

Quick Guide



Browser-Based Interface Alteon SSL Accelerator™

Part Number: 215310-B, November 2003



4655 Great America Parkway
Santa Clara, CA 95054
Phone 1-800-4Nortel
www.nortelnetworks.com

Copyright 2003 Nortel Networks, Inc., Great America Parkway, Santa Clara, California 95054, USA. All rights reserved. Part Number: 215310-B.

This document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this document may be reproduced in any form by any means without prior written authorization of Nortel Networks, Inc. Documentation is provided “as is” without warranty of any kind, either express or implied, including any kind of implied or express warranty of non-infringement or the implied warranties of merchantability or fitness for a particular purpose.

U.S. Government End Users: This document is provided with a “commercial item” as defined by FAR 2.101 (Oct 1995) and contains “commercial technical data” and “commercial software documentation” as those terms are used in FAR 12.211-12.212 (Oct 1995). Government End Users are authorized to use this documentation only in accordance with those rights and restrictions set forth herein, consistent with FAR 12.211- 12.212 (Oct 1995), DFARS 227.7202 (JUN 1995) and DFARS 252.227-7015 (Nov 1995).

Nortel Networks, Inc. reserves the right to change any products described herein at any time, and without notice. Nortel Networks, Inc. assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Nortel Networks, Inc. The use and purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of Nortel Networks, Inc.

Browser-Based Interface, BBI, Alteon 2424, 2424-SSL, and Alteon 2448 are the trademarks of Nortel Networks in the United States and certain other countries. Microsoft®, Windows®, and Windows NT® are registered trademarks of Microsoft Corporation in the United States and in other countries. Netscape® and Netscape Navigator® are registered trademarks of Netscape Communications Corporation in the United States and other countries. Any other trademarks appearing in this manual are owned by their respective companies.

Contents

Preface 5

Who Should Use This Book 5

Related Documentation 5

Hardware Installation 5

ASA System Information and Software Configuration 6

Where to Find Documentation 6

Typographic Conventions 7

How to Get Help 8

Chapter 1: Getting Started 9

Features 9

Requirements 10

Minimum Setup 10

SSL BBI Setup for ASAs 10

SSL BBI Setup on 2000-SSL Series Switches 12

IP Interface and VLAN Configuration Commands 12

SSL Processor MIP Address and SSL BBI Port Setup 13

SSL Processor Setup 13

Chapter 2: The SSL Browser-Based Interface 15

Web Browser Setup 15

Host Setup 15

Starting the SSL BBI 16

Basics of the Browser-Based Interface 18

Interface Components 18

Basic Operation 19

SSL BBI Forms Reference 20

Global Command Forms 20

Apply 20

Diff 22

Revert 23

Logout 23

Help 24

Site Map 25



Preface

This *Quick Guide* provides an overview of how to access and use the Browser-Based Interface (BBI) that is part of the Alteon Secure Sockets Layer (SSL) Accelerator (ASA) software. The SSL BBI lets you use your Web browser to access most ASA configuration and monitoring functions available through the Command Line Interface (CLI).

Who Should Use This Book

This *Quick Guide* is intended for network installers and system administrators engaged in configuring and maintaining a network. It assumes that you are familiar with your ASA product (ASA 310, ASA 310-FIPS, ASA 410 or Alteon Application Switch 2000-SSL Series), your Web browser, Ethernet concepts, IP addressing, the IEEE 802.1d Spanning-Tree Protocol, and SNMP configuration parameters.

Related Documentation

Hardware Installation

For documentation on installing the ASA hardware, see the *Hardware Installation Guide* for your model.

- ASA 310, ASA 310-FIPS, ASA 410:

Alteon SSL Accelerator Hardware Installation Guide (212941-B, August 2002)

- Alteon Application Switch 2000-SSL Series:

NOTE: No ASA hardware installation is required for 2000-SSL Series Switches. The ASA software resides on the SSL Processor which is mounted inside the Switch chassis.

The SSL Processor is a full-featured ASA that runs the same software and system configurations as ASA models, with one restriction: That is, the SSL Processor has only one port that is internally connected to the Switch via back-to-back Gigabit interfaces.

ASA System Information and Software Configuration

For details about the information, statistics, and configuration parameters that you can manage using the SSL BBI, see the *Command Reference* and *Application Guide* for your model.

