Version 6.0

Part No. 318451-B Rev 00
August 2005

600 Technology Park Drive
Billerica, MA 01821-4130

Configuring SSL VPN Services on the Contivity Secure IP Services Gateway

NORTEL

Nortel Networks Inc. software license agreement

This Software License Agreement ("License Agreement") is between you, the end-user ("Customer") and Nortel Networks Corporation and its subsidiaries and affiliates ("Nortel Networks"). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

"Software" is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment ("CFE"), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer's Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided "AS IS" without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States

Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

Tables

Figures

Preface

This guide introduces the Nortel* Contivity* Secure IP Services Gateway SSL VPN.

Before you begin

This guide is for network managers who are responsible for setting up and configuring the Contivity Secure IP Services Gateway. This guide assumes that you have experience with windowing systems or graphical user interfaces (GUIs) and familiarity with network management.

Text conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is **ping** *<ip_address>*, you enter **ping 192.32.10.12**
bold Courier text	Indicates command names and options and text that you need to enter. Example: Use the **show health** command. Example: Enter **terminal paging** {**off** | **on**}.

braces ({})	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is **`ldap-server source {external | internal}`**, you must enter either **`ldap-server source external`** or **`ldap-server source internal`**, but not both.
brackets ([ ])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is **`show ntp [associations]`**, you can enter either **`show ntp`** or **`show ntp associations`**. Example: If the command syntax is **`default rsvp`** [**`token-bucket`** {**`depth`** | **`rate`**}], you can enter **`default rsvp`**, **`default rsvp token-bucket depth`**, or **`default rsvp token-bucket rate`**.
ellipsis points (. . .)	Indicate that you repeat the last element of the command as needed. Example: If the command syntax is **`more disk`***n*`:`*<directory>*`/...`*<file_name>*, you enter **`more`** and the fully qualified name of the file.
italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is **`ping`** *<ip_address>*, *ip_address* is one variable and you substitute one value for it.
`plain Courier text`	Indicates system output, for example, prompts and system messages. Example: `File not found.`

separator (>)	Shows menu paths. Example: Choose Status > Health Check.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is **`terminal paging`** {**`off`** | **`on`**}, you enter either **`terminal paging off`** or **`terminal paging on`**, but not both.

Acronyms

This guide uses the following acronyms:

ACK	acknowledgement
CA	certificate authority
CHAP	Challenge Handshake Authentication protocol
CRL	certificate revocation list
DN	distinguished name
DNS	domain name system
EAC	Extranet Access Client
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
IP	Internet Protocol
IKE	IPsec Key Exchange
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet service provider
L2TP	Layer2 Tunneling Protocol
LDAP	Lightweight Directory Access Protocol
LAN	local area network

MAC	media access control address
NAT	network address translation
NOC	network operations center
NTP	Network Time Protocol
OSPF	Open Shortest Path First
OSS	operations support systems
PAP	Password Authentication Protocol
PDN	public data networks
POP	point-of-presence
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
RSVP	Resource Reservation Protocol
RIP	Routing Information Protocol
SNMP	Simple Network Management Protocol
UDP	User Datagram Protocol
URL	uniform resource locator
VPN	virtual private network
VRRP	Virtual Router Redundancy Protocol
WAN	wide area network

Related publications

For more information about the Contivity Secure IP Services Gateway, refer to the following publications:

- *Configuring Servers, Authentication, and Certificates for the Contivity Secure IP Services Gateway* provides instructions for configuring authentication services and digital certificates.
- *Configuring Firewalls, Filters, NAT, and QoS for the Contivity Secure IP Services Gateway* provides instructions for configuring the Contivity Stateful Firewall and Contivity interface and tunnel filters.
- *Configuring Advanced Features for the Contivity Secure IP Services Gateway* provides instructions for configuring advanced LAN and WAN settings, PPP, frame relay, PPPoE, ADSL and ATM, T1CSU/DSU, dial services and Demand Services, DLSw, IPX, and SSL VPN.
- *Configuring Tunneling Protocols for the Contivity Secure IP Services Gateway* configuration information for the tunneling protocols IPsec, L2TP, PPTP, and L2F.
- *Configuring Routing for the Contivity Secure IP Services Gateway* provides instructions for configuring RIP, OSPF, BGP, and VRRP, as well as instructions for configuring ECMP, routing policy services, and client address redistribution (CAR).
- *Managing and Troubleshooting the Contivity Secure IP Services Gateway* provides information about system administrator tasks such as backup and recovery, file management, and upgrading software, and instructions for monitoring gateway status and performance. Also, provides troubleshooting information and inter operability considerations.
- *Reference for the Contivity Secure IP Services Gateway Command Line Interface* provides syntax, descriptions, and examples for the commands that you can use from the command line interface.
- *Configuring TunnelGuard for the Contivity Secure IP Services Gateway* provides information about configuring and using the TunnelGuard feature.

Hard-copy technical manuals

To print selected technical manuals and release notes free, directly from the Internet, navigate to www.nortel.com/products. Find the product for which you need documentation, then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems website at www.adobe.com to download a free copy of the Adobe Acrobat Reader.

How to get Help

This section explains how to get help for Nortel products and services.

Getting Help from the Nortel Web site

The best source of support for Nortel products is the Nortel Support Web site:

http://www.nortel.com/support

This site enables customers to:

- download software and related tools
- download technical documents, release notes, and product bulletins
- sign up for automatic notification of new software and documentation
- search the Support Web site and Nortel Knowledge Base
- open and manage technical support cases

Getting Help over the phone from a Nortel Solutions Center

If you have a Nortel support contract and cannot find the information you require on the Nortel Support Web site, you can get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the Web site below and look up the phone number that applies in your region:

http://www.nortel.com/callus

When you speak to the phone agent, you can reference an Express Routing Code (ERC) to more quickly route your call to the appropriate support specialist. To locate the ERC for your product or service, go to:

http://www.nortel.com/erc

Getting Help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, you can contact the technical support staff for that distributor or reseller.

Chapter 1
SSL VPN Overview

SSL VPN enables remote access to intranet resources (such as applications, mail, files, intranet Web pages) through a secure connection. The underlying protocol used for these sessions is SSL.

With SSL VPN activated, mobile workers, telecommuters, and partners can access information and applications on the intranet. Information accessible to the user is determined by access rules from the access control list (ACL) configured for the group in which a user is a member.

All SSL VPN services are available to the remote user on Contivity gateway IP addresses (physical and CLIP). The Contivity gateway distinguishes between services that it provides and the services the SSL VPN provides and immediately forwards the appropriate traffic to the SSL VPN module.

Traffic between users and SSL VPN virtual servers has either a destination IP address equal to the Contivity gateway physical IP or a CLIP address. You must use CLIP addresses when using SSL VPN if you want access from a user tunnel or branch office tunnel. A unique destination IP and port combination identifies virtual server traffic.

SSL VPN is added to the SSL acceleration features, which makes it possible to combine SSL acceleration and VPN.

Hardware platforms

The SSL VPN Module 1000 card has been supported on Contivity 1740, 2700, and 5000 platforms since Version 5.00 software. The software enforces the requirement of installation in slot 1. If you install the SSL card in a different slot, the software holds the card in reset and logs a persistent warning telling you to reinstall it in slot 1.

Features

The following features are supported on the software:

- Management
  - — Configuration through the SSL VPN Manager applet, which is launched from the Contivity Services > SSL VPN screen
  - — Ability to control remote access through Telnet and Secure Shell down to specific machines
- Performance

  Depending on the model, supports up to 600 SSL transactions per second for each Contivity Secure IP Services Gateway device. It scales up to 1000 users simultaneously logged in.
- Scalability and Redundancy

  Supports 256 virtual SSL servers and up to 1500 certificates
- Certificate and Key Management
  - — Private keys generated in Apache, OpenSSL, Stronghold, WebLogic, and Microsoft IIS 4.0 can be imported
  - — Supports client authentication, generation of client certificates, revocation of client certificates, and automatic retrieval of CRLs
  - — Supports Entrust
  - — Supports validation of private keys and certificates
  - — Supports generation of certificate signing requests (CSR)
  - — Supports creation of test certificates (self-signed)
  - — Supports automatic retrieval of Certificate Revocation Lists (CRL) through HTTP, TFTP, or LDAP (version 3)
  - — Supports PKCS7 certificates, where the user is prompted to select a certificate when the certificate file contains multiple certificates
  - — Supports adding an X-Client-Cert multiline HTTP header to a client request. Using this feature will make the Contivity gateway insert the entire client certificate (in PEM format) as a multiline HTTP header. The back end Web servers can then perform additional user authentication, based on the information in the client certificate. The back end servers can also make use of any auxiliary fields in the client certificate.
- Advanced Processing

  - — Supports rewriting of client requests—customized error messages can be sent to the client's Web browser if the browser is unable to perform the required cipher strength. Without this feature, the client request would simply be rejected during the SSL handshake.
  - — Ability to transmit extra SSL information to the back end servers, such as the negotiated cipher suite and client certificate information (in case client certificates were required by the virtual SSL server). The information is conveyed by configuring the virtual SSL server to add an extra SSL header to the client's request.
- Logging Capabilities
  - — Support for traffic logging through UDP syslog messages. UDP syslog messages for all HTTP requests handled by an SSL server can be sent to a configured syslog server. This feature can be used as an alternative to performing traffic logging on the back end Web servers in environments where traffic logging *must* be performed on the SSL terminating device itself, due to laws or regulations.
  - — Support for RADIUS accounting and auditing
- Supported Standards
  - — Supports SSL version 2.0 and 3.0, plus TLS version 1.0
  - — Supports SMTPs, POP3s, and IMAPs in addition to the standard HTTPS
  - — Supports SNMP version 1 and SNMP version 2c

Chapter 2
Using the SSL VPN portal

For a partner or mobile worker to access intranet resources from any computer with Internet connectivity, access is established through the clientless or browser-based mode. No manual software installation is required.

In clientless mode, all interaction with the intranet is done through HTTP, Java applets, and ActiveX controls, which gives the client full HTTP access to the intranet. Clientless mode also provides FTP and SMB (Windows file shares) access from the browser. All network traffic between the client and the Contivity Secure IP Services Gateway is sent through a secure SSL connection.

The clientless mode enables:

- Intranet browsing
- File server access from the portal screen
- HTTP proxy
- Telnet/SSH access
- Port forwarding

To enable the SSL VPN for more than 10 concurrent users, you must obtain a license key from Nortel. To obtain the license key, you must provide the MAC address of the SSL VPN Module 1000.

To obtain a license key, find out the MAC address of the SSL VPN Module 1000 on which the license must be installed. Launch the SSL VPN Manager from the Services > SSL VPN screen. Navigate to the Device IP > IP Address tab to view the MAC address of your SSL VPN Module 1000. Contact Nortel support and provide the MAC address to receive a license key.

Browser requirements

In clientless mode, any JavaScript and SSL-enabled browser works with the VPN portal. When utilizing the Telnet/SSH access, HTTP proxy and port forwarder, the following browser and Java combinations are supported:

- Windows

  Internet Explorer 5 or better with the Sun JRE 1.3 or better
  Internet Explorer 5 or better with the Microsoft JVM 4 or better
  Netscape Navigator 7 with the Sun JRE 1.3 or better
  Mozilla 1.3 or better with the Sun JRE 1.3 or better

- *nix

  Netscape Navigator 7 with Sun's JRE 1.3 or better
  Mozilla 1.3 or better with Sun's JRE 1.3 or better

Login screen

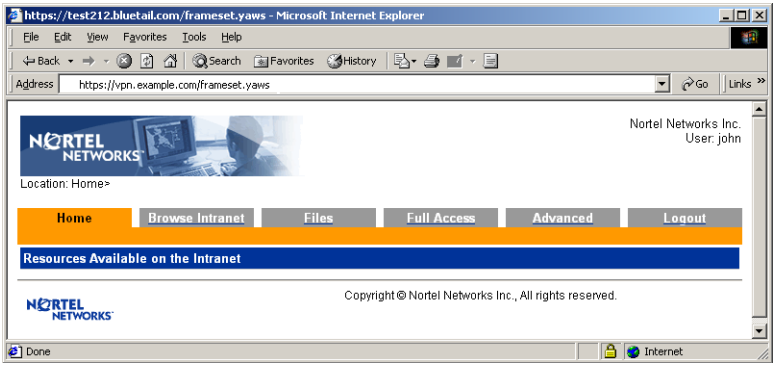
With the clientless mode, the user enters the VPN address to the portal (https://vpn.example.com) in the available Web browser and logs in using the login screen (Figure 1 on page 33).

Figure 1 Login screen

Unified access portal

Having successfully logged in, the SSL VPN Unified Access Portal screen is displayed as in Figure 2. The portal consists of different tabs from which the remote user can access intranet resources. The available resources are determined by the access rules associated with the user.

Figure 2 Unified access portal



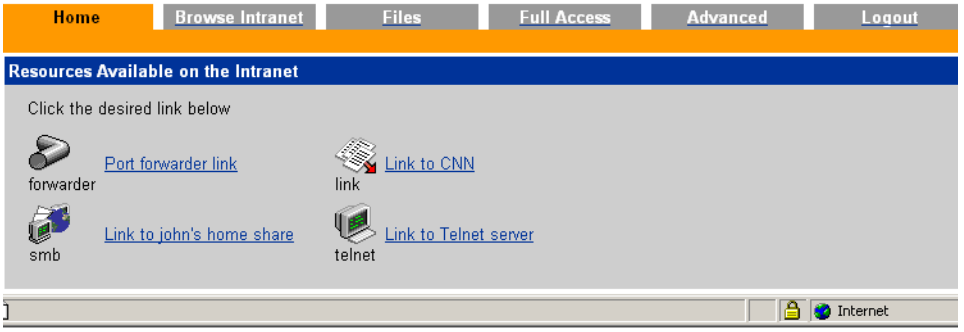
With clientless mode activated, the following services are enabled:

- Intranet Web browsing
- Access to SMB (Windows file shares) and FTP file servers
- Intranet mail access through external Web-based solutions, such as Outlook Web Access
- Telnet and SSH access to intranet servers through terminal Java applet
- Handling plugins, Flash, and Java applets using HTTP proxy Java applet
- Port forwarding (application tunneling) through SOCKS encapsulated in SSL

Home tab

The Home tab (Figure 3) is the default tab on the portal screen. If links are defined for access to specific Web pages or servers on the intranet, they are displayed here.

Figure 3 Home tab



The non-underlined text appearing under the “Resources Available on the Intranet” heading is a static link text.

Links are defined within the context of a particular user access group, which means that all remote users who are members in that group can access the links you define.

Examples of links are:

- SSL or clear-text link
- Automatic logon link to password-protected Web page (through SSL or clear-text)
- Link to FTP or Samba (SMB) file server

- Port forwarder link using SOCKS
- HTTP proxy link
- Link to Telnet or SSHv1 server
- Outlook

Browse Intranet tab

The Browse Intranet tab (Figure 4) allows access to a Web server on the intranet or Internet (for example, to visit a specific Web page or to access a Web mail server). To simplify access, you can also define a link to the desired URL on the Home tab.

Figure 4 Browse Intranet

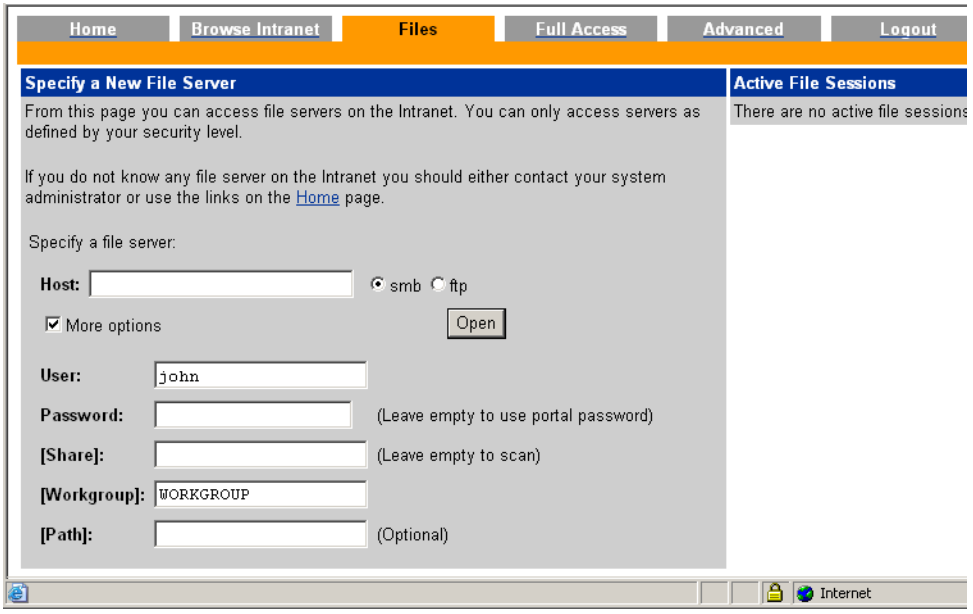
To access the Web server, type the URL or IP address in the available field and click on Open. When the user later clicks on a link on the requested Web page, the client browser sends the request to the Contivity gateway, such as http://inside.example.com. A new browser window opens, but now the request is rewritten with the Contivity gateway rewrite prefix (boldface); for example, https://vpn.example.com/http/inside.example.com. This ensures that the Contivity gateway secures traffic.

Note: Some URLs that include certain plug-ins, such as Flash or Java applets, may not display properly. To avoid this problem, configure an HTTP proxy link on the Home tab. Users with access to the Advanced tab can set up an HTTP proxy connection manually.

Files tab

The Files tab (Figure 5) lets you access an SMB (Windows file share) or FTP file server.

Figure 5 Files tab



To access the file server:

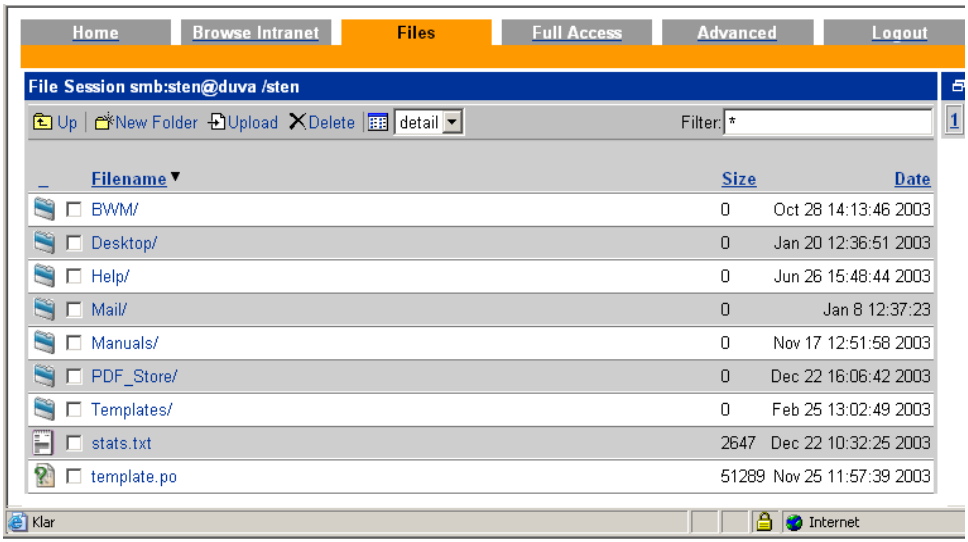
1. Enter the host name or IP address of the file server in the Host field. Also select the desired file server type, such as SMB (Windows file share) or FTP.
2. To display more options, select the More options check box.
3. To limit the view to a specific user's home share folder, enter the user's name in the [Share] field (optional). This field is ignored for FTP servers. To browse to a specific share folder, combine this field with the [Path] field.
4. To limit the view to a specific workgroup, enter the workgroup's name in the [Workgroup] field (optional). This field is ignored for FTP servers.
5. To specify a path to a specific folder, enter the desired path in the [Path] field. This field is dependent on what is entered in the [Share] field.

For example, to browse to the folder /temp/mystuff under the share folder john, enter john in the [Share] field and /temp/mystuff in the [Path] field.

6 Click on Open.

Files and folders contained in the specified folder appear by file type icon, file name, size, and date.

Figure 6 File session folder



- To open a folder, click on the folder name or icon.
- To open or download a file from the file server to your computer, click on the file name or icon.
- To step up one level in the folder hierarchy, click on Up.
- To create a new folder on the file server, click on New Folder, enter a folder name in the field Create new directory named, and click on Create directory.
- To upload a file from your computer to the file server, click on Upload. Locate the desired file in the window. To upload the file to the current folder, click on Start Upload.
- To delete a file or folder, select the corresponding box and click on Delete.
- To view files and folders as icons, select icons instead of detail in the box to the right of the Delete option.

- To limit the view to files of a specific format, enter the file extension after the asterisk (*) in the Filter field.

To simplify access, you can define a link to the file server on the Home tab.

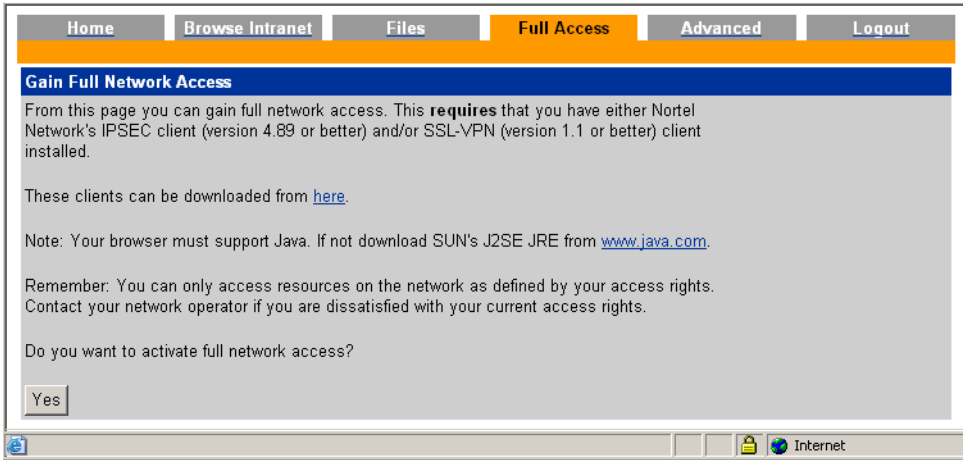
Full access tab

The Full Access tab provides a way for the remote user to launch the Contivity VPN client from within the portal. In a manner similar to when the user starts a VPN client manually, transparent access to the intranet is enabled and no further login to the VPN is required.

Transparent access implies that the user can request resources as if working from within the intranet with no further portal interaction required. Supported VPN clients are Nortel Contivity VPN client and Nortel SSL VPN client.

The Full Access tab (Figure 7) is not displayed on the portal by default.

Figure 7 Full Access tab



Contivity VPN Client

When downloaded, the Java applet checks whether the Contivity VPN client is installed and able to connect to a Contivity server. If so, the Contivity VPN client is silently activated on the remote user's machine. It automatically tries to authenticate to the Contivity server using either *group authentication* or *user name and password* authentication. The user name and password supplied on the Web portal are used for authentication to the Contivity server.

Having received information about user name and password, the Contivity server connects to a local or external authentication database (for example, RADIUS or LDAP) to authenticate the user. When the user is successfully authenticated, a secure IPsec tunnel is set up between the user's local machine and the Contivity server (not through the Contivity gateway). The remote user can now start any TCP-based client application to request an intranet resource. The user's group membership determines the access rights.

Note: Users and user groups should be configured on the Contivity server by the Contivity server administrator.

SSL VPN Client

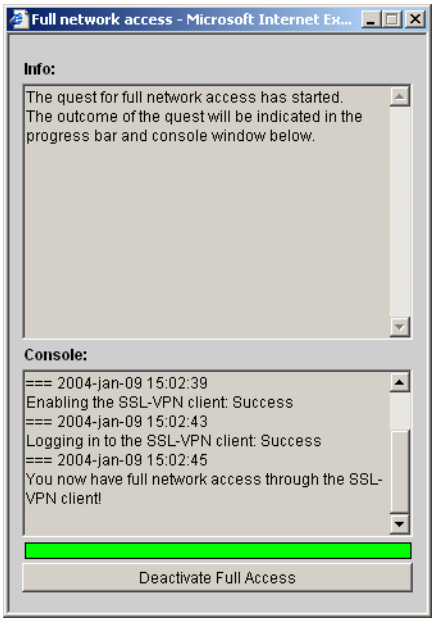
If the Contivity VPN client is *not* installed on the remote user's machine or unable to connect, the Java applet checks whether the Nortel SSL VPN client is installed and if it can connect to the Contivity gateway. If so, the SSL VPN client is silently activated on the remote user's machine. It automatically tries to authenticate to the Contivity gateway using the user name and password supplied on the Web portal.

When the user is successfully authenticated, a secure SOCKS tunnel (encapsulated in SSL) is set up between the remote user's machine and the Contivity gateway. The user can now start any TCP- or UDP-based client application to request the desired intranet resource. The user's group membership determines the access rights.

If neither of the VPN clients are installed or able to connect, intranet resources can only be accessed in *clientless mode* (by requesting resources from the other portal tabs).

Figure 8 shows the Java applet window when a connection to the Contivity gateway is established with the SSL VPN client.

Figure 8 Java applet window

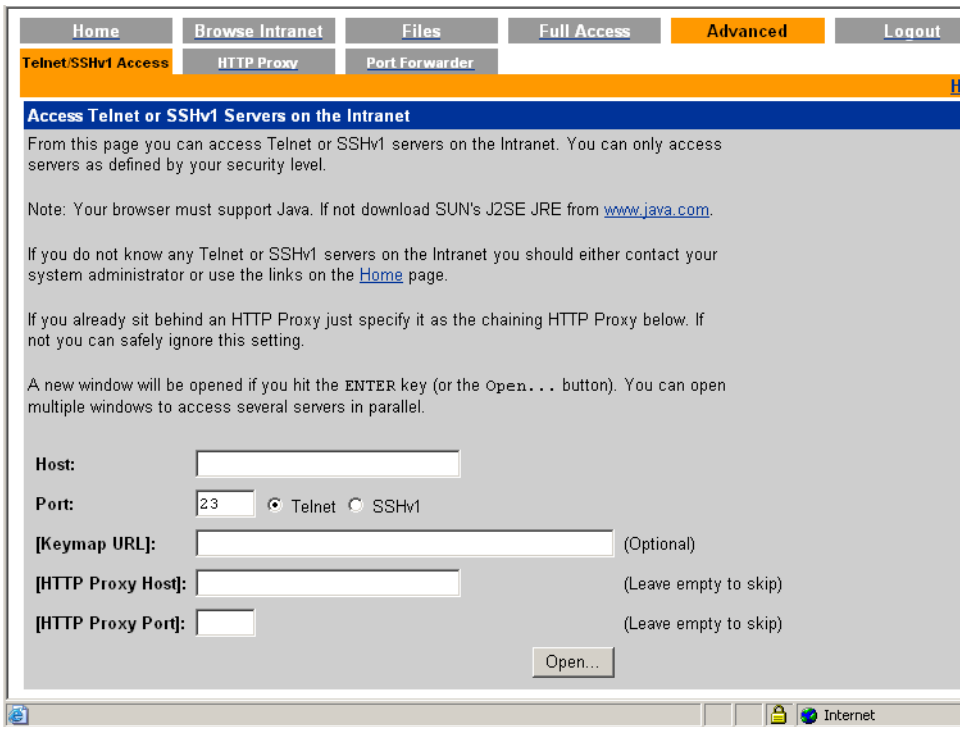


To close the connection to the intranet VPN server and exit the VPN client, click on the Deactivate Full Access button.

Advanced tab, Telnet/SSHv1 access

Telnet/SSHv1 access allows you to run a Telnet or SSH session to a specified server on the intranet. The session runs in a Java terminal emulation applet window. To simplify access, you can define a link to the server on the Home tab (Figure 7 on page 38).

Figure 9 Telnet/SSHv1 access



To start a session:

1 Enter the server's host name or IP address in the Host field.

2 Select the desired protocol (Telnet or SSH) to insert the relevant port number in the Port field. You can choose to modify the default SSH port 22 to 2222 and the default Telnet port 23 to 2323.

3 If you have a non-standard keyboard, you can use the [Keymap URL] field to point to a keyboard mapping file located on an intranet file server. Keystrokes to be sent to the remote server automatically translate to the proper keys. Syntax example: http://inside.example.com/keyCodes.at386.

   Documentation describing the configuration file properties can be found in Appendix E, Key code definitions".

4 In the [HTTP Proxy Host] and [HTTP Proxy Port] fields, enter the IP address and port number of an intermediate HTTP Proxy server (if any).

If you are working from a location requiring traffic to pass through an intermediate HTTP proxy server on the intranet, enter the IP address (or VPN name) and port of that proxy server. All applet traffic is tunneled to the Contivity gateway through the HTTP proxy server. The HTTP Proxy server has connect support.

Users should be informed if this step is required. If the HTTP proxy host and port fields are left blank, all applet traffic is tunneled directly to the Contivity gateway.

5 Click on Open. The browser login screen appears.

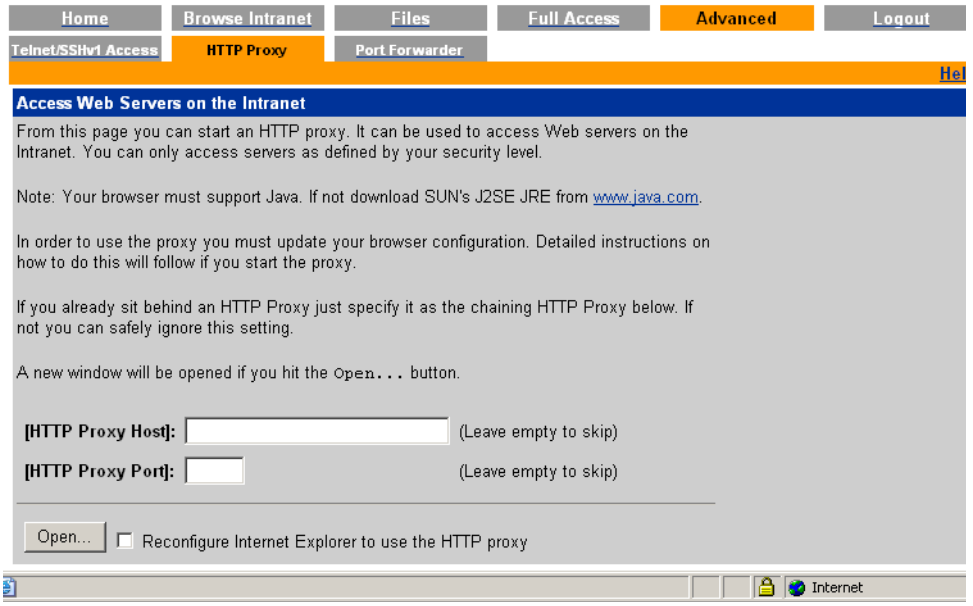
To quit the session, exit the terminal session and click on Close.

HTTP proxy advanced tab

The Browse Intranet tab allows access to the intranet Web pages in a secure mode. However, a Web page can contain plugins (for example, a Flash movie) which, in turn, can include embedded links to other Web pages. If a user executes such an embedded link, the HTTP request may not reach the Contivity gateway and the URL is not displayed.

To ensure display of all URLs (including ones that are embedded in plugins), use the HTTP proxy feature (Figure 10 on page 43) to download a Java applet to the client. Once the applet is downloaded, change the client browser's proxy settings to direct all HTTP requests to this Java applet. The Java applet in turn routes each request through a secure SSL tunnel to the Contivity gateway's proxy server, where it is unpacked and redirected to its proper destination.

Figure 10 HTTP proxy Advanced tab



To start an HTTP Proxy session:

1 In the [HTTP Proxy Host] and [HTTP Proxy Port] fields, enter the IP address and port number of an intermediate HTTP Proxy server (if any).

   If you are working from a location requiring traffic to pass through an *intermediate* HTTP Proxy server, enter the IP address (or VPN name) and port of that proxy server. All applet traffic is tunneled to the Contivity gateway through the HTTP proxy server. The HTTP proxy server has connect support.

   Users should be informed if this step is required. If the HTTP proxy host and port fields are left blank, all applet traffic is tunneled directly to the Contivity gateway.

2 If Internet Explorer is used as the client browser, select the check box Reconfigure Internet Explorer to use the HTTP proxy.

   With this check box selected, you do not have to change the browser's proxy settings manually; for example, Step 4 below can be ignored. Also, when you exit the HTTP Proxy session, the browser's original proxy settings are automatically restored.

3 Click on Open.

The user is asked to install a signed applet (certified by Nortel). When done, a Java applet window opens to confirm that an HTTP Proxy applet is started.

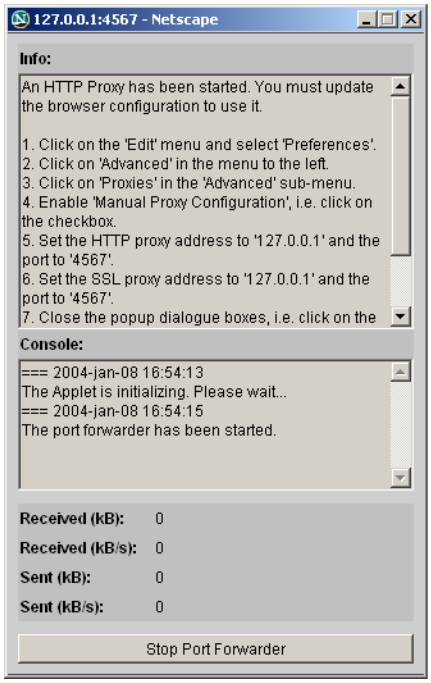
4 Reconfigure the browser's proxy settings (Figure 11 on page 45) (not required for Internet Explorer).

Unless Internet Explorer is used as client browser, you must reconfigure the browser's proxy settings manually. Instructions (related to the type of browser used) are displayed in the Info part of the Java applet window.

When the proxy settings are changed, you can open a new browser window and surf the intranet in encrypted mode through the Contivity gateway's HTTP Proxy. The Java applet window and the portal session must be active.

To quit the HTTP Proxy session, click on Stop Port Forwarder in the Java applet window. If the browser was reconfigured manually, change the browser settings back to the original settings.

Figure 11 Reconfigure browser proxy settings



Note: Outlook port forwarder links (if configured) or Outlook port forwarder portal sessions (Advanced tab) do not work if a proxy server is configured in the client browser.

Advanced tab, port forwarder

Using the Port Forwarder tab, you can set up a secure SSL connection to an intranet application server and run a TCP- or UDP-based client application. This is done by downloading a Java applet instructed to listen to a port number on the user's own computer. The applet then forwards all incoming traffic to the application server. The Port Forwarder tab includes two options:

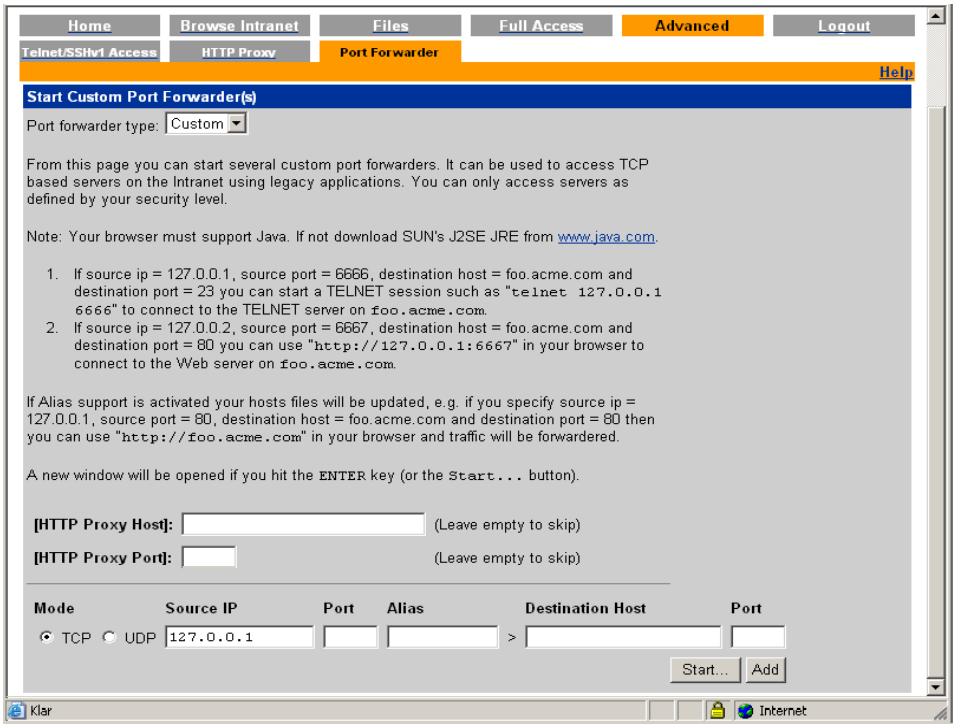
Custom

Outlook

Custom port forwarder

The custom port forwarder (Figure 12) allows you to start an optional TCP- or UDP-based application (for example, Telnet or Outlook Express). To start a custom port forwarder, keep the `Custom` option in the Port forwarder type box.

Figure 12 Custom port forwarder



Access to Outlook Express example

In this example, the user wants to access the intranet's POP3 and SMTP mail servers using Outlook Express.

Supply the following information:

1 In the [HTTP Proxy Host] and [HTTP Proxy Port] fields, enter the IP address and port number of an intermediate HTTP Proxy server (if any).

If you are working from a location requiring traffic to pass through an *intermediate* HTTP Proxy server, enter the IP address (or VPN name) and port of that proxy server. All applet traffic is then tunneled to the Contivity gateway through the HTTP proxy server. The HTTP Proxy server has connect support.

Users should be informed if this step is required. If the HTTP Proxy host and port fields are left blank, all applet traffic is tunneled directly to the Contivity gateway.

2. Under Mode, select the desired packet transfer protocol; for example, TCP or UDP.
3. In the Source IP field, enter an IP address in the 127.x.y.z range; for example, 127.0.0.1.
4. In the Port field, enter a free "local" port number; for example, 5025.

   Port numbers just above 5000 are usually free to use. The application-specific port number can also be used; for example, 25 for SMTP.

5. Using the [Host Alias] box (optional) is explained on the next screen.
6. In the Destination Host field, enter the VPN name (or IP address) of the intranet server you want to connect to; for example, pop3.example.com.
7. In the Port field, enter the application-specific port number; for example, 110 for a POP3 session.
8. Click on Add to display a second row of input fields.

   To set up a connection to the SMTP server, enter a new IP address in the 127.x.y.z range in the Source IP field (for example, 127.0.0.2), enter a new port number in the Port field (for example, 5026), and enter the IP address or VPN name to the SMTP server in the Destination Host field and the port to use in the Port field (for example, 25).

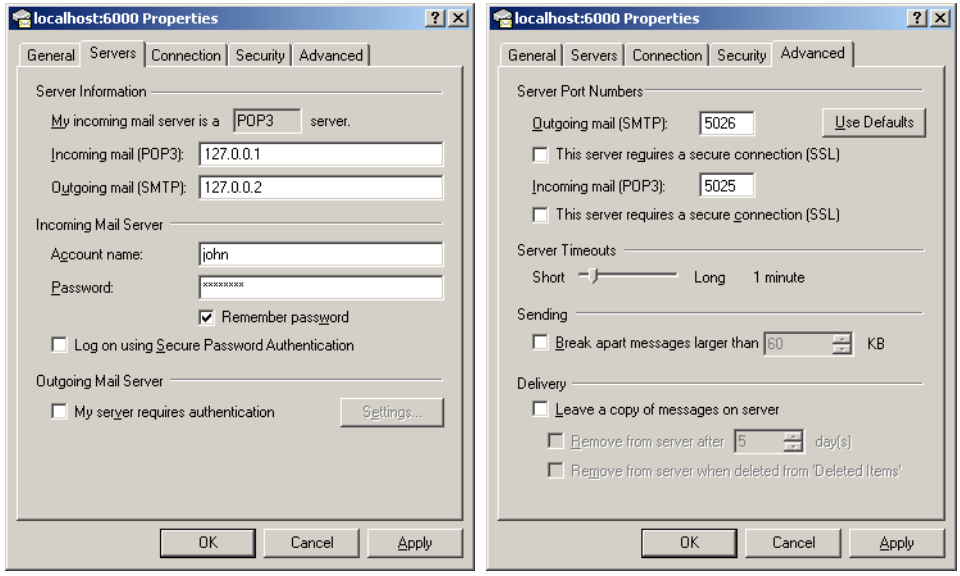
9. Click on Start.

   You are asked to install a signed applet for this session. When you accept, a Java applet window opens to confirm the information specified for the port forwarders.

Client application configuration example

Now two connections are established, one to the POP3 server and one to the SMTP server as shown in Figure 13. In the client application, in this case Outlook Express, specify that incoming and outgoing mail is delivered to, and collected by, hosts 127.0.0.1 and 127.0.0.2, respectively.

Figure 13 Local host properties



The port numbers to use are the ones entered in the “local” Port field for the POP3 and SMTP servers, respectively; for example, 5025 and 5026. By entering the application-specific port numbers in the “local” Port field, for example, 110 (for POP3) and 25 (for SMTP), you can keep existing port number settings in the mail client.

If the Alias check box is selected, and application-specific port numbers are used as “local” port numbers, no modifications to the client application are required. The address specified as destination host automatically maps to the specified source IP. Note that use of host aliases is only possible if the user has administrator privileges on his client *or* has write access enabled for hosts and lmhosts files. Hosts and lmhosts files are located in %windir%\hosts on Windows 98 and ME and in %windir%\system32\drivers\etc\hosts on NT, XP and Windows 2000.

If you expect the connection to include more than 15 minutes of inactivity, increase the TCP connection idle timeout value.

To quit the port forwarder, click on Stop Port Forwarder in the Java applet window.

Telnet port forwarder

To establish a secure Telnet session using the custom port forwarder, proceed as described above, only enter the host address to the Telnet server in the Destination Host field (for example, telnet.example.com) and port number 23 in the “remote” Port field instead. The user can then start the Telnet client and connect to, for example, 127.0.0.1 5025. If the Alias check box is selected, the user can instead connect to the actual destination host and the local port number in the Telnet client, for example, telnet.example.com 5025. The address specified as destination host automatically maps to the specified source IP.

HTTP port forwarder

To establish a secure HTTP session using the custom port forwarder, proceed as described above, only enter the host address to the Web server in the Destination Host field and port number 80 in the “remote” Port field instead. The user can then start his or her browser and type for example, 127.0.0.1:5025 in the Address field. If the Alias check box is selected, the user can instead type the actual URL and the local port number in the browser’s Address field, for example, www.example.com:5025. The address specified as destination host automatically maps to the specified source IP.

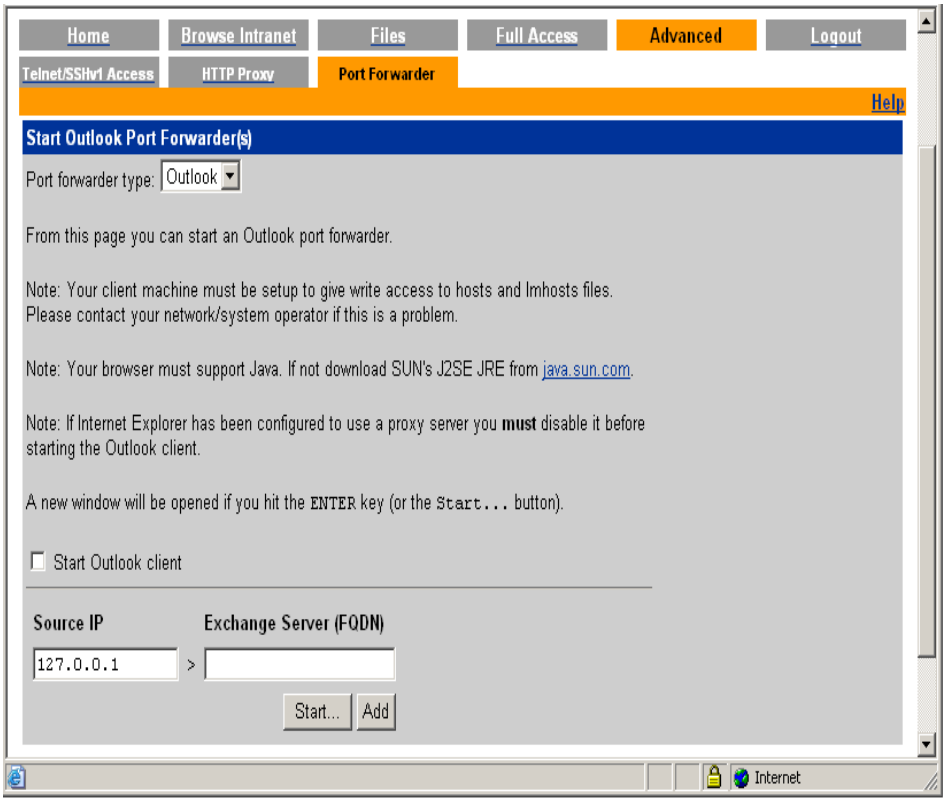
Port forwarder links

To simplify access, the Contivity gateway operator can define custom port forwarder links on the Home tab. The gateway operator can define the custom port forwarder link to launch the application automatically.

Native Outlook port forwarder

You can use the Outlook port forwarder (Figure 14 on page 50) to start a native Outlook session to a specified Exchange server on the intranet. To start the Outlook port forwarder, select the Outlook option in the Port forwarder type box. This displays a different set of input fields.

Figure 14 Outlook port forwarder



For the Outlook port forwarder to work, the following prerequisites must be fulfilled:

- The Exchange server's VPN name must be configured using the Server ID > DNS tab > Search List parameter. Using the above example, enter example.com in the Search list. If several Exchange servers are used, all the Exchange servers' VPN names must be configured in the DNS search list.
- You must have administrator's rights on the user's computer *or* have write access enabled for hosts and lmhosts files. Hosts and lmhosts files are located in %windir%\hosts on Windows 98 and ME and in %windir%\system32\drivers\etc\hosts on NT, XP and Windows 2000.
- The Outlook port forwarder is used by clients connecting to the Contivity gateway from outside the intranet. If the client has direct connectivity to the intranet, the port forwarder fails. If the client has access to intranet DNS servers, communication fails as well.

- Your Outlook account must be hosted on the Exchange server(s) specified in the port forwarder.
- Your client machine must be of the Hybrid or Unknown node type. You can check the node type by entering ipconfig /all at the DOS prompt.

To change the node type to Hybrid (if needed), go to the registry editor folder HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters. If it is not already present, add a new DWORD Value called NodeType. Double-click NodeType and enter 8 in the Value Data field. Click on OK and restart the computer.

