About SSL VPN

This section provides information on how to configure the SSL VPN features on the SonicWall network security appliance. SonicWall’s SSL VPN features provide secure remote access to the network using the NetExtender client.

NetExtender is an SSL VPN client for Windows, Mac, or Linux users that is downloaded transparently. It allows you to run any application securely on the network and uses Point-to-Point Protocol (PPP). NetExtender allows remote clients seamless access to resources on your local network. Users can access NetExtender two ways:

- Logging in to the Virtual Office web portal provided by the SonicWall network security appliance
- Launching the standalone NetExtender client

Each SonicWall appliance supports a maximum number of concurrent remote users. Refer to the following table for details.

<table>
<thead>
<tr>
<th>SonicWall appliance model</th>
<th>Maximum concurrent SSL VPN connections</th>
<th>SonicWall appliance model</th>
<th>Maximum concurrent SSL VPN connections</th>
<th>SonicWall appliance model</th>
<th>Maximum concurrent SSL VPN connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSa 9650</td>
<td>3000</td>
<td>SM 9600</td>
<td>3000</td>
<td>TZ600</td>
<td>200</td>
</tr>
<tr>
<td>NSa 9450</td>
<td>3000</td>
<td>SM 9400</td>
<td>3000</td>
<td>TZ500/TZ500 W</td>
<td>150</td>
</tr>
<tr>
<td>NSa 9250</td>
<td>3000</td>
<td>SM 9200</td>
<td>3000</td>
<td>TZ400/TZ400 W</td>
<td>100</td>
</tr>
<tr>
<td>NSa 6650</td>
<td>1500</td>
<td>NSA 6600</td>
<td>1500</td>
<td>TZ300/TZ300 W</td>
<td>50</td>
</tr>
<tr>
<td>NSa 5650</td>
<td>1500</td>
<td>NSA 5600</td>
<td>1000</td>
<td>SOHO W</td>
<td>50</td>
</tr>
<tr>
<td>NSa 4650</td>
<td>1000</td>
<td>NSA 4600</td>
<td>500</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSa 3650</td>
<td>500</td>
<td>NSA 3600</td>
<td>350</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSa 2650</td>
<td>350</td>
<td>NSA 2600</td>
<td>250</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SonicOS supports NetExtender connections for users with IPv6 addresses. The address objects drop-down list includes all the predefined IPv6 address objects.

**NOTE:** IPv6 Wins Server is not supported. IPv6 FQDN is supported.

Topics:
- About NetExtender
- Configuring Users for SSL VPN Access
- Biometric Authentication

About NetExtender

The NetExtender standalone client is installed the first time you launch NetExtender. Thereafter, it can be accessed directly from the Start menu on Windows systems, from the Application folder or dock on macOS systems, or by the path name or from the shortcut bar on Linux systems.

SonicWall’s SSL VPN NetExtender is a transparent software application for Windows, Mac, and Linux users that enables remote users to securely connect to the company network. With NetExtender, remote users can securely run any application on the company network. Users can upload and download files, mount network drives, and access resources as if they were on the local network.

NetExtender provides remote users with full access to your protected internal network. The experience is virtually identical to that of using a traditional IPSec VPN client, but the NetExtender Windows client is automatically installed on a remote user’s PC using the XPCOM plugin when using Firefox. On macOS systems, supported browsers use Java controls to automatically install NetExtender from the Virtual Office portal. Linux systems can also install and use the NetExtender client. Windows users need to download the client from the portal, and those with mobile devices need to download Mobile Connect from the app store.

The NetExtender standalone client is installed the first time the user launches NetExtender. Thereafter, it can be accessed directly from the Start menu on Windows systems and from the Application folder or dock on on macOS systems or by the path name or from the shortcut bar on Linux systems.

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

As a part of the NetExtender configuration, you need to create an address object for the NetExtender IP address range. This address object is then used when configuring the Device Profiles.

You can create address objects for both an IPv4 address range and an IPv6 address range to be used in the SSL VPN > Client Settings configuration. The address range configured in the address object defines the IP address pool from which addresses are assigned to remote users during NetExtender sessions. The range needs to be large enough to accommodate the maximum number of concurrent NetExtender users you intend to support. You may want to a few extra addresses for growth, but it’s not required.

