetExtender session events. The log file name is saved as `NetExtender.dbg` stored in `C:\Program Files\SonicWall\SSLVPN\NetExtender`.

1. To view the NetExtender log, log in to the NetExtender and click .
2. To view details of a log message, double-click a log entry,

   Or

   Go to **View** > **Log Detail** to open the log detail pane.
3. To save the log, click the **Export** icon.

   Or

   Go to **Log** > **Export**.
4. To filter the log to display entries from a specific duration of time, go to the Filter menu and select the cutoff threshold.
5. To filter the log by type of entry, go to **Filter** > **Level** and select one of the level categories.

The available options are **Fatal**, **Error**, **Warning**, and **Info**, in descending order of severity. The log displays all entries that match or exceed the severity level. For example, when selecting the **Error** level, the log displays all **Error** and **Fatal** entries, but not **Warning** or **Info** entries.

> ⓘ **NOTE:** It could take several minutes for the Debug Log to load. During this time, the Log window is not accessible, although you can open a new Log window while the Debug Log is loading.

6. To clear the log, click **Log** > **Clear Log**.

# Disconnecting NetExtender

***To disconnect NetExtender:***

1. Right click the NetExtender icon in the system tray to display the NetExtender icon menu and click **Disconnect**.

   Or

   You can also disconnect by double-clicking on the NetExtender icon to open the NetExtender window and then click **Disconnect**.

   The NetExtender session disconnects after few seconds.

   When NetExtender is disconnected, the NetExtender window displays and gives you the option to either Reconnect or Close NetExtender.

# Upgrading NetExtender

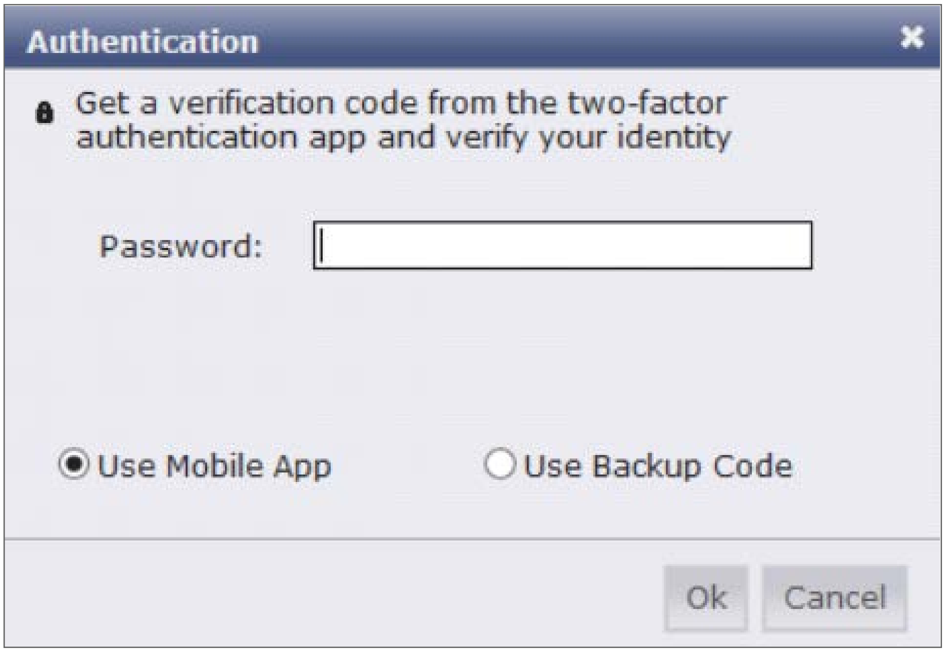
NetExtender automatically notifies users when an updated version of NetExtender is available. Users are prompted to click **OK** and NetExtender downloads and installs the update from the SMA security appliance.

# Changing Passwords

Before connecting to the new version of NetExtender, users might be required to reset their password by suppling their old password, along with providing and re-verifying a new one.

# Authentication Methods

NetExtender supports various two factor authentication methods, including one-time password, RSA, and Vasco, and authentications in mobile applications using Google, Microsoft, and Duo. If an Administrator has configured one-time passwords to be required to connect through NetExtender, you are asked to provide this information before connecting.


Authentication

Get a verification code from the two-factor authentication app and verify your identity

Password:

● Use Mobile App ○ Use Backup Code

If an Administrator has configured RSA pin-mode authentication to be required to connect through NetExtender, users are asked whether they want to create their own pin, or receive one that is system-generated.

After the pin has been accepted, you must wait for the token to change before logging in to NetExtender with the new passcode.

