SonicWALL SSL VPN 5.0: NetExtender

Document Scope
This document describes how to plan, design, implement, and manage the NetExtender feature in a SonicWALL SSL VPN Environment. This document contains the following sections:

- “Feature Overview” section on page 1
- “Configuring NetExtender” section on page 5
- “Using NetExtender” section on page 14

Feature Overview
This section provides an introduction to the NetExtender feature. This section contains the following subsections:

- “What is NetExtender?” section on page 1
- “Benefits” section on page 1
- “NetExtender Concepts” section on page 2
- “Supported Platforms” section on page 4

What is NetExtender?
SonicWALL NetExtender is a transparent software application for users that enables 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
NetExtender can provide remote users with full access to your protected internal network. The experience is virtually identical to that delivered by traditional IPSec VPN clients, but NetExtender does not require any manual client installation. Instead, the stand-alone NetExtender client is automatically installed on a remote user’s PC by an installer. NetExtender then automatically launches and connects a virtual adapter for SSL-secure point-to-point access to permitted hosts and subnets on the internal network.
NetExtender Concepts

The following sections describe advanced NetExtender concepts:

- Stand-Alone Client
- Multiple Ranges and Routes
- NetExtender with External Authentication Methods
- PPP Server IP Address
- Tunnel All Mode
- Connection Scripts
- Proxy Configuration
- IPv6 Support

Stand-Alone Client

SonicWALL SSL VPN release 1.5 introduced a stand-alone NetExtender application. NetExtender is a browser-based application that provides comprehensive remote access without requiring users to manually download and install the application. The first time a user launches NetExtender, an installer installs the NetExtender stand-alone client 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 will first uninstall the old NetExtender and install the new version.

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

Multiple Ranges and Routes

Multiple range and route support for NetExtender enables network administrators to easily segment groups and users without the need of configuring firewall rules to govern access. This user segmentation allows for granular control of access to the network—allowing users access to necessary resources while restricting access to sensitive resources to only those who require it.

For networks that do not require segmentation, client addresses and routes can be configured globally as in the SSL VPN 1.0 version of NetExtender. The following sections describe the new multiple range and route enhancements:

- IP Address User Segmentation
- Client Routes

IP Address User Segmentation

Administrators can now 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 SonicWALL SSL-VPN appliance assigns IP addresses. When assigning an IP address to a NetExtender client, the SonicWALL SSL-VPN appliance uses the following hierarchy of ranges:

1. An IP address from the range defined in the user’s local profile.
2. An IP address from the range defined in the group profile the user belongs to.
3. 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. Client routes can also be configured 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 to specify that all possible permutations of user, group, and global routes can be applied (such as only group routes, only user routes, group and global routes, user, group, and global routes, etc.). This segmentation is controlled by the Add Global NetExtender Client routes and Add Group NetExtender Client routes checkboxes.

NetExtender with External Authentication Methods

Networks that use an external authentication server will not configure local usernames on the SonicWALL SSL-VPN appliance. In such cases, when a user is successfully authenticated, a local user account is created with the Add Global NetExtender Client routes and Add Group NetExtender Client routes settings enabled.

PPP Server IP Address

In the SonicWALL SSL VPN 1.0 release, the first IP address in the global NetExtender address pool was used for the PPP server. In SonicWALL SSL VPN 1.5 release, 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. Therefore, all IP addresses in the global NetExtender address pool will be used for NetExtender clients.

Tunnel All Mode

Tunnel All mode routes all traffic to and from the remote user over the SSL VPN NetExtender tunnel—including traffic destined to the remote users local network. This is accomplished by adding the following routes to all remote client’s route table:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Subnet mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>128.0.0.0</td>
</tr>
<tr>
<td>128.0.0.0</td>
<td>128.0.0.0</td>
</tr>
</tbody>
</table>

NetExtender also adds routes for the local networks of all connected Network Connections. These routes have higher metrics than any existing routes to force traffic destined for the local network over the SSL VPN 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 SSL VPN tunnel.

Tunnel All mode can be configured at the global, group, and user levels.
Connection Scripts

SonicWALL SSL VPN release 2.0 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 configure NetExtender Connection Scripts, perform the following tasks. NetExtender Connection Scripts can support any valid batch file commands.

Proxy Configuration

(Windows only) SonicWALL SSL VPN release 2.1 introduces support for 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.

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

IPv6 Support

(Windows only) NetExtender supports IPv6 client connections from Windows systems running Vista or newer, and from Linux clients.

Supported Platforms

SonicWALL SSL VPN 5.0 NetExtender is available on the following SonicWALL security appliances:

- SRA 4200
- SRA 1200

For information on supported client systems, see the “User Prerequisites” section on page 14.
Configuring NetExtender

The following sections describe how to configure NetExtender on the SonicWALL SSL-VPN appliance:

- “Viewing NetExtender Status” section on page 5
- “Configuring the Global NetExtender IP Address Range” section on page 6
- “Configuring Global NetExtender Settings” section on page 7
- “Adding NetExtender Client Routes” section on page 7
- “Configuring User-Level NetExtender Settings” section on page 8
- “Configuring Group-Level NetExtender Settings” section on page 11
- “Configuring NetExtender Options for the Portal” section on page 13

Viewing NetExtender Status

The NetExtender > Status window displays information about active NetExtender sessions. It also enables you to disconnect active NetExtender sessions.

![NetExtender Status Window](image)

<table>
<thead>
<tr>
<th>Status Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The user name.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the workstation on which the user is logged into.</td>
</tr>
<tr>
<td>Login Time</td>
<td>The time when the user first established connection with the SonicWALL SSL-VPN appliance expressed as day, date, and time (HH:MM:SS).</td>
</tr>
<tr>
<td>Logged in</td>
<td>The amount of time since the user first established connection with the SonicWALL SSL-VPN appliance expressed as number of days and time (HH:MM:SS).</td>
</tr>
<tr>
<td>Logout</td>
<td>Provides the administrator the ability to logout a NetExtender session.</td>
</tr>
</tbody>
</table>
Configuring the Global NetExtender IP Address Range

The global NetExtender IP range defines the IP address pool from which addresses will be assigned to remote users during NetExtender sessions. The address range can be specified for both IPv4 and IPv6. The range needs to be large enough to accommodate the maximum number of concurrent NetExtender users you wish to support plus one (for example, 15 users, require 16 addresses like 192.168.200.100 to 192.168.200.115).

The range should fall within the same subnet as the interface to which the SSL-VPN appliance is connected, and in cases where there are other hosts on the same segment as the SSL-VPN appliance, it must not overlap or collide with any assigned addresses. You can determine the correct subnet in one of the following ways:

- You may leave the NetExtender range at the default (192.168.200.100 to 192.168.200.200).
- Select a range that falls within your existing DMZ subnet. For example, if your DMZ uses the 192.168.50.0/24 subnet, and you want to support up to 30 concurrent NetExtender sessions, you could use 192.168.50.220 to 192.168.50.250, providing they are not already in use.
- Select a range that falls within your existing LAN subnet. For example, if your LAN uses the 192.168.168.0/24 subnet, and you want to support up to 10 concurrent NetExtender sessions, you could use 192.168.168.240 to 192.168.168.250, providing they are not already in use.

To specify your global NetExtender address range, perform the following steps:

**Step 1** Navigate to the NetExtender > Client Settings page.

**Step 2** Under NetExtender Client Address Range, supply a beginning client IPv4 address in the Client Address Range Begin field.

