

Configuring SSL VPNs

This guide describes how to use the Unified Threat Management appliance (UTM) SSL VPN Wizard to configure the Secure Sockets Layer (SSL) virtual private networking (VPN) feature. This feature provides remote access for mobile users to their corporate resources, bypassing the need for a preinstalled VPN client on their computer. Using the Secure Sockets Layer (SSL) protocol 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 complete, the server and client can establish an encrypted connection.

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

This guide contains the following sections:

- [SSL VPN Portal Options](#)
- [Use the SSL VPN Wizard for Client Configurations](#)

SSL VPN Portal Options

The UTM's SSL VPN portal can provide two levels of SSL service to the 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.

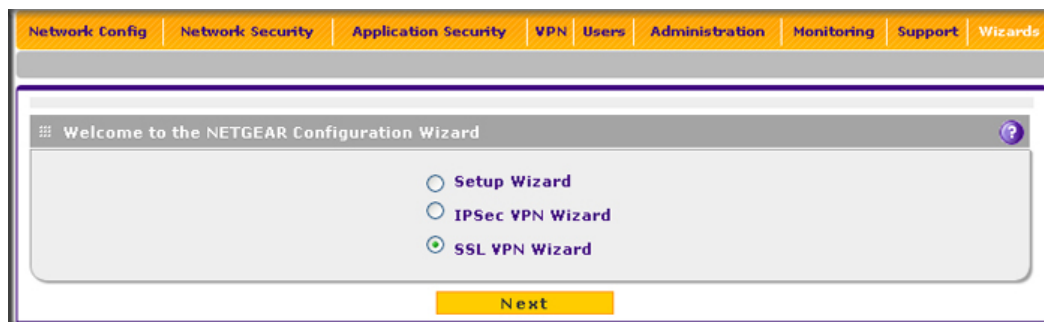
The SSL VPN portal can present the remote user with one or both of these SSL service levels, depending on how you set up the configuration.

Use the SSL VPN Wizard for Client Configurations

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. For information about how to edit policies or to configure policies manually, see the reference manual.

➤ To start the SSL VPN Wizard:

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



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

The tables in the following sections explain the buttons and fields of the SSL VPN Wizard screens. See the reference manual for additional information about the settings in the SSL VPN Wizard screens.

SSL VPN Wizard Step 1 of 6 (Portal Settings)

SSL VPN Wizard Step 1 of 6

Portal Layout and Theme Name

Portal Layout Name:

Portal Site Title:

Banner Title:

Banner Message:

Display banner message on login page: ☐

HTTP meta tags for cache control (recommended): ☐

ActiveX web cache cleaner: ☐

SSL VPN Portal Pages to Display

VPN Tunnel page: ☐

Port Forwarding: ☐

Note:
 Leave the **Portal Layout Name** field blank if you wish to use the system default portal layout **SSL-VPN** without any changes. Otherwise the wizard will attempt to create a new portal layout.
 Please make sure that the portal layout name is **NOT** used.
 If the **Portal Layout Name** already exists, the wizard will not be able to create a new portal layout under that name.

You should check at least one of **VPN Tunnel page** and **Port Forwarding** if input a new portal layout name.
 In this case, SSL VPN Wizard will skip step 4 if **VPN Tunnel page** is not selected.
 And the wizard will skip step 5 if **Port Forwarding** is unchecked.

Back **Next** **Cancel**

Figure 1. Portal Settings

➤ **Configure the portal settings:**

1. Enter the settings as explained in the following table.

Note: If you leave the Portal Layout Name field blank, the SSL VPN Wizard uses the default portal layout. 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. Do not enter an existing portal layout name in the Portal Layout Name field. If you do, the SSL VPN Wizard fails. The UTM does not reboot.

