

SSL VPN Server Guide

Access Manager Appliance 4.0

November 2013



Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

© 2013 NetIQ Corporation and its affiliates. All Rights Reserved.

For information about NetIQ trademarks, see <https://www.netiq.com/company/legal/>.

Contents

About NetIQ Corporation	7
About This Book and the Library	9
1 Overview of SSL VPN	11
1.1 SSL VPN Features	11
1.2 NetIQ SSL VPNs	14
1.2.1 High-Bandwidth and Low-Bandwidth SSL VPNs	15
1.3 SSL VPN Client Modes	15
1.3.1 Enterprise Mode	16
1.3.2 Kiosk Mode	18
2 Basic Configuration for SSL VPN	21
2.1 Configuring the IP Address, Port, and Network Address Translation	21
2.1.1 Configuring the SSL VPN Gateway behind NAT or L4	22
2.1.2 Configuring the SSL VPN Gateway without NAT or an L4 Switch	24
2.2 Configuring Route and Source NAT for Enterprise Mode	26
2.2.1 Configuring the OpenVPN Subnet in Routing Tables	26
2.2.2 Configuring Source NAT	26
2.2.3 Configuring Source NAT for SSL VPN	26
2.3 Configuring DNS Servers	28
2.4 Configuring Certificate Settings	29
3 Configuring End-Point Security and Access Policies for SSL VPN	31
3.1 Configuring Policies to Check the Integrity of the Client Machine	32
3.1.1 Selecting the Operating System	32
3.1.2 Configuring the Category	33
3.1.3 Configuring Applications for a Category	34
3.1.4 Configuring Attributes for an Application	34
3.1.5 Exporting and Importing Client Integrity Check Policies	38
3.2 Configuring Client Security Levels	39
3.2.1 Client Security Levels	39
3.2.2 Configuring a Security Level	39
3.3 Configuring Traffic Policies	40
3.3.1 Configuring Policies	41
3.3.2 Ordering Traffic Policies	43
3.3.3 Exporting and Importing Traffic Policies	44
3.4 Configuring Full Tunneling	44
3.4.1 Creating a Full Tunneling Policy	44
4 Configuring How Users Connect to SSL VPN	47
4.1 Preinstalling the SSL VPN Client Components	47
4.1.1 Installing Client Components for Linux	47
4.1.2 Installing Client Components for Macintosh	47
4.1.3 Installing Client Components for Windows	48
4.2 Configuring Client Policies	48
4.2.1 Configuring Users to Connect Only in Enterprise Mode or Kiosk Mode	48
4.2.2 Allowing Users to Select the SSL VPN Mode	50

4.2.3	Configuring Client Cleanup Options	50
4.2.4	Configuring SSL VPN to Download the Java Applet on Internet Explorer	51
4.2.5	Configuring a Custom Login Policy for SSL VPN	52
4.3	Configuring SSL VPN to Connect through a Forward Proxy	53
4.3.1	Understanding How SSL VPN Connects through a Forward Proxy	53
4.3.2	Creating the proxy.conf File	53
4.4	Configuring SSL VPN for Citrix Clients	54
4.4.1	Prerequisites	54
4.4.2	How It Works	55
4.4.3	Configuring a Custom Login Policy for Citrix Clients	56
4.4.4	Configuring the Access Gateway to Protect the Citrix Server	56
4.4.5	Configuring Single Sign-On between Citrix and SSL VPN	57
5	Clustering the High-Bandwidth SSL VPN Servers	59
5.1	Prerequisites	60
5.2	Limitations	60
5.3	Creating a Cluster of SSL VPN Servers	60
5.3.1	Creating a Cluster of SSL VPN Servers	60
5.3.2	Adding an SSL VPN Server to a Cluster	62
5.3.3	Removing an SSL VPN Server from a Cluster	62
5.4	Clustering SSL VPN by Using an L4 Switch	63
5.4.1	Configuring a Cluster of Traditional SSL VPNs by Using an L4 Switch	63
5.5	Clustering SSL VPNs by Using the Access Gateway without an L4 Switch	64
5.5.1	Configuring the Access Gateway	64
5.5.2	Installing the Scripts	65
5.5.3	Testing the Scripts	65
5.6	Configuring SSL VPN to Monitor the Health of the Cluster	66
5.6.1	Services of the Real Server	66
5.6.2	Monitoring the SSL VPN Server Health	67
6	Monitoring the SSL VPN Servers	69
6.1	Viewing and Editing SSL VPN Server Details	69
6.2	Enabling SSL VPN Audit Events	70
6.3	Viewing SSL VPN Statistics	71
6.3.1	Viewing the SSL VPN Server Statistics	71
6.3.2	Viewing SSL VPN Server Statistics for the Cluster	73
6.3.3	Viewing the Bytes Graphs	73
6.4	Disconnecting Active SSL VPN Connections	74
6.5	Monitoring the Health of SSL VPN Servers	75
6.5.1	Monitoring the Health of a Single Server	75
6.5.2	Monitoring the Health of an SSL VPN Cluster	76
6.6	Viewing the Command Status of SSL VPN Server	77
6.6.1	Viewing Command Information	78
6.7	Monitoring SSL VPN Alerts	79
6.7.1	Configuring SSL VPN Alerts	79
6.7.2	Viewing SSL VPN Alerts	80
6.7.3	Viewing SSL VPN Cluster Alerts	81
7	Additional Configurations	83
7.1	Customizing SSL VPN User Interface	83
7.1.1	Customizing the Home Page and Exit Page	83
7.1.2	Customizing Error Messages	83
7.2	Creating DH Certificates with Different Key Sizes	84
7.3	Creating a Configuration File to Add Additional Configuration Changes	84

