

Version 5.00

Part No. 318451-A Rev 00
June 2004

600 Technology Park Drive
Billerica, MA 01821-4130

Configuring SSL VPN Services on the Contivity Secure IP Services Gateway

NORTEL
NETWORKS™

Copyright © 2004 Nortel Networks

All rights reserved. June 2004.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

Nortel Networks, the Nortel Networks logo, and Contivity are trademarks of Nortel Networks.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Java is a trademark of Sun Microsystems.

Microsoft, Windows, Windows NT, and MS-DOS are trademarks of Microsoft Corporation.

NETVIEW is a trademark of International Business Machines Corp (IBM).

OPENView is a trademark of Hewlett-Packard Company.

SPECTRUM is a trademark of Cabletron Systems, Inc.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

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

Preface	17
Before you begin	17
Text conventions	17
Acronyms	19
Related publications	21
Hard-copy technical manuals	22
How to get help	22
Chapter 1	
SSL VPN Overview	23
Hardware platforms	23
Features	24
Chapter 2	
Using the SSL VPN portal	27
Browser requirements	28
Login screen	28
Unified access portal	29
Home tab	30
Browse Intranet tab	31
Files tab	32
Full access tab	34
Contivity VPN Client	34
SSL VPN Client	35
Advanced tab, Telnet/SSHv1 access	36
HTTP proxy advanced tab	38
Advanced tab, port forwarder	41
Custom port forwarder	42

Access to Outlook Express example	42
Client application configuration example	44
Telnet port forwarder	45
HTTP port forwarder	45
Port forwarder links	45
Native Outlook port forwarder	45
Logout tab	48
Using the Domain Quick Wizard	52
Customizing the portal	54
Using the General tab	55
Configuring portal full access	55
Default appearance	57
Common colors	58
Changing colors	59
Changing banner images	60
Changing company name	61
Hiding logo	62
Changing static text on login screen	62
Checking new appearance	62
Naming login services	63
Automatic redirection to internal site	64
Group-controlled redirection to internal sites	64
Chapter 3	
Initial configuration	67
Configuration considerations	67
Initializing SSL VPN Module 1000	68
Configuring Web interface parameters	72
SSL VPN and Contivity Stateful Firewall	76
Launching SSL VPN manager	78
Installing JRE 1.4.2	79
SSL VPN manager login	79
Configuring SSL VPN system settings	80
Upgrading the software	84
Activating SSL VPN upgrade packages	86

Generating certificates	88
Generating and submitting CSRs	88
Adding certificates to the Contivity gateway	91
Copy-and-paste certificates	92
Updating existing certificates	93
Updating DNS servers	94
Chapter 4	
Configuring domains	95
Configuring authorization	96
Access rules	97
Access rules configuration	99
Access rule ordering	99
Creating service definitions	100
Creating path (Appspec) definition	100
User type	101
Default groups	102
Multiple groups	103
Extended profiles	104
Defining Portal Links	105
Full access	106
Front End Authorization requirements - Filters	106
Defining client filters	107
Networks	107
Configuring authentication	109
External server authentication	110
SSL VPN authentication and IPsec client authentication	112
External database authentication	117
Client certificate authentication	118
Managing client certificate revocation	120
Making use of the Contivity RADIUS authentication	121
SSL VPN authentication of Contivity internal users using RADIUS	123
SSL VPN authentication of users stored in external RADIUS	124
RADIUS returning a group attribute	124
SSL VPN authentication of users stored in external LDAP	125

Using SSL VPN native authentication methods	126
LDAP authentication	126
NTLM authentication	131
SiteMinder authentication	134
Single sign-on domains	136
Accounting	138
Common Portal Settings	139
Chapter 5	
Configuring virtual servers	141
Configuring portal servers	141
URL Rewrite White-list	143
Configuring HTTP and generic servers	144
Configuring HTTP to HTTPs redirect	144
Configuring SOCKS servers	146
Configuring load balancing for back end servers	146
Appendix A	
Configuration examples	149
Portal links examples	149
Linking to Samba (SMB) file server	149
Linking to FTP file server	150
Creating direct link to Web page	152
Creating secured links to Web pages	153
Creating automatic login links (direct)	154
Using internal auto login link	156
Linking to terminal servers	157
Customizing port forwarder link (Citrix)	159
Using Telnet port forwarder link	163
Creating Outlook port forwarder link	165
Creating HTTP proxy links	168
Creating Citrix links	171
Creating Netdrive links	173
Access rule sample configurations	174
Access to Outlook Web access server	174

Access to intranet Web server	176
Access to intranet file server	178
Access allowed to specific subnet	179
Access denied to specific subnet	180
Group configuration examples	180
Defining staff groups	180
Defining the base profile	181
Creating network identifying branch office network	181
Defining client filter for the client network	182
Defining extended profiles	182
Results	183
Defining engineering groups	183
Defining base profiles	184
Defining client filters for token login	185
Creating extended profiles for token login	185
Results	186
Extended profile for users with client certificate	186
Extended profile for users with IE cache wiper	187
Appendix B	
Supported ciphers	189
Cipher list formats	191
Modifying a cipher list	191
Supported cipher strings and meanings	192
Appendix C	
SNMP agent	195
Supported MIBs	195
SNMPv2 MIB	196
IP-MIB	196
IP-FORWARD-MIB	196
IF-MIB	196
Limitations	196
Alteon iSD platform MIB	197
Alteon iSD-SSL MIB	197

SNMP-TARGET-MIB	198
Supported traps	198
Appendix D	
Syslog messages	199
Operating system messages	199
EMERG	200
CRITICAL	200
ERROR	200
System control messages	201
INFO	201
ALARM	202
EVENT	204
Traffic processing messages	205
CRITICAL	206
ERROR	206
WARNING	209
INFO	209
Startup messages	210
INFO	210
Configuration reload messages	211
INFO	211
Syslog messages in alphabetical order	212
Appendix E	
Key code definitions	221
Syntax description	221
Allowed special characters	222
Redefinable keys	223
Example of key code definition file	224
Appendix F	
Troubleshooting	225
Index	229

Figures

Figure 1	Login screen	29
Figure 2	Unified access portal	29
Figure 3	Home tab	30
Figure 4	Browse intranet	31
Figure 5	Files tab	32
Figure 6	File session folder	33
Figure 7	Full Access tab	34
Figure 8	Java applet window	36
Figure 9	Telnet/SSHv1 access	37
Figure 10	HTTP proxy Advanced tab	39
Figure 11	Reconfigure browser proxy settings	41
Figure 12	Custom port forwarder	42
Figure 13	Local host properties	44
Figure 14	Outlook port forwarder	46
Figure 15	Logout warning	49
Figure 16	Warning message	49
Figure 17	Clear browser history	49
Figure 18	Portal login screen	50
Figure 19	Portal logout screen	51
Figure 20	Delete history message	51
Figure 21	Quick Wizard	52
Figure 22	Customize portal	55
Figure 23	Full Access tab	56
Figure 24	Default portal	58
Figure 25	Change colors	60
Figure 26	Change banner	61
Figure 27	Verify changes	63
Figure 28	Updated view	64
Figure 29	SSL VPN screen	69

Figure 30	Initialization time	70
Figure 31	Required initialization fields	71
Figure 32	Initialized SSL VPN	72
Figure 33	System Identity screen	73
Figure 34	RADIUS Service screen	74
Figure 35	Firewall/NAT screen	75
Figure 36	CSF configuration example	76
Figure 37	Insert firewall implied rule	77
Figure 38	Do not insert firewall implied rule	77
Figure 39	New firewall policy that disallows traffic	78
Figure 40	New policy that allows traffic	78
Figure 41	JRE certificate	79
Figure 42	SSL VPN manager login	80
Figure 43	New SSL VPN installation screen	80
Figure 44	DNS tab	81
Figure 45	Add DNS servers	81
Figure 46	DNS server added	82
Figure 47	Add certificates	83
Figure 48	Review setup	84
Figure 49	Upgrades	85
Figure 50	Upload version	86
Figure 51	Activate software	87
Figure 52	Group access rules	98
Figure 53	Access rules	99
Figure 54	Add application	101
Figure 55	Default groups	102
Figure 56	Add filters	107
Figure 57	Add network	108
Figure 58	Add subnet	109
Figure 59	Authentication infrastructure	111
Figure 60	Configuring the RADIUS server	116
Figure 61	RADIUS client pointing to RADIUS service	116
Figure 62	Default group for a domain	117
Figure 63	Certificate authentication server	118
Figure 64	Virtual server configured to require client certificates	119

Figure 65	Configuring automatic CRL retrieval	120
Figure 66	Creating your own CRL	121
Figure 67	Contivity RADIUS service configuration	122
Figure 68	SSL VPN module RADIUS client aimed at Contivity RADIUS service . .	123
Figure 69	Authentication through intranet LDAP server	127
Figure 70	LDAP server IP address and port	128
Figure 71	NTLM authentication	132
Figure 72	SiteMinder configuration	134
Figure 73	Single sign on domains	137
Figure 74	Accounting screen	138
Figure 75	Add Server	141
Figure 76	Samba file server link	150
Figure 77	FTP file server link	151
Figure 78	External Web link	152
Figure 79	Secured Web link	153
Figure 80	External auto login link	155
Figure 81	Internal auto login link	156
Figure 82	Terminal link	158
Figure 83	Custom Citrix link	160
Figure 84	Telnet port forwarder link	164
Figure 85	Outlook port forwarder link	167
Figure 86	HTTP proxy	169
Figure 87	Example Citrix link	172
Figure 88	Example Netdrive link	173
Figure 89	Add network	175
Figure 90	Add subnet	176
Figure 91	Add network example	177
Figure 92	Add subnet example	178
Figure 93	Intranet file server	179
Figure 94	Configuration summary	226

Tables

Table 1	Common colors with hexadecimal color codes.	59
Table 2	Valid access rules users belonging to multiple groups	103
Table 3	Authentication mechanisms	114
Table 4	Supported Ciphers	189
Table 5	Cipher Strings and Meanings	192
Table 6	Traps supported by the Contivity gateway	198
Table 7	Alarm severity	202
Table 8	Syslog Messages in Alphabetical Order	212
Table 9	Allowed special characters	222
Table 10	Redefinable keys	223

Preface

This guide introduces the Nortel Networks* 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 ({})	<p>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.</p> <p>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.</p>
brackets ([])	<p>Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.</p> <p>Example: If the command syntax is show ntp [associations], you can enter either show ntp or show ntp associations.</p> <p>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.</p>
ellipsis points (. . .)	<p>Indicate that you repeat the last element of the command as needed.</p> <p>Example: If the command syntax is more diskn:<directory>/...<file_name>, you enter more and the fully qualified name of the file.</p>
<i>italic text</i>	<p>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.</p> <p>Example: If the command syntax is ping <ip_address>, <i>ip_address</i> is one variable and you substitute one value for it.</p>
plain Courier text	<p>Indicates system output, for example, prompts and system messages.</p> <p>Example: File not found.</p>

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:

- Release notes provide the latest information, including brief descriptions of the new features, problems fixed in this release, and known problems and workarounds.
- *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 BIS, DSLsw, 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, 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

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. 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 at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

How to get help

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

If you purchased a Nortel Networks service program, contact Nortel Networks Technical Support. To obtain contact information online, go to the www.nortelnetworks.com/cgi-bin/comments/comments.cgi URL, then click on Technical Support.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, you can call 1-800-4NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the <http://www.nortelnetworks.com/help/contact/erc/index.html> URL.

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 made 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 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 on to the SSL acceleration features, which makes it possible to combine SSL acceleration and VPN.

Hardware platforms

The SSL VPN Module 1000 card is supported on Contivity 1740, 2700, and 5000 platforms with 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 your 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) via 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 via 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 Networks. 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 should 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 Networks support and provide the MAC address to receive a license key.

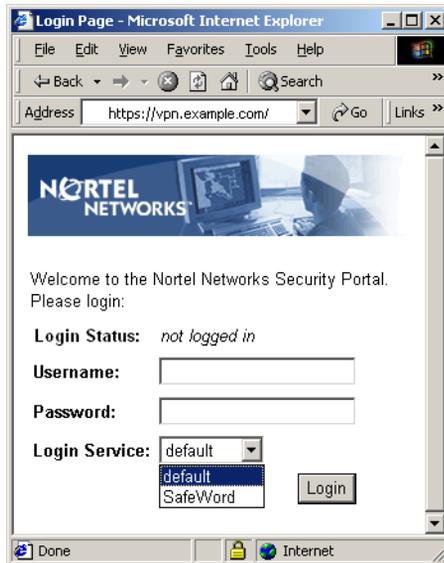
Browser requirements

In clientless mode, any JavaScript and SSL-enabled browser will work 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

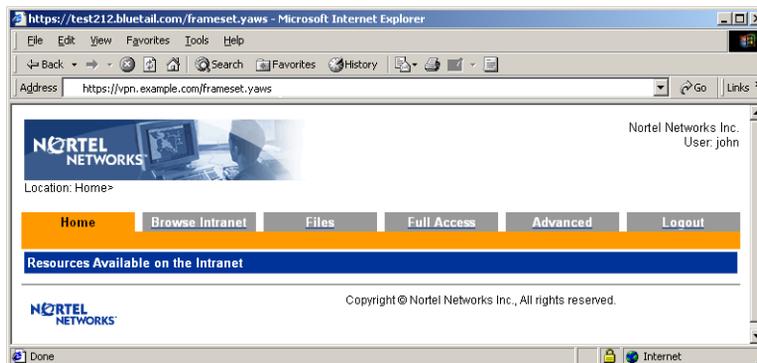
Login screen

With the clientless mode, the user enters the domain address to the portal (<https://vpn.example.com>) in the available Web browser and logs in using the login screen.

Figure 1 Login screen

Unified access portal

Having successfully logged in, the SSL VPN Unified Access Portal screen is displayed. The portal consists of different tabs from which the remote user can access intranet resources. The available resources is 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 is the default tab on the portal screen. If links have been 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 will have access to 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 SMB file server

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

Browse Intranet tab

This tab 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, you can 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 lets you access an SMB (Windows file share) or FTP file server.

Figure 5 Files tab

The screenshot shows a web interface with a navigation bar at the top containing tabs: Home, Browse Intranet, Files (highlighted in orange), Full Access, Advanced, and Logout. Below the navigation bar, there are two main sections. The left section is titled "Specify a New File Server" and contains the following text: "From this page you can access file servers on the Intranet. You can only access servers as defined by your security level." and "If you do not know any file server on the Intranet you should either contact your system administrator or use the links on the [Home](#) page." Below this text is a form with the following fields and options: "Specify a file server:" followed by a "Host:" text box, radio buttons for "smb" (selected) and "ftp", a checked "More options" checkbox, and an "Open" button. Below these are "User:" (text box with "john"), "Password:" (text box with "(Leave empty to use portal password)"), "[Share]:" (text box with "(Leave empty to scan)"), "[Workgroup]:" (text box with "WORKGROUP"), and "[Path]:" (text box with "(Optional)"). The right section is titled "Active File Sessions" and contains the text "There are no active file sessions". At the bottom of the browser window, there is a taskbar with a lock icon and the text "Internet".

To access the file server:

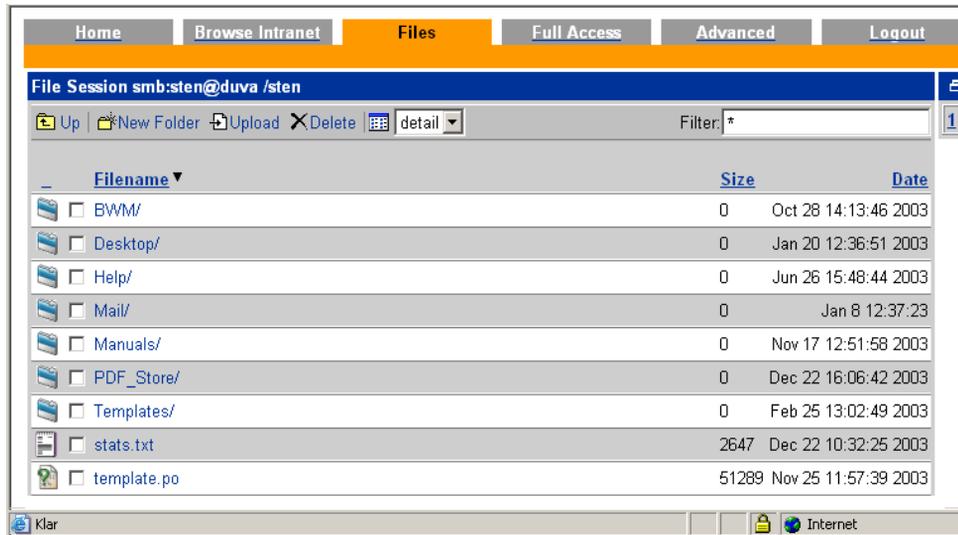
- 1 Enter the host name or IP address of the file server in the Host field. Also select the desired file server type, such as SMB (Windows file share) or FTP.
- 2 To display more options, select the More options check box.
- 3 To limit the view to a specific user's home share folder, enter the user's 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/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. Then enter a folder name in the field Create new directory named. Finally 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.

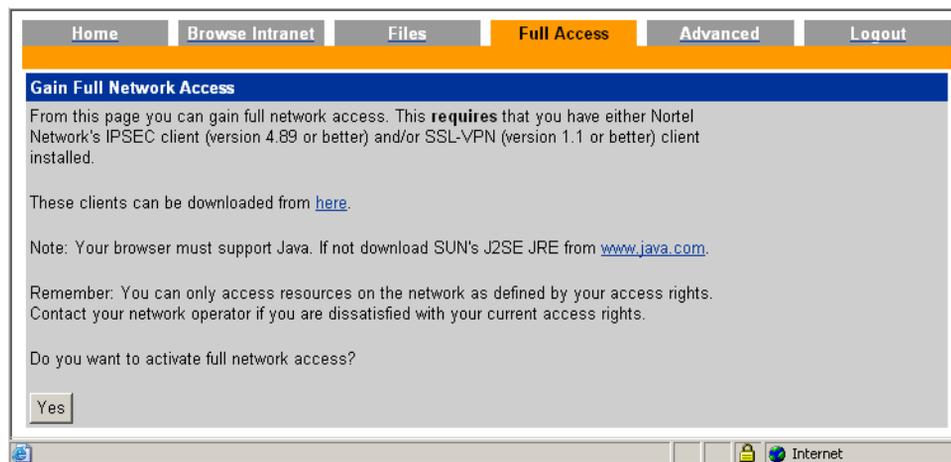
Full access tab

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

The Full Access tab 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

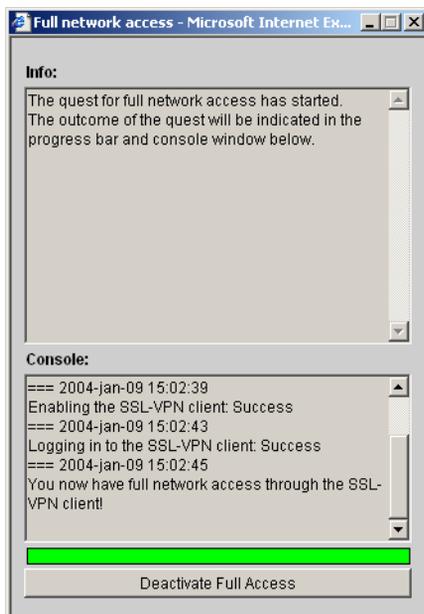
If the Contivity VPN client is *not* installed on the remote user's machine or unable to connect, the Java applet checks whether the Nortel Networks SSL VPN client is installed and if it is able to connect to the Contivity gateway. If so, the SSL VPN client is silently activated on the remote user's 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 9 Telnet/SSHv1 access

Home Browse Intranet Files Full Access **Advanced** Logout

Telnet/SSHv1 Access HTTP Proxy Port Forwarder

Access Telnet or SSHv1 Servers on the Intranet

From this page you can access Telnet or SSHv1 servers on the Intranet. You can only access servers as defined by your security level.

Note: Your browser must support Java. If not download SUN's J2SE JRE from www.java.com.

If you do not know any Telnet or SSHv1 servers on the Intranet you should either contact your system administrator or use the links on the [Home](#) page.

If you already sit behind an HTTP Proxy just specify it as the chaining HTTP Proxy below. If not you can safely ignore this setting.

A new window will be opened if you hit the ENTER key (or the Open... button). You can open multiple windows to access several servers in parallel.

Host:

Port: Telnet SSHv1

[Keymap URL]: (Optional)

[HTTP Proxy Host]: (Leave empty to skip)

[HTTP Proxy Port]: (Leave empty to skip)

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).

Users who are working from a location requiring traffic to pass through an intermediate HTTP proxy server on the intranet should enter the IP address (or domain name) and port of that proxy server. All applet traffic will be tunneled to the Contivity gateway through the HTTP proxy server. The HTTP Proxy server should have 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 will be 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 may contain plugins (for example, a Flash movie) which, in turn, may 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 will not be displayed.

To ensure display of all URLs (including ones that are embedded in plugins) the HTTP proxy feature lets you download a Java applet to the client. The client browser's proxy settings should then be changed 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

Home Browse Intranet Files Full Access **Advanced** Logout

Telnet/SSH/1 Access **HTTP Proxy** Port Forwarder

Access Web Servers on the Intranet

From this page you can start an HTTP proxy. It can be used to access Web servers on the Intranet. You can only access servers as defined by your security level.

Note: Your browser must support Java. If not download SUN's J2SE JRE from www.java.com.

In order to use the proxy you must update your browser configuration. Detailed instructions on how to do this will follow if you start the proxy.

If you already sit behind an HTTP Proxy just specify it as the chaining HTTP Proxy below. If not you can safely ignore this setting.

A new window will be opened if you hit the Open... button.

[HTTP Proxy Host]: (Leave empty to skip)

[HTTP Proxy Port]: (Leave empty to skip)

Open... Reconfigure Internet Explorer to use the HTTP proxy

Internet

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).

Users who are working from a location requiring traffic to pass through an *intermediate* HTTP Proxy server should enter the IP address (or domain 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 should have 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, the user may select the check box Reconfigure Internet Explorer to use the HTTP proxy.

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

3 Click on Open.

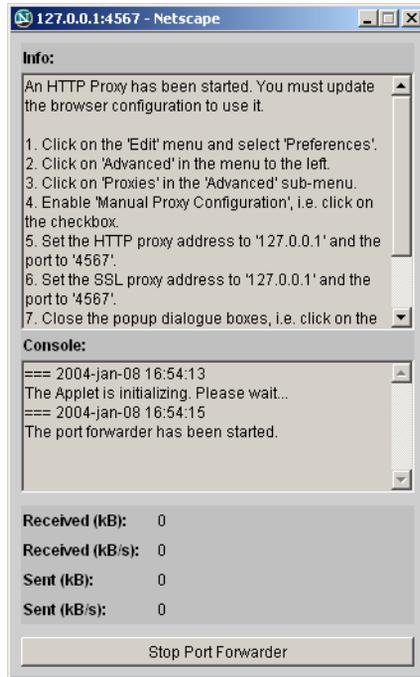
The user will be asked to install a signed applet (certified by Nortel Networks). When done, a Java applet window opens to confirm that an HTTP Proxy applet has been started.

4 Reconfigure the browser's proxy settings (not required for Internet Explorer).

Unless Internet Explorer is used as client browser, the browser's proxy settings have to be reconfigured manually by the user. Instructions (related to the type of browser used) are displayed in the Info part of the Java applet window.

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

To quit the HTTP Proxy session, the user should click on Stop Port Forwarder in the Java applet window. If the browser was reconfigured manually, the user should also 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) will 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 lets the user start an optional TCP- or UDP-based application (for example, Citrix Metaframe, Telnet or Outlook Express). To start a custom port forwarder, the user should keep the Custom option in the Port forwarder type box.

Figure 12 Custom port forwarder

Home Browse Intranet Files Full Access **Advanced** Logout

Telnet/SSH/v1 Access HTTP Proxy **Port Forwarder**

Start Custom Port Forwarder(s)

Port forwarder type:

From this page you can start several custom port forwarders. It can be used to access TCP based servers on the Intranet using legacy applications. You can only access servers as defined by your security level.

Note: Your browser must support Java. If not download SUN's J2SE JRE from www.java.com.

1. If source ip = 127.0.0.1, source port = 6666, destination host = foo.acme.com and destination port = 23 you can start a TELNET session such as "telnet 127.0.0.1 6666" to connect to the TELNET server on foo.acme.com.
2. If source ip = 127.0.0.2, source port = 6667, destination host = foo.acme.com and destination port = 80 you can use "http://127.0.0.1:6667" in your browser to connect to the Web server on foo.acme.com.

If Alias support is activated your hosts files will be updated, e.g. if you specify source ip = 127.0.0.1, source port = 80, destination host = foo.acme.com and destination port = 80 then you can use "http://foo.acme.com" in your browser and traffic will be forwarded.

A new window will be opened if you hit the ENTER key (or the Start... button).

[HTTP Proxy Host]: (Leave empty to skip)

[HTTP Proxy Port]: (Leave empty to skip)

Mode	Source IP	Port	Alias	Destination Host	Port
<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text" value="127.0.0.1"/>	<input type="text"/>	<input type="text"/>	> <input type="text"/>	<input type="text"/>

Start... Add

Klar Internet

Access to Outlook Express example

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

The following information should be supplied:

- 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).

Users who are working from a location requiring traffic to pass through an *intermediate* HTTP Proxy server should enter the IP address (or domain name) and port of that proxy server. All applet traffic will thus be tunneled to the Contivity gateway via the HTTP proxy server. The HTTP Proxy server should have 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 will be 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, e.g 25 for SMTP.

- 5 Using the [Host Alias] box (optional) is explained on the next screen.
- 6 In the Destination Host field, enter the domain 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. Then enter a new port number in the Port field (for example, 5026). Finally enter the IP address or domain name to the SMTP server in the Destination Host field and the port to use in the Port field, in this case 25.