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

Setting	Description
Portal Layout and Theme Name	
Portal Layout Name	<p>A descriptive name for the portal layout. This name is part of the path of the SSL VPN portal URL.</p> <p>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.</p> <p>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.</p> <p>Note: Unlike most other URLs, this name is case-sensitive.</p>
Portal Site Title	The title that displays at the top of the user's web browser window, for example, <i>Company Customer Support</i> .
Banner Title	The banner title of a banner message that users see before they log in to the portal, for example, <i>Welcome to Customer Support</i> .
Banner Message	The text of a banner message that users see before they log in to the portal, for example, <i>In case of login difficulty, call 123-456-7890</i> . Enter a plain text message, or include HTML and JavaScript tags. The maximum length of the login screen message is 255 characters.
Display banner message on login page	Select this check box to show the banner title and banner message text on the login screen that is shown in step 2 on page 17.
HTTP meta tags for cache control (recommended)	<p>Select this check box to apply HTTP meta tag cache control directives to this portal layout. Cache control directives include:</p> <pre><meta http-equiv="pragma" content="no-cache"> <meta http-equiv="cache-control" content="no-cache"> <meta http-equiv="cache-control" content="must-revalidate"></pre> <p>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.</p>
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. Web browsers that do not support ActiveX ignore the ActiveX web cache control.

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

Setting	Description
SSL VPN Portal Pages to Display	
VPN Tunnel page	To provide full network connectivity, select this check box.
Port Forwarding	<p>To provide access to defined network services, select this check box.</p> <p>Note: Any pages that are not selected are not visible from the SSL VPN portal; however, users can still access the hidden pages unless you create SSL VPN access policies to prevent access to these pages.</p>

2. Click Next.

After you have completed the SSL VPN Wizard, you can change the portal settings by selecting **VPN > SSL VPN > Portal Layout**.

SSL VPN Wizard Step 2 of 6 (Domain Settings)

SSL VPN Wizard Step 2 of 6

Add Domain

Domain Name:

Authentication Type: **Local User Database (default)**

Portal: **CustomerSupport**

Authentication Server:

Authentication Secret:

Workgroup:

LDAP Base DN:

Active Directory Domain:

LDAP Port:

Bind DN:

Bind Password:

LDAP Encryption: **None**

Search Base:

(Example: CN=users,DC=domain,DC=com)

UID Attribute:

Member Groups Attribute:

Group Members Attribute:

Additional Filter: (Optional)

Radius Port:

Repeat:

Timeout:

Note:
 Leave the **DOMAIN NAME** field blank if you wish to use the system default domain **geardomain** without any changes.
 If you assign it an **existing** domain name, a new user will be created for it,
 however the settings of the domain will **NOT** be changed.
 Otherwise the wizard will attempt to create a new domain.

Back **Next** **Cancel**

Figure 2. Domain Settings

➤ **To configure the domain settings:**

1. Enter the settings as explained in the following table.

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. If you do, the SSL VPN Wizard fails and the UTM reboots to recover its configuration.

Table 2. SSL VPN Wizard Step 2 of 6 screen settings (domain settings)

Setting	Description
Domain Name	A descriptive (alphanumeric) name of the domain for identification and management purposes.
Authentication Type	<p>From the drop-down list, select the authentication method that the UTM applies:</p> <ul style="list-style-type: none"> • Local User Database (default). Users are authenticated locally on the UTM. You do not need to complete any other fields on this screen. • Radius-PAP. RADIUS Password Authentication Protocol (PAP). Complete the following fields: <ul style="list-style-type: none"> - Authentication Server - Authentication Secret - Radius Port - Repeat - Timeout • Radius-CHAP. RADIUS Challenge Handshake Authentication Protocol (CHAP). Complete the following fields: <ul style="list-style-type: none"> - Authentication Server - Authentication Secret - Radius Port - Repeat - Timeout • Radius-MSCHAP. RADIUS Microsoft CHAP. Complete the following fields: <ul style="list-style-type: none"> - Authentication Server - Authentication Secret • Radius-MSCHAPv2. RADIUS Microsoft CHAP version 2. Complete the following fields: <ul style="list-style-type: none"> - Authentication Server - Authentication Secret • WIKID-PAP. WiKID Systems PAP. Complete the following fields: <ul style="list-style-type: none"> - Authentication Server - Authentication Secret - Radius Port - Repeat - Timeout <p>Note: If you select any type of RADIUS authentication, make sure that one or more RADIUS servers are configured (see the reference manual).</p>