**Step 3** Supply an ending client IPv4 address in the Client Address Range End field.

**Step 4** Under NetExtender Client IPv6 Address Range, supply a beginning client IPv6 address in the Client Address Range Begin field.

**Step 5** Supply an ending client IPv6 address in the Client Address Range End field.

**Step 6** Click Apply.

**Step 7** The Status message displays Update Successful. Restart for current clients to obtain new addresses.
Configuring Global NetExtender Settings

To configure global NetExtender client settings, which customize the behavior of NetExtender when users connect and disconnect, perform the following steps:

**Step 1** Navigate to the NetExtender > Client Settings page.

**Step 2** The following options can be enabled or disabled for all users:

- **Exit Client After Disconnect** - The NetExtender client exits when it becomes disconnected from the SSL-VPN server. To reconnect, users will have to either return to the SSL-VPN portal or launch NetExtender from their Programs menu. This option applies to all supported platforms except Android smartphones.

- **Uninstall Client After Exit** - The NetExtender client automatically uninstalls when the user exits the client user interface. This occurs when the user right-clicks the NetExtender tray icon and selects Exit. To reconnect, users will have to return to the SSL-VPN portal. This option only applies to Windows clients. It does not apply to Windows Mobile, Android, Mac, or Linux clients.

- **Create Client Connection Profile** - The NetExtender client will create a connection profile recording the SSL-VPN Server name, the Domain name and optionally the username and password.

**Step 3** The User Name & Password Caching options provide flexibility in allowing users to cache their usernames and passwords in the NetExtender client. The three options are Allow saving of user name only, Allow saving of user name & password, and Prohibit saving of user name & password. These options enable administrators to balance security needs against ease of use for users.

**Step 4** Click Apply.

Adding NetExtender Client Routes

The NetExtender client routes are passed to all NetExtender clients and are used to govern which private networks and resources remote users can access via the SSL VPN connection.

**Caution** With group access policies, all traffic is allowed by default. This is the opposite of the default behavior of SonicWALL Unified Threat Management (UTM) appliances, where all inbound traffic is denied by default. If you do not create policies for your SSL-VPN appliance then all NetExtender users may be able to access all resources on your internal network(s).

Additional allow and deny policies may be created by destination address or address range and by service type.

**Note** The most specific policy will take precedence over less specific policies. For example, a policy that applies to only one IP address will have priority over a policy that applies to a range of IP addresses. If there are two policies that apply to a single IP address, then a policy for a specific service (for example RDP) will take precedence over a policy that applies to all services.

User policies take precedence over group policies and group policies take precedence over global policies, regardless of the policy definition. A user policy that allows access to all IP addresses will take precedence over a group policy that denies access to a single IP address.
To add NetExtender client routes, perform the following steps:

**Step 1** Navigate to the NetExtender > Client Routes page.

**Step 2** Select Enabled from the Tunnel All Mode pulldown menu to force all traffic for this user—including traffic destined to the remote users’ local network—over the SSL VPN NetExtender tunnel.

**Step 3** Click the Add Client Route button. The Add Client Route dialog box displays.

**Step 4** Type the IP address or IPv6 address of the trusted network to which you would like to provide access with NetExtender in the Destination Network field. For example, if you are connecting to an existing DMZ with the network 192.168.50.0/24 and you want to provide access to your LAN network 192.168.168.0/24, you would enter 192.168.168.0.

**Note** You can optionally tunnel-all SSL VPN client traffic through the NetExtender connection by entering 0.0.0.0 for the Destination Network and Subnet Mask.

**Step 5** For an IPv4 destination network, type the subnet mask in the Subnet Mask/Prefix field using decimal format (255.0.0.0, 255.255.0.0, or 255.255.255.0). For an IPv6 destination network, type the prefix, such as 112.

**Step 6** Click Add.

**Step 7** Repeat steps 1 through 5 for all necessary routes.

**Configuring User-Level NetExtender Settings**

All of the global settings for NetExtender (IP address ranges, client routes, and client connection settings) can be configured at the user and group levels. Multiple range and route support for NetExtender enables network administrators to easily segment groups and users without the need of configuring firewall rules to govern access. This user segmentation allows
for granular control of access to the network—allowing users access to necessary resources while restricting access to sensitive resources to only those who require it. To configure custom settings for individual users, perform the following steps:

**Step 1** Navigate to the Users > Local Users page.
**Step 2** Click on the configure icon for the user you want to edit. The Edit User window is launched.
**Step 3** Click on the NX Settings tab.

### Configuring User Client IP Address Range

**Step 1** To configure an IP address range for this user, enter the beginning of the range in the Client Address Range Begin: field and the end of the range in the Client Address Range End: field.

**Step 2** To configure an IPv6 address range for this user, enter the beginning of the range in the Client IPv6 Address Range Begin: field and the end of the range in the Client IPv6 Address Range End: field.

**Step 3** To give this user the same IP address or IPv6 address every time the user connects, enter the IP address in both fields.

**Tip** Unless more than one user will be using the same username, which is not recommended, there is no need to configure more than one IP address for the user client IP address range.

**Step 4** Click Ok.
Configuring User Net Extender Settings

The following NetExtender settings can be configured for the user:

- **Exit Client After Disconnect** - The NetExtender client exit when it becomes disconnected from the SSL-VPN server. To reconnect, users will have to either return to the SSL-VPN portal or launch NetExtender from their Programs menu. This option applies to all supported platforms except Android smartphones.

- **Uninstall Client After Disconnect** - The NetExtender client automatically uninstalls when it becomes disconnected from the SSL-VPN server. To reconnect, users will have to return to the SSL-VPN portal. This option only applies to Windows clients. It does not apply to Windows Mobile, Android, Mac, or Linux clients.

- **Create Client Connection Profile** - The NetExtender client will create a connection profile recording the SSL-VPN Server name, the Domain name and optionally the username and password.

- The **User Name & Password Caching** options provide flexibility in allowing users to cache their usernames and passwords in the NetExtender client. The three options are **Allow saving of user name only**, **Allow saving of user name & password**, and **Prohibit saving of user name & password**. These options enable administrators to balance security needs against ease of use for users.

To have the user inherent the NetExtender settings from the group it belongs to (or from the global NetExtender settings if the user does not belong to a group), select **Use Group Settings** for any of the above options.

Configuring User NetExtender Routes

**Step 1** To add a NetExtender client route that will only be added to this user, click the **NX Routes** tab in the **Edit User Settings** window.

![NetExtender Routes Tab](image)

**Step 2** **Add Client Route...** button.

**Step 3** Type the IP address or IPv6 address of the trusted network to which you would like to provide access with NetExtender in the **Destination Network** field.
Configuring NetExtender

**Step 4** For an IPv4 destination network, type the subnet mask in the **Subnet Mask/Prefix** field using decimal format (255.0.0.0, 255.255.0.0, or 255.255.255.0). For an IPv6 destination network, type the prefix, such as 112.

**Step 5** Click **Add**.

**Step 6** Repeat steps 1 through 5 for all necessary routes.

**Step 7** Select **Enabled** from the **Tunnel All Mode** pulldown menu to force all traffic for this user—including traffic destined to the remote users’ local network—over the SSL VPN NetExtender tunnel.