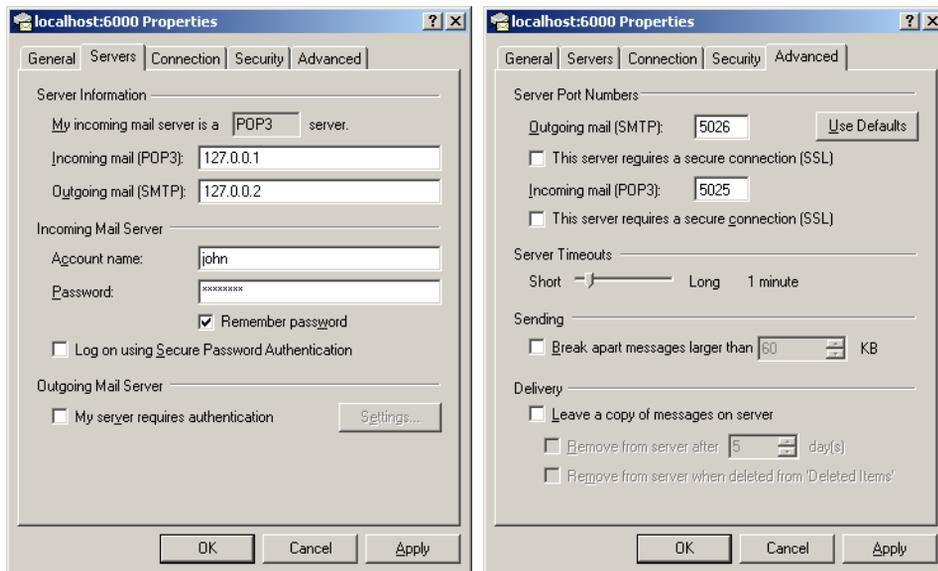
- 9 Click on Start.

You will be 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 you have established two connections, one to the POP3 server and one to the SMTP server. 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), existing port number settings in the mail client can be kept.

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 will automatically be mapped 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 will automatically be mapped 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 will automatically be mapped to the specified source IP.

Port forwarder links

To simplify access, custom port forwarder links can be defined on the Home tab by the Contivity gateway operator. A custom port forwarder link can be defined to launch the application automatically.

Native Outlook port forwarder

The Outlook port forwarder lets you start a native Outlook session to a specified Exchange server on the intranet. To start the Outlook port forwarder, you should select the Outlook option in the Port forwarder type box. This will display a different set of input fields.

Figure 14 Outlook port forwarder

Home Browse Intranet Files Full Access **Advanced** Logout

Telnet/SSHv1 Access HTTP Proxy **Port Forwarder**

Start Outlook Port Forwarder(s)

Port forwarder type: Outlook

From this page you can start an Outlook port forwarder.

Note: Your client machine must be setup to give write access to hosts and lmhosts files. Please contact your network/system operator if this is a problem.

Note: Your browser must support Java. If not download SUN's J2SE JRE from java.sun.com.

Note: If Internet Explorer has been configured to use a proxy server you **must** disable it before starting the Outlook client.

A new window will be opened if you hit the ENTER key (or the Start... button).

Start Outlook client

Source IP Exchange Server (FQDN)

127.0.0.1 >

Start... Add

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

- The Exchange server's domain name must be configured using the Server ID > DNS tab > Search List parameter. Using the above example, example.com should be entered in the Search list. If several Exchange servers are used, all the Exchange servers' domain names must be configured in the DNS search list.
- You must have administrator's rights on his/her 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 meant to be used by clients connecting to the Contivity 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.
- 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. 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 `NodeType` and enter 8 in the Value Data field. Click on OK and restart the computer.

- The Outlook port forwarder 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 (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 may 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/keep` command.

The following information should be supplied by you on the Port Forwarder tab:

- 1** Select the Start Outlook client check box if Microsoft Outlook should be started 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 domain 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) 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.

5 Click on Start.

You will be 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.

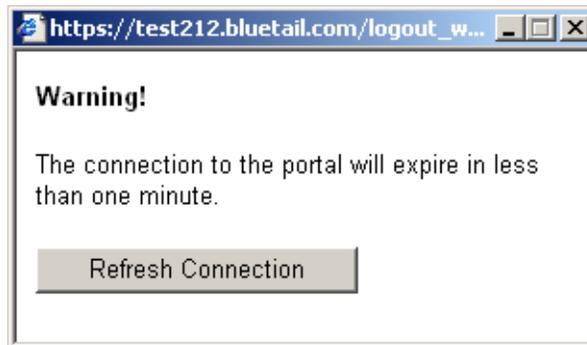


Note: You should not close the Java applet window as the last browser window, because the host's files may not be cleaned up properly.

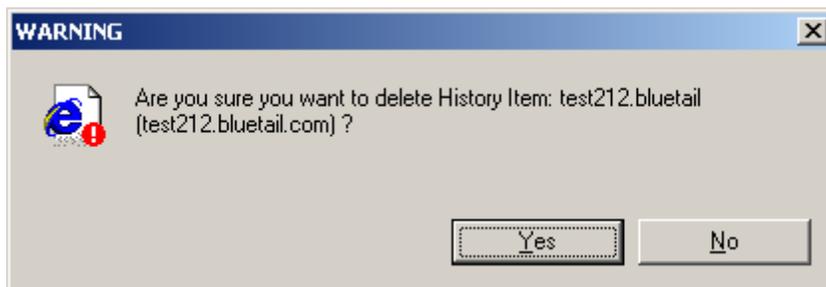
Logout tab

The Logout tab simply contains a button for you to confirm that he wishes to log out. However, you are logged out automatically after the time specified as Time To Live for the VPN domain, using the `/cfg/xnet/ttl` command.

One minute before you are automatically logged out, a message displays 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 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.

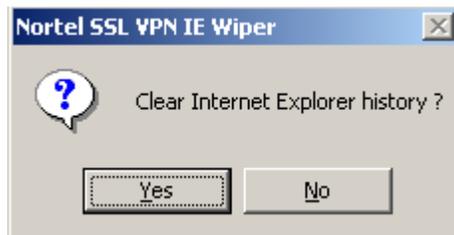
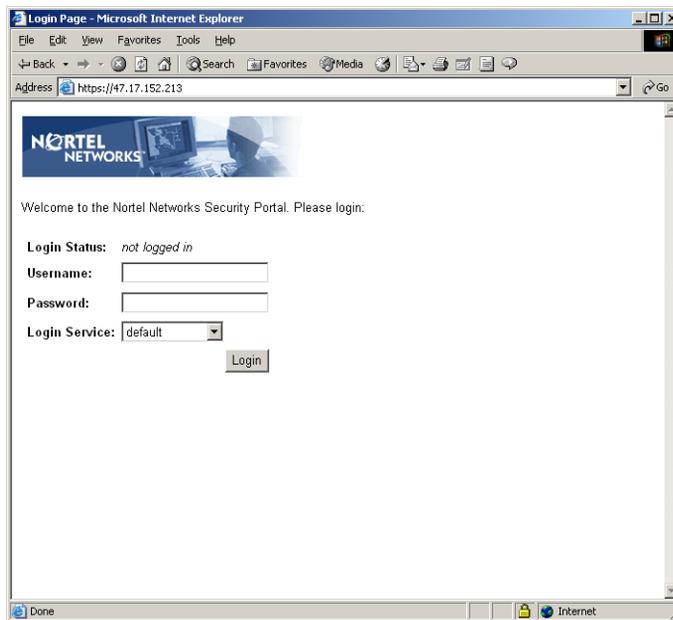
Figure 17 Clear browser history

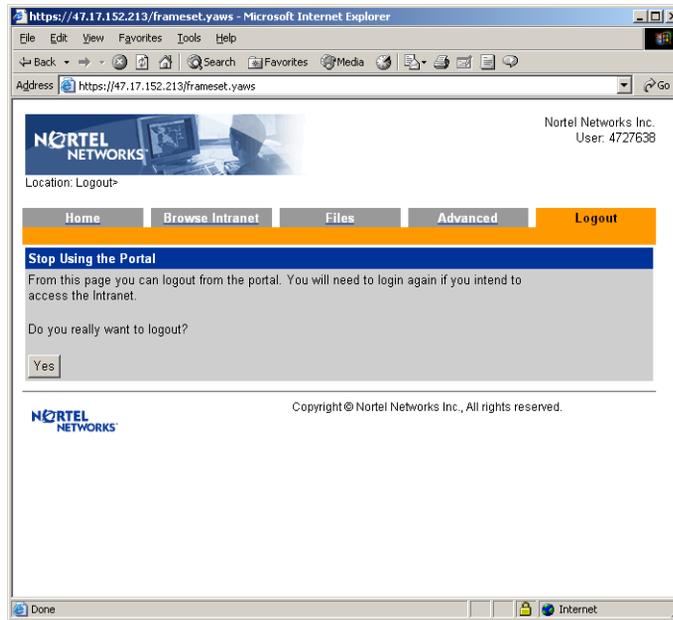
Figure 18 Portal login screen



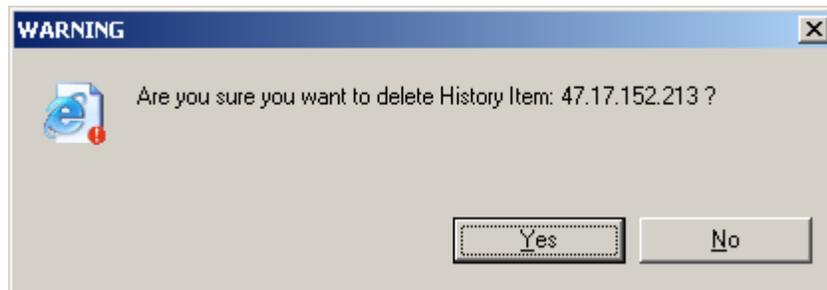
- 9 Use a known user name and password as configured on the Contivity gateway for login. This works because you have created mirrored SSL VPN groups from the Contivity groups using the wizard earlier.

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

- 10 A successful login brings up the portal home page. Although you still need to add links to the portal tabs, you have established working SSL VPN access and 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). 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/disallow services for different groups or add some links. The test Certificate should be substituted for a real certificate, signed by a CA Authority at this point.

Using the Domain Quick Wizard

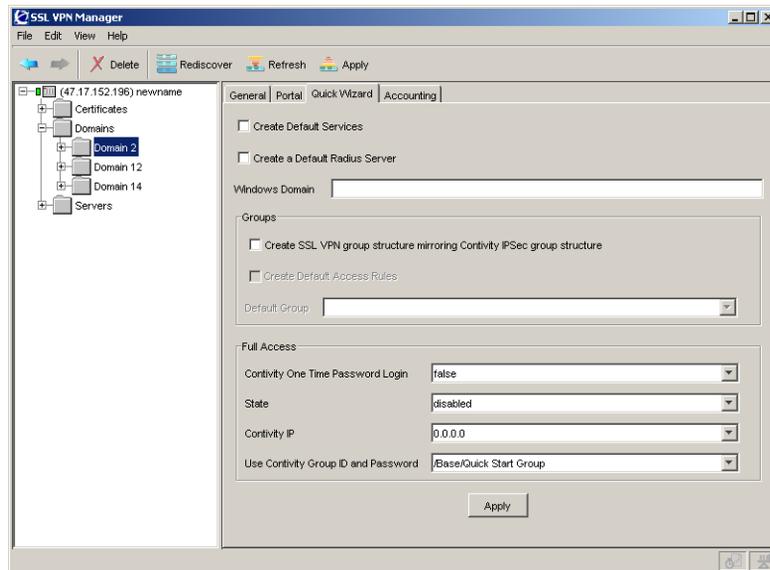
The domain quick wizard can be used to quickly configure all of the aspects of a domain that are relevant to most SSL VPN administrators. The advantages of using the Quick Wizard rather than manually configuring a domain are:

- 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 domain 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 the Quick Wizard tab (Figure 21).

Figure 21 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.

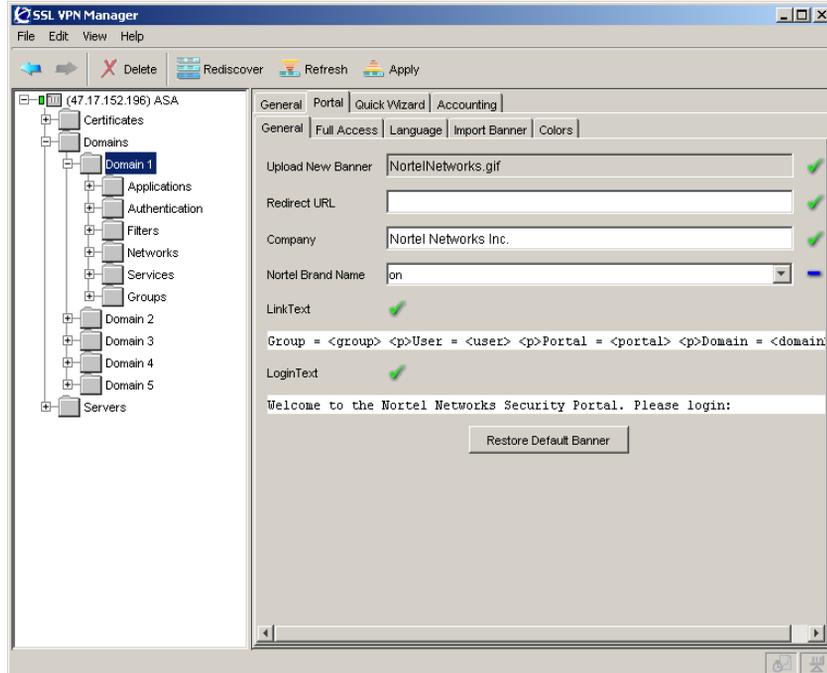
Customizing the portal

These sections explain how to customize the portal logo, company name, color, static link text and language version.

Using the General tab

Select the Domain ID > Portal > General tab (Figure 22) to customize the portal appearance to be applied to the selected domain.

Figure 22 Customize portal

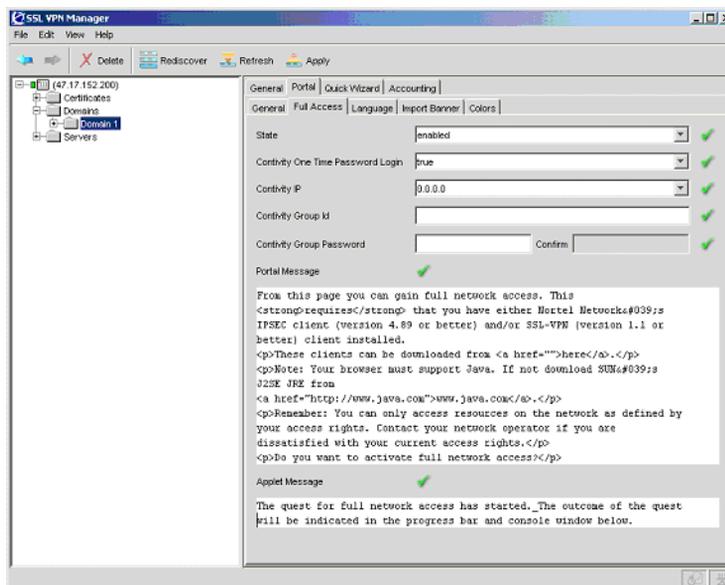


Configuring portal full access

The Portal 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 displayed on the portal.

To enable full access:

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

Figure 23 Full Access tab

2 Configure the Contivity One Time Password

The Contivity gateway one-time password is an authentication method that you can use to launch the Contivity VPN Client with a temporary user ID. It is primarily intended to be used when certificate or SecurID tokens are used to log in to the SSL Portal. One-time password allows the Contivity VPN Client to launch 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 also need to 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 will not work when the One Time Password option is enabled. Because of these limitations, Nortel Networks recommends that you use one-time password only when using certificates or SecurID tokens for the SSL portal login.

3 Set the Contivity gateway IP address.

The Contivity gateway IP address determines what address the Contivity VPN Client will connect 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 will connect to the same address as the one used for the portal.

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

4 Set the group ID and password.

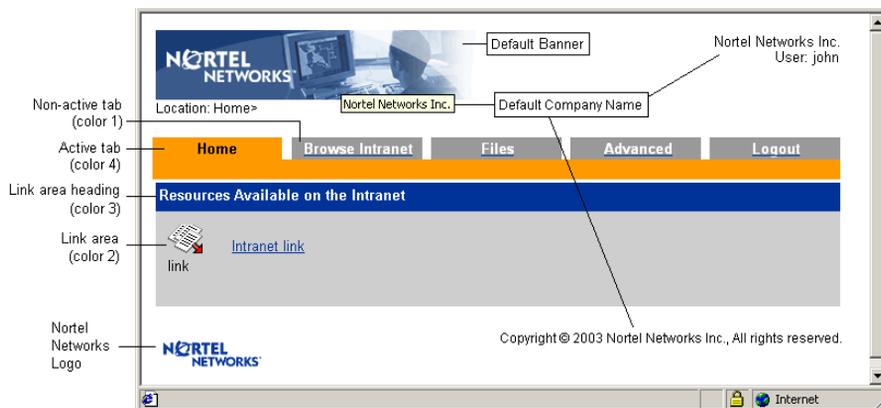
These should be set only if the Contivity VPN Client needs to perform a Radius Group authentication before logging in with your name and password. If the Contivity VPN Client should perform a straight username/password login, these should be left blank. If the One Time Password option is enabled, the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

5 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 will initially display as it starts the Contivity VPN Client.

Default appearance

The default appearance of the portal is displayed in [Figure 24](#).

Figure 24 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” and you will get access to 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

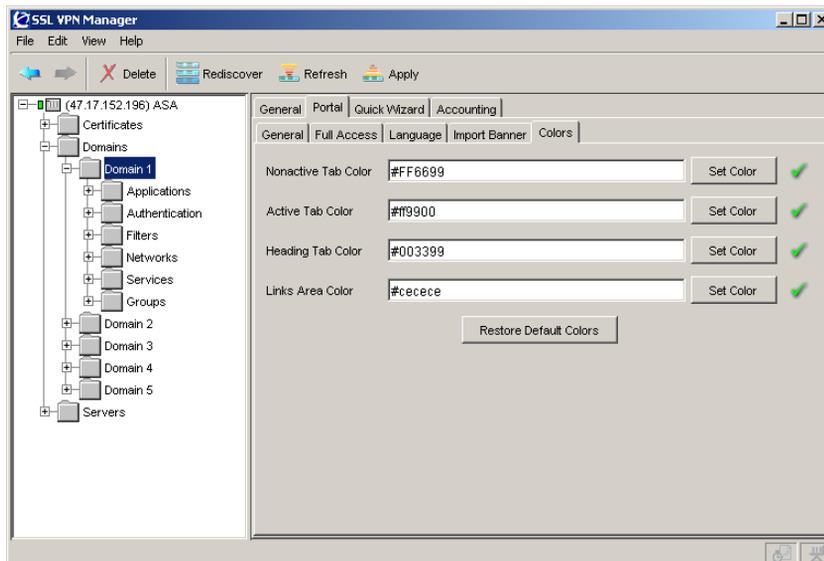
Changing colors

To change the portal colors ([Figure 25](#)):

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

- 2 Select the Portal tab.
- 3 Select the Colors tab.

Figure 25 Change colors

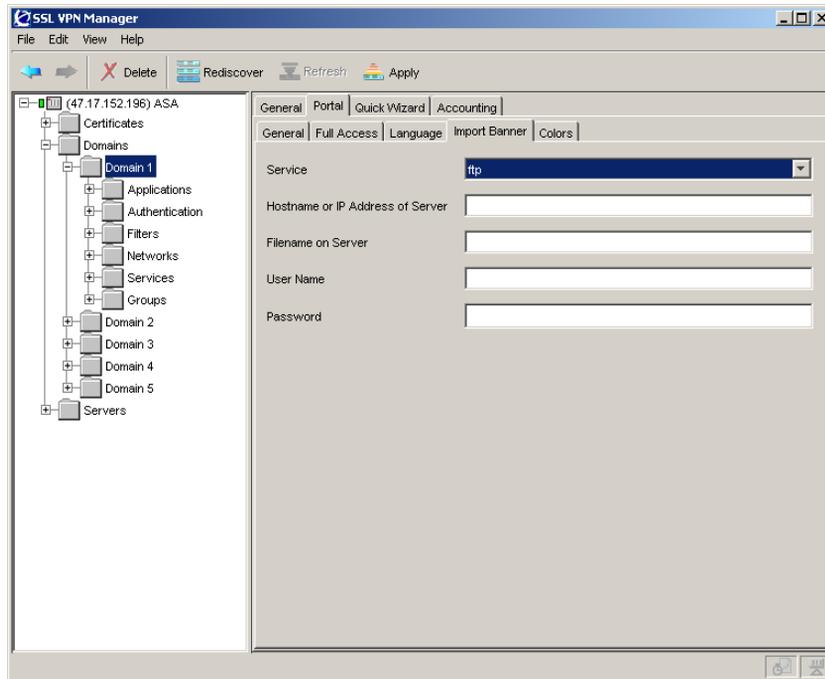


- 4 Configure the colors as desired and click the Set Color buttons to make the changes.

Changing banner images

To substitute the Nortel Networks banner image for your own company banner (Figure 26), make the desired image file (in .gif format) available on a TFTP or FTP server. Then proceed as follows:

- 1 Select the Domain ID for which you wish to change the logo.
- 2 Select the Portal tab.
- 3 Select the Import Banner tab.

Figure 26 Change banner

- 4 Configure the parameters described below on the Import Banner tab.
 - a Specify the service to use, such as FTP.
 - b Enter the DNS host name or IP address of the server.
 - c Specify the filename of the file to be uploaded from the server.
 - d Enter the user name.
 - e Enter the password.

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 will 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 Domain ID 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 Networks logo displayed at the bottom left on the portal, proceed as follows:

- 1 Select the Domain ID 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 Domain ID 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 27](#)), connect to the portal by entering the VPN domain name in your browser. The default logo will be replaced on the Login screen as well as on the portal.

Figure 27 Verify changes

After login, the portal is displayed with a new logo, company name, static link text and color (Figure 28).

Naming login services

To support redirection to a specific authentication server, such as token login or redirection to a specific Windows domain, you can 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 28 Updated view

Automatic redirection to internal site

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

- 1 Select the Domain ID 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.

For the visitor to be able to log out from the portal from the internal site, a logout link should be inserted 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 Domain ID 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.

For the visitor to be able to log out from the portal from the internal site, a logout link should be inserted on that screen.



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

Chapter 3

Initial configuration

This chapter provides information about SSL VPN Module 1000 initialization and initial configuration.

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 mis-configuration occurs, the SSL device always takes priority; therefore you will no longer be able to manage the Contivity gateway using SSL from the public interface. Nortel Networks 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 need to use a CLIP address.
- If you are using interface filters, you should set all private interfaces to Permit All.
- When configured, the physical private interface of the Contivity gateway has four IP addresses assigned to it as follows:
 - Contivity management IP address

- Contivity interface IP address
- SSL management IP address
- SSL interface IP address
- If the SSL VPN time zone does not match the Contivity time zone and you see errors, you may need to specifically set the time zone to the correct one.

Initializing SSL VPN Module 1000

Before you configure the SSL VPN Module 1000, you must initialize it to ensure that the Contivity gateway can communicate with it.

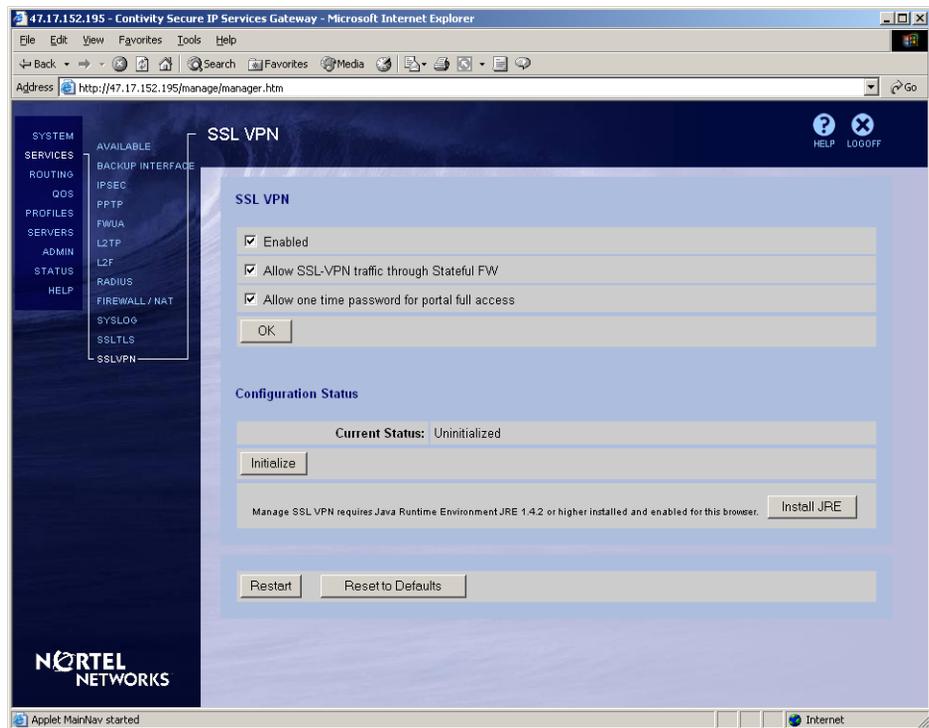


Note: The SSL VPN card takes time rebooting for it to reach operational status.

To initialize the SSL VPN Module 1000:

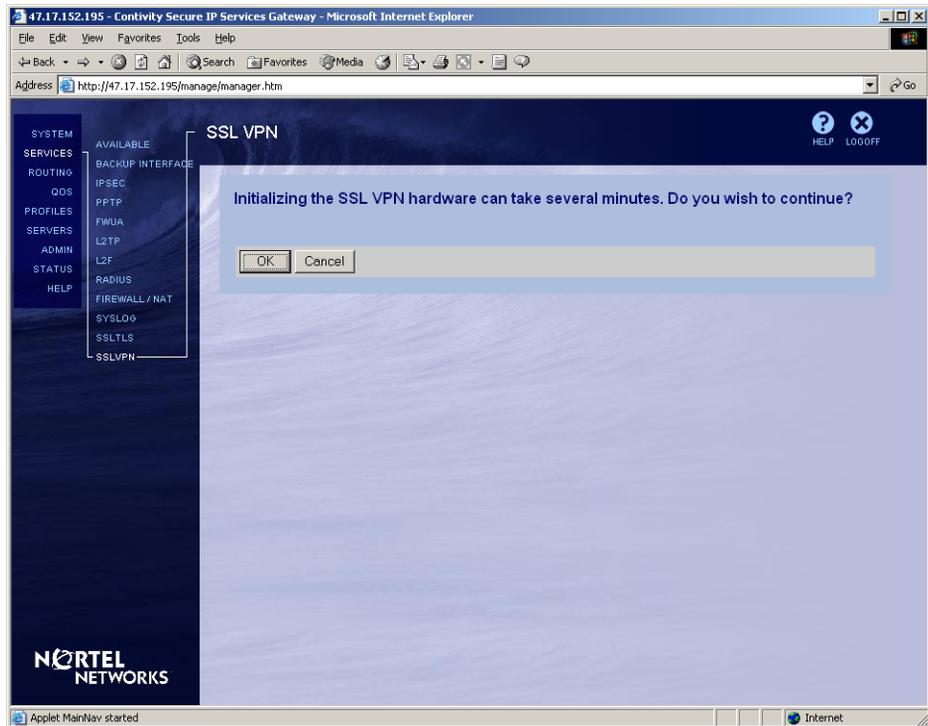
- 1 Log in to the Contivity gateway.
- 2 Select Services > SSL VPN.