Table 2. SSL VPN Wizard Step 2 of 6 screen settings (domain settings) (continued)

Setting	Description
Authentication Type (continued)	<ul style="list-style-type: none"> • WIKID-CHAP. WiKID Systems CHAP. Complete the following fields: <ul style="list-style-type: none"> - Authentication Server - Authentication Secret - Radius Port - Repeat - Timeout • MIAS-PAP. Microsoft Internet Authentication Service (MIAS) PAP. Complete the following fields: <ul style="list-style-type: none"> - Authentication Server - Authentication Secret - Radius Port - Repeat - Timeout • MIAS-CHAP. Microsoft Internet Authentication Service (MIAS) CHAP. Complete the following fields: <ul style="list-style-type: none"> - Authentication Server - Authentication Secret - Radius Port - Repeat - Timeout • NT Domain. Microsoft Windows NT Domain. Complete the following fields: <ul style="list-style-type: none"> - Authentication Server - Workgroup • Active Directory. Microsoft Active Directory. Complete the following fields, and make a selection from the LDAP Encryption drop-down list: <ul style="list-style-type: none"> - Authentication Server - Active Directory Domain - LDAP Port - Bind DN - Bind Password - Search Base - Additional Filter (optional) • LDAP. Lightweight Directory Access Protocol (LDAP). Complete the following fields, and make a selection from the LDAP Encryption drop-down list: <ul style="list-style-type: none"> - Authentication Server - LDAP Base DN - LDAP Port - Bind DN - Bind Password - Search Base - UID Attribute - Member Groups Attribute (optional) - Group Members Attribute (optional) - Additional Filter (optional)

Table 2. SSL VPN Wizard Step 2 of 6 screen settings (domain settings) (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 for any type of authentication other than authentication through the local user database.
Authentication Secret	The authentication secret or password that is required to access the authentication server for RADIUS, WIKID, or MIAS authentication.
Workgroup	The workgroup that is required for Microsoft NT Domain authentication.
LDAP Base DN	The LDAP base distinguished name (DN) that is required for LDAP authentication.
Active Directory Domain	The Active Directory domain name that is required for Microsoft Active Directory 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	<p>The LDAP or Active Directory DN that is required to access the LDAP or Active Directory authentication server. Enter 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:</p> <ul style="list-style-type: none"> • 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	<p>From the drop-down list, select the encryption type for the connection between the UTM and the LDAP or Active Directory server:</p> <ul style="list-style-type: none"> • None (default). The connection is not encrypted. • TLS. The connection uses Transport Layer Security (TLS) encryption. • SSL. The connection uses Secure Socket Layer (SSL) encryption.
Search Base	The DN at which to start the search. The DN is 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	<p>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.</p>
Member Groups Attribute	<p>The attribute that is used to identify the groups that an entry belongs to. This field is optional. For an Active Directory, enter memberOf. For OpenLDAP, you can enter a customized attribute to identify the groups of an entry.</p>

Table 2. SSL VPN Wizard Step 2 of 6 screen settings (domain settings) (continued)

Setting	Description
Group Members Attribute	The attribute that is used to identify the members of a group. This field is optional. For an Active Directory, enter member . For OpenLDAP, you can enter a customized attribute to identify the members of a group.
Additional Filter	A filter that is used when the UTM is searching the LDAP server for matching entries while excluding others. (See RFC 2254.) This field is optional. The following search term examples match users only: Active Directory. objectClass=user Open LDAP. objectClass=posixAccount
Radius Port	The port number for the RADIUS server. You can enter a value from 1 through 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 from 1 through 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 from 3 through 30. The default is 5 times.

2. Click Next.

After you have completed the SSL VPN Wizard, you can change the domain settings by selecting **Users > Domains**. For more information about domain settings, see the reference manual.

SSL VPN Wizard Step 3 of 6 (User Settings)

SSL VPN Wizard Step 3 of 6

Add User

User Name:

User Type: **SSL VPN User**

Group: **Support1**

Password:

Confirm Password:

Idle Timeout: Minutes

Note:
Please make sure that the user name has **NOT** been used.
If the user name already exists, the wizard will not set SSL VPN configuration but output message and stop.