**Step 8** To also add the global NetExtender client routes (which are configured on **NetExtender > Client Routes** page) to the user, check the **Add Global NetExtender Client Routes** checkbox.

**Step 9** To also add the group NetExtender client routes for the group the user belongs to, check the **Add Group NetExtender Client Routes** checkbox. Group NetExtender routes are configured on the **NetExtender** tab of the **Edit Group** window, which is accessed through the **Users > Local Groups** page.

**Step 10** Click **Ok**.

---

**Note**
When using an external authentication server, local usernames are not typically configured on the SonicWALL SSL-VPN appliance. In such cases, when a user is successfully authenticated, a local user account is created with the **Add Global NetExtender Client routes** and **Add Group NetExtender Client routes** settings enabled.

---

**Configuring Group-Level NetExtender Settings**

Multiple range and route support for NetExtender enables network administrators to easily segment groups and users without the need of configuring firewall rules to govern access. This user segmentation allows for granular control of access to the network—allowing users access to necessary resources while restricting access to sensitive resources to only those who require it. To configure custom settings for groups, perform the following steps:

**Step 1** Navigate to the **Users > Local Groups** page.

**Step 2** Click on the configure icon for the group you want to edit. The **Edit Group** window is launched.

**Step 3** Click on the **NX Settings** tab.

**Configuring Group Client IP Address Range**

**Step 1** To configure an IP address range for this group, enter the beginning of the range in the **Client Address Range Begin** field and the end of the range in the **Client Address Range End** field.

**Step 2** To configure an IPv6 address range for this group, enter the beginning of the range in the **Client IPv6 Address Range Begin** field and the end of the range in the **Client IPv6 Address Range End** field.

**Step 3** Click **Ok**.
Configuring Group Net Extender Settings

The following NetExtender settings can be configured for the user:

- **Exit Client After Disconnect** - The NetExtender client exit when it becomes disconnected from the SSL-VPN server. To reconnect, users will have to either return to the SSL-VPN portal or launch NetExtender from their Programs menu. This option applies to all supported platforms except Android smartphones.

- **Uninstall Client After Disconnect** - The NetExtender client automatically uninstalls when it becomes disconnected from the SSL-VPN server. To reconnect, users will have to return to the SSL-VPN portal. This option only applies to Windows clients. It does not apply to Windows Mobile, Android, Mac, or Linux clients.

- **Create Client Connection Profile** - The NetExtender client will create a connection profile recording the SSL-VPN Server name, the Domain name and optionally the username and password.

- **User Name & Password Caching** options provide flexibility in allowing users to cache their usernames and passwords in the NetExtender client. The three options are Allow saving of user name only, Allow saving of user name & password, and Prohibit saving of user name & password. These options enable administrators to balance security needs against ease of use for users.

To have the user inherit the NetExtender settings from the global NetExtender settings, select Use Global Settings for any of the above options.

Configuring Group NetExtender Routes

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>To add a NetExtender client route that will only be added to users in this group, click the Add Client Route... button.</td>
</tr>
<tr>
<td>2</td>
<td>Type the IP address or IPv6 address of the trusted network to which you would like to provide access with NetExtender in the <strong>Destination Network</strong>: field.</td>
</tr>
<tr>
<td>3</td>
<td>For an IPv4 destination network, type the subnet mask in the <strong>Subnet Mask/Prefix</strong> field using decimal format (255.0.0.0, 255.255.0.0, or 255.255.255.0). For an IPv6 destination network, type the prefix, such as 112.</td>
</tr>
<tr>
<td>4</td>
<td>Click <strong>Add</strong>.</td>
</tr>
<tr>
<td>5</td>
<td>Repeat steps 1 through 5 for all necessary routes.</td>
</tr>
<tr>
<td>6</td>
<td>Select <strong>Enabled</strong> from the <strong>Tunnel All Mode</strong> pulldown menu to force all traffic for this user—including traffic destined to the remote users’ local network—over the SSL VPN NetExtender tunnel.</td>
</tr>
<tr>
<td>7</td>
<td>To also add the global NetExtender client routes (which are configured on NetExtender &gt; Client Routes page) to users in this group, check the <strong>Add Global NetExtender Client Routes</strong> checkbox.</td>
</tr>
<tr>
<td>8</td>
<td>Click <strong>Ok</strong>.</td>
</tr>
</tbody>
</table>
Configuring NetExtender Options for the Portal

On the virtual office portal, you can configure whether or not NetExtender is displayed and if you want NetExtender to automatically launch when users log in to the portal. To configure NetExtender portal options, perform the following steps:

Step 1 Navigate to the Portal > Portal Layouts page.

Step 2 Click on the configure icon for the portal you want to edit. The Portal Layout window is launched.

Step 3 Click on the Home Page tab.

Step 4 Uncheck the Display NetExtender checkbox to not allow users to access NetExtender through this portal.

Step 5 Check the Launch NetExtender after login button to have NetExtender automatically launch when users log in to the portal.

Step 6 Click Ok.
Using NetExtender

The following sections describe how to use NetExtender:

- "User Prerequisites" section on page 14
- "User Configuration Tasks" section on page 16
- "Verifying NetExtender Operation from the System Tray" section on page 33

User Prerequisites

See the following sections:

- "Windows Clients" on page 14
- "Windows Mobile Clients" on page 15
- "Macintosh Clients" on page 15
- "Linux Clients" on page 15
- "Android Smartphone Clients" on page 15

Windows Clients

Windows 32-bit or 64-bit clients must meet the following prerequisites in order to use NetExtender:

- One of the following platforms, 32-bit or 64-bit:
  - Windows 7
  - Windows Vista, Windows Vista Service Pack 1
  - Windows XP Home or Professional, Windows XP Service Pack 3
  - Windows 2000 Professional
- One of the following browsers:
  - Internet Explorer 6.0 and higher
  - Mozilla Firefox 2 and higher
  - Google Chrome
- To initially install the NetExtender client, the user must be logged in to the PC with administrative privileges.
- Downloading and running scripted ActiveX files must be enabled on Internet Explorer.
- If the SSL-VPN gateway uses a self-signed SSL certificate for HTTPS authentication, then it is necessary to install the certificate before establishing a NetExtender connection. If you are unsure whether 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 the Import Certificate button at the bottom of the Virtual Office home page.
Windows Mobile Clients

NetExtender supports the following Windows Mobile platforms:

- Windows Mobile 5 PocketPC version
- Windows Mobile 6 Professional/Classic version

Windows Mobile 5 Smart Phone version and Windows Mobile 6 Standard version are not currently supported.

Macintosh Clients

Macintosh clients must meet the following prerequisites in order to use NetExtender:

- MacOS X 10.5 and higher
- Java 1.5 and higher
- Both PowerPC and Intel Macs are supported.

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 8+
- Ubuntu 7+
- OpenSUSE 10.3+

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

Java is required as follows:

- Sun Java 1.5 and higher is required for using the NetExtender GUI.
  If you do not have Sun Java 1.5, you can use the command-line interface version of NetExtender.

Note
Open source Java Virtual Machines (VMs) are not currently supported.