Figure 29 SSL VPN screen

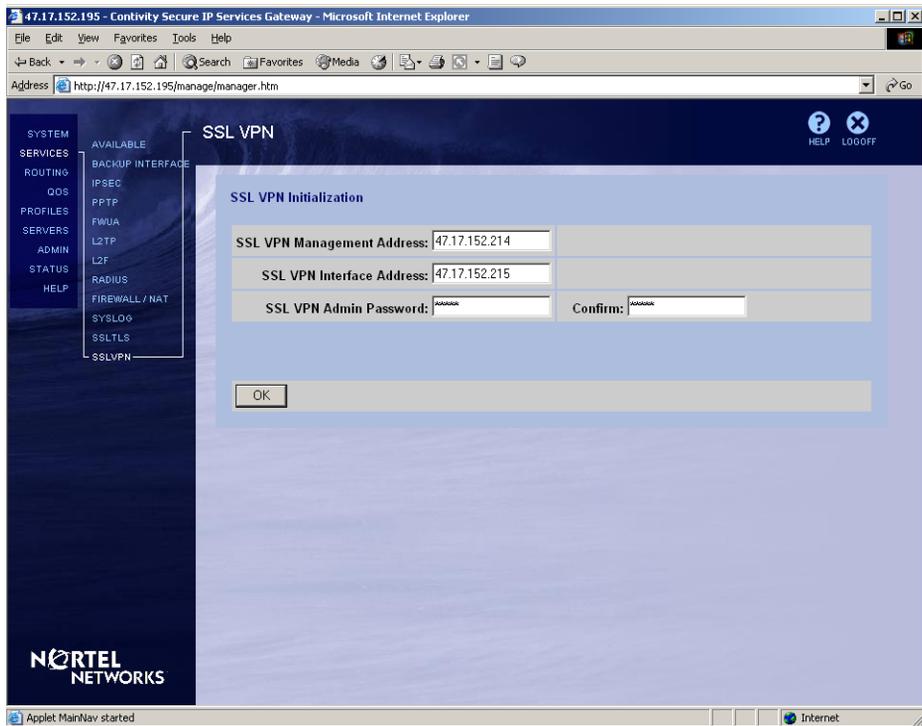


- 3 Click on Initialize in the Configuration Status section of the screen. The next screen advises you of the time it may take to initialize the hardware.

Figure 30 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 31 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. It also must 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. It also must be within the management subnet as defined on the Contivity gateway.

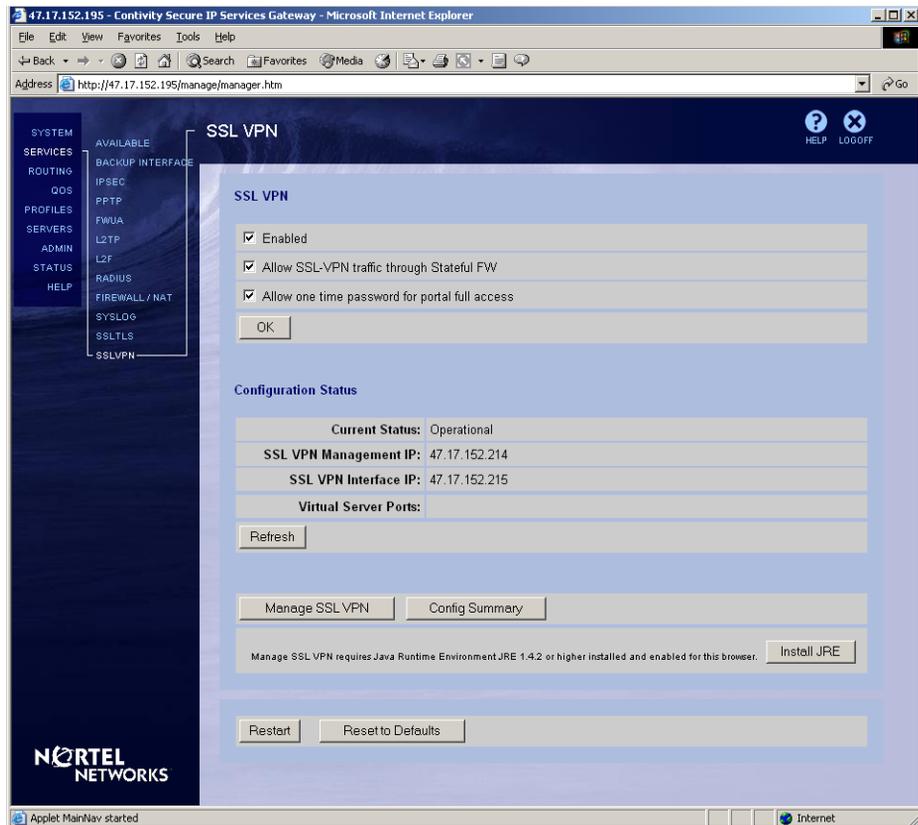
- SSL VPN admin password

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

- 7 Click on OK. It could take approximately a minute or more to complete the initialization.

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

Figure 32 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, you must 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 33) 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.
 - c The Contivity gateway has DNS Proxy enabled in the DNS Server Configuration section of the screen.

Figure 33 System Identity screen

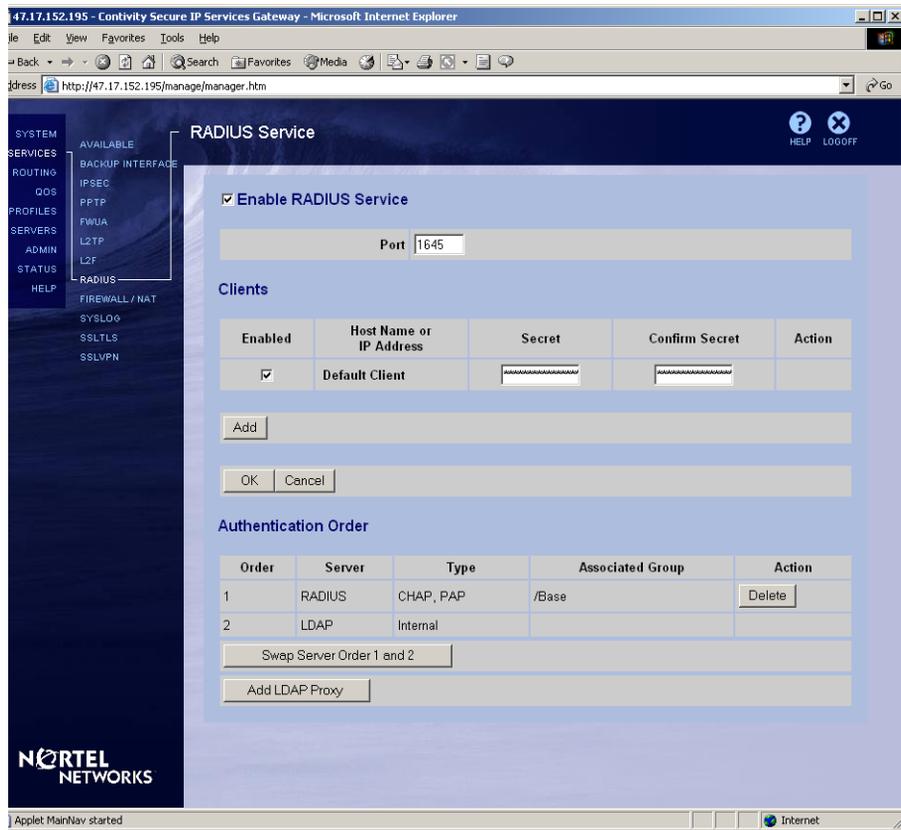
The screenshot shows the 'System Identity' configuration page in a web browser. The browser address bar shows 'http://47.17.152.195/manage/manager.htm'. The page has a dark blue sidebar with a menu including SYSTEM, SERVICES, ROUTING, QOS, PROFILES, SERVERS, ADMIN, STATUS, HELP, SETTINGS, and FORWARDING. The main content area is titled 'System Identity' and contains the following sections:

- Management IP Address:** 47.17.152.195 (Web Management, FTP, etc. Subnet:255.255.255.224)
- Domain Identity:**
 - DNS Host Name: [Empty field]
 - DNS Domain Name: [Empty field]
- DNS Server Configuration:**
 - DNS Proxy: ENABLED
 - Split DNS: ENABLED
 - Primary: 47.16.1.20 (Operational)
 - Second Server: 0.0.0.0 (*Optional) (Server not configured)
 - Third Server: 0.0.0.0 (*Optional) (Server not configured)
 - Fourth Server: 0.0.0.0 (*Optional) (Server not configured)
- ISP Provided DNS Servers:** No Provided Servers

At the bottom of the form are buttons for 'OK', 'Cancel', and 'Refresh'. The Nortel Networks logo is visible in the bottom left corner of the page.

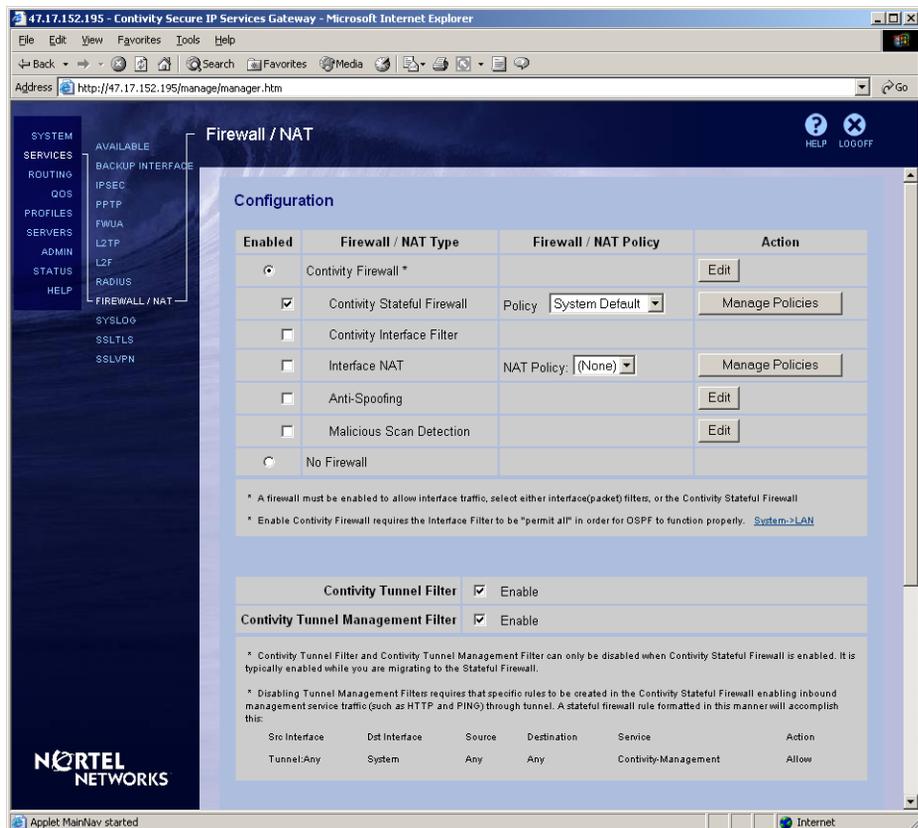
- 2 Select Services > RADIUS to enable RADIUS Service (Figure 34). Enable the default client and enter a shared secret. Set the Authentication order to match how you are authenticating Contivity users.

Figure 34 RADIUS Service screen



3 Select Services > Firewall/NAT in the Contivity Web interface (Figure 35).

Figure 35 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, then implied rules will automatically be added giving the SSL VPN the access it needs. When you enable either type of firewall for the first time, you need to reboot. If you must reboot, continue with the next step after restart.
- 5 Go to Services > SSLVPN and check to be sure that the status is “Operational”.

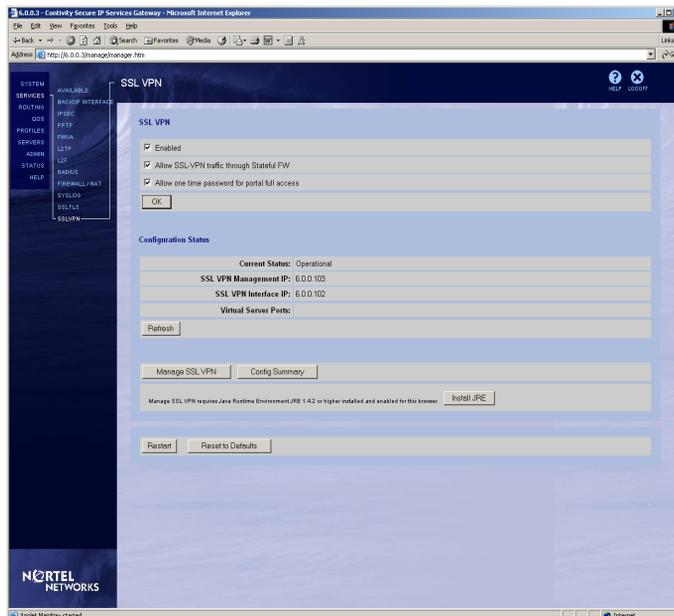
SSL VPN and Contivity Stateful Firewall

The SSL VPN fully integrates with the Contivity Stateful Firewall, and access can be permitted/denied via 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 36) and uncheck the option Allow SSL-VPN traffic through Stateful FW.

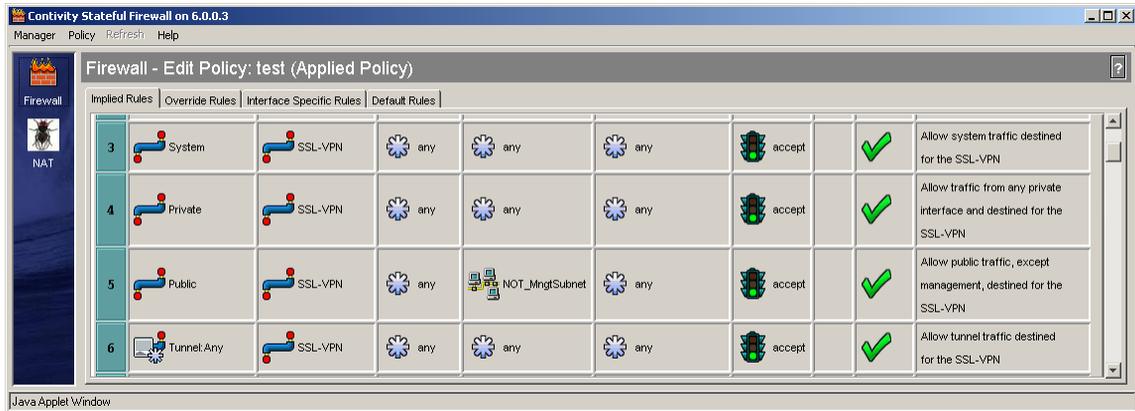
Figure 36 CSF configuration example



The difference between these settings is this:

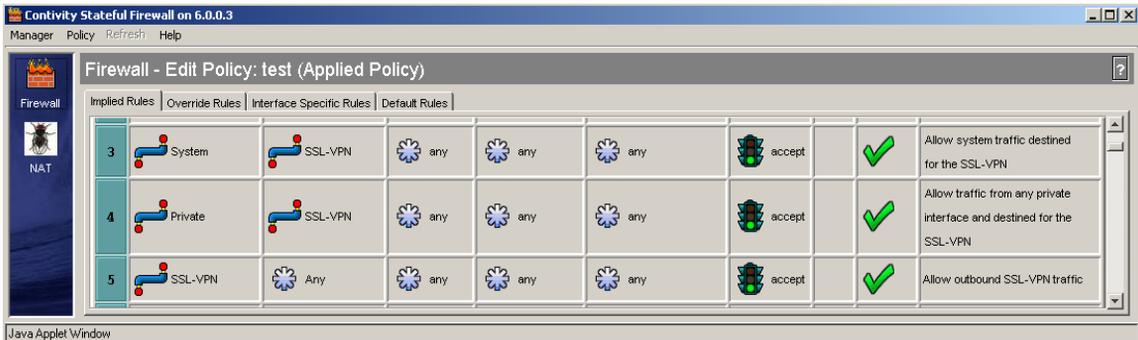
- When you check Allow SSL-VPN traffic through Stateful FW in configuration 1, it allows ALL traffic from the public side of the Contivity gateway to access the SSL device. This inserts an implied rule into the firewall.

Figure 37 Insert firewall implied rule



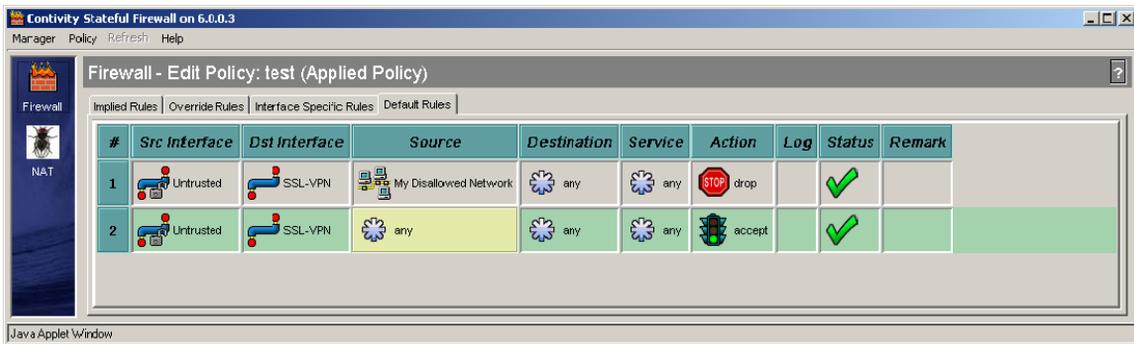
- If you uncheck Allow SSL-VPN traffic through Stateful FW in configuration 2, it does not insert any implied rules (except those required to manage the SSL device and for the SSL device to send to the public).

Figure 38 Do not insert firewall implied rule



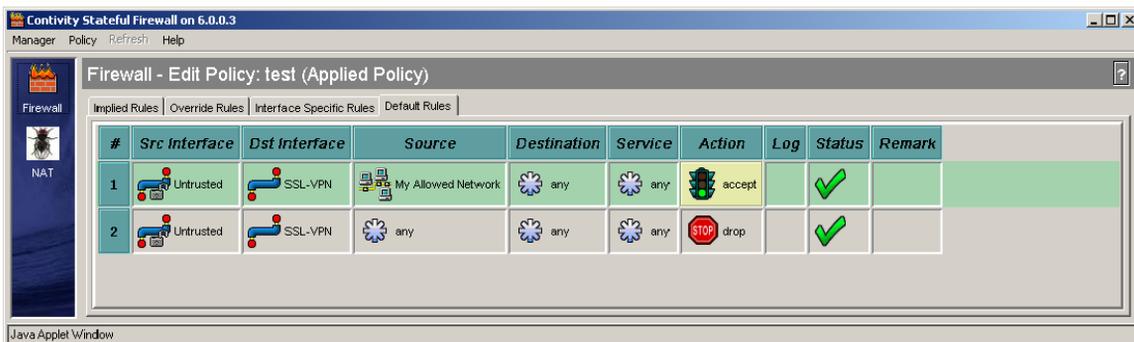
The second configuration allows the administrator to control access to the SSL VPN within the firewall. For example, if you are using the system default policy (Deny All), the first configuration allows SSL through because the implied rules override all other rules.

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 39 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 40 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.

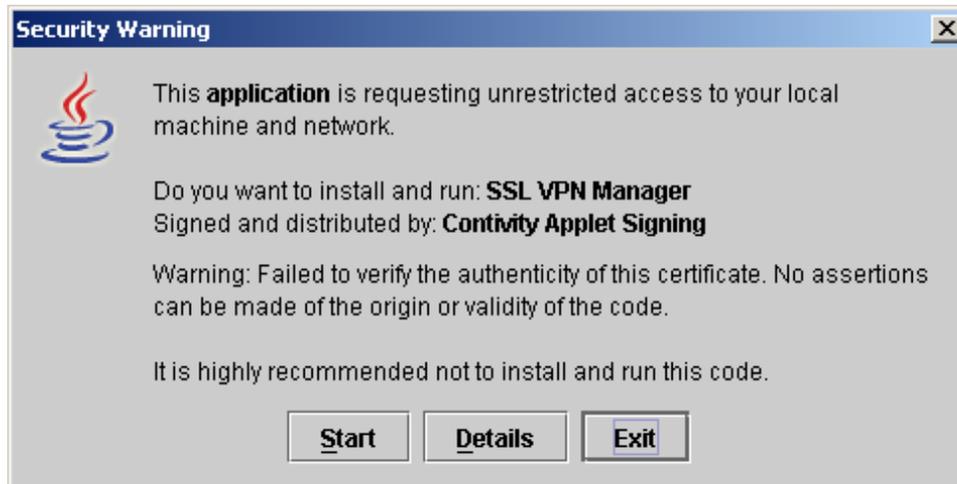
Installing JRE 1.4.2

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 41). You must accept the certificate to proceed with the installation.

Figure 41 JRE certificate



SSL VPN manager login

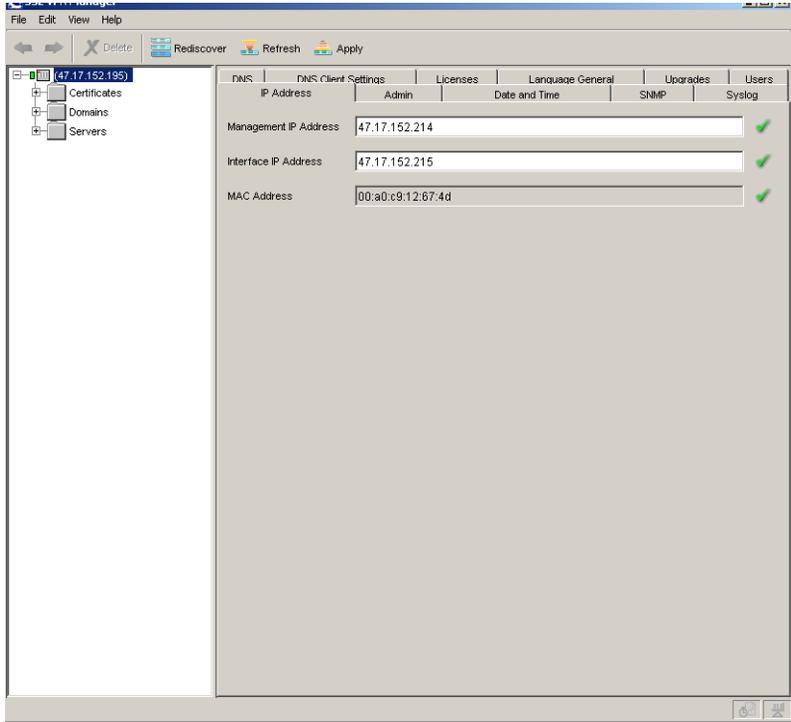
The login screen (Figure 42) appears when you launch the SSL VPN manager applet. Log in with a valid Contivity Administrator username and password. When you log in, the applet launches and discovers the SSL VPN Module 1000 device.

Figure 42 SSL VPN manager login

A login dialog box titled "Login" with a question mark icon. It contains two input fields: "Username" and "Password". Below the fields are "OK" and "Cancel" buttons.

Configuring SSL VPN system settings

The SSL VPN manager screen (Figure 43) appears in a new SSL VPN installation when the SSL VPN Module 1000 is discovered.

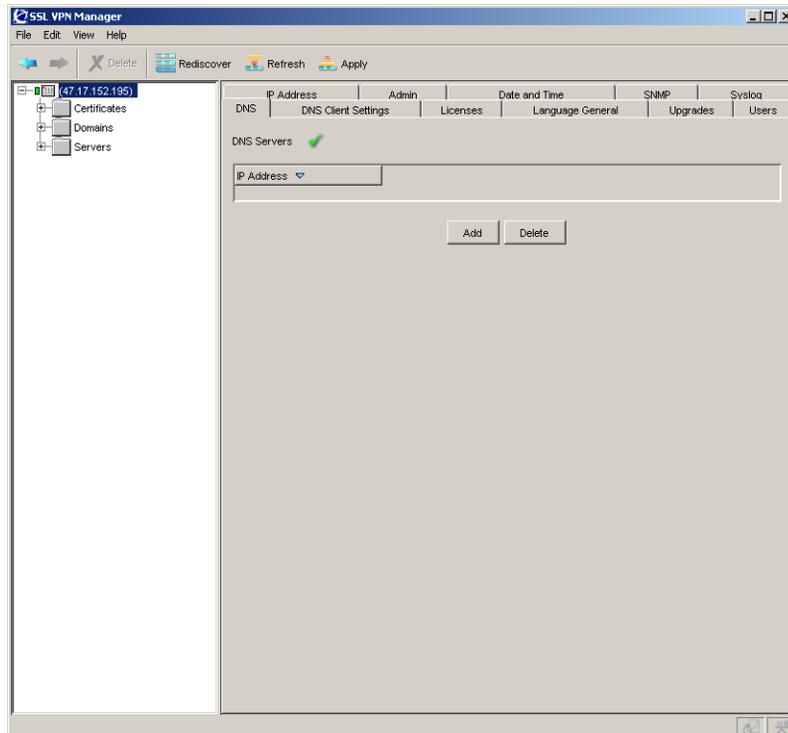
Figure 43 New SSL VPN installation screen

The "New SSL VPN installation screen" shows a configuration window with a tree view on the left and a configuration table on the right. The tree view includes "Certificates", "Domains", and "Servers". The configuration table has columns for "DNS", "DNS Client Settings", "Licenses", "Language General", "Upgrades", and "Users". The table contains the following data:

DNS	DNS Client Settings	Licenses	Language General	Upgrades	Users
IP Address	Admin	Date and Time	SNMP	Syslog	
Management IP Address	47.17.152.214				✓
Interface IP Address	47.17.152.215				✓
MAC Address	00:a0:c9:12:67:4d				✓

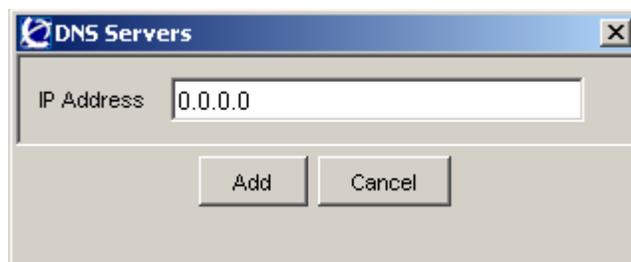
- 1 The root of the menu will show the IP address or host name of your Contivity Management IP address. Below this, there are 3 submenu items. To expand all menu items, click on the + sign.
- 2 Ensure that the Device IPAddress/Hostname is selected at the root of the menu tree. In the right-hand pane, click on the DNS tab ([Figure 44](#)).