- The Outlook port forwarder does not work if a proxy server is configured in the client browser. This also means that an HTTP Proxy link or HTTP Proxy portal session (Advanced tab) cannot be active at the same time as the Outlook port forwarder.
- If a firewall exists between the Contivity gateway and the Exchange server, the firewall settings must allow traffic to the required Exchange server ports. Note that these can vary with your environment. More information can be found at **support.microsoft.com**, such as Knowledge Base Articles 280132, 270836, 155831, 176466, 148732, 155831, 298369, 194952, 256976, 302914, 180795 and 176466.
- When a user clicks on an embedded link in an e-mail message, the Web site associated with the link must be displayed in a new instance of Internet Explorer. In Internet Explorer, go to the Tools menu and select Internet Options. Under the Advanced tab, go to Browsing and deselect the “Reuse windows for launching shortcuts” option.
- If you expect the connection to include more than 15 minutes of inactivity, increase the TCP connection idle timeout value, using the /cfg/ssl/server #/tcp/ckeep command.

Supply the following information on the Port Forwarder tab:

1. Select the Start Outlook client check box if Microsoft Outlook starts automatically when the port forwarder is started.
2. In the Source IP field, enter an IP address in the 127.x.y.z range; for example 127.0.0.1.
3. In the Exchange Server (FQDN) field, enter the fully qualified VPN name (FQDN) of the Microsoft Exchange Server; for example, exchange.example.com.

4 Click on Add to enter information for yet another Outlook port forwarder.

Services provided (mail, calendar, address book) can be distributed between different Exchange servers. If this is the case, you can create several Outlook port forwarders where the relevant Exchange servers can be specified.

If several port forwarders are required, note that each port forwarder must have a unique source IP address. A new source IP address is automatically suggested by the system if you choose to add another port forwarder.

5 Click on Start.

You are asked to install a signed applet for this session.

6 Click on Yes.

A Java applet window opens to confirm the information specified for the port forwarders. Carefully read the instructions, warnings and validation messages provided in the Java applet window. If the port forwarder is not configured to start the Outlook client automatically, wait until the applet is fully initialized before invoking the Outlook client manually.

7 Start the Outlook client (if not started automatically).

8 To quit the session, exit the Outlook client, then click on Stop Port Forwarder in the Java applet window.

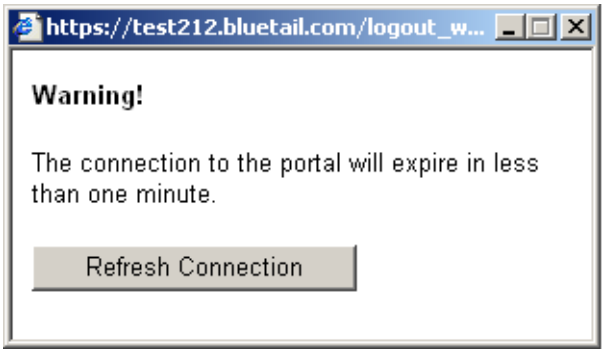
Note: Do not close the Java applet window as the last browser window, because the host's files may not clean up properly.

Logout tab

The Logout tab simply contains a button to confirm that you want to log out. However, you are logged out automatically after the time specified as Time To Live for the VPN, using the /cfg/vpn #/aaa/ttl command.

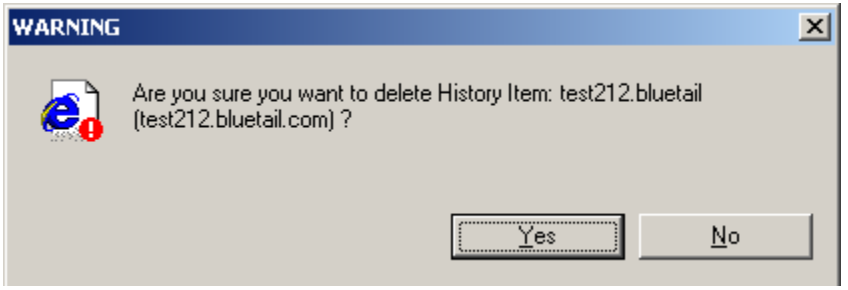
One minute before you are automatically logged out, a message displays (Figure 15 on page 53) that warns you about the upcoming logout and offers to refresh the portal connection.

Figure 15 Logout warning



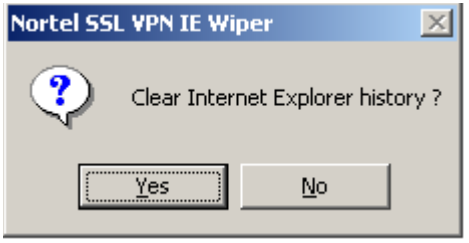
If files have been cached during the portal session, the following message on Figure 16 is displayed when you log out. By clicking on Yes, the cache is cleared.

Figure 16 Warning message



When the browser window is closed, you also have the option to clear the browser history as shown in Figure 17.

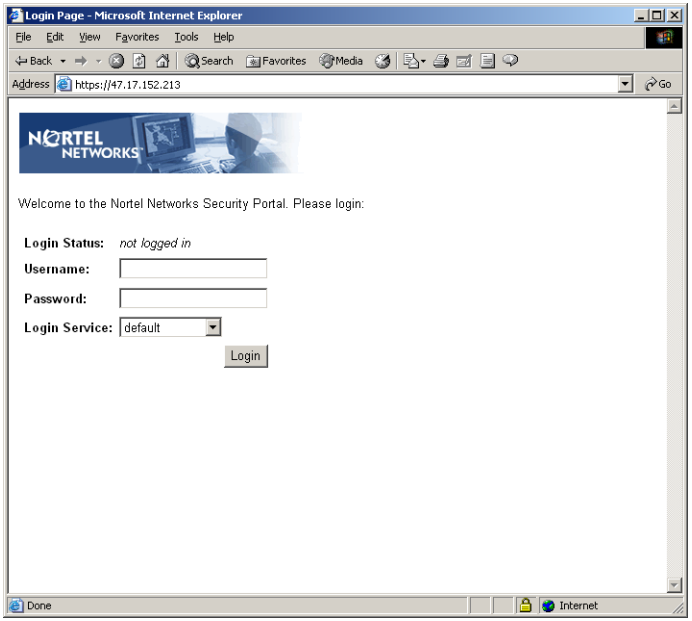
Figure 17 Clear browser history



9 Use a known user name and password as configured on the Contivity gateway for login as shown in Figure 18 on page 54. This works because you created mirrored SSL VPN groups from the Contivity groups using the wizard earlier.

On the first login from any PC, you are prompted to install and run the "Nortel Cache Wiper." It is strongly advised for security purposes to download this ActiveX component. You can disable this feature on the portal in the manager in Server > Server 1 > Portal > "Use ActiveX Component For Clearing Cache."

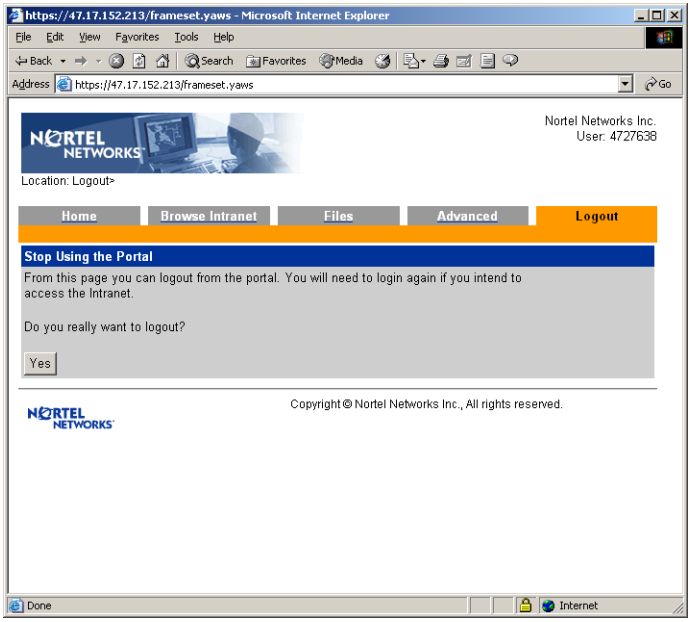
Figure 18 Portal login screen



10 A successful login brings up the portal home page. Although you still need to add links to the portal tabs, SSL VPN access is established and you can browse the intranet using an IP address or DNS name using the Browse Intranet tab.

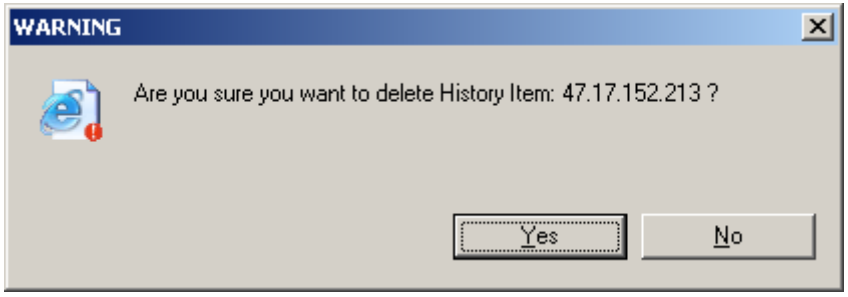
11 To log out, select the logout tab (Figure 19 on page 55). Click on Yes to logout.

Figure 19 Portal logout screen



12 A message box (Figure 20) prompts you to clear the browser history cache. For security reasons it is recommended that you select Yes to clear the cache. You are returned to the portal Login screen upon logout.

Figure 20 Delete history message



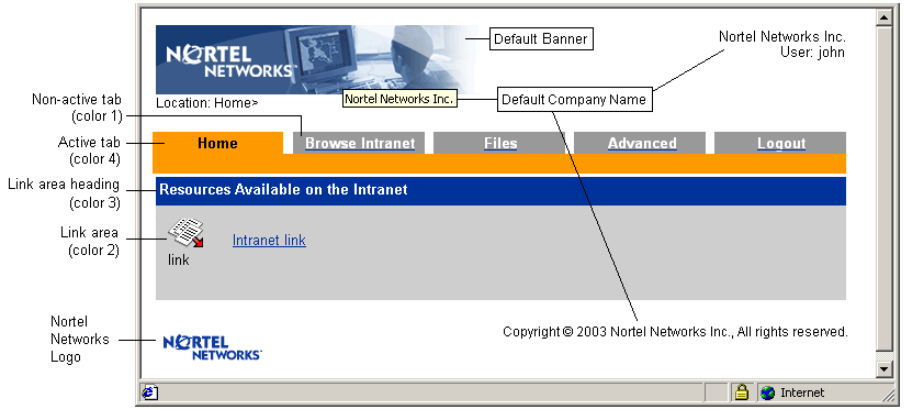
This completes the basic setup for SSL VPN. Having tested the portal, the next step is to customize your server settings. You may want to add access rules to allow or disallow services for different groups or add some links. At this point, substitute the test Certificate for a real certificate, signed by a CA Authority.

Customizing the SSL VPN Manager GUI

Default appearance

The default appearance of the portal is displayed in Figure 21.

Figure 21 Default portal



Colors are defined as hexadecimal codes. The default colors are:

- Non-active tabs — Dark gray (#999999)
- Link area — Light gray (#CECECE)
- Link area heading — Dark blue (#003399)
- Active tab — Orange (#FF9900)

Common colors

The table below lists a number of common Web safe colors. For further reference, search the Internet for “web colors” to access sites with full reference to hexadecimal color codes.

Table 1 Common colors with hexadecimal color codes.

Color	Hexadecimal code
White	FFFFFF
Black	000000
Dark gray	A9A9A9
Light gray	D3D3D3
Red	FF0000
Green	008000
Blue	0000FF
Yellow	FFFF00
Orange	FFA500
Violet	EE82EE
Dark violet	9400D3
Pink	FFC0CB
Brown	A52A2A
Beige	F5F5DC
Lime green	32CD32
Light green	90EE90
Dark blue	00008B
Navy	000080
Light sky blue	87CEFA
Medium blue	0000CD
Dark red	8B0000

Changing colors

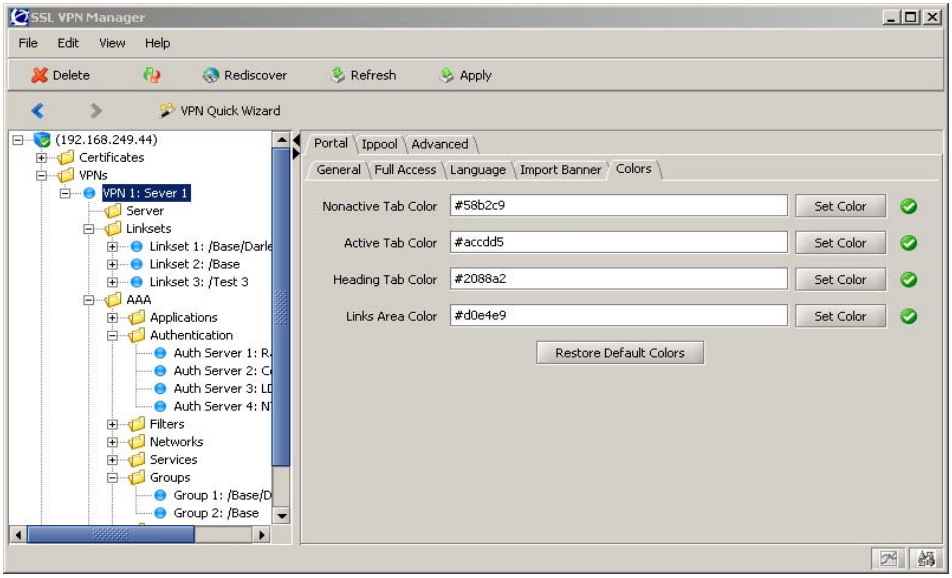
To change the portal colors (Figure 22 on page 58):

1 Select the VPN ID for which you wish to change the colors.

2 Select the Portal tab.

3 Select the Colors tab.

Figure 22 Change colors



4 Configure the colors as desired.

5 Click the Set Color buttons to make the changes.

Changing banner images

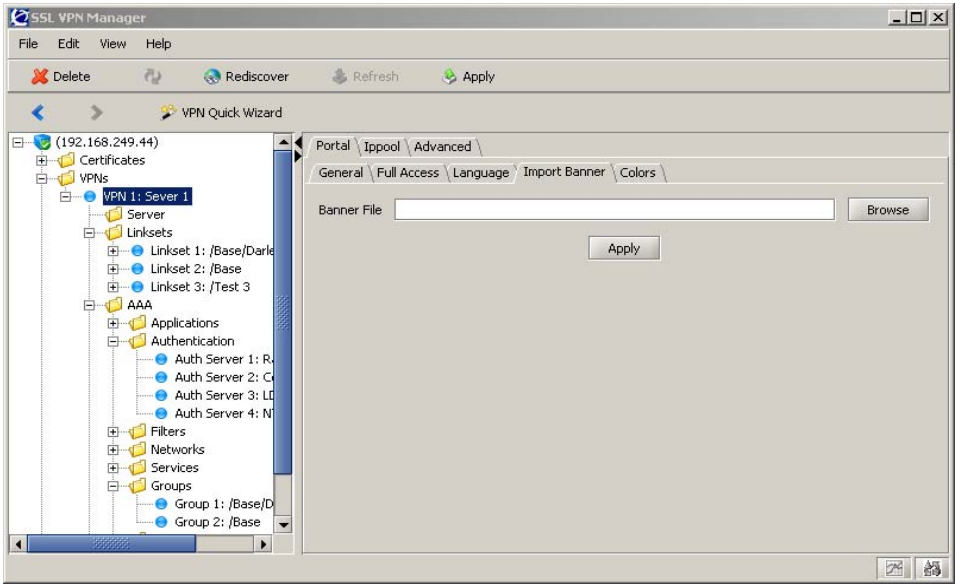
To substitute the Nortel banner image for your own company banner (Figure 23 on page 59), make the desired image file (in .gif format) available on a TFTP or FTP server. Then proceed as follows:

1 Select the VPN ID for which you wish to change the logo.

2 Select the Portal tab.

3 Select the Import Banner tab.

Figure 23 Change banner



4 Browse to the banner image.

5 Click Apply.

When the upload image is complete and the changes are applied, the current banner image on the portal Web page is replaced. Note that users currently logged in do not notice the change unless they reload the portal Web Page.

Changing company name

The company name is displayed at the top right on the portal page and in the copyright notice at the bottom of the portal screen. It is also shown as a tool tip when you move the mouse pointer over the logo and as the browser window name.

1 Select the VPN for which you wish to change the logo.

2 Select the Portal tab.

3 Select the General tab.

4 Rewrite the company name in the Company field.

Hiding logo

To hide the Nortel logo displayed at the bottom left on the portal:

1. Select the VPN for which you wish to change the logo.
2. Select the Portal tab.
3. Select the General tab.
4. Set the Nortel Brand Name parameter to Off.

Changing static text on login screen

The static text displayed on the portal login screen can be changed. The default text is "*Welcome to the Nortel Networks Security Portal. Please log in:*".

1. Select the VPN for which you wish to change the logo.
2. Select the Portal tab.
3. Select the General tab.
4. Type or paste the desired text message in the Login Text field. Click on Enter to create a new line and type three periods "..." (without the quotation marks).

Checking new appearance

To check the new appearance of the portal (Figure 24 on page 61), connect to the portal by entering the VPN name in your browser. The default logo is replaced on the Login screen as well as on the portal.

Figure 24 Verify changes

After login, the portal is displayed with a new logo, company name, static link text and color (Figure 25 on page 62).

Changing the language

To select the language used in the SSL VPN Manager:

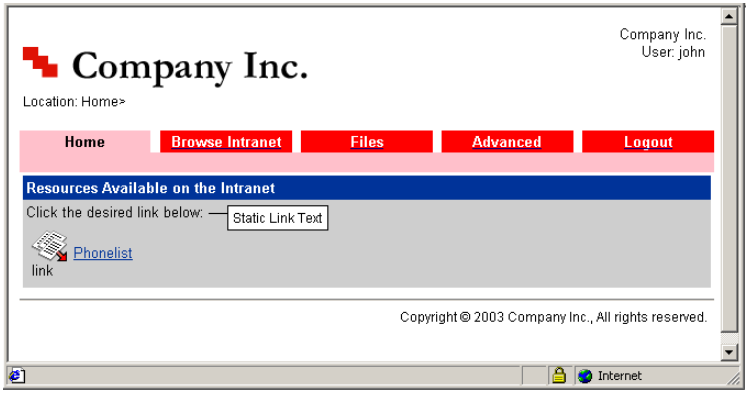
1. Select the VPN for which you wish to change the language.
2. Select the Portal tab.
3. Select the Language tab.
4. Select the desired language from the drop-down list.

Redirecting visitors

Naming login services

To support redirection to a specific authentication server, such as token login or redirection to a specific Windows domain, assign a display name to the authentication method. This name is selectable in the Login Service list on the portal login screen and in the SSL VPN client login window. It directs the user to the correct server for authentication. If the user selects the `default` option in the Login Service list, authentication is carried out according to the configured authentication order.

Figure 25 Updated view



Automatic redirection to internal site

To automatically redirect a visitor to an internal site by passing the default portal altogether:

1. Select the VPN for which you wish to change the logo.
2. Select the Portal tab.
3. Select the General tab.
4. Enter the site to which to redirect the user in the Redirect URL field.

To enable a visitor to log out from the portal from the internal site, insert a logout link on that screen. This is what it might look like:

```
<a href=https://vpn.example.com/logout.yaws> Logout from portal </
a>
```

Group-controlled redirection to internal sites

Using the <*group*> macro, you can also redirect visitors to different internal sites, depending on their group membership.

1. Select the VPN for which you wish to change the logo.
2. Select the Portal tab.
3. Select the General tab.
4. Insert a logout link on the internal site.

To enable a visitor to log out from the portal from the internal site, insert a logout link on that screen.

Note: In the same way as the <*group*> macro, the <*user*> macro can be used to control the action taken, depending on which user is currently logged in.

Chapter 3
Configuring the SSL VPN Module

This chapter provides information about SSL VPN Module initialization and initial configuration.

To configure the SSL VPN module, complete the following steps:

a Initialize the SSL VPN module.

b Enable DNS proxy and RADIUS service.

c Enable Contivity Stateful Firewall.

d Launch the SSL VPN Manager.

e Configure SSL VPN system settings.

f If required, upgrade and activate SSL VPN software.

g Generate certificates.

h Create a VPN portal with the VPN Quick Wizard.

i Update DNS servers.

j If required, configure the NetDirect Agent.

Configuration considerations

The following considerations should be noted:

- The Contivity gateway provides most services for SSL access and acts as a RADIUS server and DNS proxy service for the SSL device.
- Groups on the SSL card can mirror those on the Contivity gateway by using the wizard in the SSL VPN Manager applet. Groups that mirror the Contivity gateway groups are given SSL VPN access.

- You cannot use the same TCP port on any Contivity gateway interface for a Contivity service *and* an SSL service.

  For example, if you use SSL to manage the Contivity gateway on the public interface on TCP port 443, you cannot set up an SSL portal on this same interface on TCP Port 443. If this misconfiguration occurs, the SSL device always takes priority; therefore you can no longer manage the Contivity gateway using SSL from the public interface. Nortel recommends that you change the Contivity SSL port to a non-standard port from the Contivity gateway Services > SSLTLS screen.

- If you require access over a tunnel, you must use a CLIP address.
- When configured, the physical private interface of the Contivity gateway has the following four IP addresses assigned to it:
  - Contivity management IP address
  - Contivity interface IP address
  - SSL management IP address
  - SSL interface IP address
- If the SSL VPN applet time zone does not match the Contivity time zone and you see errors, set the time zone to the correct one by using the following command:

  ```
  tzone "Etc/GMT-5".
  ```

Initializing the SSL VPN Module

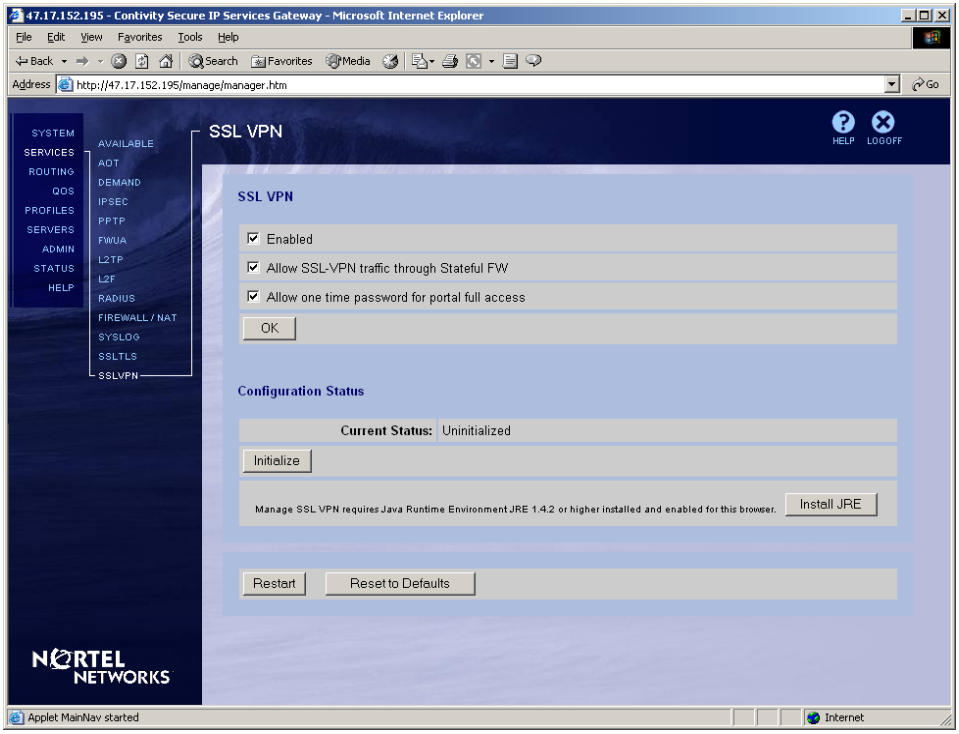
Before you configure the SSL VPN Module, you must initialize it to ensure that the Contivity gateway can communicate with it.

Note: The SSL VPN card takes time rebooting before it reaches operational status.

To initialize the SSL VPN Module:

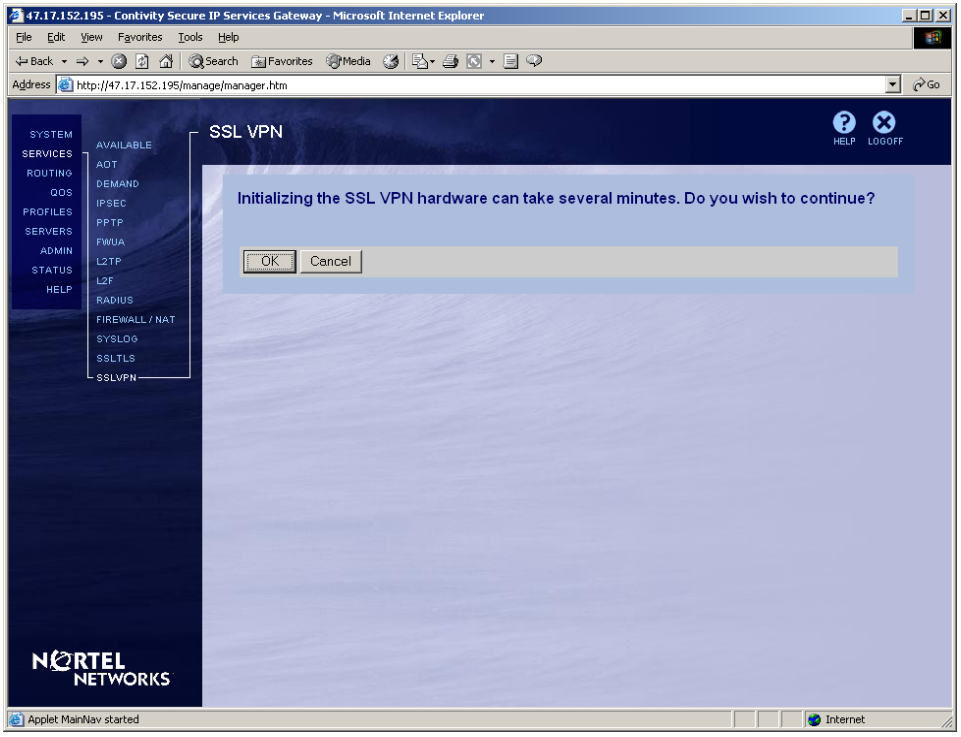
1. Log in to the Contivity gateway.
2. Select Services > SSL VPN.

Figure 26 SSL VPN screen



3 Click on Initialize in the Configuration Status section of the screen. The next screen advises you of the time it takes to initialize the hardware.

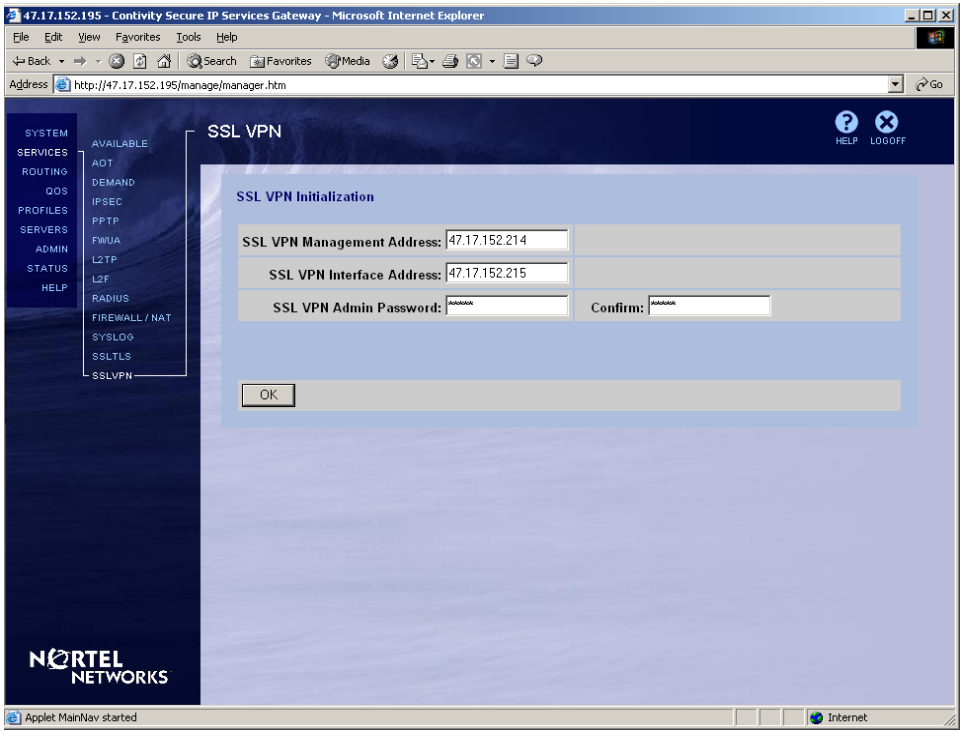
Figure 27 Initialization time



4 Click on OK to confirm that you want to continue.

5 The SSL VPN screen is redrawn with the SSL VPN Initialization screen showing the fields required for initialization.

Figure 28 Required initialization fields



6 Enter the following:

- SSL VPN management address

  This IP address provides access to the SSL VPN Module 1000 for management through the SSL VPN Manager applet. The IP address must also be within the management subnet as defined on the Contivity gateway.

- SSL VPN interface address

  This IP address is used as the source IP address for all proxy requests that the SSL VPN makes to private-side back end servers. The IP address must also be within the management subnet as defined on the Contivity gateway.

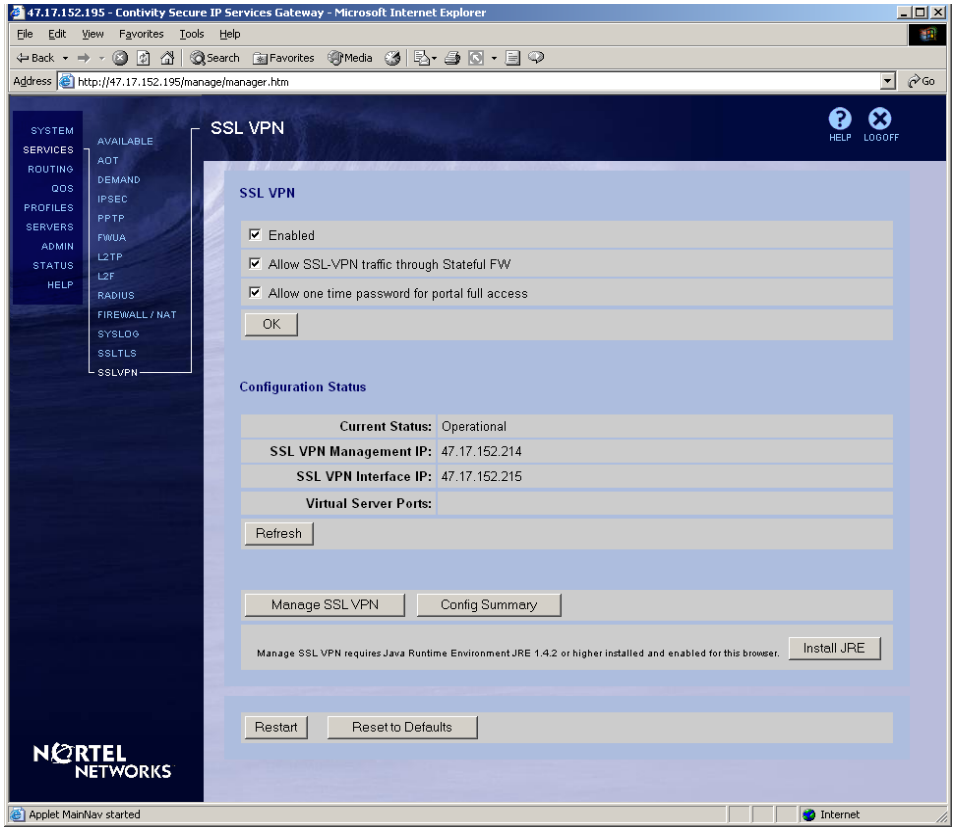
- SSL VPN admin password

This sets the password for the Admin account on the SSL VPN module. The Contivity gateway needs this password to support the card initialization and subsequent configuration and monitoring that occurs over a private control channel.

7 Click on OK. It takes approximately a minute to complete the initialization.

The Services > SSL VPN screen is updated. Because there are no SSL VPN servers configured, the Virtual Server Ports section is empty.

Figure 29 Initialized SSL VPN



Configuring Web interface parameters

To utilize the Contivity gateway for RADIUS authentication service or DNS proxy, you must enable them. When you enable DNS proxy, define a primary DNS server and configure the Contivity Stateful Firewall or interface filters to support the SSL VPN.

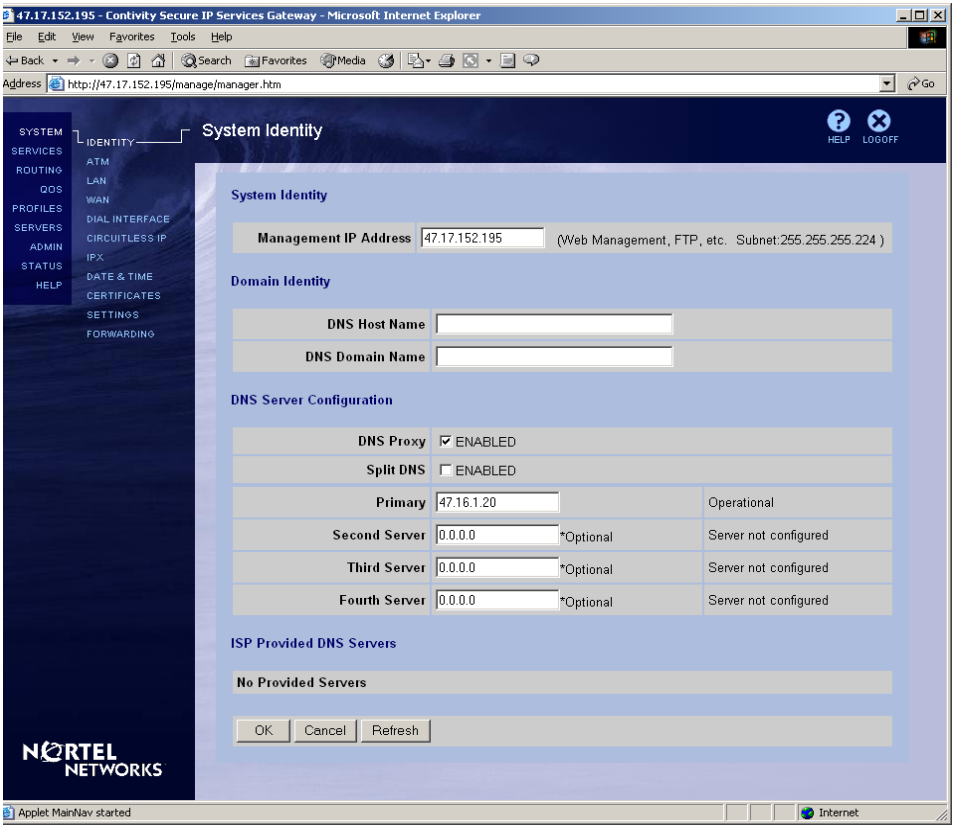
To define a DNS server:

1 Select System > Identity Figure 30 and ensure that:

   a The Contivity has a functional Primary DNS server configured.

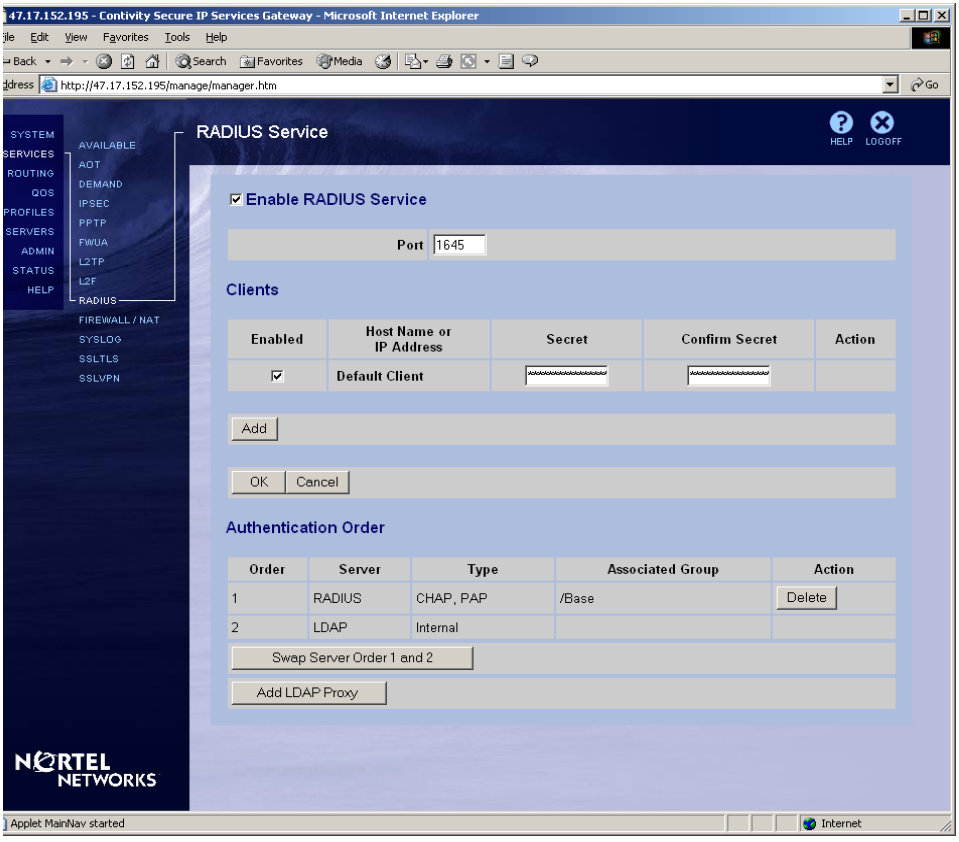
   b The Contivity gateway has DNS Proxy enabled in the DNS Server Configuration section of the screen.

Figure 30 System Identity screen



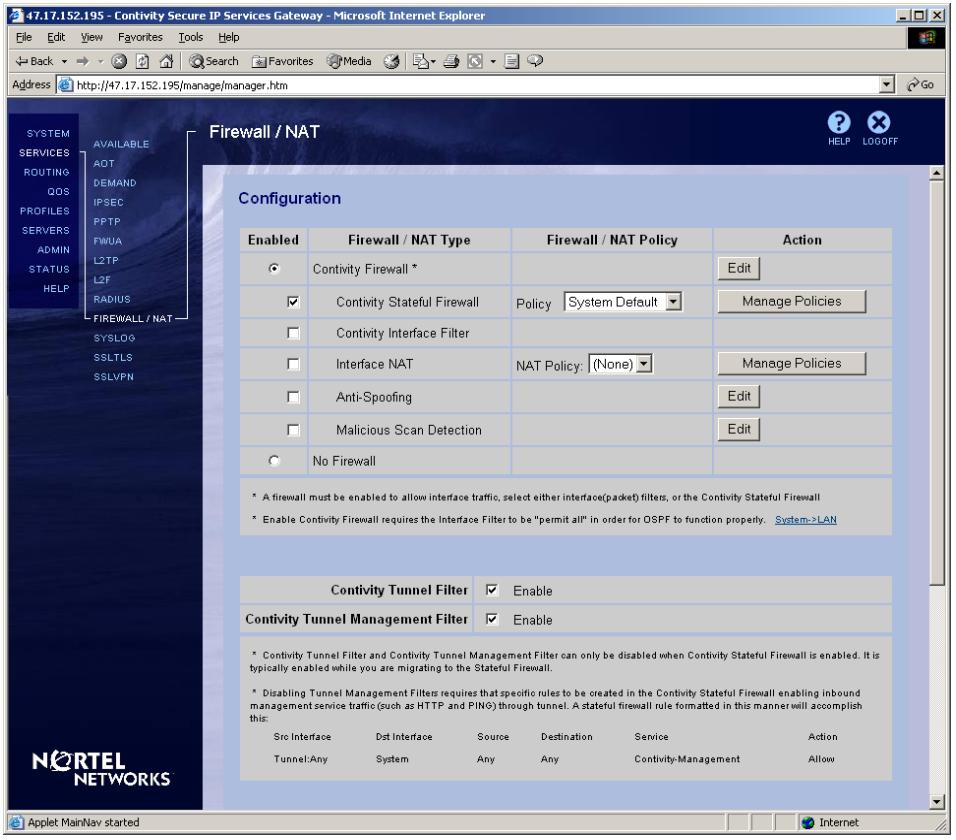
2 Select Services > RADIUS to enable RADIUS Service (Figure 31). Enable the default client and enter a shared secret. Set the Authentication order to match how you are authenticating Contivity users.

Figure 31 RADIUS Service screen



3 Select Services > Firewall/NAT in the Contivity Web interface (Figure 32 on page 73).

Figure 32 Firewall/NAT screen



4 You must enable either the Contivity Stateful Firewall or Contivity interface filters to support SSL VPN access. If you are unfamiliar with interface filters, go to the System > LAN screen and configure the private interface for Permit All. If you use the Stateful Firewall, ensure that Allow SSL-VPN traffic through Stateful FW is checked on the Services > SSL VPN page. If Stateful FW is checked, implied rules are automatically added, giving the SSL VPN the access it needs. When you enable either type of firewall for the first time, you must reboot. If you reboot, continue with the next step after restart.

5 Go to Services > SSLVPN and check to ensure that the status is “Operational”.

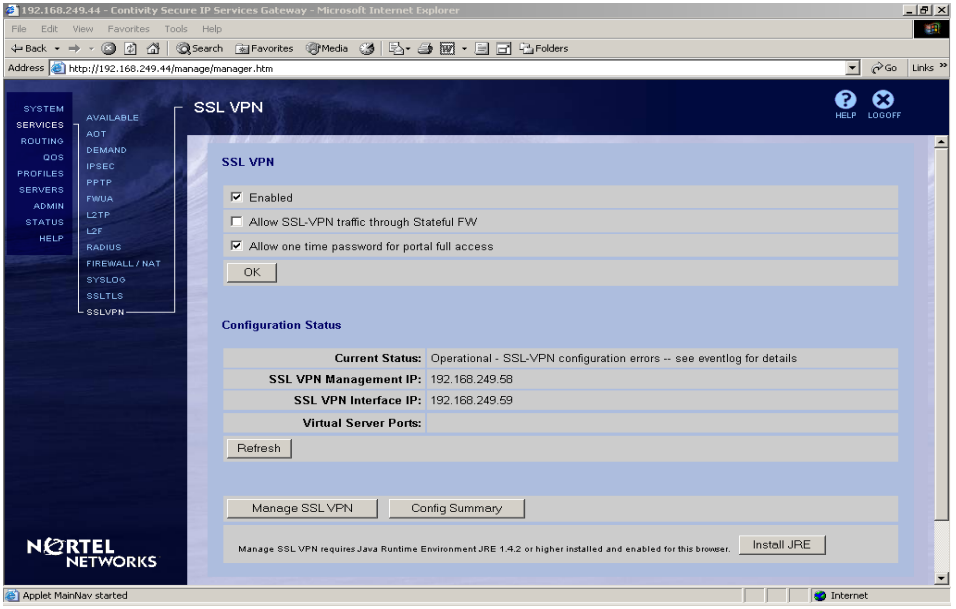
SSL VPN and Contivity Stateful Firewall

The SSL VPN fully integrates with the Contivity Stateful Firewall, and access can be permitted or denied through Firewall settings.

Contivity Stateful Firewall has two ways to configure SSL VPN access:

1. In the Contivity gateway Web management interface select the Services > SSL VPN screen and check the option Allow SSL-VPN traffic through Stateful FW (default setting).
2. In the Contivity gateway Web management interface, select the Services > SSL VPN screen Figure 33 and uncheck the option Allow SSL-VPN traffic through Stateful FW.

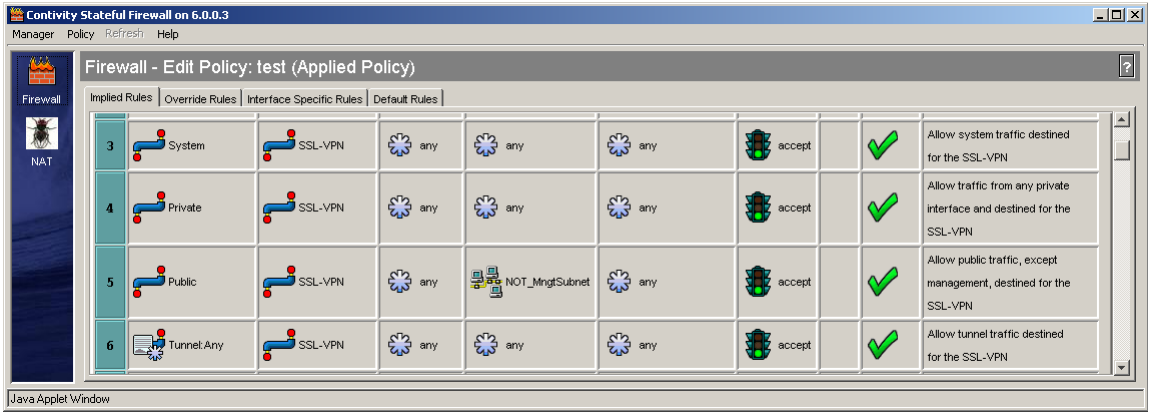
Figure 33 CSF configuration example



The difference between these settings is:

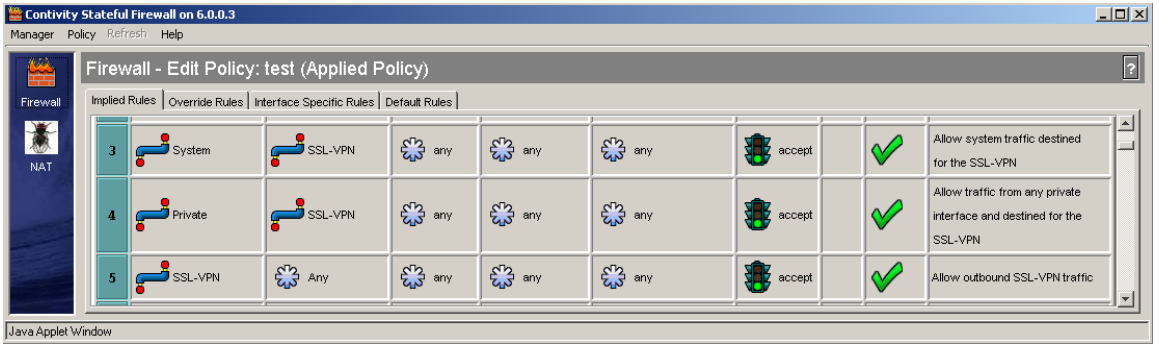
- When you check Allow SSL-VPN traffic through Stateful FW in configuration 1, it allows ALL traffic from the public side of the Contivity gateway to access the SSL device. This inserts an implied rule into the firewall.

