Create SSL VPN Portals with the Wizard

ProSecure UTM Quick Start Guide

This quick start guide describes how to use the SSL VPN Wizard to configure SSL VPN portals on the ProSecure Unified Threat Management (UTM) Appliance. The Secure Sockets Layer (SSL) virtual private networking (VPN) feature provides remote access for mobile users to corporate or commercial resources, bypassing the need for a preinstalled VPN client on their computers.

For information about other features and for complete configuration steps, see the *ProSecure Unified Threat Management (UTM) Appliance Reference Manual*, available at *http://downloadcenter.netgear.com*.

This guide contains the following sections:

- *SSL VPN Portal Options*
- *Build a Portal Using the SSL VPN Wizard*
- *Access the New Portal*
- *For More Information*

SSL VPN Portal Options

Using SSL, commonly used for e-commerce transactions, the UTM can authenticate itself to an SSL-enabled client, such as a standard web browser. Once the authentication and negotiation of encryption information are completed, the server and client can establish an encrypted connection.

The UTM's SSL VPN portal can provide two levels of SSL service to a remote user:

- **SSL VPN tunnel**. The UTM can provide the full network connectivity of a VPN tunnel using the remote user's browser instead of a traditional IPSec VPN client. The SSL capability of the user's browser provides authentication and encryption, establishing a secure connection to the UTM. Upon successful connection, an ActiveX-based SSL VPN client is downloaded to the remote computer to allow the remote user to access the corporate network.

  The SSL VPN client provides a point-to-point (PPP) connection between the client and the UTM, and a virtual network interface is created on the user's computer. The UTM assigns the computer an IP address and DNS server IP addresses, allowing the remote computer to access network resources in the same manner as if it were connected directly to the corporate network.

- **SSL port forwarding**. Like an SSL VPN tunnel, SSL port forwarding is a web-based client that is installed transparently and then creates a virtual, encrypted tunnel to the remote network. However, port forwarding differs from an SSL VPN tunnel in several ways:
  - Port forwarding supports only TCP connections, but not UDP connections or connections using other IP protocols.
  - Port forwarding detects and reroutes individual data streams on the user's computer to the port-forwarding connection rather than opening up a full tunnel to the corporate network.
  - Port forwarding offers more fine-grained management than an SSL VPN tunnel. You define individual applications and resources that are available to remote users.

The SSL VPN portal can present the remote user with one or both of these SSL service levels, depending on how you set up the configuration.

Build a Portal Using the SSL VPN Wizard

The SSL VPN Wizard facilitates the configuration of the SSL VPN client connections by taking you through six screens, the last of which allows you to save the SSL VPN policy.

➢ **To start the SSL VPN Wizard:**

1. Select **Wizards** from the main navigation menu. The Welcome to the Netgear Configuration Wizard screen displays:

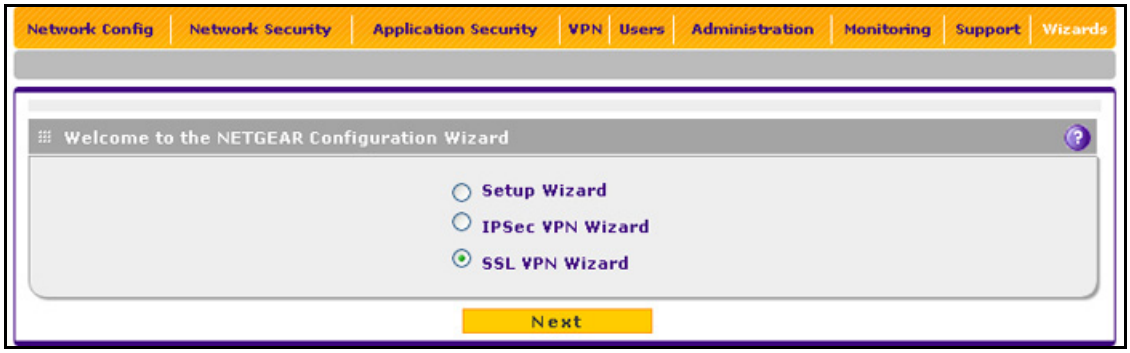

Figure 1.

2. Select the **SSL VPN Wizard** radio button.
3. Click **Next**. The first SSL VPN Wizard screen displays.

The following sections explain the five configuration screens of the SSL VPN Wizard. On the sixth screen, you can save your SSL VPN policy.

The tables in the following sections explain the buttons and fields of the SSL VPN Wizard screens.

SSL VPN Wizard Step 1 of 6 (Portal Settings)