8	Server Configuration Settings	85
8.1	Managing SSL VPN Servers	85
8.2	Configuring SSL VPN Servers	87
8.3	Modifying SSL VPN Server Details	88
A	Troubleshooting SSL VPN Configuration	91
A.1	Successfully Connecting to the Server	92
A.1.1	Connection Problems with Mozilla Firefox	92
A.1.2	Connection Problems with Internet Explorer	93
A.2	The SSL VPN Server Is in a Pending State	93
A.3	SSL VPN Connects in Kiosk Mode, But There Is No Data Transfer	94
A.4	The TFTP Application and GroupWise Notify Do Not Work in Enterprise Mode	94
A.5	SSL VPN Does Not Report	94
A.5.1	Verifying and Restarting JCC	94
A.5.2	Verifying and Restarting the SSL VPN Server	94
A.6	Verifying SSL VPN Components	95
A.6.1	SSL VPN Server	95
A.6.2	SSL VPN Linux Client	95
A.6.3	SSL VPN Macintosh Client	95
A.6.4	SSL VPN Windows Client	96
A.7	Unable to Contact the SSL VPN Server	96
A.8	Unable to Get Authentication Headers	96
A.9	The SSL VPN Connection Is Successful But There Is No Data Transfer	96
A.10	Unable to Connect to SSL VPN Gateway	97
A.11	Multiple Instances of SSL VPN Are Running	97
A.12	Issue with the Preinstalled Enterprise Mode Client	97
A.13	Socket Exception Error After Upgrading SSL VPN	97
A.14	SSL VPN Server Is Unable to Handle the Session	98
A.15	Embedded Service Provider Status Is Red	98
A.16	Connection Manager Log Does Not Display the Client IP Address	98
A.17	SSL VPN Full Tunnel Connection Disconnects on VMware	98
A.18	Clustering Issues	98
A.18.1	Bringing Up the Server If a Cluster Member Is Down	99
A.18.2	Bringing Up a Binary If It Is Down	99
A.18.3	Debugging a Cluster If Session Sharing Doesn't Properly Happen	99
A.19	On Windows XP and 7, Loading ActiveX Takes More than Three Minutes to Connect to SSL VPN	99
A.20	If There Is An Install Log Error, SSL VPN Client In Kiosk Mode Fails To Start	100

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- ♦ Identity & Access Governance
- ♦ Access Management
- ♦ Security Management
- ♦ Systems & Application Management
- ♦ Workload Management
- ♦ Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit <http://community.netiq.com>.

About This Book and the Library

The NetIQ Access Manager Appliance SSL VPN uses encryption and other security mechanisms to ensure that data cannot be intercepted and only authorized users have access to the network. Users can access SSL VPN services from any Web browser.