NOTE: In cases where other hosts are on the same segment as the SSL VPN appliance, the address range must not overlap or collide with any assigned addresses.

Details for how to configure an address object is provided in SonicWall SonicOS 6.5 Policies, in the Address Objects section. Refer to the quick reference that follows for the settings needed to define an SSL address object.

To create an address object for the NetExtender IP address range:

1. Select the MANAGE view.
2. Navigate to Object > Address Objects.
3. Click Add.
4. Type a descriptive name in the Name field.
5. For Zone Assignment, select SSLVPN from the drop-down list.
6. For Type, select Range.
7. In the Starting IP Address field, type in the lowest IP address in the range you want to use.

NOTE: The IP address range must be on the same subnet as the interface used for SSL VPN services.

8. In the Ending IP Address field, type in the highest IP address in the range you want to use.
9. Click Add.
10. Click Close.

Setting Up Access

NetExtender client routes are used to allow and deny access for SSL VPN users to various network resources. Address objects are used to easily and dynamically configure access to network resources. Tunnel All mode routes all traffic to and from the remote user over the SSL VPN NetExtender tunnel—including traffic destined for the remote user’s local network. This is done by adding the following routes to the 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 are configured with 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.

NOTE: To configure Tunnel All mode, you must also configure an address object for 0.0.0.0, and assign SSL VPN NetExtender users and groups to have access to this address object.

Administrators also have 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 Web sites. NetExtender Connection Scripts can support any valid batch file commands.

Configuring Proxies

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

NetExtender provides three options for configuring proxy settings:

- **Automatically detect settings** - To use this setting, the proxy server must support Web Proxy Auto Discovery Protocol, 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, you can select this option and provide the URL of the script.

Use proxy server - You can use this option to specify the IP address and port of the proxy server. Optionally, you can enter an IP address or domain in the BypassProxy field to allow direct connections to those addresses and bypass the proxy server. If required, you can enter a user name and password for the proxy server. If the proxy server requires a username and password, but you do not specify them, a NetExtender pop-up window will prompt you to enter them when you first connect.

When NetExtender connects using proxy settings, it establishes an HTTPS connection to the proxy server instead of connecting to the firewall 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, of which the proxy server has no knowledge. The connecting process is identical for proxy and non-proxy users.

Installing the Stand-Alone Client

The first time a user launches NetExtender, the NetExtender stand-alone client is automatically installed on the user’s PC or Mac. 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 uninstall the old NetExtender first and then installs the new version.

Once the NetExtender stand-alone client has been installed, Windows users can launch NetExtender from their PC’s Start > Programs menu and configure NetExtender to launch when Windows boots. Mac users can launch NetExtender from their system Applications folder, or drag the icon to the dock for quick access. On Linux systems, the installer creates a desktop shortcut in /usr/share/NetExtender. This can be dragged to the shortcut bar in environments like Gnome and KDE.

NOTE: Complete instructions for installing NetExtender on a SonicWall appliance can be found in How to setup SSL-VPN feature (NetExtender Access) on SonicOS 5.9 & above (SW10657) in the Knowledge Base.

VIDEO: The video, How to configure SSL VPN, also explains the procedure for configuring NetExtender.

Configuring Users for SSL VPN Access

For users to be able to access SSL VPN services, they must be assigned to the SSLVPN Services group. Users attempting to login through the Virtual Office and who do not belong to the SSLVPN Services group are denied access.

Topics:
- For Local Users
- For RADIUS and LDAP Users
- For Tunnel All Mode Access

For Local Users

The detailed process for adding and configuring local users and groups is described in SonicWall SonicOS 6.5 System Setup, in the Users section. The following is a quick reference, listing the User settings needed to enable SSLVPN Services.