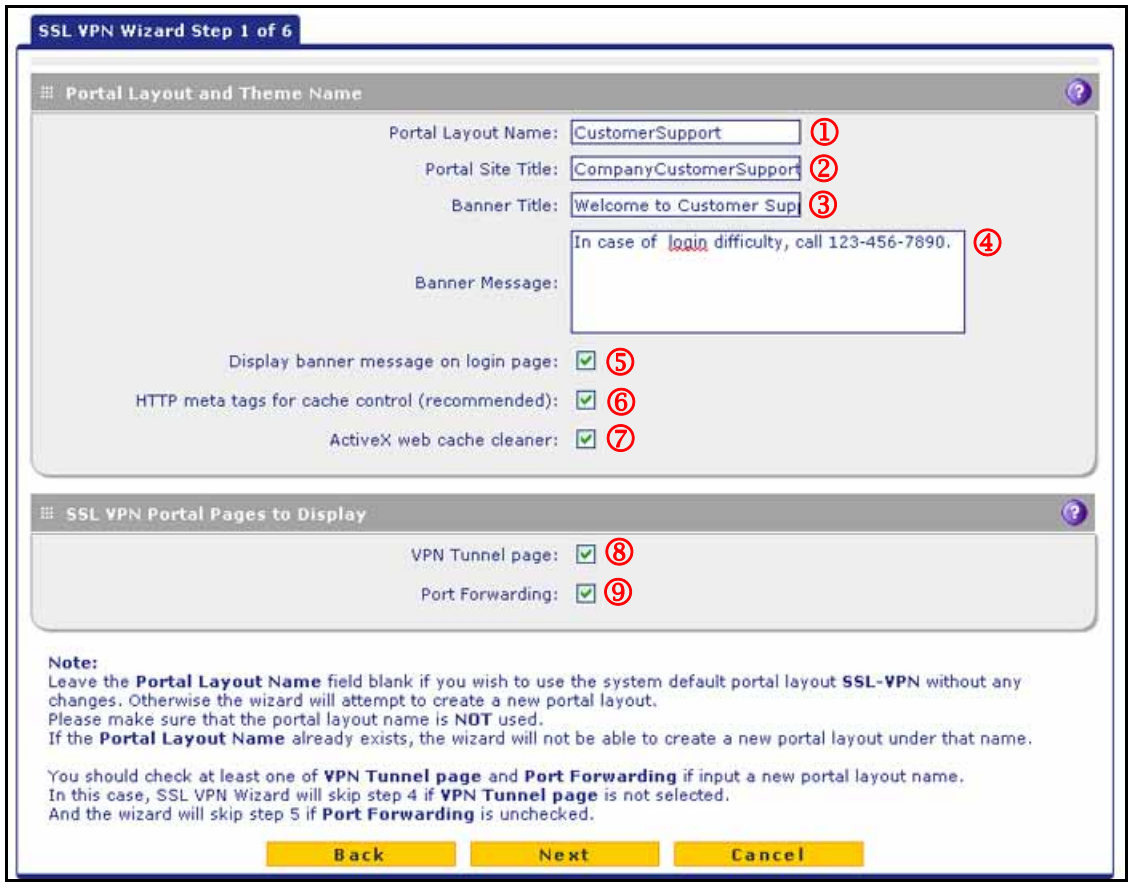

Figure 2.

Note that the previous figure contains a layout example. Enter the settings as explained in the following table, and then click **Next** to go the next screen.

WARNING:

Do not enter an existing portal layout name in the Portal Layout Name field; otherwise, the SSL VPN Wizard fails when you attempt to apply the settings (although the UTM does not reboot in this situation).

If you leave the Portal Layout Name field blank, the SSL VPN Wizard uses the default portal layout. (The name of the default portal is SSL-VPN). You need to enter a name other than SSL-VPN in the Portal Layout Name field to enable the SSL VPN Wizard to create a portal layout.

Table 1. SSL VPN Wizard Step 1 of 6 screen settings (portal settings)

#	Setting	Description
Portal Layout and Theme Name		
①	Portal Layout Name	A descriptive name for the portal layout. This name is part of the path of the SSL VPN portal URL. **Note:** Custom portals are accessed at a different URL than the default portal. For example, if your SSL VPN portal is hosted at https://vpn.company.com, and you create a portal layout named CustomerSupport, then users access the subsite at https://vpn.company.com/portal/CustomerSupport. **Note:** Only alphanumeric characters, hyphens (-), and underscores (_) are accepted in the Portal Layout Name field. If you enter other types of characters or spaces, the layout name is truncated before the first nonalphanumeric character. **Note:** Unlike most other URLs, this name is case-sensitive.
②	Portal Site Title	The title that displays at the top of the user's web browser window, for example, *Company Customer Support*.
③	Banner Title	The banner title of a banner message that users see before they log in to the portal, for example, *Welcome to Customer Support*.
④	Banner Message	The text of a banner message that users see before they log in to the portal, for example, *In case of login difficulty, call 123-456-7890*. Enter a plain text message, or include HTML and JavaScript tags. The maximum length of the login screen message is 4096 characters.
⑤	Display banner message on login page	Select this check box to show the banner title and banner message text on the login screen as shown in *Figure 9* on page 17.
⑥	HTTP meta tags for cache control (recommended)	Select this check box to apply HTTP meta tag cache control directives to this portal layout. Cache control directives include: <meta http-equiv="pragma" content="no-cache"> <meta http-equiv="cache-control" content="no-cache"> <meta http-equiv="cache-control" content="must-revalidate"> **Note:** NETGEAR strongly recommends enabling HTTP meta tags for security reasons and to prevent out-of-date web pages, themes, and data being stored in a user's web browser cache.
⑦	ActiveX web cache cleaner	Select this check box to enable ActiveX cache control to be loaded when users log in to the SSL VPN portal. The web cache cleaner prompts the user to delete all temporary Internet files, cookies, and browser history when the user logs out or closes the web browser window. The ActiveX web cache control is ignored by web browsers that do not support ActiveX.
SSL VPN Portal Pages to Display		
⑧	VPN Tunnel page	To provide full network connectivity, select this check box. For information about how to assign IP addresses and routes to clients, see *SSL VPN Wizard Step 4 of 6 (Client IP Addresses and Routes)* on page 11.

Table 1. SSL VPN Wizard Step 1 of 6 screen settings (portal settings) (continued)

#	Setting	Description
⑨	Port Forwarding	To provide access to specific defined network services, select this check box. For information about how to select network services, see *SSL VPN Wizard Step 5 of 6 (Port Forwarding)* on page 13. **Note:** Any services that are not selected are not visible from the SSL VPN portal; however, users can still access hidden services unless you create SSL VPN access policies to prevent access to these services.

