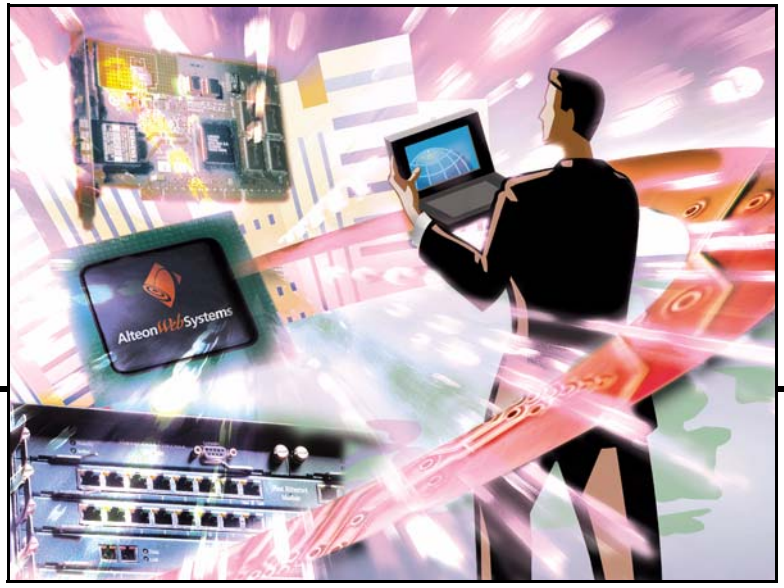
Release Notes



Alteon SSL Accelerator

SSL VPN version 4.2.1

Part Number: 216372-A, May 2004

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

Export

This product, software and related technology is subject to U.S. export control and may be subject to export or import regulations in other countries. Purchaser must strictly comply with all such laws and regulations. A license to export or reexport may be required by the U.S. Department of Commerce.

Licensing

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
This product includes software written by Tim Hudson (tjh@cryptsoft.com).
This product includes software developed by the Apache Software Foundation (http://www.apache.org/).
See Appendix D, "License Information", in the *User's Guide* for more information

Release Notes

These Release Notes provide the latest information regarding your Nortel Networks Alteon SSL Accelerator (ASA) with SSL VPN version 4.2.1 software. This supplement lists the new features and modifies some information found in the complete documentation:

- *SSL VPN User's Guide* (part number 216368-A)
- *SSL VPN Command Reference* (part number 216369-A)
- *Application Guide for SSL Acceleration* (part number 216370-A)
- *Application Guide for VPN* (part number 216371-A)
- *Alteon SSL Accelerator Hardware Installation Guide* (part number 212941-B)
- *SSL VPN BBI Quick Guide* (part number 215310-C)

These manuals are available for download from Nortel Networks Customer Support Web site. To access the site, proceed as follows:

1. **Point your browser to: http://www.nortelnetworks.com/cs.**
2. **Select Alteon ▸ Alteon SSL VPN (Documentation)**

   For documentation specific to VPN solutions.

   OR

   Select Alteon ▸ Alteon SSL Accelerator (Documentation)

   For documentation specific to SSL Acceleration.
3. **Select the desired document.**

New Features and Enhancements in Software Version 4.2.1

This section lists software features and enhancements added since version 4.1.2. Where applicable, a reference to where the new feature can be found is also included – both as a Command Line Interface (CLI) path or as directions to the proper web form in the Browser-Based Management Interface (BBI).

General

- Support added for cipher suites using AES encryption algorithms.
- Support added for FTP server login, e.g. when downloading a new software version from an FTP server. Previously, anonymous mode was the only option.
- Two-armed configuration wizard added to the Initial Setup procedure in the Command Line Interface (CLI). Lets you configure an ASA with a public and a private interface.
- New command for checking the configuration with respect to connectivity. The command checks that all configured IP connections work, e.g. network, DNS, NTP and RADIUS servers.
  CLI path: `/maint/chkcfg`
  BBI path: Expert>Diagnostics>Maintenance>Check Configuration
- There is now one SNMP agent on each ASA (previously one per ASA cluster), and the agent listens to the IP address of that particular ASA. On the ASA that currently holds the cluster's Management IP address (MIP), the SNMP agent also listens to the MIP.