- ASA 310, ASA 310-FIPS, ASA 410:
 - *Alteon SSL Accelerator User's Guide and Command Reference* (212939-F, Nov. 2003)
 - *Alteon SSL Accelerator Application Guide* (212940-F, Nov. 2003)
 - Alteon Application Switch 2000-SSL Series:
 - *Alteon SSL Accelerator User's Guide and Command Reference* (212939-F, Nov. 2003)
 - *Alteon SSL Accelerator Application Guide* (212940-F, Nov. 2003)
- NOTE:** Because of the operational similarities, the same ASA documentation you use for ASA models applies to the ASA functionality on 2000-SSL Series Switches.
- *Alteon Application Switch 2000-SSL Series Quick Setup Guide* (215102-B, Nov. 2003)
This *Quick Setup Guide* includes system description and setup instructions that are specific to 2000-SSL Series Switches.
 - *Alteon OS Browser-Based Interface Quick Guide* (315395-C, Nov. 2003)
This *Quick Guide* documents the Switch BBI for the Alteon OS software that runs on 2000-SSL Series Switches. The Switch BBI also provides access to the SSL BBI, which is documented in this *Quick Guide* as well.

Where to Find Documentation

These manuals are on the Documentation CD that shipped with your system. You can also download these manuals from the Nortel Networks Customer Support Web site. To access the site:

- Point your browser to: <http://www.nortelnetworks.com/cs>.
- Enter the registered user name and password previously assigned to you by Nortel Networks Customer Support.

If you are not a registered user at Nortel Networks, please click on the **Register** button on the left-hand column of the Nortel Networks Customer Support Web site, and follow the 5-step registration process.
- Select Alteon ► Alteon SSL Accelerator (Documentation)

or

Select Alteon ► Alteon Application Switch 2424-SSL (Documentation)

Typographic Conventions

The following table describes the typographic styles used in this book.

Table 1 Typographic Conventions

Typeface or Symbol	Meaning	Example
AaBbCc123	This type is used for names of commands, files, and directories used within the text. It also depicts on-screen computer output and prompts.	View the <code>readme.txt</code> file. Main#
AaBbCc123	This bold type appears in command examples. It shows text that must be typed in exactly as shown.	Main# sys
<AaBbCc123>	This italicized type appears in command examples as a parameter placeholder. Replace the indicated text with the appropriate real name or value when using the command. Do not type the brackets. This also shows book titles, special terms, or words to be emphasized.	To establish a Telnet session, enter: host# telnet <IP address> Read your <i>User's Guide</i> thoroughly.
[]	Command items shown inside brackets are optional and can be used or excluded as the situation demands. Do not type the brackets.	host# ls [-a]

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 one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone
Europe, Middle East, and Africa	(33) (4) 92-966-968
North America	(800) 4NORTEL or (800) 466-7835
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

Additional information about the Nortel Networks Technical Solutions Centers is available at the following URL:

<http://www.nortelnetworks.com/help/contact/global>

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, refer to the following URL:

<http://www.nortelnetworks.com/help/contact/erc/index.html>



CHAPTER 1

Getting Started

This chapter describes the software features and requirements for the Alteon SSL Accelerator (ASA) Browser-Based Interface (SSL BBI) and explains how to access the SSL BBI start page.

Features

You can access virtually all ASA configuration and monitoring functions through the SSL BBI, a Web-based management interface for the ASA. The SSL BBI has the following features:

- Most of the configuration and monitoring functions of the Command Line Interface (CLI)
- Intuitive, easy-to-use interface structure
- Nothing to install; the SSL BBI is part of the SSL software
- Two levels of password protection
- Can be upgraded as future software releases are available
- Can be accessed using HTTP, or secure HTTPS
- Up to 10 simultaneous BBI sessions

Requirements

- ASA hardware:
 - ASA 310, ASA 310-FIPS, ASA 410
 - Alteon 2000-SSL Series Application Switch (with internally-mounted SSL Processor)
- ASA software Release 4.1.2 or higher
- PC or workstation with network access to the device
- Frame-capable Web-browser software, such as the following:
 - Netscape Navigator 4.7x or higher
 - Internet Explorer 5.5x or higher
- JavaScript enabled in your Web browser

Minimum Setup

To access the SSL BBI, a minimum configuration is required on your ASA hardware (ASA 310, ASA 310-FIPS, ASA 410). If you have a 2000-SSL Series Switch, the same setup is required on your SSL Processor with some notable differences.

SSL BBI Setup for ASAs

After completing the Initial Setup procedure for your model (see the *ASA User's Guide and Command Reference*), additional configuration is required to permit SSL BBI access.

NOTE – Make sure that the host IP and MIP addresses that you entered during Initial Setup are accessible to your browser host's network.

1. Enable the SSL BBI.

By default, the SSL BBI is disabled for HTTP and HTTPS access. The SSL BBI can be enabled for HTTP and/or HTTPS.

NOTE – HTTP is not a secure protocol. All data (including passwords) between an HTTP client and the Alteon SSL Accelerator is unencrypted and is subject only to weak authentication. If secure remote access is required, consider using HTTPS instead of HTTP.

To allow remote SSL BBI access, enter the following commands in the CLI.