Figure 44 DNS tab



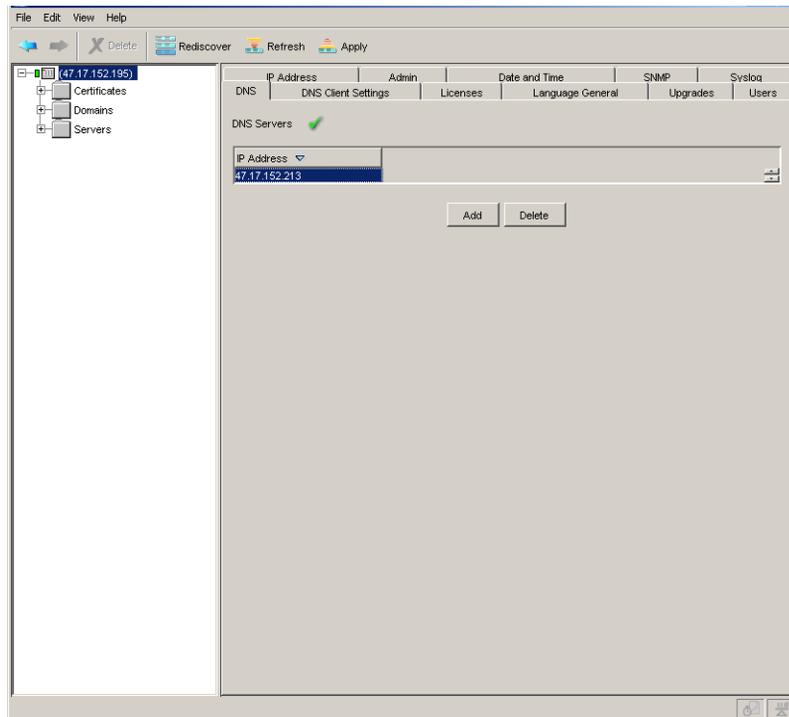
- 3 Click on Add. The DNS Servers IP address screen appears ([Figure 45](#)).

Figure 45 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 46](#) shows the DNS server added in the SSL VPN manager.

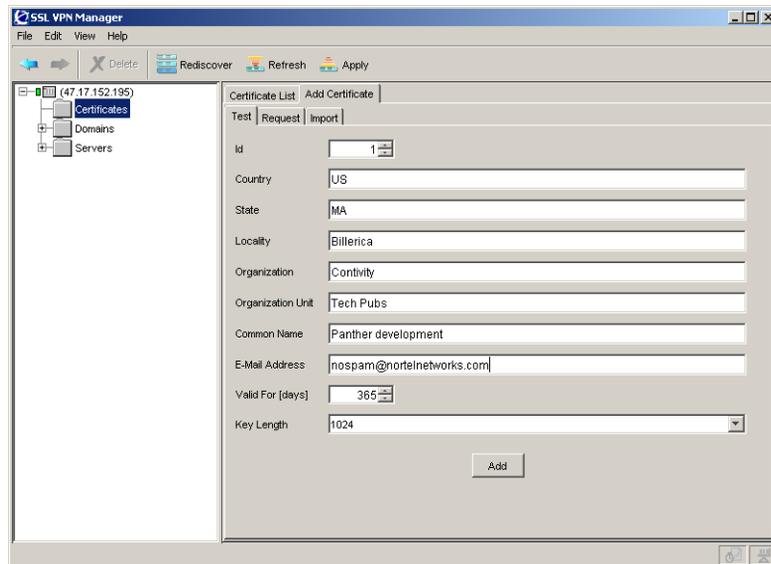
Figure 46 DNS server added



- 5 Use a test certificate to make the SSL VPN portal operational. Select Certificates in the menu.
- 6 Select the Add Certificate tab ([Figure 47](#)). The Test tab appears beneath the Add Certificate tab.

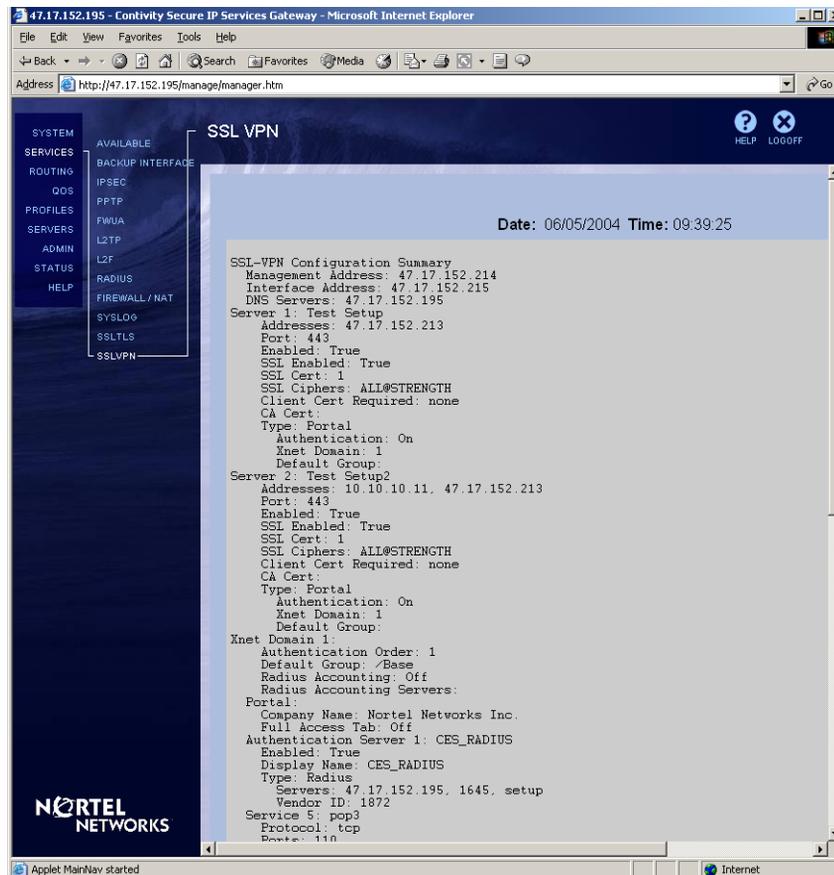


Note: You should replace the test certificate with a valid certificate before deploying the SSL VPN.

Figure 47 Add certificates

- 7** Fill out the details for the certificate and use the fully qualified domain name of the Contivity gateway for the Common Name.
- 8** Click on Add.
- 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 48 Review setup



Upgrading the software

The SSL VPN software image is the executable code running on the SSL VPN Module 1000. 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

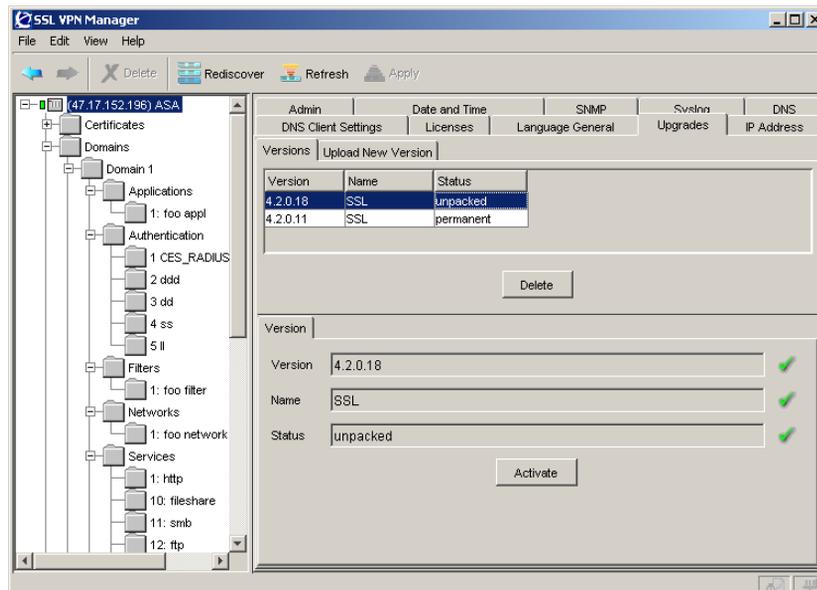
This type of release may contain bug fixes as well as feature enhancements. The SSL VPN Module 1000 may automatically reboot after a major upgrade, because the operating system may have been enhanced with new features. All configuration data is retained.

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 (Figure 49).

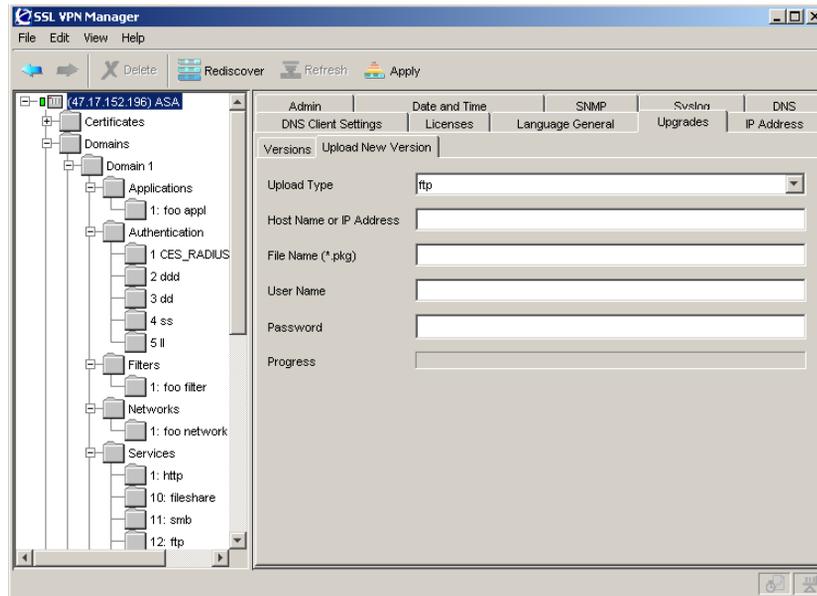
Figure 49 Upgrades



- 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 50), browse to the location of the .pkg file, and click on Apply.

Figure 50 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:

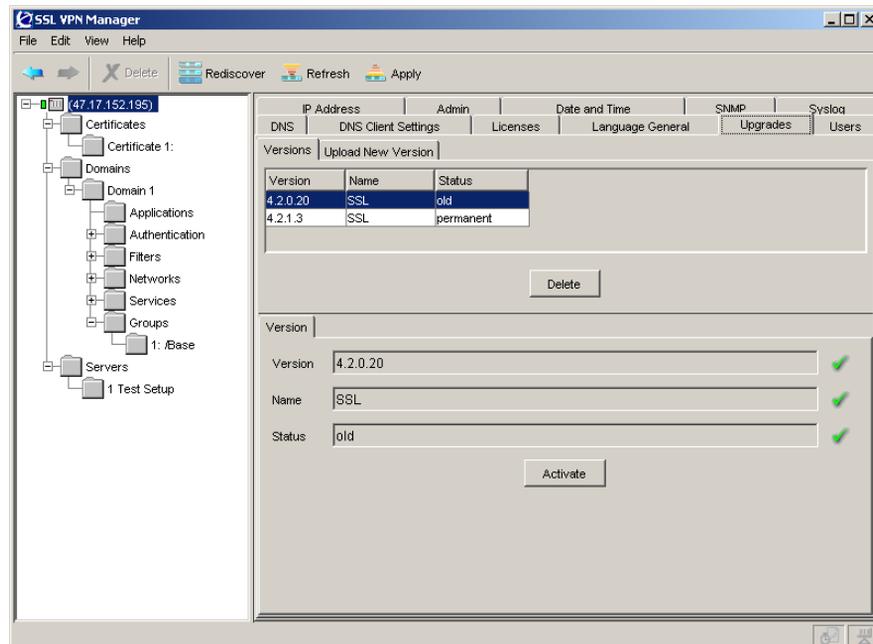
- *unpacked* means that the software upgrade package has been downloaded and automatically decompressed.

- 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 51).

Figure 51 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 > 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 domain 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 domain 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 the Generate PKCS# Request box 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 the Certificate and click on the 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+jCCAAMCAQAwwZQxCzAJBgNVBAYTA1NFMRIWEAYDVQQIEw1TdG9ja2hvbG0x
DjAMBgNVBAcTBUp3c3RhMREwDwYDVQQKEWhCbHVldGFpbDENMAsGA1UECXMERG9j
dTEZMBcGA1UEAxMQd3d3LmJsdWV0YWlsLmNvbTEkMCIGCSqGSIb3DQEJARYVdG9y
Ympvcn5AYmx1ZXRhaWwuy29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCX
2rSY81cgKJODuUreGF3ZnK7Rv1RqSV/TIMS4UerqXPkPtj fMAWdjBG77hjIAOOZO
FQKFB5x/Zs9kNMBUmPBokA1/GXghomOvBhMIJBZBiUVtJNGmv2sjeqNXxsUg5XfJ
iwV2LjUvW65EzCLpq5dhq6ZPEX7tAgqB2Wgu8MolwQIDAQABoCUwIwYJKoZiHvcN
AQkHMRyTFEEgY2hhbGxlbmdlIHhbc3N3b3JkMA0GCSqGSIb3DQEBAUAA4GBACem
SJr8Xuk9PQZPuIPV7iCDG+eWneU3HH3F3DigW3MILCLNqweljKw5pZdAr9HbDwU+
2iQGbtSH0nVeoqn4TJujq96XpIrbIAfDE1tR7Lmf6oGdrwG8ypfRpp3PmfId6lp+
HJ2fUGliPYyNtd/94AL6wW8un208+icCHq/S0yjjz
-----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 well 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 the import 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 91](#).
- 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.

Updating DNS servers

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

To create a VPN domain:

- 1** Create an Xnet (VPN) domain.

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

For each VPN domain, you should also configure the 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 domain.

- 2** Apply your changes.

Chapter 4

Configuring domains

This chapter describes the various aspects of configuring SSL VPN domains. Every virtual server configured as type Portal, HTTP, or SOCKS will need to have a domain associated with it. Domains 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. In general terms, domain configuration can be thought of as encompassing the following four areas:

- 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 via the SSL-VPN that is using this particular domain for authentication.
 - The User Type is one of <Advanced, Medium, Novice> and determines what tabs are displayed for Portal servers.
 - Full Access, if enabled for that particular domain, 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 domain.
- Front end requirements: Every domain 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.

- Authentication

Every domain 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 domain, and an authentication order established. Single Sign On (SSO) Domains can be established such that back end server authentication requests are automatically handled without credential input from the user.

- Accounting

RADIUS accounting is available.

- Common portal settings

There are several portal configuration items that are associated with the domain, so that all portals that use that particular domain will have them in common. These include banners, a redirect URL, Citrix support, login and link text, and a complete full-access control mechanism. Configuration items unique to a particular server are configured for that server alone (server specific configuration is covered in chapter 5).

Configuring authorization

Authorization control mechanisms can generally be 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 group structure mirrors the group structure of the Contivity gateway. If you used the domain 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 domain using the Domain ID > Groups > Add Group tab. Every domain 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 should 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.

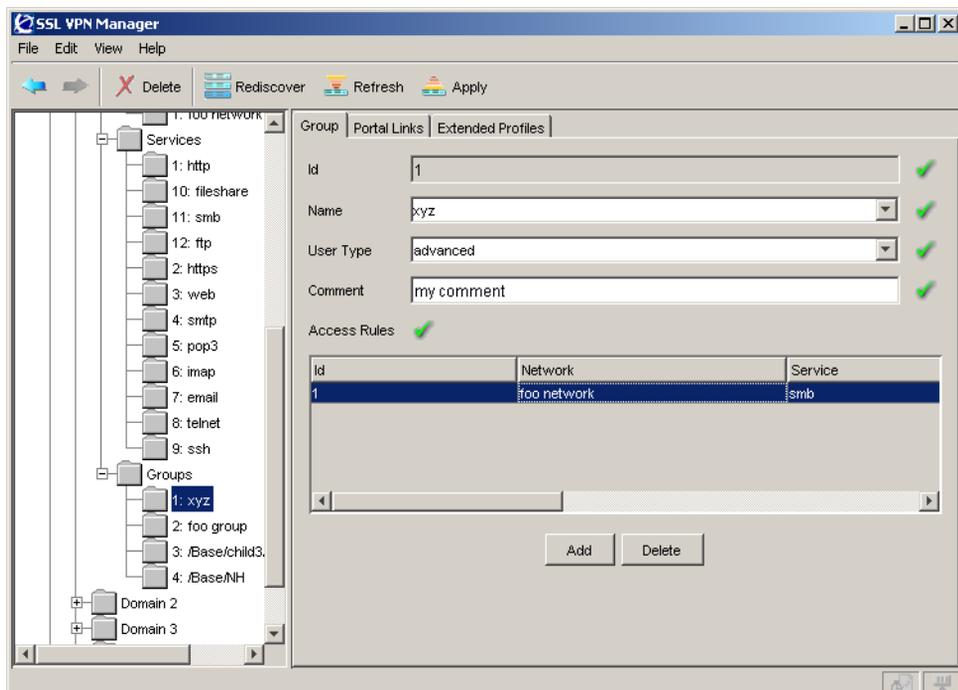
The extended profile's access rules are executed prior to those of the base profile. This means that if a matching extended profile is found (for example, the profile's client filter matches the user's source network), and a match is found in any of the profile's access rules (the access rule's network 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 52](#) shows an access rule defined for a group.

Figure 52 Group access rules



Access rules configuration

You add and edit access rules from the Groups tab, using the Access Rules screen in [Figure 53](#).

Figure 53 Access rules

The image shows a dialog box titled "Access Rules" with a close button in the top right corner. The dialog contains several fields: "Id" is a numeric spinner box set to "1"; "Network" is a dropdown menu with "foo network" selected; "Service" is a dropdown menu with "smb" selected; "Application" is a dropdown menu with "foo appl" selected; "Action" is a dropdown menu with "reject" selected; and "Comment" is an empty text input field. At the bottom of the dialog are two buttons: "Add" and "Cancel".

Each access rule defines:

- Access rule ID
- A network
- An application
- A service
- An 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 domain to which you want to add the service definition by selecting Domains > Domain ID > Services, where Domain ID is the desired domain.
- 2 Specify a service name and allowed port numbers.
- 3 Apply the changes.



Note: If you ran the Domains > Domain ID > Quick Wizard with the option Create Default Services, then 10 services have already been defined within the domain 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.

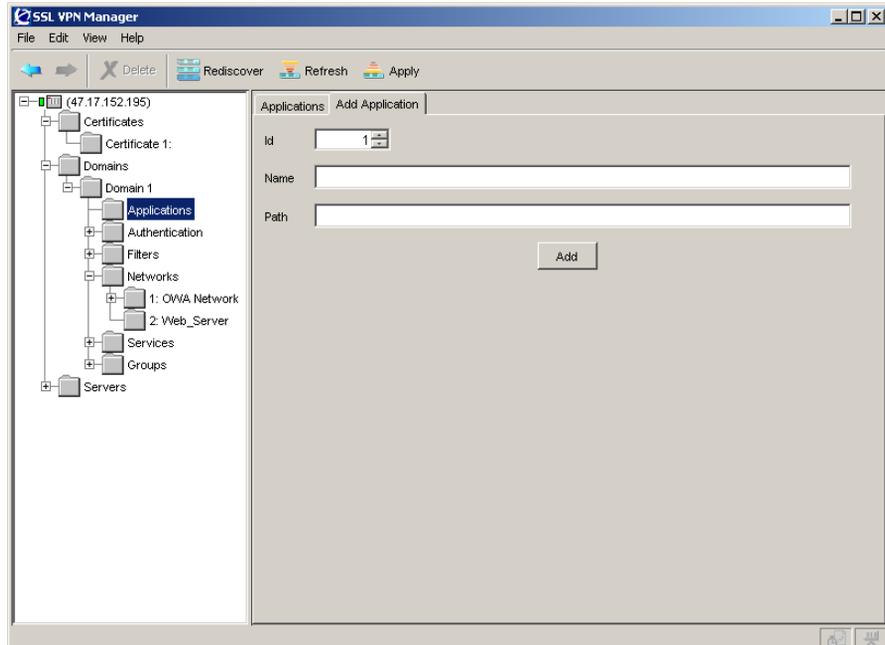
The path setting is checked for the following protocols: HTTP, HTTPS, FTP and SMB (Windows file share). The syntax for entering the path is shown below:

- 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/domain.
- 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 Domains > Domain ID > Applications > Add Application tab (Figure 54).

Figure 54 Add application



- 2 Specify a name for the application definition and enter the desired path.
- 3 Apply the changes.
- 4 This application will now be 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.

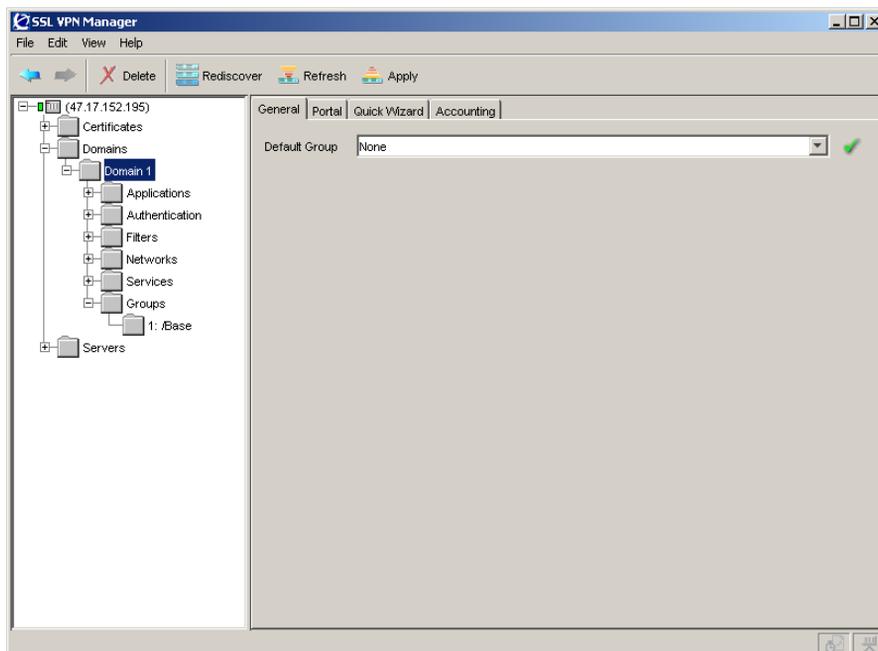
The highest user type assigned to the user group's extended profile and base profile will be applied. This means that if the extended profile has the *novice* user type assigned to it and the base profile uses the *advanced* user type, the *advanced* user type will be applied; for example, all of the portal's tabs will be 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 domain.

To configure default groups for each domain, use the Domains > Domain ID > General tab (Figure 55).

Figure 55 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 will be 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 will be 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 will be 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 will first check 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 will be 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 should be 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) will be applied. Data defined for the base profile will be 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 will be applied.

Defining Portal Links

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

The links you create are automatically associated with the selected group (and domain). Only users who are members of the selected group (identified by the group ID) will have access to the links you create within the group. Also, you must make sure that access to the resource provided via 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. Which links are displayed for the logged-on user depends on the user's group membership.

Any hypertext links configured for the group will appear on the portal's Home tab when a group member is logged in. Examples are links to intranet Web or mail servers. Make sure the links defined for the group are not contradicted by the access rules specified for the group.

The following link types are available:

- **SMB**. Gives the user access to folders on an 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 via the Contivity gateway) to Web page. Suitable for internal Web pages.
- **Eauto**. Automatic login link (direct) to password-protected Web page.
- **Iauto**. Automatic login link (secured via the Contivity gateway) to password-protected Web page.
- **Terminal**. Link to terminal server via Java applet for Telnet or SSH connections.
- **Proxy**. Link for accessing Web pages via 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).
- **Citrix.** Port forwarder link to Citrix Metaframe server.
- **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.”](#)

Full access

The full access tab provides a way for the remote user to launch the Contivity VPN client from within the portal. Just as when the user starts a VPN client manually, transparent access to the intranet is enabled and no further login to the VPN domain 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 54](#) 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 domain. Filters are defined (created) under Domains > Filters, and require the definition of a network from which the SSL VPN user originated from. Multiple filters can be created for a domain; all matching filters are applied to incoming SSL VPN user traffic.