Back **Next** **Cancel**

Figure 3. User Settings

➤ **To configure the user settings:**

1. Enter the settings as explained in the following table.



WARNING:

Do not enter an existing user name in the User Name field. If you do, the SSL VPN Wizard fails and the UTM reboots to recover its configuration.

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

Setting	Description
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.
Password	The user must enter the password to gain access to the UTM. The password needs to contain alphanumeric, hyphen (-), or underscore (_) characters.
Confirm Password	This field needs to be identical to the password that you entered in the Password field.
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.

2. Click **Next**.

After you have completed the SSL VPN Wizard, you can change the user settings by selecting **Users > Users** on the main menu.

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

The screenshot shows the 'SSL VPN Wizard Step 4 of 6' window. The title bar indicates 'Client IP Address Range'. The main configuration area includes the following fields:

- Enable Full Tunnel Support:** ☒
- DNS Suffix:**
- Primary DNS Server:** 192 168 50 1
- Secondary DNS Server:**
- Client Address Range Begin:** 192 168 251 1
- Client Address Range End:** 192 168 251 254

Note:
 Static routes should be added to reach any secure network in "SPLIT TUNNEL" mode.
 In "FULL TUNNEL" mode all client routes will be ineffective.
 You can leave the **Destination Network** and **Subnet Mask** fields blank or assign a network address which has **NOT** been set already.
 Otherwise, the wizard will fail and the UTM will have to reboot to recover a previously working configuration.

Below the note is a section titled 'Add Routes for VPN Tunnel Clients' with a table for entering routes:

Destination Network	Subnet Mask
<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>

At the bottom of the window are three buttons: **Back**, **Next**, and **Cancel**.

Figure 4. Client Addresses and Routes

➤ **To configure the client addresses and routes:**

1. Enter the settings as explained in the following table.



WARNING:

Do not enter an existing route for a VPN tunnel client in the **Destination Network** and **Subnet Mask** fields. If you do, the SSL VPN Wizard fails and the UTM reboots to recover its configuration.

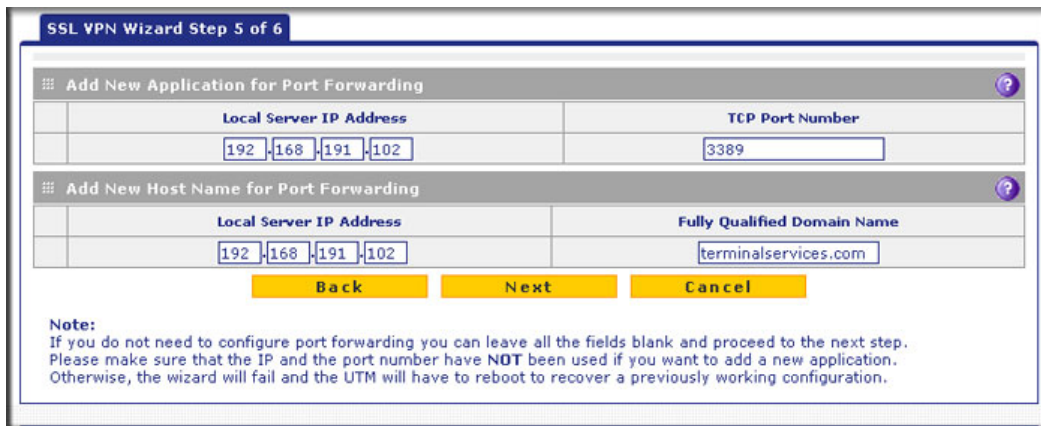
Table 4. SSL VPN Wizard Step 4 of 6 screen settings (client addresses and routes)

Setting	Description
Client IP Address Range	
Enable Full Tunnel Support	<p>Select this check box to enable full-tunnel support. If you leave this check box cleared (default setting), full-tunnel support is disabled but split-tunnel support is enabled, and you need to add a client route. Add a client route by completing the Destination Network and Subnet Mask fields.</p> <p>Note: When full-tunnel support is enabled, client routes are not operable.</p>
DNS Suffix	The DNS suffix appended to incomplete DNS search strings. This setting is optional.
Primary DNS Server	<p>The IP address of the primary DNS server that is assigned to the VPN tunnel clients. This setting is optional.</p> <p>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.</p>
Secondary DNS Server	The IP address of the secondary DNS server that is assigned to the VPN tunnel clients. This setting is optional.
Client Address Range Begin	The first IP address of the IP address range that you want to assign to the VPN tunnel clients.
Client Address Range End	The last IP address of the IP address range that you want to assign to the VPN tunnel clients.
Add Routes for VPN Tunnel Clients	
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.
Subnet Mask	Leave this field blank to specify the address of the appropriate subnet mask.