- To enable HTTP access and set the HTTP logical port:

```
>> Main# /cfg/sys/adm/http/ena           HTTP access enabled
>> Main# /cfg/sys/adm/http/port 80       HTTP port set to 80 (default)
```

NOTE – The default HTTP port value is well-known HTTP port 80. If you change this value (e.g., to 81), users must append the port value to the host IP address (e.g., http://10.10.1.110:81) when opening a connection to the ASA or SSL Processor.

- To enable HTTPS access:

```
>> Main# /cfg/sys/adm/https/ena          HTTPS access enabled
>> Main# /cfg/sys/adm/https/port 1025    HTTPS port set to 1025
```

You may choose any port for SSL BBI traffic, except one that is used by other traffic on your system (the SSL CLI, in fact, will reject the selection of ports that are known to bear traffic).

2. Add your browser host's network address to the access list:

```
>> Main# /cfg/sys/adm/accesslist/add <network IP address>
```

This step is optional. If the list is empty, there are no access restrictions based on the client network IP address.

3. Enter the netmask and default gateway information:

```
>> Main# /cfg/sys/netmask <network mask>
>> Main# /cfg/sys/gateway <default gateway address>
```

4. Apply the changes.

```
>> Main# apply
```

SSL BBI Setup on 2000-SSL Series Switches

After completing the Initial Setup procedures for your model (refer to “[Related Documentation](#)” on page 5), you must configure SSL BBI access to the SSL Processor. This information allows direct access to the SSL Processor for HTTP or HTTPS connections:

- At least one IP interface must be configured on the Switch that is:
 - On a data port designated for remote management of the SSL Processor
 - On the same network as the SSL Processor host IP and Master IP (MIP) address
 - Accessible by the browser host network
- VLAN 4090 (the SSL VLAN) must be enabled and the Switch data port designated for remote SSL Processor management access must be assigned to VLAN 4090.
- The Switch must *know* the SSL Processor MIP and HTTPS port number (see NOTE TO 2000-SSL SERIES SWITCH USERS on [page 1-13](#)).
- The SSL Processor host IP and MIP must be on the same network as the interface IP address.
- The SSL Processor default gateway must be set to the interface IP address.

IP Interface and VLAN Configuration Commands

You can enter IP interface and VLAN information during Initial Setup (refer to the *Alteon Application Switch 2000-SSL Series Quick Setup Guide* for Initial Setup instructions). Below are the specific CLI commands you must use. For this example, IP interface 1 on data port 7 is designated for remote SSL Processor management access:

>> Main# /cfg/port 7/pvid 4090	Port 7 VLAN ID
>> Main# /cfg/ip/ifa 1/ena	Interface 1 enabled
>> Main# /cfg/ip/ifa 1/addr 10.10.10.102	Interface 1 IP address
>> Main# /cfg/ip/ifa 1/mask 255.255.255.0	Interface 1 netmask
>> Main# /cfg/ip/ifa 1/vlan 4090	Interface 1 VLAN (same as Port 7)
>> Main# /cfg/ip/gw 1/ena	Default gateway 1 enabled
>> Main# /cfg/ip/gw 1/10.10.10.1	Default gateway 1 IP address
>> Main# apply	Apply changes

SSL Processor MIP Address and SSL BBI Port Setup

To establish an HTTPS link with the SSL Processor, the switch must know the SSL Processor MIP address and SSL BBI port. These values are set at the SSL Processor Setup Menu:

>> Main# /cfg/sslproc/mip 10.10.10.108	<i>SSL Processor IP address</i>
>> Main# /cfg/sslproc/port 1025	<i>SSL Processor BBI port</i>
>> Main# apply	<i>Apply changes</i>

NOTE TO 2000-SSL SERIES SWITCH USERS – You may choose any port for SSL BBI traffic, except one that is used by other traffic (the SSL CLI, in fact, will reject the selection of ports that are known to bear traffic). For example, do not select port 443; the SSL Processor uses this port to accelerate traffic. Also, the port you choose must be the same one you chose with the SSL /cfg/sys/adm/https/port command (see “[SSL Processor Setup](#)” below).

SSL Processor Setup

The procedure for ensuring SSL BBI access on an SSL Processor is the same as for an external ASA (see “[SSL BBI Setup for ASAs](#)” on page 10). Refer to the *AAS 2000-SSL Series Quick Setup Guide* for Initial Setup instructions.

There are several additional considerations you must observe:

- For the SSL Processor default gateway, enter the IP interface address of the Switch data port designated for remote SSL Processor management access.
- There is only one SSL Processor port (port 1).
- The port value you select for HTTPS access must be the same as the value entered at the Switch CLI using the /cfg/sslproc/mip command (see “[SSL Processor MIP Address and SSL BBI Port Setup](#)”).