To configure SSL VPN access for local users:

1. Select the MANAGE view.
2. Navigate to Users > Local Users & Groups.
3. Click the Edit icon for the user you want to set up, or click the Add User button to create a new user.
4. Select Groups.
5. In the User Groups column, select SSLVPN Services and click the Right Arrow to move it to the Member Of column.
6. Select VPN Access and move the appropriate network resources VPN users (GVC, NetExtender, or Virtual Office bookmarks) to the Access List.

NOTE: The VPN Access tab affects the ability of remote clients using GVC, NetExtender, and SSL VPN Virtual Office bookmarks to access network resources. To allow GVC, NetExtender, or Virtual Office users to access a network resource, the network address objects or groups must be added to the Access List on the VPN Access tab.
7. Click OK.

For RADIUS and LDAP Users

The procedure for configuring RADIUS user and LDAP users is similar. You need to add the users to the SSLVPN Services user group.

The detailed process for configuring user groups is described in SonicWall SonicOS 6.5 System Setup, in the Users section. The following is a quick reference, listing the User settings needed to add users to the right group.

To configure SSL VPN access for RADIUS and LDAP users:

<table>
<thead>
<tr>
<th>Common Steps</th>
<th>Setting Up RADIUS Users</th>
<th>Setting Up LDAP Users</th>
</tr>
</thead>
</table>
1. Select the MANAGE view.
2. Navigate to Users > Settings.
3. Select Authentication.
4. In the User authentication method field: Select RADIUS or RADIUS + Local Users. Select LDAP or LDAP + Local Users.
5. Select: CONFIGURE RADIUS CONFIGURE LDAP
6. Select: RADIUS Users Groups
7. Select SSLVPN Services in the appropriate field: Default user group to which all RADIUS users belong Default LDAP User Group
8. Click OK.

For Tunnel All Mode Access

The detailed process for adding and configuring local users and groups is described in SonicWall SonicOS 6.5 System Setup, in the Users section. The following is a quick reference, listing the User settings needed to set up users and groups for Tunnel All mode.

To configure SSL VPN NetExtender users and groups for Tunnel All Mode:

1. Select the MANAGE view.
2. Navigate to Users > Local Users & Groups.
3. Click the Configure icon for an SSL VPN NetExtender user or group.
5. Select the WAN RemoteAccess Networks address object and click the Right Arrow button to move it to the Access List.
6. Click OK.
7. Repeat the processes for all local users and groups that use SSL VPN NetExtender.

Biometric Authentication

IMPORTANT: To use biometric authentication, Mobile Connect 4.0 or higher must be installed on the mobile device and configured to connect with the firewall.

SonicOS supports biometric authentication in conjunction with SonicWall Mobile Connect. Mobile Connect is an app that allows users to securely access private networks from a mobile device. With Mobile Connect 4.0 you can use finger-touch for authentication as a substitute for username and password.

The configuration settings to allow this method of authentication are on the SSL VPN > Client Settings page. These options only show when Mobile Connect is used to connect to the firewall.

After configuring biometric authentication on the SSL VPN > Client Settings page, Touch ID (iOS) or Fingerprint Authentication (Android) need to be enabled on the user’s smart phone or other mobile device.

Configuring SSL VPN Server Behavior

The SSL VPN > Server Settings page configures firewall to act as an SSL VPN server.
SSL VPN Status on Zones

This section displays the SSL VPN Access status on each zone:

- Green indicates active SSL VPN status.
- Red indicates inactive SSL VPN status.

Enable or disable SSL VPN access by clicking the zone name.

SSL VPN Server Settings

The following settings configure the SSL VPN server:

- SSL VPN Port - Enter the SSL VPN port number in the field. The default is 4433.
- Certificate Selection – From this drop-down menu, select the certificate that is used to authenticate SSL VPN users. The default method is Use Selfsigned Certificate.
- User Domain – Enter the user’s domain, which must match the domain field in the NetExtender client. The default is LocalDomain.

NOTE: If authentication partitioning is not being used, this field has to match with the domain field in the NetExtender client.

If authentication partitioning is being used, then in NetExtender, the user can enter any of the domain names configured with the partitions, hence selecting the partition for authenticating their name/password externally via RADIUS or LDAP. In this case, the name set here as default for the user to enter for local authentication, or if they have no local account, for authentication in the default partition.