Filters identify the following:

- Source network (such as a branch office)

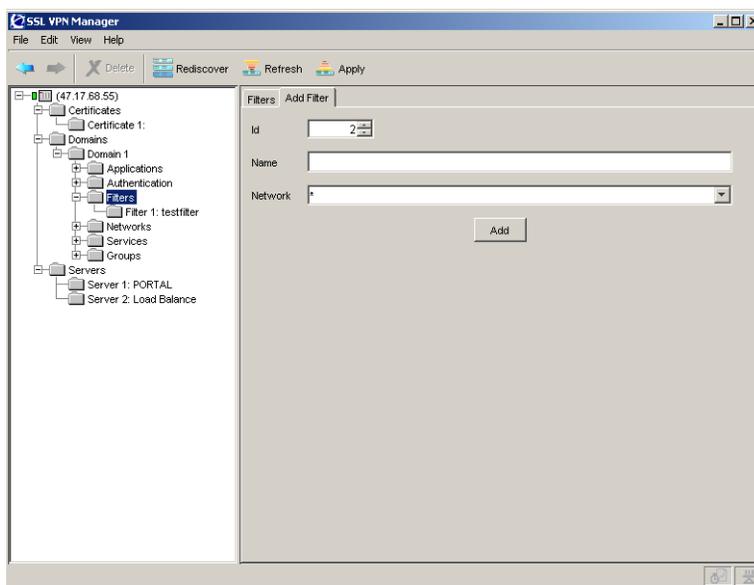
- Authentication method (such as RADIUS)
- If a client certificate is installed on the remote user's machine
- If the IE cache wiper is installed on the remote user's machine
- User type

Defining client filters

To define client filters:

- 1 Select Domains > Domain ID > Filters > Add Filter tab (Figure 56).

Figure 56 Add filters



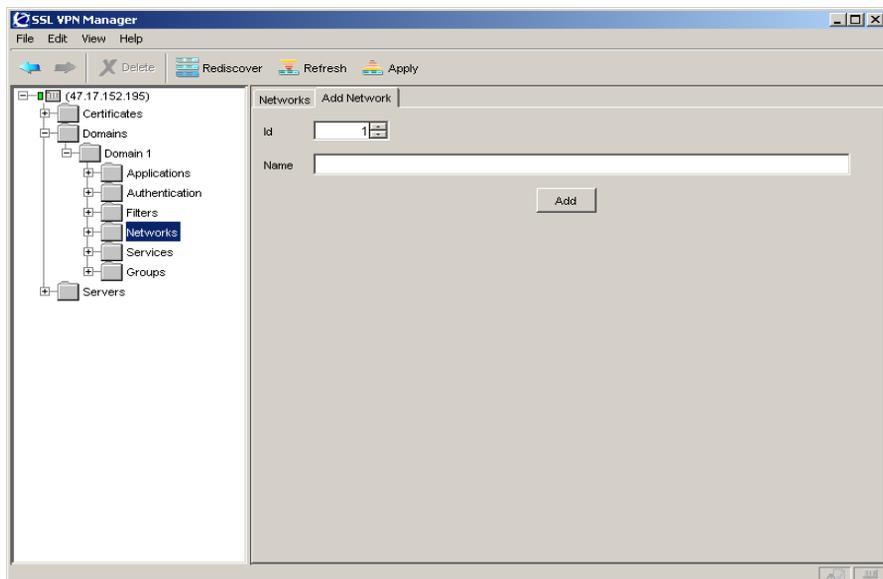
- 2 Specify the client filter's name and reference the previously created network.
- 3 Click on Add to add the filter.

Networks

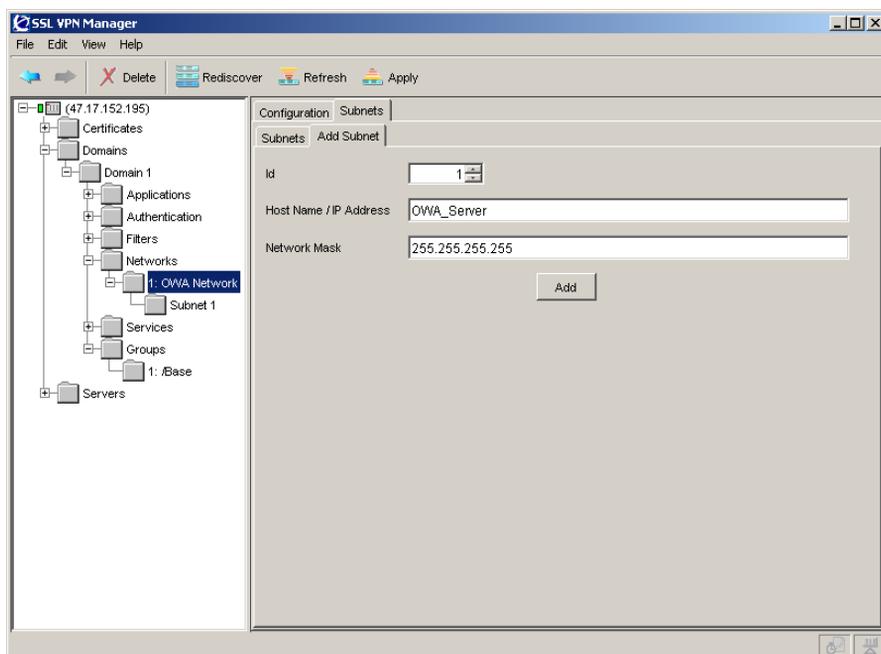
To add networks:

- 1 Select Domain ID > Networks > Add Network tab (Figure 57).

Figure 57 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 on Add. 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 Select Add Subnet ([Figure 58](#)).

Figure 58 Add subnet

- 8 The ID will default to 1 if this is the first subnet being added and 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.

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, SiteMinder and Certificates.

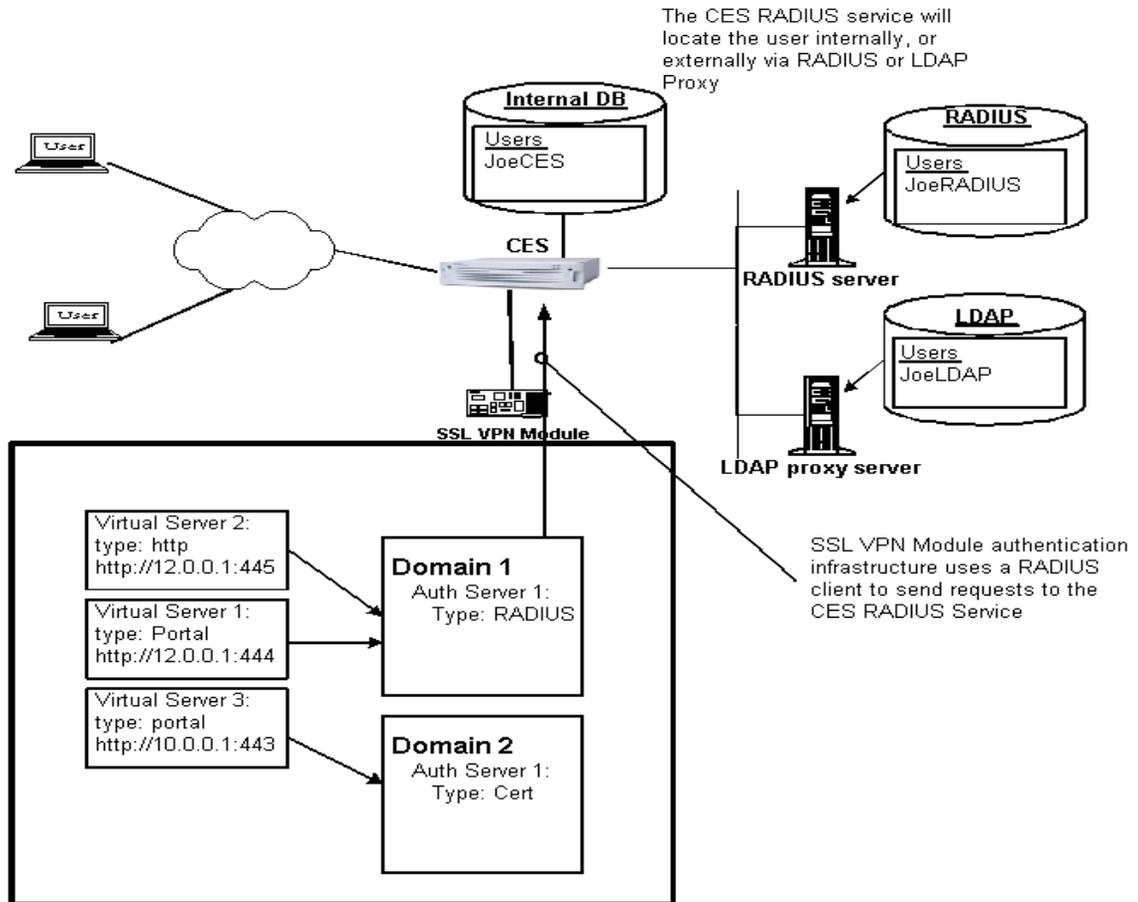
In general, SSL VPN authentication can be configured such that it directly connects to external servers such as RADIUS, or alternately, it can be configured to access the Contivity gateway authentication infrastructure (RADIUS and LDAP) using a RADIUS client. The Contivity RADIUS service will then proxy 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 59](#) describes the authentication infrastructure of the Contivity SSL VPN. Every virtual server has a domain associated with it, and all SSL VPN user authentication is performed by the domain. Multiple virtual servers can point to the same domain.

Figure 59 Authentication infrastructure



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

A typical use of the SSL VPN module is to create two domains: 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 domain 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 users user ID and password that were collected in the portal login screen, 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 domain must be created.
- An SSL VPN authentication server must be added to the domain. 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 domain 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 as 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.
- 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. It is not necessary then 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.	<ul style="list-style-type: none"> - Contivity RADIUS service - SSL VPN RADIUS authentication server pointing at Contivity gateway - Contivity one-time password enabled
Contivity local internal database	<p>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.</p> <p>IPsec user tunnel authentication of the user stored in the Contivity internal database occurs normally.</p>	<ul style="list-style-type: none"> - 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	<p>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.</p> <p>IPsec user tunnel authentication occurs normally after successful RADIUS authentication.</p>	<ul style="list-style-type: none"> - Contivity RADIUS service - SSL VPN RADIUS authentication server pointing at the Contivity gateway - Contivity RADIUS authentication server
LDAP proxy	<p>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.</p> <p>IPsec user tunnel authentication occurs normally after a successful LDAP proxy authentication.</p>	<ul style="list-style-type: none"> - Contivity RADIUS service - SSL VPN RADIUS authentication server pointing at Contivity - External LDAP Directory
NTLM	<p>The SSL VPN portal must be configured to directly access the external NT authentication server.</p> <p>IPsec user tunnel authentication occurs via the use of a one-time generated password.</p>	<ul style="list-style-type: none"> - SSL VPN NTLM authentication server - Contivity one-time password enabled
Siteminder	<p>The SSL VPN portal must be configured to directly access the external Siteminder authentication server.</p> <p>IPsec user tunnel authentication occurs via the use of a one-time generated password.</p>	<ul style="list-style-type: none"> - SSL VPN Netegrity Siteminder authentication server - Contivity one-time password enabled
Certificates	<p>The SSL VPN portal must have the appropriate CA and CRL location configured.</p> <p>IPsec user tunnel authentication occurs via the use of a one-time generated password.</p>	<ul style="list-style-type: none"> - Contivity one-time password enabled

Figure 60 shows the settings for configuring the Contivity RADIUS service to accept requests from the SSL VPN.

Figure 60 Configuring the RADIUS server

Enable RADIUS Service

Port

Clients

Enabled	Host Name or IP Address	Secret	Confirm Secret
<input checked="" type="checkbox"/>	Default Client	XXXXXXXXXXXXXXXX	XXXXXXXXXXXXXXXX

Authentication Order

Order	Server	Type	Associated Group
1	LDAP	Internal	
2	RADIUS	CHAP, PAP	/Base <input type="button" value="Del"/>
3	LDAP Proxy	PAP	/Base <input type="button" value="Del"/>

Figure 61 shows the settings for configuring the SSL VPN RADIUS client to point to the Contivity gateway RADIUS service.

Figure 61 RADIUS client pointing to RADIUS service

SSL VPN Manager

File Edit View Help

(15.0.0.5)

- Certificates
- Domains
 - Domain 1
 - Applications
 - Authentication
 - CES_RADIUS**
 - Filters
 - Networks
 - Services
 - Groups
 - Servers

General | RADIUS

Id

Name

Mechanism

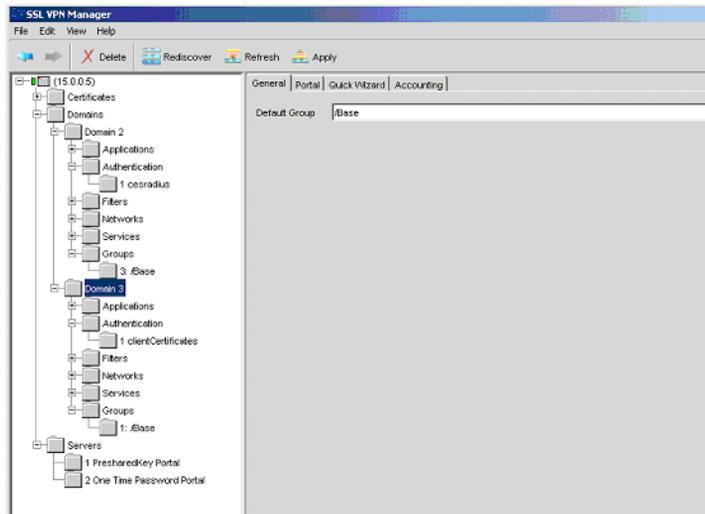
Display Name

Domain

Group Authentication Servers

Group assignments include the following:

- All of the groups within an SSL VPN domain should be created so that they correspond to the groups that exist on the Contivity gateway.
- The SSL VPN default group should correspond to the default group setting on the Servers > RADIUS auth screen (Figure 62).

Figure 62 Default group for a domain

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 domain, the Contivity gateway authenticates the user by sending a query to an external RADIUS, LDAP, NTLM domain, 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.

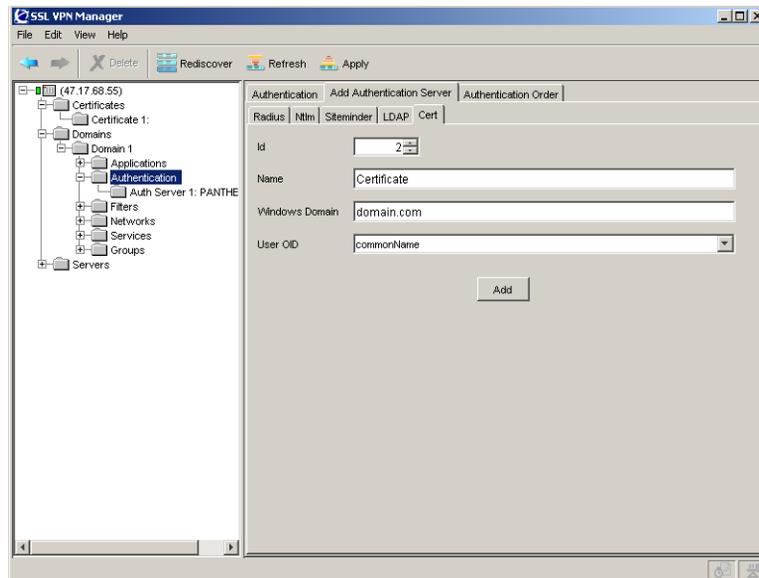
You can configure more than one authentication method within any given VPN domain (portal).

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 63). 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 64).

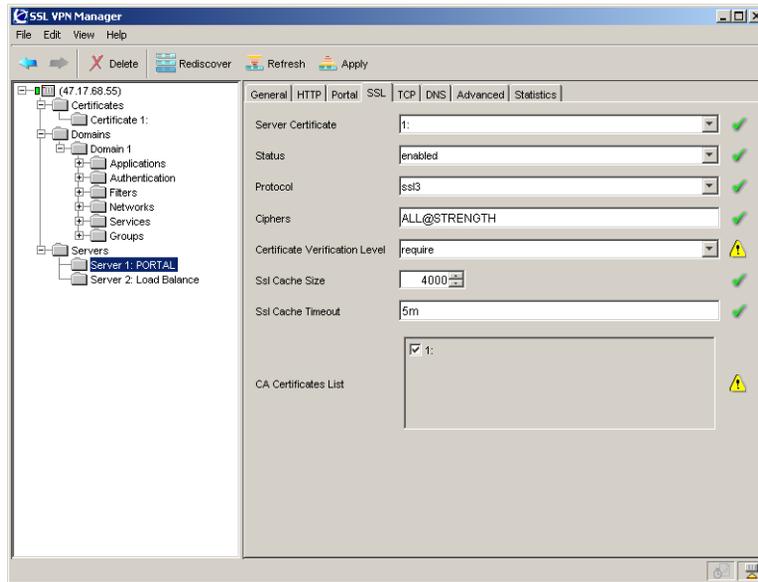
Figure 63 Certificate authentication server



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 will send 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.

Figure 64 Virtual server configured to require client certificates



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.

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 65). 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 66), 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 65 Configuring automatic CRL retrieval

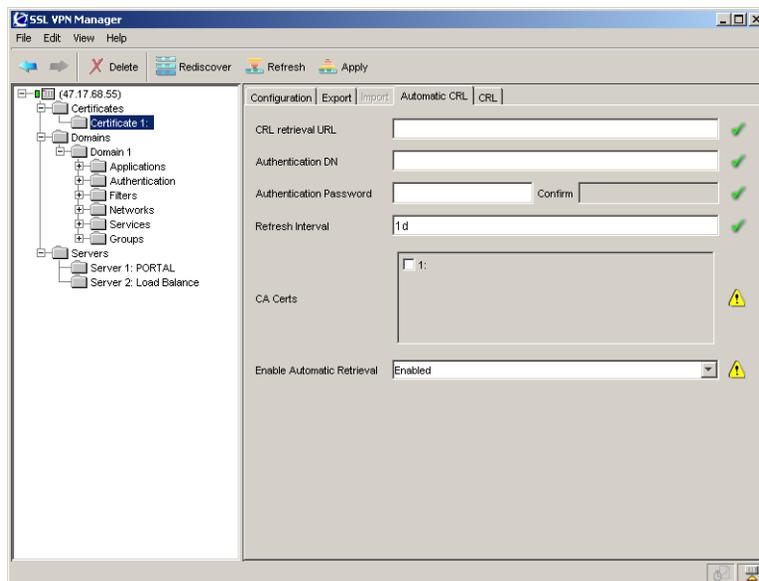
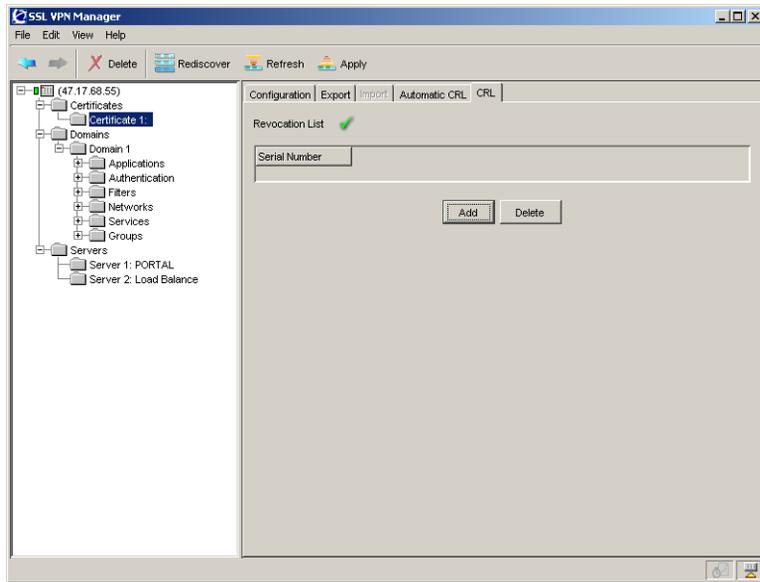


Figure 66 Creating your own CRL

Making use of the Contivity RADIUS authentication

When the SSL VPN module is set to use the Contivity RADIUS service for authentication (Figure 67), all current Contivity users can be given access to the SSL. This includes all internal users, RADIUS, SECURID, and LDAP proxy users (Figure 68).

Figure 67 Contivity RADIUS service configuration

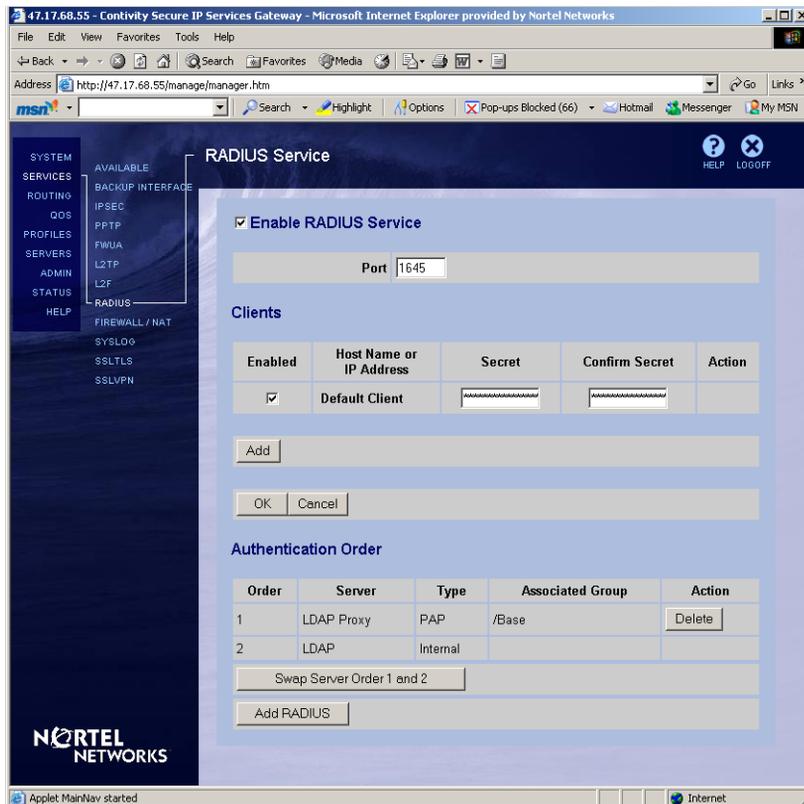
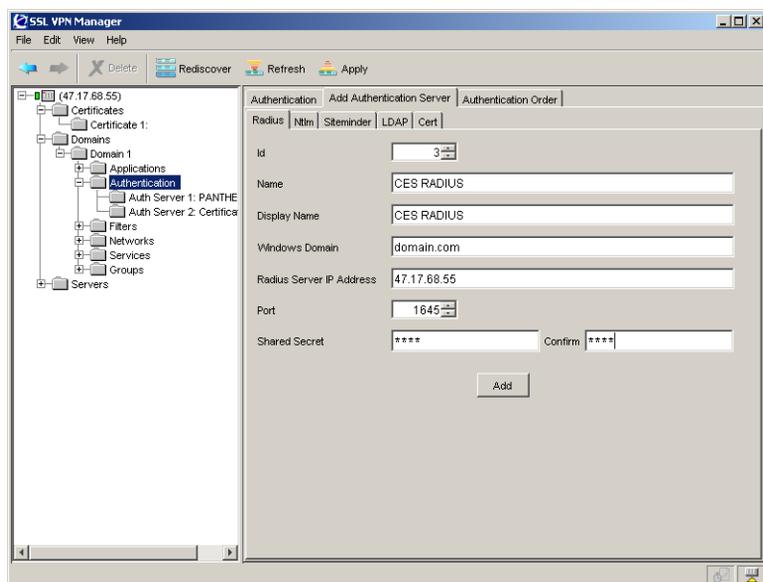


Figure 68 SSL VPN module RADIUS client aimed at Contivity RADIUS service

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 domain. 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 domain. 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 `postOfficeBox`, 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 screen 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).

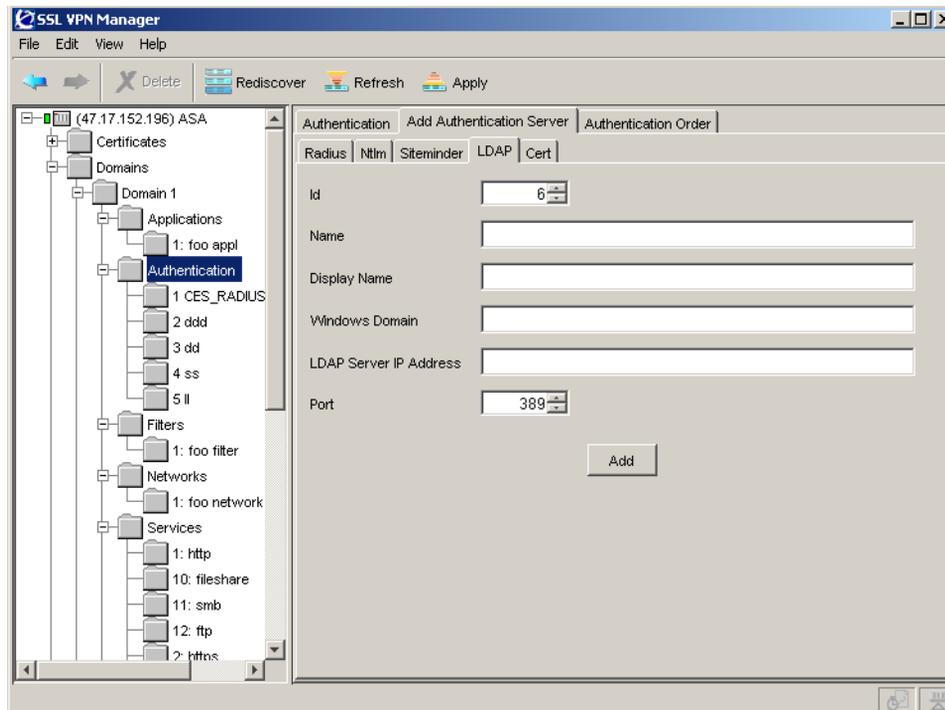
LDAP authentication

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

To configure LDAP authentication:

- 1 Create a new VPN domain, or configure an existing VPN domain (Figure 69).
If you have already created a VPN domain (=portal) to which you want to add LDAP authentication, type the domain number. To create a new VPN domain, type a domain number not currently in use.

Figure 69 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.