SSL VPN Wizard Step 2 of 6 (Domain Settings)

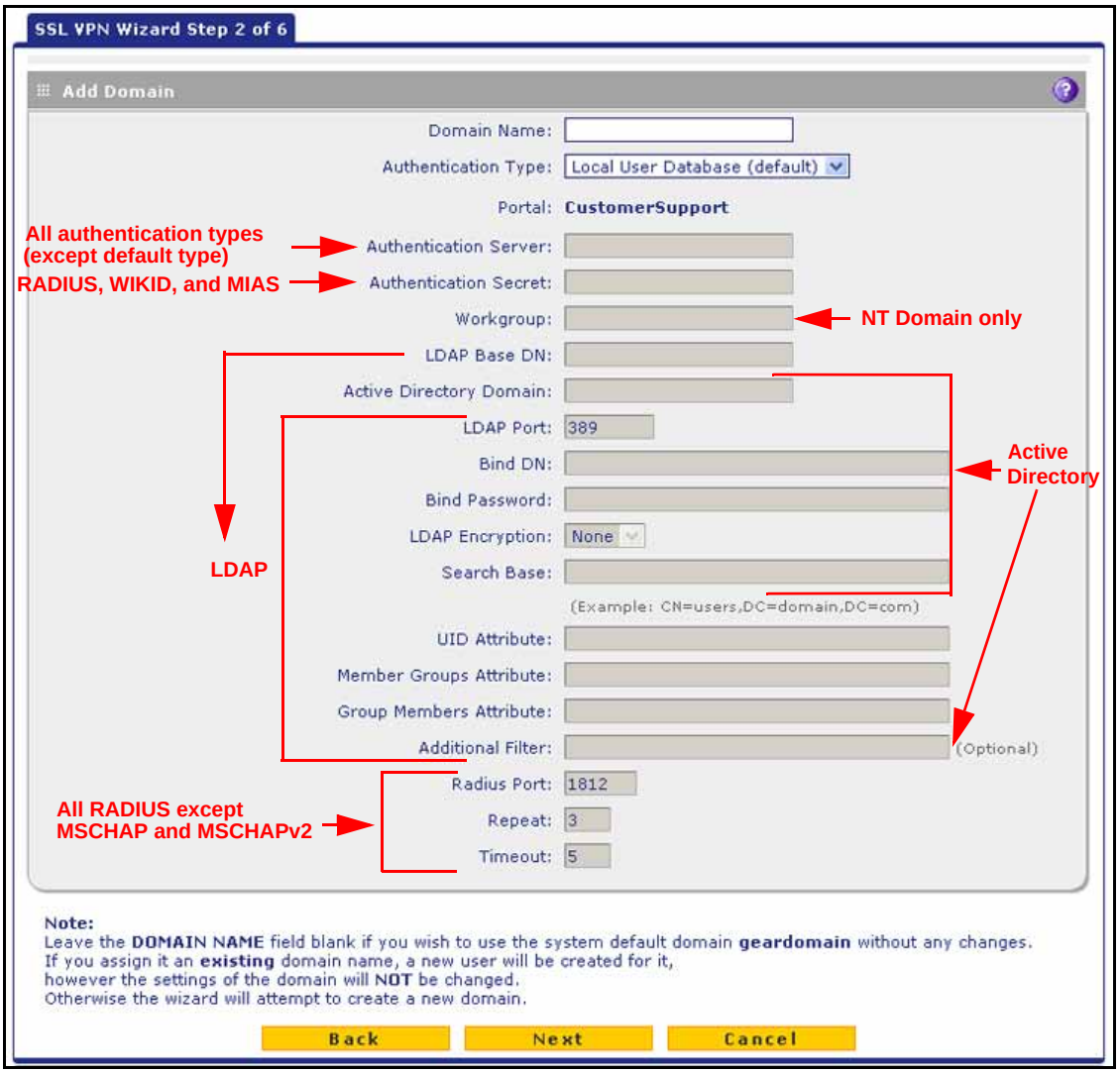

Figure 3.

Select the authentication type for the domain, enter the settings as explained in the corresponding table, and then click **Next** to go the next screen.

Note: If you leave the Domain Name field blank, the SSL VPN Wizard uses the default domain name geardomain. You need to enter a name other than geardomain in the Domain Name field to enable the SSL VPN Wizard to create a domain.

WARNING:

Do not enter an existing domain name in the Domain Name field; otherwise, the SSL VPN Wizard fails when you attempt to apply the settings, and the UTM reboots to recover its configuration.

Authentication Type: Local User Database

Table 2. SSL VPN Wizard Step 2 of 6 screen settings: Local User Database

Setting	Description
Domain Name	A descriptive (alphanumeric) name of the domain for identification and management purposes.
Authentication Type	From the drop-down list, select **Local User Database (default)**. Users are authenticated locally on the UTM. This is the default setting and most common authentication type. You do not need to complete any other fields on this screen.
Portal	The portal that you selected on the first SSL VPN Wizard screen. You cannot change the portal on this screen; the portal is displayed for information only.

Authentication Type: RADIUS-PAP, RADIUS-CHAP, WIKID-PAP, WIKID-CHAP, MIAS-PAP, or MIAS-CHAP

Table 3. SSL VPN Wizard Step 2 of 6 screen settings: RADIUS-PAP, RADIUS-CHAP, WIKID-PAP, WIKID-CHAP, MIAS-PAP, and MIAS-CHAP

Setting	Description
Domain Name	A descriptive (alphanumeric) name of the domain for identification and management purposes.
Authentication Type	From the drop-down list, select one of the following authentication methods: • **Radius-PAP**. RADIUS Password Authentication Protocol (PAP). • **Radius-CHAP**. RADIUS Challenge Handshake Authentication Protocol (CHAP). • **WIKID-PAP**. WiKID Systems PAP. • **WIKID-CHAP**. WiKID Systems CHAP. • **MIAS-PAP**. Microsoft Internet Authentication Service (MIAS) PAP. • **MIAS-CHAP**. Microsoft Internet Authentication Service (MIAS) CHAP. **Note:** Make sure that one or more RADIUS servers are configured by selecting **VPN > IPSec VPN > RADIUS Client** and configuring the RADIUS servers.