In this example, the SSL Processor information is compatible with the Switch command information entered above:

SSL >> Main# /cfg/sys/cluster/host 1/ip 10.10.10.107	<i>Cluster Host IP address</i>
SSL >> Main# /cfg/sys/cluster/mip 10.10.10.108	<i>Cluster MIP address</i>
SSL >> Main# /cfg/sys/netmask 255.255.255.0	<i>Cluster netmask</i>
SSL >> Main# /cfg/sys/gateway 10.10.10.102	<i>Cluster default gateway</i>
SSL >> Main# /cfg/sys/adm/http/ena	<i>HTTP access enabled</i>
SSL >> Main# /cfg/sys/adm/http/port 80	<i>HTTP port (default)</i>
SSL >> Main# /cfg/sys/adm/https/ena	<i>HTTPS access enabled</i>
SSL >> Main# /cfg/sys/adm/https/port 1025	<i>HTTPS port (default)</i>
SSL >> Main# apply	<i>Apply changes</i>



CHAPTER 2

The SSL Browser-Based Interface

This chapter describes the SSL BBI and how to use it. The global commands, site navigation, and on-line help access are described in detail. For detailed command reference information, refer to the on-line help or to the *ASA User's Guide and Command Reference* (see [“Related Documentation” on page 5](#)).

Web Browser Setup

Once you have configured your system for Web access, you can connect to the SSL BBI through a properly configured Web browser.

To display the SSL BBI, your browser must be configured to work with frames and JavaScript. Both the Netscape and Internet Explorer browsers that have been verified to work with the SSL BBI (see [“Requirements” on page 10](#)), are default-configured to work with frames and JavaScript, and require no additional set up. However, you should check your Web browser's features and configuration to make sure frames and JavaScript are enabled.

NOTE – JavaScript is not the same as Java. Please make sure that JavaScript is enabled in your Web browser.

Host Setup

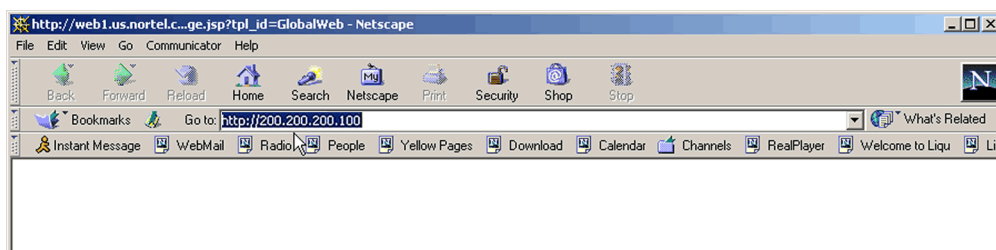
Refer to [“Minimum Setup” on page 10](#) or to the user documentation for your host (ASA or SSL Processor) for configuring web access on your system (see [“Related Documentation” on page 5](#)).

Starting the SSL BBI

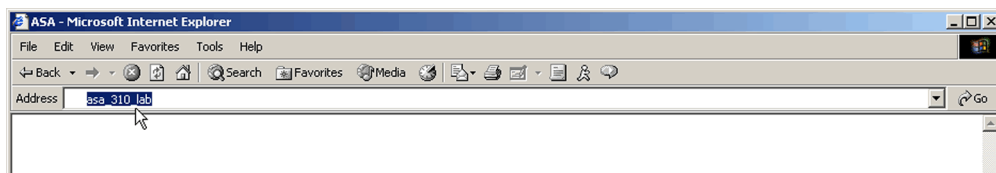
Once you have completed the necessary setup procedures, follow these steps to launch the SSL BBI:

1. **Start your Web browser.**
- 2a. **For http connections, enter `http://<host IP or MIP address or DNS name>` in the Web browser URL field.**

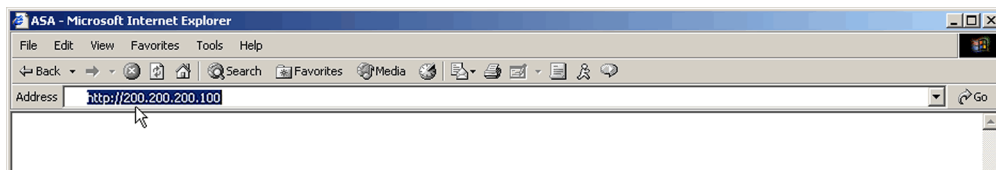
For example, if your host IP address is 200.200.200.100, using Netscape Navigator, you would enter the following:



- 2b. **If the host name (e.g., `asa_310_lab`) for 200.200.200.100 has been added to your local domain name server, you could enter it instead. Using Internet Explorer, you would enter the following:**



- 2c. **For https connections, enter `https://<host MIP address>:<port number>` in the browser URL field.**



3. Log in to the ASA or SSL Processor.

If your host and browser are properly configured, you will be asked to enter a password:

Enter the account name and password for the host's administrator or user account. For more password information, see your *Command Reference* manual.