2. Click Next.

After you have completed the SSL VPN Wizard, you can change the client IP address range and routes by selecting **VPN > SSL VPN > SSL VPN Client**. For more information about client IP address range and routes settings, see the reference manual.

SSL VPN Wizard Step 5 of 6 (Port Forwarding)



SSL VPN Wizard Step 5 of 6

Add New Application for Port Forwarding

Local Server IP Address	TCP Port Number
192.168.191.102	3389

Add New Host Name for Port Forwarding

Local Server IP Address	Fully Qualified Domain Name
192.168.191.102	terminalservices.com

Back Next Cancel

Note:
If you do not need to configure port forwarding you can leave all the fields blank and proceed to the next step. Please make sure that the IP and the port number have **NOT** been used if you want to add a new application. Otherwise, the wizard will fail and the UTM will have to reboot to recover a previously working configuration.

Figure 5. Port Forwarding

➤ **To configure port forwarding (optional):**

1. Enter the settings as explained in the following table.



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. If you do, the SSL VPN Wizard fails and the UTM reboots to recover its configuration.

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

Setting	Description
Add New Application for Port Forwarding	
Local Server IP Address	The IP address of an internal server or host computer that remote users have access to.
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 (not needed) 20
	FTP Control Protocol 21
	SSH 22 ^a
	Telnet 23 ^a
	SMTP (send mail) 25
	HTTP (web) 80
	POP3 (receive mail) 110

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

Setting	Description	
TCP Port Number (continued)	NTP (Network Time Protocol)	123
	Citrix	1494
	Terminal Services	3389
	VNC (virtual network computing)	5900 or 5800
Add New Host Name for Port Forwarding		
Local Server IP Address	The IP address of an internal server or host computer that you want to name. Note: The upper and lower Local Server IP Address fields in the Add New Application for Port Forwarding section and in the Add New Host Name for Port Forwarding section must be the same.	
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 with the host name or IP address.

2. Click **Next**.

After you have completed the SSL VPN Wizard, you can change the client IP address range and routes by selecting **VPN > SSL VPN > Port Forwarding**. For more information about port forwarding settings, see the reference manual.

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

Verify your settings. If you need to change a screen, click the **Back** action button to return to the screen you want to changes.

SSL VPN Wizard Step 6 of 6

Portal Layout and Theme Name

Portal Layout Name: CustomerSupport ☒ Display banner message on login page
 Portal Site Title: CompanyCustomerSupport ☒ HTTP meta tags for cache control (recommended)
 Banner Title: Welcome to Customer Support ☒ ActiveX web cache cleaner
 Banner Message: In case of login difficulty, call 123-456-7890.

SSL VPN Portal Pages to Display

☒ VPN Tunnel page ☒ Port Forwarding

Domain

DOMAIN NAME: SSLTestDomain
 Authentication Type: Local User Database(default)
 Select Portal: CustomerSupport
 Authentication Server:
 Authentication Secret:
 Workgroup:
 LDAP Base DN:
 Active Directory Domain:

Group

Name: SSLTestDomain
 Domain: SSLTestDomain

User

User Name: TestUser
 User Type: SSL VPN User
 Select Group: SSLTestDomain
 Password: 1234567890
 Idle Timeout: 5 Minutes

VPN Client

Full Tunnel Support: true
 DNS Suffix:
 Primary DNS Server: 192.168.50.1
 Secondary DNS Server:
 Client Address Range Begin: 192.168.251.1
 Client Address Range End: 192.168.251.254
 Client Route:

Port Forwarding

Local Server IP Address: 192.168.191.102
 TCP Port Number: 3389
 Local Server IP Address: 192.168.191.102
 Fully Qualified Domain Name: terminalservices.com

Back **Apply** **Cancel**

Figure 6. Verify and Save your Settings

➤ **To save your settings:**

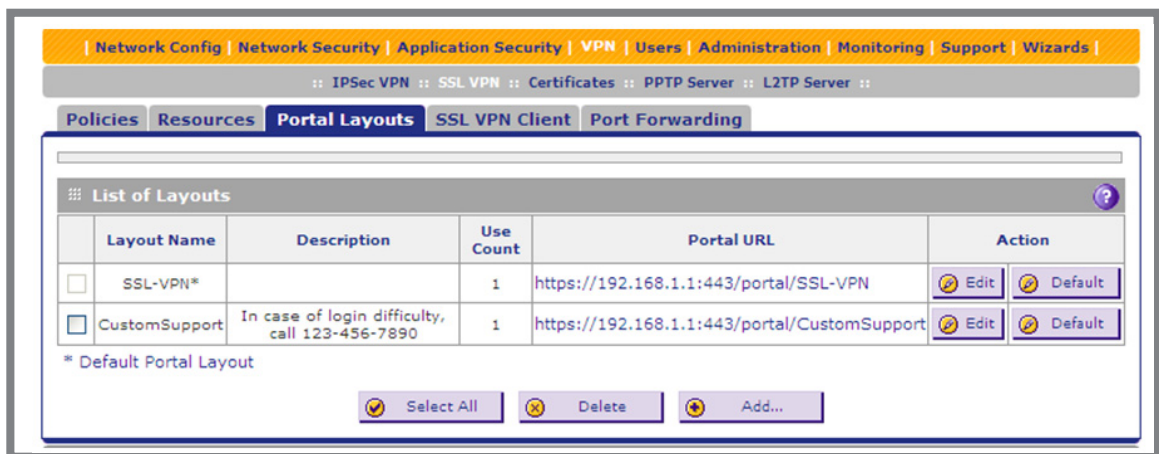
1. Click **Apply** to save your settings. If the UTM accepts the settings, the message *Operation Succeeded* displays at the top of the screen, and the Welcome to the NETGEAR Configuration Wizard screen displays.

Access the New SSL Portal Login Screen

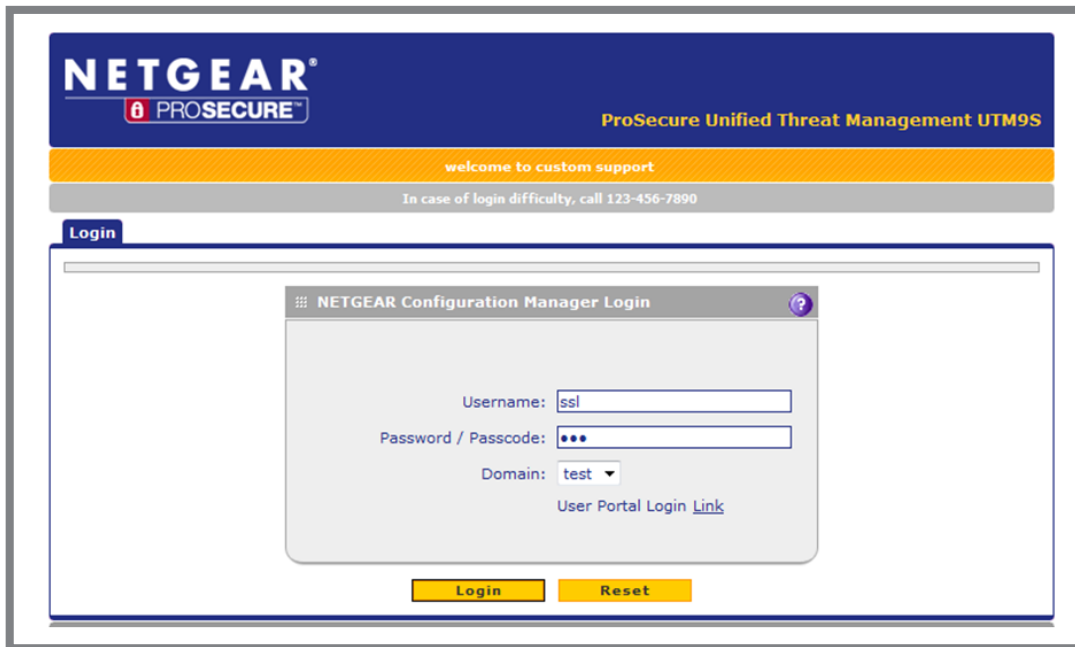
Screens that you can access from the SSL VPN configuration menu of the web management interface display a user portal link (**User Portal**) in the upper right corner of the screen. The link is the SSL VPN default portal and is not the same as the new SSL portal login screen that you defined with the SSL VPN Wizard.