Portal

- VPN setup wizard added to the Initial Setup procedure in the CLI. Lets you configure the ASA to generate a fully functional Portal in a few steps.
- The Full Access tab is added to the Portal (configurable). From this tab, remote users can activate Nortel's Contivity IPsec client or Nortel's SSL VPN client on their local machine (if installed) for transparent access to the intranet.
  Note: The SSL VPN client version that is compatible with the Full Access tab is available from Nortel Networks upon request.
  CLI path: `/cfg/xnet/domain #/portal/faccess`
  BBI path: SSL-VPN>Domains>Portal>Full Access

NORTEL NETWORKS
216372-A, May 2004

- Support for multiple languages in Portal. Lets you export a template file for translation of text strings appearing on the Portal, e.g. button and field labels, help texts etc.
  CLI path: `/cfg/xnet/lang`
  BBI path: Expert>SSL-VPN>Language

- Configuring the `iauto` Portal link is now done in a different way to support form-based login pages and to prevent the Portal user name and password from being visible in the client browser.
  CLI path: `/cfg/xnet/domain #/group #/link #/iauto`
  BBI path: Shortcuts>Create Links>Domain #>Group #>Add New Link>Link Type>Internal Auto Login URL

- Support added for using SiteMinder as authentication method. SiteMinder is an access management software developed by Netegrity.
  CLI path: `/cfg/xnet/domain #/auth #/siteminder`
  BBI path: SSL-VPN>Domains>Authentication>Auth Servers>Mechanism>siteminder

- Support added for client certificate authentication. Configured as an authentication method (like RADIUS, SiteMinder etc).
  CLI path: `/cfg/xnet/domain #/auth #/cert`
  BBI path: SSL-VPN>Domains>Authentication>Auth Servers>Mechanism>cert

- Automatic configuration of Internet Explorer's proxy settings. This feature is used in the HTTP Proxy link and on the HTTP Proxy tab available under the Portal's Advanced tab.
  CLI path: `/cfg/xnet/domain #/group #/link #/proxy`
  BBI path: Shortcuts>Create Links>Domain #>Group #>Add New Link>Link Type>HTTP Proxy

- Support added for proxy server authentication. Available for Port forwarder, HTTP Proxy and Terminal links.

- Support for proxy chaining via an intermediate intranet HTTP Proxy server has been added for the HTTP Proxy Portal link and the HTTP Proxy feature available under the Portal's Advanced tab.

- New wizards for creating port forwarder links. Supports creating links for Citrix Metaframe, Windows Terminal Server, Mail, Telnet and for network drive mapping.
  CLI path: `/cfg/xnet/domain #/group #/link #/forwarder`
  BBI path: Shortcuts>Create Links>Domain #>Group #>Add New Link>Link Type

- Enhanced file list presentation on the Portal's Files tab (previously labeled File Sharing).

- UDP support added to the Portal's Port forwarder feature (available under the Portal's Advanced tab). Applications using dynamic UDP ports (e.g. NetMeeting and TFTP) are not supported.

- UDP support added to Port forwarder links. Applications using dynamic UDP ports (e.g. NetMeeting and TFTP) are not supported.
- Compact URL. Support added for compressing the URL in port forwarder links. Recommended when defining more than 25 port forwarders in one port forwarder link.
- Support for creating extended profiles requiring client certificate and/or Internet Explorer cache wiper installed on client machine.
  CLI path: `/cfg/xnet/domain #/filter`
  BBI path: Expert>SSL VPN>Domains>Settings>Client Filters
- Support added for RADIUS session timeout. Lets you configure your VPN to retrieve a value in seconds from the RADIUS server, that controls the length of a remote user's VPN session.
  CLI path: `/cfg/xnet/domain #/auth #/radius/sessiontim`
  BBI path: SSL VPN>Domains>Authentication>Auth Servers>Radius Session Timeout
- Support added for white list domains. Feature designed to maintain the secure SSL connection when a user clicks a web link during a Portal session, e.g. on an intranet web page. If the URL matches a domain in the white list, the URL is rewritten with the ASA rewrite prefix, i.e. traffic is sent trough a secure SSL connection.
  CLI path: `/cfg/ssl/server #/portal/whitelist`
  BBI path: SSL VPN>SSL>Servers>Types>Portal>White-list Settings
- Support added for re-setting (i.e. set once again) the Portal session cookie after each HTTP request. The feature was added because some ActiveX components are designed to wipe all cookies, including the Portal session cookie.
  CLI path: `/cfg/ssl/server #/portal/resetcooki`
  BBI path: SSL VPN>SSL>Servers>Types>Portal>Re-Set Session Cookie
- Support added for BEA backend servers when the ASA is used in SSL Acceleration mode.
  CLI path: `/cfg/ssl/server #/http/addbeassl` *and* `addbeacli`
  BBI path: SSL VPN>SSL>Servers>Types>HTTP>WL-Proxy-SSL Header *and* WL-Proxy-Client-Cert Header
- VBScripts that occur in web pages are rewritten in the same way as is done for JavaScripts.
- Text in Portal login window now configurable.
  CLI path: `/cfg/xnet/domain #/portal/logintext`
  BBI path: SSL VPN>Domains>Portal>Login Text