Proper host configuration includes a host IP that is accessible to your browser network.

4. Allow the host Information page to load.

When the proper account name and password combination is entered, the iSD Information page (the first page in the SSL BBI) is displayed in your browser's viewing area:

IP Address	Status	Type	MIP	Local	CPU %	Memory %
200.200.200.100	up	master	true	true	1	42

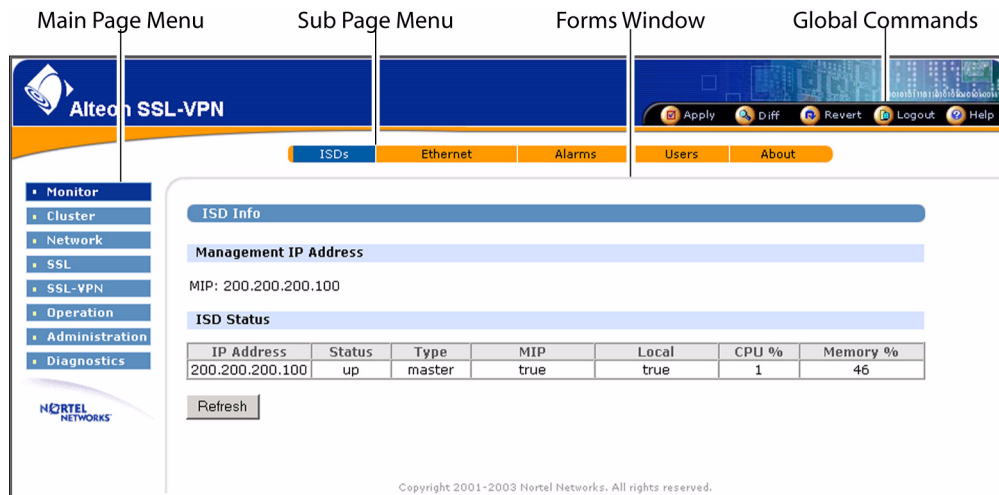
Refresh

Copyright 2001-2003 Nortel Networks. All rights reserved.

Basics of the Browser-Based Interface

Interface Components

The SSL BBI screen consists of the following areas:



■ Main Page Menu

The buttons in this area (Monitor, Cluster, and so on) represent the main categories of forms available for collecting information and configuring the system. Each main category contains a variety of sub-pages.

■ Sub-Pages Menu

These buttons represent the sub-categories under each main page. A different list of sub-pages is available for each main page. When a sub-page is selected, the appropriate information and configuration fields are displayed in the forms area.

The various pages are described in detail in the [“SSL BBI Forms Reference” on page 20](#).

■ Forms Area

This area contains fields that display information or allow you to specify information for configuring the system. The fields are different for each sub-page.

■ Global Command Buttons

These buttons are available from any page. The buttons display forms used for saving, examining, or aborting configuration changes, and for displaying help information for the current page.

Basic Operation

The Browser-Based Interface allows you to administer the Alteon SSL Accelerator in the following manner. In order to access the full functionality of the SSL BBI, you must be logged in as administrator:

- Select from a series of pages and sub-pages, and modify fields to create the desired configuration.
- When finished making changes on any given page, submit the form using the appropriate Update buttons. If you select a new form or end the session without submitting the information, the changes are lost.
Most submitted changes are considered pending and are not immediately put into effect or permanently saved. Only a few types of changes take effect as soon as the form is submitted: changes to users and passwords, and setting the time or time zone.
- Use the global Apply form to save changes and make them take effect. The apply form allows the administrator to make an entire series of updates on multiple forms and then put them into effect all at once.
- From the Apply form, validate the configuration to check for any configuration problems prior to applying them. If the configuration is in an invalid state, the Apply command will not be allowed.
- Use the global Diff form to view pending changes before they are applied.
- Use the global Revert form to clear all pending changes; then continue the configuration session, or use the global Logout form to exit from the system. Logging out manually is preferred, though closing your browser manually or through inactivity (browser sessions automatically close after five minutes of inactivity) will also discard pending changes.

NOTE – When multiple CLI or SSL BBI administrator sessions are open at the same time, only pending changes made during your current session will be affected by the Diff, Revert, or Logout commands. However, if multiple CLI or SSL BBI administrators apply changes to the same set of parameters concurrently, the latest applied changes take precedence.

SSL BBI Forms Reference

Global Command Forms

The global command buttons are always available at the top of each form:



These buttons summon pages which are used for logging out, saving, examining, or aborting configuration changes, and for displaying help information. Each global command page provides options to verify or cancel the command as appropriate.

Apply

The global Apply form is used for checking the validity of the current session's pending configuration changes, and for saving the configurations change and putting them into effect.