Table 3. SSL VPN Wizard Step 2 of 6 screen settings: RADIUS-PAP, RADIUS-CHAP, WIKID-PAP, WIKID-CHAP, MIAS-PAP, and MIAS-CHAP (continued)

Setting	Description
Portal	The portal that you selected on the first SSL VPN Wizard screen. You cannot change the portal on this screen; the portal is displayed for information only.
Authentication Server	The server IP address or server name of the authentication server.
Authentication Secret	The authentication secret or password that is required to access the authentication server for RADIUS, WiKID, or MIAS authentication.
Radius Port	The port number for the RADIUS server. You can enter a value between 1 and 65535. The default port number is 1812.
Repeat	The period in seconds that the UTM waits for a response from a RADIUS server. You can enter a value between 1 and 10. The default is 3 seconds.
Timeout	The maximum number of times that the UTM attempts to connect to a RADIUS server. You can enter a value between 3 and 30. The default is 5 times.

Authentication Type: RADIUS-MSCHAP or RADIUS-MSCHAPv2

Table 4. SSL VPN Wizard Step 2 of 6 screen settings: RADIUS-MSCHAP and RADIUS-MSCHAPv2

Setting	Description
Domain Name	A descriptive (alphanumeric) name of the domain for identification and management purposes.
Authentication Type	From the drop-down list, select one of the following authentication methods: • **Radius-MSCHAP**. RADIUS Microsoft CHAP. • **Radius-MSCHAPv2**. RADIUS Microsoft CHAP version 2. **Note:** Make sure that one or more RADIUS servers are configured by selecting **VPN > IPSec VPN > RADIUS Client** and configuring the RADIUS servers.
Portal	The portal that you selected on the first SSL VPN Wizard screen. You cannot change the portal on this screen; the portal is displayed for information only.
Authentication Server	The server IP address or server name of the authentication server.
Authentication Secret	The authentication secret or password that is required to access the authentication server for RADIUS, WiKID, or MIAS authentication.

Authentication Type: NT Domain

Table 5. SSL VPN Wizard Step 2 of 6 screen settings: NT Domain

Setting	Description
Domain Name	A descriptive (alphanumeric) name of the domain for identification and management purposes.
Authentication Type	From the drop-down list, select **NT Domain** for Microsoft Windows NT Domain.

Table 5. SSL VPN Wizard Step 2 of 6 screen settings: NT Domain (continued)

Setting	Description
Portal	The portal that you selected on the first SSL VPN Wizard screen. You cannot change the portal on this screen; the portal is displayed for information only.
Authentication Server	The server IP address or server name of the authentication server.
Workgroup	The workgroup that is required for Microsoft NT Domain authentication.

Authentication Type: Active Directory

Table 6. SSL VPN Wizard Step 2 of 6 screen settings: Active Directory

Setting	Description
Domain Name	A descriptive (alphanumeric) name of the domain for identification and management purposes.
Authentication Type	From the drop-down list, select **Active Directory** for Microsoft Active Directory.
Portal	The portal that you selected on the first SSL VPN Wizard screen. You cannot change the portal on this screen; the portal is displayed for information only.
Authentication Server	The server IP address or server name of the authentication server.
Active Directory Domain	The Active Directory domain name that is required for Microsoft Active Directory authentication.
LDAP Port	The port number for the Active Directory authentication server. The default port for the server is 389, which is generally the default port for TLS encryption or no encryption. When the encryption is SSL, the default port is generally 636.
Bind DN	The Active Directory DN that is required to access the Active Directory authentication server. This should be a user in the Active Directory who has read access to all the users that you would like to import into the UTM. The Bind DN field accepts two formats: • **A display name in the dn format**. For example: cn=Jamie Hanson,cn=users,dc=test,dc=com. • **A Windows login account name in email format**. For example: jhanson@testAD.com.
Bind Password	The authentication secret or password that is required to access the Active Directory authentication server.
LDAP Encryption	From the drop-down list, select the encryption type for the connection between the UTM and the Active Directory server: • **None**. The connection is not encrypted. This is the default setting. • **TLS**. The connection uses Transport Layer Security (TLS) encryption. • **SSL**. The connection uses Secure Socket Layer (SSL) encryption.

Table 6. SSL VPN Wizard Step 2 of 6 screen settings: Active Directory (continued)

Setting	Description
Search Base	The DN at which to start the search, specified as a sequence of relative distinguished names (RDNs), connected with commas and without any blank spaces. For most users, the search base is a variation of the domain name. For example, if your domain is yourcompany.com, your search base DN might be as follows: dc=yourcompany,dc=com.
Additional Filter	This field is optional. A filter that is used when the UTM is searching the server for matching entries while excluding others. (Use the format described by RFC 2254.) The following search term example matches users only: Active Directory. objectClass=user

Authentication Type: LDAP

Table 7. SSL VPN Wizard Step 2 of 6 screen settings: LDAP

Setting	Description
Domain Name	A descriptive (alphanumeric) name of the domain for identification and management purposes.
Authentication Type	From the drop-down list, select **LDAP** for Lightweight Directory Access Protocol (LDAP). **Note:** LDAP can query directories, including an Active Directory.
Portal	The portal that you selected on the first SSL VPN Wizard screen. You cannot change the portal on this screen; the portal is displayed for information only.
Authentication Server	The server IP address or server name of the authentication server.
LDAP Base DN	The LDAP base distinguished name (DN) that is required for LDAP authentication.
LDAP Port	The port number for the LDAP or Active Directory authentication server. The default port for the LDAP server is 389, which is generally the default port for TLS encryption or no encryption. When the encryption is SSL, the default port is generally 636.
Bind DN	The LDAP or Active Directory DN that is required to access the LDAP or Active Directory authentication server. This should be a user in the LDAP or Active Directory who has read access to all the users that you would like to import into the UTM. The Bind DN field accepts two formats: • **A display name in the dn format**. For example: cn=Jamie Hanson,cn=users,dc=test,dc=com. • **A Windows login account name in email format**. For example: jhanson@testAD.com. This last type of bind DN can be used only for a Windows Active Directory server.
Bind Password	The authentication secret or password that is required to access the LDAP or Active Directory authentication server.
LDAP Encryption	From the drop-down list, select the encryption type for the connection between the UTM and the LDAP or Active Directory server: • **None**. The connection is not encrypted. This is the default setting. • **TLS**. The connection uses Transport Layer Security (TLS) encryption. • **SSL**. The connection uses Secure Socket Layer (SSL) encryption.