NORTEL NETWORKS
216372-A, May 2004

Browser-Based Management Interface

The Browser-Based Management Interface (or Web GUI) has been completely redesigned to make configuration more user-friendly. The left panel now includes an expandable tree view showing the main configuration categories as folders. Several folders can be expanded at the same time, which gives the operator a good overview of the configuration.

For more information about the Browser-Based Management Interface, see the *SSL VPN BBI Quick Guide*.

Hardware Support

- The SSL VPN 4.2.1 server software version is currently supported on the ASA 310, ASA 410, ASA 310-FIPS, 2424-SSL and VPN Gateway 3050 hardware platforms.
- The SSL VPN client software is supported on Windows 98, Windows ME, Windows 2000 and Windows XP.
  - Windows 95 and NT 4.0 and NT 3.51 are not supported.

TFTP Server Support

- Any correctly functioning TFTP server software (regardless of operating system platform) can be used when upgrading the ASAs. However, the following TFTP server (for Microsoft Windows 95/NT) has been tested and verified to handle the upgrade process correctly:
  - TFTPd32 software (use any search engine to search for "`tftpd32`")
- The following TFTP server software are *not* supported when upgrading the ASA software:
  - Cisco TFTP server software (for Microsoft Windows 95/98/NT)
  - 3Com TFTP server software (for MS-DOS 5.x or higher)

Software Installation and Upgrade Notice

SSL VPN Server Software

The SSL VPN server software is delivered in two different forms, as described below.

- `SSL-4.2.1-upgrade_complete.pkg`

  Using this package is the preferred method for upgrading an existing ASA cluster, as the upgrade is propagated across the cluster and all current configuration is preserved.

  The upgrade procedure is described in “Performing Minor/Major Release Upgrades” in Chapter 4 in the *User's Guide*.

- `SSL-4.2.1-boot.img`

  Using this image will reset the ASA to its factory default configuration. It must be used when an ASA with a different software installed is to be added to a cluster, to bring the additional ASA to the same software version as in the cluster before joining it to the cluster.

  The software reinstall procedure is described in “Reinstalling the Software” in Chapter 3 in the *User's Guide*.

Server Software Download

The server software is available for download from Nortel Networks Customer Support Web site. To access the site, proceed as follows:

1. **Point your browser to: http://www.nortelnetworks.com/cs.**
2. **Select Alteon ▸ Alteon SSL Accelerator (Software) or Alteon SSL VPN (Software)**
3. **Select the desired software release.**
4. **Downloading software requires that you 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, click on **Register** on the left-hand column of the Nortel Networks Customer Support Web site, and follow the 5-step registration process.

Upgrading from Versions Earlier than 2.0.11.15

If you are currently running a software version earlier than 2.0.11.15, upgrade to version 2.0.11.15 (or a later 2.0.11.x version) prior to upgrading to version 3.x or later. The “intermediate” upgrade to version 2.0.11.15 is necessary in order to maintain your current configuration, and to provide reliable fallback in case the upgrade should fail.

Downgrading to Versions Prior to 4.1.1

ASA clusters running software version 4.1.1 or later cannot be downgraded to software versions prior to 4.1.1 and still retain the configuration. To downgrade such a cluster to a version lower than 4.1.1, a complete software reinstall using the boot.img must be performed, followed by manual reconfiguration of the cluster. This is due to changes in the internal database format.