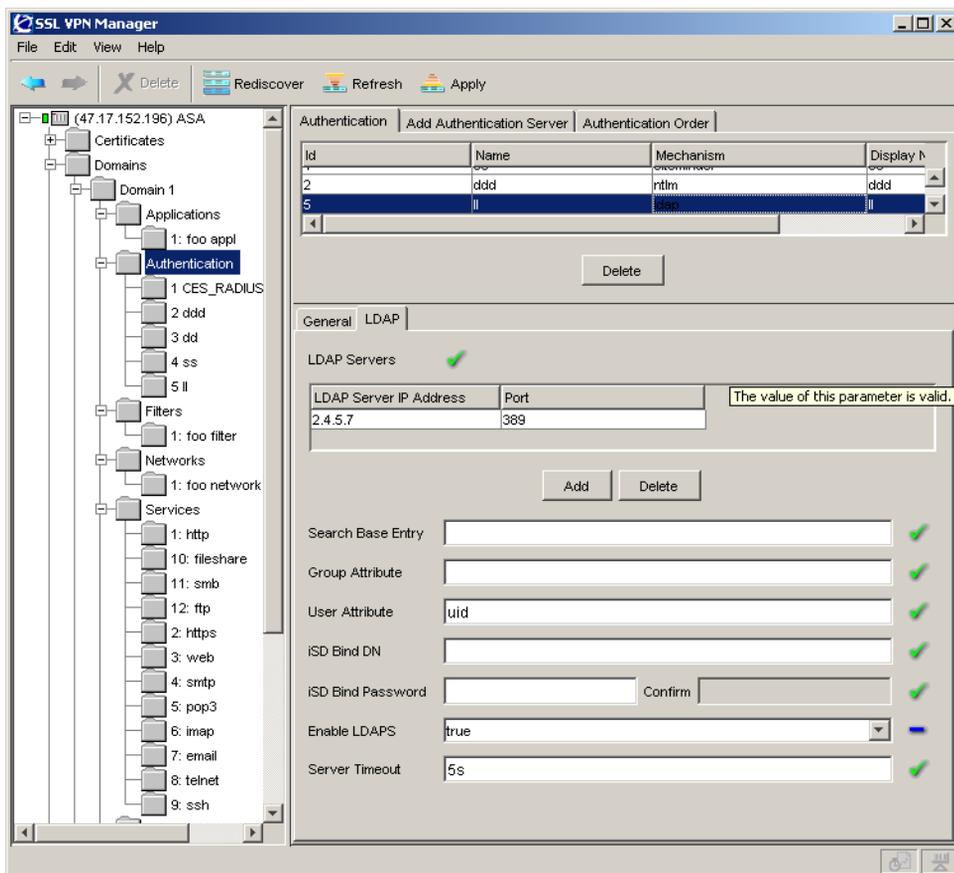
A name is mandatory. If you refer to the current authentication method later in a client filter, this name should be used.

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

5 Specify the LDAP server IP address and port (Figure 70).

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 70 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 domain 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 Domains > Domain ID > 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 screen 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.

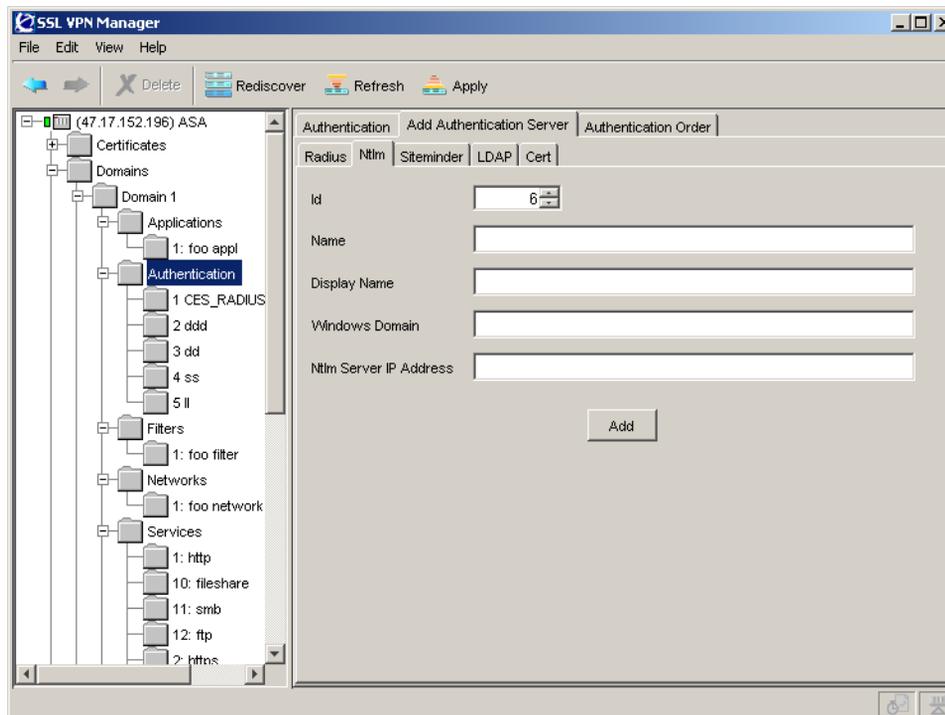
- 4 Set a password for Contivity gateway authentication.

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 71](#)).

Figure 71 NTLM authentication

- 1** Create a new VPN domain or configure an existing VPN domain.
If you already created a VPN domain (=portal) to which you want to add NTLM authentication, type the domain number. To create a new VPN domain, type a domain 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 domains, 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 screen 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 Domains > Domain ID > Authentication tab.

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

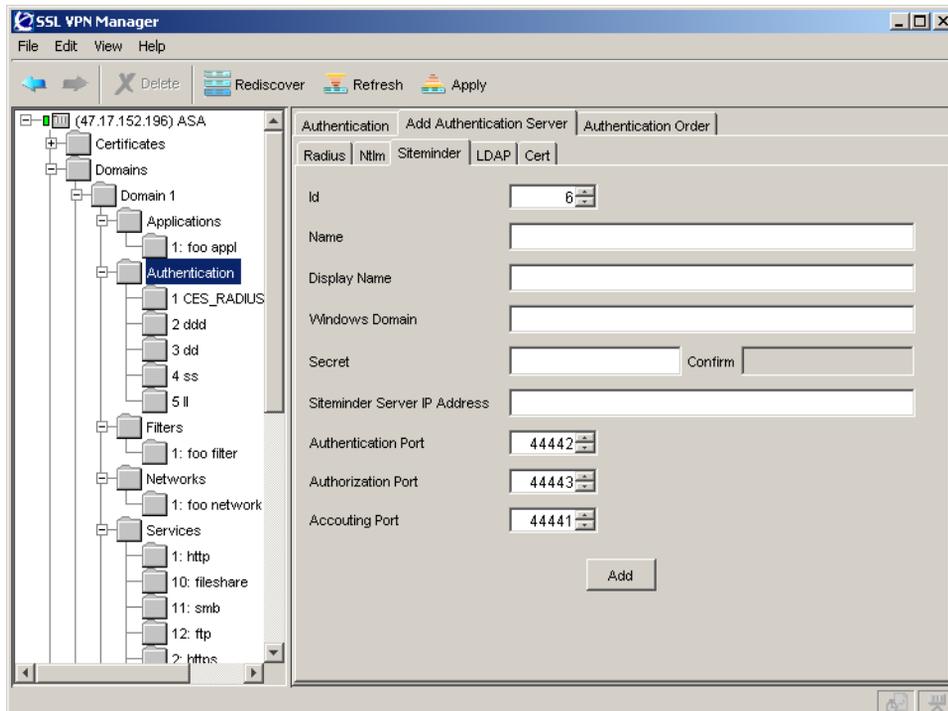
8 Apply your configuration changes.

SiteMinder authentication

To configure the Contivity gateway to use a Netegrity SiteMinder server (Figure 72) 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 72 SiteMinder configuration



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

If you have already created a VPN domain to which you want to add SiteMinder authentication, type the domain number. To create a new VPN domain, type a domain 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 screen 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 domains

This section describes the steps for configuring single sign-on domains 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 domains.

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

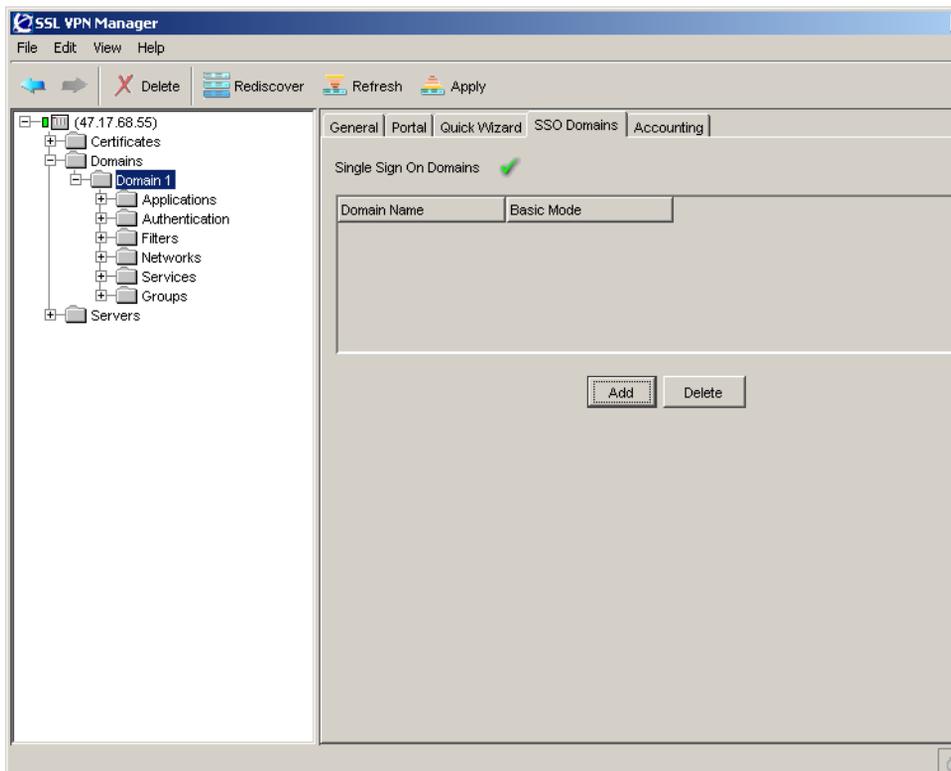
If SSO domains are configured, the username and password used to access the portal is automatically forwarded to the back end servers, resulting in single sign-on access to end users.

The SSO domain configuration can be found at Domains > Domain # > SSO Domains.

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

- 1 Go to SSO Domains (Figure 73) and enter either the fully qualified domain name ftp.test.com or enter the domain test.com.

Figure 73 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 will automatically send the username password to the back end servers.
 - Add_Domain -- When Add_Domain mode is selected, the SSL device will automatically send the domain\username password to the back end servers. The domain is populated by the Windows domain field configured on a particular users authentication server.

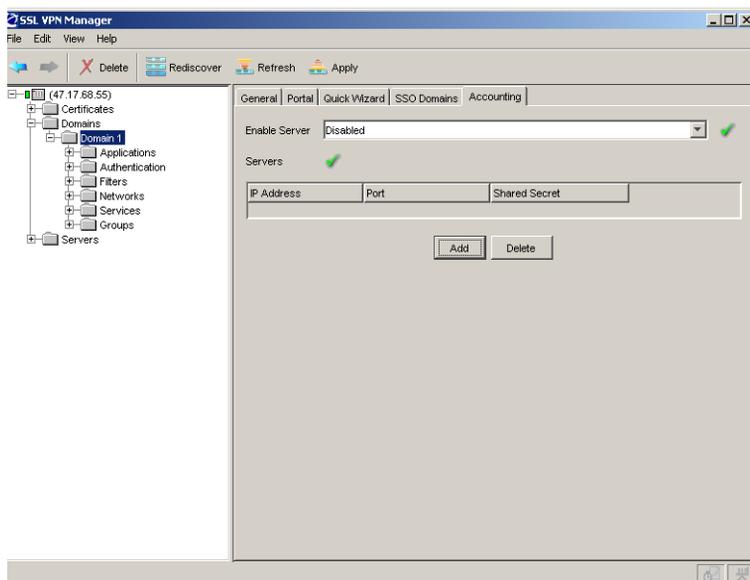
Accounting

Accounting allows you to add one or more RADIUS accounting servers to the current configuration. With a RADIUS accounting server configured (Figure 74), 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 74 Accounting screen



Common Portal Settings

There are several portal configuration settings that are associated with the domain, so that all portals that use that particular domain have these in common. Configuration items unique to a particular server are configured for that server alone (server configuration is covered in [Chapter 5](#), “Configuring Virtual Servers”).

See [Chapter 2](#), “Using the SSL VPN portal” on page 54 for further information on configuring portal settings.

Chapter 5

Configuring virtual servers

This chapter describes information that you need to configure portal servers.

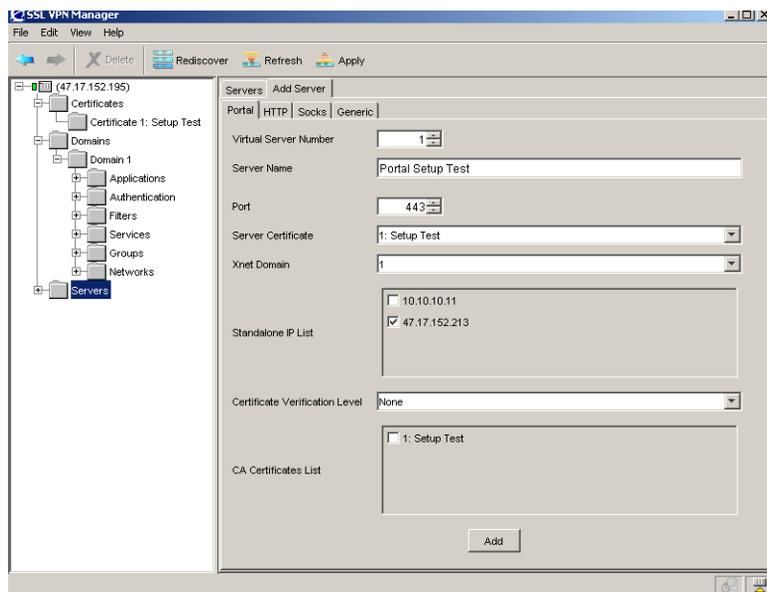
Configuring portal servers

Only one VPN domain can be mapped to a portal server, so if you plan to use several different portals, you will have to create several different virtual SSL servers of the portal type.

To configure a portal server:

- 1 Select the Add Server tab to create a portal server ([Figure 75](#)).

Figure 75 Add Server



- 2 Configure the Add Server parameters:
 - a Enter a name, such as Portal Test, and select from the Standalone IP List the interfaces from which to run the SSL VPN portal. This is the address that users will use to access the portal through a Web browser. The other fields should remain at the default values.
 - b Click on Add Server.
- 3 To review your setup, select Config Summary on the Contivity gateway Services > SSL VPN screen. You can also refer to the event log for information about errors by selecting Admin > Event Log.
- 4 To test access to the portal screen, enter HTTPS://IP Address, where *IP Address* is the standalone IP address assigned to the portal server. This IP address will always be an interface/CLIP address belonging to the Contivity gateway.

To create a virtual SSL server:

- 1 Create a virtual SSL server of the portal type.

Each virtual server listens to a specific TCP port and is connected to one or more portal IP addresses. Specify a virtual server number not currently in use by an existing virtual server.
- 2 Assign a Fully Qualified Domain Name (FQDN) to the portal server.

The domain name you specify should be registered in DNS to resolve to the virtual server IP address you specified in the previous step. The FQDN for the portal server corresponds to the URL that remote users will type in the address field of their Web browser to access the portal login screen when the SSL VPN is fully deployed.
- 3 Specify the certificate to be used by the portal server.

You are prompted to type the index number of an existing certificate. To view all certificates currently added to the Contivity gateway by index number and name, use the Certificates menu and tabs.



Note: If the certificate you specify is a chained certificate, you need to first add the CA certificates up to and including the root CA certificate, and then specify the CA certificate chain of the server certificate.

- 4 Configure the DNS settings for the portal server.

This step specifies a DNS search domain. The search domain(s) you specify is automatically appended to the host names a remote user types in the various address fields on the portal (provided a match is found).

- 5 Verify that support for Java applets and the SSL VPN client is enabled.

The default setting is on, which means that all the features on the portal Advanced tab (for example, HTTP Proxy, Telnet/SSH access and Port forwarding) are supported. In addition, support for the SSL VPN client is present.

- 6 Configure the portal settings.

This maps the portal server you previously created to the configured VPN domain.

- 7 Choose the IP address from the provided Standalone IP Address list.

This step defines the portal IP address on which client connection requests destined for port 443 are received.

- 8 Apply the changes.

Now you have created the basis for your portal. What remains to be done is to configure one or more authentication methods, add user groups with access rules, and configure group links.

URL Rewrite White-list

Internal Web sites can have links to Web servers that are external to the private network; for example, 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, you can enable URL Rewrite White-list and add the domains that you want to remain internal.

To configure the URL rewrite white list:

- 1 Select the Servers > Portal server on the left side of the SSL VPN Manager.
- 2 On the right side of the page, select the portal tab and enable SSL Rewrite White-list.

- 3 To add the domains to be rewritten, click on Add, enter the domain name, and click on Add.

You can add the full domain 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 would be treated as internal.

- 4 Click on Apply.

Configuring HTTP and generic servers

You can configure the SSL VPN Module 1000 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 Go to Servers > Add Server and select the Generic or HTTP tab.
- 2 Define a name for the server.
- 3 Assign a virtual server IP (VIP) address to the server.
- 4 Specify the certificate to be used by the server.
- 5 Configure the Xnet settings for the HTTP server if desired. Generic servers cannot be used with XNET domains.
- 6 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 domain 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 Server > HTTP.
- 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.

Configuring SOCKS servers

This section describes how to configure the SSL VPN Module 1000 to support the SSL VPN client software exclusively. No SSL VPN portal interaction will be possible.

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

- 1** Go to Servers > Add Server and select the SOCKS tab.
- 2** Define a name for the SOCKS server.
- 3** Assign a virtual server IP (VIP) address to the SOCKS server.
- 4** Specify the certificate to be used by the SOCKS server.
- 5** Configure the Xnet settings for the SOCKS server. This maps the SOCKS server to a configured Xnet domain.
- 6** Apply the changes.

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 and click on Add Server.
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 screen.

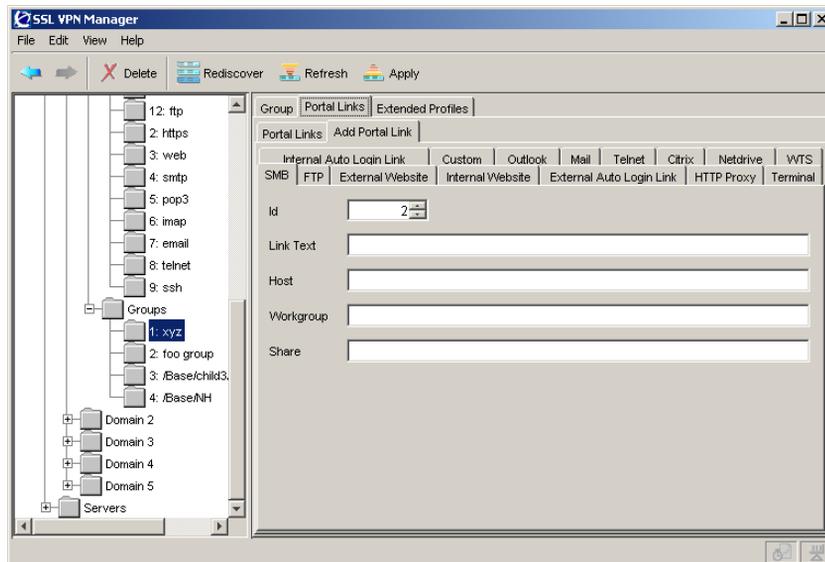
Portal links examples

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 Select the group whose members will have access to the link.
- 2 Select the Add Portal Link tab.
- 3 Select the SMB tab. The SMB Portal Link tab is shown below.

Figure 76 Samba file server link

- 4 Define the link text to appear on the portal's Home tab.
- 5 Specify file server host, workgroup (optional) and shared network folder.

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

If needed, a Windows workgroup can be specified.

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.

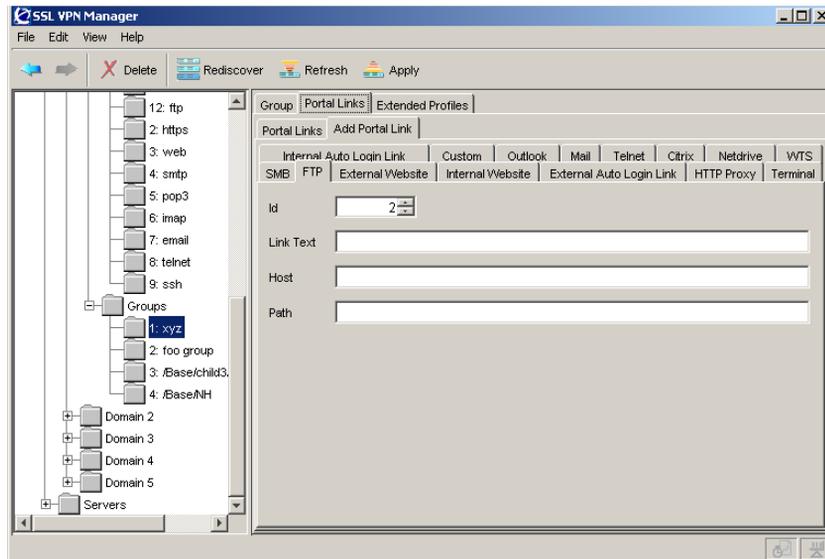
- 6 View the resulting HREF and link text by logging in to the portal.

Linking to FTP file server

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

- 1 Select the group whose members will have access to the FTP link.
- 2 Select the Add Portal Link tab.
- 3 Select the FTP tab. The FTP Portal Link tab is shown below.

Figure 77 FTP file server link



- 4 Select an ID for the link.
- 5 Define the link text to appear on the portal's Home tab.
- 6 Specify the file server host and the shared network folder.

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

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.

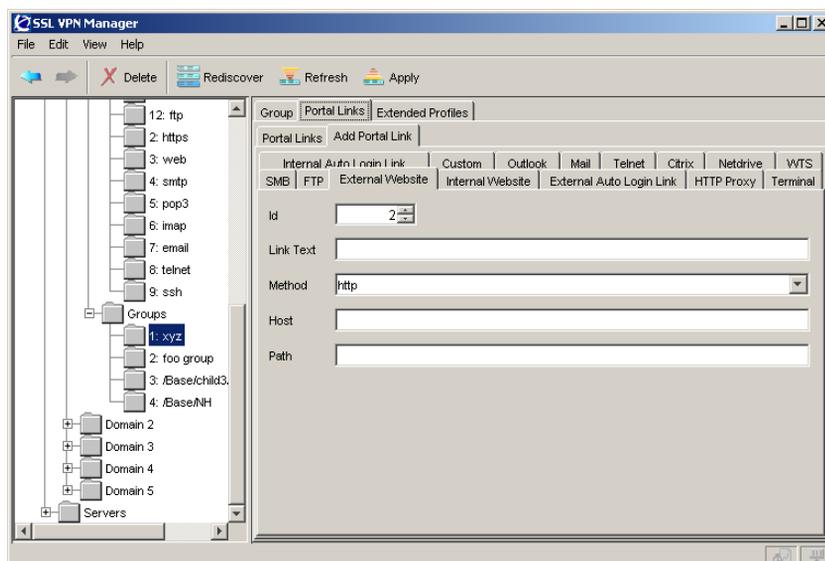
- 7 View the results and link text by logging in to the portal.

Creating direct link to 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 Select the group whose members will have access to the Web link.
- 2 Select the Add Portal Link tab.
- 3 Select the External Website tab. The External Website Portal Link tab is shown below.

Figure 78 External Web link



- 4 Select an ID for the link.
- 5 Define the link text to appear on the Portal's Home tab.
- 6 Specify the access protocol method, fully qualified domain name for the host, and 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.

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

Creating secured links to Web pages

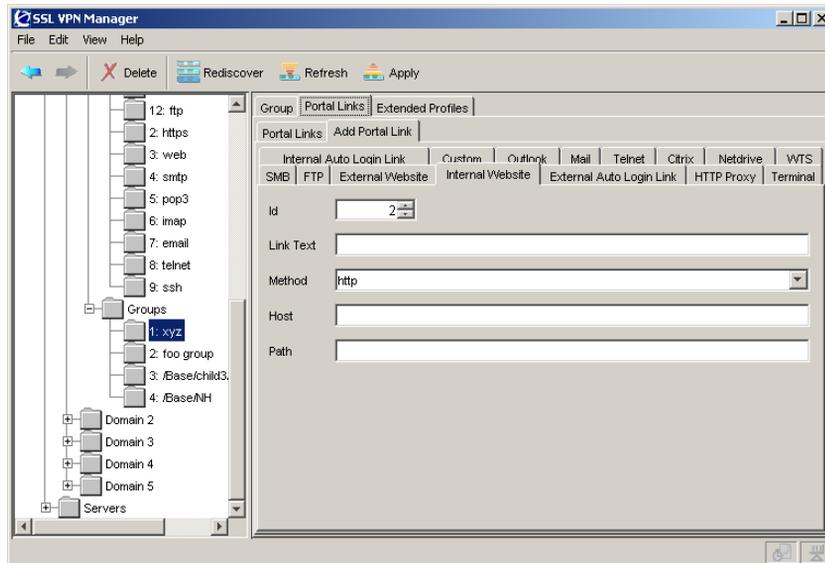
This example shows how to create a secure link to an internal Web page on your intranet. The internal link directs the HTTP request to the Contivity Secure IP Services Gateway, where the rewrite prefix (boldface) is added to the link.

Example:

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

- 1 Select the group whose members will have access to the Web page link.
- 2 Select the Add Portal Link tab.
- 3 Select the Internal Website tab. The Internal Website Portal Link tab is shown below.