Android Smartphone Clients

The NetExtender Android client is supported on rooted smartphones running the following versions of the Android operating system:

- 1.6 or higher

The NetExtender Android client is compatible with any SonicWALL SSL VPN firmware version that supports the NetExtender Linux client, specifically:

- SSL VPN 4.0 and higher

As new features are added, users must install the updated client to access all the features supported by the new firmware. Likewise, if a new client is used with older firmware, some client features may not be functional. For best results, the latest firmware should always be used with the latest client.
Using NetExtender

Note

Only rooted devices are supported for NetExtender Android in SonicWALL SSL VPN 5.0.

The rooting requirement is due to limitations and restrictions of the Android platform. A layer 3 VPN client like NetExtender requires root permission for certain necessary OS level operations. Until a future version of the Android OS provides a flexible API to do these operations without root access, the rooting requirement will remain.

Warning

Rooting your phone may void your warranty. Consult your contract or User’s Guide, or call your service provider for more information.

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 Using the Mozilla Firefox Browser” section on page 17
- “Installing NetExtender Using the Internet Explorer Browser” section on page 19

Windows Platform Usage
- “Launching NetExtender Directly from Your Computer” section on page 23
- “Configuring NetExtender Preferences” section on page 25
- “Configuring NetExtender Connection Scripts” section on page 27
- “Configuring Proxy Settings” section on page 29
- “Viewing the NetExtender Log” section on page 30
- “Disconnecting NetExtender” section on page 32
- “Upgrading NetExtender” section on page 32
- “Uninstalling NetExtender” section on page 32
- “Displaying Route Information” section on page 33
- “Displaying Connection Information” section on page 33
- “Using the NetExtender Command Line Interface” section on page 34

MacOS Platform
- “Installing NetExtender on MacOS” section on page 36
- “Using NetExtender on MacOS” section on page 37

Linux Platform
- “Installing and Using NetExtender on Linux” section on page 39

Windows Mobile Platform
- “Installing and Using NetExtender for Windows Mobile” section on page 43
Android Smartphone Platform
- “Installing NetExtender on Android Smartphones” section on page 46
- “Using NetExtender on Android Smartphones” section on page 49

Installing NetExtender Using the Mozilla Firefox Browser

To use NetExtender for the first time using the Mozilla Firefox browser, perform the following:

**Step 1** To launch NetExtender, first log in to the SSL-VPN portal.
**Step 2** Click the NetExtender button.

**Step 3** The first time you launch NetExtender, it will automatically install the NetExtender stand-alone application on your computer. If a warning message is displayed in a yellow banner at the top of your Firefox banner, click the Edit Options... button.
Step 4  The **Allowed Sites - Software Installation** window is displayed, with the address of the Virtual Office server in the address window. Click **Allow** to allow Virtual Office to install NetExtender, and click **Close**.

![Allowed Sites - Software Installation](image1.png)

Step 5  Return to the **Virtual Office** window and click **NetExtender** again.

Step 6  The **Software Installation** window is displayed. After a five second countdown, the **Install Now** button will become active. Click it.

Step 7  NetExtender is installed as a Firefox extension.

![Extensions](image2.png)
Step 8  When NetExtender completes installing, the **NetExtender Status** window displays, indicating that NetExtender successfully connected.

![NetExtender Status Window](image)

Closing the windows (clicking on the x icon in the upper right corner of the window) will not close the NetExtender session, but will minimize it to the system tray for continued operation.

Step 9  Review the following table to understand the fields in the **NetExtender Status** window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Indicates what operating state the NetExtender client is in, either Connected or Disconnected.</td>
</tr>
<tr>
<td>Server</td>
<td>Indicates the name of the server to which the NetExtender client is connected.</td>
</tr>
<tr>
<td>Client IP</td>
<td>Indicates the IP address assigned to the NetExtender client.</td>
</tr>
<tr>
<td>Sent</td>
<td>Indicates the amount of traffic the NetExtender client has transmitted since initial connection.</td>
</tr>
<tr>
<td>Received</td>
<td>Indicates the amount of traffic the NetExtender client has received since initial connection.</td>
</tr>
<tr>
<td>Duration</td>
<td>The amount of time the NetExtender has been connected, expressed as days, hours, minutes, and seconds.</td>
</tr>
</tbody>
</table>

Step 10  Additionally, a balloon icon in the system tray appears, indicating NetExtender has successfully installed.

![Balloon Icon](image)

Step 11  The NetExtender icon is displayed in the task bar.

**Installing NetExtender Using the Internet Explorer Browser**

In SonicWALL SSL VPN release 2.1, NetExtender is fully compatible with Microsoft Windows Vista and supports the same functionality as with other Windows operating systems.
Using NetExtender

**Note**
It may be necessary to restart your computer when installing NetExtender on Windows Vista.

Internet Explorer Prerequisites

It is recommended that you add the URL or domain name of your SSL-VPN server to Internet Explorer’s trusted sites list. This will simplify the process of installing NetExtender and logging in, by reducing the number of security warnings you will receive. To add a site to Internet Explorer’s trusted sites list, complete the following procedure:

**Step 1** In Internet Explorer, go to **Tools > Internet Options**.
**Step 2** Click on the **Security** tab.
**Step 3** Click on the **Trusted Sites** icon and click on the **Sites...** button to open the **Trusted sites** window.

**Step 4** Enter the URL or domain name of your SSL-VPN server in the **Add this Web site to the zone** field and click **Add**.
**Step 5** Click **OK** in the **Trusted Sites** and **Internet Options** windows.

Installing NetExtender from Internet Explorer

To use NetExtender for the first time using the Internet Explorer browser, perform the following:

**Step 1** To launch NetExtender, first log in to the SSL-VPN portal.
**Step 2** Click the **NetExtender** button.
Step 3 The first time you launch NetExtender, you must first add the SSL-VPN portal to your list of trusted sites. If you have not done so, the follow message will display.

Step 4 Click Instructions to add SSL-VPN server address into trusted sites for help.

Step 5 In Internet Explorer, go to Tools > Internet Options.

Step 6 Click on the Security tab.
Step 7  Click on the **Trusted Sites** icon and click on the **Sites...** button to open the **Trusted sites** window.

![Trusted Sites window](image)

Step 8  Enter the URL or domain name of your SSL-VPN server in the **Add this Web site to the zone** field and click **Add**.

Step 9  Click **Ok** in the **Trusted Sites** and **Internet Options** windows.

Step 10 Return to the SSL-VPN portal and click on the NetExtender button. The portal will automatically install the NetExtender stand-alone application on your computer. The NetExtender installer window opens.

![NetExtender installer](image)

Step 11 If an older version of NetExtender is installed on the computer, the NetExtender launcher will remove the old version and then install the new version.
Step 12 If the following warning message is displayed, click **Continue Anyway**. SonicWALL testing has verified that NetExtender is fully compatible with Windows 7, Vista, XP, 2000, Server 2003, and Server 2008.

![Hardware Installation Warning]

Step 13 When NetExtender completes installing, the **NetExtender Status** window displays, indicating that NetExtender successfully connected.

![NetExtender Status]

**Launching NetExtender Directly from Your Computer**

You can launch NetExtender directly from your computer without first navigating to the SSL-VPN portal. To launch NetExtender, complete the following procedure:

**Step 1** Navigate to **Start > All Programs**.

**Step 2** Select the **SonicWALL SSL-VPN NetExtender** folder, and then click on **SonicWALL SSL-VPN NetExtender**. The NetExtender login window is displayed.
Using NetExtender

Step 3  The IP address of the last SSL-VPN server you connected to is displayed in the **SSL-VPN Server** field. To display a list of recent SSL-VPN servers you have connected to, click on the arrow.