Note that in either case, when used with external authentication, this user domain name is not passed to the RADIUS/LDAP server, sending just the simple user name without it.
- Enable Web Management over SSL VPN – To enable web management over SSL VPN, select Enabled from this drop-down menu. The default is Disabled.
- Enable SSH Management over SSL VPN – To enable SSH management over SSL VPN, select Enabled from this drop-down menu. The default is Disabled.
- Inactivity Timeout (minutes) – Enter the number of minutes of inactivity before logging out the user. The default is 10 minutes.

RADIUS User Settings

This section is available only when either RADIUS or LDAP is configured to authenticate SSL VPN users.

- Use RADIUS in – Select this checkbox to have RADIUS use MSCHAP or MSCHAPv2 mode. Enabling MSCHAP-mode RADIUS allows users to change expired passwords when they log in. Choose between these two modes:
  - MSCHAP
  - MSCHAPv2 mode (allows users to change expired passwords)
In LDAP, passwords can only be changed when using either Active Directory with TLS or when binding to it using an administrative account or Novell eDirectory. If this option is set when LDAP is selected as the authentication method of login on the Users > Settings page, but LDAP is not configured in a way that allows password updates, then password updates for SSL VPN users are performed using MSCHAP-v2 mode RADIUS after using LDAP to authenticate the user.

SSL VPN Client Download URL

In this section of the page, you set up where the client system downloads the SSL VPN client from. You can choose to download the files from the appliance and put them on your SSL VPN server or you can provide your own HTTP server to host this client package.

- Click here to download the SSL VPN zip file which includes all SSL VPN client files – Select this link to download all the client SSL VPN files from the appliance. Open and unzip the file, and then put the folder on your HTTP server.
- Use customer’s HTTP server as downloading URL: (http://) – Select this checkbox to enter your SSL VPN client download URL in the supplied field.

Configuring SSL VPN Client Settings

On the SSL VPN > Client Settings page, you can edit the Default Device Profile and the SonicPoint Layer 3 Management Default Device Profile. The Default Device Profile enables SSL VPN access on zones, configures client routes, and configures the client DNS and NetExtender settings. The SonicPoint Layer 3 Management Default Device Profile enables SSL VPN access on SonicPoint zones, configures client routes, and configures the SonicPoint Layer 3 settings.

The SSL VPN > Client Settings page also displays the configured IPv4 and IPv6 network addresses and zones that have SSL VPN access enabled.

You can also edit the SonicPoint Layer 3 Management Default Device Profile on this page.

### Configuring the Default Device Profile

Edit the Default Device Profile to select the zones and NetExtender address objects, configure client routes, and configure the client DNS and NetExtender settings.

SSL VPN access must be enabled on a zone before users can access the Virtual Office web portal. SSL VPN Access can be configured on the Network > Zones page (the System Setup section of the menu). Refer to the SonicWall SonicOS 6.5 System Setup, in the Network section, for more information.

### Configuring the Settings Options

To configure the Settings options for the Default Device Profile:

1. Select the MANAGE view.
2. Under Connectivity, select SSL VPN > Client Settings.
3. Click the Edit icon for the Default Device Profile.
NOTE: The Name and Description of the Default Device Profile cannot be changed.

4 In the Zone IP V4 drop-down menu, choose SSLVPN or a custom zone to set the zone binding for this profile.
5 From the Network Address IP V4 drop-down menu, select the IPv4 NetExtender address object that you created for this profile. See Creating an Address Object for the NetExtender Range for instructions. This setting selects the IP Pool and zone binding for this profile. The NetExtender client gets the IP address from this address object if it matches this profile.
6 In the Zone IP V6 drop-down menu, choose SSLVPN or a custom zone to set the zone binding for this profile.
7 From the Network Address IP V6 drop-down menu, select the IPv6 NetExtender address object that you created.
8 Click OK to save settings and close the window.

Configuring the Client Routes

On Client Routes, you can control the network access allowed for SSL VPN users. 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.

To configure the client routes:

1 Select the MANAGE view.
2 Under Connectivity, select SSL VPN > Client Settings.
3 Click the Edit icon for the Default Device Profile.
4 Select Client Routes.