During authentication, the SMA server can be configured by the Administrator to request a client certificate. In this case, users must select a client certificate to use when connecting.

# Uninstalling NetExtender

The NetExtender utility is automatically installed on your computer. To remove NetExtender, click **Start** > **All Programs**, click **SonicWall NetExtender**, and then click **Uninstal**l.

You can also configure NetExtender to automatically uninstall when your session is disconnected.

***To configure NetExtender to automatically uninstall when your session is disconnected:***

1. Right click the NetExtender icon in the system tray and click **Properties** window is displayed.
2. Click the **Settings** tab.
3. Select **Uninstall NetExtender automatically** to have NetExtender uninstall every time you end a session.
4. Click **Apply**.

# Verifying NetExtender operation from the System Tray

To view options in the NetExtender system tray, right-click the NetExtender icon in the system tray. The following are some tasks you can complete with the system tray.

- **Displaying Route Information**: To display the routes that NetExtender has installed on your system, click the **Route Information** option in the system tray menu. The system tray menu displays the default route and the associated subnet mask.
- **Displaying Connection Information**: You can display connection information by mousing over the NetExtender icon in the system tray.

# Using the NetExtender Command Line Interface

ⓘ | **NOTE:** The NetExtender command line interface is only available on Windows platforms.

***To launch the NetExtender CLI:***

1. Launch the Windows Command Prompt by going to the **Start** > **Run**, enter `cmd`, and click **OK**.
2. Change directory to where NetExtender is installed. Type `cd Program Files\SonicWall\SSL-VPN\NetExtender`.

   ⓘ | **NOTE:** The specific command directory could be different on your computer. Use Windows Explorer to find the directory path where NetExtender is located.

**NETEXTENDER CLI COMMANDS AND OPTIONS**

| Command | Option | Description |
|---|---|---|
| NECLI addprofile | | Creates a NetExtender profile |
| | -s server | The IP address or hostname of the SMA server |
| | -u user-name | The username for the account. |
| | -p password | The password for the account. |
| | -d domain-name | The domain to connect to. |
| NECLI connect | | Initiates a NetExtender session. |
| | -s server | The IP address or hostname of the SMA server. |
| | -u user-name | The username for the account. |
| | -p password | The password for the account. |
| | -d domain-name | The domain to connect to. |

| Command | Option | Description |
|---|---|---|
| | - clientcertificatethumb thumb | The SSL Client Certificate thumbprint value. |
| | - clientcertificatename name | The SSL Client Certificate name. |
| NECLI deleteprofile | | Deletes a saved NetExtender profile. |
| | -s server | The IP address or hostname of the SMA server. |
| | -u user-name | The username for the account. |
| | -d domain-name | The domain to connect to. |
| NECLI disconnect | | Disconnects |
| | timeout | (Optional) Timeout duration, after which the session is disconnected. |
| NECLI displayprofile | | Displays all NetExtender profiles. |
| | -s server | (Optional) Displays only the profiles that are saved for the specified server |
| | -u user-name | (Optional) Displays only the profiles that are saved for the specified user name. |
| | -d domain-name | (Optional) Displays only the profiles that are saved for the specified domain name. |
| NECLI queryproxy | | Checks the connect to the proxy server. |
| NECLI reconnect | | Attempts to reconnect to the server. |
| NECLI showstatus | | Displays the status of the current NetExtender session. |
| NECLI setproxy | | Configures proxy settings for NetExtender |
| | -t [0 \|1 \| 2 \| 3] | There are three options for setting proxy settings:<br>0 - Disable proxy.<br>1 - Automatically detects proxy settings. The proxy server must support Web Proxy Auto Discovery Protocol (WPAD).<br>2 - Uses a proxy configuration script.<br>3 - Manually configure the proxy server |
| | -s proxy address | The address of the proxy script or proxy server |
| | -o port | The port number. |
| | -u user name | The user name for the proxy server. |
| | -p password | The password name for the proxy server. |
| | -b bypass-proxy | Bypasses the previously configured proxy settings. |
| | -save | Saves the proxy settings. |
| NECLI viewlog | | Displays the NetExtender log. |

4

# NetExtender Troubleshooting

This chapter provides you help with troubleshooting information for the SonicWall NetExtender utility.