Step 4  Enter your username and password.

Step 5  The last domain you connected to is displayed in the **Domain** field.

Step 6  The pulldown menu at the bottom of the window provides three options for remembering your username and password:

- Save user name & password if server allows
- Save user name only if server allows
- Always ask for user name & password

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.
Configuring NetExtender Preferences

Complete the following procedure to configure NetExtender preferences:

**Step 1** Right click on the icon in the system tray and click on **Preferences...** The NetExtender Preferences window is displayed.

**Step 2** The **Connection Profiles** tab displays the SSL-VPN connection profiles you have used, including the IP address of the SSL-VPN server, the domain, and the username.

**Step 3** To create a shortcut on your desktop that will launch NetExtender with the specified profile, highlight the profile and click **Create Shortcut**.

**Step 4** To delete a profile, highlight it by clicking on it and then click the **Remove** buttons. Click the **Remove All** buttons to delete all connection profiles.

**Step 5** The **Settings** tab allows you to customize the behavior of NetExtender.
Step 6  To have NetExtender automatically connect when you start your computer, check the **Automatically connect with Connection Profile** checkbox and select the appropriate connection profile from the pulldown menu.

**Note**  Only connection profiles that allow you to save your username and password can be set to automatically connect.

Step 7  To have NetExtender launch when you log in to your computer, check the **Automatically start NetExtender UI**. NetExtender will start, but will only be displayed in the system tray. To have the NetExtender log-in window display, check the **Display NetExtender UI** checkbox.

Step 8  Select **Minimize to the tray icon when NetExtender window is closed** to have the NetExtender icon display in the system tray. If this option is not checked, you will only be able to access the NetExtender UI through Window’s program menu.

Step 9  Select **Display Connect/Disconnect Tips from the System Tray** to have NetExtender display tips when you mouse over the NetExtender icon.

Step 10  Select **Automatically reconnect when the connection is terminated** to have NetExtender attempt to reconnect when it loses connection.

Step 11  Select **Uninstall NetExtender automatically** to have NetExtender uninstall every time you end a session.

Step 12  Select **Disconnect an active connection** to have NetExtender log out of all of your SSL VPN sessions when you exit a NetExtender session.

Step 13  Click **Apply**.
Configuring NetExtender Connection Scripts

SonicWALL SSL VPN 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 configure NetExtender Connection Scripts, perform the following tasks.

**Step 1** Right click on the icon in the task bar and click on Preferences... The NetExtender Preferences window is displayed.

**Step 2** Click on Connection Scripts.

**Step 3** To enable the domain login script, select the Attempt to execute domain login script checkbox. When enabled, NetExtender will attempt to contact the domain controller and execute the login script.

**Note** Enabling this feature may 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 via NetExtender routes

**Step 4** To enable the script that runs when NetExtender connects, select the Automatically execute the batch file “NxConnect.bat” checkbox.

**Step 5** To enable the script that runs when NetExtender disconnects, select the Automatically execute the batch file “NxDisconnect.bat” checkbox.

**Step 6** To hide either of the console windows, select the appropriate Hide the console window checkbox. If this checkbox is not selected, the DOS console window will remain open while the script runs.

**Step 7** Click Apply.
Configuring Batch File Commands

NetExtender Connection Scripts can support any valid batch file commands. For more information on batch files, see the following Wikipedia entry: http://en.wikipedia.org/wiki/.bat. The following tasks provide an introduction to some commonly used batch file commands.

Step 1 To configure the script that runs when NetExtender connects, click the Edit “NxConnect.bat” button. The NxConnect.bat file is displayed.

Step 2 To configure the script that runs when NetExtender disconnects, click the Edit “NxDisconnect.bat” button. The NxConnect.bat file is displayed.

Step 3 By default, the NxConnect.bat file contains examples of commands that can be configured, but no actual commands. To add commands, scroll to the bottom of the file.

Step 4 To map a network drive, enter a command in the following format:

```
net use drive-letter:\server\share password /user:Domain\name
```

For example, to if the drive letter is z, the server name is engineering, the share is docs, the password is 1234, the user’s domain is eng and the username is admin, the command would be the following:

```
net use z:\engineering\docs 1234 /user:eng\admin
```

Step 5 To disconnect a network drive, enter a command in the following format:

```
net use drive-letter: /delete
```

For example, to disconnect network drive z, enter the following command:

```
net use z: /delete
```

Step 6 To map a network printer, enter a command in the following format:

```
net use LPT1 \ServerName\PrinterName /user:Domain\name
```

For example, if the server name is engineering, the printer name is color-print1, the domain name is eng, and the username is admin, the command would be the following:

```
net use LPT1 \engineering\color-print1 /user:eng\admin
```

Step 7 To disconnect a network printer, enter a command in the following format:

```
net use LPT1 /delete
```

Step 8 To launch an application enter a command in the following format:

```
C:\Path-to-Application\Application.exe
```

Step 9 For example, to launch Microsoft Outlook, enter the following command:

```
C:\Program Files\Microsoft Office\OFFICE11\outlook.exe
```

Step 10 To open a website in your default browser, enter a command in the following format:

```
start http://www.website.com
```

Step 11 To open a file on your computer, enter a command in the following format:

```
C:\Path-to-file\myFile.doc
```

Step 12 When you have finished editing the scripts, save the file and close it.
Configuring Proxy Settings

SonicWALL SSL VPN 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 manually configure NetExtender proxy settings, perform the following tasks.

**Step 1** Right click on the icon in the task bar and click on **Preferences**... The NetExtender Preferences window is displayed.

**Step 2** Click on **Proxy**.

**Step 3** Select the **Enable proxy settings** checkbox.

**Step 4** 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)), which 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 script in the Address field.

- **Use proxy server** - Select this option to enter the 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 that bypass the proxy server. If required, enter a User
Using NetExtender

name and Password for the proxy server. If the proxy server requires a username and password, but you do not specify them in the Preferences window, a NetExtender pop-up window will prompt you to enter them when you first connect.

**Step 5**  Click the Internet Explorer proxy settings button to automatically import Internet Explorer’s proxy settings to be used in NetExtender.

**Viewing the NetExtender Log**

The NetExtender log displays information on NetExtender session events. The log is a file named NetExtender.dbg. It is stored in the directory: C:\Program Files\SonicWALL\SSL-VPN\NetExtender. To view the NetExtender log, right click on the NetExtender icon in the system tray, and click View Log.

To view details of a log message, double-click on a log entry, or go to View > Log Detail to open the Log Detail pane.

To save the log, either click the Export icon or go to Log > Export.
SonicWALL SSL VPN provides the ability to filter the NetExtender log. To filter the log to display entries from a specific duration of time, go to the Filter menu and select the cutoff threshold.

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.

To view the Debug Log, either click the Debug Log icon or go to Log > Debug Log.

*Note* It may take several minutes for the Debug Log to load. During this time, the Log window will not be accessible, although you can open a new Log window while the Debug Log is loading.

To clear the log, click on Log > Clear Log.
Using NetExtender

Disconnecting NetExtender

To disconnect NetExtender, perform the following steps:

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

**Step 2** Wait several seconds. The NetExtender session disconnects.

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

When NetExtender becomes 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 SonicWALL SSL-VPN security appliance.