5 Select Enabled from the Tunnel All Mode drop-down menu.

This forces all traffic for NetExtender users over the SSL VPN NetExtender tunnel—including traffic destined for the remote user’s local network.

6 Select the address object you want to allow SSL VPN access to and click the Right Arrow button to move the address object to the Client Routes list.
7 Repeat until you have moved all the address objects you want to use for Client Routes.

Creating client routes also creates access rules to be created automatically. You can also manually configure access rules for the SSL VPN zone. Refer to SonicWall SonicOS 6.5 Policies for details about access rules.

8 Click OK to save the settings and close the window.

Configuring Client Settings

The Client Settings Window has two sections of options:

• SSLVPN Client DNS Setting
• NetExtender Client Settings

SSLVPN Client DNS Setting

To configure SSLVPN Client DNS Settings:

1 Select the MANAGE view.
2 Under Connectivity, select SSL VPN > Client Settings.
3 Click the Edit icon for the Default Device Profile.
4 Select Client Settings.

Basic Settings

Name: Default Device Profile
Zone IP V4: SSLVPN
Network Address IP V4: Select a network
Zon IP V6: SSLVPN
Network Address IP V6: Select a network
In the DNS Server 1 field, choose one of the following:

- Enter the IP address of the primary DNS server.
- Click DEFAULT DNS SETTINGS to use the default settings for both the DNS Server 1 and DNS Server 2 fields. The fields are populated automatically.

**Note:** Both IP v4 and IP v6 are supported.

(Optional) In the DNS Server 2 field, if you did not click Default DNS Settings, enter the IP address of the backup DNS server.

(Optional) To build a DNS Search List:
1. In the DNS Search List (in order) field, enter the IP address for a DNS server.
2. Click ADD to add it to the list below.
3. Repeat as many times as necessary.

Use the up and down arrow buttons to scroll through the list, as needed. To remove an address from the list, select it and click REMOVE.

(Optional) In the WINS Server 1 field, enter the IP address of the primary WINS server.

**Note:** Only IPv4 is supported.

(Optional) In the WINS Server 2 field, enter the IP address of the backup WINS server.

To customize the behavior of NetExtender when users connect and disconnect, scroll down to NetExtender Client Settings.

<table>
<thead>
<tr>
<th>NetExtender Client Settings</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Client Autoupdate</td>
<td>The NetExtender client checks for updates every time it is launched.</td>
</tr>
<tr>
<td>Exit Client After Disconnect</td>
<td>The NetExtender client exits when it becomes disconnected from the SSL VPN server. To reconnect, users have to either return to the SSL VPN portal or launch NetExtender from their Programs menu.</td>
</tr>
<tr>
<td>Allow Touch ID on IOS devices</td>
<td>The NetExtender client allows Touch ID authentication on IOS smart phones.</td>
</tr>
<tr>
<td>Allow Fingerprint Authentication on Android devices</td>
<td>The NetExtender client allows fingerprint authentication on Android devices.</td>
</tr>
<tr>
<td>Enable NetBIOS over SSL VPN</td>
<td>The NetExtender client allows NetBIOS protocol.</td>
</tr>
<tr>
<td>Uninstall Client After Exit</td>
<td>The NetExtender client uninstalls when it becomes disconnected from the SSL VPN server. To reconnect, users have to return to the SSL VPN portal.</td>
</tr>
<tr>
<td>Create Client Connection Profile</td>
<td>The NetExtender client creates a connection profile recording the SSL VPN Server name, the Domain name, and optionally the username and password.</td>
</tr>
</tbody>
</table>

To provide flexibility in allowing users to cache their usernames and passwords in the NetExtender client, select one of these actions from the User Name & Password Caching field. These options enable you to balance security needs against ease of use for users.

- Allow saving of username only
- Allow saving of user name & password
- Prohibit saving of user name & password

Click OK.

**Configuring the SonicPoint L3 Management Default Device Profile**

Configuring the SonicPoint Layer 3 Management Default Device Profile sets up SSL VPN access on SonicPoint zones, configures client routes, and the L3 settings for the SonicPoint devices.