The Global Apply form includes the following items:

- Apply Changes pop-up menu. To use this menu, select one of the following options and click on the Submit button:
 - Apply Changes

When submitted, this action updates the device with any pending configuration changes. Pending changes are first validated for correctness (see below). If problems are found, applicable warning and error messages are displayed. If errors are found, the changes are not applied. If there are no errors (warnings are allowed), the changes are saved and put into effect.

This command has no effect on pending changes in other open CLI or SSL BBI sessions.

NOTE – The global **Revert** command clears pending changes. It cannot be used to restore the old configuration after the **Apply Changes** command has been issued.

□ **Validate Configuration**

When submitted, this button validates the current session's pending changes, but does not apply them. The pending configuration changes are examined to ensure that they are complete and consistent. If problems are found, the following types of messages are displayed:

Warnings. These appear in yellow. Warnings identify conditions that the administrator should pay special attention to, but which will not cause errors or prevent the configuration from being applied.

Errors. These appear in red. Errors identify serious configuration problems that must be corrected before changes can be applied. Uncorrected errors will cause the **Apply Changes** command to fail.

If the configuration is valid, the administrator must still separately submit the **Apply Changes** command.

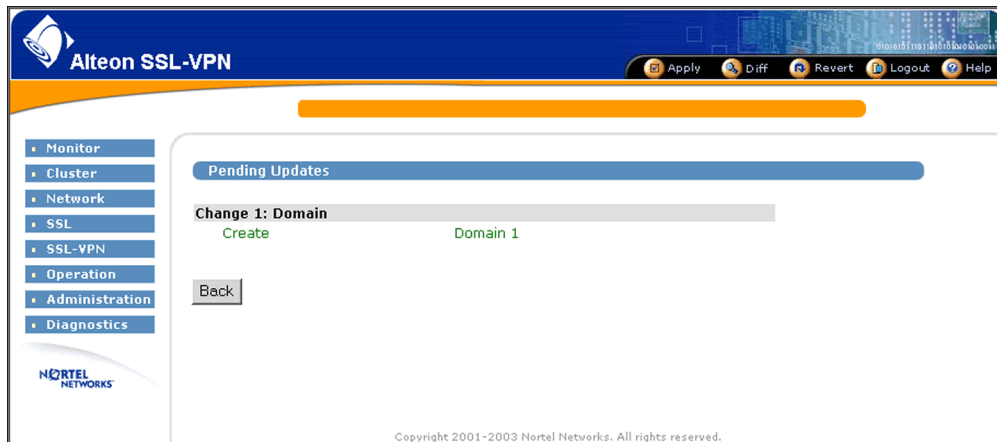
□ **Run Security Audit**

When submitted, this option lists security information, such as the status (enabled or disabled) for remote management features such as Telnet, SSH, and the SSL BBI for the cluster and the IP addresses which can access them. It also lists which users (if any) are still configured with default passwords which should be changed.

- **Submit button.** This button performs the action selected in the **Apply Changes** pop-up menu.
- **Back.** This button returns the previously viewed form without applying changes.

Diff

The global Diff form provides a list of the current session's pending configuration changes.



The list displays a change record for each submitted update. Each record may consist of many modifications, depending upon the complexity of the form and changes submitted. Modifications are color coded:

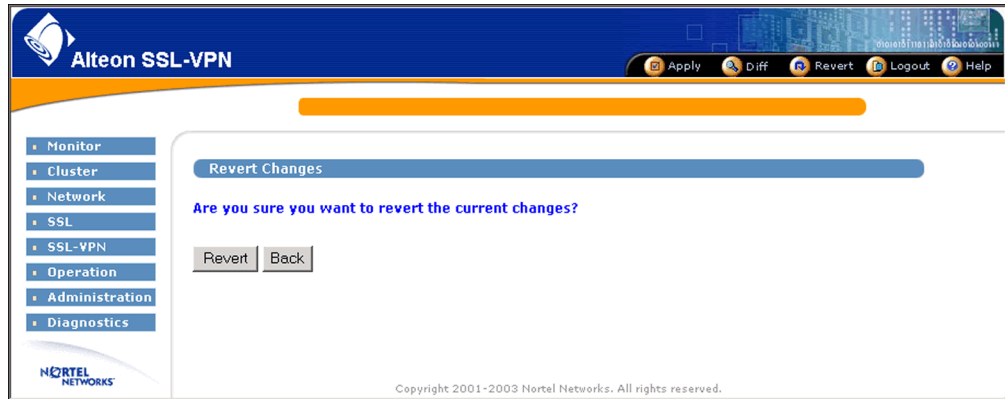
- Green: New items that will be *added* to the configuration when the global Apply command is given and verified.
- Blue: Existing items that will be *modified*.
- Red: Configuration items that will be *deleted*.