When using releases prior 2.5, users should periodically launch NetExtender from the SonicWALL Virtual Office to ensure they have the latest version. Prior to release 2.5, NetExtender does not check for updates when it is launched directly from a user’s computer.

Uninstalling NetExtender

The NetExtender utility is automatically installed on your computer. To remove NetExtender, click on **Start > All Programs**, click on **SonicWALL SSL-VPN NetExtender**, and then click on **Uninstall**.
You can also configure NetExtender to automatically uninstall when your session is disconnected. To do so, perform the following steps:

**Step 1**  
Right click on the NetExtender icon in the system tray and click on Preferences... The NetExtender Preferences window is displayed.

**Step 2**  
Click on the Settings tab.

**Step 3**  
Select Uninstall NetExtender automatically to have NetExtender uninstall every time you end a session.

---

**Verifying NetExtender Operation from the System Tray**

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

SonicWALL SSL VPN provides a command line interface (CLI) for controlling NetExtender.

![Note]
The NetExtender command line interface is only available on Windows platforms.

To launch the NetExtender CLI, perform the following tasks:

**Step 1**
Launch the Windows Command Prompt by going to the **Start** menu, select **Run**, enter **cmd**, and click **OK**.

**Step 2**
Change directory to where NetExtender is installed. To do this, you first must enter `cd ..` to move up to the root drive. The enter `cd Program Files\SonicWALL\SSL-VPN\NetExtender`.

**Step 3**
Enter **NECLI.exe**. The NetExtender CLI launches and displays a summary of the available commands.

```
C:\Program Files\SonicWALL\SSL-VPN\NetExtender>NECLI.exe
```

Table 2 describes the commands available in the NetExtender CLI and their options.

<table>
<thead>
<tr>
<th>Command</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NECLI connect</td>
<td><code>-s server</code></td>
<td>The IP address or hostname of the SSL VPN server.</td>
</tr>
<tr>
<td></td>
<td><code>-u user-name</code></td>
<td>The username for the account.</td>
</tr>
<tr>
<td></td>
<td><code>-p password</code></td>
<td>The password for the account.</td>
</tr>
<tr>
<td></td>
<td><code>-d domain-name</code></td>
<td>The domain to connect to.</td>
</tr>
<tr>
<td>NECLI createprofile</td>
<td><code>-s server</code></td>
<td>The IP address or hostname of the SSL VPN server.</td>
</tr>
<tr>
<td></td>
<td><code>-u user-name</code></td>
<td>The username for the account.</td>
</tr>
<tr>
<td></td>
<td><code>-p password</code></td>
<td>The password for the account.</td>
</tr>
<tr>
<td></td>
<td><code>-d domain-name</code></td>
<td>The domain to connect to.</td>
</tr>
</tbody>
</table>
Using NetExtender on MacOS and Linux

The following sections describe how to use NetExtender on the MacOS X and Linux platforms:

- Installing NetExtender on MacOS, page 36
- Using NetExtender on MacOS, page 37
- Installing and Using NetExtender on Linux, page 39
Installing NetExtender on MacOS

SonicWALL SSL VPN 2.5 introduces support for NetExtender on MacOS. To use NetExtender on your Macintosh, your system must meet the following prerequisites:

- MacOS X 10.5 and higher
- Java 1.5 and higher
- Both PowerPC and Intel Macs are supported.

To install NetExtender on your Macintosh, perform the following tasks:

**Step 1** Log in to the SonicWALL Virtual Office.

**Step 2** Click the **NetExtender** button.

**Step 3** The Virtual Office displays the status of NetExtender installation. A pop-up window may appear, prompting you to accept a certificate. Click **Trust**.

**Step 4** A second pop-up window may appear, prompting you to accept a certificate. Click **Trust**.
Using NetExtender on MacOS

Step 1  To launch NetExtender, go the Applications folder in the Finder and double click on NetExtender.app.

Step 2  The first time you connect, you must enter the SonicWALL SSL VPN server name in the SSL VPN Server field.

Step 3  Enter your username and password.

Step 4  The first time you connect, you must enter the domain name. The domain name is case-sensitive.

Step 5  Click Connect.
Step 6  You can instruct NetExtender remember your profile server name in the future. In the **Save profile** pulldown menu you can select **Save name and password (if allowed)**, **Save username only (if allowed)**, or **Do not save profile**.

Step 7  When NetExtender is connected, the NetExtender icon is displayed in the status bar at the top right of your display. Click on the icon to display NetExtender options.

Step 8  To display a summary of your NetExtender session, click **Connection Status**.

Step 9  To view the routes that NetExtender has installed, select the **Routes** tab in the main NetExtender window.

Step 10 To view the NetExtender Log, go to **Window > Log**.
Step 11 To generate a diagnostic report with detailed information on NetExtender performance, go to Help > Generate diagnostic report.

Step 12 Click Save to save the diagnostic report using the default nxdiag.txt file name in your NetExtender directory.

Installing and Using NetExtender on Linux

To use NetExtender on your Linux PC, your system must meet the following prerequisites:

- i386-compatible distribution of Linux
- Linux Fedora Core 8+, Ubuntu 7+ or OpenSUSE Linux 10.3+
- Sun Java 1.5 and higher is required for using the NetExtender GUI.

Note Open source Java Virtual Machines (VMs) are not currently supported. If you do not have Sun Java 1.5, you can use the command-line interface version of NetExtender.
To install NetExtender on your Linux PC, perform the following tasks:

**Step 1** Log in to the SonicWALL Virtual Office.

**Step 2** Click the NetExtender button. A pop-up window indicates that you have chosen to open the NetExtender.tgz file. Save it to your default download directory.

**Step 3** To install NetExtender from the CLI, navigate to the directory where you saved NetExtender.tgz and enter the `tar -zxf NetExtender.tgz` command.

**Step 4** Enter the `cd netExtenderClient` command.

**Step 5** Enter `./install` to install NetExtender.
Step 6  Launch the `NetExtender.tgz` file and follow the instructions in the NetExtender installer. The new netExtender directory contains a NetExtender shortcut that can be dragged to your desktop or toolbar.

Step 7  The first time you connect, you must enter the SonicWALL SSL VPN server name in the SSL VPN Server field. NetExtender will remember the server name in the future.

Step 8  Enter your username and password.

Step 9  The first time you connect, you must enter the domain name. The domain name is case-sensitive. NetExtender will remember the domain name in the future.

Note  You must be logged in as root to install NetExtender, although many Linux systems will allow the `sudo ./install` command to be used if you are not logged in as root.
Step 10  To view the NetExtender routes, select the Routes tab in the main NetExtender window.

Step 11  To view the NetExtender Log, go to NetExtender > Log.

Step 12  To generate a diagnostic report with detailed information on NetExtender performance, go to Help > Generate diagnostic report.

Step 13  Click Save to save the diagnostic report using the default nxdiag.txt file name in your NetExtender directory.
Installing and Using NetExtender for Windows Mobile

SonicWALL SSL VPN now supports NetExtender for the Windows Mobile platform. NetExtender for Windows Mobile provides the following features:

- One-time passwords
- Two-factor authentication
- HTTP proxy
- Connection profiles

NetExtender supports the following Windows Mobile platforms:

- Windows Mobile 5 PocketPC version
- Windows Mobile 6 Professional/Classic version

Note: Windows Mobile 5 Smart Phone version and Windows Mobile 6 Standard version are not currently supported.