To configure the settings for the SonicPoint L3 profile:

1. Select the MANAGE view.
2. Under Connectivity, select SSL VPN > Client Settings.
3. Click the Edit icon for the SonicPoint L3 Management Default Device Profile.
NOTE: The Name and Description of the SonicPoint L3 Management Default Devices Profile cannot be changed.

4 On the Settings tab, from the Zone IP V4 drop-down menu, select SSLVPN or a custom zone to set up the zone binding for this profile.
5 From the Network Address IP V4 drop-down menu, select the IPv4 NetExtender address object that you created. Refer to Creating an Address Object for the NetExtender Range for instructions. This setting selects the IP Pool and zone binding for this profile. The NetExtender client gets the IP address from this address object if it matches.
6 Click the Client Routes tab.

7 From the Networks list, select the address object that you want to allow SSL VPN access to and click the Right Arrow to move the address object to the Client Routes list.
8 Repeat until you have moved all the address objects you want to use for Client Routes.

Creating client routes causes access rules allowing this access to be created automatically. You can also manually configure access rules for the SSL VPN zone on the Rules > Access Rules page. For more information, refer to SonicWall SonicOS 6.5 System Setup.

NOTE: After configuring Client Routes for SSL VPN, you must also configure all SSL VPN NetExtender users and user groups to be able to access the Client Routes. Refer to Configuring Users for SSL VPN Access for more a quick reference list.
9 Click the SP L3 Settings tab.

10 Select an interface from the WLAN Tunnel Interface drop-down menu.
11 Click OK.

Configuring the SSL VPN Web Portal

On the SSL VPN > Portal Settings page, you configure the appearance and functionality of the SSL VPN Virtual Office web portal. The Virtual Office portal is the website that uses login to launch NetExtender. It can be customized to match any existing company website or design style.
Portal Settings

The portal settings customize what the user sees when attempting to log in. Make the changes you want to match your company’s requirements.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portal Site Title</td>
<td>Enter the text displayed in the top title of the web browser in this field. The default is SonicWall - Virtual Office.</td>
</tr>
<tr>
<td>Portal Banner Title</td>
<td>Enter the text displayed next to the logo at the top of the page in this field. The default is Virtual Office.</td>
</tr>
<tr>
<td>Home Page Message</td>
<td>Enter the HTML code for the message that is displayed above the NetExtender icon. Type your own text or click EXAMPLE TEMPLATE to populate with a default template that you can keep or edit. Click PREVIEW to see what the Home Page Message looks like.</td>
</tr>
<tr>
<td>Login Message</td>
<td>Enter the HTML code for the message displayed when users are prompted to log into the Virtual Office. Type your own text or click EXAMPLE TEMPLATE to populate with a default template that you can keep or edit. Click PREVIEW to see what the Login Message looks like.</td>
</tr>
</tbody>
</table>

The following options customize the functionality of the Virtual Office portal:

- **Launch NetExtender after login** - Select to launch NetExtender automatically after a user logs in. This option is not selected by default.
- **Display Import Certificate Button** - Select to display an Import Certificate button on the Virtual Office page. This initiates the process of importing the firewall’s self-signed certificate onto the web browser. This option is not selected by default.

**NOTE:** This option only applies to the Internet Explorer browser on PCs running Windows when Use Selfsigned Certificate is selected from the Certificate Selection drop-down menu on the SSL VPN > Server Settings page.

- **Enable HTTP meta tags for cache control (recommended)** - Select to inserts into the browser HTTP tags that instruct the web browser not to cache the Virtual Office page. This option is not selected by default.

**NOTE:** SonicWall recommends enabling this option.

- **Display UTM management link on SSL VPN portal (not recommended)** – Select to display the SonicWall appliance’s management link on the SSL VPN portal. This option is not selected by default.

**IMPORTANT:** SonicWall does not recommend enabling this option.

Portal Logo Settings

This section allows you to customize the logo displayed at the top of the Virtual Office portal. The logo much be a GIF format, with a size of 155 x 36. A transparent or light background is recommended.