Reverting to 4.2.1 or Higher after Downgrading to 4.1.x

An ASA cluster running software version 4.2.1 can be downgraded to version 4.1.1 or higher. However, after downgrading a cluster initiated with software version 4.2.1 or higher to version 4.1.x, the cluster cannot be upgraded to version 4.2.1 or higher and still retain the configuration. To revert the downgraded cluster to version 4.2.1 or higher, a complete software reinstall using the boot.img must be performed, followed by manual reconfiguration of the cluster. This is due to changes in the internal database format.

Upgrading Clusters Configured with RSA Authentication

The SSL VPN authentication method `rsa` that was introduced in software version 4.1.2.7 is NOT supported in version 4.2.1. Upgrading to 4.2.1 of an ASA cluster configured for RSA authentication will fail. RSA support is planned for a later patch release of 4.2.1. The SSL VPN authentication methods `cert` and `siteminder` were introduced in software version 4.2.1. Downgrading to a lower version number of an ASA cluster with any of these authentication methods configured will fail.

SSL VPN Client Software

A new version of the SSL VPN transparent client software is under controlled release, and is available from Nortel Networks upon request. This version is compatible with the Portal's Full Access tab. To request the transparent client software, point your browser to: **http://www.nortelnetworks.com/help/contact/global/**. Call one of the Technical Support Centers listed on this page.

NOTE – Version 1.0 of the SSL VPN transparent client software does not support the Portal's Full Access tab.

Contivity VPN Client Software

Like the server software (see above), the Contivity VPN client software can be downloaded from Nortel Networks Customer Support Web site. Select **Contivity ▸ Contivity Multi-OS VPN client.** Version 4.91 is the minimum requirement for use with the Portal's Full Access tab.

NOTE – Contivity VPN Client software is not supported by Windows NT 4.0.

NORTEL NETWORKS
216372-A, May 2004

Known Issues

This section lists known issues with software version 4.2.1.

Portal

- The Telnet/SSH Access feature on the Portal's Advanced tab does not work with all versions of Mozilla 1.3 and Netscape 7 (the supported browser types) if Sun's JRE 1.3.x plugin is used. When the feature is invoked from the Portal, there will be a warning message indicating that an upgrade to JRE 1.4.x is necessary on these browsers. In the next patch release, the warning message will be displayed for terminal links as well. (Q00834510)
- Authentication is not performed automatically when using proxy chaining with authentication, if Sun's JRE 1.4.x plugin is used. This however works fine with native JVM and Sun's JRE 1.3.x plugin. (Proxy chaining is an option to specify an intermediate HTTP Proxy host and port, e.g. for the Portal's Telnet/SSH and Custom Port forwarder features). (Q00856931)
- The netdrive port forwarder wizard (`/cfg/xnet/domain #/group #/link #/forwarder/netdrive`) does not work in this version. This will be fixed in the next patch release. (Q00881738)
- The default.htm page presented by web-based WTS (Windows Terminal Server) is not supported through the ASA rewrite engine. This will be fixed in the next patch release. (Q00867149)
- If an iauto (automatic login) link is configured for automatic login to a backend server and that server issues a 401 message (authorization required), followed by a 302 redirection, the client will have to log in manually to the secondary server. This will be fixed in the next patch release. (Q00882254) (Q00886176)
- When configuring an iauto link, the system inspects the type of authentication required by the specified web server and lets you specify the credentials to be filled in detected fields. For form-based Outlook Web Access servers however, the inspection does not discover radio buttons properly and it is not possible to manually configure these parameters using the `/cfg/xnet/domain #/group #/link #/iautoconf/mapping` command. (Q00890579) (Q00890011) (Q00890561)
- URL query filtering (can e.g. be used with Outlook Web Access to prevent users from opening attachments) is not possible in this release. This will be fixed in the next patch release. (Q00881524)

- Users who log out of Outlook Web Access 2003 manually (by clicking the logout button) when using Internet Explorer 6.0 with Service Pack 1, will be kicked out of the Portal session. This will be fixed in the next patch release. (Q00885429)

Documentation

The Release Notes issued for SSL VPN 4.1.2 stated that the `/cfg/xnet/domain # /auth #/adv/groupauth` command required the ASA to authenticate towards the LDAP server to be able to retrieve group information from an LDAP authentication server. This is no longer necessary.