To install NetExtender for Windows Mobile, perform the following tasks:

Step 1 Log in to http://mySonicWALL.com.
Step 2 Click on Downloads.
Step 3 In the Software Type pulldown menu, select one of the following:
   - SRA 1200 Firmware
   - SRA 4200 Firmware
Step 4 Click on the SSLVPN NetExtender (Windows Mobile) link.
Step 5 Save the .cab file onto your Windows Mobile device.
Step 6 Double-click on the .cab file to install NetExtender.
Step 7 Go to your Programs folder to launch NetExtender.
Step 8 When NetExtender is installed, you may be prompted to restart your device. Click Yes.
To use NetExtender for Windows Mobile, perform the following tasks:

**Step 1** From your Windows Mobile device, launch NetExtender. The NetExtender login screen displays.

**Step 2** Enter the IP address or domain name for your SSL VPN server in the **Server** field. The IP address of the last SSL VPN server you connected to is displayed by default. To display a list of recent SSL VPN servers you have connected to, click on the arrow.

**Step 3** Enter your username and password.

**Step 4** The last domain you connected to is displayed in the **Domain** field.

**Step 5** The pulldown menu at the bottom of the window provides three options for remembering your username and password:

- Save user name & password if server allows
- Save user name only if server allows
- Always ask for user name & password

**Step 6** Click **Connect**. When NetExtender successfully connects, the NetExtender Status window displays.

**Step 7** To configure NetExtender options, click the **Menu** button. The following options are displayed:
• **Connection Profiles** - Displays all of the NetExtender connections that you have used on this device. To remove a Connection Profile, highlight the profile, click the **Menu** button, and click **Remove**.

- **System Settings** - Provides several configuration options.

  – **Hide NetExtender when closing window** - Hides NetExtender when you click the **ok** button.
  – **Display precise number in status** - Displays the exact numbers of sent and receive data.
  – **Use Connection Manager to establish underlying connections** - Uses the Windows Mobile Connection Manager to establish the device’s connection to the mobile network. The Connection Manager is designed to determine the optimum network type (such as 3G or wi-fi). If this option is disabled, the user manages the connection manually.
  – **Enable NetExtender log** - Records log entries for NetExtender events.
  – **Overwrite the previous log when NetExtender starts** - Maintains a single NetExtender log file that is overwritten with each new NetExtender session. Disabling this option will create a separate log file for each NetExtender session.
• **Proxy Settings** - Provides the ability to manually specify a proxy server.

![Proxy Settings](image)

### Installing NetExtender on Android Smartphones

SonicWALL SSL VPN 5.0 introduces support for NetExtender on smartphones running the Android operating system. The NetExtender Android client supports the following features:

- One-time passwords
- Two-factor authentication
- HTTP/HTTPS proxy
- Connection profiles

The NetExtender Android installer is available on MySonicWALL in the standard **.apk** package format. The installer is also available from Android Market as the NetExtender Technology Preview.

The following features are not supported or not applicable on NetExtender Android in SonicWALL SSL VPN 5.0:

- Automatic connection of NetExtender before Windows login
- Automatic proxy support and Internet Explorer proxy synchronization
- Connection scripts
- IPv6 support
- Client certificate support
- Exit client after disconnect

To install NetExtender on an Android smartphone using the **.apk** package from MySonicWALL, perform the following tasks:

**Step 1** On a computer, log in to [http://mySonicWALL.com](http://mySonicWALL.com).

**Step 2** Click on **Downloads**.

**Step 3** In the **Software Type** pulldown menu, select one of the following:

- SRA 4200 Firmware
- SRA 1200 Firmware

**Step 4** Click on the **NetExtender (Android)** link.

**Step 5** Save the **.apk** file onto your computer.

**Step 6** Using the USB cable, connect your computer to the Android smartphone.
**Step 7**  On the Android smartphone, pull down the notifications.

**Step 8**  Tap **USB connected** to connect to the computer. The next screen shows the connection.
Step 9  Tap **Turn on USB storage** to prepare for copying the **apk** installer to the Android smartphone.

![USB Mss Storage](image)

**Step 10**  On the computer, copy the **apk** file to the Android SD card.

**Step 11**  Unmount the Android SD card from your computer. On Windows, it shows up under "My Computer" as a new drive. On Mac, a new drive shows up on the desktop.

**Step 12**  After unmounting the Android SD card from your computer, tap **Turn off USB storage**.

**Step 13**  On your Android smartphone, launch a file browser application.
Using NetExtender on Android Smartphones

Instructions for using NetExtender on your Android smartphone are available in the following sections:

- “Connecting to NetExtender” on page 50
- “Exiting or Disconnecting from NetExtender” on page 55
- “Checking Status, Routes, and DNS Settings” on page 57
- “Configuring Profiles, Preferences, and Proxy Servers” on page 59
- “Changing Your Password” on page 62
Connecting to NetExtender

To launch NetExtender on your Android smartphone and connect to the network through the SonicWALL SRA or SSL-VPN appliance, perform the following steps:

**Step 1** On your Android smartphone, start NetExtender by tapping the application icon. The NetExtender connection options screen displays. Enter the information into the **Server**, **User**, **Password**, and **Domain** fields.

**Step 2** Tap **Connect** to accept the default option (**Save user name & password**) or select a **Save...** or **Always ask...** option from the drop-down list. The available profile options depend on how NetExtender is configured on the SonicWALL appliance.
Step 3  The smartphone displays the **Login - Initializing engine** screen. After a successful connection, the entered values are saved as a profile that you can select when starting NetExtender. NetExtender saves the information in a secure file on the smartphone.

Step 4  If One Time Password is enabled on the SonicWALL SRA or SSL-VPN appliance, the One Time Password prompt is displayed. Enter the temporary password that was emailed to your configured account, and tap **OK**.

If your smartphone is synchronized to your email account, you can pull down the email notification from the top bar, or switch to your home page and access your email from there. After viewing the temporary password in your email or copying it to your clipboard, tap the NetExtender application icon to return directly to this screen.
Using NetExtender

To use the clipboard, press the password in your email and select **Select Text**. Press the selected text again and select **Copy**. Then in the OTP screen, press the field and select **Paste**. Some Android smartphones require you to hold the **OK** button for clipboard access.

**Step 5** If Two Factor Authentication is enabled on the SonicWALL SRA or SSL-VPN appliance, you may be prompted to update your **PIN** (Personal Identification Number) or create a new one.

If no PIN has yet been configured, or if the administrator has reset the account, the following screen asks if the system should generate a new PIN. To allow the system to generate it, tap **Yes**. To type in a PIN yourself, tap **No** and skip to **Step 7**.

**Step 6** If you chose to allow the system to generate the PIN, the display then prompts you to accept the generated PIN. Tap **Yes** to accept it, or tap **No** to have the system generate a different PIN. You are prompted each time until you tap **Yes**.
Step 7  If you chose to generate the PIN yourself, type a PIN into the PIN field and again in the second field to confirm it. Typically, PINs are required to be 4 to 8 digits. Tap OK.

Step 8  After entering the PIN or creating a new PIN, the Two Factor Authentication process requires you to enter the token code shown on your token device. Wait for the token code to change on the device, and then type the code into the field on your smartphone and tap OK.
Step 9  If a proxy server is configured in the smartphone (via Preferences), the Proxy Authentication screen is displayed next. Enter the username and password for the proxy and tap **OK**.