Figure 79 Secured Web link



- 4 Select an ID for the link.
- 5 Define the link text to appear on the Portal's Home tab.
- 6 Specify the access protocol method, fully qualified domain name for the host, and 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>

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

Creating automatic login links (direct)

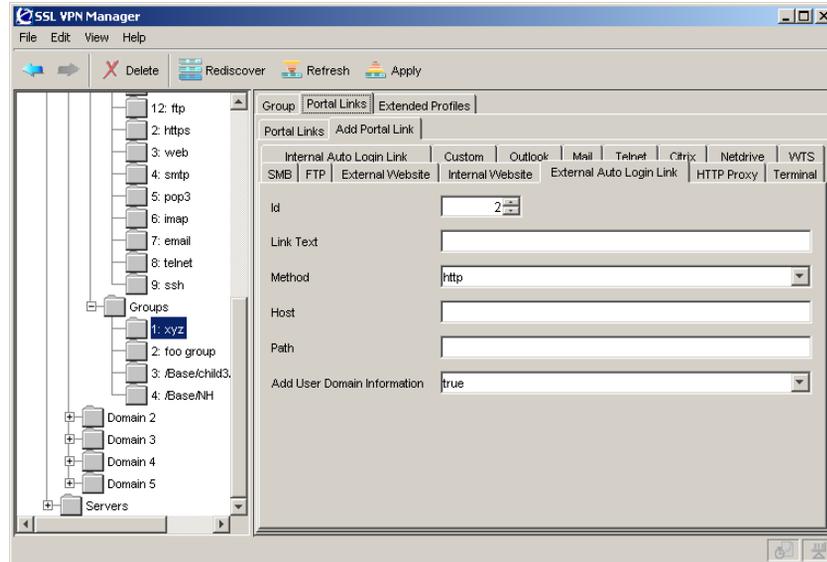
This example shows how to create an automatic login link to a password-protected Web page. The HTTP request is directed straight to the specified resource; the Contivity gateway rewrite prefix is not added to the URL.

The link automatically includes the <user> and <password> macros in the URL. The macros expand to the credentials provided by the remote user on Portal login. User name and password are transferred to the specified Web page and the user can thus be logged in automatically. For the remote user to be successfully logged in to the external Web page, the required credentials must be identical to those required by the authentication mechanism for Portal login.



Note: When you configure automatic login links with this method, the Portal user name and password may leak outside the protected intranet. Use this feature with great caution.

- 1 Select the group whose members will have access to the external auto login site link.
- 2 Select the Add Portal Link tab.
- 3 Select the External Auto Login Link tab. The External Auto Login Portal Link tab is shown below.

Figure 80 External auto login link

- 4 Select an ID for the link.
- 5 Define the link text to appear on the Portal's Home tab.
- 6 Specify the access protocol method, fully qualified domain name for the host, and path.

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

If user authentication is performed towards an NTLM server, the user's Windows domain can be included in the login link. The domain name will be retrieved from the current authentication method, provided a domain name is set using the `/cfg/xnet/domain #/auth #/domain` command.

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

Using internal auto login link

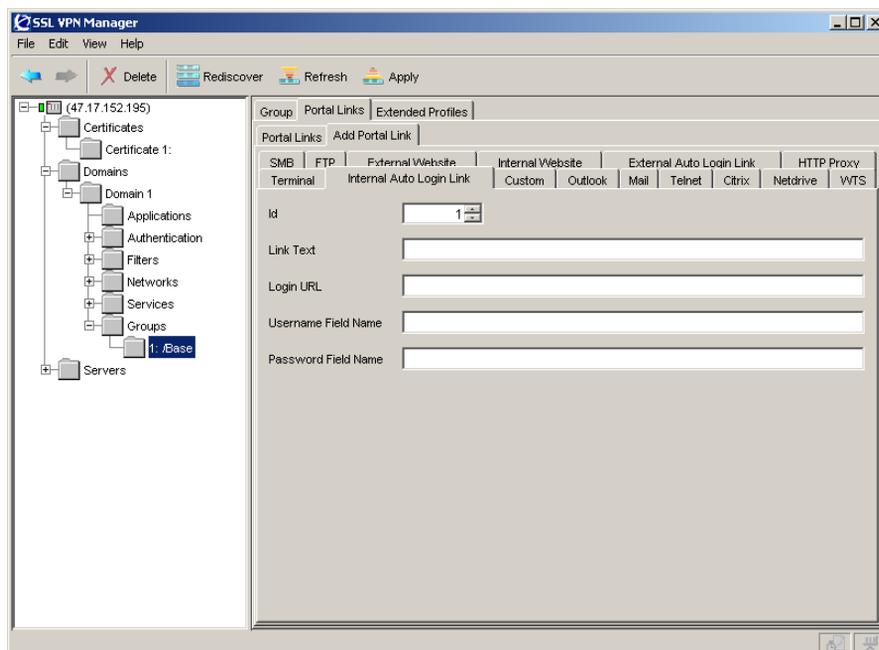
This example shows how to use the Internal Auto Login link type to create an automatic login link to a password-protected Web page. As opposed to the eauto link, the HTTP request is directed to the Contivity gateway, where the rewrite prefix (boldface) is added to the link.

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 Select the group whose members will have access to the internal auto login link.
- 2 Select the Add Portal Link tab.
- 3 Select the Internal Auto Login Link tab. The Internal Auto Login Portal Link tab is shown below.

Figure 81 Internal auto login link



- 4 Select an ID for the link.
- 5 Define the link text to appear on the Portal's Home tab.
- 6 Specify the login URL to the password-protected Web page.
- 7 When a user enters the URL, the Contivity VPN gateway automatically retrieves the URL to analyze which authentication type it uses.
- 8 Specify the user and password fields found on the form. The names correspond to the input name value in the Web page's source code.

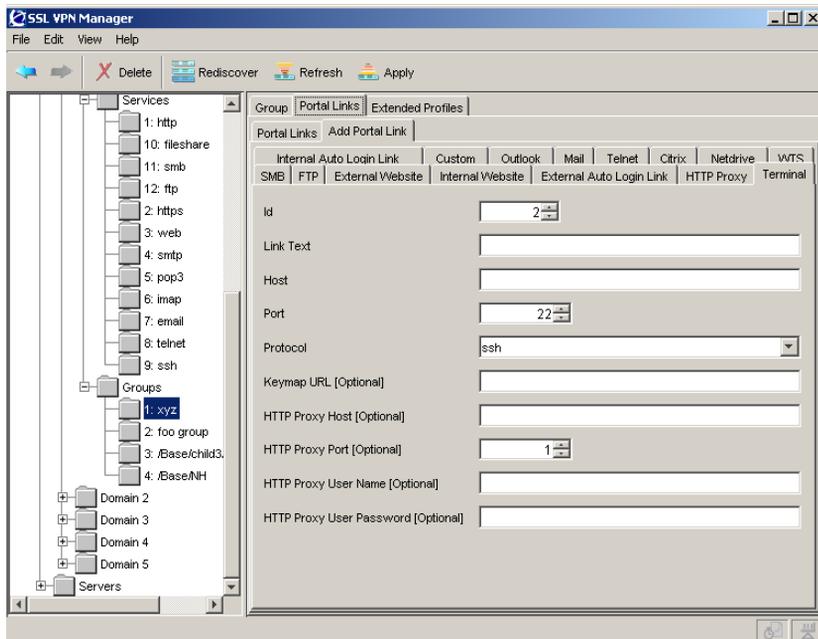
Enter the values to be inserted in the fields. Macros, text strings or a combination of both can be used. By using the <user> and <password> macros as values (as in the example above), the macros will expand to the credentials provided by the remote user on the Portal login screen. If these are the credentials that the target Web page requires, the user is automatically logged in. If not, the Web page's form is displayed instead.

The <domain> macro can be used if the form includes an input field for a Windows domain. In this case, the macro will expand to the domain name specified for the current authentication ID.

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 Select the group whose members will have access to the terminal server link.
- 2 Select the Add Portal Link tab.
- 3 Select the Terminal Link tab. The Terminal Link tab is shown below.

Figure 82 Terminal link

- 4 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.

- 5 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`.

- 6 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 domain 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 will be tunneled directly to the Contivity gateway.

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

This step will not be displayed if the previous step was skipped.

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

Customizing port forwarder link (Citrix)

By clicking a Port Forwarder link, the user is provided with one or more secure tunnels to an intranet application server. The purpose is to be able to run one or more UDP- or TCP-based client applications, for example, Citrix Metaframe or Telnet, towards the specified application servers.

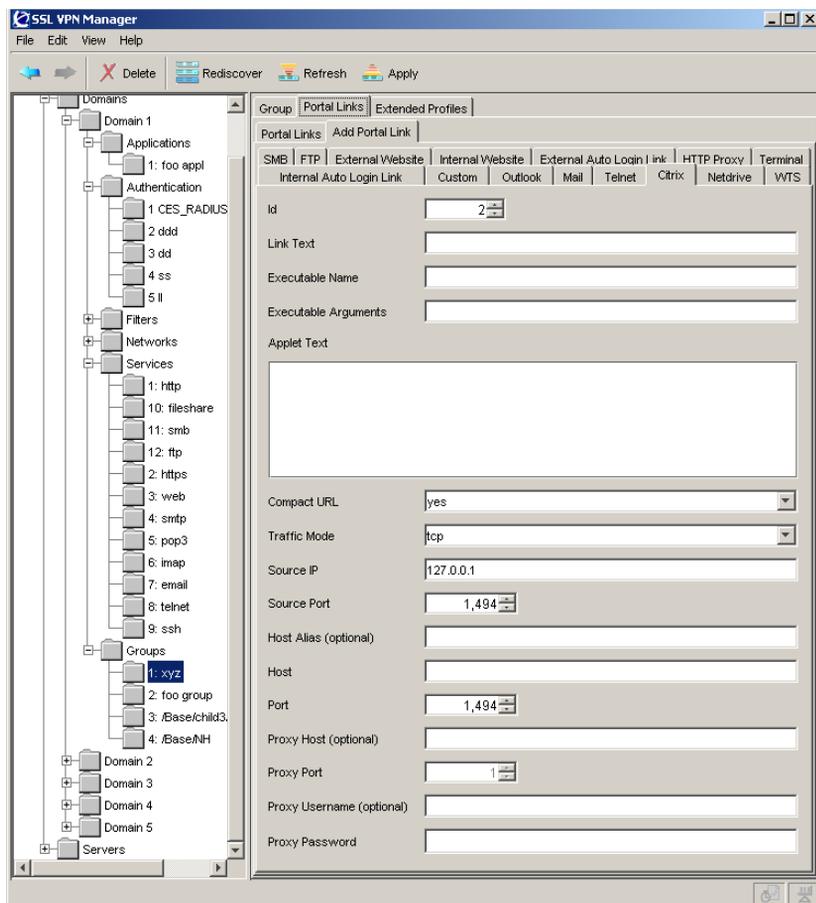
When the user clicks the link, a Java applet is downloaded. The Java applet is instructed to listen to a port number on the user's own computer (for example, 127.0.0.1 or any other IP address within the 127.x.y.z range). The applet then forwards all incoming traffic to an application server on the intranet.

Setting up a port forwarder link to be displayed on the Portal's Home tab (instead of letting the user set up a Port Forwarder on the Portal's Advanced tab) is a way of making application access simpler for the user. In addition, group members whose user type is set to `novice` or `medium` will not have access to the Advanced tab. A third advantage of the Port Forwarder link is that it can be set to launch the application automatically.

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

- 1 Select the group whose members will have access to the terminal server link.
- 2 Select the Add Portal Link tab.
- 3 Select the Citrix tab. The Citrix tab is shown below.

Figure 83 Custom Citrix link



4 Specify the desired traffic mode.

TCP is a *connection-oriented* protocol. It does not transfer any data until a connection between two hosts has been established. TCP guarantees that all data will be delivered to the receiving host in the same order as it is sent.

UDP is a *connection-less* protocol. No connection to a receiving host needs to be established before the data is transferred. UDP does not guarantee delivery but is lightweight and efficient.

5 Enter the source IP address and source port.

The SSL tunnel will be established between the specified TCP/UDP port (source port) on the user's local machine (source IP = any IP address within the 127.x.y.z range) and the Contivity Secure IP Services Gateway.

When specifying the source port, use port numbers just above 5000, which are usually free to use, or use the application-specific port number. On Windows machines any port number can be used.

6 Specify a host alias (optional).

Host aliases can be specified; for example, if the user should start the application manually. For example, if the executable is pn.exe, the host alias citrix, and the source port 1494, you can start the Citrix Metaframe client and then use citrix as the host name to connect to the server specified as destination host.



Note: Usage of host aliases requires the alias to be mentioned in the Java applet window. It also requires the user to have administrator privileges on the client 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.

7 Specify destination host (IP address or host name) and destination port.

The Contivity Secure IP Services Gateway relays data from the user's local machine to the specified target (destination host) and application-specific port (destination port).

In this example, one connection is sufficient for the link we are configuring. However, one single port forwarder link can be configured to set up multiple connections. For example, to configure an Outlook Express link, you would have to configure the port forwarder link to set up one connection to an SMTP server and another to a POP3 server.

8 Optionally, specify the application to be started.

This defines the application to be started when the user clicks on the link. Start by entering the name of the executable; for example, pn.exe for a Citrix Metaframe pn client. By pressing Enter to skip, no application will be started when the user clicks the link. The user can however be instructed to start the application manually (see Step 10). If the browser is entered as executable, the user's default browser will be started.



Note: The Contivity gateway must be able to find the executable either via the PATH variable or in the registry (on Windows clients); for example, HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\App Paths. To make sure the program is found, you can enter the complete path to the executable after the executable prompt.

The path to the executable is entered. The Program Files folder could be called something else in another language version.

9 Optionally, specify an argument to the program.

The argument identifies the command-line argument to be used by the application; for example, http://127.0.0.1:5025 if the executable is browser or /app:calc if the executable is pn.exe (Citrix Metaframe pn client). Each application has its own set of arguments.

10 Optionally, enter custom text (such as user instructions) to appear in the Java applet window.

The custom text displayed in the Java applet window is automatically displayed when the user clicks on the link. The instructions can be used to explain the purpose of the port forwarders or how to launch the application (for example, by using the specified host alias). If custom text is entered or pasted, click on Enter after the last line, followed by three periods (...). Then click on Enter to view the next prompt.

If no custom text is desired, simply type the three periods and click on Enter to view the next prompt. This will result in a standard text being displayed in the Java applet window, with information about the host/ lmhost file mappings and the sockets that are opened for the port forwarder. Below is an example of a Java applet standard text:

```
Started port forwarder(s):
tcp;127.0.0.1:5025 -> inside.example.com:1494

Host alias mapping(s):
citrix -> 127.0.0.1
```

11 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 domain 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.

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

13 If more than 25 port forwarders is included in one port forwarder link, reply *yes* to compress the URL; otherwise accept the default value *no*.

14 View the resulting HREF and link text.

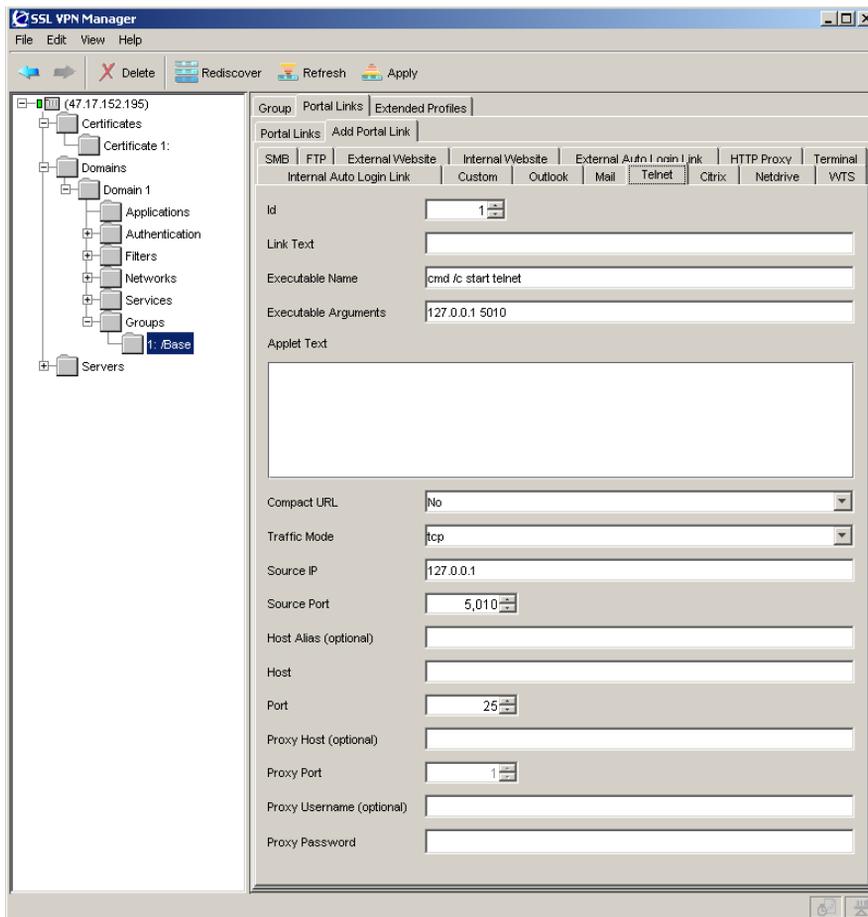
15 Apply the changes.

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 Select the group whose members will have access to the link.

- 2 Select the Add Portal Link tab.
- 3 Select the Telnet tab. The Telnet tab is shown below.

Figure 84 Telnet port forwarder link

- 4 Define the link text to appear on the Portal's Home tab.
- 5 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).
- 6 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 domain 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 Servers > ID# Server Name > TCP tab.

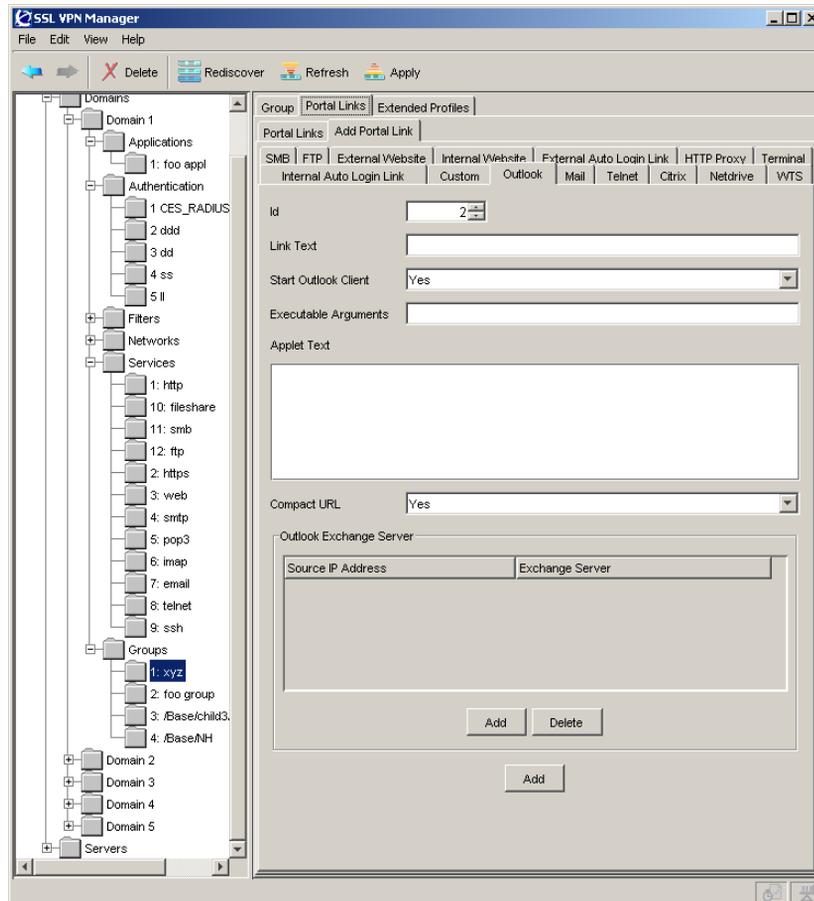
To ensure proper operation, specify the DNS name of the portal server.

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** Select the group whose members will have access to the Outlook link.
- 2** Select the Add Portal Link tab.
- 3** Select the Outlook tab. The Outlook tab is shown below.

Figure 85 Outlook port forwarder link

- 4 Define the link text to appear on the Portal's Home tab.
- 5 Enter the Forwarder menu to select the Outlook option.
- 6 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.

- 7 Specify whether or not the Outlook client should be started automatically when the user clicks the link.

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

- 8 If desired, enter arguments to the Outlook client.

An example of an argument would be `/Profile myprofile`.

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

- 10 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`.

- 11 Configure the Exchange servers' domain 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 domain names.

- 12 Apply the changes.

Creating HTTP proxy links

Like the internal link, the proxy link lets the user access a Web page through a secure SSL connection. However, a Web page may contain plugins (such as a Flash movie) which, in their turn, may include embedded links to other Web pages. If a user executes such an embedded link, the HTTP request may not reach the Contivity Secure IP Services Gateway and the URL will not be displayed.

To ensure display of all URLs (including ones that are embedded in plugins), HTTP proxy lets the user download a Java applet to the client. The client browser's proxy settings should then be changed to direct all HTTP requests to this Java applet. The Java applet in its turn routes each request through a secure SSL tunnel to the Contivity Secure IP Services Gateway's proxy server, where it is unpacked and redirected to its proper destination.

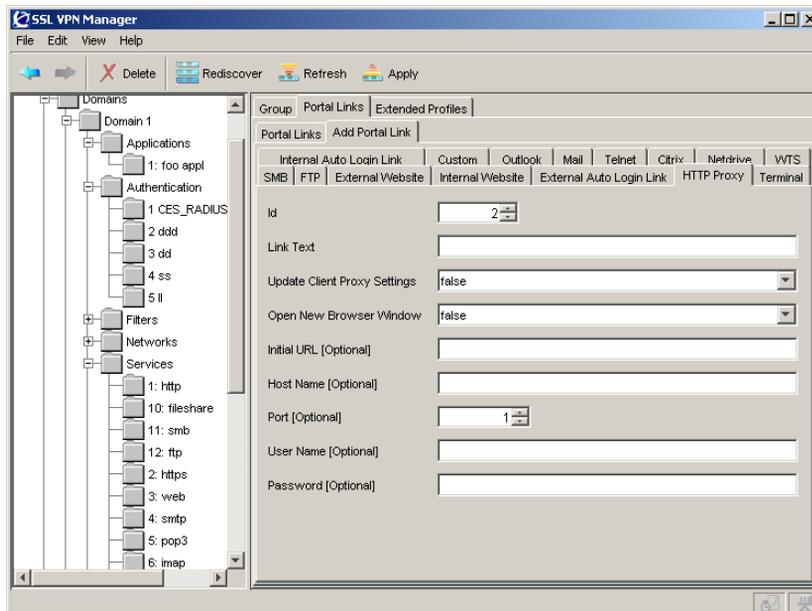
For users with Internet Explorer, the link can be configured to change/clear the proxy settings automatically.



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

- 1 Select the group whose members will have access to the HTTP Proxy link.
- 2 Select the Add Portal Link tab.
- 3 Select the HTTP Proxy tab. The HTTP Proxy tab is shown below.

Figure 86 HTTP proxy



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

5 Select the `proxy` option.

6 Select whether or not to reconfigure the client browser's proxy settings.

If you enter `yes` here, the user does not have to reconfigure the browser's proxy settings manually. They are automatically reconfigured to use 127.0.0.1 and 4567 as proxy server address and port. This is specified for both HTTP and HTTPS (Secure) traffic in the Internet Explorer proxy settings window. When the user exits the Java applet window, the proxy settings are automatically restored to the original settings.

Note that automatic updating and clearing of the proxy settings are only possible for Internet Explorer running on Windows.

If set to `no`, or if a browser other than Internet Explorer is used (for example, Netscape), instructions on how to reconfigure the proxy settings manually is provided in the Java applet window displayed when the user clicks the HTTP Proxy link.

7 Select whether or not to open a new browser window.

If you enter `yes` here, a new browser window will automatically be opened when the user clicks the HTTP Proxy link.

If set to `no`, the user should open a new browser window to start browsing in HTTP Proxy mode.

8 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).

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 domain 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.

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

To access a Web page in HTTP Proxy mode, the remote user should first click on the link to download the HTTP Proxy applet, then reconfigure the browser's proxy settings (instructions are provided in the Java applet window). For users with Internet Explorer, the link can be configured to change/clear the proxy settings automatically.

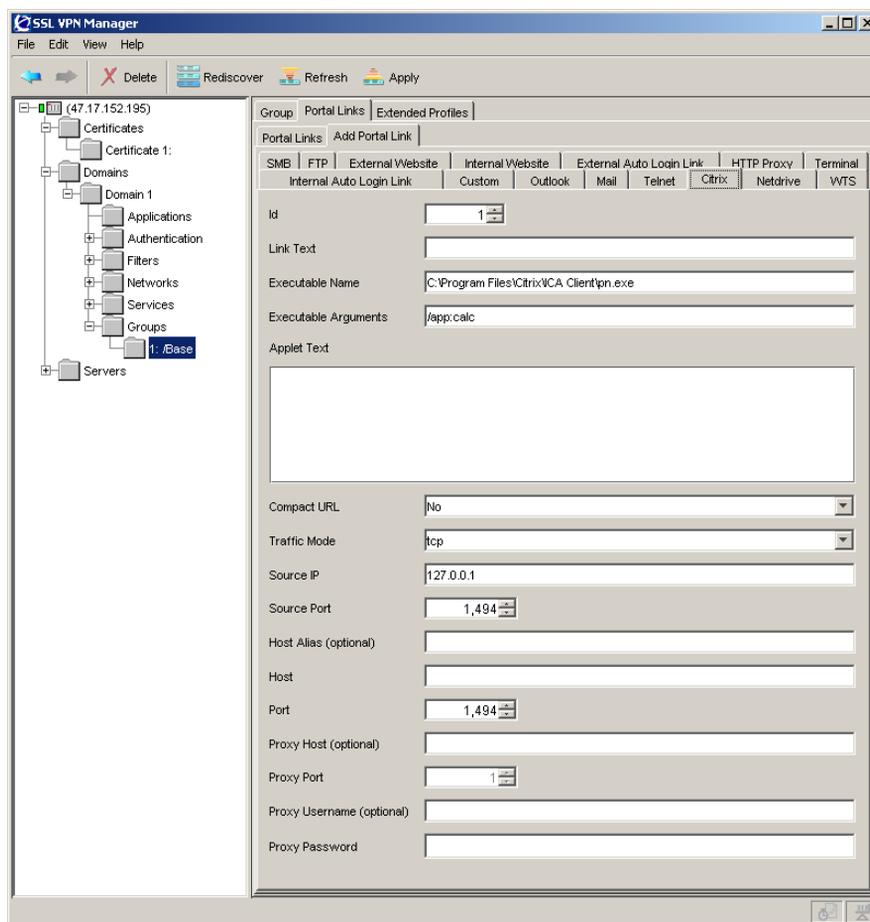
Finally, the user should open a new browser window to start browsing in HTTP Proxy mode. As an alternative, the link can be configured to open a new browser window automatically.