Table 7. SSL VPN Wizard Step 2 of 6 screen settings: LDAP (continued)

Setting	Description
Search Base	The DN at which to start the search, specified as a sequence of relative distinguished names (RDNs), connected with commas and without any blank spaces. For most users, the search base is a variation of the domain name. For example, if your domain is yourcompany.com, your search base DN might be as follows: dc=yourcompany,dc=com.
UID Attribute	The attribute in the LDAP directory that contains the user's identifier (UID). For an Active Directory, enter **sAMAccountName**. For an OpenLDAP directory, enter **uid**.
Member Groups Attribute	This field is optional. The attribute that is used to identify the groups that an entry belongs to. For an Active Directory, enter **memberOf**. For OpenLDAP, you can enter a customized attribute to identify the groups of an entry.
Group Members Attribute	This field is optional. The attribute that is used to identify the members of a group. For an Active Directory, enter **member**. For OpenLDAP, you can enter a customized attribute to identify the members of a group.
Additional Filter	This field is optional. A filter that is used when the UTM is searching the LDAP server for matching entries while excluding others. (Use the format described by RFC 2254.) The following search term examples match users only: Active Directory. objectClass=user Open LDAP. objectClass=posixAccount

SSL VPN Wizard Step 3 of 6 (User Settings)

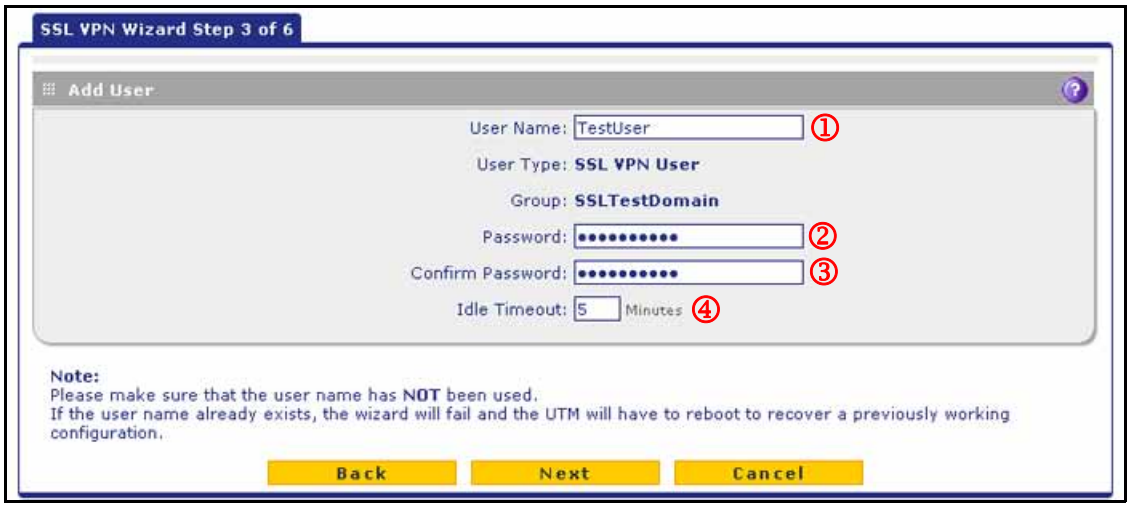

Figure 4.

Note that the previous figure contains an example. Enter the settings as explained in the following table, and then click **Next** to go the next screen.

WARNING:

Do not enter an existing user name in the User Name field; otherwise, the SSL VPN Wizard fails when you attempt to apply the settings, and the UTM reboots to recover its configuration.

Table 8. SSL VPN Wizard Step 3 of 6 screen settings (user settings)

#	Setting	Description
①	User Name	A descriptive (alphanumeric) name of the user for identification and management purposes.
	User Type	When you use the SSL VPN Wizard, the user type is always SSL VPN User. You cannot change the user type on this screen; the user type is displayed for information only.
	Group	When you create a domain on the second SSL VPN Wizard screen, a group with the same name is automatically created. (A user belongs to a group, and a group belongs to a domain.) You cannot change the group on this screen; the group is displayed for information only.
②	Password	The password that needs to be entered by the user to gain access to the UTM. The password needs to contain alphanumeric, hyphen (-), or underscore (_) characters.
③	Confirm Password	This field needs to be identical to the password that you entered in the Password field.
④	Idle Timeout	The period after which an idle user is automatically logged out of the web management interface. The default idle time-out period is 5 minutes.

SSL VPN Wizard Step 4 of 6 (Client IP Addresses and Routes)