![Proxy Authentication Screen](image)

Step 10  NetExtender will connect at this point, unless there is a problem or error. You will see the NetExtender traffic indicator appear in the notification bar at the top of the display, unless it is disabled in Preferences.

The up and down arrows appear **white** when data is passing through the VPN tunnel. When no data is currently passing, the arrows appear **gray**. Control traffic does not affect the arrow colors.

The up arrow indicates that data is being sent from the smartphone to the network, and the down arrow indicates that data is being received from the network by the smartphone.

Step 11  If the NetExtender service running on the smartphone has a problem or has stopped running, the following screen is displayed. Tap **Exit** to quit the application. You may need to restart the service, possibly by turning the phone off and on again, or you may need to re-install NetExtender.

![Error Screen](image)
Exiting or Disconnecting from NetExtender

EXIT
Exiting and restarting NetExtender is useful when NetExtender cannot connect, possibly after a long period of disuse. To exit from NetExtender, perform the following steps:

**Step 1**
To access the Exit option, press the options or menu button while on the NetExtender screen. The options are displayed at the bottom of the screen.

**Step 2**
To cause NetExtender to exit completely, including the services component, select the Exit option and tap OK. You can restart NetExtender by clicking its icon on your smartphone.

DISCONNECT
To disconnect NetExtender, perform the following steps:

**Step 1**
Pull down the notification bar and click NetExtender to open the NetExtender user interface.
Step 2  In the NetExtender user interface, tap the Disconnect button and tap OK to confirm.

NetExtender notifies you while disconnecting.
Checking Status, Routes, and DNS Settings

While NetExtender is connected, you can view status information, routes, and DNS settings on your smartphone.

**Step 1** To open the NetExtender user interface, pull down the notification bar and tap **NetExtender**.

If you are connected to a SonicWALL SRA or SSL-VPN appliance running 5.0 or higher, and you have an Active Directory account, the **User** field contains your display name, such as “Sonia Eng”. If you are connected to an appliance running the 4.0 release or you do not have an Active Directory account, the **User** field displays the login name, such as “seng”.

**Step 2** To view status information, tap the **Status** tab. You can tap on the **Sent**, **Received**, or **Throughput** fields to change the units between bytes and packets.
Step 3  To view NetExtender routes, tap the Routes tab. The display shows all subnets currently available from the smartphone.

Step 4  To view the configured DNS servers, tap the DNS tab.

NetExtender Android supports DNS only; WINS or DNS suffix are not supported.
Configuring Profiles, Preferences, and Proxy Servers

To configure NetExtender profiles and preferences, including proxy servers, on your Android smartphone, perform the following steps:

**Step 1** To display NetExtender options, start NetExtender and then press the options or menu button on the smartphone. The options are displayed at the bottom of the screen.

**Profiles**

**Step 2** To display the *NetExtender Profiles* screen, start NetExtender and then press the options or menu button on the smartphone and tap *Profiles*.

**Step 3** To display the *Remove selected*, *Remove all*, and *Close* options on this *NetExtender Profiles* screen, press the options button while on the screen.
Step 4  Tap **Remove selected** to remove the profiles that have check marks next to them.
Step 5  Tap **Remove all** to remove all profiles from the smartphone.
Step 6  Tap **Close** to close the option display on this screen.
Step 7  To display the **Remove this profile**, **Remove selected profiles**, and **Remove all profiles** options, press and hold the **NetExtender Profiles** screen.

Step 8  Tap **Remove this profile** to remove the profile that you pressed on to bring up this screen.
Step 9  Tap **Remove selected** to remove the profiles that have check marks next to them.
Step 10 Tap **Remove all** to remove all profiles from the smartphone.
Step 11 Tap **Close** to close the option display on this screen.

**EXPORT LOG**

Step 12 To export the log file of NetExtender Android activity, select the **Export Log** option and enter the requested information.

**ABOUT**

Step 13 To view NetExtender version information, select the **About** option.
PREFERENCES / PROXY SETTINGS

Step 14 To configure NetExtender preferences including proxy and notification settings, select the Preferences option.

Step 15 Under General settings, select the Connection notification checkbox to display the NetExtender traffic indicator in the notification bar.

Clear the checkbox to prevent the indicator from being displayed.

Step 16 Under Proxy, select the Use Proxy checkbox to configure NetExtender Android to access external networks through a proxy server.

A proxy server is often used for access to the Internet if the initial connection is made to a local zone, such as LAN or WLAN.

Step 17 After selecting the Use Proxy checkbox, tap Proxy settings to open the configuration screen for the proxy server.

Step 18 Type the IP address of the proxy server into the Server field. Type the port number of the port that the server listens on into the Port field. This field displays “8080” by default, but there is no standard listening port for a proxy server.
Using NetExtender

Step 19  Optionally enter your login credentials for the server in the User and Password fields. Entering your credentials here causes NetExtender to save them, so that you can automatically connect to the proxy server during subsequent logins without being prompted for credentials.

NetExtender Android supports basic authentication using a username and password for proxy servers. Microsoft NTLM authentication is not currently supported.

Step 20  When finished configuring the proxy server settings, tap OK.

Changing Your Password

To change your password when prompted by NetExtender, perform the following steps:

Step 1  After connecting, a password expiration notice may be displayed on your Android smartphone. Tap Yes to change your password, or No to delay until a later time. NetExtender will remind you each time you connect.
Step 2  If you select Yes, the Change password screen is displayed. Type your password into the Current Password field, then type a new password into the New password field and again into the Type it again field. Tap OK.

Step 3  If your password expires before you change it, the Change password screen is displayed when you connect, with the message “Login failed – you must change your password.”

Type your old password into the Current Password field, then type a new password into the New password field and again into the Type it again field. Tap OK.
Related Documents

The following Technical Notes provide more information on advanced NetExtender scenarios:

- Running NetExtender on a Different TCP Port
- Using the SonicWALL CDP Agent over a SonicWALL NetExtender Connection
- Using SonicWALL NetExtender to Access FTP Servers
- Resolving NetExtender Error With McAfee Enterprise 8.5

Solution Document Version History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4/28/2006</td>
<td>This document was created.</td>
</tr>
<tr>
<td>2</td>
<td>5/18/2006</td>
<td>Updated with review comments and 1.5.0.1 changes.</td>
</tr>
<tr>
<td>3</td>
<td>8/18/2006</td>
<td>Added supported platforms.</td>
</tr>
<tr>
<td>4</td>
<td>3/14/2007</td>
<td>Updated for SonicWALL SSL VPN 2.1 release.</td>
</tr>
<tr>
<td>5</td>
<td>10/19/2007</td>
<td>Updated for SonicWALL SSL VPN 2.5 release.</td>
</tr>
<tr>
<td>6</td>
<td>5/13/2008</td>
<td>Updated for SonicWALL SSL VPN 3.0 release.</td>
</tr>
<tr>
<td>7</td>
<td>2/24/2009</td>
<td>Updated for Windows Mobile and CLI support in SonicWALL SSL VPN 3.5 release.</td>
</tr>
<tr>
<td>8</td>
<td>11/9/2010</td>
<td>Updated for Android smartphones, 64-bit Linux in 5.0 release</td>
</tr>
</tbody>
</table>

P/N 232-001965-00 Rev A