To quit surfing in HTTP Proxy mode, the user should click on the Stop Port Forwarder button in the Java applet window and manually restore the original browser settings. Note that this last step is not required if the link is set to configure/clear the browser's proxy settings automatically.

Creating Citrix links

You can create a portal link to Citrix Metaframe using the Citrix tab.

- 1** Select the group whose members will have access to the HTTP Proxy link.
- 2** Select the Add Portal Link tab.
- 3** Select the Citrix tab. The Citrix tab is shown below.

Figure 87 Example Citrix link

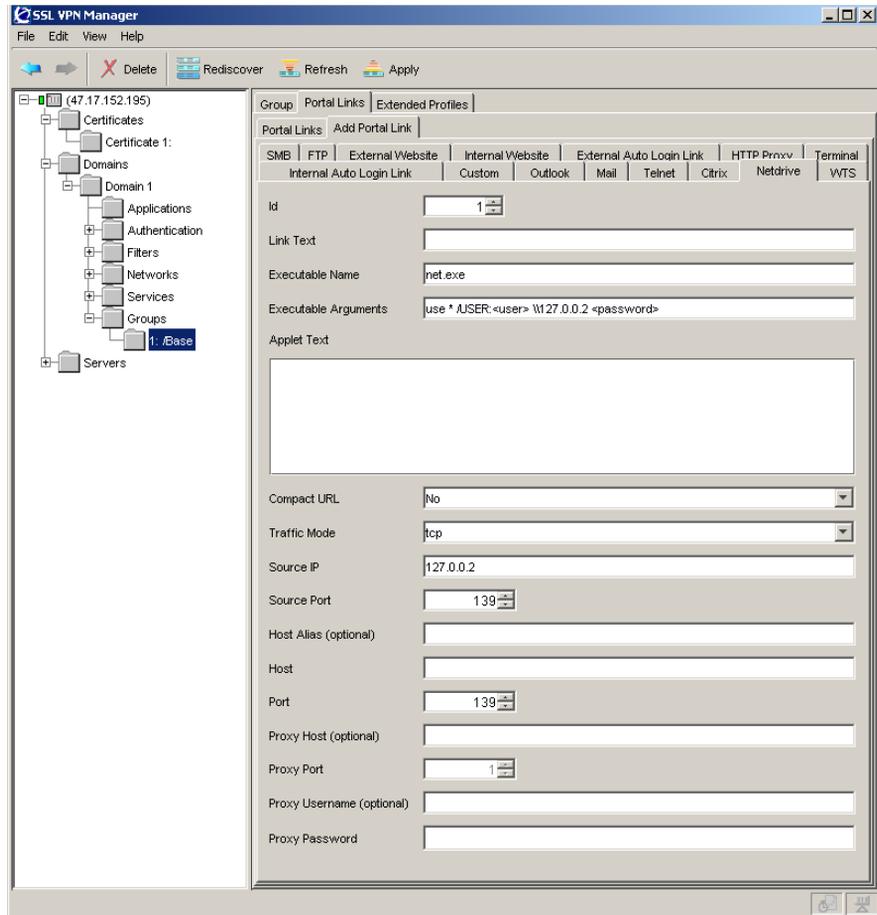
- 4 Define the link text to appear on the Portal's Home tab.
- 5 Specify the executable filename, including the path. The default is:
C:\Program Files\Citrix\ICA Client\pn.exe.
- 6 Specify source IP and port, host alias (if desired), destination host and port, application to be started, arguments, custom Java applet text (optional), HTTP proxy server (if any) and compact URL (yes or no).
- 7 Apply the changes.

Creating Netdrive links

You can create a portal link to Netdrive using the Domain > Domain ID > Groups > ID#: /Groupname > Add Portal Links > Netdrive tab. ID#: /Groupname represents the group in the menu tree for which you want to include the link on the portal.

- 1 Select the group whose members will have access to the HTTP Proxy link.
- 2 Select the Add Portal Link tab.
- 3 Select the Netdrive tab. The Netdrive tab is shown below.

Figure 88 Example Netdrive link



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

- 5 Specify the executable filename, including the path. The default is: net.exe.
- 6 Specify any command line arguments. The default is: use */USER:<user> \\127.0.0.2 <password>.
- 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.

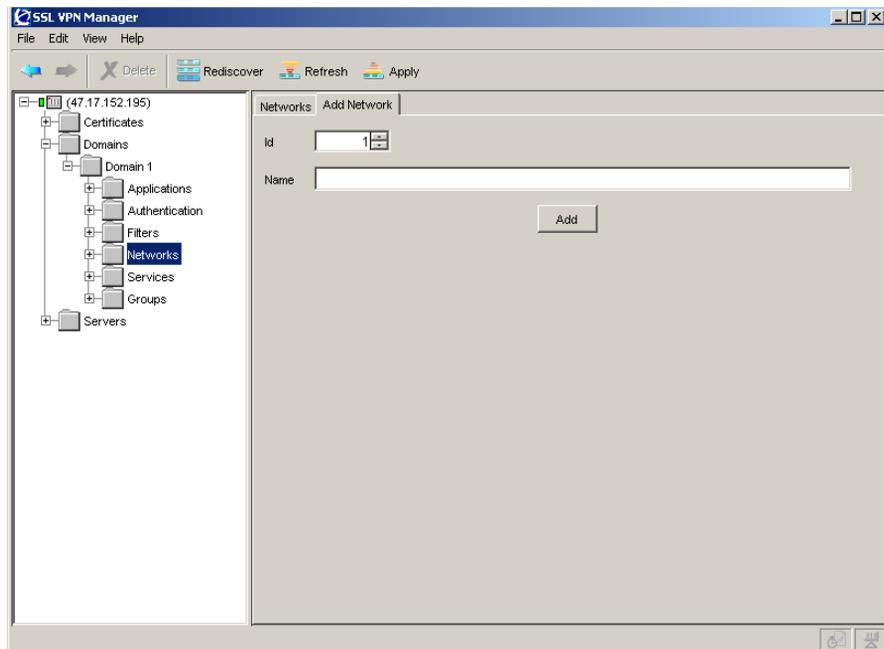
Access rule sample configurations

The following section provide examples of access rule configurations.

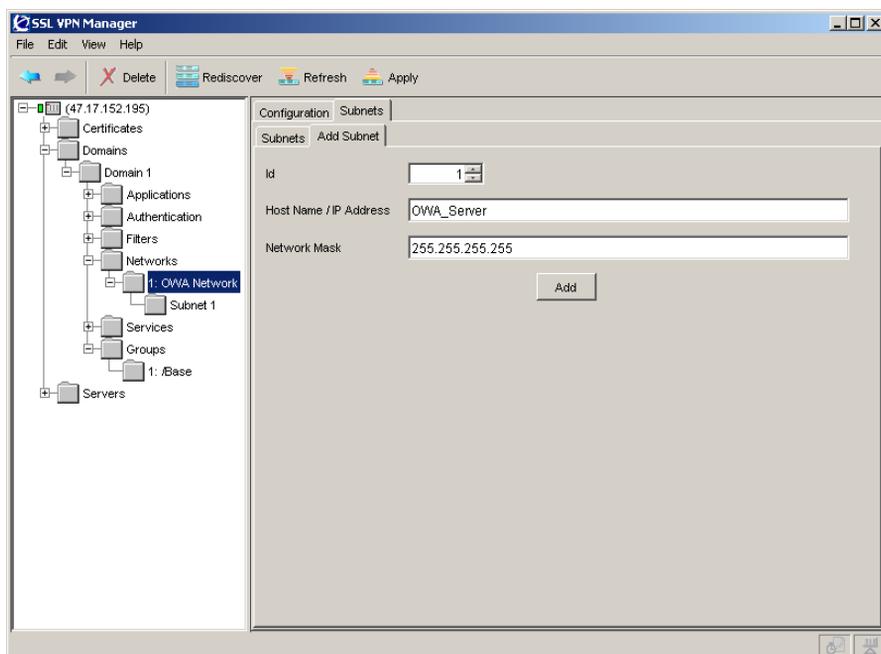
Access to Outlook Web access server

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

- 1 Select Domain *ID* > Networks > Add Network tab.

Figure 89 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 on Add. 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 Select the Add Subnet.

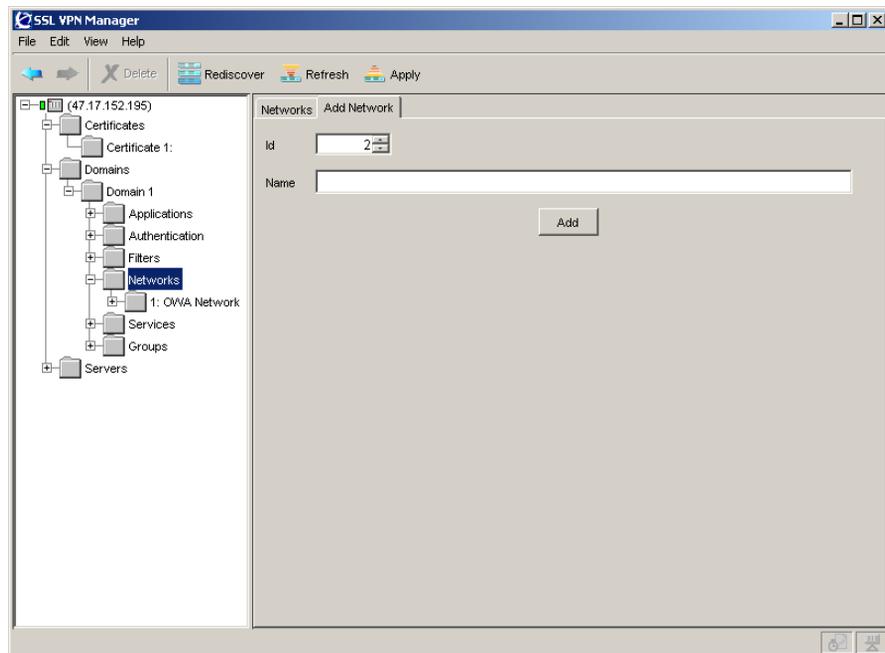
Figure 90 Add subnet

- 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.

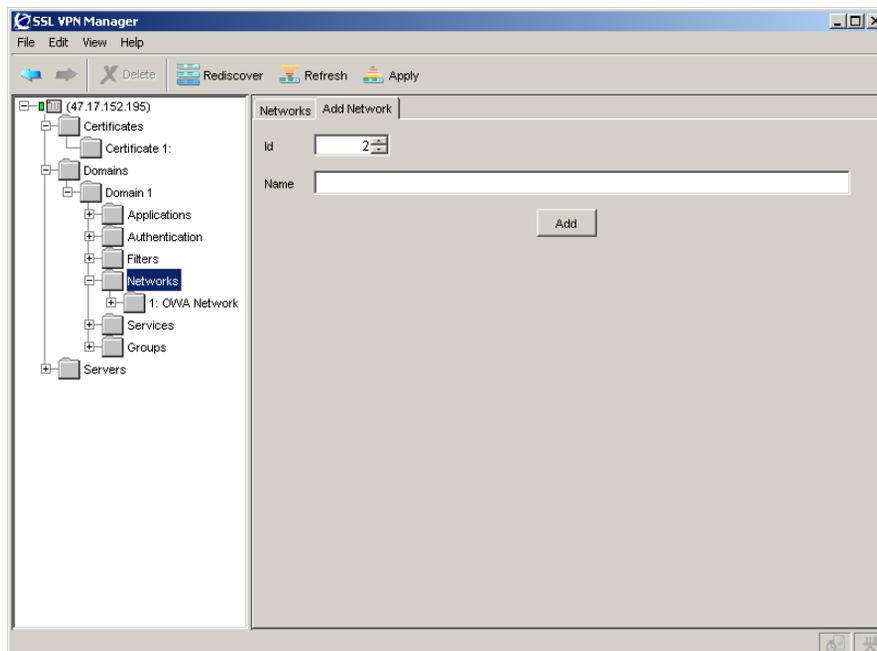
Access to intranet Web server

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** Using the Domain ID > Network > Add Network tab.

Figure 91 Add network example

- 2 Specify a network name and click on Add.
- 3 Click on the plus sign (+) to expand the Networks tree and select the network you have added.
- 4 Click on Subnets.
- 5 Select Add Subnet.

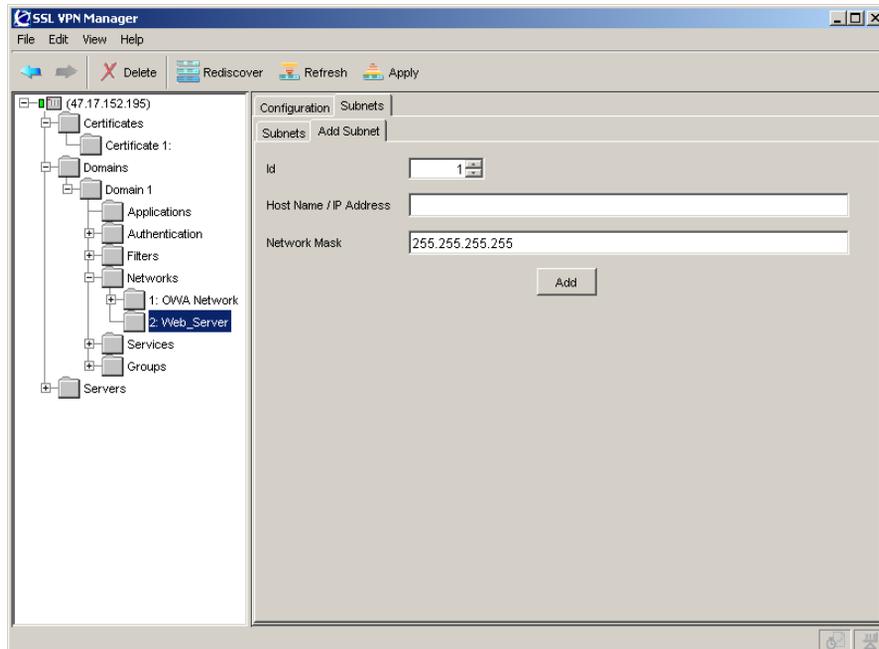
Figure 92 Add subnet example

- 6 Define a subnet identifying the intranet Web server.
- 7 Apply the changes.

Access to intranet file server

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

- 1 Using the Domain ID > Network > Add Network tab, specify a network name and click on 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 Subnet.

Figure 93 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 subdomain in a company's intranet to which the group members should be authorized. The subdomain is called `sales.example.com`.

- 1 Using the Domain ID > Network > Add Network tab, specify a network name and click on Add.
- 2 Apply the changes.
- 3 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 subdomain, you can use an asterisk (*) as a wildcard.

- 4 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 subdomain in the company intranet to which the group members should be unauthorized. The subdomain is called `secret.example.com`.

- 1 Using the Domain ID > Network > Add Network tab, specify a network name and click on Add.
- 2 Click on the plus sign (+) to expand the Networks tree and select the network you have added.
- 3 Click on the Subnets tab.
- 4 Select the Add Subnet tab.
- 5 When creating a subnet, enter either the host name or the network address/netmask. To specify all hosts within a subdomain, you can use an asterisk (*) as a wildcard.
- 6 Define a subnet identifying the intranet file server.
- 7 Apply the changes.

Group configuration examples

The following sections describe various examples of group configurations.

Defining staff groups

In this example, we will create a group called `staff`. The base profile should contain a link to an Outlook Web Access server and an access rule that allows access to that OWA server. Access to the OWA server should be 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 Domains > Domain ID > Groups > Add Group tab and specify the group name and user type.
- 2 Click on Add 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 Domains > Domain ID > Quick Wizard 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 will be 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 Domains > Domain ID > Networks > Networks tab.
- 2 Specify the network name.

- 3 Click on Add.
- 4 Expand the Networks tree and select the network just added.
- 5 Select the Subnets > Add Subnet tab.
- 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 subdomain, you can use an asterisk (*) as a wildcard.

Defining client filter for the client network

To be able to reference the client filter in the extended profile, you have to first define the client filter.

- 1 Select Domains > Domain ID > Filers > Add Filter tab.
- 2 Specify the client filter's name and reference the previously created network.
- 3 Click on Add 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 > Add Extended Profile tab.
- 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 will be applied.

- 5 Select the Extended Profiles tab and click on the extended profile in the list to select it.
- 6 At the bottom of the screen, click on Portal Links > Add Portal link.
- 7 Select the FTP tab and create a group link to an FTP file server on the intranet.
- 8 This link will be displayed on the portal's Home tab. The link defined for the base profile will be appended to this link, for example, both links will be displayed for group members accessing the portal from the branch office network.
- 9 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 will not be triggered. This is 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, will be 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 will be allowed. A match will be found between the requested resource and the network referenced in Access rule 1. If Bill tries to request any other resource, no match will be found in the access rule and access will be denied.
- **From the branch office network:** The extended profile will be 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 will be displayed because the base profile's links are always appended to those of the extended profile. The access rule defined for the extended profile will be applied, which means Bill is granted access to all hosts and protocols on the intranet and the internet. The base profile's access rule will be appended but has no real effect in this example.

Defining engineering groups

In this example, we will create a group called `engineer`. The base profile should contain a link to an intranet Web server and an access rule that allows access to all hosts in the `sales.example.com` subdomain.

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 should be applied. The Advanced tab should not be visible on the portal. For users logging in to the portal using RADIUS authentication, links and access rules defined for the extended profile should be applied. The extended profile should contain an extra set of links, an access rule that allows access to all hosts and a user type allowing display of 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 lets you specify the group's name and user type. By setting the user type to `medium`, the Advanced tab will not be 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 can make use of the network definition we created in the example on [-179](#), 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 you should define the client filter. The client filter should later be referenced in the extended profile. The extended profile in its turn should be triggered when a group member authenticates via the RADIUS server.

- 1 Set the client filter's name and specify which authentication server it refers to.
- 2 Set the authentication server name.

This step lets you specify the authentication server used. The authentication server should be referenced by the name that was assigned to the authentication method, using the `/cfg/xnet/domain 1/auth #/name` command.

- 3 Apply the changes.

This client filter should now be 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, we should add an extended profile to the group. The extended profile should be triggered when a group member authenticates via 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 via token login. The group members should be granted access to hosts on all networks. All services should be available.

3 Add links to the extended profile.

Links added to the extended profile will be displayed when the user authenticates via token login. Links defined for the base profile will be appended to those of the extended profile.

4 Apply the changes.**Results**

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

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

In the same way, an extended profile could be created for users with a valid client certificate installed. Because client certificate authentication is considered more secure, the extended profile could provide 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 should 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 have just created.

5 Specify the access rules pertaining to the extended profile.

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

6 Apply the changes.

Extended profile for users with IE cache wiper

To make sure 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) could 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, he or she 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 should 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 have just created.
- 5** Specify the access rules pertaining to the extended profile.
These access rules are configured for the Extended profile and should 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
altonISDSSLHwFail	Signifies that the SSL accelerator hardware failed. The Contivity Secure IP Services Gateway will continue to handle traffic, but with severely degraded performance.
altonISDDown	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 212](#).

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 limit_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 | nohidden | name_resolve | 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 xnet domain can be found. Make sure that there is a portal running using the same xnet id.
- Bad IP:PORT data <line> in the 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 ASA 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 nameserver <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 Processin g	Failed to detect SSL acceleration hardware.
css error: <reason>	ERROR	Traffic Processin g	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 Processin g	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 Processin g	At least one DNS server is now up.
Failed to initialize SSL hardware	ERROR	Traffic Processin g	Problem initializing SSL acceleration hardware. This will cause the ASA to run with degraded performance.
failed to locate corresponding portal for portal authenticated http server	ERROR	Traffic Processin g	Portal authentication has been configured for an http server, but no portal using the same xnet domain can be found. Make sure that there is a portal running using the same xnet id.
failed to parse Set-Cookie <header>	ERROR	Traffic Processin g	The Contivity gateway got a malformed Set-Cookie header from the backend Web server.
Failed to syslog traffic :<reason> -- disabling traf log	ERROR	Traffic Processin g	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 nameserver <ip>:<port>	ERROR	Traffic Processin g	Contivity gateway received reply for non-configured DNS server.
internal error: <no>	ERROR	Traffic Processin g	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 Processin g	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.
jsript.encode error: <reason>	ERROR	Traffic Processin g	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 XnetId=<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_perman ent_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.
Xnet 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.
Xnet 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.
Xnet 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 <i>number</i> in the ISO Latin1 character set. The <i>number</i> 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 Domains > 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:

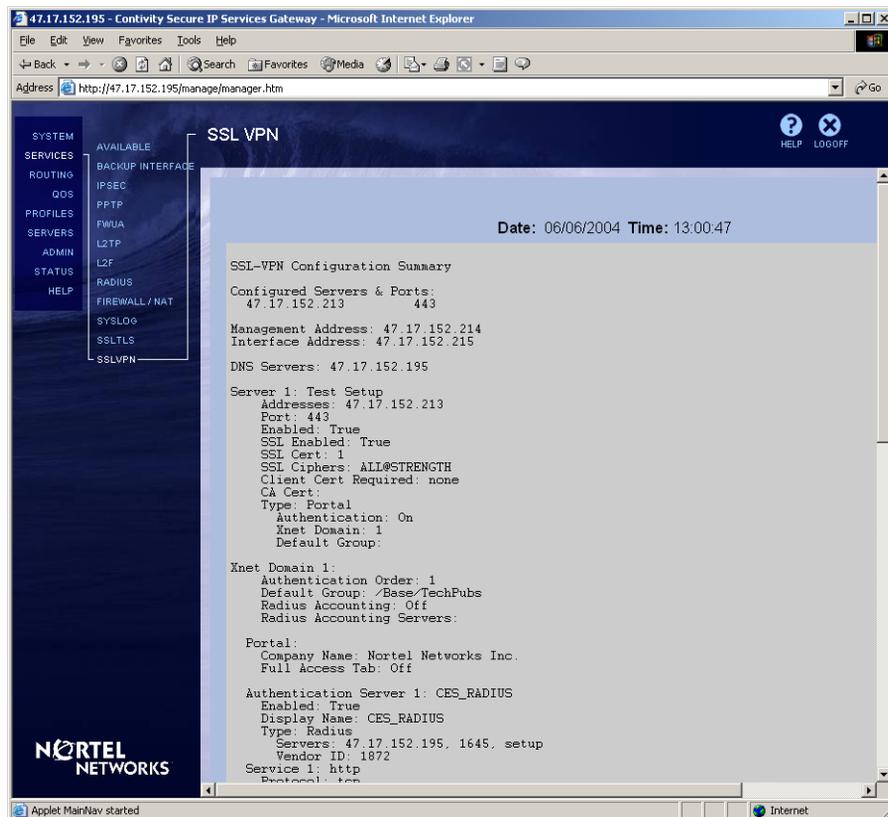
```
https://x.x.x.x/  
or  
https://<domain_name>
```

where *x.x.x.x* is the public interface of the Contivity gateway and *<domain_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 94 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 Domains > Domain 1 > Authentication.
- 3 Right-click on 1 CES_RADIUS (if it exists) and delete it.
- 4 Click on Domains > Domain 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 Domains > Domain 1 > Groups > 1: <name>.
 - 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

A

access rules 97
accounting 138
Advanced tab 36
alarms 202
authentication
 client certificate 118
 external database 117
 LDAP 126
 NTLM 131
 RADIUS 121
 SiteMinder 134

B

Browse Intranet tab 31
browser requirements 28

C

certificate revocation list (CRL)
 revoke certificates issued by CA 63
certificate signing request (CSR)
 generate 88
 submit 88
certificates 88
 adding 91
 revoking 120
 updating 93
certificates formats 91
ciphers 189
 list format 191
 modifying list 191

 strings 192
client authentication 88
clientless mode 27
colors, customize the portal 59
company name, customize the portal 61
CRL, see certificate revocation list
CSR, see certificate signing request
customer support 22

E

events 204

F

feature summary 24
file server link 149, 150
Files tab 32

G

group portal links 105
 defining 105
 examples 149

H

hardware platforms 23
Home tab 30
HTTP proxy 38
HTTP to HTTPS redirect service 144

K

key code definition file 224
key code definitions 221
key formats 91

L

LDAP
 authentication 126
LDAP authentication 126
LDAP dictionary information tree 130
links, on Portal
 file server link 150
links, on portal
 file server link 149
load balancing 146
 metrics 147
login screen 28
logo, customize the portal 60
Logout tab 48

M

macros
 password 154
 user 150, 154
messages
 troubleshooting 225
MIBs 195

N

naming login services 63
Netegrity SiteMinder, authentication 134
NTLM authentication 131

O

outlook port forwarder 45

P

port forwarder, general 41
portal
 Advanced tab 36
 automatic redirection 64
 Browse Intranet tab 31
 changing colors 59
 colors 59
 company name 61
 default appearance 57
 Files tab 32
 general tab 55
 Home tab 30
 logo 60
 Logout tab 48
portal settings 139
product support 22
publications
 hard copy 22

R

RADIUS accounting 138
RADIUS authentication 121
 external users 124
 internal users 123
RADIUS proxy
 group attribute 124
redefinable keys 223
redirect service 144
redirect user 64
revoke
 certificates issued by external CA 63

S

single sign-on domains 136
SiteMinder authentication 134
SNMP
 supported MIBs 195
 supported traps 198

- SOCKS server 146
- special characters 222
- special keys 221
- SSL virtual server
 - configuring 118
- SSL VPN
 - authentication mechanisms 114
 - configuring authentication 110
 - features 24
 - license key 27
 - overview 23
 - upgrading 84
- support, Nortel Networks 22
- supported
 - certificate formats 91
 - key formats 91
- syslog messages 199
 - alphabetical 212
 - configuration reload 211
 - control process 201
 - operating system 199
 - processing subsystem 205
 - startup 210
- syslog messages, list of 199

T

- technical publications 22
- technical support 22
- Telnet/SSH access 36
 - link 157
- traps 198
- troubleshooting 225

U

- unified access portal 29
- upgrades 85
 - activating 86