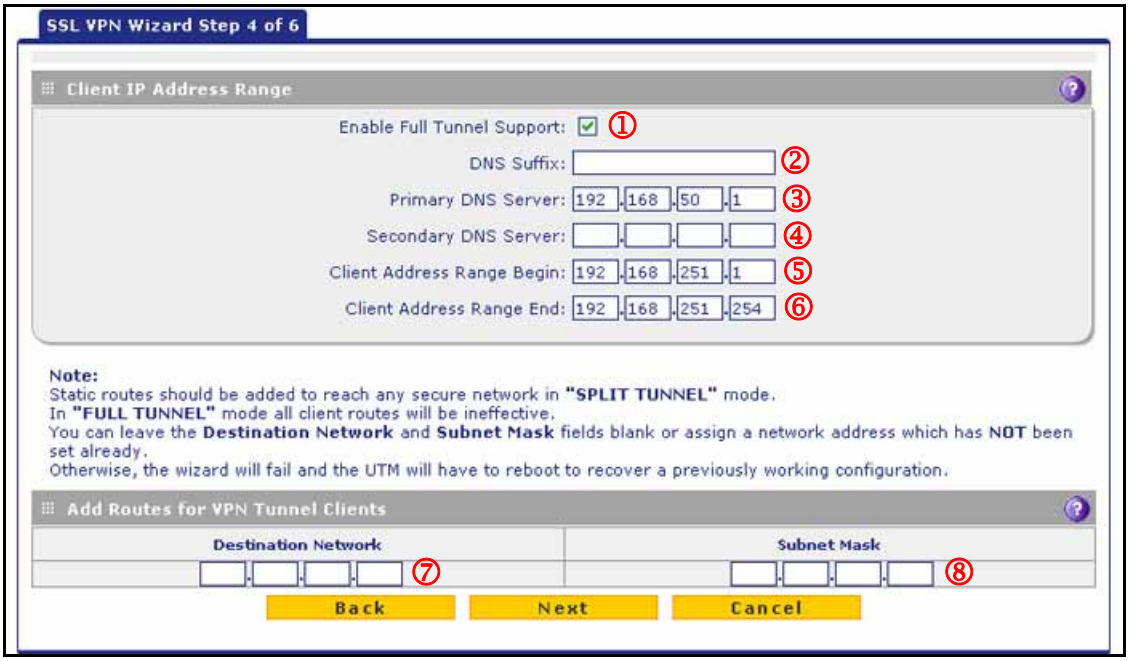

Figure 5.

Note: This screen displays only if you have selected the VPN Tunnel page check box on the SSL VPN Wizard Step 1 of 6 screen (see *Figure 2* on page 3).

Note that the previous figure contains an example. Enter the settings as explained in the following table, and then click **Next** to go the next screen.

WARNING:

Do not enter an existing route for a VPN tunnel client in the Destination Network and Subnet Mask fields; otherwise, the SSL VPN Wizard fails when you attempt to apply the settings, and the UTM reboots to recover its configuration.

Table 9. SSL VPN Wizard Step 4 of 6 screen settings (client addresses and routes)

#	Setting	Description
Client IP Address Range		
①	Enable Full Tunnel Support	Select this check box to enable full-tunnel support. If you leave this check box cleared (which is the default setting), full-tunnel support is disabled but split-tunnel support is enabled, and you need to add a client route by completing the Destination Network and Subnet Mask fields. **Note:** When full-tunnel support is enabled, client routes are not operable.
②	DNS Suffix	A DNS suffix to be appended to incomplete DNS search strings. This setting is optional.
③	Primary DNS Server	The IP address of the primary DNS server that is assigned to the VPN tunnel clients. This setting is optional. **Note:** If you do not assign a DNS server, the DNS settings remain unchanged in the VPN client after a VPN tunnel has been established.
④	Secondary DNS Server	The IP address of the secondary DNS server that is assigned to the VPN tunnel clients. This setting is optional.
⑤	Client Address Range Begin	The first IP address of the IP address range that you want to assign to the VPN tunnel clients.
⑥	Client Address Range End	The last IP address of the IP address range that you want to assign to the VPN tunnel clients.

Table 9. SSL VPN Wizard Step 4 of 6 screen settings (client addresses and routes) (continued)

#	Setting	Description
Add Routes for VPN Tunnel Clients		
⑦	Destination Network	Leave this field blank, or specify a destination network IP address of a local network or subnet that has not yet been used. This setting applies only when full-tunnel support is disabled.
⑧	Subnet Mask	Leave this field blank, or specify the address of the appropriate subnet mask This setting applies only when full-tunnel support is disabled.

SSL VPN Wizard Step 5 of 6 (Port Forwarding)

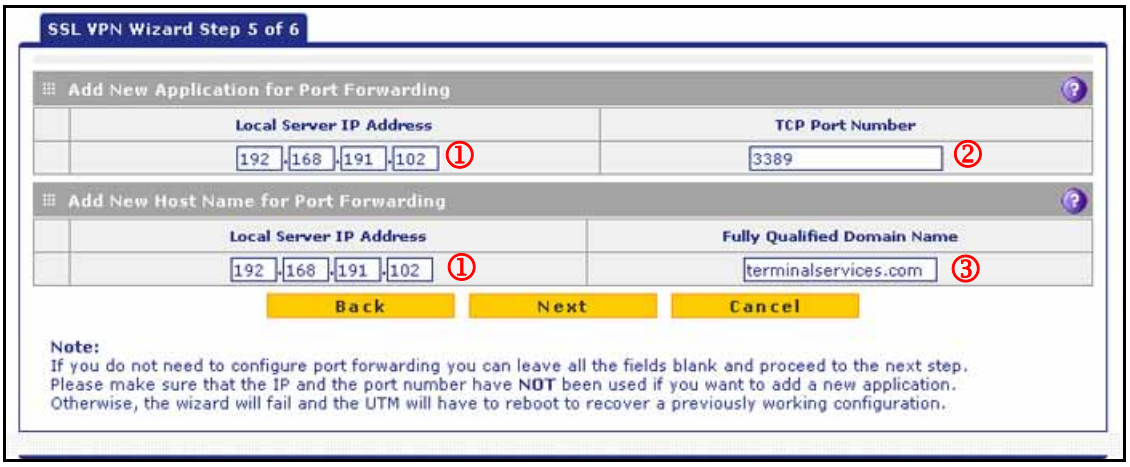

Figure 6.

Note: This screen displays only if you have selected the Port Forwarding check box on the SSL VPN Wizard Step 1 of 6 screen (see *Figure 2* on page 3).

Note that the previous figure contains an example. Enter the settings as explained in the following table, and then click **Next** to go the next screen.

WARNING:

Do not enter an IP address that is already in use in the upper Local Server IP Address field or a port number that is already in use in the TCP Port Number field; otherwise, the SSL VPN Wizard fails when you attempt to apply the settings, and the UTM reboots to recover its configuration.