Known Limitations

Browser Requirements

- To support the Telnet/SSH Access, HTTP Proxy and Port forwarder features, the following browser and Java combinations are recommended:
  - Windows:
    Internet Explorer 5 or better with Sun's JRE 1.3 or better
    Internet Explorer 5 or better with Microsoft's JVM 4 or better
    Netscape Navigator 7 with Sun's JRE 1.3 or better
    Mozilla 1.3 or better with Sun's 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
- Configuration via the Browser-Based Management Interface is supported when the following browsers are used:
  - Windows:
    Internet Explorer 5.5 or better
    Netscape Navigator 7.1 or better
    Mozilla 1.5 or better
  - *nix:
    Netscape Navigator 7.1 or better
    Mozilla 1.5 or better

NORTEL NETWORKS
216372-A, May 2004

License

The license is not part of the configuration and will not be included when exporting the configuration using the `/cfg/ptcfg` command. If an ASA configuration is deleted, the license will be deleted as well.

Portal

- A maximum of 256 VPN domains can be created.
- Contivity VPN client 4.91 is the minimum version required for use with the Portal's Full Access tab.
- SSL VPN client 1.1.x (available from Nortel Networks upon request) is the minimum version required for use with the Portal's Full Access tab.
- The language template will not be part of a configuration dump. Import or export the language template manually.
- Proxy chaining (option to specify an intermediate HTTP Proxy host and port, e.g. for the Portal's Telnet/SSH and Custom Port forwarder features) is only supported if SSL is enabled on the portal server.
- Proxy chaining is not supported for the Outlook Port forwarder feature.
- Microsoft Outlook 2003 is not supported when using the Outlook Port forwarder.
- Running the Outlook Port forwarder on a Windows 2000 client requires installing the latest service pack for the operating system.
- Applications using *dynamic* UDP port number allocation (e.g. NetMeeting, TFTP and all streaming media) are not supported by the Port forwarder feature. Applications using *static* port number allocation (e.g. DNS, SNMP) are supported.
- When specifying a URL without a path for an iauto (automatic login) link, e.g. http://www.example.com, enter the URL as `http://www.example.com/`. This will ensure that the root path is implied in the link. Iauto links are created using the `/cfg/xnet/domain #/group #/link #/iauto` command.
- When an iauto link should be used for login to web servers using two-tier basic authentication with domain (i.e. one field for domain\user and one for password), the `/cfg/xnet/domain #/group #/link #/iautoconf/mode` command must be set to `add_domain`.
- Creating a Port forwarder link for mapping a network drive is not supported on Windows 98 and XP clients.

- To create a Port forwarder link for mapping a network drive – and the link is to be used on a Windows 2003 server acting as client – port 445 has to be used instead of the suggested port 139. On the Windows 2003 server, port 445 should be disabled by following these steps:
  - Click Start, select Run and enter `regedit`. The registry editor is started.
  - Locate and select the following key: `HKLM\System\CurrentControlSet\Services\NetBT\Parameters`.
  - On the right panel, double-click the `TransportBindName` entry.
  - In the **Edit string** dialog, delete the displayed value. No value should be specified.
  - Click OK, exit the registry editor and restart the computer.
- The features available on the Portal's Advanced tab (i.e. Telnet/SSH access, HTTP Proxy and Port forwarder) are supported only with SSL v3 and cipher type RC4-MD5.
- The features available on the Portal's Advanced tab are not supported for the TLS protocol.
- Some SSH versions may not be supported when using the SSH feature on the Portal's Advanced tab, e.g. Alteon 184 SSH-1.5-1.2.27.
- Some of Microsoft's Telnet server versions may not be supported when using the Telnet feature on the Portal's Advanced tab.
- Terminal applets do not work with all versions of Mozilla and Netscape 7.x (our supported browser types) if using the Sun JRE plugin 1.3.x. There will be a warning message indicating that an upgrade to JRE 1.4.x is necessary for terminal applet functionality on these browsers (CRQ00834510). The warning message only pops up with terminal applets that are spawned from the manual advanced terminal applet portal page. The fix for a warning message with terminal links will be available in a patch release after version 4.2.1.