The Diff list is cleared when configuration changes are applied or reverted, or when the administrator logs out or closes the browser window.

This command does not include pending changes made in other open CLI or SSL BBI sessions.

Revert

The global Revert form is used for canceling pending configuration changes.

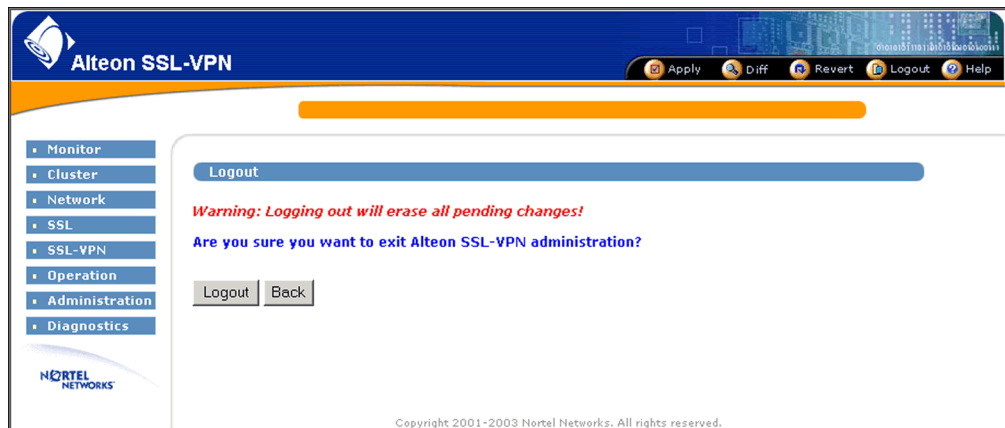


This form includes the following items:

- Revert Changes button. This button cancels the current session's pending configuration changes. Applied changes are not affected. Pending changes made in other open CLI or SSL BBI sessions are not affected.
- Back button. This button returns the previously viewed form without cancelling pending changes.

Logout

The global Logout form is used to terminate the current user session.



This form includes the following items:

- Logout button. This button terminates the current user session. Any configuration changes made during this session that have not yet been applied will be lost. This command has no effect on pending changes in other open CLI or SSL BBI sessions.
- Cancel button. This button returns the previously viewed form without logging out.

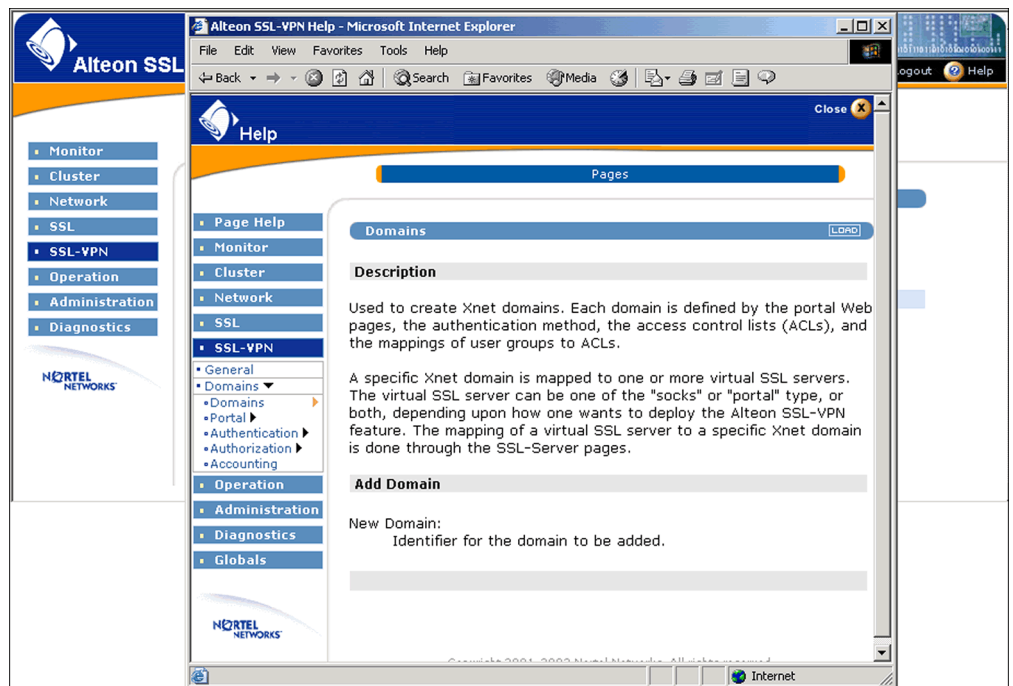
NOTE – For thorough security, close all SSL BBI windows (including help) after logging out.

Help

The global Help form provides assistance with forms and tasks in the SSL BBI. There are two kinds of help: context-sensitive help and task-based help.