Table 10. SSL VPN Wizard Step 5 of 6 screen settings (port-forwarding settings)

#	Setting	Description	
Add New Application for Port Forwarding			
①	Local Server IP Address	The IP address of an internal server or host computer that remote users have access to.	
②	TCP Port Number	The TCP port number of the application that is accessed through the SSL VPN tunnel. Following are some commonly used TCP applications and port numbers.	
		FTP Data (usually not needed)	20
		FTP Control Protocol	21
		SSH	22[a]
		Telnet	23[a]
		SMTP (send mail)	25
		HTTP (web)	80
		POP3 (receive mail)	110
		NTP (Network Time Protocol)	123
		Citrix	1494
		Terminal Services	3389
		VNC (virtual network computing)	5900 or 5800
Add New Host Name for Port Forwarding			
①	Local Server IP Address	The IP address of an internal server or host computer that you want to name. **Note:** Both the upper and lower Local Server IP Address fields on this screen (that is, the field in the Add New Application for Port Forwarding section and the field in the Add New Host Name for Port Forwarding section) need to contain the same IP address.	
③	Fully Qualified Domain Name	The full server name, that is, the host name–to–IP address resolution for the network server as a convenience for remote users.	

a. Users can specify the port number together with the host name or IP address.

SSL VPN Wizard Step 6 of 6 (Verify and Save Your Settings)

Verify your settings; if you need to make any changes, click the **Back** action button (if necessary several times) to return to the screen on which you want to make changes.

Figure 7.

Click **Apply** to save your settings. If the settings are accepted by the UTM, a message *Operation Succeeded* displays at the top of the screen, and the Welcome to the Netgear Configuration Wizard screen displays again (see *Figure 1* on page 2).

Access the New Portal

➢ **To access the new portal that you created with the SSL VPN Wizard:**

1. Select **VPN > SSL VPN > Portal Layouts**. The Portal Layouts screen displays:

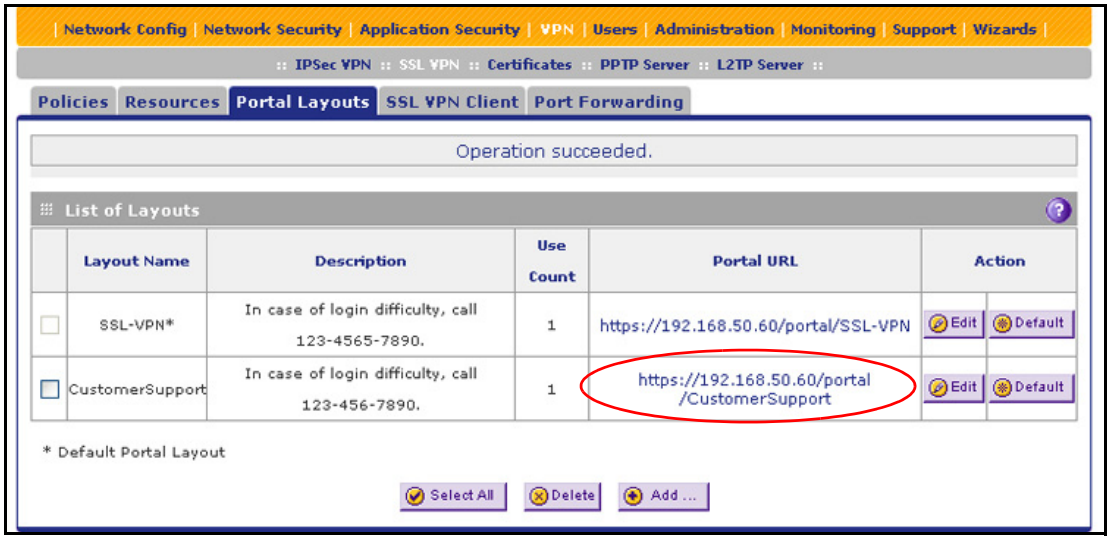

Figure 8.

2. In the Portal URL column of the List of Layouts table, click the URL that ends with the portal layout name that you created with the help of the SSL VPN Wizard (see the red oval in the previous figure). A login screen displays. This is the login screen for the portal that you created with the help of the SSL VPN Wizard. (The following figure shows an SSL portal login screen on the UTM10.)

IMPORTANT:

Provide a user who needs to access the portal with the corresponding URL from the Portal URL column. The user needs to paste or type this URL in the navigation toolbar of a browser. To enable a user outside the UTM's local network to access the portal, the URL needs to have a public IP address.