- **Default Portal Logo** – Displays the default portal logo which is the SonicWall logo.
- **Use Default SonicWall Logo** – Check the box to use the SonicWall logo supplied with the appliance. This option is not selected by default.
- **Customized Logo (Input URL of the Logo)** — Enter the URL for the logo you want to display.

**TIP:** The logo must be in GIF format of size 155 x 36; a transparent or light background is recommended.

Configuring Virtual Office

The SSL VPN > Virtual Office page displays the Virtual Office web portal inside of the SonicOS management interface.
Accessing the Virtual Office Portal

You can access the Virtual Office Portal two different ways. System administrators can access it through the appliance interface and have rights to make changes applicable to the entire site. User access it differently through different process and can only make changes that affect their particular profile.

For system administrators to access the SSL VPN Virtual Office portal:

1. Select the MANAGE view.
2. Under Connectivity, select SSL VPN > Virtual Office.

For users to view the SSL VPN Virtual Office web portal:

1. Navigate to the IP address of the firewall.
2. Click the link at the bottom of the Login page that says Click here for sslvpn login.

Configuring SSL VPN Bookmarks

User bookmarks can be defined to appear on the Virtual Office home page. Individual users cannot modify or delete bookmarks created by the administrator.

When creating bookmarks, remember that some services can run on non-standard ports, and some expect a path when connecting. When you configure a portal bookmark, you need to match the Service type with the right format for the Name or IP Address. Refer to the following table when setting those options.

**NOTE:** Service types for ActiveX and Java do not exist in SonicOS 6.5. Preferences from older versions convert to HTML5 during an upgrade.

<table>
<thead>
<tr>
<th>Service Type</th>
<th>Format</th>
<th>Example for Name or IP Address Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>RDP - ActiveX</td>
<td>IP Address</td>
<td>10.20.30.4</td>
</tr>
<tr>
<td>RDP - Java</td>
<td>IP:Port (non-standard)</td>
<td>10.20.30.4:6818</td>
</tr>
<tr>
<td></td>
<td>FQDN</td>
<td>JBJONES-PC.sv.us.sonicwall.com</td>
</tr>
<tr>
<td></td>
<td>Host name</td>
<td>JBJONES-PC</td>
</tr>
<tr>
<td>VNC</td>
<td>IP Address</td>
<td>10.20.30.4</td>
</tr>
<tr>
<td></td>
<td>IP:Port (mapped to session)</td>
<td>10.20.30.4:5901 (mapped to session 1)</td>
</tr>
<tr>
<td></td>
<td>FQDN</td>
<td>JBJONES-PC.sv.us.sonicwall.com</td>
</tr>
<tr>
<td></td>
<td>Host name</td>
<td>JBJONES-PC</td>
</tr>
<tr>
<td></td>
<td>NOTE: Do not use session or display number instead of port.</td>
<td>NOTE: Do not use 10.20.30.4:1</td>
</tr>
<tr>
<td></td>
<td>TIP: For a bookmark to a Linux server, see the Tip below this table.</td>
<td></td>
</tr>
<tr>
<td>Telnet</td>
<td>IP Address</td>
<td>10.20.30.4</td>
</tr>
<tr>
<td></td>
<td>IP:Port (non-standard)</td>
<td>10.20.30.4:6818</td>
</tr>
<tr>
<td></td>
<td>FQDN</td>
<td>JBJONES-PC.sv.us.sonicwall.com</td>
</tr>
<tr>
<td></td>
<td>Host name</td>
<td>JBJONES-PC</td>
</tr>
<tr>
<td>SSHv1</td>
<td>IP Address</td>
<td>10.20.30.4</td>
</tr>
<tr>
<td>SSHv2</td>
<td>IP:Port (non-standard)</td>
<td>10.20.30.4:6818</td>
</tr>
</tbody>
</table>
To add a portal bookmark:

1. Select the MANAGE view.
2. Under Connectivity, select SSL VPN > Portal Office.
3. Click ADD.

4. Type a descriptive name for the bookmark in the Bookmark Name field.
5. In the Name or IP Address field, enter the fully qualified domain name (FQDN) or the IPv4 address of a host machine on the LAN. Refer to Bookmark Name or IP Address Formats by Service Type (the previous table) for examples of the Name or IP Address expected for a given Service type.
6. In the Service drop-down menu, chose the appropriate service type:
   - RDP (HTML5-RDP)
   - SSHv2 (HTML5-SSHv2)
   - TELNET (HTML5-TELNET)
   - VNC (HTML5-VNC)

Different options display, depending on what you selected.