## NETEXTENDER CANNOT BE INSTALLED

- Problem: NetExtender cannot be installed.
- Solution:
  1. Check your OS Version, NetExtender only supports Linux OpenSUSE, CentOS, Red Hat Enterprise in addition to Fedora Core and Ubuntu. An i386-compatible Linux distribution is required, along with Sun Java 1.6.0_10+.
  2. Check that the user has administrator privilege, NetExtender can only install/work under the user account with administrator privileges.
  3. Check if ActiveX has been blocked by Internet Explorer or third-party blockers.
  4. If the problem still exists, obtain the following information and send to support:
     - The version of Secure Mobile Access NetExtender Adapter from Device Manager.
     - The log file located at `C:\Program files\SonicWall\SMA\NetExtender.dbg`.
     - The event logs in the **Event Viewer** found under the **Windows**> **Control Panel** >**Administrator Tools** folder. Select Applications and System events and use the **Action /Save Log File** menu to save the events in a log file.

## NETEXTENDER CONNECTION ENTRY CANNOT BE CREATED

- Problem: NetExtender connection entry cannot be created.
- Solution:
  1. Navigate to Device Manager and check if the Secure Mobile Access NetExtender Adapter has been installed successfully. If not, delete the adapter from the device list, reboot the machine and install NetExtender again.
  2. Navigate to Windows Service manager under **Control Panel** > **Administrator Tools** > **Services**. Look for the **Remote Access Auto Connection Manager** and **Remote Access Connection Manager** to see if those two services have been started. If not, set them to automatic start, reboot the machine, and install NetExtender again.
  3. Check if there is another dial-up connection in use. If so, disconnect the connection, reboot the machine and install NetExtender again.

4. If problem still exists, obtain the following information and send them to support:
    - The version of Secure Mobile Access NetExtender Adapter from Device Manager.
    - The log file located at `C:\Program files\SonicWall\SMA\NetExtender.dbg`.
    - The event logs in **Control Panel** > **Administrator Tools** > **Event Viewer**. Select **Applications and System** events and use the **Action /Save Log File** menu to save the events in a log file.

## NETEXTENDER CANNOT CONNECT

- Problem: NetExtender cannot connect.
- Solution:
    1. Navigate to **Device Manager** and check if the Secure Mobile Access NetExtender Adapter has been installed successfully. If not, delete the adapter from the device list, reboot the machine and install NetExtender again.
    2. Navigate to Network connections to check if the Secure Mobile Access NetExtender Dialup entry has been created. If not, reboot the machine and install NetExtender again.
    3. Check if there is another dial-up connection in use, if so, disconnect the connection and reboot the machine and connect NetExtender again.
    4. If problem still exists, obtain the following information and send them to support:
        - The version of Secure Mobile Access NetExtender Adapter from Device Manager.
        - The log file located at `C:\Program files\SonicWall\SMA\NetExtender.dbg`.
        - The event logs in **Control Panel** > **Administrator Tools** > **Event Viewer**. Select **Applications and System** events and use the **Action /Save Log File** menu to save the events in a log file.

## NETEXTENDER BSOD AFTER CONNECTED

- Problem: NetExtender BSOD after connected
- Solution:
    1. Uninstall NetExtender, reboot machine, reinstall the latest version NetExtender.
    2. Obtain the following information and send them to support:
        - The version of Secure Mobile Access NetExtender Adapter from Device Manager.
        - The log file located at `C:\Program files\SonicWall\SMA\NetExtender.dbg`.
        - Windows memory dump file located at `C:\Windows\MEMORY.DMP`. If you cannot find this file, then open **System Properties** click **Startup** and **Recovery Settings** under the **Advanced** tab.
        - Select **Complete Memory Dump**, **Kernel Memory Dump** or **Small Memory Dump** in the **Write Debugging Information** drop-down list. You should also reproduce the BSOD to get the dump file.

- The event logs in **Control Panel** > **Administrator Tools** > **Event Viewer**. Select **Applications** and **System Events** and use the **Action /Save Log File** menu to save the events in a log file.

# Related Topics:

- https://www.sonicwall.com/support/search-results/?searchtext=netextender+config
- https://www.sonicwall.com/support/knowledge-base/dns-ip-not-getting-updated-on-netextender-after-changing-the-dns-on-the-box/180619133203645/
- https://www.sonicwall.com/support/knowledge-base/enable-proxy-settings-in-the-netextender/170505506096633/
- https://www.sonicwall.com/support/knowledge-base/sonicwall-net-extender-service-is-grayed-out-with-9-0-x-msi-file/190314150454875/
- https://www.sonicwall.com/support/knowledge-base/damaged-version-of-net-extender-error-message-on-windows-10/170707194358278/
- https://www.sonicwall.com/support/knowledge-base/unable-to-log-in-with-netextender-while-using-german-special-characters/170502534932980/

5

# 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

Secure Mobile Access  NetExtender Feature Guide
Updated - September 2023
Software Version - 10.2
232-005421-00 Rev B

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.

## 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