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 4
- “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
- “Platforms” section on page 4

What is NetExtender?
SonicWALL NetExtender is a transparent software application for Windows 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. NetExtender acts as an IP-level mechanism provided by the virtual interface that negotiates the ActiveX component. 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 ActiveX 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

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 ActiveX 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

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 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.

Platforms

NetExtender is available on SonicWALL SSL-VPN security appliances.

The NetExtender multiple ranges and routes feature is available on the SonicWALL SSL-VPN 2000 security appliance running the SSL-VPN 1.5 firmware release.

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 5
• “Configuring Global NetExtender Settings” section on page 6
• “Adding NetExtender Client Routes” section on page 7
• “Configuring User-Level NetExtender Settings” section on page 9
• “Configuring Group-Level NetExtender Settings” section on page 11
• “Configuring NetExtender Options for the Portal” section on page 14
Viewing NetExtender Status

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

<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 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** Supply a beginning client address range in the Client Address Range Begin field.

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

**Step 4** Click Apply.

**Step 5** The Status message displays Update Successful. Restart for current clients to obtain new addresses.

### Configuring Global NetExtender Settings

SonicWALL SSL-VPN release 2.1 introduces several settings to customize the behavior of NetExtender when users connect and disconnect. To configure global NetExtender client settings, 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 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.

- **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.

- **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 user 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 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** Type the subnet mask in the Subnet Mask: field.

**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 give this user the same IP 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 3** Click **Ok.**
Configuring User NetExtender Settings

The following NetExtender settings can be configured for the user:

- **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.

- **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.

- **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 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.

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

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

**Step 4** Type the subnet mask in the **Subnet Mask** field.
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  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 disconnnected 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.

- **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.

- **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 global NetExtender settings, select Use Global Settings for any of the above options.
Configuring Group 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.

Step 2 Type the IP address of the trusted network to which you would like to provide access with NetExtender in the Destination Network: field.

Step 3 Type the subnet mask in the Subnet Mask: field.

Step 4 Click Add.

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

Step 6 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 7 To also add the global NetExtender client routes (which are configured on NetExtender > Client Routes page) to users in this group, check the Add Global NetExtender Client Routes checkbox.

Step 8 Click Ok.
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 15
- “Verifying NetExtender Operation from the System Tray” section on page 30

User Prerequisites

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

- One of the following platforms:
- One of the following browsers:
  - Internet Explorer 5.0.1 and higher
  - Mozilla Firefox 1.5 and higher
- 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.

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

- MacOS 10.4 and higher
- Java 1.4 and higher
- Both PowerPC and Intel Macs are supported.

Linux clients must meet the following prerequisites in order to use NetExtender:
• Linux Fedora Core 3 or higher, or Ubuntu 7 or higher
• Sun Java 1.4 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 1.4, 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 install NetExtender on a Windows platform:
• “Installing NetExtender Using the Mozilla Firefox Browser” section on page 15
• “Installing NetExtender Using the Internet Explorer Browser” section on page 18

The following sections describe how to use NetExtender on a Windows platform:
• “Launching NetExtender Directly from Your Computer” section on page 22
• “Configuring NetExtender Preferences” section on page 23
• “Configuring NetExtender Connection Scripts” section on page 25
• “Configuring Proxy Settings” section on page 27
• “Viewing the NetExtender Log” section on page 28
• “Disconnecting NetExtender” section on page 29
• “Upgrading NetExtender” section on page 30
• “Uninstalling NetExtender” section on page 30
• “Displaying Route Information” section on page 31
• “Displaying Connection Information” section on page 31

The following section describe how to install and use NetExtender on a Macintosh platform:
• “Installing and Using NetExtender on MacOS” section on page 31

The following section describe how to install and use NetExtender on a Linux platform:
• “Installing and Using NetExtender on Linux” section on page 35

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."

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.

![NetExtender installed as Firefox extension](image)

**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>
Using NetExtender

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

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.

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.
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 following message will display.

![NetExtender Message](image-url)
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  Click **Instructions to add SSL-VPN server address into trusted sites** for help.
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.

Step 6 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.

Step 7 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 8 If the following warning message is displayed, click Continue Anyway. SonicWALL testing has verified that NetExtender is fully compatible with Windows XP and 2000.
Step 9 When NetExtender completes installing, the NetExtender Status window displays, indicating that NetExtender successfully connected.

![NetExtender Status Window](image)

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.

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.

![NetExtender Login Window](image)

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
Using NetExtender

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

![Settings Tab](image)

Step 5 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 6 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 7 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 8 Select **Display Connect/Disconnect Tips from the System Tray** to have NetExtender display tips when you mouse over the NetExtender icon.

Step 9 Select **Automatically reconnect when the connection is terminated** to have NetExtender attempt to reconnect when it loses connection.

Step 10 Select **Uninstall NetExtender automatically** to have NetExtender uninstall every time you end a session.

Step 11 Select **Disconnect an active connection** to have NetExtender log out of all of your SSL-VPN sessions when you exit a NetExtender session.

Step 12 Click **Apply**.
Configuring NetExtender 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.

**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](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 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.

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 a User 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.

Step 5  Click the Internet Explorer proxy settings button to open Internet Explorer's proxy settings.
Using 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 release 2.5 introduces 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.

**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.
Using NetExtender

Upgrading NetExtender

Beginning with SonicWALL SSL VPN release 2.5, 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.

Installing and Using 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 10.4 and higher
- Java 1.4 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  A pop-up window indicates that you have chosen to open the NetExtender.dmg file. Click OK to save it to your default download directory.

Step 4  Launch the NetExtender.dmg file. It will mount a drive that contains the NetExtender installer. Double click on the NetExtender-2.5.pkg file.
**Step 5** The NetExtender installer launches. Click **Continue**.

**Step 6** Select the volume you want to install NetExtender on and click **Continue**.

**Step 7** Click **Install**. NetExtender installs.

**Step 8** To launch NetExtender, go the Applications folder in the Finder and double click on **NetExtender.app**.

**Step 9** 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 10** Enter your username and password.

**Step 11** The first time you connect, you must enter the **domain** name. NetExtender will remember the domain name in the future.
Step 12 To view the NetExtender routes, go to the NetExtender menu and select Routes.

Step 13 To view the NetExtender Log, go to NetExtender > Log.

Step 14 To generate a diagnostic report with detailed information on NetExtender performance, go to Help > Generate diagnostic report.

Step 15 Click Save to save the diagnostic report using the default nxdiag.txt file name in your NetExtender directory.
Installing and Using NetExtender on Linux

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

• Linux Fedora Core 3+ and Ubuntu 7
• Sun Java 1.4 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 1.4, you can use the command-line interface version of NetExtender.

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. A pop-up window indicates that you have chosen to open the NetExtender.tgz file. Click OK to save it to your default download directory.

Step 3 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 4  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 5  Enter your username and password.

Step 6  The first time you connect, you must enter the **domain** name. 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 7  To install NetExtender from the CLI, navigate to the directory where you saved `NetExtender.tgz` and enter the `tar -zxf NetExtender.tgz` command.

Step 8  Enter the `cd netExtenderClient` command.

Step 9  Enter `./install` to install NetExtender.
**Step 10** To view the NetExtender routes, go to the **NetExtender** menu and select **Routes**.

**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.
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>
</tbody>
</table>