7. Complete the remaining fields for the service you selected. For the options and definitions, refer to the following table:

If Service is set to RDP (HTML5-RDP), configure the following:

<table>
<thead>
<tr>
<th>Screen Size</th>
<th>From the drop-down menu, choose the default terminal services screen size to be used when users execute this bookmark.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Colors</td>
<td>In the drop-down menu, select the default color depth for the terminal service screen when users select this bookmark.</td>
</tr>
<tr>
<td>Application and Path (optional)</td>
<td>If you want, enter the local path to where your application resides on your remote computer.</td>
</tr>
<tr>
<td>Start in the following folder</td>
<td>If you want, enter the local folder from which to execute application commands.</td>
</tr>
<tr>
<td>Show windows advanced options</td>
<td>Click the arrow to expand this and see all the Windows advanced options. Check the box to enable those that you want:</td>
</tr>
<tr>
<td></td>
<td>• Redirect clipboard</td>
</tr>
<tr>
<td></td>
<td>• Auto reconnection</td>
</tr>
<tr>
<td></td>
<td>• Window drag</td>
</tr>
<tr>
<td></td>
<td>• Redirect audio</td>
</tr>
<tr>
<td></td>
<td>• Desktop background</td>
</tr>
<tr>
<td></td>
<td>• Menu/window animation</td>
</tr>
</tbody>
</table>

Automatically log in

Check the box to enable automatic login. If selected, choose which credentials to use:

• Use SSL-VPN account credentials
• Use custom credentials
If you choose custom credentials, enter the username, password and domain for the credentials.

NOTE: You can use dynamic variables for the username and domain. Refer to Dynamic variables.

- **Display Bookmark to Mobile Connect clients**
  - Check the box to display the bookmarks to Mobile Connect users.

**If Service is set to SSHv2 (HTML5-SSHv2), configure the following:**
- **Automatically accept host key**
  - Check the box to enable.
- **Display Bookmark to Mobile Connect clients**
  - Check the box to display the bookmarks to Mobile Connect users.

**If Service is set to TELNET (HTML5-TELNET), configure the following:**
- **Display Bookmark to Mobile Connect clients**
  - Check the box to display the bookmarks to Mobile Connect users.

**If Service is set to VNC (HTML5-VNC), configure the following:**
- **View Only**
  - Check the box to set the bookmark to view only mode.
- **Share Desktop**
  - Enables the shared desktop feature.
- **Display Bookmark to Mobile Connect clients**
  - Check the box to display the bookmarks to Mobile Connect users.

8. Click **OK** to save the configuration.

<table>
<thead>
<tr>
<th>Text</th>
<th>Usage</th>
<th>Variable</th>
<th>Example Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login</td>
<td>Name</td>
<td>%USERNAME%</td>
<td>US:%USERNAME%</td>
</tr>
<tr>
<td>Domain</td>
<td>Name</td>
<td>%USERDOMAIN%</td>
<td>%USERDOMAIN%:%USERNAME%</td>
</tr>
</tbody>
</table>

**Dynamic variables**

**Configuring Device Profile Settings for IPv6**

SonicOS supports NetExtender connections for users with IPv6 addresses. On the SSL VPN > Client Settings page, first configure the traditional IPv6 IP address pool, and then configure an IPv6 IP Pool. Clients will be assigned two internal addresses: one IPv4 and one IPv6.

**NOTE:** IPv6 Wins Server is not supported.

On the SSL VPN > Client Routes page, user can select a client routes from the drop-down list of all address objects including all the pre-defined IPv6 address objects.

**NOTE:** IPv6 FQDN is supported.