Figure 34 Insert firewall implied rule



- If you uncheck Allow SSL-VPN traffic through Stateful FW in configuration 2, it does not insert any implied rules (except those required to manage the SSL device and for the SSL device to send to the public).

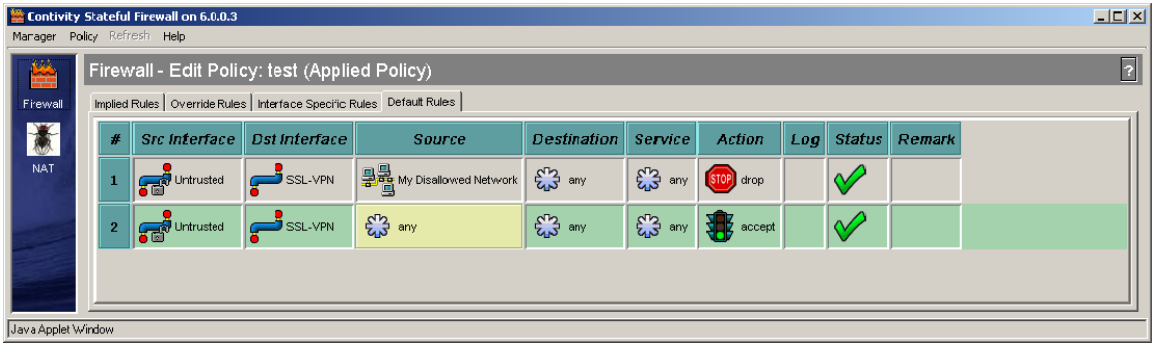
Figure 35 Do not insert firewall implied rule



The second configuration allows the administrator to control access to the SSL VPN within the firewall. For example, if you are using the system default policy (Deny All), the first configuration allows SSL through because the implied rules override all other rules.

The second configuration does not allow SSL through. To allow SSL through, you need to create a new policy with a rule that makes SSL VPN accessible.

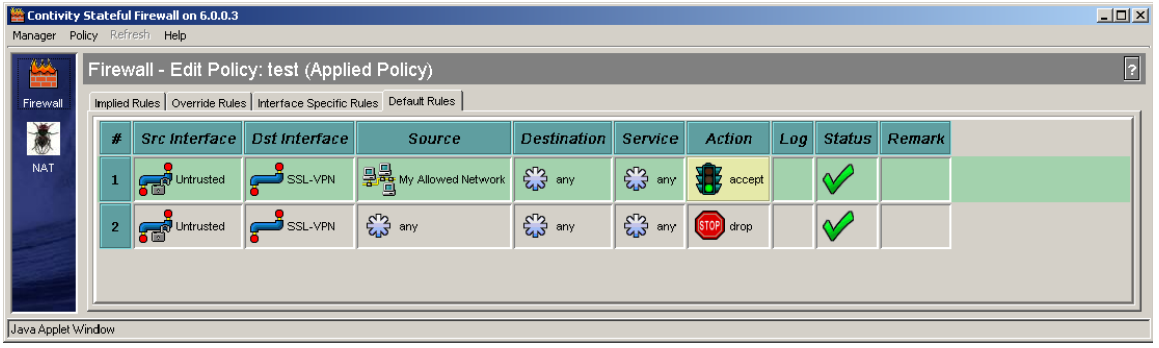
Figure 36 New firewall policy that disallows traffic



In the above case, anyone coming in on an untrusted interface (public) from "My Disallowed Network" (a created network) should be dropped. All other traffic should be allowed.

Or you could do the opposite:

Figure 37 New policy that allows traffic



Anyone coming in on an untrusted interface (public) from "My Allowed Network" (a created network) should be allowed. All other traffic should be dropped. Interface filters do not provide this functionality.

Launching SSL VPN manager

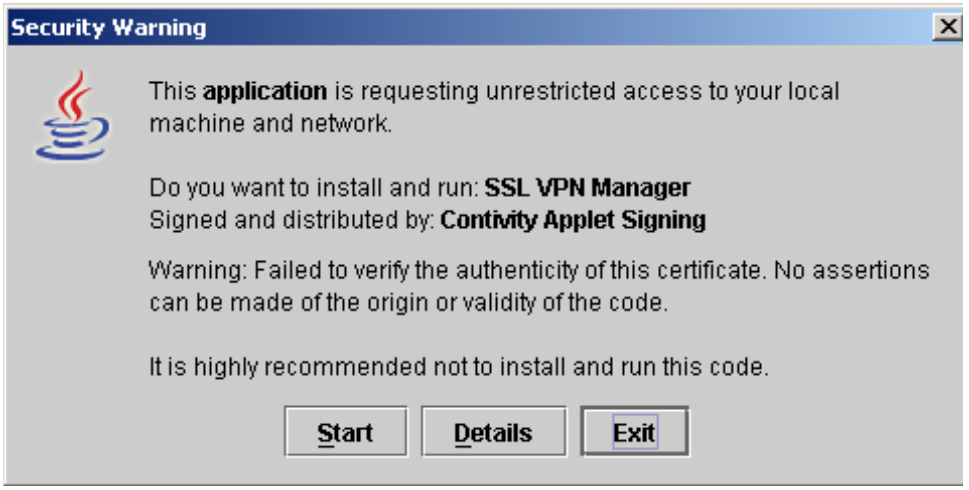
Click on the Manage SSL VPN button on the Services > SSL VPN screen to launch the SSL VPN Manager Java applet.

Installing JRE 1.4.2

You can use the Install JRE button to install the required Java Runtime Environment JRE 1.4.2 on your system.

Note: When installing and launching the SSL VPN Manager for the first time, you are prompted to accept a signed certificate for installation purposes (Figure 38). You must accept the certificate to proceed with the installation.

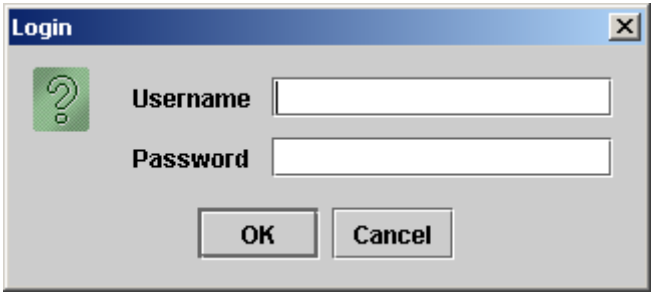
Figure 38 JRE certificate



SSL VPN manager login

The login screen (Figure 39 on page 78) appears when you launch the SSL VPN manager applet. Log in with a valid Contivity Administrator username and password. When you log in, the applet launches and discovers the SSL VPN Module 1000 device.

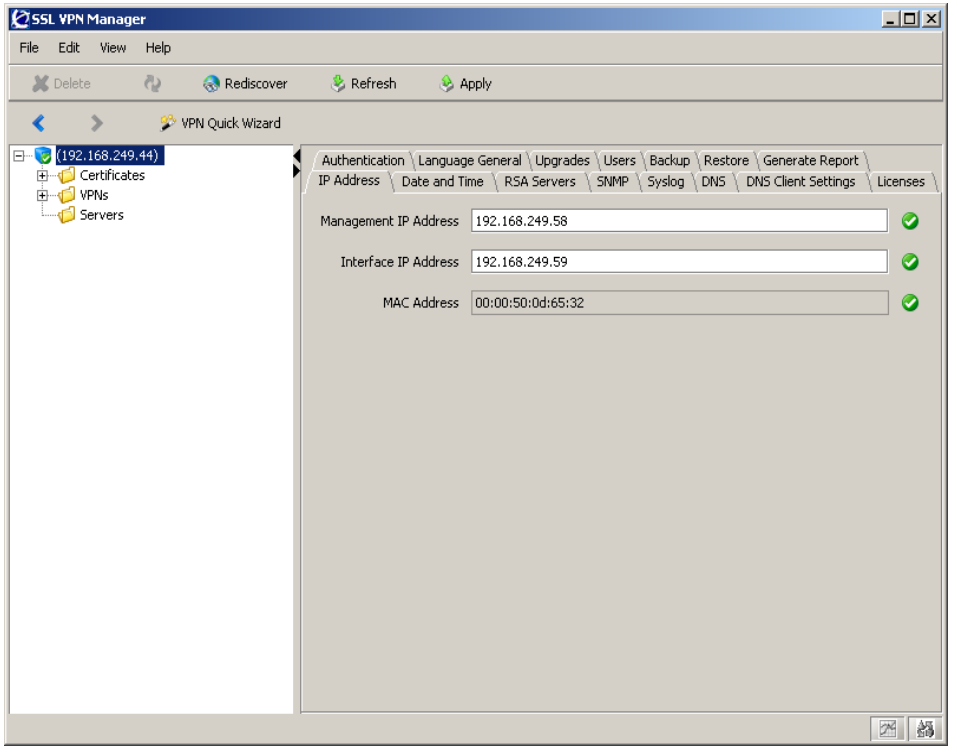
Figure 39 SSL VPN manager login



Configuring SSL VPN system settings

The SSL VPN manager screen (Figure 40) appears in a new SSL VPN installation when the SSL VPN is discovered.

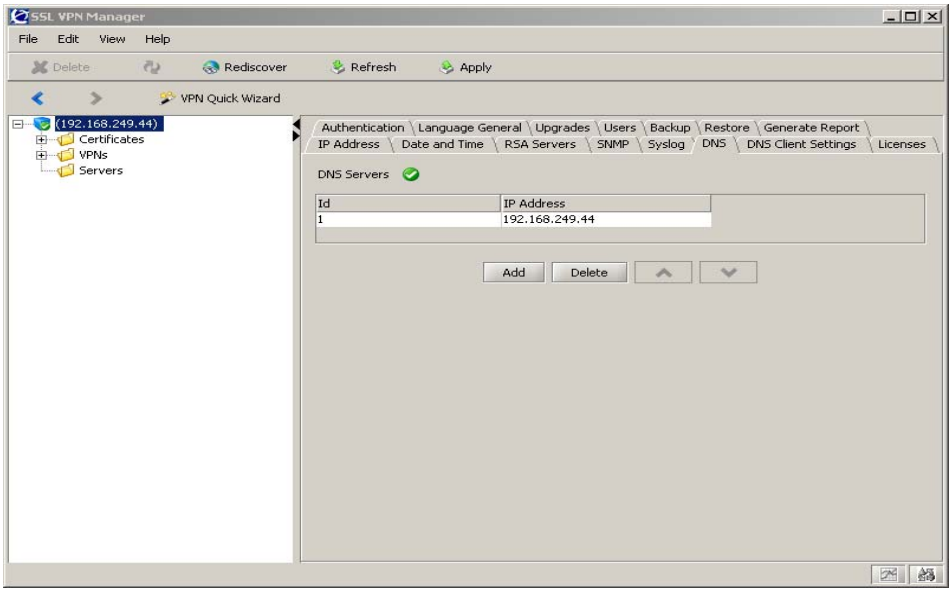
Figure 40 New SSL VPN installation screen



1 The root of the menu will show the IP address or host name of your Contivity Management IP address. Below this, there are 3 submenu items. To expand all menu items, click on the + sign.

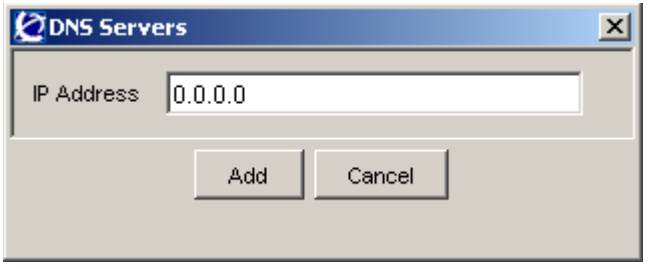
2 Ensure that the Device IPaddress/Hostname is selected at the root of the menu tree. In the right-hand pane, click on the DNS tab (Figure 41).

Figure 41 DNS tab



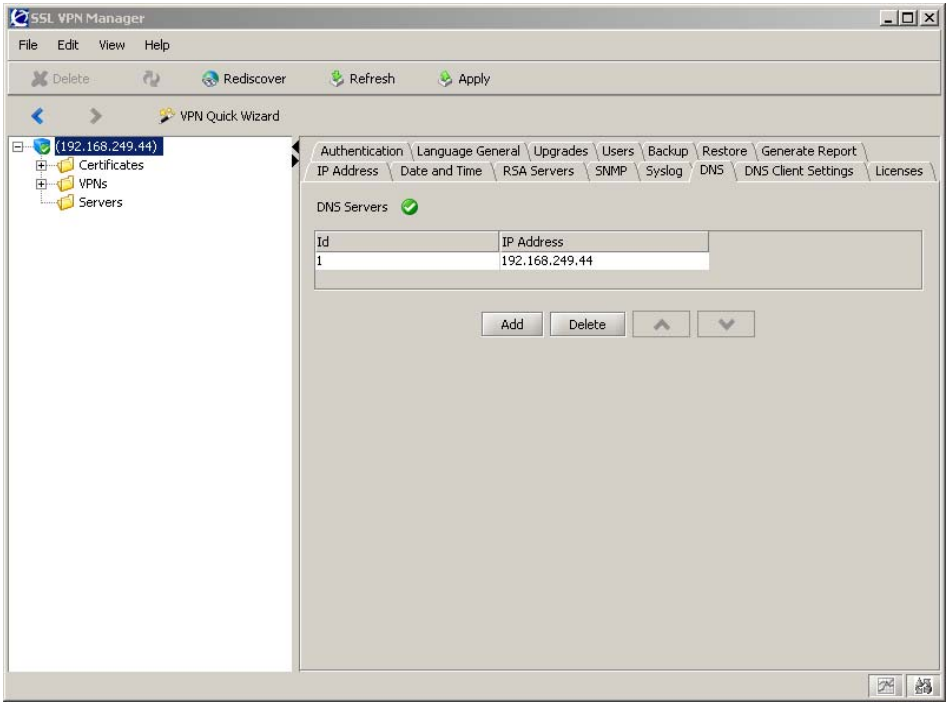
3 Click on Add. The DNS Servers IP address screen appears (Figure 42).

Figure 42 Add DNS servers



4 Enter the Contivity management IP address. This will proxy DNS requests to the Contivity gateway. The Contivity gateway must have a primary DNS server configured. Figure 43 on page 80 shows the DNS server added in the SSL VPN manager.

Figure 43 DNS server added

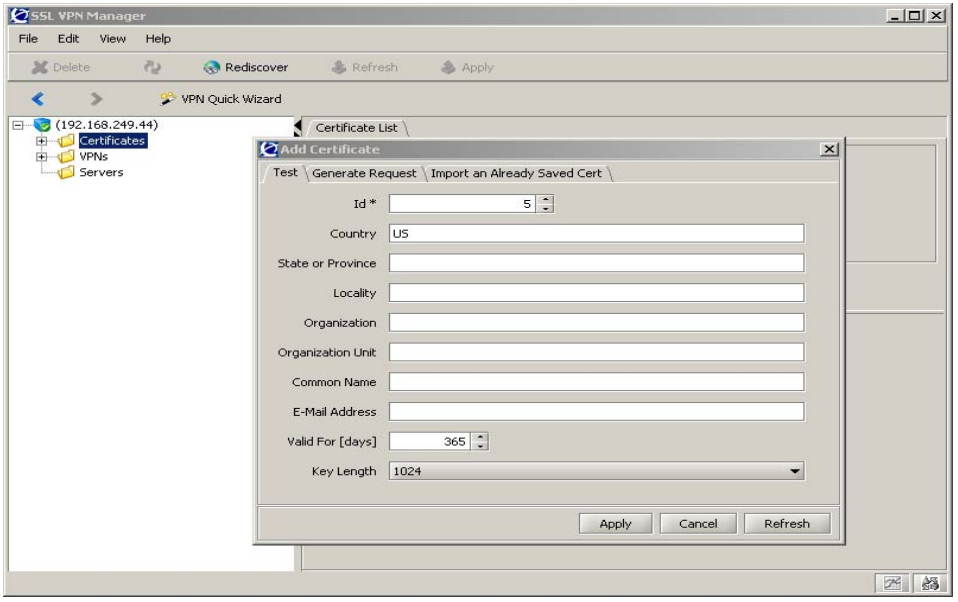


5 Use a test certificate to make the SSL VPN portal operational. Select Certificates in the menu.

6 Select the Add Certificate tab (Figure 44 on page 81). The Add Certificate screen appears displaying the Test tab.

Note: You should replace the test certificate with a valid certificate before deploying the SSL VPN.

Figure 44 Add certificate



7 Fill out the details for the certificate and use the fully qualified VPN name of the Contivity gateway for the Common Name.

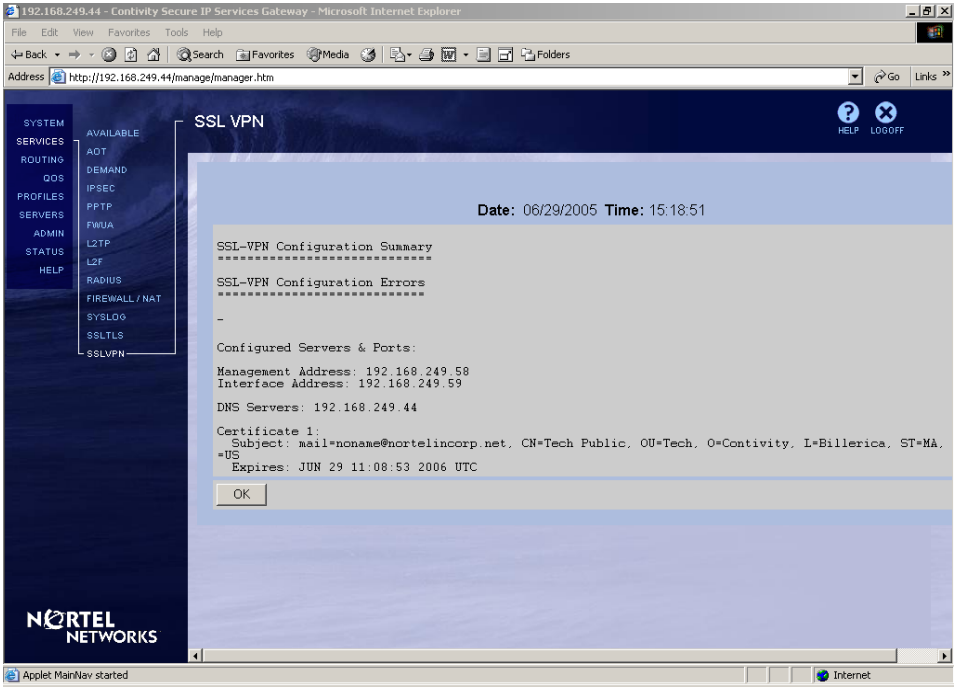
8 Click on Apply.

9 Click on the plus sign (+) to expand the Certificates folder in the menu and then select the newly created certificate, listed as Certificate 1.

10 Enter a name, such as Test Portal, in the name field and click on Apply.

11 To review your setup, select Config Summary on the Contivity gateway Services > SSL VPN screen. You can also refer to the eventlog for information about errors by selecting Admin > Event Log.

Figure 45 Review setup



Upgrading the software

The SSL VPN software image is the executable code running on the SSL VPN Module. A version of the image ships with the card. As new versions of the image are released, you can have two types of upgrades:

- Minor release upgrade

  This is typically a bug fix release. Usually this type of upgrade can be done without rebooting the SSL VPN Module 1000. Therefore, the normal operation and traffic flow is maintained and all configuration data is retained.

- Major release upgrade

  This type of release may contain bug fixes as well as feature enhancements. The SSL VPN Module 1000 may automatically reboot after a major upgrade, because the operating system may have been enhanced with new features. All configuration data is retained.

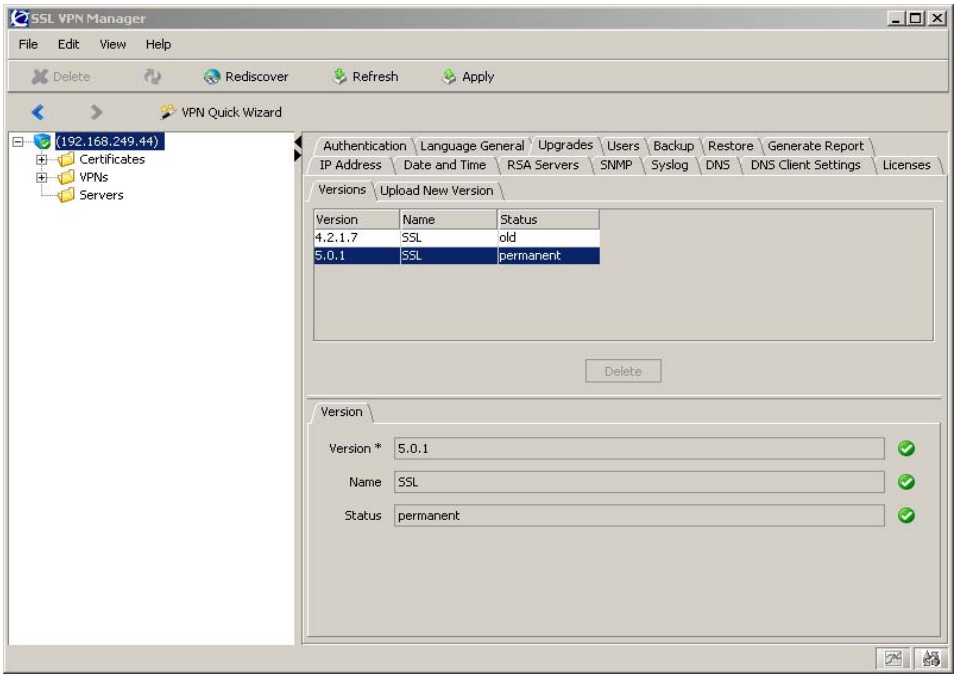
To upgrade the SSL VPN Module you will need the name of the software upgrade package (upgrade packages are identified by the .pkg file name extension). You do not have to reboot the Contivity gateway after you upgrade the SSL VPN Module.

To upgrade the Contivity gateway for either a minor or major release:

1 Select the device IP address at the top of the menu tree.

2 Select the Upgrades tab and the Versions screen appears (Figure 46).

Figure 46 Versions

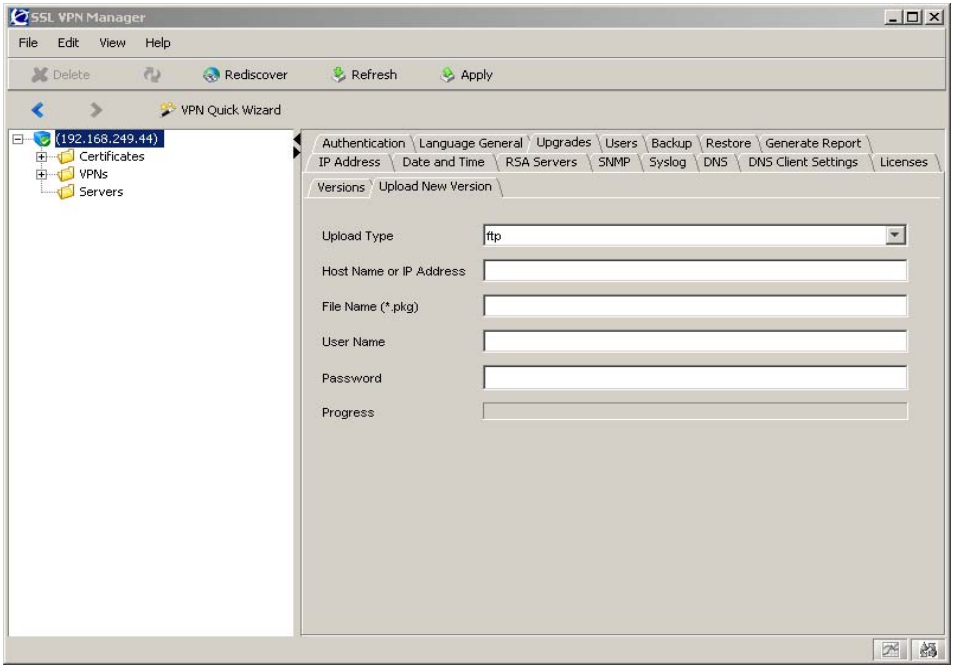


3 The Versions tab shows current versions and the following status:

- Permanent is currently operational and will survive a system reboot.
- Old is the version that preceded the current version.
- Unpacked is a downloaded version that is not yet activated.
- Current means a version marked old or unpacked has been activated.

4 Select the Upload New Version tab (Figure 47), browse to the location of the .pkg file, and click on Apply.

Figure 47 Upload version



5 Configure the parameters on the tab. See the online help for more information about specific parameters.

Activating SSL VPN upgrade packages

When a new version of the software is downloaded to the Contivity Secure IP Services Gateway, the software package is decompressed automatically and marked as *unpacked*. After you *activate* the unpacked software version (which may cause the Contivity Secure IP Services Gateway to reboot), the software version is marked as *permanent*. The software version previously marked as *permanent* will then be marked as *old*.

The downloaded software upgrade package is indicated with the status unpacked. The software versions can be marked with one of four possible status values:

- unpacked means that the software upgrade package has been downloaded and automatically decompressed.
- permanent means that the software is operational and will survive a reboot of the system.

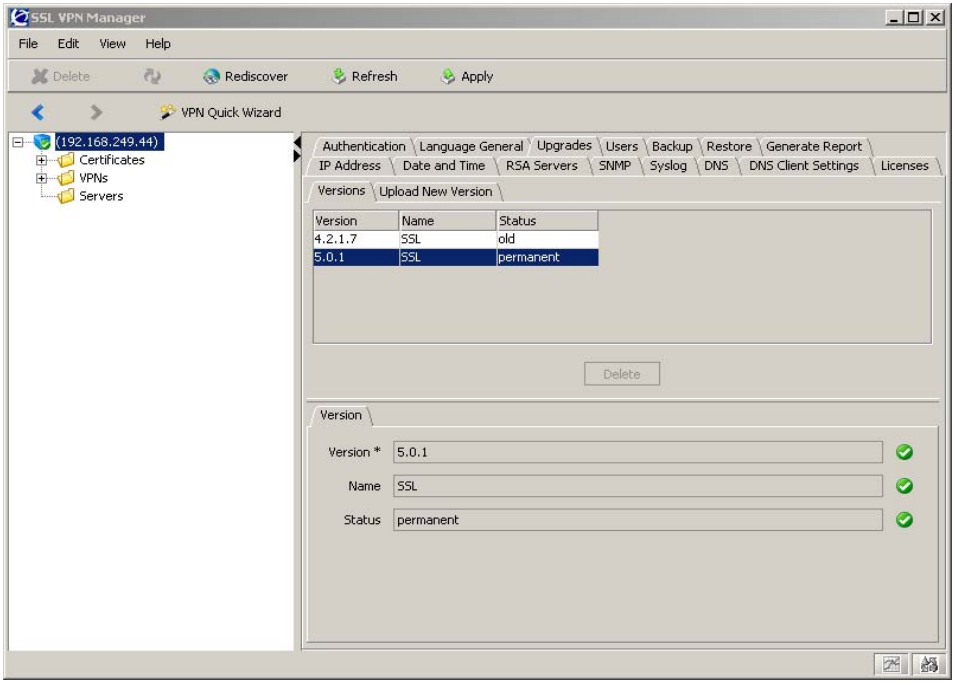
- old means the software version has been permanent but is not currently operational. If a software version marked *old* is available, it is possible to switch back to this version by *activating* it again.
- current means that a software version marked as *old* or *unpacked* has been activated. As soon as the system has performed the necessary health checks, the *current* status changes to *permanent*.

To activate the new software:

1 Select the Device IP Address at the top of the menu tree.

2 Select the Upgrades > Versions tab (Figure 48).

Figure 48 Activate software



3 Select the version you want to activate by clicking on it in the top section of the screen. The Version tab display at the bottom of the screen will show information about the selected version, including the version number, name and status.

4 Click on Activate to activate the software.

Generating certificates

The Contivity gateway supports importing certificates in the PEM, NET, DER, PKSCS7, and PKCS12 formats. The certificates must conform to the X.509 standard. You can create a new certificate or use an existing certificate. The Contivity gateway supports using up to 1500 certificates.

The basic steps to create a new certificate using the Contivity gateway are:

- Generate a Certificate Signing Request (CSR) and send it to a Certificate Authority (CA, such as Entrust or VeriSign) for certification.
- Add the signed certificate to the Contivity gateway.

Note: Even though the Contivity gateway supports keys and certificates created by using Apache-SSL, OpenSSL, or Stronghold SSL, the preferred method from a security point of view is to create keys and generate certificate signing requests from within the Contivity gateway. This way, the encrypted private key never leaves the Contivity gateway, and is invisible to the user.

Generating and submitting CSRs

To generate and submit CSRs:

1 Select the Certificates > Add Certificate > Generate Request tab in the SSL VPN Manager. Initiate requesting a certificate signing request (CSR), and provide the necessary information.

Note: When specifying a certificate number, make sure not to use a number currently used by an existing certificate. To view basic information about all configured certificates, use the Certificates menu tree and tabs. The information displayed lists all configured certificates by their main attributes, including the certificate number (this is also indicated in the expanded menu tree beneath Certificates; for example, “1:Test_Certificate”).

Explanations for the requested units of information:

- **Country Name:** The two-letter ISO code for the country where the Web server is located. For current information about ISO country codes, visit for example http://www.iana.org.
- **State or Province Name:** This is the name of the state or province where the head office of the organization is located. Enter the full name of the state or province.
- **Locality Name:** The name of the city where the head office of the organization is located.
- **Organization Name:** The registered name of the organization. This organization must own the VPN name that appears in the common name of the Web server.

  Do not abbreviate the organization name and do not use any of the following characters:

  < > ~ ! @ # $ % ^ * / \ ( ) ?
- **Organizational Unit Name:** The name of the department or group that uses the secure Web server.
- **Common Name:** The name of the Web server as it appears in the URL. This name must be the same as the VPN name of the Web server that is requesting a certificate. If the Web server name does not match the common name in the certificate, some browsers will refuse a secure connection with your site. Do not enter the protocol specifier (http://) or any port numbers or path names in the common name. Wild cards (such as * or ?) and IP address are not allowed.
- **E-mail Address:** The user's e-mail address.
- **Key size [1024]:** The key length of the generated key. The default value is 1024.

2. Click on Apply to generate the certificate request.
3. Click on Copy to copy the request to the clipboard.
4. Paste the request into a text editor and save the file.
5. When the request is submitted to the CA and you have the certificate, click on the submit button. Then click the import tab and paste the new Certificate into the window and click Apply.

6 Save the private key to a file.

Note: Provided you intend to use the same certificate number when adding the certificate returned to you (after the CSR has been processed by a certificate authority), this step is only necessary if you want to create a backup copy of the private key. When generating a CSR, the private key is created and stored (encrypted) on the Contivity gateway using the specified certificate number. When you receive the certificate (containing the corresponding public key) and add it to the Contivity gateway, make sure you specify the same certificate number that is used for storing the private key. Otherwise, the private key and the public key in the certificate will not match.

a Click on a certificate > Export tab. Enter the private key password and confirm the password.

b Click on export and the window will populate with the private key.

c Click on copy and then paste the private key into a text editor. This file should be saved in a secure location.