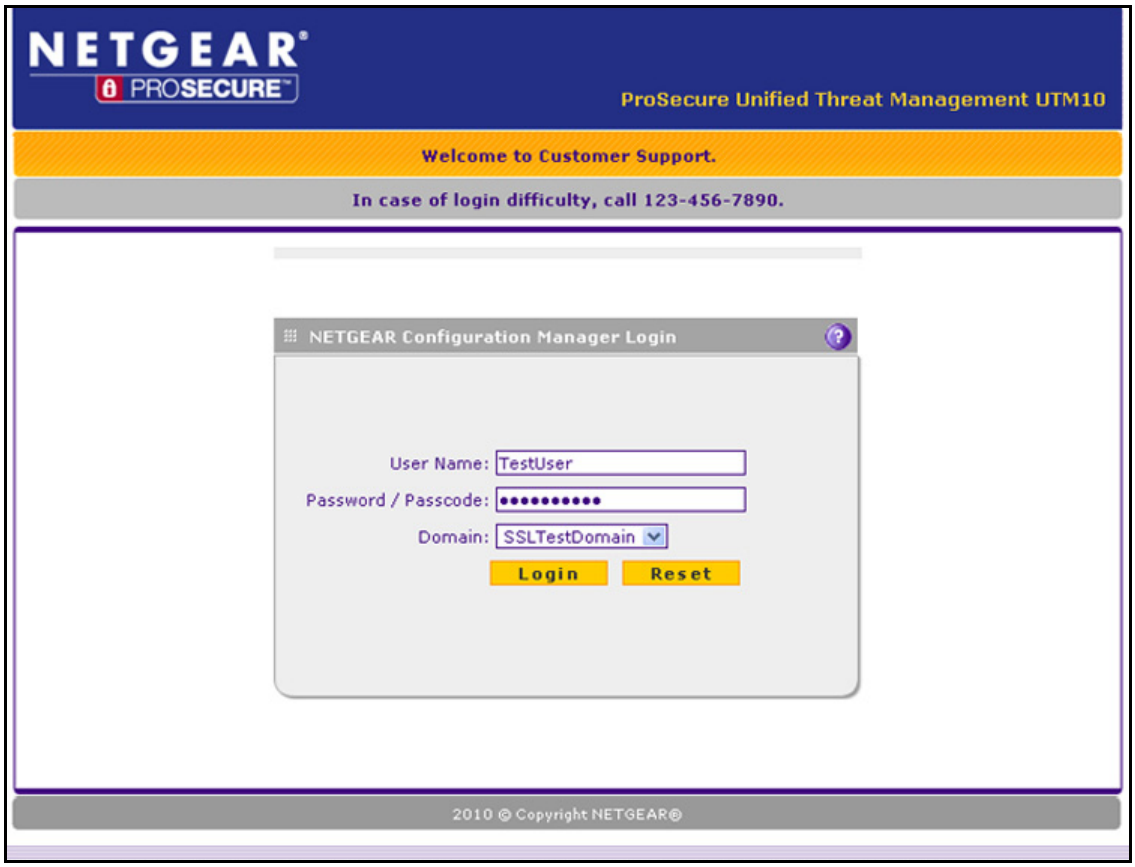

Figure 9.

3. To verify access, enter the user name and password that you created with the SSL VPN Wizard.

   Note: *Any user for whom you have set up a user account that is linked to the domain for the portal and who has knowledge of the portal URL can access the portal. To set up user accounts, select* ***Users > Users****.*

4. Click **Login**. A portal screen displays. The format of the portal screen depends on the settings that you selected on the first screen of the SSL VPN Wizard (see *SSL VPN Wizard Step 1 of 6 (Portal Settings)* on page 3):

   - *Figure 10* shows a portal screen with both a VPN Tunnel and a Port Forwarding menu option. (If you did not change its configuration, the default portal screen for the default SSL-VPN portal looks identical.)
   - *Figure 11* shows a portal screen with a Port Forwarding menu option only. The VPN Tunnel menu option is not displayed. (If you disabled the VPN tunnel, the default portal screen for the default SSL-VPN portal looks identical.)

     You could also disable the port forwarding option and enable the VPN tunnel, in which case the screen would display the VPN Tunnel menu option only.

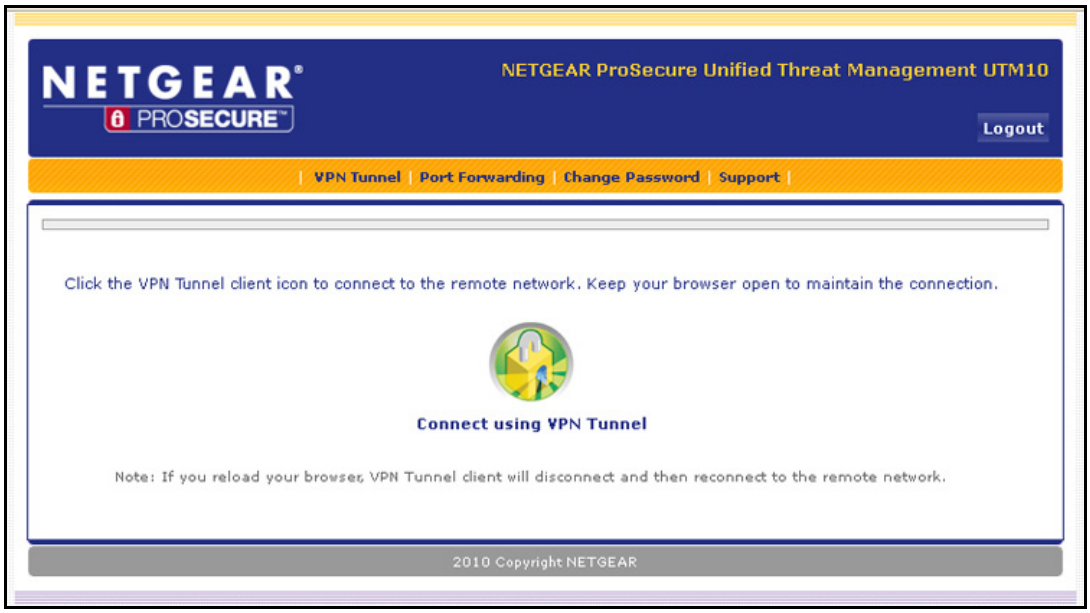

Figure 10.

Figure 11.

The default User Portal screen displays a simple menu that provides the SSL user with the following menu selections:

- **VPN Tunnel**. Provides full network connectivity.
- **Port Forwarding**. Provides access to the network services that you defined as described in *SSL VPN Wizard Step 5 of 6 (Port Forwarding)* on page 13.
- **Change Password**. Allows the user to change his or her password.
- **Support**. Provides access to the NETGEAR website.

Note: The first time that a user attempts to connect through the VPN tunnel, the NETGEAR SSL VPN tunnel adapter is installed; the first time that a user attempts to connect through the port-forwarding tunnel, the NETGEAR port-forwarding engine is installed.

For More Information

Chapter 8, “Virtual Private Networking Using SSL Connections,” of the reference manual provides information about the following SSL VPN topics:

- Modifying the portal layout
- Configuring applications for port forwarding
- Configuring the SSL VPN client
- Using network resource objects to simplify policies
- Configuring user, group, and global policies

Chapter 9, “Configure Authentication Domains, Groups, and Users,” of the reference manual provides information about the following SSL VPN topics:

- Modifying domains, groups, and user accounts
- Adding user accounts and assigning users to a domain that is associated with an SSL VPN portal