Page Help

Page Help help displays detailed information about the form that is presently displayed. When you click on the global Help button, a new window appears with information appropriate to your current options:



The help window consists of the following areas:

- **Help Topic Menu.** Select a new help topic using the menu on the left side of the Page Help window. Each main menu item is listed. Sub-menu items are listed when a main menu item is selected. Select any sub-menu item to display help for the relevant form.
 - The Page Help selection contains general instructions on how to use the SSL BBI to administer the system.
- **Pages Bar.** Refreshes Help Page.
- **Forms Area.** Displays detailed information about the selected topic.
- **Load Button.** Jumps directly to the form currently referenced by the Page Help window.
- **Close Button (top right corner).** Closes the Page Help window.

Site Map

The Site Map table below provides the list of sub-page menus and status/command labels for each form to aid navigation through the SSL BBI. Items in parenthesis are for clarification or to indicate the operations that can be performed.

Table 2-1 SSL BBI Site Map

Form	Sub-Page Menu	Status and Command Labels
Monitor	iSD	Management IP, Host IP, Status, Type, MIP (True/False), Local (True/False), CPU Usage, Memory
	Ethernet	Transmit/Receive Statistics (Per Host/Network)
	Alarms	Name, Sender, Cause, Severity, Time
	Users	List Current Users per Domain #/Prefix
	About	Product Name: (Alteon SSL-VPN) and Software Version
Cluster	iSD	General (Halt/Reboot/Delete iSD per MIP), Interfaces (Add/Modify/Delete per Host #) Ports (Define/Add per Host #), Gateway (Define/Add per Host #) Routes (Define/Add per Host #) License (List/Add per Host #)
	Trace	Enable/Disable
	Time	Settings: Date, Time, Timezone (Modify)
	Syslog	Current Remote Servers (Add/Modify/Delete Remote Servers)

Table 2-1 SSL BBI Site Map

Network	DNS	DNS Servers (Add/Modify/Delete New DNS IP)
	NTP	NTP Server (Update)
	Routes	Destination IP, Gateway IP (Add/Modify/Delete Routes)
SSL	Servers	List, General Settings (Modify/Update), Types (HTTP, Portals, SOCKS) SSL, TCP, Load Balancing (General, Cookies, Health Check, Remote Connect, Backend Servers), Advanced (Strings, Blocking Strings, Pooling, Traffic Log, Standalone, SSL Connect)
	Certificates	List, Import (File, Text) Generate (Request, Signed Certificate, Test Certificate, Private Key), Sign Request, Revoke (General, Automatic CRL), Export (To File, Key Encryption)
	DNS Client	Settings (DNS Cache Size, Retransmit Interval, Retransmit Counter, Max TTL, Health Check Interval, Health Check Down Counter, Health Check Up Counter)
SSL VPN	General	Login Session Time-To-Live, User Session Logging (Update)
	Domains	Current Domains (List/Delete) Add New Domains
	Domains/ Portal	General (Domain #, Brand Name Enter/Update), Banner (Current Banner, New Banner Browse/Submit), Redirect URL (Enter/Update per Domain #), Link Text (Enter/Update per Domain), Colors (Text Colors Enter/Update per Domain #), Company (Company Name Enter/Update per Domain #)
	Domains/ Authentication	Authentication Server (Define/Add per Domain #) Authentication Order (Available/Selected Update per Domain #)
	Domains/ Authorization	Groups (Define/Add per Domain #), Networks (Define/Add per Domain #), Services (Define/Add per Domain #), Application (Define/Add per Domain #), Client Filters (Define/Add per Domain #)
	Domains/ Accounting	RADIUS Accounting (Enable/Define/Add per Domain #)
Operation	Configuration	Secret Key (Export), Import Cluster Configuration (Browse for File, Paste, Submit)
	Software	Packages (Activate), Upload New Package (Browse for File, Submit)
Administra- tion	Users	Administration Users (Add Modify/Delete; except default usernames), Password (Update), Password Expire Time (Update)

Table 2-1 SSL BBI Site Map

	Accesslist	Client Access List (Add/Delete/Modify) NOTE – Access is restricted to clients in the list. An empty list means access is unrestricted.
	Telnet-SSH	Telnet-SSH Settings (Enable/Disable), CLI Timeout, SSH Key Generation (Generate)
	Web	HTTP/HTTPS (Enable/Disable), Port # (Modify)
	SNMP	System (SNMP v2 MIBs, Authentication Traps), Community (Read, Write, Trap), Notification Target (IP Address, Port, Version)
	Auditing	General (Status, Vendor ID/Type), RADIUS Server
	Diagnostics	
	Logs	File Name, Size, Last Modification Date (Download)
	Events	List Events Log per iSD
	Maintenance	Dump Logs/Statistics (Protocol, Server, File, iSDs)