7 Open and copy the CSR.

In a text editor, open the **.csr** file you created in Step 5. It should appear similar to the following:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB+jCCAWMCAQAwgZQxCzAJBgNVBAYTAlNFMRIwEAYDVQQIEwlTdG9ja2hvbG0x
DjAMBgNVBAcTBUtpc3RhMREwDwYDVQQKEwhCbHVldGFpbDENMAsGA1UECxMERG9j
dTEZMBcGA1UEAxMQd3d3LmJsdWV0YWlsLmNvbTEkMCIGCSqGSIb3DQEJARYVdG9y
Ympvcm5AYmx1ZXRhaWwuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCX
2rSY81cgKJODuUreGF3ZnK7RvlRqSV/TIMS4UerqXPKpTjfMAWDjBG77hjIAOOZO
FQKFB5x/Zs9kNMBUmPBokA1/GXghomOvBhMIJBZBiUVtJNGmv2sjeqNXxsUg5XfJ
iwV2LjUvw65EzCLpq5dhq6ZPEx7tAgqB2Wgu8MolwQIDAQABoCUwIwYJKoZIhvcN
AQkHMRYTFEEgY2hhbGxlbmdlIHBhc3N3b3JkMA0GCSqGSIb3DQEBBAUAA4GBACem
SJr8Xuk9PQZPuIPV7iCDG+eWneU3HH3F3DigW3MILCLNqweljKw5pZdAr9HbDwU+
2iQGbTSH0nVeoqn4TJujq96XpIrbiAFdE1tR7Lmf6oGdrwG8ypfRpp3PmfId6lp+
HJ2fUGliPYyNtd/94AL6wW8un208+icCHq/S0yjz
-----END CERTIFICATE REQUEST-----
```

Copy the entire CSR, including the "-----BEGIN CERTIFICATE REQUEST-----" and "-----END CERTIFICATE REQUEST-----" lines.

8 Submit the CSR to Verisign, Entrust, or any other CA.

The process for submitting the CSR varies with each CA. Use your Web browser to access your CA's Web site and follow the online instructions. When prompted, paste the CSR into the space provided on the CA's online request process. If the CA requires that you specify a server software vendor whose software you used to generate the CSR, specify Apache.

The CA will return the signed certificate for installation. The certificate is then ready to be added into the Contivity gateway.

Adding certificates to the Contivity gateway

Using the encryption capabilities of the Contivity gateway requires adding a key and certificate that conforms to the X.509 standard to the Contivity gateway.

The Contivity gateway supports importing certificates and keys in these formats:

- PEM
- NET
- DER
- PKCS7 (certificate only)
- PKCS8 (keys only, used in WebLogic)
- PKCS12 (also known as PFX)

Besides these formats, keys in the proprietary format used in MS IIS 4 can be imported by the Contivity gateway, as wells as keys from Netscape Enterprise Server or iPlanet Server. Importing keys from Netscape Enterprise Server or iPlanet Server however, require that you first use a conversion tool. For more information about the conversion tool, contact Nortel Networks.

When exporting certificates and keys from the Contivity gateway, you can specify to save in the PEM, NET, DER, or PKCS12 format using the `export` command. If you choose to use the `display` command (which requires a copy-and-paste operation), you are restricted to saving certificates and keys in the PEM format only.

Note: When performing a copy-and-paste operation to add a certificate or key, you must always use the PEM format.

Copy-and-paste certificates

The following steps demonstrate how to add a certificate using the copy-and-paste method.

Note: If you connect to the Contivity gateway by using a console connection, note that HyperTerminal under Microsoft Windows may be slow to complete copy-and-paste operations. If your security policy permits enabling Telnet or SSH access to the Contivity gateway, use a Telnet or SSH client and connect to the Management IP address instead.

1. Select Certificates on the left side of the screen.
2. Select the same Certificate number that you used to create the request.
3. Click on Import Issued Cert tab.
4. Open the Certificate that you received from the CA with a text editor.
5. Copy the entire Certificate, including the BEGIN CERTIFICATE and the END CERTIFICATE lines.
6. On the SSL VPN Manager, click on Paste. The screen will be populated.
7. Click on Import.

In most cases you should specify the same certificate number as the certificate number you used when generating the CSR. By doing so, you do not have to add the private key, because this key remains connected to the certificate number that you used when you generated the CSR.

If you have obtained a certificate by other means, you must import the private keys before importing the certificate.

To Import the private key:

1. Select Certificates in the left column.
2. Select Add Certificate > Import.
3. Select an ID number that has not been used and enter a name for the certificate.
4. Enter the Private Key password.
5. Open the saved private key with a text editor.
6. Copy the entire Certificate including the "-----BEGIN RSA PRIVATE KEY-----" and "-----END RSA PRIVATE KEY-----" lines.
7. On the SSL VPN Manager, click on paste.
8. When the screen is populated with the key, click on the import box.

Updating existing certificates

Whenever you wish to substitute an existing certificate for a new certificate, you should keep the existing certificate until it is verified that the new certificate works as designed.

To create a new certificate:

1. Check the certificate numbers currently in use.

   For example, if two different certificates exist as Certificate 1 and Certificate 2, create Certificate 3 for your new certificate.

2. Add a certificate with a new certificate number.
3. Add the new certificate according to the instructions in "Adding certificates to the Contivity gateway" on page 89.
4. Apply the new certificate to the desired servers.

After you have tested that the new certificate works on your SSL servers, you can delete the old certificates.

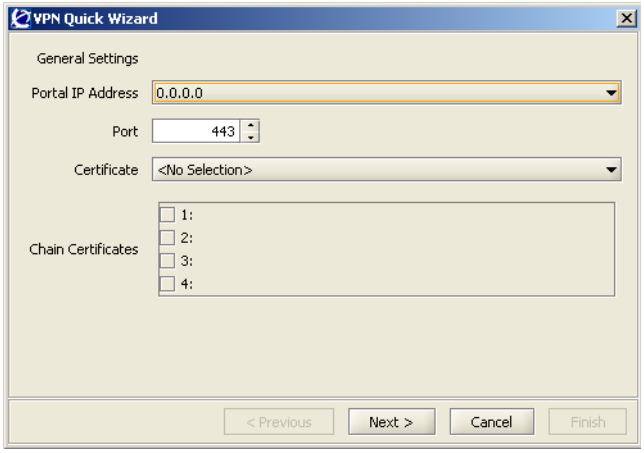
Configuring a VPN portal with VPN Quick Wizard

Running the VPN Quick Wizard during initial setup configures the SSL VPN cluster with all of the required settings for a fully functional VPN portal (clientless mode), as well as support for the SSL VPN client (transparent mode).

To configure VPN with the VPN Quick Wizard:

1 Select VPN Quick Wizard from the menu bar. The General Settings window opens (Figure 49).

Figure 49 General Settings



2 Select a portal IP address from the drop-down list. The portal IP address is used by the remote user to connect to the VPN.

If 0.0.0.0 is selected from the drop-down list, the users Full Access session is terminated on the interface that terminates their Portal session.

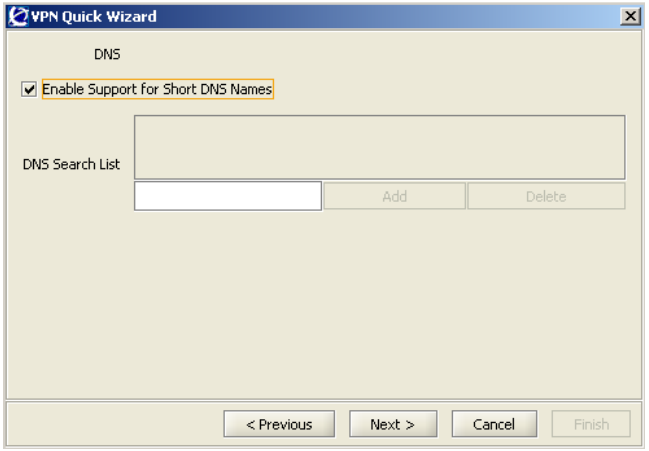
3 Select a port number from the drop-down list.

4 Select a Certificate from the drop-down list.

5 Select multiple certificates for Chain Certificate.

6 Click Next. The DNS window opens. (Figure 50 on page 93)

Figure 50 DNS



7 Click the check box to disable support for short DNS names. The default is enabled.

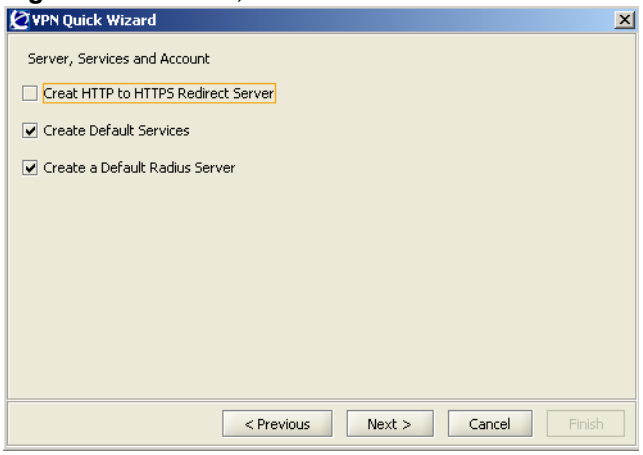
8 To add a DNS name(s) to the DNS Search List, type the name in the text box and click Add.

9 To delete a DNS name(s) from the DNS Search List, select a name and click Delete.

10 Click Next. The NetDirect window opens. Click the check box to enable support for the NetDirect client. Enter the upper and lower Ippool addresses in Pool Range.

11 Click Next. The Servers, Services and Account window opens (Figure 51 on page 94).

Figure 51 Servers, Services and Account



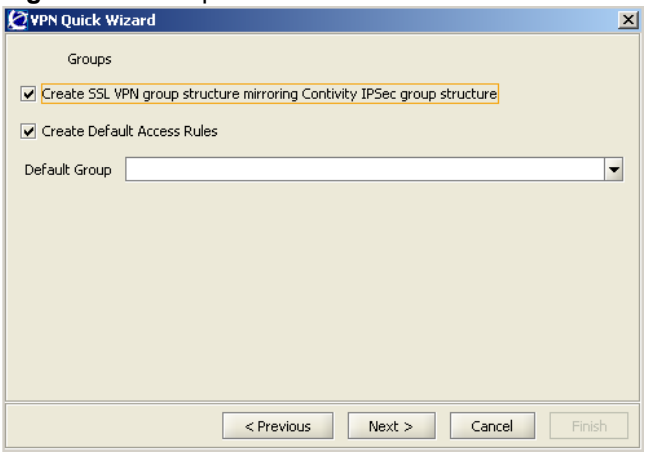
12 Click the check box to enable Create HTTP to HTTPS Redirect Server. The redirect service is configured by adding an additional server. When the virtual HTTP server on the SSL VPN device receives a request, it directs the browser to the virtual HTTPS server by sending an HTTP location header to the browser.

13 Click the check box to enable Create Default Services. Default services creates service definitions, such as port numbers or protocols, to which the user is authorized or unauthorized. When this box is enabled, default services are automatically created for the VPN.

14 Click the check box to enable Create a Default Radius Server. When this box is enabled, the default server is a Radius server.

15 Click Next. The Groups window opens (Figure 52 on page 95).

Figure 52 Groups



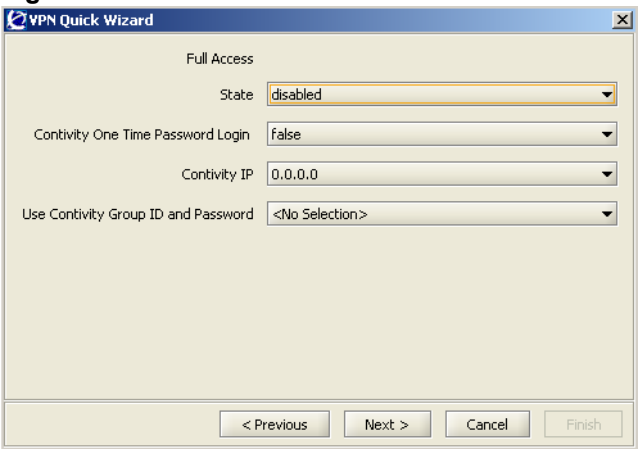
16 Click the check box to enable Create SSL VPN group structure mirroring Contivity IPsec group structure. When you enable this box, a user group structure within the SSL VPN is automatically created to mirror the group structure that is in place on the Contivity gateway.

17 Click the check box to enable Create Default Access Rules. When you enable this box, default access rules are created that define the user's access rights to resources on the corporate intranet.

18 Select a Default Group from the drop-down list, or add a group name to the text box. If a default group is selected, the user is automatically mapped to that default group.

19 Click Next. The Full Access window opens (Figure 53 on page 96).

Figure 53 Full Access



20 Select Enabled or Disabled for State.

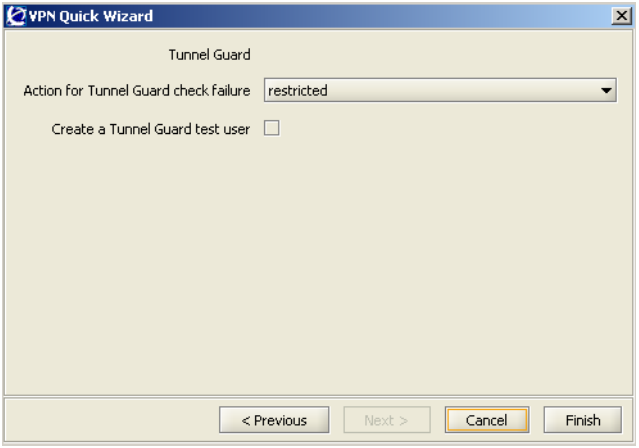
21 Select False or True for Contivity One Time Password login.

22 Select an IP from the Contivity IP drop-down list.

23 Select a group ID and password from the Use Contivity Group ID and Password drop-down list.

24 Click Next. The TunnelGuard window opens (Figure 54).

Figure 54 TunnelGuard



25 Select either restricted or teardown from the Action for TunnelGuard check failure drop-down list. By setting the action to teardown, the tunnel is torn

down if the TunnelGuard checks fail. By setting the action to restricted, the remote user can be given limited access if the TunnelGuard checks fail.

26 Click the check box to enable Create a TunnelGuard test user.

27 Click Finish.

Updating DNS servers

The local DNS server should be updated with the VPN name, and be configured to perform reverse DNS lookups.

To update a DNS server:

1 Create an VPN.

The VPN identifies your Portal. You can have several VPNs, where each VPN identifies a unique portal. Thus, you can have several different portals; for example, with different layout and links.

For each VPN, configure how the user should be authenticated, which user groups should be granted access, which access rules should apply to the different groups and which links to for each group on the portal Home tab. The portal layout can be also customized for each VPN.

2 Apply your changes.

NetDirect Agent

The NetDirect agent is an SSL VPN client that can be downloaded from the Portal for each user session. Once downloaded, the remote user can access intranet resources through native applications without the need to install VPN client software manually. When the user exits the NetDirect agent or the Portal, the agent is uninstalled.

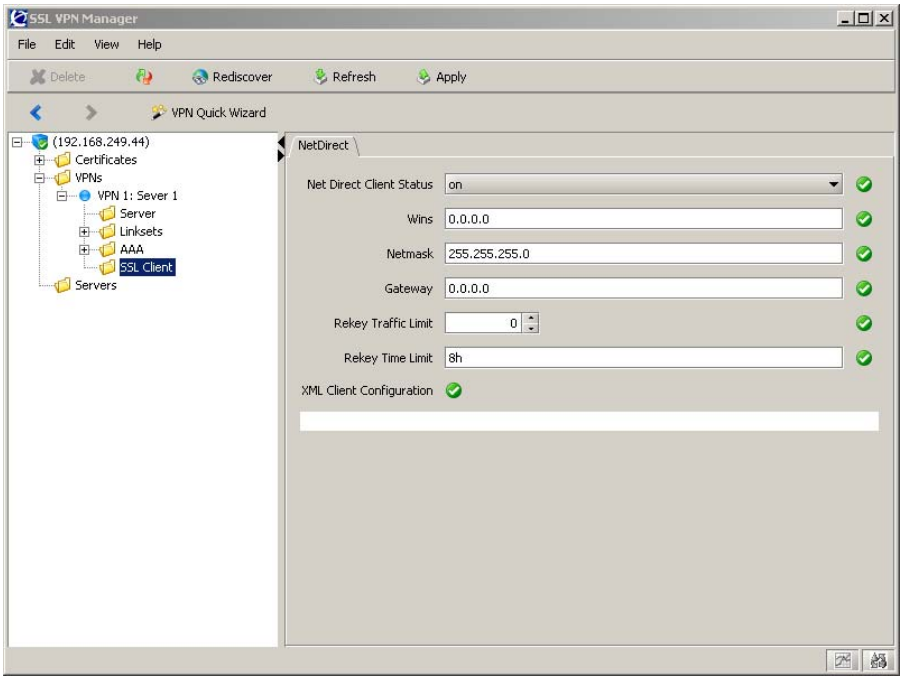
Compared to the full version of the SSL VPN client that is installed permanently on the remote user's machine, the NetDirect agent does not have a user interface. Another difference is that the NetDirect agent is packet-based, while the installed client uses system calls.

Configuring the NetDirect agent

To enable the NetDirect agent on the SSL VPN device, complete the following:

1 Select VPNs > VPN <*name*> > SSL Client. The NetDirect window appears (Figure 55).

Figure 55 NetDirect



2 In Net Direct Client Status, select on from the drop-down list.

3 Enter the following information:

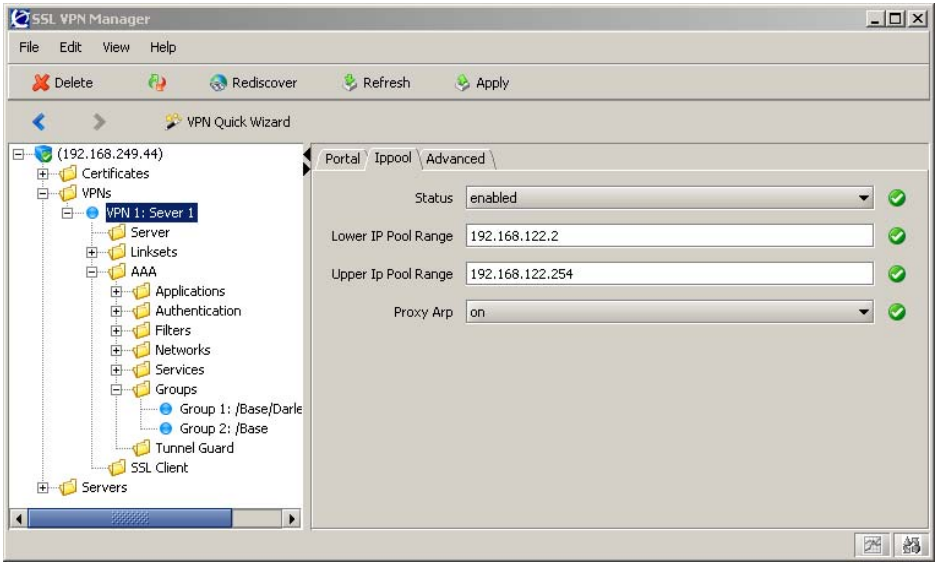
- **Wins:** If required, enter the IP address of a Windows Domain Name Server for name resolution.
- **Netmask**: Enter a netmask address NetDirect agent.
- **Gateway**: Enter a known gateway for the NetDirect agent. This entry becomes the default gateway for NetDirect. The NetDirect agent automatically sets up a temporary gateway that is not recognized as a known gateway address.

- **Rekey Traffic Limit**: Enter in, kilobytes, the maximum traffic allowed before new session keys are exchanged between the NetDirect agent and the SSL VPN device. This option can be enabled instead of the Rekey Time Limit option or both can be enabled. The default value is 0, which disables the service. This field is editable only if NetDirect clients are allowed.
- **Rekey Time Limit**: Enter, in seconds, the maximum lifetime of the single session key. The default value is 28800 seconds (or 8 hours). A setting of 0 disables the service. This field editable only if NetDirect clients are allowed.
- **xml Client Configuration:** An configuration file can be pasted into this field.

4 Click Apply.

5 Select VPNs > VPN <*name*> > Ippool tab. The Ippool window appears as in Figure 56.

Figure 56 Ippool



6 Select enable from the Status drop-down list.

7 Enter the lower and upper IP address ranges.

8 Select Proxy Arp to on from the drop-down list.

9 Click Apply.

Chapter 4
Configuring VPNs

This chapter describes the various aspects of configuring SSL VPNs. Every virtual server configured as type HTTP or SOCKS needs a VPN associated with it. VPNs provide the authorization, authentication, and accounting infrastructure that is used to determine whether users are valid, what they are allowed to access, and to track their activities.

To configure a VPN, complete the following steps:

a If required, enable Full Access.

b If not already configured, configure the VPN's AAA settings with the AAA Quick Wizard.

c Configure Authorization.

The SSL VPN has extensive authorization control mechanisms, which can be divided into two general categories:

Back end resource access control. Based on the group that the user was assigned to when logging in, a User Type is established, Access Rules are applied, Full Access to the network may be granted, Portal Links are presented, and Extended Profiles are consulted.

- Access rules allow configuration of which back end (private side or server) networks, services and applications can be accessed through the SSL-VPN that is using this particular VPN for authentication.
- The User Type is one of <Advanced, Medium, Novice> and determines what tabs are displayed for VPN servers.
- Full Access, if enabled for that particular VPN, gives the user the ability to start a transport-layer VPN (either IPsec or SSL), which will give the user complete access to all private-side resources.
- Portal Links are a set of various types of links that are displayed in the portal for all users authenticating to that VPN.

Front end requirements: Every VPN has associated with it certain requirements (filters) that can be established for SSL VPN users logging in from a particular network. Filter configuration elements include the requirement to have a client certificate and/or IE Cache Wiper present and what authentication type was used when logging in.

d Configure Authentication.

Every VPN will have an associated, ordered list of one or more authentication servers. A rich configuration capability of RADIUS, NTLM, SiteMinder, LDAP and Certificates is available. Multiple authentication servers can be configured for each VPN, and an authentication order established. Single Sign On (SSO) VPNs can be established such that back end server authentication requests are automatically handled without credential input from the user.

e Configure Accounting.

RADIUS accounting is available.

f Configure TunnelGuard.

TunnelGuard ensures that the required components (executables, DLLs, configuration files) are installed and active on the remote user's machine.

Configuring Full Access

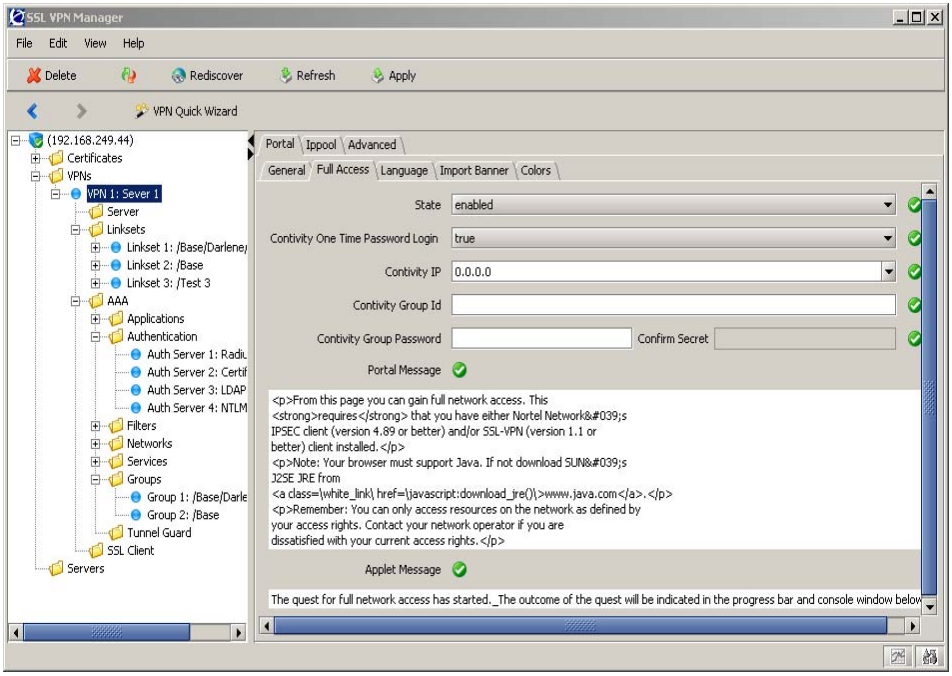
The Full Access tab controls how the Contivity VPN Client is launched when you request full access from the portal screen. By default, full access is disabled and the Full Access tab is not be displayed on the portal.

To enable full access:

1 Select the VPNs > VPN <*name* > > Full Access tab.

2 Set the state to enabled. Full Access is only available to advanced portal users.

Figure 57 Full Access tab



3 Configure the Contivity One Time Password

The Contivity gateway one-time password is an authentication method that uses a temporary user ID to launch the Contivity VPN Client. It is used primarily when certificate or SecurID tokens are used to log in to the SSL Portal. One-time password launches the Contivity VPN Client without requiring additional credentials from you.

When one-time password is enabled, the Contivity gateway creates a temporary username and password, which is then used by the Contivity VPN Client to start the IPsec tunnel. To enhance the security of the one time password, it has the following restrictions:

- Password is good only for a single Contivity VPN Client login
- Password automatically expires after 2 minutes
- Contivity VPN Client must connect from the same IP address used to log into the SSL portal

One time-password logins must be enabled on the Contivity server under the Services > SSLVPN screen. If the One Time Password option is disabled, the Contivity VPN Client uses the same user name and password as the one used to log in to the SSL portal.

The restrictions on the one-time password also mean that the failover and load balancing features of the Contivity VPN Client do not work when the one-time password option is enabled. Because of these limitations, Nortel recommends that you use one-time password only when using certificates or SecurID tokens for the SSL portal login.

4 Set the Contivity gateway IP address.

The Contivity gateway IP address determines what address the Contivity VPN Client connects to when starting. Typically, the default of 0.0.0.0 is appropriate. When the Contivity gateway IP address is 0.0.0.0, the Contivity VPN Client connects to the same address as the one used for the portal.

Setting the Contivity gateway IP address to a specific address connects the Contivity VPN Client to that address only, regardless of the address used for the VPN portal.

5 Set the group ID and password.

Set the group ID and password only if the Contivity VPN Client needs to perform a Radius Group authentication before logging in with your name and password. If the Contivity VPN Client performs a straight username/password login, leave these blank. If the One Time Password option is enabled, the group ID and password are not used.

6 Customize the full access text.

The portal message box contains the text that is displayed under the portal Full Access tab. The Applet Message box contains the text that the applet initially displays as it starts the Contivity VPN Client.

Configuring the VPN AAA with the AAA Quick Wizard

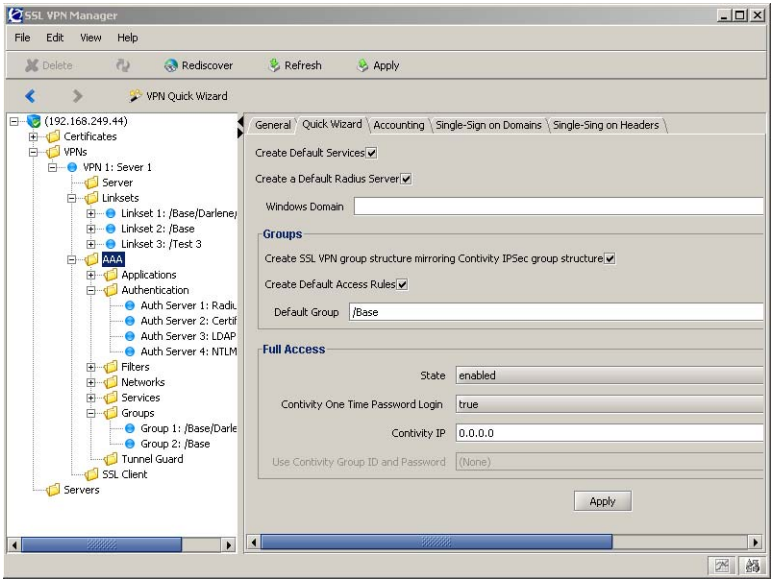
The AAA Quick Wizard is used to quickly configure all of the aspects of a VPN that are relevant to most SSL VPN administrators. The advantages of using the AAA Quick Wizard rather than manually configuring a VPN are:

- Automated configuration of the SSL VPN RADIUS client aimed at the Contivity RADIUS service
- Automatic creation of a user group structure within the SSL VPN that mirrors the group structure that is in place on the Contivity gateway
- Guided configuration for all full access parameters, and the default login group

To configure an SSL environment:

1 Select VPNs > VPN <*name*> > AAA > Quick Wizard tab (Figure 58).

Figure 58 AAA Quick Wizard



2 Set the Wizard tab fields and settings as follows:

- Create Default Services

This option automatically creates the following service definitions, which are used to create SSL VPN access rules.

- HTTP uses TCP port 80
- HTTPS uses TCP port 443
- Web uses TCP ports 20, 21, 80 and 443
- SMTP uses TCP port 25
- POP3 uses TCP port 110
- IMAP uses TCP port 143
- Email uses TCP ports 25, 110 and 443
- Telnet uses TCP port 23
- SSH uses TCP port 22
- FTP uses TCP ports 20 and 21

- Create Default RADIUS Server

  This option creates a default RADIUS server for authentication. It automatically configures a RADIUS authentication server pointing to the Contivity gateway as a client - the password is automatically retrieved from the Contivity default client or (if a default client is not configured) from the client with the IP address of the SSL VPN Module 1000.

- Windows Domain

  This optional field sets the Windows domain.

- Create SSL groups mirrored from existing Contivity IPsec groups

  When checked, this option creates a complete mirror image of the groups already configured on the Contivity gateway for IPsec access. This automatically gives these IPsec users SSL VPN access.

- Create Default Access Rule

  This option, available when the above option is enabled, creates a default access rule with ID 1 that accepts access to all networks, services and applications.

- Default Group

  Use this field to select a default group. It is automatically mapped to */Base* group as the default when you enable the Create SSL groups mirrored from Existing Contivity IPsec Groups option.

- Full Access

The parameters in this section of the wizard tab apply to the Full Access Tab on the Unified Access Portal.

— Contivity One Time Password

When Client Certificate Authentication, Siteminder, SecurID, or NTLM is used for the SSL authentication mechanism, the Contivity One Time Password must be enabled if you require silent Single Signon for IPsec Full Access. If this feature is not enabled, you are prompted for your log on credentials when Full Access is requested. It is not necessary then to configure Contivity groupID/password when using Contivity One Time Password. When users are stored in external RADIUS or LDAP proxy, one-time password does not need to be enabled. In this case the Contivity GroupID/password must be configured.

— State

Enables/disables the Full Access tab.

— Contivity IP

The IP address of the interface that will be used to establish IPsec connectivity. When 0.0.0.0 is used as the Contivity IP address value instead of the pre-configuration of the Contivity IP address, the address is determined dynamically at run time. The SSL VPN Module uses the Virtual Server IP Address for the end point of the IPsec user tunnel.

— Use Contivity Group ID and Password

Select an existing Contivity Group to use the Group ID and Password already used by the group for RADIUS and LDAP Authentication. This defaults to */Base*.

3 Click on Add to run the wizard. The wizard runs and sets up the initial configuration according to the parameter settings. It can take a minute or more for the wizard to complete the configuration.

Configuring authorization

Authorization control mechanisms are generally divided into back end resource, access control, and front end requirements.

Back end resource access control - configuring group settings

Back end resource access control is a combination of group attributes that determines what the private side users in each group are able to access. You configure the specific data for each user group to determine the tabs and hypertext links to display on the portal for a logged-in group member, as well as the intranet hosts and subnets the group member should be authorized to access.

Note: The SSL VPN has its own database and group structure (independent of the groups that are created on the Contivity gateway). Although it is not required, administration is easier if the SSL VPN Module (using LC) group structure mirrors the group structure of the Contivity gateway. If you used the AAA Quick Wizard, this is automatically done for you.

The following parameters can be configured for a group:

- Access rules
- User type
- Default group
- Extended profiles
- Portal Links

Groups are created within a VPN using the VPNs > VPN <*name*> > AAA > Add. Every VPN has a default group associated with it. If no access group is defined for a certain user, a configurable default access group can be used.

Access rules

Each user is mapped to one or more groups stored in the Contivity gateway. The access rules associated with the group define the user's access rights to resources on the corporate intranet. The access rules permit or deny access to servers based on a combination of criteria:

- Destination host or network
- Ports or protocol

- Path (for HTTP, SMB and FTP file browsing)
- Source IP address (if extended profiles are used)
- Authentication method (if extended profiles are used)

The extended profile determines the access rules that apply during the currently logged-in group member's session. For example, the access rules defined for an extended profile that references a secure authentication method could be more generous. As with links, the base profile's access rules are appended to those of the extended profile.

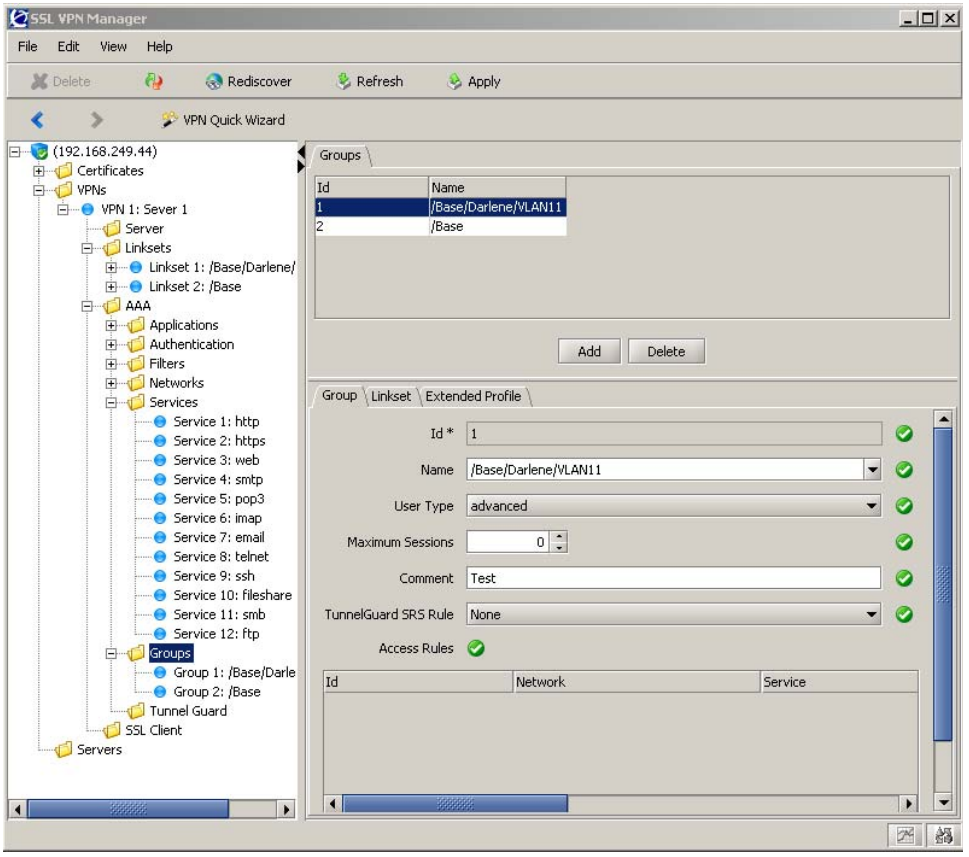
The extended profile's access rules are executed prior to those of the base profile. This means that if a matching extended profile is found (for example, the profile's client filter matches the user's source network), and a match is found in any of the profile's access rules (the access rule's network definition matches the user's requested network), the action specified for the access rule (such as accept) will be performed. The base profile may contain an access rule with the same network definition, but this access rule is ignored.

Access rules are defined on a group basis. They include references to networks, services, applications, and an accept or reject action. To be able to configure an access rule, you first create the network, service, and application-specific definitions.

- A network definition identifies hosts or subnets to which the user should be authorized (or not authorized).
- A service definition identifies ports or protocols to which the user should be authorized (or not authorized).
- An application-specific definition identifies a path to a subfolder or file to which the user should be authorized (or not authorized). The access rule is configured by referencing the desired network, service, and application-specific definitions in the access rule.

When the user requests a resource (such as an intranet Web server), the access rules associated with the user's group are applied in order until a match is found. The system first checks Access rule 1, then Access rule 2, and so on. Figure 59 on page 110 shows an access rule defined for a group.

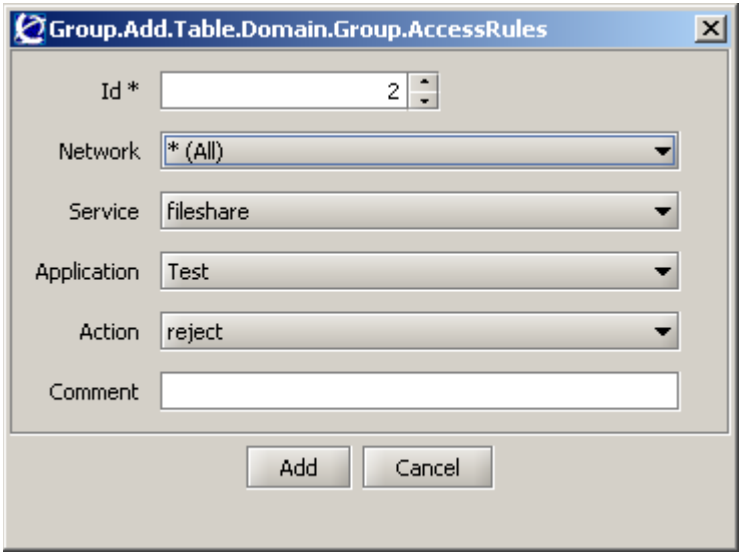
Figure 59 Group access rules



Access rules configuration

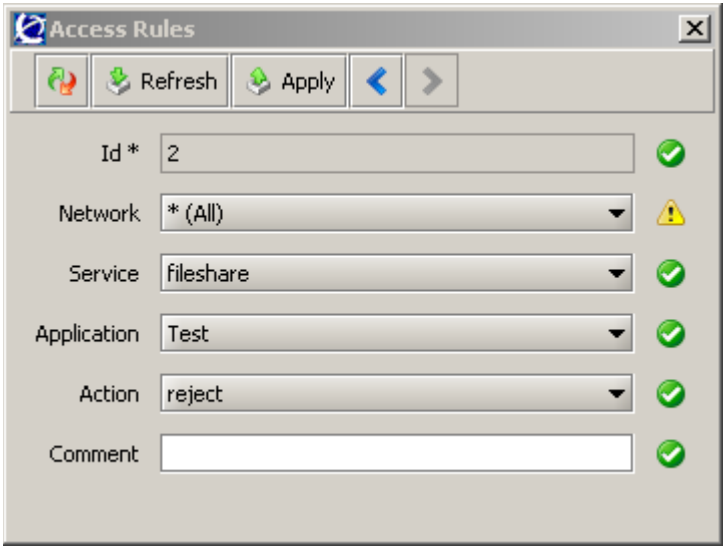
To add access rules, click on the Group tab and then click Add. The Add Access Rules window is shown in Figure 60 on page 111.

Figure 60 Access Add rules



You can edit access rules from the Groups tab using Access Rules. From the Groups window, highlight an existing rule, click Edit, and the Access Rules window appears as shown in Figure 61.

Figure 61 Access Rules



Each access rule defines:

- Access rule ID
- Network
- Application
- Service
- Action - Accept or Reject

Access rule ordering

If a match is found between the requested resource and the network, service, and path referenced in the access rule, the action (accept or reject) specified for the access rule is performed. The remaining access rules (with higher numbers) are ignored. This means that the order in which the access rules are defined could be important. If no match is found in any access rule, the request is rejected.

Creating service definitions

This example describes how to create a service definition allowing access to the FTP and SMB application protocols.

1. Select the VPN to which you want to add the service definition by selecting VPNs > VPN <*name*>> AAA > Services. Click Add to add the service.
2. Specify a service name and allowed port numbers.
3. Apply the changes.

Note: If you ran the VPNs >VPN <*name* > AAA > Quick Wizard with the option Create Default Services, then 10 services are already defined within the VPN and are listed individually in the Services list in the Access Rules dialog.

Creating path (Appspec) definition

This example describes how to create an application definition identifying a path to a subfolder.

The path to define in this example is /public. When the remote user tries to access the Web server identified in the web server network definition, the following URL will create a match: `192.168.201.10/public`.

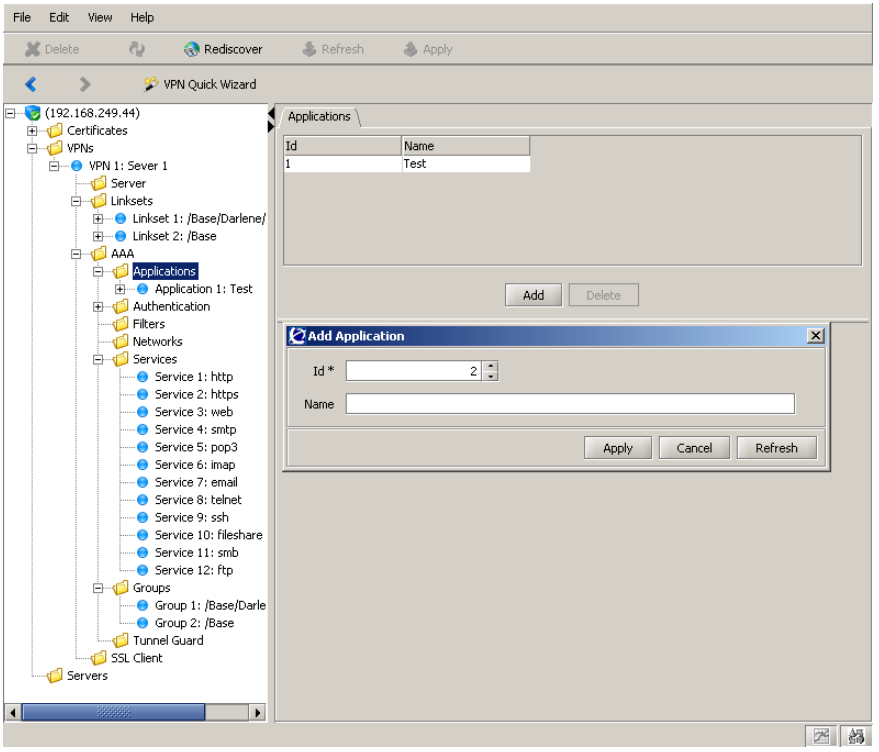
The path setting is checked for the following protocols: HTTP, HTTPS, FTP and SMB (Windows file share). The syntax for entering the path is shown below:

- For SMB, write the path as /WORKGROUP/FILESHARE/FILE PATH, for example, /NORTEL/homes/public. This will give access to the public directory in the homes share in the NORTEL workgroup/VPN.
- For FTP, write the path as ABSOLUTE FILE PATH; for example, /home/share/public/. This will give access to the /home/share/public directory. Note that all paths are absolute from the root.
- For Web servers (HTTP or HTTPS), write the path as SERVER PATH; for example, /intranet. This will give access to the /intranet path on the Web server.

To create an application definition:

1 Select the VPNs > VPN <*name*> > AAA > Applications > Add (Figure 62 on page 114).

Figure 62 Add application



2 Specify a name for the application definition and enter the desired path.

3 Apply the changes.

4 This application is now listed in the Access Rules dialog box in the Application list.

User type

The user type determines the portal tabs that are displayed for the user. The user type distinction has no effect on access rules and vice versa.

The following user types are available:

- Novice displays the Home and Logout tabs.
- Medium displays the Browse Intranet, Files and Full Access tabs (if enabled).
- Advanced displays all tabs, including the Advanced tab.

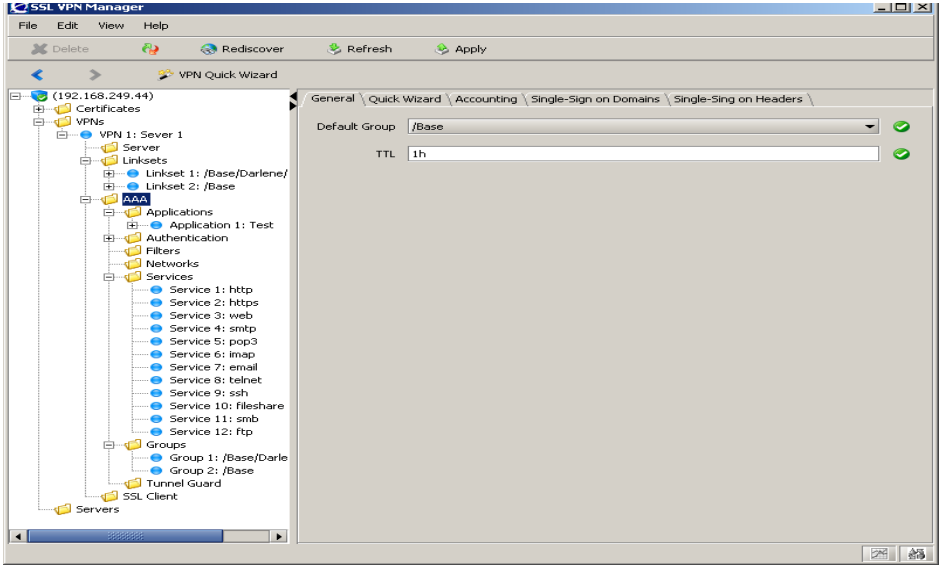
The highest user type assigned to the user group's extended profile and base profile is applied. This means that if the extended profile has the *novice* user type assigned to it and the base profile uses the *advanced* user type, the *advanced* user type is applied; for example, all of the portal's tabs are displayed for the logged-in user.

Default groups

If a user group that is returned from the authentication database does not match any group configured on the Contivity gateway, the user is automatically mapped to the default group (if configured) for the VPN.

To configure default groups for each VPN, use the VPNs > VPN <*name*> > AAA > General tab (Figure 63).

Figure 63 Default groups



Multiple groups

If a user belongs to several groups, the system starts by checking Group 1 (as defined on the Contivity gateway) to see if that group name matches any of the group names returned from the authentication database. It then continues with Group 2 and so on until all matches are found. A list of matching groups is then maintained by the system during the user's login session.

When the user requests a resource, the access rules associated with Group 1 in this session-based list are checked in sequential order until a match is found. If a match is found, the remaining groups are ignored. If no match is found, the access rules associated with Group 2 are checked, and so on.

All the links configured for the user's different groups are displayed on the portal's Home tab.

The highest user type assigned to the user's different groups are applied. This means that if the user belongs to one group configured with the *novice* user type and another with the *advanced* user type, all of the portal's tabs are displayed.

Table 2 Valid access rules users belonging to multiple groups

Group 1	Group 2	Group 3
Extended profile 1 (no match)	Extended profile 1 (no match)	Extended profile 1 (match)
Extended profile 2 (match)	Extended profile 2 (no match)	
Base profile	Base profile	Base profile
Result: The access rules of Extended profile 2 and the base profile will be valid for the user's current session.	Result: Only the base profile's access rules will be valid for the user's current session.	Result: The access rules of Extended profile 1 and the base profile will be valid for the user's current session.

When the user requests a resource, for example, an intranet host, the system first checks the access rules that are valid for Group 1. The extended profile's access rules are checked prior to the base profile's access rules.

If no match is found between the user's request and the network, such as services specified in Group 1's access rules, the system goes on to check Group 2; only the base profile's access rules in this example. If a match is found in any of Group 2's access rules, the access rules pertaining to Group 3 are ignored. If no match is found in Group 2, the system goes on to check the access rules valid for Group 3.

To avoid the complexity of overlapping access rules when multiple access groups are configured, we recommend that each individual group's access rules cover separate areas.

Extended profiles

All the data that can be defined for a group on Group level (access rules, links, and user type) can also be defined for an extended profile. For example, data defined on Group level directly under the Group menu adhere to the group's *base profile*. Data defined on the Extended profile tab adhere to the group's *extended profile*.

The *client filter* referenced in the extended profile determines when the extended profile's access rules are applied.

The client filter identifies:

- Source network (such as a branch office)
- Authentication method (such as RADIUS)
- Whether a client certificate is installed on the remote user's machine
- Whether the IE cache wiper is installed on the remote user's machine
- User type

When the user is authenticated, the system starts by checking Extended profile 1 to see if a match can be found between the client filter's condition and the security status of the user.

If no match is found in Extended profile 1, the system goes on to check Extended profile 2 for a matching client filter and so on. When a match is found, that particular extended profile's data (for example, access rules or links) is applied. Data defined for the base profile is appended to the extended profile's data. If no match can be found in any of the extended profiles, only the base profile's data is applied.

Defining Portal Linksets

You can define linksets to which any remote group can be granted access (by group ID) to the links contained in that set.

Links are automatically associated with the selected group (and VPN). Only users who are members of the selected group (identified by the group ID) have access to the links within the group. Also, ensure that access to the resource provided through the link is not contradicted by any access rules that apply to the group(s) of which the SSL VPN user is a member. Each link you define corresponds to a specific link number.

Hypertext links to intranet and Internet Web pages and server applications can easily be configured. Links appear on the portal's Home tab. The links that are displayed for the logged-on user depends on the user's group membership.

Any hypertext links configured for the group appear on the portal's Home tab when a group member is logged in. Examples are links to intranet Web or mail servers.

Adding a group linkset

To add a linkset of a specific type to a specific group:

1. Select VPNs > VPN <*name*> > Linksets > Add.
2. Select the key for the linkset.
3. Fill in the name of the group.
4. Fill in the text that is to be displayed.
5. Click Apply. The linkset is added to the Linkset tree.

Configuring specific portal linksets

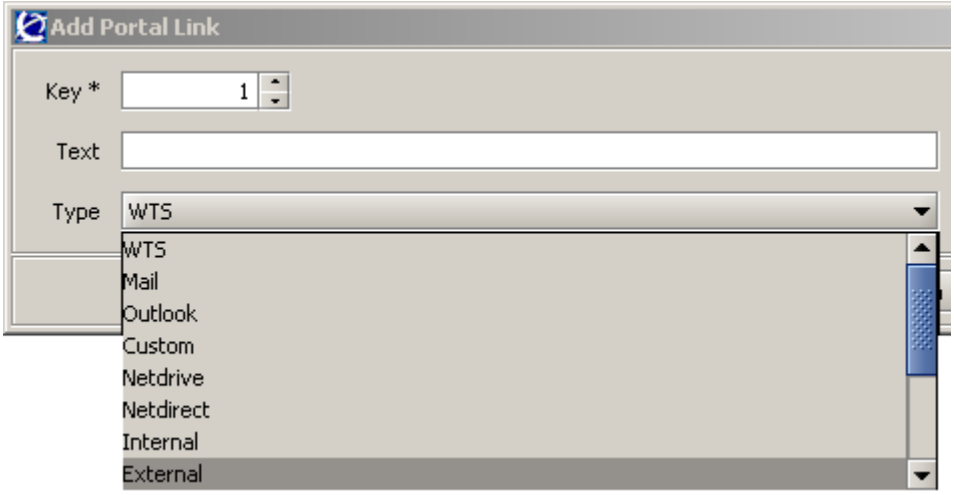
To configure a linkset of a specific type to a specific group:

1. Select VPNs > VPN <*name*> > Linksets. Click on the plus sign (+) to expand the Linkset tree.
2. Select a group name.

3 Select the Portal Link tab.

4 Click Add. The Add Portal Link window appears (Figure 64).

Figure 64 Add Portal Link



5 Select a key number.

6 Add the text that is to be displayed.

7 Select one of the following available link types from the drop-down list:

- SMB — gives the user access to folders on a Samba (SMB) file server (Windows file share).
- FTP — gives the user access to folders on an FTP file server.
- External — link (direct) to Web page. Suitable for external Web sites.
- Internal — link (secured through the Contivity gateway) to Web page. Suitable for internal Web pages.
- Iauto — automatic login link (secured through the Contivity gateway) to password-protected Web page.
- Terminal — link to terminal server through Java applet for Telnet or SSH connections.
- Proxy — link for accessing Web pages through the Contivity gateway's HTTP Proxy server (required for complex Web pages).
- Custom — custom port forwarder link to the specified application server.
- Telnet — port forwarder link to terminal server for Telnet connections.

- Mail — port forwarder link to mail server (for example, Outlook Express).
- Netdrive — port forwarder link for mapping a network drive to an SMB (Windows file share) file server.
- Wts — port forwarder link to Windows Terminal Server.
- Outlook — port forwarder link to Microsoft Exchange server.

You can find example link configurations in Appendix A, "Configuration examples" on page 169.

Full Access

The Full Access tab provides a way for the remote user to launch the Contivity VPN client from within the portal. In a manner similar to when the user starts a VPN client manually, transparent access to the intranet is enabled and no further login to the VPN is required.

Transparent access implies that the user can request resources as if working from within the intranet with no further portal interaction required. Supported VPN clients are Nortel Networks Contivity VPN client and Nortel Networks SSL VPN client.

See Chapter 2, "Using the SSL VPN portal" on page 56 for further information on configuring full access.

Front End Authorization requirements - Filters

Filters allow the SSL VPN administrator to require a certain configuration of public or client-side authentications to virtual servers using this particular VPN. Filters are defined (created) under VPNs > Filters, and require the definition of a network from which the SSL VPN user originated from. Multiple filters can be created for a VPN; all matching filters are applied to incoming SSL VPN user traffic.

Filters identify the following:

- Source network (such as a branch office)
- Authentication method (such as RADIUS)
- If a client certificate is installed on the remote user's machine

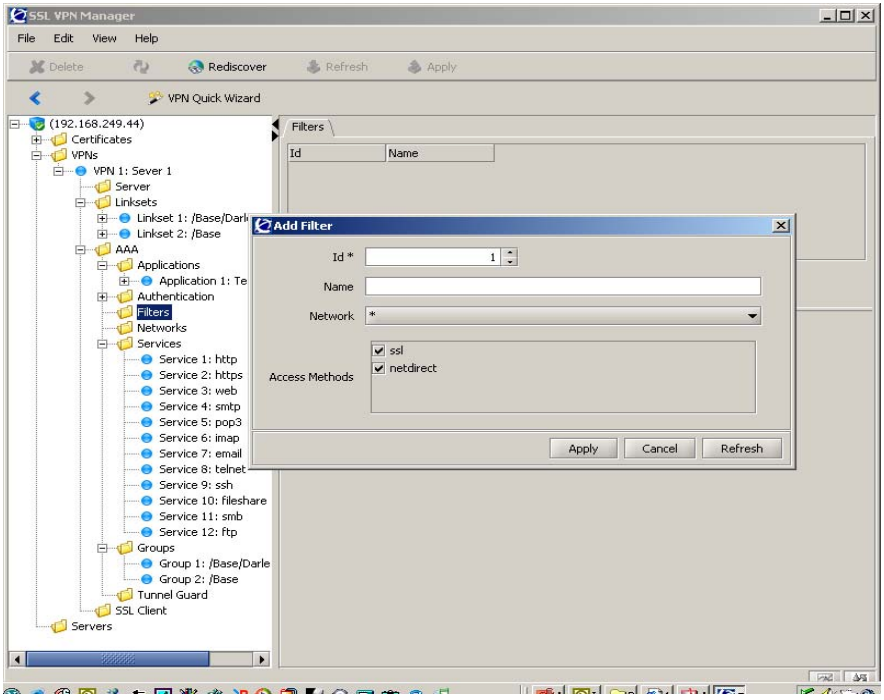
- If the IE cache wiper is installed on the remote user's machine
- User type

Defining client filters

To define client filters:

1 Select VPNs > VPN <*name*> > AAA > Filters > Add. The Add Filters window displays (Figure 65).

Figure 65 Add filters



2 Specify the client filter's name.

3 Reference the previously created network.

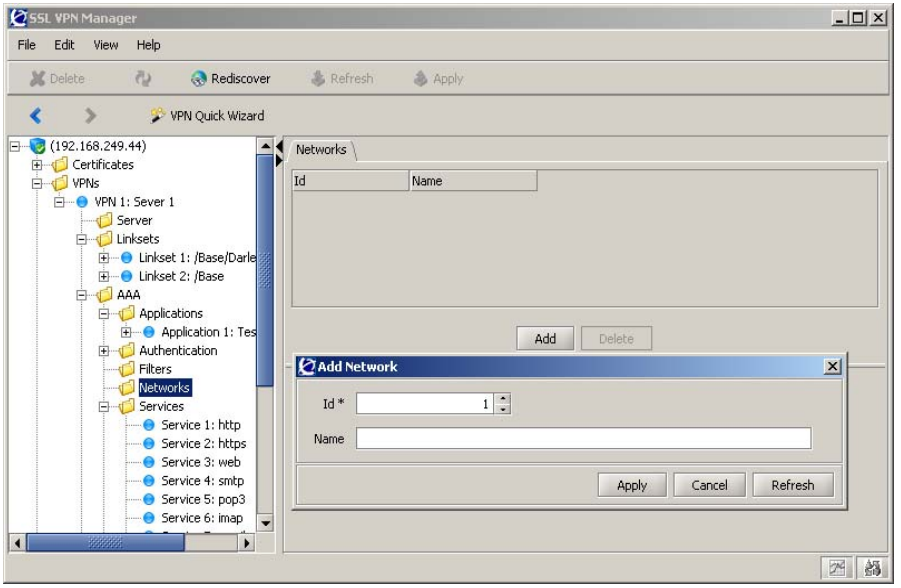
4 Click Apply to add the filter.

Networks

To add networks:

1 Select VPNs > VPN <*name*> > AAA > Networks > Add (Figure 66).

Figure 66 Add network



2 Select an ID for the network to be added. By default the ID starts at 1 for the first network added, the next defaults to 2, etc.

3 Specify a network name.

4 Click Apply. The network is added beneath Networks in the menu tree.

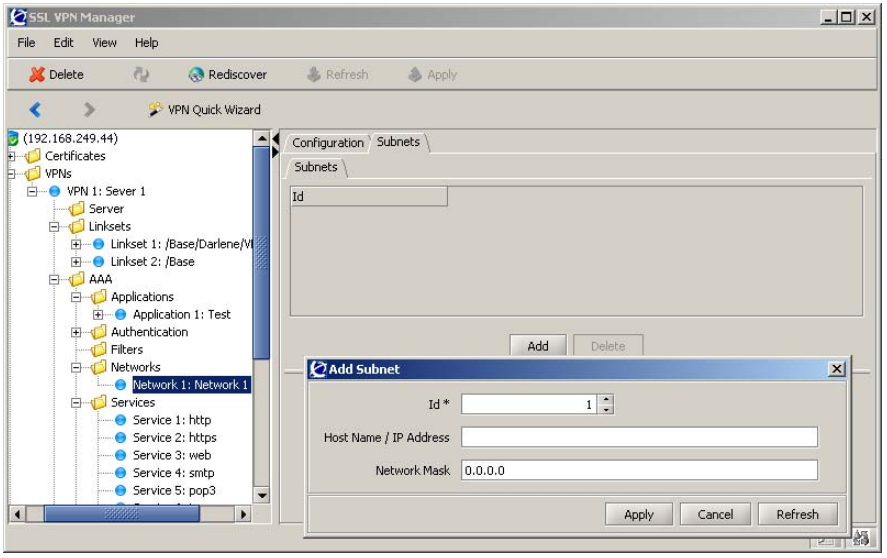
5 Click on the plus sign (+) to expand the Networks tree.

6 Select the network you have added.

7 Click on the Subnets tab.

8 Click Add. The Add Subnet window displays, as shown in Figure 67 on page 123.

Figure 67 Add subnet



9 The ID defaults to 1 if this is the first subnet being added and automatically increments to the next ID when you select the tab.

10 Enter the host name or IP address identifying the Outlook Web Access server.

11 Enter the desired network mask. Note that the network mask can be entered in number of bits, for example, 32 instead of 255.255.255.255.

12 Click Apply. The subnet is added to the menu tree beneath the Network ID: Name.

Configuring authentication

The SSL VPN module has a complete authentication infrastructure separate from the authentication capabilities of the Contivity gateway. Five different SSL VPN authentication methods (servers) are available: RADIUS, LDAP, NTLM, RSA SecurID, SiteMinder and Certificates.

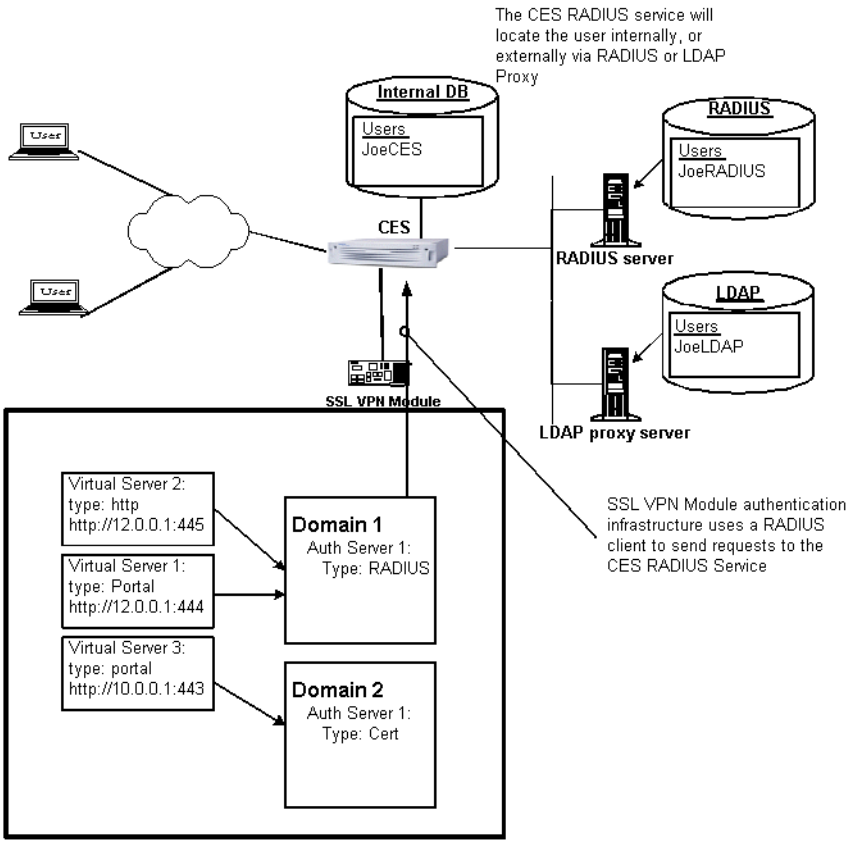
In general, SSL VPN authentication can be configured so that it directly connects to external servers such as RADIUS. Alternately, it can be configured to access the Contivity gateway authentication infrastructure (RADIUS and LDAP) using a RADIUS client. The Contivity RADIUS service will then proxy these access requests by formulating authentication requests against its internal db, external RADIUS or external LDAP proxy. Figure 59 details this configuration.

External server authentication

Companies with external authentication servers (RADIUS, LDAP and/or NTLM) can use these servers for authentication without modification. Which server and fallback order to use is defined in the Contivity gateway.

Figure 68 on page 125 describes the authentication infrastructure of the Contivity SSL VPN. Every virtual server has a VPN associated with it, and all SSL VPN user authentication is performed by the VPN. Multiple virtual servers can point to the same VPN.

Figure 68 Authentication infrastructure



Each VPN has a list of authentication servers associated with it. In the example, each VPN authentication list has one authentication server in it.

A typical use of the SSL VPN module is to create two VPNs: one for shared secret authentications (user name/password, RADIUS, LDAP Proxy, Tokens), and the second for certificate authentication. External authentication services can be accessed by the SSL VPN itself directly, or SSL VPN authentication requests can be proxied through the Contivity RADIUS service.

There are two authentication types which are available only directly from the SSL VPN Module: Netegrity Siteminder and NT VPN login (NTLM). If either of these two authentication types is used, you must configure the SSL VPN Module authentication server to access these directly. Using the One Time Password authentication option, it is possible to authenticate SSL VPN users with Siteminder or NTLM, then later create an IPsec user tunnel.

SSL VPN authentication and IPsec client authentication

After you successfully authenticate to the SSL VPN virtual server and are presented with the portal page, you can opt to start a full network access client (IPsec or SSL), providing a complete secure transport layer connectivity to the private side resources. Launching a full network access client (for example, starting the Contivity VPN Client requires a second authentication step). This authentication can occur in one of two ways:

- Re-use of the portal credentials — in this authentication scenario, the user ID and password that were collected in the portal login window are used for the full network access client user ID and password. This implies that the user must be authenticated against the Contivity gateway authentication infrastructure. For example, if a user, JoeUser, is stored in an external LDAP database, the following steps would occur:
  - — JoeUser is a valid user, provisioned into an external LDAP database.
  - — The Contivity has the RADIUS service configured to accept access requests from the SSL VPN module.
  - — The SSL VPN module has its RADIUS authentication server pointed at the Contivity RADIUS service.
  - — JoeUser points a browser to the portal login page, providing the user ID and password.
  - — The SSL VPN module formulates a RADIUS access request, sending it to the Contivity RADIUS service.
  - — The Contivity RADIUS service takes the information from the access request and re-bundles it as an LDAP user bind (or RADIUS access request or just queries its internal database, depending on the “Authentication Order” configuration settings in Services > RADIUS)