➤ **To open the new SSL portal login screen:**

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



2. In the Portal URL field of the List of Layouts table, select the URL that ends with the portal layout name that you defined with the SSL VPN Wizard. The new SSL portal login screen displays. The following figure shows an SSL portal login screen.



3. Enter the user name and password that you created with the help of the SSL VPN Wizard.
4. Click **Login**. The default User Portal screen displays. The format of the User 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 7 shows the User Portal screen with both a VPN Tunnel and a Port Forwarding menu option.

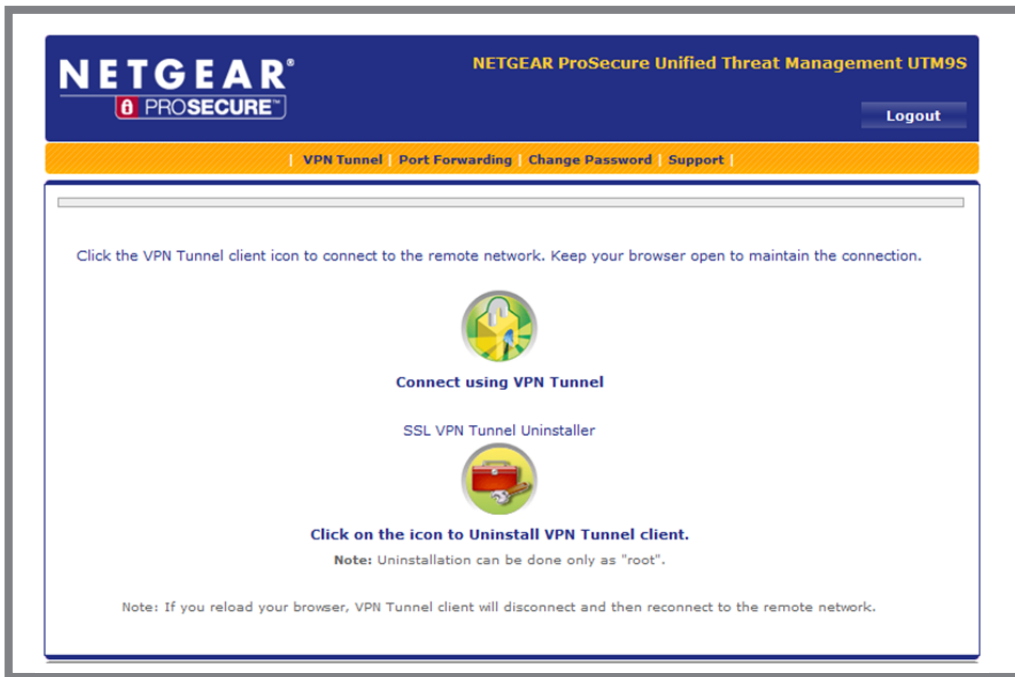


Figure 7. Portal screen with both a VPN Tunnel and a Port Forwarding menu option.

Figure 8 shows the User Portal screen with a Port Forwarding menu option only. The VPN Tunnel menu option is not displayed.



Figure 8. User Portal screen with a Port Forwarding menu option only.

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 14.
- **Change Password.** Allows users to change their passwords.
- **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 on the user's computer. The first time a user attempts to connect using the port forwarding tunnel, the NETGEAR port forwarding engine installs.