  - — Following a successful user bind to the external LDAP database, the Contivity RADIUS service creates and sends to the SSL VPN module, an RADIUS access accept.

  - — Successfully authenticated by the Contivity authentication infrastructure, the users portal page is presented.
  - — JoeUser then selects the Full Access tab, and the Contivity IPsec client is launched with the exact same credentials that were collected by the portal login page.
- One Time Password--in this authentication scenario, the user does not have to be located in the Contivity authentication infrastructure. Login proceeds as:
  - — JoeUser is a valid user, provisioned into an external SiteMinder database.
  - — The SSL VPN module has its authentication server pointed at the SiteMinder database.
  - — JoeUser points a browser to the portal login page, providing user ID and password.
  - — SSL VPN module authenticates the user against SiteMinder, successfully authenticated, the users portal page is presented.
  - — JoeUser then selects the Full Access tab; a one time password is generated by the SSL VPN Module and communicated to the Contivity gateway along with the user ID and IP address of JoeUser.
  - — The Contivity IPsec client is launched using the User ID and One Time Password.

Using One Time Password, it is possible to make use of authentication methods available only on the SSL VPN module to authenticate full access (IPsec/SSL clients). Authentication methods available only on the SSL VPN are SiteMinder, NTLM, and client certificates.

There are several steps that must be completed to completely configure SSL VPN authentication infrastructure:

- Contivity RADIUS service must be configured to accept RADIUS access requests from the SSL VPN Module.
- An SSL VPN must be created.
- An SSL VPN authentication server must be added to the VPN. If the Contivity RADIUS service is the destination, it must be configured appropriately. An external authentication server can also be configured.
- A group must be added to the SSL VPN that corresponds to the Contivity group.
- If full network access is desired, the portal Full Access tab elements must be configured appropriately:

— Contivity One Time Password must be configured appropriately for user tunnel launch types listed below.

— State is enabled.

— Contivity IP address (use the Contivity public physical or CLIP address that you want the IPsec user tunnel to connect to). When 0.0.0.0 is used the as Contivity IP address value instead of the preconfiguration of the Contivity IP address, the address is determined dynamically at run time. The SSL VPN Module uses the Virtual Server IP Address for the end point of the IPsec user tunnel.

— Contivity group ID must be the same value as is configured on Profiles > Groups > IPsec > Authentication > Group ID and Password.

When client certificate authentication, SECURID, NTLM, or Siteminder is used, or when users are stored in a Contivity internal database, One Time Password must be enabled. When One Time Password is enabled, it is not necessary to configure Contivity groupID/password.

When users are stored in an external RADIUS or LDAP proxy, One Time Password does not need to be enabled. In this case the Contivity GroupID/ password must be configured.

Table 3 describes the authentication mechanisms that are available.

Table 3 Authentication mechanisms

If your users are stored here	Authentication mechanism	Required configuration items
Contivity SSL VPN database	Storing users in the SSL VPN internal database is not a recommended configuration, as Contivity IPsec authentication is only possible if Contivity One Time Password is enabled.	- Contivity RADIUS service - SSL VPN RADIUS authentication server pointing at Contivity gateway - Contivity One Time Password enabled
Contivity local internal database	The SSL VPN portal will generate a RADIUS access request, sending this to the Contivity RADIUS service. The Contivity gateway will find that local user and authorize the access request with an access-accept. IPsec user tunnel authentication of the user stored in the Contivity internal database occurs normally.	- Contivity RADIUS service - SSL VPN RADIUS authentication server pointing at Contivity

Table 3 Authentication mechanisms

If your users are stored here	Authentication mechanism	Required configuration items
RADIUS	The SSL VPN portal generates a RADIUS access request, sending this to the Contivity RADIUS service. The Contivity gateway then generates a RADIUS access request, sending it to its configured RADIUS authentication servers. The access reply is proxied back to the SSL VPN. IPsec user tunnel authentication occurs normally after successful RADIUS authentication.	- Contivity RADIUS service - SSL VPN RADIUS authentication server pointing at the Contivity gateway - Contivity RADIUS authentication server
LDAP proxy	The SSL VPN portal generates a RADIUS access request, sending this to the Contivity RADIUS service. The Contivity translates the credentials into an LDAP bind query. The result of the bind is sent to the SSL VPN in the form of a RADIUS access message. IPsec user tunnel authentication occurs normally after a successful LDAP proxy authentication.	- Contivity RADIUS service - SSL VPN RADIUS authentication server pointing at Contivity - External LDAP Directory
NTLM	The SSL VPN portal must be configured to directly access the external NT authentication server. IPsec user tunnel authentication occurs through the use of a one-time generated password.	- SSL VPN NTLM authentication server - Contivity One Time Password enabled
RSA SecurID	The SSL VPN portal must be configured to directly access the external NT authentication server.	- Contivity RSA service - SSL VPN RSA authentication server - configure RSA server settings - import sdconf.rec file

Table 3 Authentication mechanisms

If your users are stored here	Authentication mechanism	Required configuration items
Siteminder	The SSL VPN portal must be configured to directly access the external Siteminder authentication server. IPsec user tunnel authentication occurs through the use of a one-time generated password.	- SSL VPN Netegrity Siteminder authentication server - Contivity One Time Password enabled
Certificates	The SSL VPN portal must have the appropriate CA and CRL location configured. IPsec user tunnel authentication occurs through the use of a one-time generated password.	- Contivity One Time Password enabled

Figure 69 shows the settings for configuring the Contivity RADIUS service to accept requests from the SSL VPN.

Figure 69 Configuring the RADIUS server

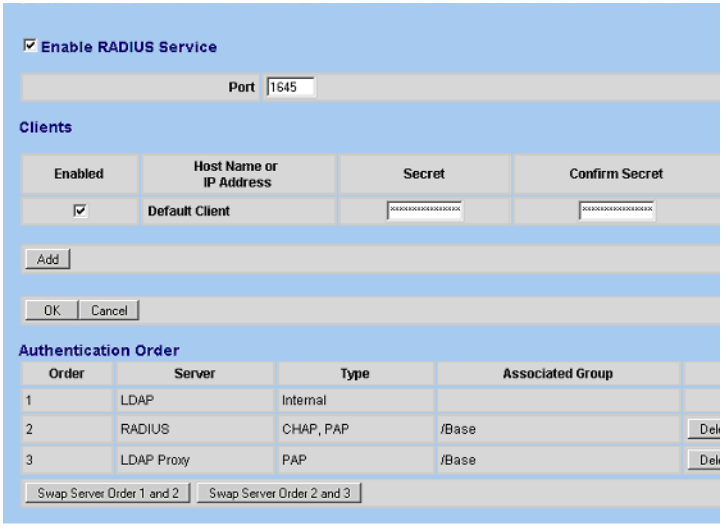
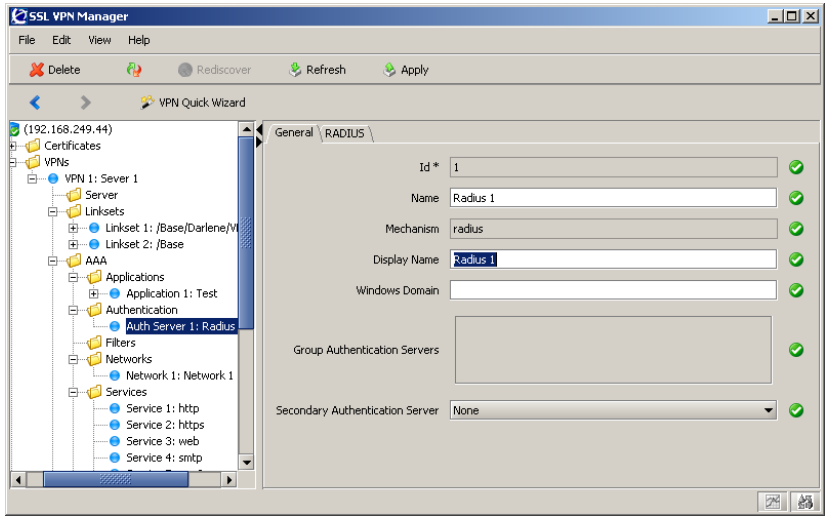


Figure 70 shows the settings for configuring the SSL VPN RADIUS client to point to the Contivity gateway RADIUS service.

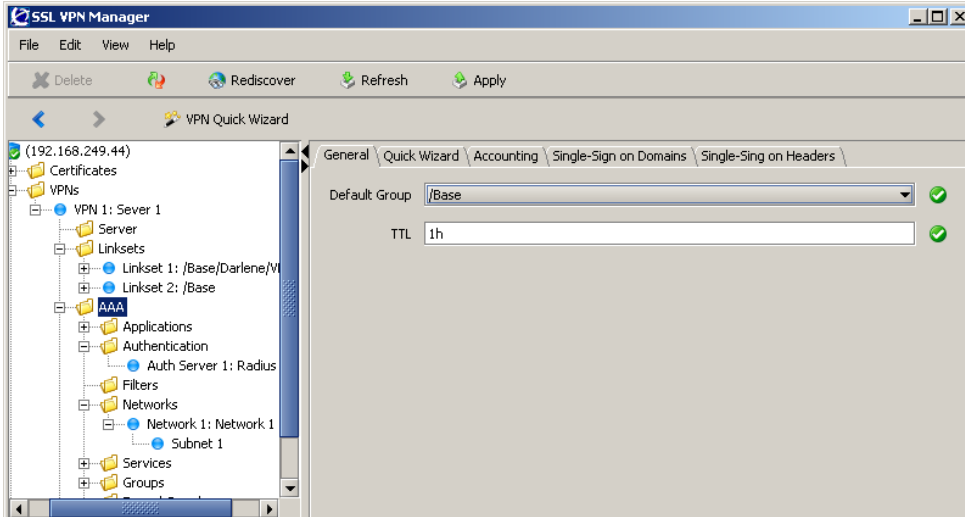
Figure 70 RADIUS client pointing to RADIUS service



Group assignments include the following:

- All of the groups within an SSL VPN should be created so that they correspond to the groups that exist on the Contivity gateway.
- The SSL VPN default group as shown in Figure 71 corresponds to the default group setting on the Servers > RADIUS auth window.

Figure 71 Default group for a VPN



External database authentication

The SSL VPN feature supports using the following external database authentication methods:

- RADIUS
- LDAP
- NTLM
- SiteMinder

IPsec and SSL users can be stored in either the same or different internal and external databases.

When a remote user wants to access a resource provided in the VPN, the Contivity gateway authenticates the user by sending a query to an external RADIUS, LDAP, NTLM VPN, or Netegrity SiteMinder server. This makes it possible to use already existing authentication databases within the intranet. The Contivity gateway includes username and password in the query and requires the name of one or more access groups in return. The name of the LDAP and RADIUS access group attribute is configurable.

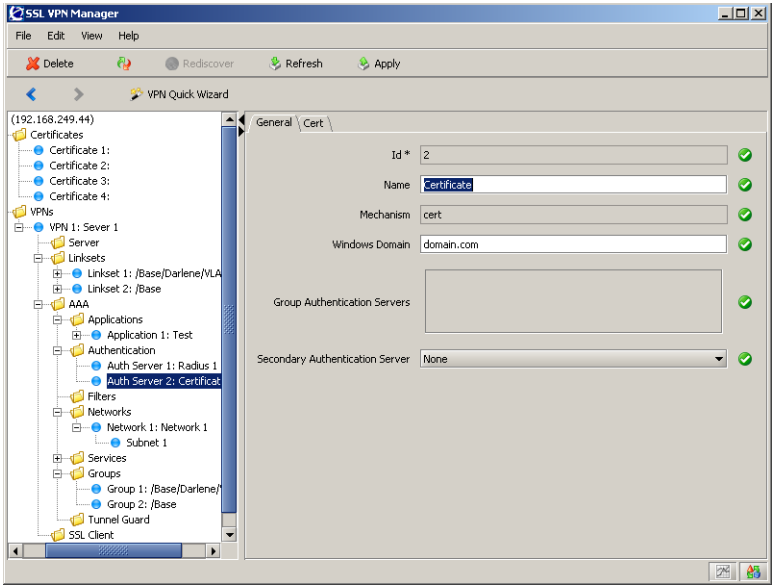
You can configure more than one authentication method within any given VPN (portal).

Client certificate authentication

With client certificate authentication enabled on the Contivity gateway, remote users with a valid client certificate installed on their computers do not need a portal login. When the Contivity gateway has accepted the certificate, the user is directed to the portal's home tab.

In each Contivity gateway, you can create an unlimited number of virtual SSL servers (Figure 72 on page 133). Each virtual SSL server can handle a specific service, such as HTTPS, SMTPS, IMAPS, or POP3S. A virtual SSL server uses a server certificate to authenticate itself to clients. You can also configure a virtual SSL server to require client certificates to authenticate clients before granting access to the requested service (Figure 72 on page 133).

Figure 72 Certificate authentication server



When a virtual SSL server is set to require client certificates, a certificate request message is sent from the server to the client during the SSL handshake. The client responds by sending its public key certificate in a certificate message. After that, the client sends a CertificateVerify message to the server. The CertificateVerify message is signed by using the client's private key, and contains important information about the SSL session known to both the client and the server. When it receives the CertificateVerify message, the virtual SSL server uses the public key from the client certificate to authenticate the client's identity.

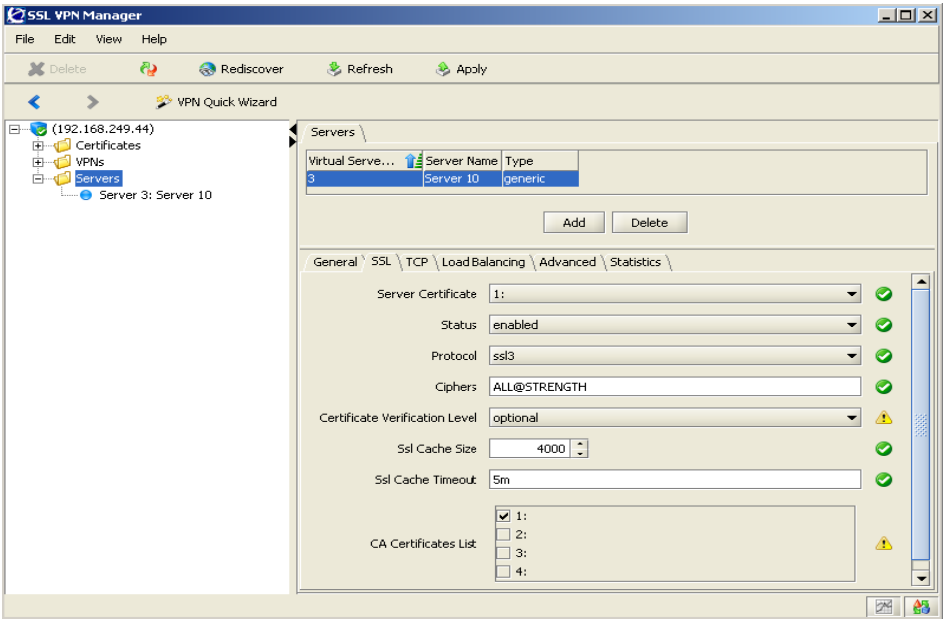
The virtual SSL server also checks whether the certificate the client presents is signed by an accepted certificate authority. Accepted certificate authorities are defined by the CA certificates you have specified in the virtual SSL server. The certificate you use for generating client certificates must therefore also be specified as a CA certificate in the virtual SSL server.

The virtual SSL server also checks the client certificate should be revoked, by comparing the serial number of the presented client certificate with entries in the certificate revocation list.

The following steps demonstrate how to configure a virtual SSL server to require client certificates for authentication purposes.

1 Go to Servers and select the SSL tab. The SSL window opens.(Figure 73)

Figure 73 Virtual SSL server



2 Select a Server Certificate number from the drop-down list to assign to the certificate.

3 Select Enabled or Disabled for Status.

4 Select a protocol from the drop-down list.

5 Select a Certificate Verification level from the drop-down list.

6 Use the up and down arrows to set the Cache size.

7 Enter the amount of time before the Set Cache times out.

Managing client certificate revocation

Certificate revocation lists (CRLs) are maintained by certificate authorities to recall client certificates that are no longer considered trustworthy. The reasons for this can be that the client certificate may have been issued by mistake, or that the subject accidentally has revealed the private key.

If you keep a certificate revocation list on your SSL server, client certificates sent to the server are checked against the CRL (Figure 74). If a match is found, the SSL session is terminated. This mode of operation requires, first of all, that you have configured the virtual SSL server to always require client certificates. You must also regularly check with the certificate authorities you trust for their latest CRLs.

Moreover, if you take on the role of a certificate authority by issuing your own client certificates (Figure 75 on page 136), you will also need to maintain your own certificate revocation lists. This can be done by listing the serial numbers of the client certificates you want to revoke in an ASCII file.

Figure 74 Configuring automatic CRL retrieval

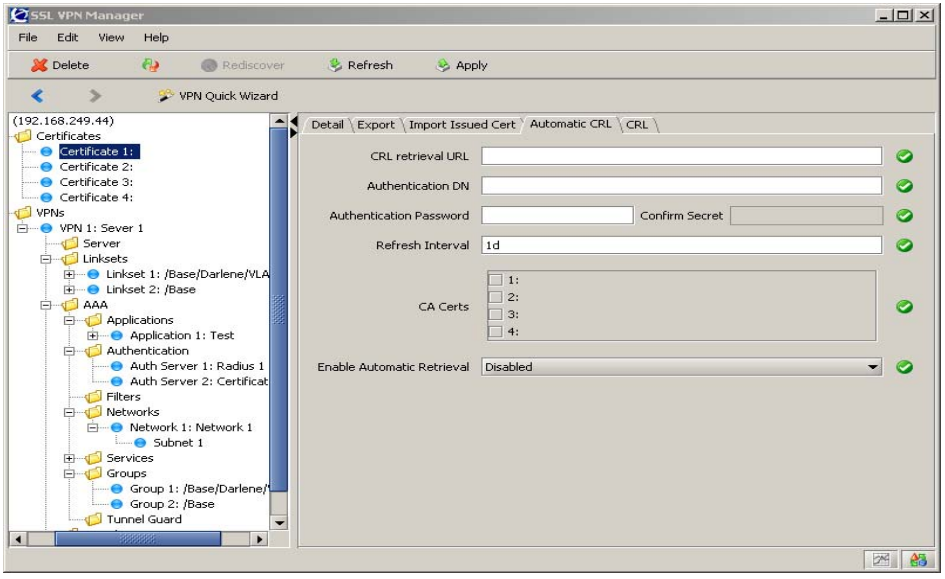
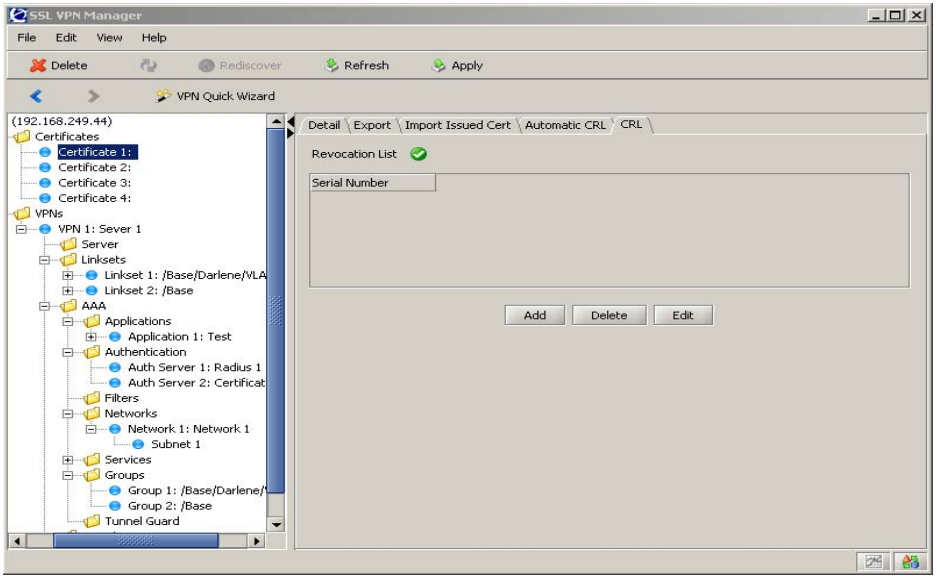


Figure 75 Creating your own CRL



Making use of the Contivity RADIUS authentication

When the SSL VPN module is set to use the Contivity RADIUS service for authentication (Figure 76 on page 137), all current Contivity users can be given access to the SSL. This includes all internal users, RADIUS, SECURID, and LDAP proxy users (Figure 77 on page 137).

Figure 76 Contivity RADIUS service configuration

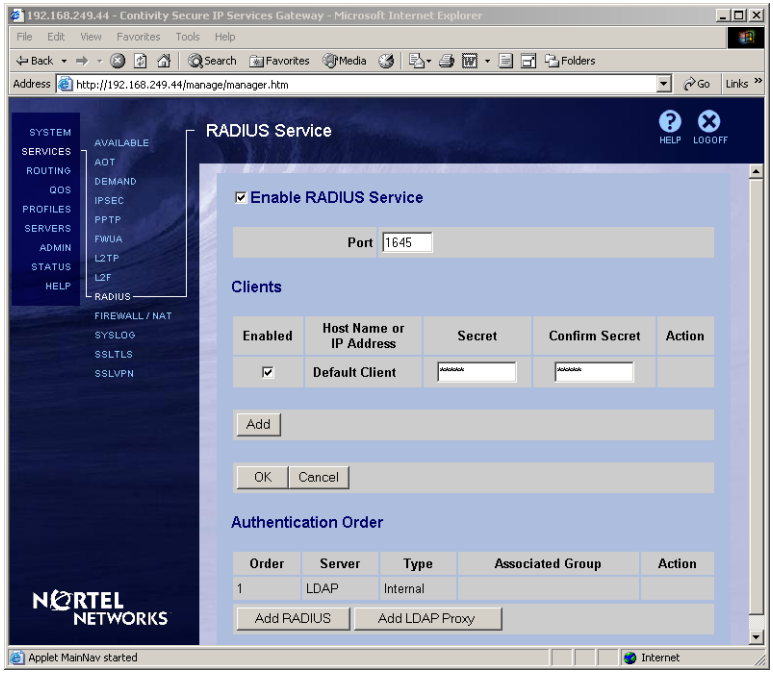
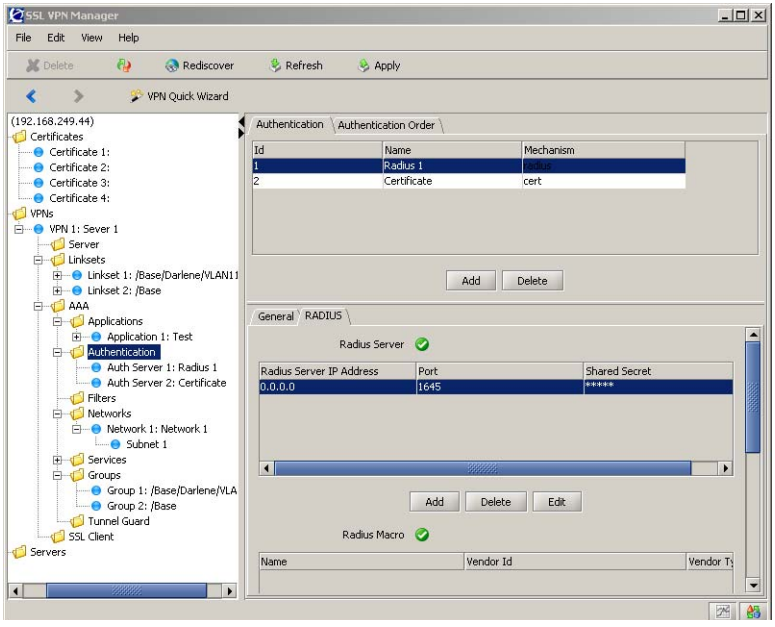


Figure 77 SSL VPN module RADIUS client aimed at Contivity RADIUS service



SSL VPN authentication of Contivity internal users using RADIUS

To enable SSL VPN portal access for users stored in Contivity internal DB:

1. Go to Services > RADIUS and enable the Contivity RADIUS service.
2. Set the port number that you use for RADIUS authentication.
3. You can either set the Default Client shared secret or you can specify a shared secret to a particular host address. If the default client is enabled, any network host that knows the shared secret is allowed to use the Contivity gateway for RADIUS Authentication. If just a host address is allowed, only that particular host address will be allowed for RADIUS authentication. Nortel Networks recommends that you configure the Contivity to allow RADIUS authorization requests from the SSL Module Interface IP Address.
4. Under Authentication Order, verify that LDAP is set to the 1 in the authentication order.
5. The Contivity gateway returns a vendor-specific attribute number 26, vendor id 1872. This attribute is populated with the Contivity gateway user group of which the user is a member.
6. If the SSL card is configured with the same group name as the group name returned by the Contivity gateway RADIUS service, the users SSL session has access rights as defined by this particular SSL group. When a group is returned by the Contivity RADIUS service that corresponds to a Contivity gateway user group, all Contivity user accounts located within the group have access to the SSL VPN module. This includes all IPsec, PPTP, L2TP and L2F accounts. FWUA accounts will not have access.

   If the group that is returned by the Contivity gateway RADIUS service does not actually exist on the SSL VPN, the user will not be given access unless a default group has been specified to the SSL VPN. In this case the user session will receive rights from the default group.

SSL VPN authentication of users stored in external RADIUS

The Contivity RADIUS service is capable of authenticating external RADIUS users as well as internal users. SecurID users are also supported over the Contivity RADIUS proxy. Axent Defender is not supported at this time.

To configure the Contivity gateway to allow external RADIUS users:

1. Go to Service > RADIUS and enable the Contivity RADIUS Service.
2. Set the port number that you want to use for RADIUS authentication.
3. You can either set the default client shared secret or you can specify a shared secret to a particular host address. If the default client is enabled, any network host that knows the shared secret can use the Contivity gateway for RADIUS authentication. If just a host address is allowed, only that particular host address is allowed to have RADIUS authentication. Nortel Networks recommends that the user configure the contivity to allow RADIUS Authorization requests from the SSL module interface IP address.
4. Under Authentication Order, verify that RADIUS is enabled within the authentication order.

RADIUS returning a group attribute

If your RADIUS server is configured to return a class attribute that corresponds to a Contivity user group, this user group is returned to the SSL module.

For example, RADIUS user1 returns a class attribute of ou=contivity, ou=test. This group corresponds to Contivity gateway group /Base/Test/Contivity. The group name /Base/Test/Contivity is returned as a vendor-specific attribute number 26-vendor id 1872 to the SSL card. If the group /Base/Test/Contivity exists on the SSL card, the user sessions obtain the rights defined in the SSL group configuration. If the group /Base/Test/Contivity does not exist and no default group is specified, the user will not be able to log in to the SSL session. If /Base/Test/Contivity does not exist on the SSL card and a default group is enabled, the user session obtains the rights defined in the default group configuration.

If the RADIUS user does not return a group attribute, the user will not be authorized unless a default group is specified within the VPN. The user session obtains rights as defined in the default group configuration.

SSL VPN authentication of users stored in external LDAP

To enable and configure RADIUS service:

1. Select Services > RADIUS and select Enable RADIUS Service. The default port is 1645. It is advised to leave this as the default.

2. Select Enabled for the default client.
3. Add a secret and confirm the secret.
4. Click on OK.
5. Under Authentication Order, click on Add LDAP Proxy.
6. Click on Swap Server Order 1 and 2.
7. To enable and configure the LDAP proxy, go to Servers > LDAP Proxy.
8. Select Enable Access to LDAP Proxy Server.
9. Enter the IP address of the master LDAP.
10. Choose the port. Nortel Networks strongly advises that you leave this at the default of 389 (or 636 if you are using LDAPS).
11. Enter the Bind DN. The user only needs permission to read the LDAP. For example, the root of LDAP is dc=example,dc=com.

    If a user whose name is Bob A Smith is in the users group, the bind DN goes to CN=Bob A Smith,CN=Users,DC=example,DC=com (on Active Directory).

12. Enter the secret for this user.
13. If you have slave LDAPs, enter the details.
14. Select Username/Password Access.
15. Enter the username attribute for the particular LDAP that you are using, For Active Directory use sAMAccountName and for Netscape and Novell use LDAP user UID.
16. Leave User Password Attribute blank.
17. Leave LDAP Filter blank.
18. Under User Policy Attributes, choose an attribute to assign to the group that the users will be assigned to. In Active Directory you can choose postOficeBox, and in the postOfficeBox attribute of the user on the LDAP, enter /Base/*groupname* where *groupname* is the actual name of the group that you want the user forced into. These groups must be present on the Contivity gateway and SSL VPN Module 1000.

    If the user does not have a group assigned, the default group on the LDAP Proxy window is passed back.

Using SSL VPN native authentication methods

This section details configuration of SSL VPN authentication servers directly at external authentication databases. Using this authentication model (as opposed to proxying the authentication through the Contivity RADIUS service) provides access to authentication mechanisms that are not natively supported by the Contivity gateway (such as certificates, SiteMinder and NTLM).

Note that when SSL VPN module authentication servers are configured to directly access external authentication databases, you must use One Time Password to start the full access client (IPsec or SSL).

LDAP authentication

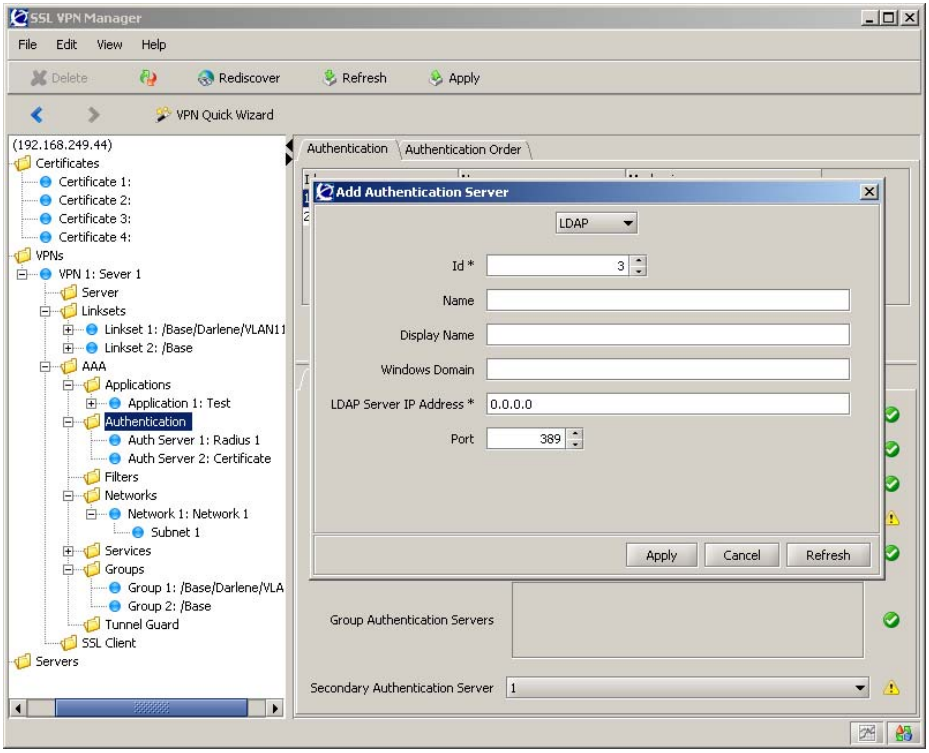
LDAP authentication lets you configure user authentication through an existing intranet LDAP server.

To configure LDAP authentication:

1 Create a new VPN, or configure an existing VPN (Figure 78 on page 142).

If you have already created a VPN (=portal) to which you want to add LDAP authentication, type the VPN number. To create a new VPN, type a VPN number not currently in use.

Figure 78 Authentication through intranet LDAP server



2 Create an authentication ID for LDAP authentication.

Each time you create a new authentication ID, you enter a wizard that prompts you for the required information. When the wizard is complete, you go to the menu for the current object.

3 Select the authentication method, such as ldap.

This wizard step corresponds to entering the type on the authentication menu and selecting the authentication method.

4 Specify a name for the authentication method.

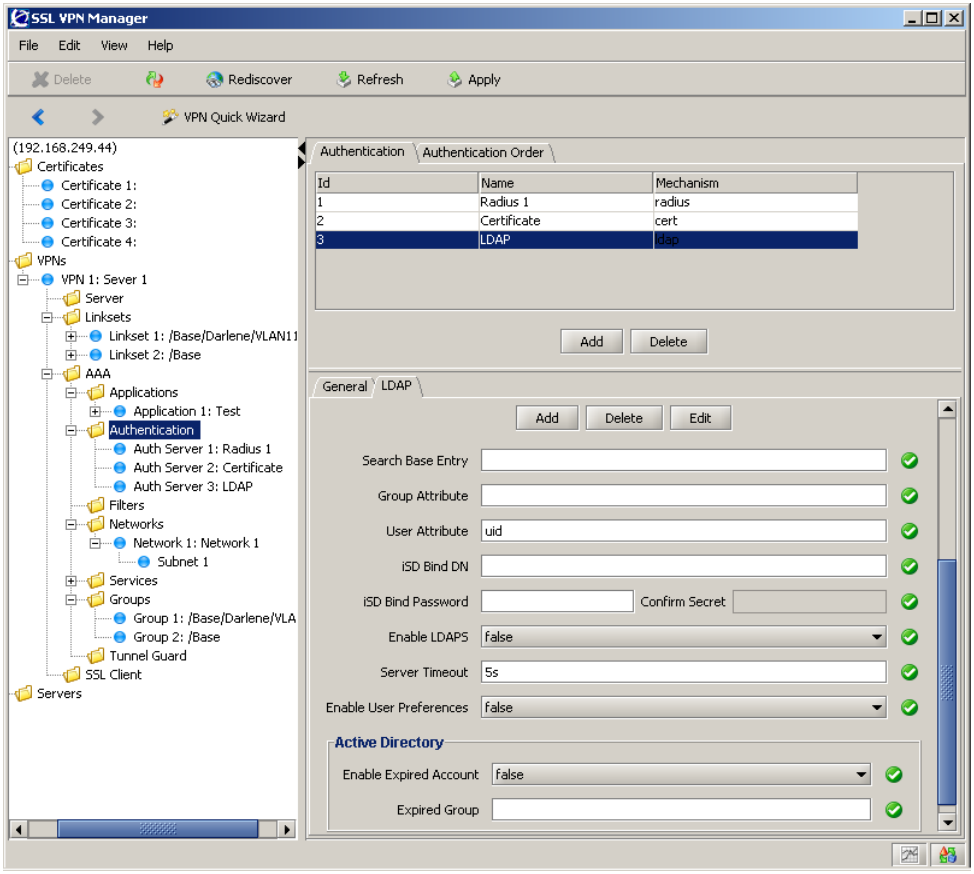
A name is mandatory. If you refer to the current authentication method later in a client filter, this name should be used.

This wizard step corresponds to entering the name on the Authentication menu.

5 Specify the LDAP server IP address and port (Figure 79).

This adds an LDAP server that is queried to perform authentication of a remote user prior to accessing resources on the portal. Port number 389 is the default number, but you can change it. If LDAPS is used for traffic sent between the Contivity gateway and the LDAP server, you should use port number 636.

Figure 79 LDAP server IP address and port



6 Specify the search base entry.

This step assigns the DN (Distinguished Name) that points to the entry that is one level up from where all user entries are found.

If user entries are located in several different places in the LDAP Dictionary Information Tree (DIT) or if the user's portal login name is not identical to the user record identifier (RDN), you should assign a DN pointing to an entry from where the entire DIT can be searched. However, this requires the Contivity gateway to authenticate itself to the LDAP server, using the values specified for isdBindDN and isdBindPassword.

7 Specify the LDAP group attribute name.

This step defines the LDAP attribute that contains the group names of which a particular user is a member. The group names contained in the LDAP attribute must be defined for the VPN on the Contivity Secure IP Services Gateway, complete with one or more access rules. If you specify more than one group attribute name, separate the names using a comma (,).

8 Specify the LDAP user attribute name.

This step defines the LDAP attribute that contains the user names. The default user attribute name is uid.

9 Specify the isdBindDN entry and isdBindPassword (optional).

This step lets you point out an LDAP entry (distinguished name) which the Contivity gateway should authenticate. Generally, you can skip this step. It is only required if the Contivity gateway should authenticate to the LDAP server (for example, to be able to search the DIT).

10 Specify whether LDAPS should be used for traffic between the Contivity gateway and the LDAP server.

By setting this command to true, LDAP requests between the Contivity gateway and the LDAP server are made using a secure SSL connection, such as LDAPS. The default value is false, which you keep by clicking on Enter.

When the above information is supplied, the Authentication menu is displayed. The ldap option is added to the menu because the current authentication type is now set to ldap.

If needed, you can edit the IP address and port settings from the VPN > AAA > Authentication tab. This is also where you can add additional LDAP servers for redundancy. Other LDAP commands (for example, to edit the search base entry, group, and user attributes and the LDAP server timeout value) are found under LDAP.

11 Set the display name for this authentication method (optional).

The display name appears in the Login service list on the portal login window and in the SSL VPN client's login window. This is a way to quickly direct the remote user to the proper authentication server if the portal uses different authentication methods. If the user selects default from the list, authentication is carried out according to the configured authentication order.

12 Specify the authentication fallback order.

This step sets the preferred order in which the defined authentication methods are applied when a remote user logs in to the portal. Even if you have defined only one authentication method, you should specify the authentication ID.

If you are using more than one authentication method, specify the authentication ID that represents the method by which the majority of users are authenticated as the first number. This ensures the best performance.

13 Apply your configuration changes.

You should search the LDAP dictionary information (DIT) if:

- User entries are located in several different places in the DIT
- The user's portal login name is not identical to the user record identifier (RDN) on the LDAP server

The following procedure shows the adjustments that you must make to the LDAP configuration if the user's portal login name is not identical to the user record identifier (RDN) on the LDAP server.

1 Set the LDAP search base entry.

This step assigns a DN pointing to a position in the DIT where all user records are found.

2 Set the LDAP user attribute name.

The user's portal login name is not identical with the user record identifier (RDN). To find the user record in the LDAP Dictionary Information Tree (DIT), a combination of the user's login name and a user attribute is used when searching the tree.

In Active Directory, the sAMAccountName attribute contains the value that corresponds to the user's login name. Thus, if the user's login name is bill, the user record will be found because it matches the sAMAccountName attribute value for the user whose record identifier (RDN) is cn=bill smith.

3 Point out an LDAP entry to be used for Contivity gateway authentication.

To be able to search the DIT, the Contivity gateway must authenticate itself towards the LDAP server.

4 Set a password for Contivity gateway authentication.

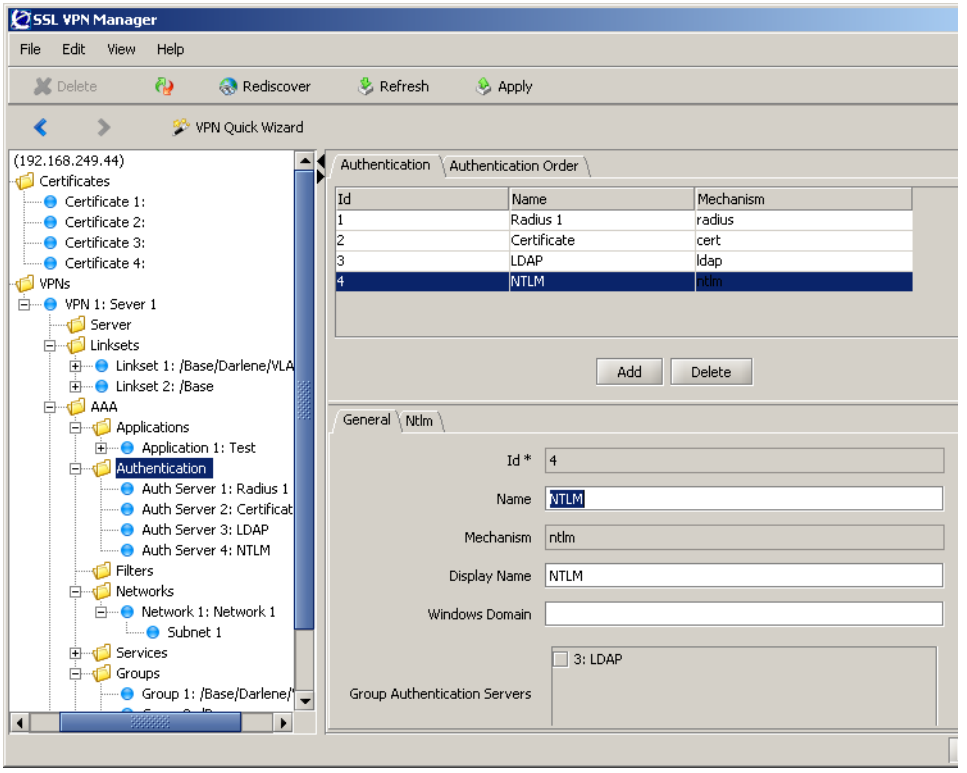
This step sets the password to be used when the Contivity gateway authenticates itself to the LDAP entry pointed out with the isdbinddn command.

5 Apply your configuration changes.

NTLM authentication

NTLM authentication allows you to configure user authentication through an existing intranet NTLM server (Figure 80 on page 147).

Figure 80 NTLM authentication



1 Create a new VPN or configure an existing VPN.

If you already created a VPN (=portal) to which you want to add NTLM authentication, type the VPN number. To create a new VPN, type a VPN number not currently in use.

2 Create an authentication ID for NTLM authentication.

Each time you create a new authentication ID, you enter a wizard that prompts you for the required information. When the wizard is complete, you go to the menu for the current object.

3 Set the authentication method to NTLM.

This wizard step corresponds to entering the type on the Authentication menu and selecting the authentication method.

4 Set the name for this authentication method.

A name is required. If the authentication method is later referenced in a client filter, it is the method name that should be referenced.

This wizard step corresponds to entering the name on the Authentication menu.

5 Configure the NTLM server settings.

This step adds an NTLM server that is queried to perform user authentication.

When you supply this information, the Authentication menu appears. The ntlm option has been added to the menu because the current authentication type is now set to ntlm.

If needed, you can edit the IP address at ntlm/servers. This is also where you can add additional NTLM servers for redundancy. Other NTLM commands are found under ntlm.

6 If you have multiple NTLM VPNs, set the display name (optional).

Set the display name to the Windows domain name of the NTLM server. The name will appear in the Login Service list on the portal login window and in the SSL VPN client's login window. If the user selects this name from the list, the authentication method associated with the name will automatically be used. If the user selects default instead, authentication will be carried out according to the configured authentication order.

7 Specify the authentication fallback order.

This step sets the preferred order in which the defined authentication methods are applied when a remote user logs in to the portal. Even if you have defined only one authentication method, the authentication ID representing that method should be specified. To view which authentication ID number corresponds to a currently configured authentication method, use the VPN > AAA > Authentication tab.

When using more than one authentication method, specify the authentication ID that represents the method by which the majority of users are authenticated as the first number for best performance.

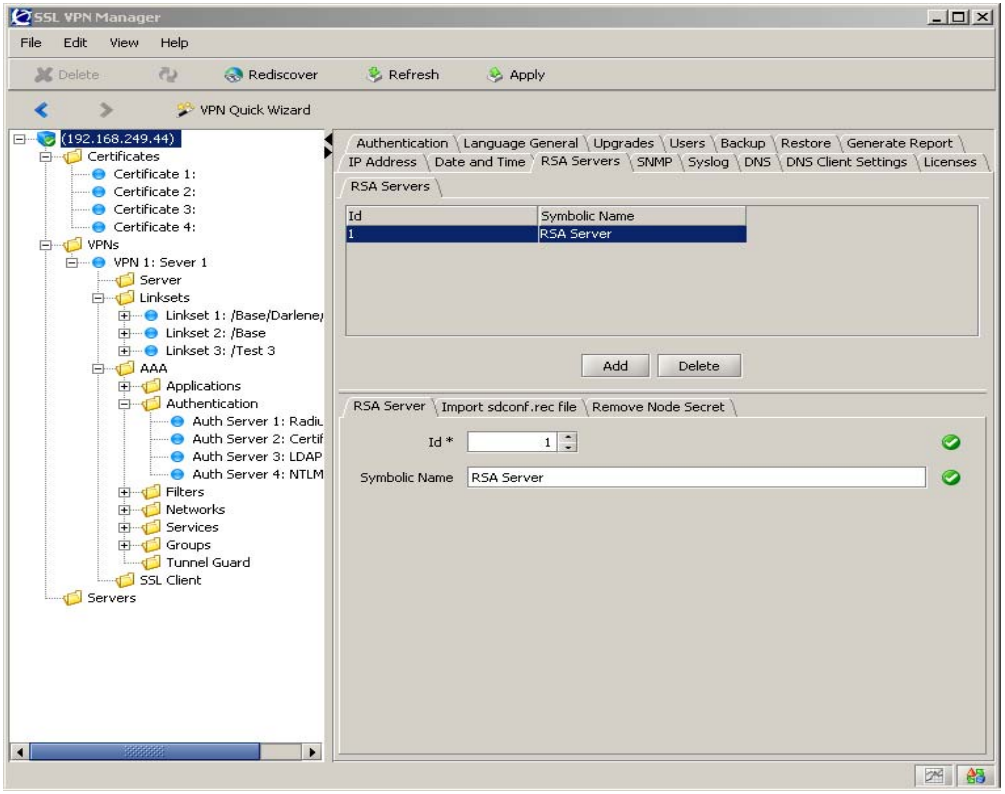
8 Apply your configuration changes.

RSA SecurID authentication

Configure the RSA server settings.

1. Select VPN url > RSA Servers > RSA Server tab.
2. Click Add.
3. Create an ID.
4. Create a symbolic name for the server.
5. Click Apply. The window closes and a server has been added Figure 81.

Figure 81 RSA configuration



6. Highlight the server you created from the RSA and select Import sdconf. rec file tab.

7 Browse to import the file. The sdconf.rec file is a configuration file that contains critical RSA ACE/Server information. Contact your RSA ACE/Server administrator to obtain the file and make it available on the desired TFTP/FTP/SCP/SFTP server.

8 Highlight the server just created and from the RSA General tab and enter the RSA server display name.

Configure the RSA Authentication Method

1 Select VPNs > VPN < *name*> > AAA > Authentication.

2 Click Add. The Add Authentication Server window opens.

3 Select RSA from the drop down list.

4 Select the ID for this server.

5 Set the desired name for this authentication method. A name is required. If the authentication method should later be referenced in a client filter, it is the method's name that should be referenced.

6 Click Apply.

7 From the RSA General tab, enter the RSA server display name.

8 Select the Group Authentication and Secondary Authentication servers.

9 From the RSA tab, select the RSA symbolic and group names from the drop-down lists.

10 Select the Authentication Order tab to specify the authentication fallback order.

This step sets the preferred order in which the defined authentication methods are applied when a remote user logs in to the portal. Even if you have defined only one authentication method, the authentication ID representing that method should be specified.

When using more than one authentication method, specify the authentication ID that represents the method by which the majority of users are authenticated as the first number for best performance.

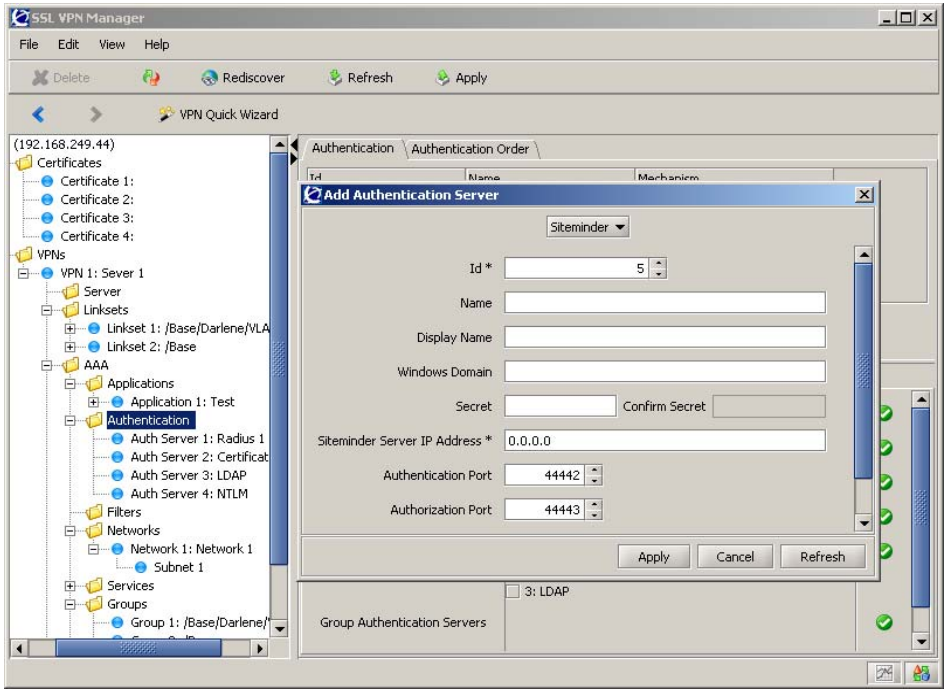
11 Apply your changes.

SiteMinder authentication

To configure the Contivity gateway to use a Netegrity SiteMinder server (Figure 82) for user authentication is relatively easy. On the other hand, a great deal of configuration is required on the SiteMinder side. The Contivity gateway acts as a client, or agent, to the SiteMinder server. Therefore, the Contivity gateway should be configured as an agent in SiteMinder.

It is assumed that you are familiar with SiteMinder or have access to SiteMinder documentation.

Figure 82 SiteMinder configuration



1 Create a new VPN, or configure an existing VPN.

   If you have already created a VPN to which you want to add SiteMinder authentication, type the VPN number. To create a new VPN, type a VPN number not currently in use.

2 Create an authentication ID for SiteMinder authentication.

Each time you create a *new* authentication ID, you will automatically enter a wizard that prompts you for the required information. Once the wizard is completed, you will enter the regular menu for the current object.

3 Select the authentication mechanism, such as `siteminder`.

This step is equivalent to entering the type on the Authentication menu and select the authentication method.

4 Set the name for this authentication method.

A name is mandatory. If you later refer to the current authentication method in a client filter, this name should be used. This wizard step corresponds to entering the name on the Authentication menu.

5 Configure the SiteMinder server settings.

This step adds a SiteMinder server that will be queried to perform user authentication.

6 Confirm the suggested port numbers for authentication, authorization and accounting.

7 Enter a unique shared secret (password) that the Contivity gateway will use to authenticate itself to the SiteMinder server.

Apart from the shared secret, the Contivity gateway also uses its agent name (default agent name is `Nortel Agent`) and a group attribute (default group attribute is `64`). These three values MUST be the same as those defined for Agent and Agent Type in the SiteMinder Policy Server configuration. See the Netegrity technical configuration guide *Using Netegrity SiteMinder with SSL VPN*.

When the information is supplied, the Authentication menu appears. The siteminder option is added to the menu, because the current authentication type is now set to siteminder.

If needed, the IP address can be edited under siteminder/servers. This is also where additional SiteMinder servers can be added for redundancy. Other SiteMinder commands for changing agent name, shared secret or group attribute are found under siteminder.

8 Set the display name (optional).

This step sets a display name for this particular authentication method. The name will appear in the Login Service list on the portal login window and in the SSL VPN client's login window. If the user selects this name from the list, the authentication method associated with the name is automatically used. If the user selects default instead, authentication will be carried out according to the configured authentication order.

9 Specify the authentication fallback order.

This sets the preferred order in which the defined authentication methods are applied when a remote user logs in to the portal. Even if you have defined only one authentication method, the authentication ID representing that method should be specified.

When using more than one authentication method, specify the authentication ID that represents the method by which the majority of users are authenticated as the first number for best performance.

10 Apply your configuration changes.

Single sign-on VPNs

This section describes the steps for configuring single sign-on VPNs to allow users single sign-on access to back end servers. If you want single sign-on to back end servers using internal auto-login, external-auto login FTP, and SMB links, you must configure single sign-on VPNs.

If the single sign-on VPN is left blank on a particular SSL VPN, the SSL device does not automatically send the user credentials to the back end server. Users are prompted to enter their logon credentials.

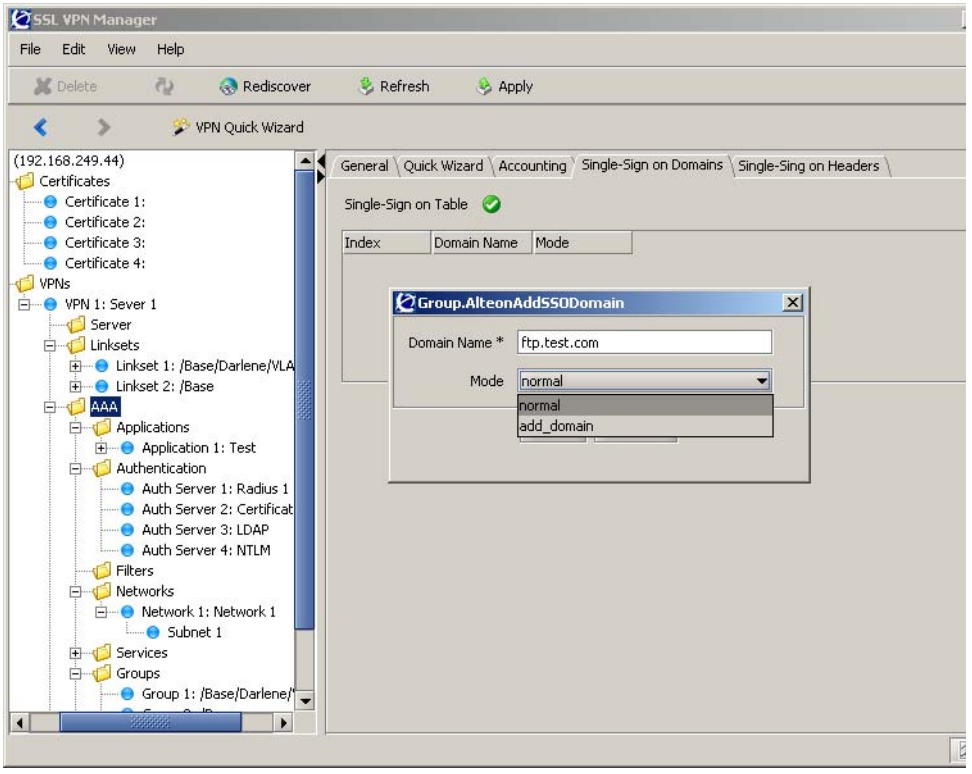
If SSO VPNs are configured, the username and password used to access the portal is automatically forwarded to the back end servers, resulting in single sign-on access to end users.

The SSO VPN configuration can be found at VPN > AAA > SSO Domains.

To create an FTP link for single sign-on for an FTP server ftp.test.com:

1 Go to VPNs > VPN <*name*> > AAA > Single Sign on Domains tab (Figure 83) and enter either the fully qualified VPN ftp.test.com or enter the VPN test.com.

Figure 83 Single Sign On domains



If test.com is used for an SSO domain, then all hosts located within the test.com domain can be used for single sign-on access links.

2 Select one of the following modes:

- Normal — When normal mode is selected, the SSL device automatically sends the username password to the back end servers.
- Add_Domain — When Add_Domain mode is selected, the SSL device automatically sends the domain\username password to the back end servers. The VPN is populated by the Windows domain field configured on a particular users authentication server.

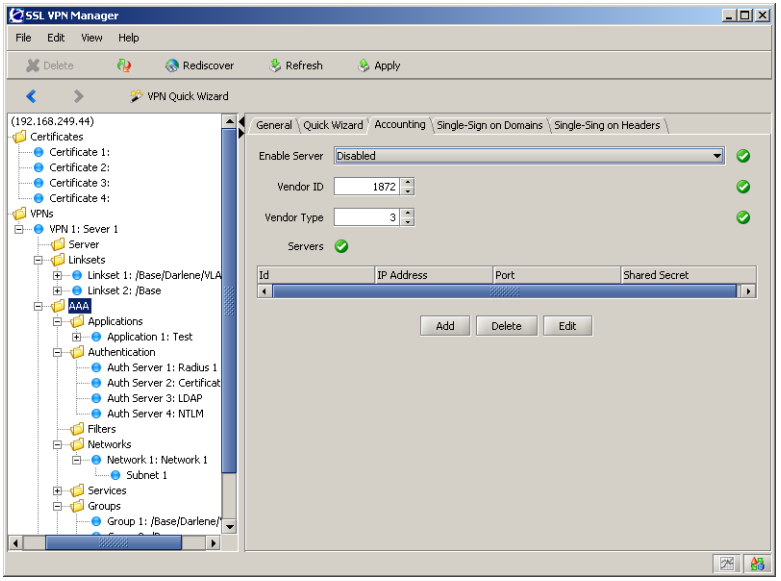
Accounting

Accounting allows you to add one or more RADIUS accounting servers to the current configuration. With a RADIUS accounting server configured (Figure 84), an accounting request start packet is automatically sent to the accounting server for each user who successfully authenticates to the SSL VPN. The start packet contains the following information:

- Client user name
- SSL VON IP address
- SessionID

When a user session terminates, an accounting stop packet request is sent to the accounting server that contains the session ID, session time, and cause of termination.

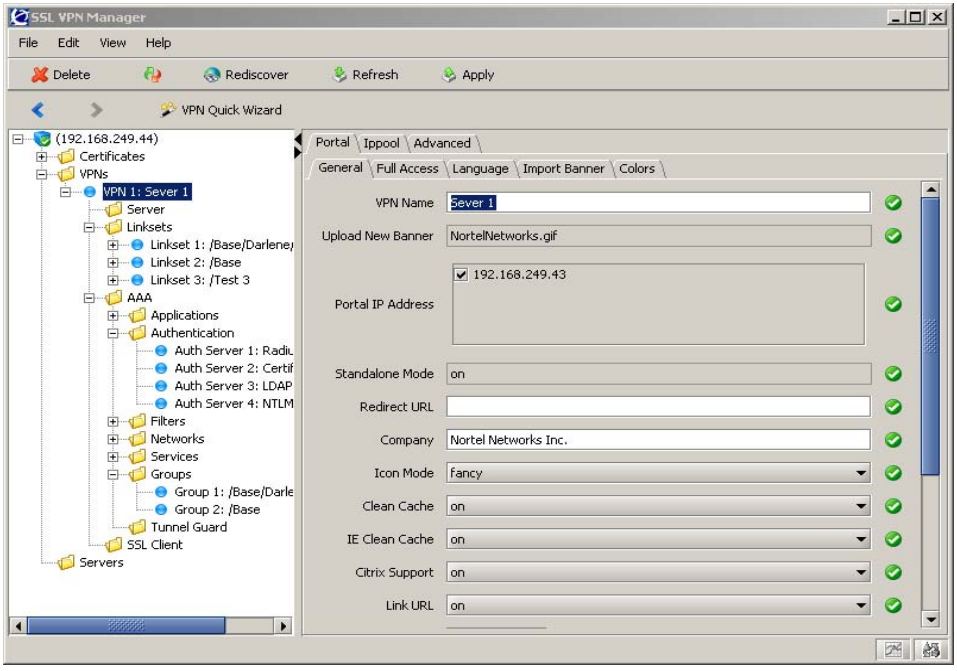
Figure 84 Accounting window



Customizing the VPN portal appearance

Select the VPNs > VPN <*name* > > General tab (Figure 85) to customize the portal appearance that is applied to the selected VPN.

Figure 85 Customize portal



TunnelGuard

For SSL connections, the TunnelGuard applet is downloaded to the client machine and started as soon as the user successfully logs in to the Portal as in an established an SSL session.

For IPsec connections, the TunnelGuard application is activated when the remote user logs in to the SSL VPN device directly from their Contivity VPN client and not through the Portal.

While using SSL access, if the user decides to go into Full Access mode, the IPsec tunnel is launched and TunnelGuard protects the IPsec session.

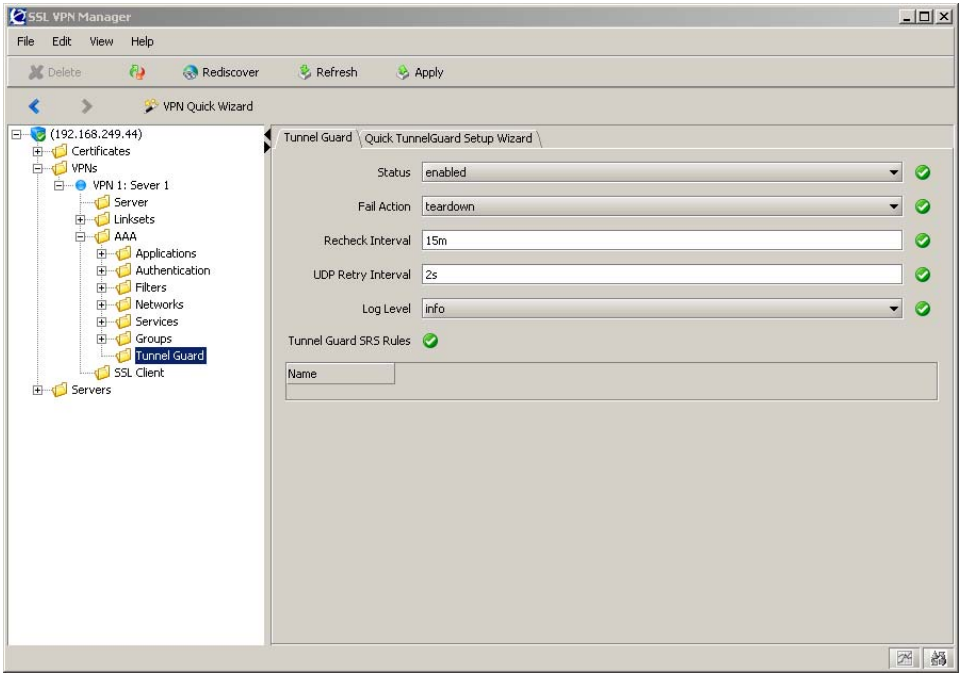
Note: TunnelGuard rules must be configured by the TunnelGuard applet. To configure TunnelGuard rules, refer to *Configuring Tunnel Guard for the Contivity Secure IP Services Gateway* (317017-B).

Configuring TunnelGuard

To configure TunnelGuard for the VPN:

1 Select VPNs > VPN <*name*> > AAA > TunnelGuard. The TunnelGuard tab appears (Figure 86).

Figure 86 TunnelGuard



2 Select enabled from the Status drop-down list

In the Fail Action list box, set the desired fail action. By setting the action to teardown, the tunnel is torn down if the TunnelGuard checks fail. By setting the action to restricted, the remote user can be given limited access if the TunnelGuard checks fail.

3 In the Recheck Interval field, set the desired time interval for SRS rule rechecks.

This step sets the time interval for SRS rule rechecks made by TunnelGuard on the client machine. If a recheck fails, the tunnel or session is terminated. This can happen if the required file is no longer present or the required process is no longer running. Depending on the access method, the remote user can be kicked out from the Portal or have the IPsec tunnel torn down.

The default recheck interval is 900 seconds = 15 minutes.

4 In the UDP Retry Interval field, specify the interval between connection attempts.

This step lets you specify the interval between connection attempts from the TunnelGuard server (on the SSL VPN device) to the TunnelGuard client (on the client machine). This setting only applies to clients with the TunnelGuard application installed, not TunnelGuard applets downloaded from the Portal.

The default value is 2 seconds.

5 Click Apply.

Applying a TunnelGuard SRS Rule to a group

To apply a SRS Rule to a selected group:

1 Select VPNs > VPN <*name*> > AAA > Groups > Click the plus sign (+) to expand the Groups tree and select a group.

2 Select a TunnelGuard SRS Rule from the drop-down list to apply to the group.

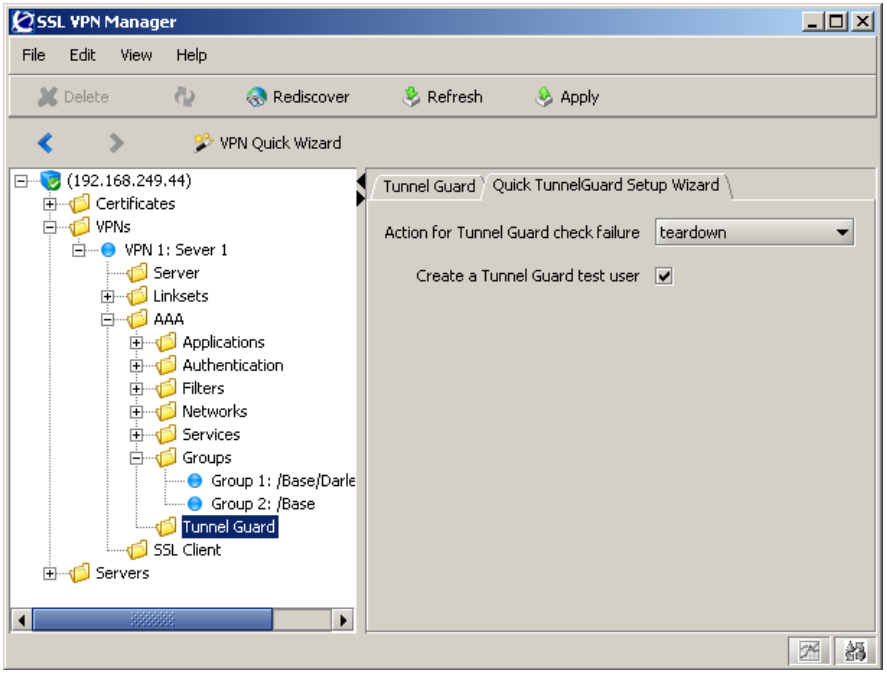
3 Click Apply.

Configuring TunnelGuard with the TunnelGuard Quick Wizard

To configure TunnelGuard with the TunnelGuard Quick wizard:

1 Select VPNs > VPN <*name*> > AAA > TunnelGuard > TunnelGuard Quick Wizard tab (Figure 87).

Figure 87 TunnelGuard Quick Wizard



2 Choose one of the following modes from the drop-down list:

   a Restricted as fail action. The tunnel is not torn down even if the TunnelGuard checks fail. The result is displayed on the Portal page.

   b Teardown as fail action. The remote user will not get past the login page. A message is displayed telling the user that the TunnelGuard checks have failed.

3 Select the Create a TunnelGuard test user check box.

4 Click Apply.

Chapter 5
Configuring HTTP, Generic, and SOCKS servers

This chapter describes information that you need to configure the following servers, including:

- Configuring HTTP and Generic servers
- SOCKS servers
- HTTP to HTTPs redirect
- URL/Rewrite White list
- Load balancing for back end servers

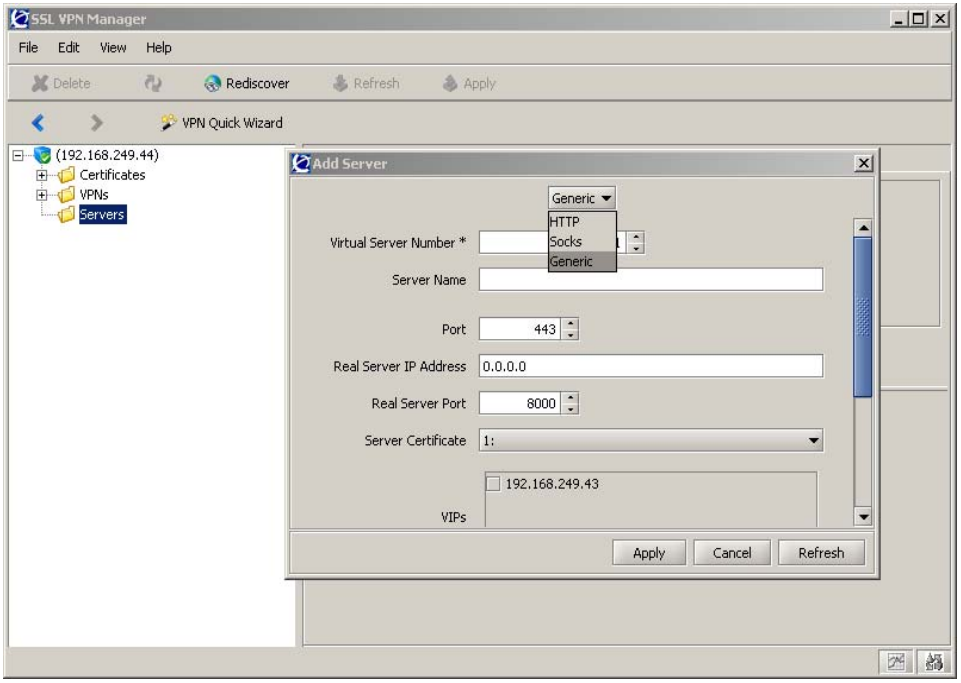
Configuring HTTP and Generic servers

You can configure the SSL VPN for Generic and HTTP servers. Generic and HTTP servers are used for SSL acceleration and load balancing.

To create and configure a virtual server of the generic/HTTP type:

1 Select Servers and click Add. The Add Server window appears (Figure 88 on page 162).

Figure 88 Add Server



2 Select Generic or HTTP option from the drop-down list.

3 Select an unique virtual server identifier from the Virtual Server Number drop down list.

4 Enter a Server name and select a Port number.

5 Enter a Real Server IP address and Real Server Port number.

6 Select the Server Certificate to be used by the server.

7 For a HTTP type server, select the VPN number. This setting does not apply to a Generic type server.

8 Select the VIP that is associated with this VPN.

9 Select a Certificate Verification Level.

10 Select one or more certificates from the CA Certificate list.

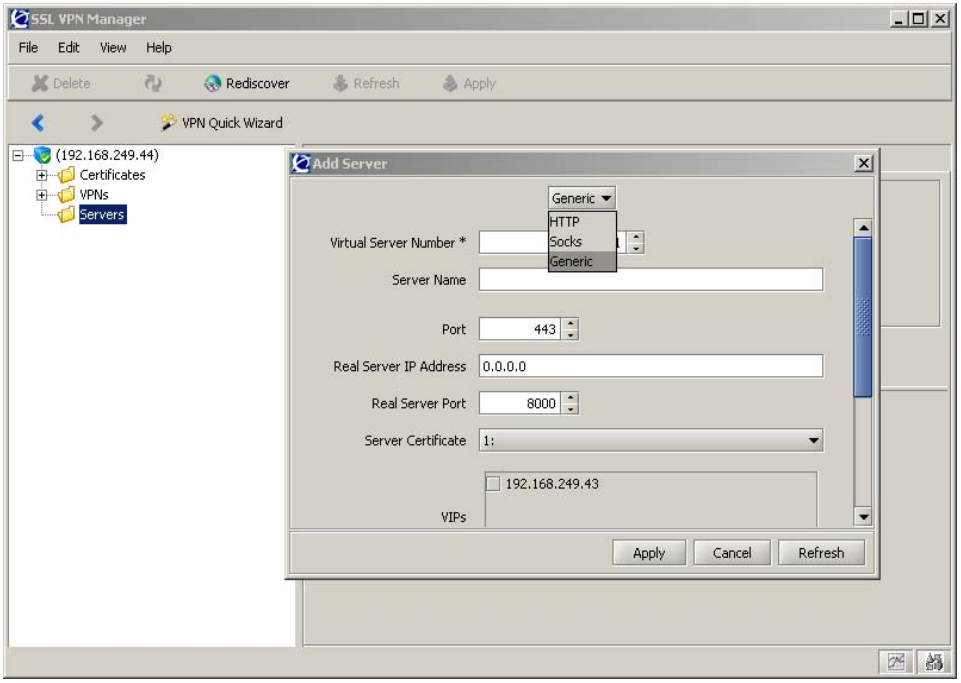
11 Apply the changes.

Configuring SOCKS servers

To create and configure a virtual server of the SOCKS type:

1 Select Servers and click Add. The Add Server window appears (Figure 88).

Figure 89 Add Server



2 Select SOCKS option from the drop-down list.

3 Select an unique virtual server identifier from the Virtual Server Number drop down list.

4 Enter a Server name and select a Port number.

5 Select the Server Certificate to be used by the server.

6 Select the VPN number.

7 Select the VIP that is associated with this VPN.

8 Select a Certificate Verification Level.

9 Select one or more certificates from the CA Certificate list.

10 Apply the changes.

Configuring HTTP to HTTPs redirect

You can configure the Contivity Secure IP Services Gateway to automatically transform an HTTP client request into the required HTTPS request. By configuring a redirect service on the Contivity gateway, the user can simply enter the fully-qualified VPN name in the Web browser address field, without having to specify the protocol required to establish a secure connection.

You configure the redirect service by adding an additional virtual HTTP server. When the virtual HTTP server on the Contivity gateway receives a request, it redirects the browser to the virtual HTTPS server by sending an HTTP location header to the browser.

The following configuration procedure assumes that you have already set up a working HTTPS server for the portal.

To configure the redirect service:

1 Log in as the administrator to the Contivity gateway and launch the SSL VPN Manager from the Services > SSL VPN screen.

2 To create a new virtual HTTP server on the Contivity gateway, go to Servers > Add > select HTTP from the drop-down list.

3 Define a name for the virtual HTTP server. The name you specify is intended for your own reference and is not critical for the configuration itself. The name can indicate the service for which the virtual server is created.

4 Set the port for the HTTP server. Each time you create a new virtual server, the listen port is automatically set to 443. For the HTTP to HTTPS redirect service, the virtual HTTP server must be set to listen to port 80 (the default port used for HTTP).

5 Disable SSL for the virtual HTTP server.

6 Create a back end server and set the IP address and port. The back end server will be the virtual HTTPS server to which the browser should be redirected.

7 Define the back end server as remote and specify the host name. The host name is used in the redirect message sent to the client Web browser.

8 Define the remote server as an SSL server. The back end server defined as remote uses SSL. This makes the generated redirect an HTTPS redirect even though the local server is defined as an HTTP server.

9 Enable load balancing and disable health checks. Because the redirect is done to an SSL server on the Contivity gateway itself, health checking is not needed. Also, health checking may prevent the redirect service from functioning because of filter configuration on the application switch.

10 Apply the changes.

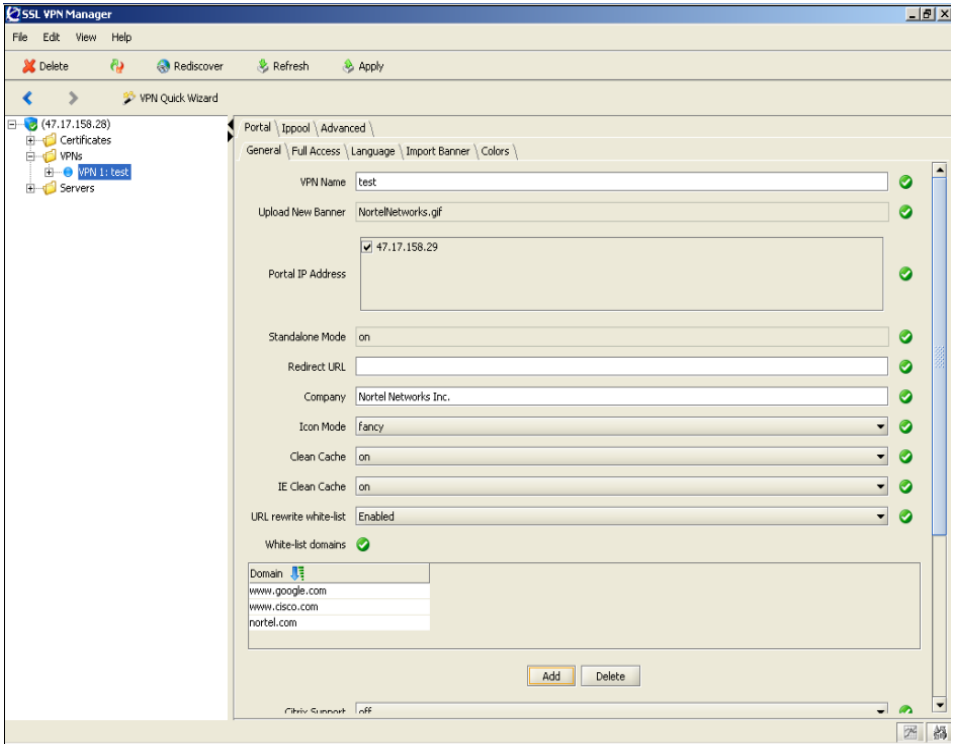
URL Rewrite White-list

Internal Web sites can have links to Web servers that are external to the private network. An example is a company intranet home page that has links to a weather or news web site. If you want SSL portal users to connect directly to the external Web sites without going through the SSL tunnel, enable URL Rewrite White-list.

To add or delete URLs from the URL rewrite white list:

1 Select VPNs > VPN <*name*>> Portal tab > General tab. (Figure 90 on page 166)

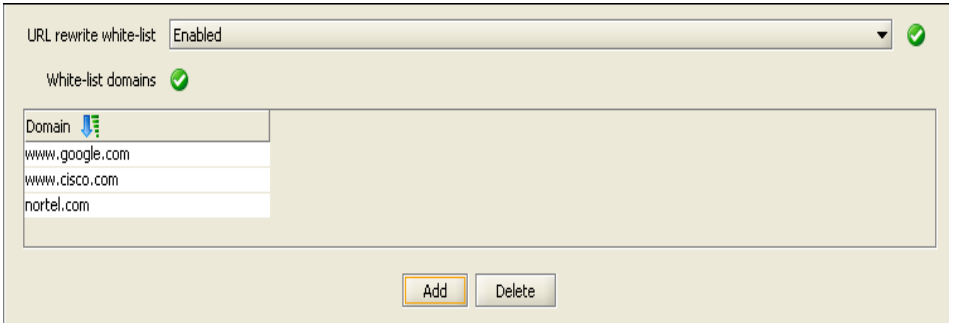
Figure 90 Portal tab with white list enabled



2 Enable the URL Rewrite White-list.

3 Click Add. The White-list domains window opens (Figure 91).

Figure 91 White-list domains window



4 Enter the URL for the site you want to add to the rewrite white list.

5 Click Add to confirm your entry and save the URL to the rewrite list.

You can add the full VPN name, such as us.nortel.com, or part of the name, such as nortel.com. In the nortel.com example, all links that end in nortel.com are treated as internal.

Note: To remove a URL from the rewrite white list, select the domain name and click Delete. SSL VPN Manager removes the domain name from the list.

Configuring load balancing for back end servers

The SSL VPN device can load balance both encrypted and unencrypted back end server connections. All connections must be terminated on the SSL VIP, and then a connection must be established between the SSL VPN device and the back end server. A virtual SSL server must be configured on the SSL VPN device prior to configuring server load balancing.

To configure load balancing:

1. Create a virtual SSL server, through which load balancing is performed. Generic and HTTP servers support load balancing.
2. In the SSL VPN Manager, go to Servers > click Add.

   Ensure that this is of type HTTP or Generic, and set up a port for it to listen on; in this example port 443 (HTTPS).

   a. Define each back end server by specifying IP address and TCP port. The virtual SSL server will initiate requests to the specified IP address and TCP port of the back end server. In this configuration example, the TCP port is set to 80 (HTTP).

   b. In the SSL VPN Manager, click on the new server and in the right pane, click on the “Load Balancing” tab.

   c. Click on “Add back end Server” and add all servers which require load balancing.
3. To enable load balancing and verify the configuration in SSL VPN Manager, go to the new server and click on the General tab. Change the status to Enabled.

4 Apply your changes.

Metrics are used for selecting which back end server, configured within the realm of a virtual SSL server, will receive the next client connection. The available metrics are hash, round-robin (round robin), and leastconn (least connections). The default metric is hash.

A mathematical hash on the client source IP is used when selecting a back end server. All requests from a specific client will be sent to the same back end server, provided the health check mechanism declares the back end server as up during the complete session. Persistency in client connections is therefore inherent in the hash load balancing metric. However, hash is not recommended when many clients share the same source IP address (such as proxied clients), because all clients are directed to the same back end server without the benefit of load balancing the traffic across the available back end servers.

With the round-robin metric, new client connections are issued to each available back end server in turn. The first back end server gets the first connection, the second back end server gets the next connection, followed by the third back end server, and so on. When all configured back end servers have received at least one connection, the issuing process starts over with the first back end server. The round-robin metric can be combined with persistency based on cookies or information in the SSL session.

With the least connection metric, the number of connections currently open on each back end server is measured in real time. The back end server with the fewest connections is considered to be the best choice for the next incoming client connection request. This option is the most self-regulating, with the fastest servers typically getting the most connections over time. The leastconn metric can be combined with persistency based on cookies or information in the SSL session.

Appendix A
Configuration examples

All configuration examples require that you have logged in to the Contivity gateway as the Administrator user and have launched the SSL VPN Manager applet from the Services > SSL VPN window.

Portal links examples

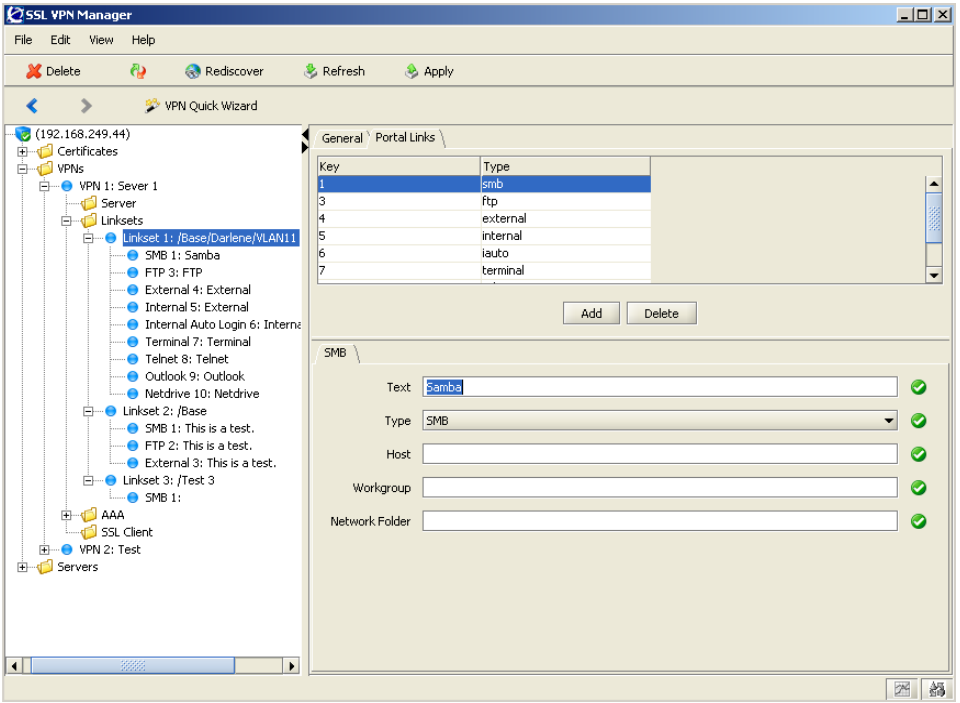
To create a new link (as in the configuration examples that follow), specify a link ID number not currently in use by the system. To edit the properties of an existing link, select the corresponding link ID number.

Linking to Samba (SMB) file server

This example shows how to create a direct link to the home share folder of the currently logged-on user. This link type should be used for SMB (Windows file share) file servers.

1. From VPNs > VPN <*name*> > Linksets, select the group whose members will have access to the Samba link.
2. Select the Portal Links tab and click Add.
3. Select a Key number.
4. Enter the link text to appear on the portal's Home tab in the Text box.
5. Select SMB from the Type drop-down list.
6. Click Apply. The Samba link window appears (Figure 92 on page 170).

Figure 92 Samba file server link



7 Specify file server host. You can enter the file server host as an IP address or a host name.

8 Specify a workgroup (optional). If needed, you can specify a Windows workgroup.

9 Specify a shared network folder. You can create a link to the currently logged-in user's home share folder by including the `<user>` macro. The macro expands to the remote user's user name as provided on the portal login screen.

To provide access to a folder or file on a lower level in the file structure, simply add a forward slash (/) and the folder or file name; for example, `home share/<user>/manuals/drafts/user guide.pdf`. Folder/file names are not case sensitive. Spaces can be used in folder and file names.

10 View the resulting HREF and link text by logging in to the portal.

Linking to FTP file server

This example shows how to create a direct link to an FTP file server.

1 From VPNs > VPN <*name*> > Linksets, select the group whose members will have access to the FTP link.

2 Select the Portal Links tab and click Add.

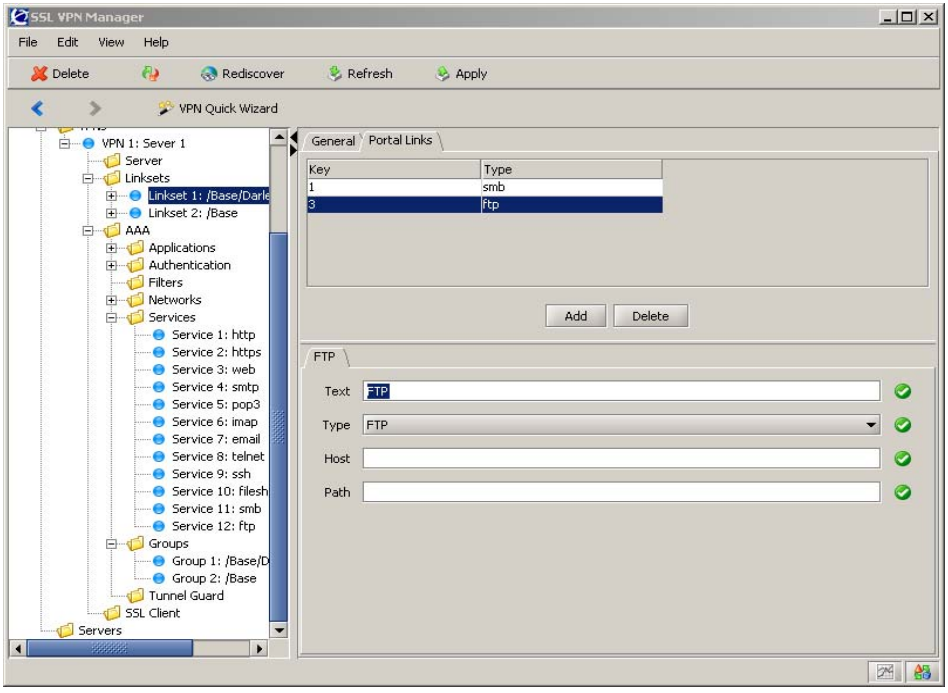
3 Select a Key number.

4 Enter the link text to appear on the portal's Home tab in the Text box.

5 Select FTP from the Type drop-down list.

6 Click Apply. The FTP link window appears (Figure 93).

Figure 93 FTP file server link



7 Specify the file server host. The file server host can be entered as an IP address or a host name.

8 Specify the path to be used when the user clicks a link.

By specifying an initial path, a specific directory can be listed right away when the user clicks the link. In this example, the initial path / ! is specified. For FTP servers, this translates into the currently logged-in user's home directory.

As with the SMB link, macros can also be used. To provide access to a folder or file on a lower level in the file structure, the initial path syntax could be as follows: /home/share/<*user*>/manuals/drafts/user guide.pdf. Folder and file names are case sensitive for FTP file servers. However, spaces can be used in folder and file names.

9 View the results and link text by logging in to the portal.

Creating a direct link to a Web page

This example shows how to create a link to a Web page. As opposed to the internal link, the external link directs the HTTP request straight to the specified resource, without adding the Contivity gateway rewrite prefix.

1 From VPNs > VPN <*name*> > Linksets, select the group whose members will have access to the external link.

2 Select the Portal Links tab and click Add.

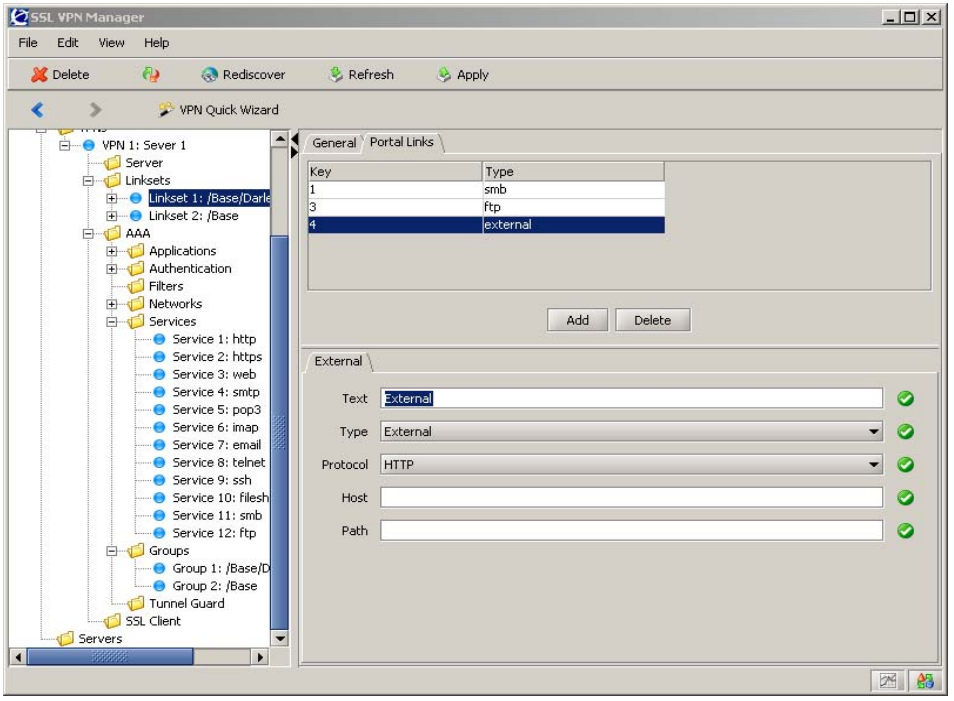
3 Select a Key number.

4 Enter the link text to appear on the portal's Home tab in the Text box.

5 Select External from the Type drop-down list.

1 Click Apply. The external link window appears. (Figure 94 on page 173)

Figure 94 External Web link



2 Specify the access protocol method.

3 Specify the fully qualified VPN name for the host.

4 Specify the path. A path must always be specified. When a forward slash (/) is specified as the path, the document root of the Web server is implied.

5 View the results and link text by logging in to the portal.

Creating secured links to Web pages

This example shows how to create a secure link to an internal Web page on your intranet. The internal link directs the HTTP request to the Contivity Secure IP Services Gateway, where the rewrite prefix (boldface) is added to the link. Example:

`https://vip.example.com``/http/inside.example.com/`

1 From VPNs > VPN <*name*> > Linksets, select the group whose members will have access to the Web page link.

2 Select Portal Links tab and click Add.

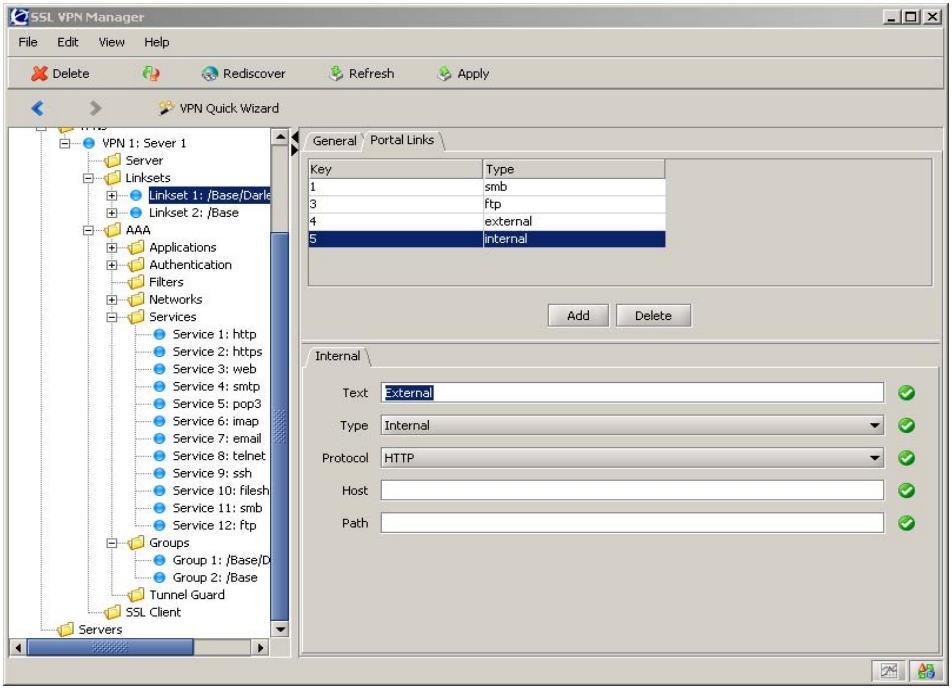
3 Select a Key number.

4 Define the link text to appear on the Portal Links window.

5 Select Internal from the Type drop-down list.

6 Click Apply. The Secured Link window appears as shown in Figure 95.

Figure 95 Secured Web link



7 Specify the access protocol method.

8 Specify the fully qualified VPN name for the host.

9 Specify the path. A path must always be specified. When a forward slash (/) is specified as the path, the document root of the Web server is implied.

To create a link to the currently logged-in user's home page (if any) on the intranet, you can use the `<user>` macro as an element in the specified path: Example: `/~<user>`

10 View the results and link text by logging in to the portal.

Using internal auto login link

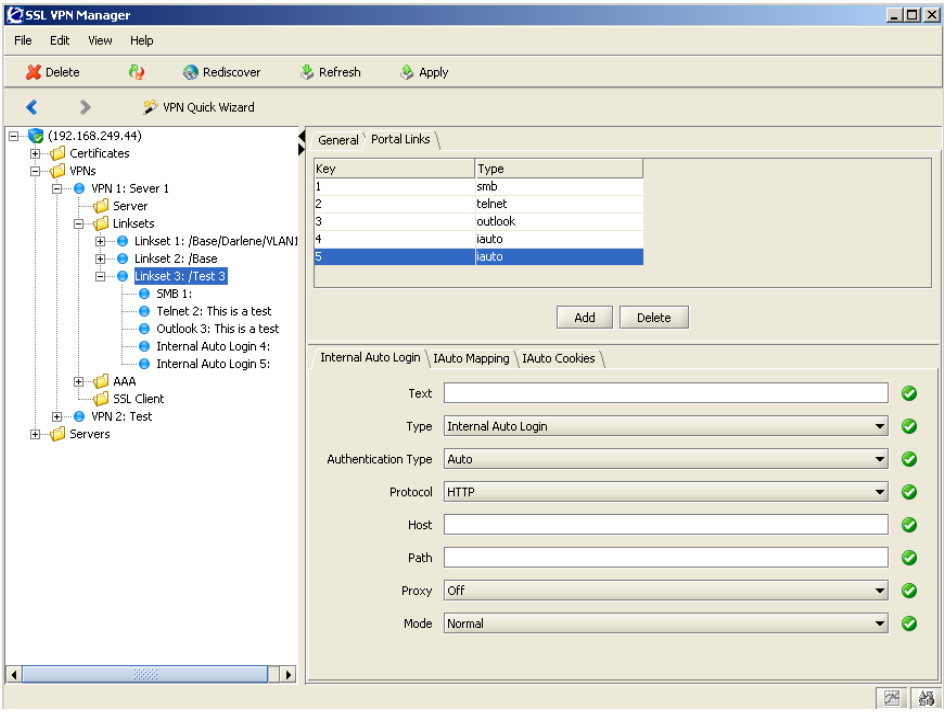
This example shows how to use the Internal Auto Login link type to create an automatic login link to a password-protected Web page. The HTTP request is directed to the Contivity gateway, where the rewrite prefix (boldface) is added to the link.

`Example: https://vip.example.com/https/inside.example.com/`

The `internal auto login` link supports form-based authentication as well as HTTP-based authentication, such as NTLM or basic (www-authenticate). The Contivity gateway automatically retrieves the URL to analyze which type of authentication method it uses.

1. From VPNs > VPN <*name*> > Linksets, select the group whose members will have access to the Internal Auto Login link.
2. Select the Portal Link tab and click Add.
3. Select a Key number.
4. Enter the link text to appear on the Portal Links window,
5. Select Internal Auto Login from the Type drop-down list.
6. Click Apply. A window opens asking for the URL for the IAuto Link.
7. Specify the login URL to the password-protected Web page.
8. Click OK. The Internal Auto link window appears as shown in Figure 96 on page 176.

Figure 96 Internal auto login link



9 Select an authentication type.

10 Select a protocol.

11 Enter the host name.

12 Enter the path.

13 Select On or Off for Proxy.

14 Select Normal or Add Domain for Mode.

Linking to terminal servers

This example shows how to create a link to a terminal server using Telnet or SSH. When the remote user clicks the link, a terminal window is opened in a new browser window by way of a Telnet/SSH terminal Java applet.

1 From VPNs > VPN <*name*> > Linksets, select the group whose members will have access to the terminal server.

2 Select the Portal Links tab and click Add.

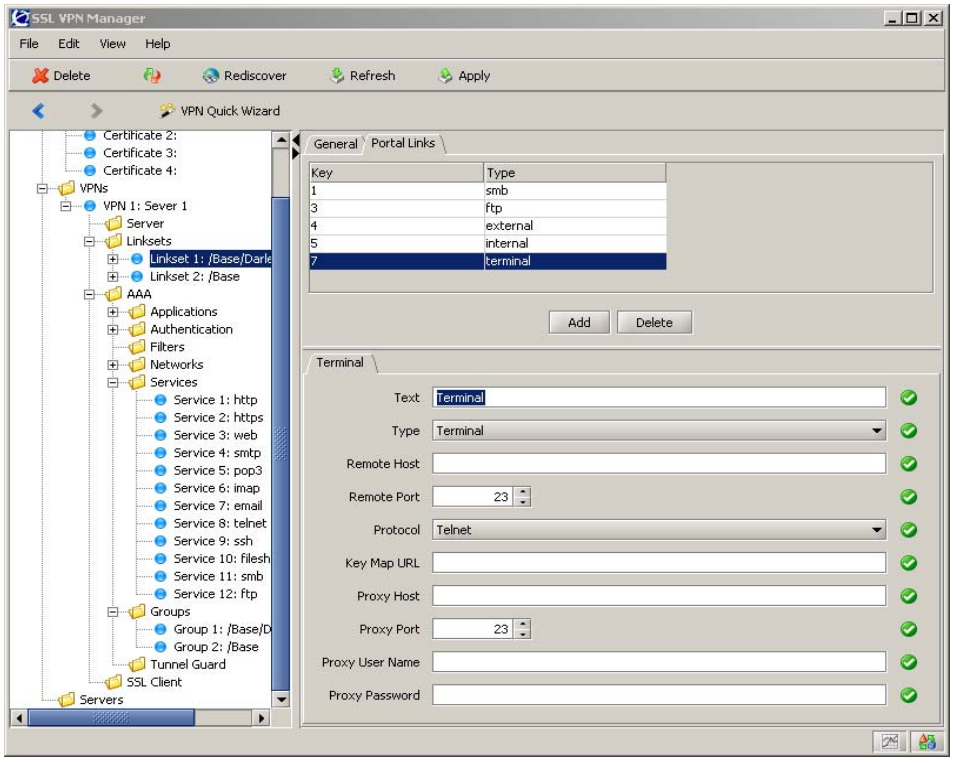
3 Select a Type number

4 Define the link text to appear on the Portal Links window.

5 Select Terminal from the Type drop-down list.

6 Click Apply. The Terminal Link window appears as shown in (Figure 97 on page 177).

Figure 97 Terminal link



7 Specify the remote host, the remote port, and the terminal access protocol.

Enter the IP address or host name of the Telnet or SSH server. TCP port 23 is the default port used for Telnet. If you want to use SSH, specify TCP port 22 as the remote port.

8 If a keymap URL is specified, the user's keyboard mappings can be configured via an external configuration file located on the specified Web server.

This feature is designed for users with non-standard keyboards. Example: When prompted for a keymap URL, enter the URL, path (if any) and finally the name of the keyboard mapping file; for example, http://inside.example.com/keyCodes.at386.

9 Enter the address and port of an intermediate HTTP Proxy server (if any).

If users are working from a location requiring traffic to pass through an intermediate HTTP Proxy server on the intranet, enter the IP address (or VPN name) and port of that proxy server. All applet traffic will thus be tunneled to the Contivity Secure IP Services Gateway via the HTTP proxy server. The HTTP Proxy server should have CONNECT support.

Skipping the prompts means that all applet traffic is tunneled directly to the Contivity gateway.

10 If an intermediate HTTP Proxy server is specified, enter the credentials to access this server (if required).

This step is not displayed if the previous step was skipped.

11 View the results and link text by logging in to the portal.

Using Telnet port forwarder link

Generally, only graphical applications (applications that open their own windows) can be started using the Port forwarder link. This example describes a work around where the Command window (cmd.exe) is opened to run the Telnet session.

1 From VPNs > VPN <*name*> > Linksets, select the group whose members will have access to the link.

2 Select the Portal Links tab and click Add.

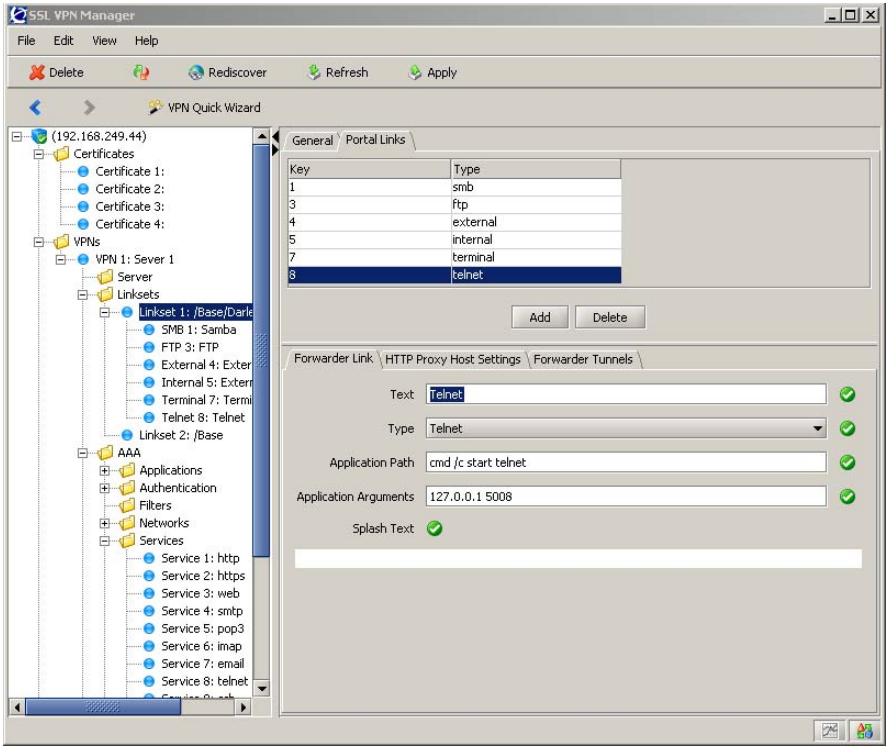
3 Select a Key number.

4 Define the link text to appear on the Portal Links window.

5 Select Telnet from the Type drop-down list.

6 Click Apply. The Telnet Link window appears as shown in Figure 98 on page 179.

Figure 98 Telnet port forwarder link



7 Specify source IP and port, host alias (if desired), destination host and port, application to be started, arguments, custom Java applet text (optional), HTTP proxy server (if any) and compact URL (yes or no).

8 Apply the changes.

Creating Outlook port forwarder link

This example shows how to create a Port forwarder link to a Microsoft Exchange server on the intranet, enabling secure transfer of mail messages, calendar, address and book entries.

For the Outlook Port forwarder to work, the following prerequisites must be fulfilled:

- The Exchange server's VPN name suffix must be configured in the DNS Search List on the Servers > ID# Server Name > DNS tab.

- The user must have administrator's rights on his/her computer *or* have write access enabled for the hosts and lmhosts files. Hosts and lmhosts files are located in `%windir%\hosts` on Windows 98 and ME and in `%windir%\system32\drivers\etc\hosts` on NT, XP and Windows 2000.
- The user's client machine must be of the Hybrid or Unknown node type. The node type can be checked by entering ipconfig /all at the DOS prompt.

  To change the node type to Hybrid (if needed), go to the registry editor folder: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters.
  If it is not already present, add a new DWORD Value called NodeType.
  Double-click on NodeType and enter 8 in the Value Data field.
  Click on OK and restart the computer.
- The Outlook Port forwarder link is meant to be used by clients connecting to the Contivity Secure IP Services Gateway from outside the intranet. If the client has direct connectivity to the intranet, the Port forwarder will fail. If the client has access to intranet DNS servers, communication will fail as well.
- To test DNS resolution, the Contivity Secure IP Services Gateway should be able to ping the Exchange server using the fully qualified name (FQDN).
- The user's Outlook account must be hosted on the Exchange server(s) specified in the Port forwarder.

The Outlook Port forwarder link will not work if a proxy server is configured in the client browser. This also means that an HTTP Proxy link or HTTP Proxy portal session cannot be active at the same time as the Outlook Port forwarder.

If you expect the connection to include more than 15 minutes of inactivity, increase the TCP connection idle time-out value using the VPNs > VPN <*name*> > Server > TCP tab.

To ensure proper operation, specify the DNS name of the portal server.

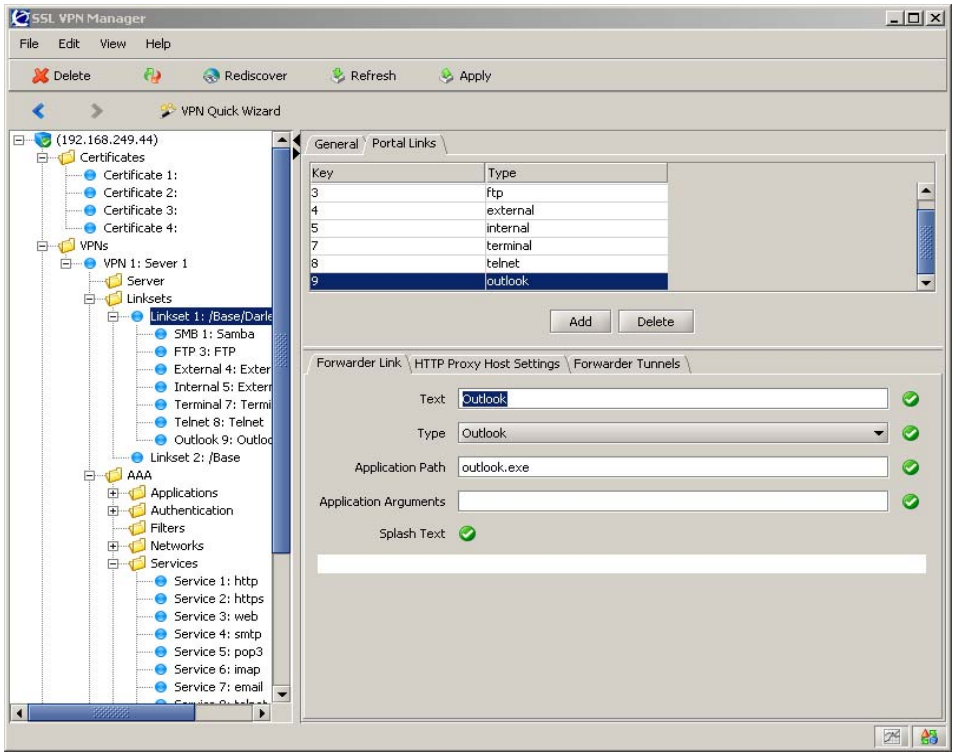
If a firewall exists between the Contivity Secure IP Services Gateway and the Exchange server, the firewall settings must allow traffic to the required Exchange server ports. Note that these may vary with your environment. More information can be found on http://support.microsoft.com,; for example, Knowledge Base Articles 280132, 270836, 155831, 176466, 148732, 155831, 298369, 194952, 256976, 302914, 180795 and 176466.

When a user clicks an embedded link in an e-mail message, the Web site associated with the link must be displayed in a new instance of Internet Explorer. In Internet Explorer, go to the Tools menu and select Internet Options. Under the Advanced tab, go to Browsing and deselect the “Reuse windows for launching shortcuts” option.

To create an Outlook port forwarder link to be displayed on the Portal:

1. From VPNs > VPN <*name*> > Linksets, select the group whose members will have access to the link.
2. Select the Portal Links tab and click Add.
3. Select a Key number
4. Define the link text to appear on the Portal Links window.
5. Select Outlook from the Type drop-down list.
6. Click Apply. The Outlook Link window appears as shown in Figure 99 on page 182.

Figure 99 Outlook port forwarder link



7 Define the link text to appear on the Portal's Home tab.

8 Enter the Forwarder menu to select the `Outlook` option.

9 Specify the desired source IP and the FQDN of the Exchange server.

The source IP address should be set to 127.0.0.1 or any other IP address in the 127.x.y.z range. The Exchange server address must be entered as a fully qualified domain name (FQDN) and not as an IP address.

The services provided by the Exchange server (such as mail, calendar, and address book) may be distributed between different Exchange servers. If this is the case, you have the option to create several Outlook port forwarders where the relevant Exchange servers can be specified.

If several port forwarders are required, note that each port forwarder must have a unique source IP address. A new source IP address is automatically suggested by the system if you choose to add another port forwarder.

10 Specify whether or not the Outlook client is started automatically when the user clicks the link.

If you choose not to start the Outlook client, you can start the application manually, after clicking the Port forwarder link and downloading the Java applet. Custom user instructions can be provided in the Java applet window.

11 If desired, enter arguments to the Outlook client.

An example of an argument would be /Profile myprofile.

12 Enter a custom text (for example, with user instructions) to be displayed in the Java applet window (optional).

13 If more than 25 port forwarders are included in one Outlook Port forwarder link, set Compress URL to `yes` to compress the URL; otherwise accept the default value `no`.

14 Configure the Exchange servers' VPN name suffixes as DNS search entries for the portal server.

This step is necessary for the Outlook Port forwarder to work. Using the Exchange servers in Step 6, enter the VPN names.

15 Apply the changes.

16 If desired, specify the URL to be opened.

URL is required if you chose to open a new browser window (see the previous step).

When you enter the URL, also specify the protocol, http or https (see example below).

17 Enter the address and port of an intermediate HTTP Proxy server (if any).

If users are working from a location requiring traffic to pass through an intermediate HTTP Proxy server on the intranet, enter the IP address (or VPN name) and port of that proxy server. All applet traffic will thus be tunneled to the Contivity Secure IP Services Gateway via the HTTP proxy server. The HTTP Proxy server should have CONNECT support.

Skipping the prompt means that all applet traffic is tunneled straight to the Contivity Secure IP Services Gateway.

18 If an intermediate HTTP Proxy server is specified, enter the credentials to access this server (if required).

19 Apply the changes.

Creating Netdrive links

You can create a portal link to Netdrive.

1 From VPNs > VPN <*name*> > Linksets, select the group whose members will have access to the Netdrive link.

2 Select the Portal Links tab and click Add.

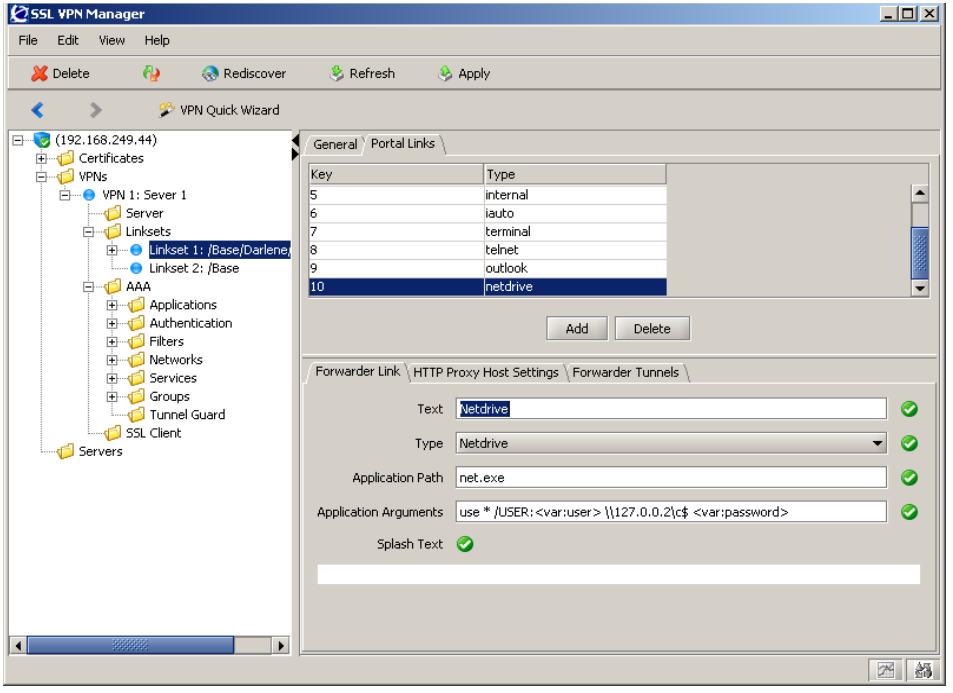
3 Select a Key number.

4 Define the link text to appear on the Portal Links window.

5 Select Netdrive from the Type drop-down list.

6 Click Apply. The Netdrive Link window appears as shown in (Figure 100).

Figure 100 Example Netdrive link



7 Define the link text to appear on the Portal's Home tab.

8 Specify the executable filename, including the path. The default is: net.exe.

9 Specify any command line arguments. The default is: use * /USER:<user> \\127.0.0.2 <password>.

10 Specify source IP and port, host alias (if desired), destination host and port, application to be started, arguments, custom Java applet text (optional), HTTP proxy server (if any) and compact URL (yes or no).

11 Apply the changes.

Access rule sample configurations

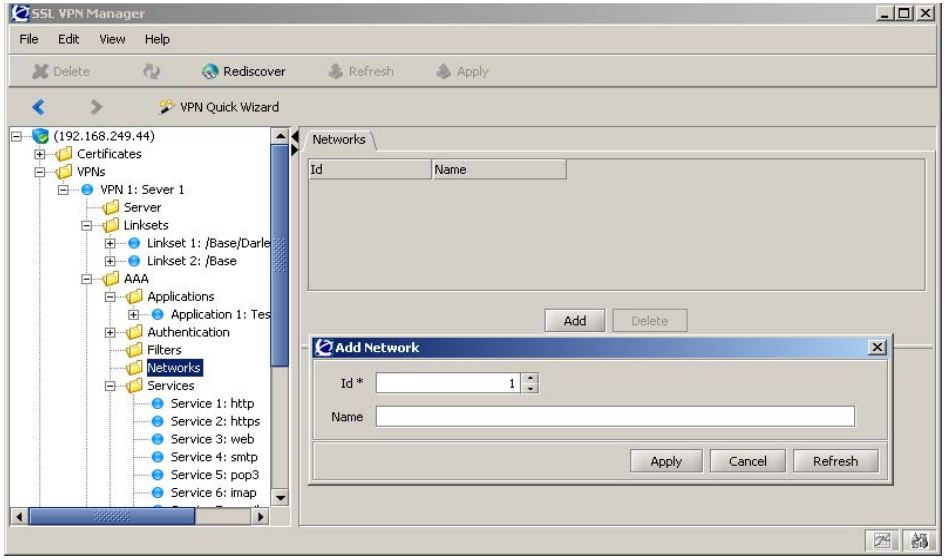
The following section provide examples of access rule configurations.

Access to Outlook Web access server

This example describes how to create a network definition identifying an Outlook Web Access server on the intranet.

1 Select VPNs > VPN <*name*> > AAA > Networks > click Add. The Add Network window opens (Figure 101 on page 186).

Figure 101 Add network



2 Select an ID for the network to be added. By default the ID starts at 1 for the first network added, the next defaults to 2, etc.

3 Specify a network name.

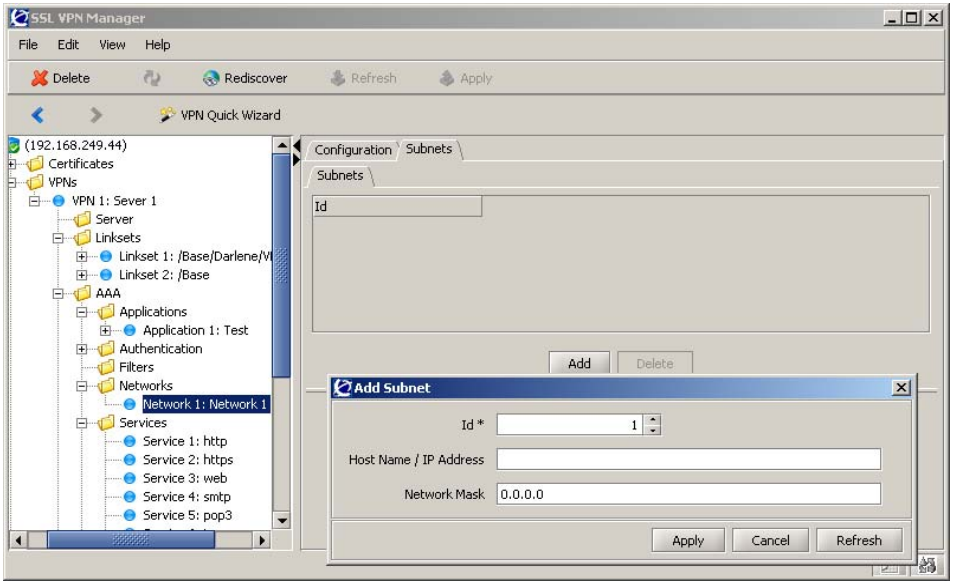
4 Click Apply. The network is added beneath Networks in the menu tree.

5 Click on the plus sign (+) to expand the Networks tree and select the network you have added.

6 Click on the Subnets tab.

7 Click Add. The Add Subnets window opens (Figure 102 on page 187).

Figure 102 Add subnet



8 The ID defaults to 1 if this is the first subnet added and it automatically increments to the next ID when you select the tab.

9 Enter the Host Name or IP address identifying the Outlook Web Access server.

10 Enter the desired Network Mask. Note that the network mask can be entered in number of bits, for example, 32 instead of 255.255.255.255.

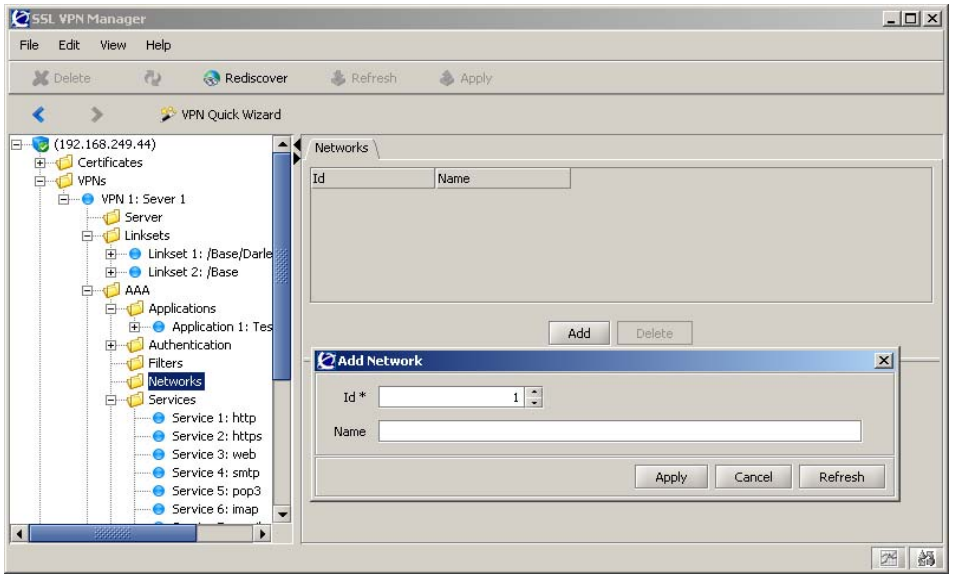
11 Click on Add. The subnet is added to the menu tree beneath the Network ID: Name it has been added to as Subnet ID.

Access to intranet Web server

This example describes how to create a network definition identifying a Web server on the intranet. The steps are the same as in the previous example, except for the network name and host IP address.

1 Select VPNs > VPN <*name*> > AAA > Networks > click Add. The Add Network window opens (Figure 103 on page 188).

Figure 103 Add network example



2 Specify a network name.

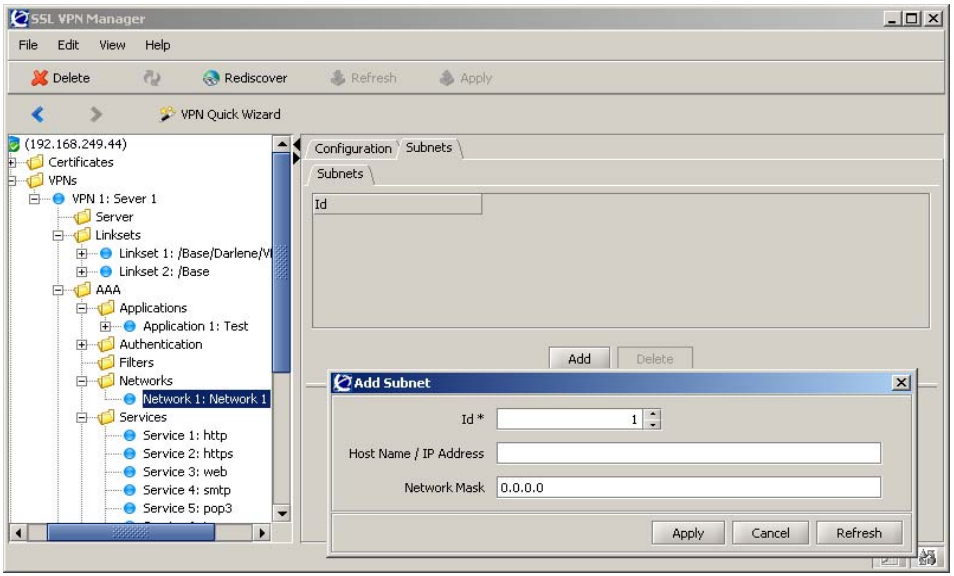
3 Click Apply.

4 Click on the plus sign (+) to expand the Networks tree and select the network you have added.

5 Click on Subnets.

6 Click Add. The Add Subnets window opens (Figure 104 on page 189).

Figure 104 Add subnet example



7 Define a subnet identifying the intranet Web server.

8 Apply the changes.

Access to intranet file server

This example describes how to create a network definition identifying an intranet file server.

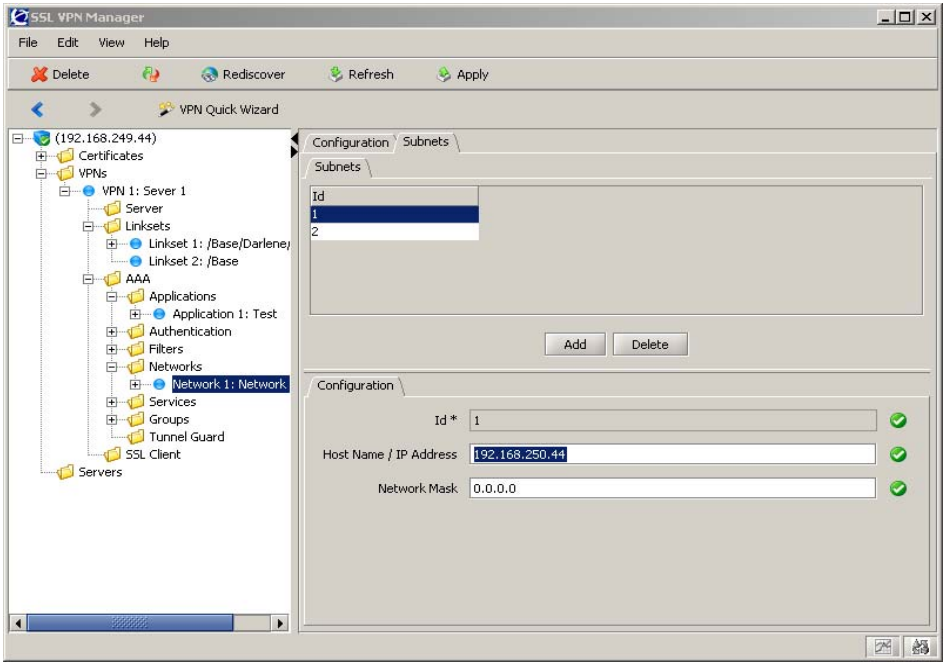
1 Select VPNs > VPN <*name*> > AAA > Networks > click Add.

2 Click on the plus sign (+) to expand the Networks tree and select the network you have added.

3 Click on Subnets.

4 Select Add.

Figure 105 Intranet file server



5 Define a subnet identifying the intranet file server.

6 Apply the changes.

Access allowed to specific subnet

This example describes how to create a network definition identifying a specific sub VPN in a company's intranet to which the group members are authorized. The sub VPN is called `sales.example.com`.

1 Select VPNs > VPN <*name*> > AAA > Networks > click Add.

2 Specify a network name.

3 Click Apply.

4 Define the subnet to include in the current network definition.

When creating a subnet, enter either the host name or the network address/ netmask. To specify all hosts within a sub VPN, you can use an asterisk (*) as a wildcard.

5 Apply the changes.

Note: It is possible to create a network definition consisting of several subnet definitions.

Access denied to specific subnet

This example describes how to create a network definition identifying a specific sub VPN in the company intranet to which the group members are unauthorized. The sub VPN is called `secret.example.com`.

1 Select VPNs > VPN <*name*> > AAA > Networks > click Add.

2 Specify a network name and click Apply.

3 Click on the plus sign (+) to expand the Networks tree and select the network you have added.

4 Click on the Subnets tab.

5 Click Add.

6 When creating a subnet, enter either the host name or the network address/ netmask. To specify all hosts within a sub VPN, you can use an asterisk (*) as a wildcard.

7 Define a subnet identifying the intranet file server.

8 Apply the changes.

Group configuration examples

The following sections describe various examples of group configurations.

Defining staff groups

In this example, a group called `staff` is created. The base profile contains a link to an Outlook Web Access server and an access rule that allows access to that OWA server. Access to the OWA server is allowed, regardless whether the user requests the server from an Internet café or from a secure network.

We will also add an extended profile to the `staff` group. The extended profile references a client filter which, in its turn, references a client network. The client network consists of a subnet identifying a secure network, for example, a branch office. When a group member connects to the SSL VPN from the branch office network over the internet, that group member should have more generous access rights.

Defining the base profile

1. Select VPNs > VPN <*name*> > AAA > Groups > click Add.
2. Click Apply to add the group.
3. Expand the Groups tree and select the new group.
4. Click on Add on the Groups tab to access the Access Rules dialog.
5. Specify the access rule pertaining to the base profile.

This step references a previously defined network definition for an Outlook Web Access (OWA) server. It consists of a subnet definition identifying an Outlook Web Access server. You are also making use of the default service definition `http`, corresponding to TCP port number 80.

Note: To create 10 default service definitions, use the VPNs > VPN <*name*>> AAA > Quick tab. If you ran the Quick Setup wizard, these service definitions have already been created.

6. Create a group link to the OWA server. The defined link is displayed on the portal's Home tab.
7. Apply the changes.

Creating network identifying branch office network

To be able to reference the client network in the client filter, you should first create the network definition identifying the branch office network.

1. Select VPNs > VPN <*name*> > AAA > Networks > click Add.
2. Specify the network name.
3. Click on Apply.

4 Expand the Networks tree and select the network just added.

5 Select the Subnets tab and click Add.

6 Define the subnets to be included in the network definition. When creating a subnet, enter either the host name or the network address/netmask. To specify all hosts within a sub VPN, you can use an asterisk (*) as a wildcard.

Defining client filter for the client network

To reference the client filter in the extended profile, you must first define the client filter.

1 Select VPNs > VPN <*name*>> AAA > Filters > click Add.

2 Specify the client filter's name and reference the previously created network.

3 Click Apply to add the Filter.

Defining extended profiles

Now it is time to define the extended profile. The extended profile is triggered when the group member accesses the portal from the network referenced in the extended profile's client filter.

Because the user is connecting from a secure network, more generous access rules can be presented to the user.

1 Select the group for you which you want to define an extended profile from the Groups menu tree.

2 Select the Extended Profiles tab and click Add.

3 Define the extended profile and reference the previously created client filter.

4 Define and add an Access rule that allows access to all networks and protocols.

Note: Leaving an extended profile without access rules is not the same as denying all traffic. If no access rule at all is specified for the extended profile, the base profile's access rules is applied.

5 Select the Extended Profiles tab.

6 Select the extended profile.

7 At the bottom of the screen, click on Portal Links and add Portal link.

8 Select the FTP tab and create a group link to an FTP file server on the intranet.

9 This link is displayed on the portal's Home tab. The link defined for the base profile is appended to this link, for example, both links are displayed for group members accessing the portal from the branch office network.

10 Apply the changes.

Results

Bill is a member of the `staff` group. This is what will happen, depending on how Bill accesses the portal:

- **From an Internet café:** The extended profile is not triggered because the client filter referenced in the extended profile points to the branch office network, not the Internet café's network. Only the link defined for the base profile, for example, directly under the Group menu, is displayed on the portal's Home tab. If Bill tries to access the Outlook Web Access server, either by clicking the link or by using the Browse Intranet tab, access is allowed. A match is found between the requested resource and the network referenced in Access rule 1. If Bill tries to request any other resource, no match is found in the access rule and access is denied.
- **From the branch office network**: The extended profile is triggered. This is because a match is found between Bill's source network and the client network referenced in the extended profile's client filter. Both links are displayed because the base profile's links are always appended to those of the extended profile. The access rule defined for the extended profile is applied, which means Bill is granted access to all hosts and protocols on the intranet and the internet. The base profile's access rule is appended, but has no real effect in this example.

Defining engineering groups

In this example, a group called `engineer` is created. The base profile contains a link to an intranet Web server and an access rule that allows access to all hosts in the `sales.example.com` sub VPN.

Members of the engineer group exist in the Contivity Secure IP Services Gateway's local database as well as in a RADIUS authentication server's database. Thus, group members can authenticate to the portal using local database authentication or RADIUS authentication. The latter is used for token login and is considered more secure.

For users logging in to the portal using local database authentication, only the base profile's links and access rules are applied. The Advanced tab is not visible on the portal. For users logging in to the portal using RADIUS authentication, links and access rules defined for the extended profile are applied. The extended profile contains an extra set of links, an access rule that allows access to all hosts, and a user type displaying all of the portal's tabs.

Defining base profiles

This example describes how to configure the engineer group with the required links and access rules.

1 Define the engineer group.

   This step allows you to specify the group's name and user type. By setting the user type to medium, the Advanced tab is not visible on the Portal for the logged in group member.

2 Specify the access rules pertaining to the group's base profile.

   In this example we use the network definition we created in the example on page 190, for example, sales. To allow all services and paths (for example, application specific name), click on ENTER when prompted.

3 Create a link to the intranet Web server.

4 Specify the link type and host name.

5 Apply the changes.

Defining client filters for token login

Before you create the extended profile, define the client filter. The client filter is later referenced in the extended profile. The extended profile, in its turn, is triggered when a group member authenticates via the RADIUS server.

1 Set the client filter's name.

2 Specify which authentication server the client filter's name refers to.

3 Set the authentication server name.

   This step allows you to specify the authentication server used. Reference the authentication server by the name that was assigned to the authentication method, using the `/cfg/vpn 1/aaa/auth #/name` command.

4 Apply the changes.

This client filter is now referenced in the extended profile. The access rules specified in this profile determine the access rights for group member's authenticating by means of token authentication.

Creating extended profiles for token login

To grant members of the `engineer` group better access rights when using token login, add an extended profile to the group. The extended profile is triggered when a group member authenticates through token login, supplied by the RADIUS server. Reference the client filter we created in the example in the previous section.

1 Specify the group for which you wish to create the extended profile, then create the extended profile and reference the client filter's name.

   The base profile's user type is `medium`. To provide better access rights for users using token login, specify `advanced` as user type.

2 Specify the access rules pertaining to the extended profile.

   This step lets you specify the group member's access rights when the user authenticates through token login. The group members are granted access to hosts on all networks. All services are available.

3 Add links to the extended profile.

   Links added to the extended profile are displayed when the user authenticates through token login. Links defined for the base profile are appended to those of the extended profile.

4 Apply the changes.

Results

Lisa is a member of the `engineer` group. This is what happens, depending on how Lisa authenticates to the portal.

- Local database authentication. The extended profile is not triggered because Lisa authenticated to the portal through local database authentication. Only the base profile is used in Lisa's session. The link defined for the base profile is displayed on the portal's Home tab. If Lisa tries to access a host within the `sales.example.com` sub VPN, for example by using the Browse Intranet tab, access is allowed. A match is found between the requested resource and the network referenced in Access rule 1. If Lisa tries to request any other host, access is denied.
- **RADIUS authentication**. The extended profile is triggered because Lisa authenticated to the portal via RADIUS database authentication. Any links defined for the extended profile are displayed on the portal's Home tab. The base profile's link is also displayed because the base profile links and access rules are always appended to the extended profile. The access rule defined for the extended profile are applied, which means Lisa is granted access to all hosts and protocols on the intranet and the internet.

Note: If a match for the requested resource cannot be found in any of the access rules defined for the extended profile, the access rules of the base profile are applied in sequential order.

Extended profile for users with client certificate

The two previous examples describe how to create extended profiles for remote users connection from a secure network and through a secure authentication method.

In the same way, an extended profile is created for users with a valid client certificate installed. Because client certificate authentication is considered more secure, the extended profile provides more generous access rules.

1 Configure a group with access rules.

These access rules are configured directly under the Group level and constitutes the base profile. The access rules apply to users without a client certificate.

2 Create a new client filter.

3 Set the cert option to true.

4 Create an extended profile for users with a client certificate.

Reference the client filter you just created.

5 Specify the access rules pertaining to the extended profile.

These access rules are configured for the Extended profile and apply to users with a valid client certificate installed.

6 Apply the changes.

Extended profile for users with IE cache wiper

To ensure that sensitive information is not left in the computer's cache memory after a portal session, a user group can be configured to reject access to certain intranet resources if the remote user is not running the Internet Explorer cache wiper. On the other hand, an extended profile (with more generous access rules) can be created for those who actually run the cache wiper.

When a user logs in to the portal from a computer for the first time, the user is asked whether or not to install the IE cache wiper. The cache wiper clears the cache after a portal session.

1 Configure a group with access rules.

These access rules are configured directly under the Group level and constitute the base profile. The access rules apply to users without the cache wiper running.

2 Create a new client filter.

3 Set the iewiper option to `true`.

4 Create an extended profile for users with the IE cache wiper installed.

Reference the client filter you just created.

5 Specify the access rules pertaining to the extended profile.

These access rules are configured for the Extended profile and apply to users with the IE cache wiper running.

6 Apply the changes.

Appendix B
Supported ciphers

The Contivity gateway supports SSL version 2.0, SSL version 3.0, and TLS version 1.0. All ciphers covered in these versions of SSL are supported, except the IDEA and FORTEZZA ciphers and ciphers using DH or DSS authentication.

Table 4 Supported Ciphers

Cipher Name	SSL Protocol	Key Exchange Algorithm, Authentication	Encryption Algorithm	MAC Digest Algorithm
DHE-RSA-AES256-SHA	SSLv3	DH, RSA	AES (256)	SHA1
AES256-SHA	SSLv3	RSA, RSA	AES (256)	SHA1
EDH-RSA-DES-CBC3-SHA	SSLv3	DH, RSA	3DES (168)	SHA1
DES-CBC3-SHA	SSLv3	RSA, RSA	3DES (168)	SHA1
DES-CBC3-MD5	SSLv2	RSA, RSA	3DES (168)	MD5
DHE-RSA-AES128-SHA	SSLv3	DH, RSA	AES (128)	SHA1
AES128-SHA	SSLv3	RSA, RSA	AES (128)	SHA1
RC4-SHA	SSLv3	RSA, RSA	RC4 (128)	SHA1
RC4-MD5	SSLv3	RSA, RSA	RC4 (128)	MD5
RC2-CBC-MD5	SSLv2	RSA, RSA	RC2 (128)	MD5
RC4-MD5	SSLv2	RSA, RSA	RC4 (128)	MD5
RC4-64-MD5	SSLv2	RSA, RSA	RC4 (64)	MD5
EXP1024-RC4-SHA	SSLv3	RSA(1024), RSA	RC4 (56)	SHA1 EXPORT
EXP1024-DES-CBC-SHA	SSLv3	RSA (1024), RSA	DES (56)	SHA1 EXPORT

Table 4 Supported Ciphers

Cipher Name	SSL Protocol	Key Exchange Algorithm, Authentication	Encryption Algorithm	MAC Digest Algorithm
EXP1024-RC2-CBC-MD5	SSLv3	RSA (1024), RSA	RC2 (56)	MD5 EXPORT
EXP1024-RC4-MD5	SSLv3	RSA (1024), RSA	RC4 (56)	MD5 EXPORT
EDH-RSA-DES-CBC-SHA	SSLv3	DH, RSA	DES (56)	SHA1
DES-CBC-SHA	SSLv3	RSA, RSA	DES (56)	SHA1
DES-CBC-MD5	SSLv2	RSA, RSA	DES (56)	MD5
EXP-EDH-RSA-DES-CBC-SHA	SSLv3	DH (512), RSA	DES (40)	SHA1 EXPORT
EXP-DES-CBC-SHA	SSLv3	RSA (512), RSA	DES (40)	SHA1 EXPORT
EXP-RC2-CBC-MD5	SSLv3	RSA (512), RSA	RC2 (40)	MD5 EXPORT
EXP-RC4-MD5	SSLv3	RSA (512), RSA	RC4 (40)	MD5 EXPORT
EXP-RC2-CBC-MD5	SSLv2	RSA (512), RSA	RC2 (40)	MD5 EXPORT
EXP-RC4-MD5	SSLv2	RSA (512), RSA	RC4 (40)	MD5 EXPORT
ADH-AES256-SHA	SSLv3	DH, NONE	AES (256)	SHA1
ADH-DES-CBC3-SHA	SSLv3	DH, NONE	3DES (168)	SHA1
ADH-AES128-SHA	SSLv3	DH, NONE	AES (128)	SHA1
ADH-RC4-MD5	SSLv3	DH, None	RC4 (128)	MD5
ADH-DES-CBC-SHA	SSLv3	DH, NONE	DES (56)	SHA1
EXP-ADH-DES-CBC-SHA	SSLv3	DH (512), None	DES (40)	SHA1 EXPORT
EXP-ADH-RC4-MD5	SSLv3	DH (512), None	RC4 (40)	MD5 EXPORT

Cipher list formats

The cipher list you specify for a virtual SSL server consists of one or more cipher strings separated by colons (for example, RC4:+RSA:+ALL:!NULL:!DH:!EXPORT@STRENGTH). Lists of ciphers can be combined using a logical **and** operation (+) (for example, SHA1+DES represents all cipher suites containing the SHA1 and the DES algorithms).

In the colon-separated list, any cipher string can be preceded by the characters !, - or +. These characters serve as modifiers, with the following meanings:

- `!` permanently deletes the ciphers from the list (for example, !RSA).
- − deletes the ciphers from the list, but the ciphers can be added again by later options.
- + moves the ciphers to the end of the list. This option does not add any new ciphers; it just moves matching existing ones.
- `@STRENGTH` is placed at the end of the cipher list, and sorts the list in order of encryption algorithm key length.

The default cipher list used for all virtual SSL servers on the Contivity Secure IP Services Gateway is `ALL@STRENGTH`.

A cipher list consisting of the string `RC4:ALL:!DH` translates into a preferred list of ciphers that begins with all ciphers using RC4 as the encryption algorithm, followed by all cipher suites except the eNULL ciphers (ALL). The final `!DH` string means that all cipher suites containing the DH (Diffie-Hellman) cipher are removed from the list. (Few of the major Web browsers support these ciphers.)

Modifying a cipher list

Starting from the `RC4:ALL:!DH` cipher list, an example of a slightly modified cipher list can be: `RC4:ALL:!EXPORT:!DH`

This example will remove all EXPORT ciphers, besides the DH-related cipher suites. Removing the EXPORT ciphers means that all ciphers using either 40- or 56-bit symmetric ciphers are removed from the list. This means that browsers running export-controlled crypto software cannot access the server.

Using the OpenSSL command line tool (on a UNIX machine), it is possible to check which cipher suites a particular cipher list corresponds to. The example above yields the following output:

```
# openssl ciphers -v 'RC4:ALL:!EXPORT:!DH
RC4-SHA          SSLv3 Kx=RSA    Au=RSA   Enc=RC4(128)    Mac=SHA1
RC4-MD5          SSLv3 Kx=RSA    Au=RSA   Enc=RC4(128)    Mac=MD5
RC4-64-MD5       SSLv2 Kx=RSA    Au=RSA   Enc=RC4(64)     Mac=MD5
RC4-MD5          SSLv2 Kx=RSA    Au=RSA   Enc=RC4(128)    Mac=MD5
DES-CBC3-SHA     SSLv3 Kx=RSA    Au=RSA   Enc=3DES(168)   Mac=SHA1
DES-CBC-SHA      SSLv3 Kx=RSA    Au=RSA   Enc=DES(56)     Mac=SHA1
DES-CBC3-MD5     SSLv2 Kx=RSA    Au=RSA   Enc=3DES(168)   Mac=MD5
DES-CBC-MD5      SSLv2 Kx=RSA    Au=RSA   Enc=DES(56)     Mac=MD5
RC2-CBC-MD5      SSLv2 Kx=RSA    Au=RSA   Enc=RC2(128)    Mac=MD5
```

Supported cipher strings and meanings

The table below lists each supported cipher string alias and its significance.

Table 5 Cipher Strings and Meanings

Cipher String Aliases	Meaning
DEFAULT	The default cipher list, which corresponds to `ALL@STRENGTH`.
ALL	All cipher suites except the eNULL ciphers, which must be explicitly enabled.
HIGH	Cipher suites with key lengths larger than 128 bits.
MEDIUM	Cipher suites using 128-bit encryption.
LOW	Includes cipher suites using 64- or 56-bit encryption, but excludes export cipher suites.
EXPORT	Includes cipher suites using 40- and 56-bit encryption.
EXPORT40	Cipher suites using 40-bit export encryption only.
EXPORT56	Cipher suites using 56-bit export encryption only.
Cipher String Aliases	Meaning

Table 5 Cipher Strings and Meanings

eNULL, NULL	Cipher suites that do not offer any encryption at all because they pose a security threat; they are disabled unless explicitly included.
aNULL	Cipher suites that do not offer authentication, like anonymous DH algorithms. The use of such cipher suites is not recommended, because they facilitate man-in-the-middle attacks.
kRSA, RSA	Cipher suites using RSA key exchange.
kEDH	Cipher suites using ephemeral Diffie-Hellman key agreement.
aRSA	Cipher suites using RSA authentication, which implies that the certificates carry RSA keys.
SSLv3, SSLv2	SSL version 3.0 and SSL version 2.0 cipher suites, respectively.
DH	Cipher suites using DH encryption algorithms, including anonymous DH.
ADH	Cipher suites using anonymous DH encryption algorithms.
AES	Cipher suites using AES encryption algorithms.
3DES	Cipher suites using triple DES encryption algorithms.
Cipher String Aliases	Meaning
DES	Cipher suites using DES encryption algorithms, but not triple DES.
RC4	Cipher suites using RC4 encryption algorithms.
RC2	Cipher suites using RC2 encryption algorithms.
MD5	Cipher suites using MD5 encryption algorithms.
SHA1, SHA	Cipher suites using SHA1 encryption algorithms.

Appendix C
SNMP agent

There is one SNMP agent on the Contivity gateway, and the agent listens to the IP address of that particular device. The SNMP agent also listens to the MIP.

The SNMP agent supports SNMP version 1 and version 2c. Notification targets (the SNMP managers receiving trap messages sent by the agent) can be configured to use either SNMP v1 or SNMP v2c (with the default being SNMP v2c). You can specify any number of notification targets on the Contivity Secure IP Services Gateway.

Supported MIBs

The Contivity Secure IP Services Gateway supports the following MIBs:

- SNMPv2-MIB (host-specific)
- IP-MIB (host-specific)
- IP-FORWARD-MIB (host-specific)
- IF-MIB (host-specific)
- ALTEON-ISD-PLATFORM-MIB (cluster-specific)
- ALTEON-ISD-SSL-MIB (cluster-specific)
- SNMP-TARGET-MIB (cluster-specific)

The MIB is either host-specific or cluster-specific. Host-specific MIBs are supported by the SNMP agent on every Contivity Secure IP Services Gateway and contains host-specific information. Cluster-specific MIBs are only supported by the MIB agent (the agent on the Contivity gateway that currently holds the MIB) and contain cluster-specific information.

SNMPv2 MIB

The SNMPv2-MIB is a standard MIB which all agents implement and it contains the following groups and objects:

- System group, which is a collection of objects common to all managed systems.
- SNMP group, which is a collection of objects providing basic instrumentation and control of an SNMP entity.

IP-MIB

The following groups are implemented:

- ipGroup
- icmpGroup

IP-FORWARD-MIB

The following group is implemented:

- ipCidrRouteGroup

IF-MIB

The following groups are implemented:

- ifPacketGroup
- ifStackGroup

Limitations

The agent does not implement the following objects:

- ifType
- ifSpeed
- ifLastChange

- ifInUnknownProtos
- ifOutNUnicast

The agent does not implement the following traps:

- linkUp
- linkDown

Alteon iSD platform MIB

The ALTEON-ISD-PLATFORM-MIB contains the following groups and objects:

- Cluster group, whose objects provide information about the operational status of each Contivity Secure IP Services Gateway, IP address assignment, master/slave assignment, and the iSD host number.
- Performance group, whose objects provide information about CPU and memory utilization.
- Current Alarm group, whose objects provide information about the number of active alarms, alarm IDs, alarm severity levels, alarm cause, and the time when the alarm was triggered.
- Event group, whose objects provide information about the time when the event was generated, as well as a description of the event.

Alteon iSD-SSL MIB

The ALTEON-ISD-SSL-MIB contains objects for monitoring the SSL gateways. The objects provide information about the following:

- Number of SSL transactions per second.
- Number of initiated client SSL connections.
- Number of renegotiated client SSL connections.
- Number of successfully completed SSL handshakes.
- Number of client requests for a session ID found in the SSL cache.
- Number of client requests for a session ID not found in the SSL cache.
- Number of times a session ID could not be cached because the SSL cache was full.

- Number of client requests for a session ID that was found in the SSL cache, but inaccessible due to the fact that the Time To Live value for the session was exceeded.

SNMP-TARGET-MIB

The SNMP-TARGET-MIB contains information about where to send traps.

Supported traps

The following SNMP traps are supported by the Contivity gateway:

Table 6 Traps supported by the Contivity gateway

Trap Name	Description
alteonISDSSLHwFail	Signifies that the SSL accelerator hardware failed. The Contivity Secure IP Services Gateway will continue to handle traffic, but with severely degraded performance.
alteonISDDown	Signifies that the Contivity Secure IP Services Gateway is down and out of service.

Appendix D
Syslog messages

This appendix contains a list of the syslog messages that are sent from the Contivity gateway to a syslog server (when added to the system configuration). Syslog servers are added to the system configuration by using the menu options in the Syslog Servers menu.

This section lists the Syslog messages that can be sent from a Contivity gateway to a configured syslog server. The messages are divided into the following message types:

- Operating system (OS)
- System control
- Traffic processing
- Startup
- Configuration reload
- AAA

To view a list of syslog messages in alphabetical order, see section "Syslog messages in alphabetical order" on page 224.

Operating system messages

The operating system (OS) messages are divided into three categories:

- EMERG
- CRITICAL
- ERROR

EMERG

The following lists the EMERG messages:

- Root filesystem corrupt
- The system cannot boot, but stops with a single-user prompt. fsck failed. Reinstall in order to recover.
- Config filesystem corrupt beyond repair
- The system cannot boot, but stops with a single-user prompt. Reinstall in order to recover.
- Failed to write to config filesystem
- Probable hardware error. Reinstall.

CRITICAL

The following lists the CRITICAL messages:

- Config filesystem re-initialized - reinstall required
- Reinstall.
- Application filesystem corrupt - reinstall required
- Reinstall.

ERROR

The following lists the ERROR messages:

- Config filesystem corrupt

  Possible loss of configuration. Followed by the message Config filesystem re-initialized - reinstall required or Config filesystem restored from backup.

- Missing files in config filesystem

  Possible loss of configuration. Followed by the message Config filesystem re-initialized - reinstall required or Config filesystem restored from backup.

- Logs filesystem re-initialized

  Loss of logs.

- Root filesystem repaired - rebooting

  fsck found and fixed errors. Probably OK.

- Config filesystem restored from backup

  Loss of recent configuration changes.

- Rebooting to revert to permanent OS version

  Happens after Config filesystem re-initialized - reinstall required or Config filesystem restored from backup if software upgrade is in progress (if failure at first boot on new OS version).

System control messages

The system control process messages are divided into three categories:

- INFO
- ALARM
- EVENT

Both events and alarms are stored in the event log file.

INFO

System started [isdssl-<version>]

Sent whenever the system control process has been (re)started.

ALARM

Alarms are sent at a syslog level corresponding to the alarm severity as shown in the table below:

Table 7 Alarm severity

Alarm Severity	Syslog Level
CRITICAL	ALERT
MAJOR	CRITICAL
MINOR	ERROR
WARNING	WARNING
*	ERROR

Alarms are formatted according to the following pattern:

Id: <alarm sequence number>
Severity: <severity>
Name: <name of alarm>
Time. <date and time of the alarm>
Sender: <sender, for example, system or the Contivity Secure IP Services Gateway's IP address>
Cause: <cause of the alarm>
Extra: <additional information about the alarm>

To simplify finding the desired alarm messages, this section lists alarms with the **name** parameter on top.

- Name: **isd_down**
  Sender: <IP>
  Cause: down
  Extra:
  Severity: critical

  A member of the Contivity gateway cluster is down. This alarm is only sent if the cluster contains more than one Contivity Secure IP Services Gateway.

- Name: **single_master**
  Sender: system
  Cause: down
  Extra:
  Severity: warning

  Only one master Contivity Secure IP Services Gateway in the cluster is up and running.

- Name: **log_open_failed**
  Sender: <IP>, event
  Cause and Extra are explanations of the fault.
  Severity: major

  The event log (where all events and alarms are stored) could not be opened.

- Name: **make_software_release_permanent_failed**
  Sender: <IP>
  Cause: file_error | not_installed
  Extra: "Detailed info"
  Severity: critical

  Failed to make a new software release permanent after being activated. The system will automatically revert to the previous version.

- Name: **copy_software_release_failed**
  Sender: <IP>
  Cause: copy_failed | bad_release_package | no_release_package | unpack_failed
  Extra: "Detailed info"
  Severity: critical

  A Contivity Secure IP Services Gateway failed to install a software release while trying to install the same version as all other Contivity Secure IP Services Gateways in the cluster. The failing Contivity Secure IP Services Gateway tries to catch up with the other cluster members as it was not up and running when the new software version was installed.

- Name: **license**
  Sender: license_server
  Cause: license_not_loaded
  Extra: "All iSDs do not have the same license loaded"
  Severity: warning

One or several Contivity Secure IP Services Gateways in the cluster do not have the same SSL VPN license (with reference to number of concurrent users).

- Name: **ssl_hw_fail**
  Sender: <IP>
  Cause: find_error |init_error
  Extra:
  Severity: major

  The SSL hardware acceleration card could not be found or initiated. This will cause the Contivity Secure IP Services Gateway to run with degraded performance.

- Name: **hsm_not_logged_in**
  Sender: <IP>, <Token>
  Cause: reboot
  Extra: “Card<Token>”
  Severity: critical

  After a reboot, login to the HSM card is required.

- Name: **hsm_tampered_with**
  Sender: <IP>, <Token>
  Cause: hsm_detected
  Extra: “Card<Token>”
  Severity: critical

- Name: **slave_not_starting**
  Sender: <IP>, <SlaveNo>
  Cause: start_error | connect_timeout | fdsend | nothidden | name_resolv | nodename_occupied
  Extra:”
  Severity: warning

  The portal handling subsystem cannot be started.

EVENT

Events are sent at the NOTICE syslog level. They are formatted according to the following pattern:

Name: <Name>
Sender: <Sender>
Extra: <Extra>

- Name: **clear_alarm**
  Sender: <ID>
  Extra:

  The alarm with <ID> has been cleared.

- Name: **partitioned_network**
  Sender and Extra is lower level information.

  Sent to indicate that an Contivity Secure IP Services Gateway is recovering from a partitioned network situation.

- Name: **software_configuration_changed**
  Sender: system
  Extra: software release version <VSN> <Status>

  Indicates that release <VSN> (version) has been <Status> (unpacked/installed/permanent).

- Name: **software_release_copying**
  Sender: <IP>
  Extra: copy software release <VSN> from other cluster member

  Indicates that <IP> is copying the release <VSN> from another cluster member.

- Name: **software_release_rebooting**
  Sender: <IP>
  Extra: reboot with release version <VSN>

  Indicates that a Contivity gateway (<IP>) is rebooting on a new release (Contivity Secure IP Services Gateway that was not up and running during the normal installation is now catching up).

Traffic processing messages

The traffic processing subsystem messages are divided into these categories:

- CRITICAL

- ERROR
- WARNING
- INFO

CRITICAL

DNS alarm: all dns servers are DOWN

All DNS servers are down. The Contivity Secure IP Services Gateway cannot perform any DNS lookups.

ERROR

The following lists the ERROR messages:

- internal error: <no>

  An internal error occurred. Please contact support with as much information as possible to reproduce this message.

- javascript error: <reason> for: <host><path>

  JavaScript parsing error encountered when parsing content from <host><path>. This could be a problem in the Contivity gateway JavaScript parser, but most likely a syntactical error in the JavaScript on that page.

- vbscript error: <reason> for: <host><path>

  VBScript parsing error encountered when parsing content from <host><path>. This could be a problem in the Contivity gateway VBScript parser, but most likely a syntactical error in the VBScript on that page.

- jscript.encode error: <reason>

  Problem encountered when parsing an encoded JavaScript. It may be a problem with the JavaScript parser in the Contivity gateway or it could be a problem on the processed page.

- css error: <reason>

  Problem encountered when parsing a style sheet. It may be a problem with the css parser in the Contivity gateway or it could be a problem on the processed page.

- Failed to syslog traffic :<reason> -- disabling traf log

  Problem occurred when the Contivity gateway tried to send traffic logging syslog messages. Traffic system logging was disabled as a result.

- www_authenticate: bad credentials

  The browser sent a malformed WWW-Authenticate: credentials header. Most likely a broken client.

- http error: <reason>, Request="<method> <host><path>"

  A problem was encountered when parsing the HTTP traffic. This is either an indication of a non-standard client/server or an indication that the Contivity gateway's HTTP parser has gotten out of sync due to an earlier non-standard transaction from the client or server on this TCP stream.

- http header warning cli: <reason> (<header>)

  The client sent a bad HTTP header.

- http header warning srv: <reason> (<header>)

  The server sent a bad HTTP header.

- unknown WWW-Authenticate method, closing

  Backend server sent unknown HTTP authentication method.

- failed to parse Set-Cookie <header>

  The Contivity gateway got a malformed Set-Cookie header from the backend Web server.

- failed to locate corresponding portal for portal authenticated http server

  Portal authentication has been configured for an HTTP server, but no portal using the same VPN can be found. Make sure that there is a portal running using the same VPN id.

- Bad IP:PORT data <line> in thc script

  Bad ip:port found in health check script. Please reconfigure the health script. This should normally be captured earlier by the CLI.

- Bad regexp (<expr>) in health check

  Bad regular expression found in health check script. Please reconfigure.

- Bad script op found <script op>

  Bad script operation found in health check script. Please reconfigure.

- Unable to use the certificate for <server nr>

  Unsuitable certificate configured for server #.

- The private key and certificate don't match for <server nr>

  Key and certificate does not match for server #. The certificate has to be changed.

- Unable to use client private key for <server #>

  Key for doing sslconnect is not valid. Please reconfigure.

- Unable to find client private key for <server #>

  Key for doing sslconnect is not valid. Please reconfigure.

- Unable to use client certificate for <server #>

  Certificate for doing sslconnect is not valid. Please reconfigure.

- Failed to initialize SSL hardware

  Problem initializing SSL acceleration hardware. This will cause the SSL VPN module firmware to run with degraded performance.

- Could not find SSL hardware.

  Failed to detect SSL acceleration hardware.

- Connect failed: <reason>

  Connect to backend server failed with <reason>

- SSL connect failed: <reason>

  SSL connect to backend server failed with <reason>

- html error: <reason>

  Error encountered when parsing HTML. Probably non-standard HTML.

- socks error: <reason>

  Error encountered when parsing the socks traffic from the client. Probably a non-standard socks client.

- socks request: socks version <version> rejected

  SOCKS request of version <version> received and rejected. Most likely a non-standard SOCKS client.

- Cannot bind to local address: <ip>:<port>: <reason>

Problem encountered when trying to set up virtual server on <ip>:<port>.

- Ignoring DNS packet was not from any of the defined namesserver <ip>:<port>

  Contivity gateway received reply for non-configured DNS server.

WARNING

TPS license limit (<limit>) exceeded

The transactions per second (TPS) limit has been exceeded.

INFO

The following lists the INFO messages:

- gzip error: <reason>

  Problem encountered when processing compressed content.

- gzip warning: <reason>

  Problem encountered when processing compressed content.

- accept() turned off (<nr>) too many fds

  The Contivity gateway has temporarily stopped accepting new connections. This will happen when the Contivity Secure IP Services Gateway is overloaded. It will start accepting connections once it has finished processing its current sessions.

- No cert supplied by backend server

  No certificate supplied by backend server when doing SSL connect. Session terminated to backend server.

- No CN supplied in server cert <subject>

  No CN found in the subject of the certificate supplied by the backend server.

- Bad CN supplied in server cert <subject>

  Malformed CN found in subject of the certificate supplied by the backend server.

- Shutting sslproxy down.

Traffic subsystem has been stopped.

- Restarting proxy due to <reason>

  Traffic subsystem restarted due to <reason>

- DNS alarm: dns server(s) are UP

  At least one DNS server is now up.

- HC: backend <ip>:<port> is down

  Backend health check detected backend <ip>:<port> to be down.

- HC: backend <ip>:<port> is up again

  Backend health check detected backend <ip>:<port> to be up.

Startup messages

The traffic processing subsystem startup messages include the INFO category.

INFO

The following lists the INFO messages:

- HSM mode: <mode>

  Hardware Security Mode <mode>.

- Disabling transparent proxy, non-compatible with pooling

  Transparent proxy mode is disabled due to pooling being enabled (startup message).

- Set CSWIFT as default

  Using CSWIFT SSL hardware acceleration. (startup message)

- Using <hwtype> hardware

  Using <hwtype> hardware for SSL acceleration. (startup message)

- Loaded <ip>:<port>

  Initializing virtual server <ip>:<port>.

- Because clicerts are used, force adjust totalcache size to : <size> per server that use clicerts

  Generated if the size of the SSL session cache has been modified.

- No more than <nr> backend supported

  Generated when more than the maximum allowed backend servers have been configured.

- TPS license limit: <limit>

  TPS limit set to <limit>

- No TPS license limit

  Unlimited TPS license used.

- Started ssl-proxy

  Traffic subsystem started.

- Found <size> meg of phys mem

  Amount of physical memory found on system.

Configuration reload messages

The traffic subsystem configuration reload messages include the INFO category.

INFO

The following lists the INFO messages:

- reload cert config start

  Starting reloading of certificates.

- reload cert config done

  Certificate reloading done.

- reload configuration start

  Virtual server configuration reloading start.

- reload configuration network down

Syslog messages in alphabetical order

This section lists the syslog messages in alphabetical order.

Table 8 Syslog Messages in Alphabetical Order

Message	Severity	Type	Explanation
accept() turned off (<nr>) too many fds	INFO	Traffic Processing	The Contivity Secure IP Services Gateway has temporarily stopped accepting new connections. This will happen when the Contivity Secure IP Services Gateway is overloaded. It will start accepting connections once it has finished processing its current sessions.
Application filesystem corrupt - reinstall required	CRITICAL	OS	Reinstall.
Bad CN supplied in server cert <subject>	INFO	Traffic Processing	Malformed CN found in subject of the certificate supplied by the backend server.
Can't bind to local address: <ip>:<port>: <reason>	ERROR	Traffic Processing	Problem encountered when trying to set up virtual server on <*ip*>:<*port*>.
clear_alarm	EVENT	System Control	The alarm with <*ID*> has been cleared.
Config filesystem corrupt	ERROR	OS	Possible loss of configuration. Followed by the message **Config filesystem re-initialized - reinstall required** or **Config filesystem restored from backup**.
Config filesystem corrupt beyond repair	EMERG	OS	The system cannot boot, but stops with a single-user prompt. Reinstall in order to recover.
Config filesystem re-initialized - reinstall required	CRITICAL	OS	Reinstall.
Config filesystem restored from backup	ERROR	OS	Loss of recent configuration changes.
Connect failed: <reason>	ERROR	Traffic Processing	Connect to backend server failed with <*reason*>.

Table 8 Syslog Messages in Alphabetical Order

Message	Severity	Type	Explanation
copy_software_release_failed	ALARM (CRITICAL)	System Control	A Contivity gateway failed to install a software release while trying to install the same version as all other Contivity Secure IP Services Gateways in the cluster. The failing Contivity Secure IP Services Gateway tries to catch up with the other cluster members as it was not up and running when the new software version was installed.
Could not find SSL hardware.	ERROR	Traffic Processing	Failed to detect SSL acceleration hardware.
css error: <reason>	ERROR	Traffic Processing	Problem encountered when parsing a style sheet. It may be a problem with the css parser in the Contivity gateway or it could be a problem on the processed page.
Disabling transparent proxy, non-compatible with pooling	INFO	Startup	Transparent proxy mode is disabled due to pooling being enabled.
DNS alarm: all dns servers are DOWN	CRITICAL	Traffic Processing	All DNS servers are down. The Contivity Secure IP Services Gateway cannot perform any DNS lookups.
DNS alarm: dns server(s) are UP	INFO	Traffic Processing	At least one DNS server is now up.
Failed to initialize SSL hardware	ERROR	Traffic Processing	Problem initializing SSL acceleration hardware. This will cause the SSL VPN module firmware to run with degraded performance.
failed to locate corresponding portal for portal authenticated http server	ERROR	Traffic Processing	Portal authentication has been configured for an http server, but no portal using the same VPN can be found. Make sure that there is a portal running using the same VPN id.
failed to parse Set-Cookie <header>	ERROR	Traffic Processing	The Contivity gateway got a malformed Set-Cookie header from the backend Web server.
Failed to syslog traffic :<reason> -- disabling traf log	ERROR	Traffic Processing	Problem occurred when the Contivity gateway tried to send traffic logging syslog messages. Traffic syslogging was disabled as a result.
Failed to write to config filesystem	EMERG	OS	Probable hardware error. Reinstall.
Found <size> meg of phys mem	INFO	Startup	Amount of physical memory found on system.

Table 8 Syslog Messages in Alphabetical Order

Message	Severity	Type	Explanation
gzip error: <reason>	INFO	Traffic Processing	Problem encountered when processing compressed content.
gzip warning: <reason>	INFO	Traffic Processing	Problem encountered when processing compressed content.
HC: backend <ip>:<port> is down	INFO	Traffic Processing	Backend health check detected backend <ip>:<port> to be down.
HC: backend <ip>:<port> is up again	INFO	Traffic Processing	Backend health check detected backend <ip>:<port> to be up.
HSM mode: <mode>	INFO	Startup	Hardware Security Mode <mode>.
hsm_not_logged_in	ALARM (CRITICAL)	System Control	After a reboot, login to the HSM card is required.
hsm_tampered_with	ALARM (CRITICAL)	System Control	
html error: <reason>	ERROR	Traffic Processing	Error encountered when parsing HTML. Probably non-standard HTML.
http error: <reason>, Request="<method> <host><path>"	ERROR	Traffic Processing	A problem was encountered when parsing the HTTP traffic. This is either an indication of a non-standard client/server or an indication that the Contivity gateway's HTTP parser has gotten out of sync due to an earlier non-standard transaction from the client or server on this TCP stream.
http header warning cli: <reason> (<header>)	ERROR	Traffic Processing	The client sent a bad HTTP header.
http header warning srv: <reason> (<header>)	ERROR	Traffic Processing	The server sent a bad HTTP header.
HTTP NotLoggedIn, SrcIP="<ip>", Request="<request>"	INFO	AAA	
HTTP Rejected User="<user>", SrcIP="<ip>", Request="<request>"	INFO	AAA	The remote failed to access the specified Web server from the portal's Browse Intranet tab.

Table 8 Syslog Messages in Alphabetical Order

Message	Severity	Type	Explanation
HTTP User="<user>", SrcIP="<ip>", Request="<request>"	INFO	AAA	The remote user has successfully accessed the specified Web server from the portal's Browse Intranet tab.
Ignoring DNS packet was not from any of the defined namesserver <ip>:<port>	ERROR	Traffic Processing	Contivity gateway received reply for non-configured DNS server.
internal error: <no>	ERROR	Traffic Processing	An internal error occurred. Please contact support with as much information as possible to reproduce this message.
isd_down	ALARM (CRITICAL)	System Control	A member of the Contivity gateway cluster is down. This alarm is only sent if the cluster contains more than one Contivity Secure IP Services Gateway.
javascript error: <reason> for: <host><path>	ERROR	Traffic Processing	JavaScript parsing error encountered when parsing content from <host><path>. This could be a problem in the Contivity gateway JavaScript parser, but most likely a syntactical error in the JavaScript on that page.
jscript.encode error: <reason>	ERROR	Traffic Processing	Problem encountered when parsing an encoded JavaScript. It may be a problem with the JavaScript parser in the Contivity gateway or it could be a problem on the processed page.
LDAP backend(s) unreachable VPNId=<id> AuthId=<authid>	ERROR	AAA	Shown if LDAP servers cannot be reached when a user tries to log in to the portal.
license	ALARM (WARNING)	System Control	One or several Contivity Secure IP Services Gateways in the cluster do not have the same SSL VPN license (with reference to number of concurrent users).
Loaded <ip>:<port>	INFO	Startup	Initializing virtual server <ip>:<port>.
log_open_failed	ALARM (MAJOR)	System Control	The event log (where all events and alarms are stored) could not be opened.
Logs filesystem re-initialized	ERROR	OS	Loss of logs.
make_software_release_permanent_failed	ALARM (CRITICAL)	System Control	Failed to make a new software release permanent after being activated. The system will automatically revert to the previous version.

Table 8 Syslog Messages in Alphabetical Order

Message	Severity	Type	Explanation
Missing files in config filesystem	ERROR	OS	Possible loss of configuration. Followed by the message “Config filesystem re-initialized - reinstall required” or “Config filesystem restored from backup”.
No cert supplied by backend server	INFO	Traffic Processing	No certificate supplied by backend server when doing SSL connect. Session terminated to backend server.
No CN supplied in server cert <subject>	INFO	Traffic Processing	No CN found in the subject of the certificate supplied by the backend server.
No more than <nr> backend supported	INFO	Startup	Generated when more than the maximum allowed backend servers have been configured.
No TPS license limit	INFO	Startup	Unlimited TPS license used.
partitioned_network	EVENT	System Control	Sent to indicate that a Contivity gateway is recovering from a partitioned network situation.
PORTAL reject User="<user>" Proto="<proto>" Host="<host>" Share="<share>" Path="<path>"	INFO	AAA	The remote user failed to access the specified folder/directory on the specified file server from the portal’s Files tab.
PORTAL User="<user>" Proto="<proto>" Host="<host>" Share="<share>" Path="<path>"	INFO	AAA	The remote user has successfully accessed the specified folder/directory on the specified file server from the portal’s Files tab.
Rebooting to revert to permanent OS version	ERROR	OS	Happens after “Config filesystem re-initialized - reinstall required” or “Config filesystem restored from backup” if software upgrade is in progress (if failure at first boot on new OS version).
reload cert config done	INFO	Config Reload	Certificate reloading done.
reload cert config start	INFO	Config Reload	Starting reloading of certificates.
reload configuration done	INFO	Config Reload	Virtual server configuration reloading done.
reload configuration network down	INFO	Config Reload	Accepting new sessions are temporarily put on hold.
reload configuration network up	INFO	Config Reload	Resuming accepting new sessions after loading new configuration.

Table 8 Syslog Messages in Alphabetical Order

Message	Severity	Type	Explanation
reload configuration start	INFO	Config Reload	Virtual server configuration reloading start.
Restarting proxy due to <reason>	INFO	Traffic Processing	Traffic subsystem restarted due to <reason>.
Root filesystem corrupt	EMERG	OS	The system cannot boot, but stops with a single-user prompt. fsck failed. Reinstall in order to recover.
Root filesystem repaired - rebooting	ERROR	OS	fsck found and fixed errors. Probably OK.
Set CSWIFT as default	INFO	Startup	Using CSWIFT SSL hardware acceleration.
Shutting sslproxy down.	INFO	Traffic Processing	Traffic subsystem has been stopped.
Because clicerts are used, force adjust totalcache size to : <size> per server that use clicerts	INFO	Startup	Generated if the size of the SSL session cache has been modified.
single_master	ALARM (WARNING)	System Control	Only one master Contivity Secure IP Services Gateway in the cluster is up and running.
slave_not_starting	ALARM (WARNING)	System Control	The portal handling subsystem cannot be started.
socks error: <reason>	ERROR	Traffic Processing	Error encountered when parsing the SOCKS traffic from the client. Probably a non-standard socks client.
SOCKS Rejected User="<user>", SrcIP="<ip>", Request="<request>"	INFO	AAA	The remote user failed to perform an operation by using one of the features available under the portal's Advanced tab.
socks request: socks version <version> rejected	ERROR	Traffic Processing	SOCKS request of version <version> received and rejected. Most likely a non-standard SOCKS client.
SOCKS User="<user>", SrcIP="<ip>", Request="<request>"	INFO	AAA	The remote user has successfully performed an operation by using one of the features available under the portal's Advanced tab.
software_configuration_changed	EVENT	System Control	Indicates that release <*VSN*> (version) has been <*Status*> (unpacked/installed/ permanent).
software_release_copying	EVENT	System Control	Indicates that <*IP*> is copying the release <*VSN*> from another cluster member.

Table 8 Syslog Messages in Alphabetical Order

Message	Severity	Type	Explanation
software_release_rebooting	EVENT	System Control	Indicates that a Contivity gateway (<*IP*>) is rebooting on a new release (Contivity Secure IP Services Gateway that was not up and running during the normal installation is now catching up).
SSL connect failed: <reason>	ERROR	Traffic Processing	SSL connect to backend server failed with <*reason*>.
ssl_hw_fail	ALARM (MAJOR)	System Control	The SSL hardware acceleration card could not be found or initiated. This will cause the Contivity Secure IP Services Gateway to run with degraded performance.
Started ssl-proxy	INFO	Startup	Traffic subsystem started.
System started [isdssl-<version>]	INFO	System Control	Sent whenever the system control process has been (re)started.
The private key and certificate don't match for <server nr>	ERROR	Traffic Processing	Key and certificate do not match for server #. The certificate has to be changed.
TPS license limit (<limit>) exceeded	WARNING	Traffic Processing	The transactions per second (TPS) limit has been exceeded.
TPS license limit: <limit>	INFO	Startup	TPS limit set to <*limit*>.
Unable to find client private key for <server #>	ERROR	Traffic Processing	Key for doing sslconnect is not valid. Please reconfigure.
Unable to use client certificate for <server #>	ERROR	Traffic Processing	Certificate for doing sslconnect is not valid. Please reconfigure.
Unable to use client private key for <server #>	ERROR	Traffic Processing	Key for doing sslconnect is not valid. Please reconfigure.
Unable to use the certificate for <server nr>	ERROR	Traffic Processing	Unsuitable certificate configured for server #.
unknown WWW-Authenticate method, closing	ERROR	Traffic Processing	Backend server sent unknown HTTP authentication method.
Using <hwtype> hardware	INFO	Startup	Using <*hwtype*> hardware for SSL acceleration.

Table 8 Syslog Messages in Alphabetical Order

Message	Severity	Type	Explanation
vbscript error: <reason> for: <host><path>	ERROR	Traffic Processing	VBScript parsing error encountered when parsing content from <*host*><*path*>. This could be a problem in the Contivity gateway VBScript parser, but most likely a syntactical error in the VBScript on that page.
www_authenticate: bad credentials	ERROR	Traffic Processing	The browser sent a malformed WWW-Authenticate: credentials header. Most likely a broken client.
VPN Login: failed - client ip: <ip> [user: <user>] error: <error>	INFO	AAA	Portal login failed. The remote user's client IP address, user name is shown along with error cause.
VPN Login: succeeded - client ip: <ip> user: <user> groups: <groups>	INFO	AAA	Portal login succeeded. The remote user's client IP address, user name and group membership is shown.
VPN Logout: user: <user>	INFO	AAA	The remote user has logged out from the portal session.

Appendix E
Key code definitions

When using the Telnet applet available under the portal's Advanced tab, there is an option to specify a keymap URL that points to a key code definition file. If your application uses a different keyboard layout than the standard VT320, a key code definition file can be created and uploaded to the keymap URL. This appendix shows how to create the key code definition file.

Syntax description

Almost all special keys can be defined according to the following syntax rule:

[**SCA**] *KEY***=***STRING*

The characters enclosed in `[` and `]` are optional. Only one of the characters `S` (SHIFT), `C` (CTRL) or `A` (ALT) can appear before *KEY*, which is a textual representation of the key you want to redefine (F1, PGUP etc.).

The new *STRING* to be sent when pressing the key should come after the equals character (**=**). Hash marks (`#`) in the file declare the line as a comment and will be ignored. The examples below explain the syntax in more detail:

Send the string "test" when pressing the `F1` key:

```
F1 = test
```

On pressing `Control + PGUP`, send the string "pgup pressed":

```
CPGUP = pgup pressed
```

Redefine the key `Alt + F12` to send an escape character:

AF12 = \\e

As can be seen, the string can contain special characters which can be escaped using the backslash (\).

Allowed special characters

The table below includes allowed special characters:

Note: For some of the escape codes you need two backslashes, because these are specific java ssh definitions not known by the Java Property mechanism.

Table 9 Allowed special characters

Special Character	Explanation
\\b	Backspace. This character is usually sent by the <- key (`Backspace` key).
\\e	Escape. This character is usually sent by the `Esc` key.
\n	Newline. This character will move the cursor to a new line. On UNIX systems, it is equivalent to carriage return + newline. Usually the `Enter` key sends this character.
\r	Carriage Return. This key moves the cursor to the beginning of the line. In conjunction with Newline, it moves the cursor to the beginning of a new line.
\t	Tabulator. The tab character is sent by the `TAB` key and moves the cursor to the next tab stop defined by the terminal.
\\v	Vertical Tabulator. Sends a vertical tabulator character.
\\a	Bell. Sends a terminal bell character which should make the terminal sound its bell.
\\number	Inserts the character that is defined by this *number* in the ISO Latin1 character set. The *number* should be an octal value.

Redefinable keys

The following table explains which keys can be redefined. As explained earlier, each of the keys can be prefixed by a character defining the redefinition that occurs if it is pressed in conjunction with the SHIFT, CONTROL or ALT keys.

Table 10 Redefinable keys

Key Representation	Remarks
F1-F20	The Function keys (F1, F2 etc. up to F20).
PGUP	The Page Up key.
PGDOWN	The Page Down key.
END	The End key.
HOME	The Home (Pos 1) key.
INSERT	The Insert key.
REMOVE	The Remove key.
UP	The Cursor Up key.
DOWN	The Cursor Down key.
LEFT	The Cursor Left key.
RIGHT	The Cursor Right key.
NUMPAD0-NUMPAD9	The numbered Numeric keypad keys.
ESCAPE	The Escape key.
BACKSPACE	The Backspace key.
TAB	The Tab key.

Example of key code definition file

Below is an example of the `keyCodes.at386` key code definition file, created for an AT-386 Terminal.

```
#
F1=\\eOP
F2=\\eOQ
F3=\\eOR
F4=\\eOS
F5=\\eOT
F6=\\eOU
F7=\\eOV
F8=\\eOW
F9=\\eOX
F10=\\eOY
F11=\\eOZ
F12=\\eOA
#
# Shift F1 thru F10
#
SF1=\\eOp
SF2=\\eOq
SF3=\\eOr
SF4=\\eOs
SF5=\\eOt
SF6=\\eOu
SF7=\\eOv
SF8=\\eOw
SF9=\\eOx
SF10=\\eOy
SF11=\\eOz
SF12=\\eOa
#
# Other cursor movement keys
#
UP=\\e[A
DOWN=\\e[B
RIGHT=\\e[C
LEFT=\\e[D
#
INSERT=\\e[@
# REMOVE=\\177  #( hex 7F  /  Decimal 127  /  Octal  177  /
DEL Key)
#
HOME=\\e[H
PGDOWN=\\e[U
PGUP=\\e[V
END=\\e[Y
#
```

Appendix F
Troubleshooting

After running the VPN Quick Wizard, you should be able to log in to the portal with the username and password of a user that is already defined on the Contivity gateway.

Listed below are a few scenarios that require troubleshooting.

If you cannot get to the Portal Login Page:

1. On the Contivity gateway, select Services > SSL VPN. The Current Status section of the screen should indicate that the status is Operational and the Virtual Server Ports list should include 443.
2. If it does not indicate the status as Operational, go to Status > Event Log.

   The eventlog will tell you what the error is. If you can not find the error in the eventlog, go back to the SERVICES > SSLVPN screen. Each time you check this screen (if there is an error), it will update the event log with another event.
3. Fix the condition indicated in the event log.

If this does not fix your issue, try the following:

1. Ensure that your user is using the following syntax on their browser:

   ```
   https://x.x.x.x/
   or
   https://<VPN_name>
   ```

   where *x.x.x.x* is the public interface of the Contivity gateway and <*VPN_name*> is the DNS entry for your Contivity gateway public interface.
2. If you have multiple public interfaces, check that the SSL VPN is listening on the correct interface:

a Launch the SSL VPN Manager from the Services > SSL VPN page of the Contivity web management interface.

b In the SSL VPN Manager, select Servers > 1 <*server_name*>.

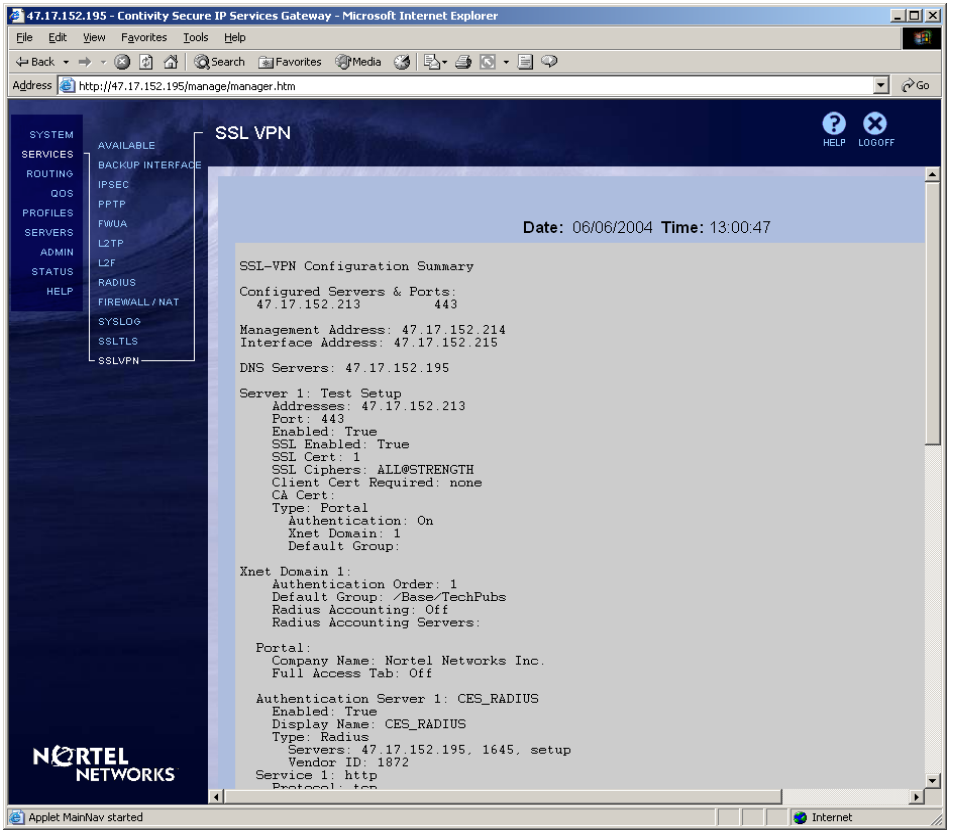
c In the right panel, select the Advanced tab.

d Select the Standalone tab.

e Check that the correct interface is listed here.

f You can also select the Config Summary button on the Services > SSL VPN page in the Contivity web interface. This accesses the SSL VPN Configuration Summary screen, shown below, which gives a big picture of all the important data configured on the SSL VPN. For example, a list of active servers and ports is at the very top.

Figure 106 Configuration summary



You can get to the Portal Page, but login fails.

After a user has attempted to log in, an event is written to the Contivity gateway event log. Go to the Contivity event log and inspect it. If there are no event log entries pertaining to this issue, then it is likely that the dialog between the SSL card RADIUS client and the Contivity RADIUS server is not working correctly. Do the following:

1. On the Contivity gateway, select Services > RADIUS. Be sure that this is enabled and set up correctly. The easiest configuration is to enable the default client and enter the password.
2. Go to the SSL VPN Manager and in the left panel select VPN > AAA > Authentication.
3. Right-click on 1 CES_RADIUS (if it exists) and delete it.
4. Click on VPNs > VPN 1 and click on the Quick Wizard tab. Select Yes to create default RADIUS and No to Create Default Services.
5. Click on Add. This recreates the RADIUS client using the credentials from the Contivity gateway.

If there are entries in the event log:

1. If the eventlog says that the user was accepted, check that the Groups on the SSL Card mirror the Groups on the Contivity gateway. If not, run the Group Synchronization Wizard from the SSL VPN Manager.
2. Check that the group on the SSL Card has the correct access permissions:
   a. In the SSL VPN Manager go to VPNs > VPN 1 > Groups > 1: .
   b. In the right pane, ensure that there is an access rule for the group that shows * * * with an action of **Accept**.
   c. If there is not one, add it.

If the event log shows that the user was denied access or not found:

The Contivity must have configured users for internal LDAP, external LDAP, or RADIUS. The SSL Card uses these same users.

1. From the Contivity gateway, select Services > RADIUS and check that the authentication order is set up correctly. If Contivity users are held in RADIUS, be sure that RADIUS is at the top of the authentication list. The same applies for LDAP proxy.
2. If there are no users, select Profiles > Users and add a user to the Contivity gateway. Make the authentication order LDAP internal.

Index

L

M

N

O

P

R

S

T

U

W