- ♦ [Chapter 1, “Overview of SSL VPN,” on page 11](#)
- ♦ [Chapter 2, “Basic Configuration for SSL VPN,” on page 21](#)
- ♦ [Chapter 3, “Configuring End-Point Security and Access Policies for SSL VPN,” on page 31](#)
- ♦ [Chapter 4, “Configuring How Users Connect to SSL VPN,” on page 47](#)
- ♦ [Chapter 5, “Clustering the High-Bandwidth SSL VPN Servers,” on page 59](#)
- ♦ [Chapter 6, “Monitoring the SSL VPN Servers,” on page 69](#)
- ♦ [Chapter 7, “Additional Configurations,” on page 83](#)
- ♦ [Chapter 8, “Server Configuration Settings,” on page 85](#)
- ♦ [Appendix A, “Troubleshooting SSL VPN Configuration,” on page 91](#)

Intended Audience

This book is intended for Access Manager Appliance administrators. It is assumed that you have knowledge of evolving Internet protocols, such as:

- ♦ Extensible Markup Language (XML)
- ♦ Simple Object Access Protocol (SOAP)
- ♦ Security Assertion Markup Language (SAML)
- ♦ Public Key Infrastructure (PKI) digital signature concepts and Internet security
- ♦ Secure Socket Layer/Transport Layer Security (SSL/TLS)
- ♦ Hypertext Transfer Protocol (HTTP and HTTPS)
- ♦ Uniform Resource Identifiers (URIs)
- ♦ Domain Name System (DNS)
- ♦ Web Services Description Language (WSDL)

Other Information in the Library

The library provides the following information resources:

- ♦ [NetIQ Access Manager Appliance 4.0 SSL VPN User Guide](#)
- ♦ [NetIQ Access Manager Appliance 4.0 Setup Guide](#)
- ♦ [NetIQ Access Manager Appliance 4.0 Administration Console Guide](#)
- ♦ [NetIQ Access Manager Appliance 4.0 Identity Server Guide](#)
- ♦ [NetIQ Access Manager Appliance 4.0 Access Gateway Guide](#)

NOTE: Contact namsdk@netiq.com for any query related to Access Manager SDK.

1 Overview of SSL VPN

The NetIQ Access Manager Appliance SSL VPN uses Secure Sockets Layer (SSL) as the underlying security protocol for network transmissions. It uses encryption and other security mechanisms to ensure that data cannot be intercepted and only authorized users have access to the network. Users can access SSL VPN services from any Web browser.

- ♦ [Section 1.1, “SSL VPN Features,” on page 11](#)
- ♦ [Section 1.2, “NetIQ SSL VPNs,” on page 14](#)
- ♦ [Section 1.3, “SSL VPN Client Modes,” on page 15](#)

1.1 SSL VPN Features

NetIQ SSL VPN comes with a number of key features that make the product secure, easy to access, and reliable.

Browser-Based End User Access

NetIQ SSL VPN has browser-based end user access that does not require users to preinstall any components on their machines. Users can access the SSL VPN services from any Web browser, from their personal computer, laptop, or from an Internet kiosk.

When users access SSL VPN through the Web browser, they are prompted to authenticate. On successful authentication, a Java applet or an ActiveX control is delivered to the client, depending on the browser. This establishes a secure tunnel between the user’s machine and the SSL VPN server.

Support on Linux, Macintosh, and Windows

The SSL VPN client is supported on Linux, Macintosh, and Windows environments. For a complete list of operating software and browsers that are supported by SSL VPN, see “[Client Machine Requirements](#)” in the *NetIQ Access Manager Appliance 4.0 SSL VPN User Guide*.

Support on 64-Bit Clients

The Enterprise mode SSL VPN can be installed on 64-bit client configurations.

High-Bandwidth and Low-Bandwidth Versions

The SSL VPN comes in high-bandwidth and low-bandwidth versions. The default low-bandwidth SSL VPN server is restricted to 249 simultaneous user connections and a transfer rate of 90 Mbits per second because of export restrictions.

If the export law permits, you can install the high-bandwidth SSL VPN RPM to get the high-bandwidth capabilities, because that version does not have connection and performance restrictions. You can order the high-bandwidth SSL VPN key at no extra cost. It is essential to have the high-bandwidth SSL VPN if you want to cluster the SSL VPN servers.

SSL VPN Installation

The SSL VPN gets installed with the Identity Server and the Administration Console.

Enterprise and Kiosk Modes for End User Access

The NetIQ SSL VPN uses both clientless and thin-client access methods. The clientless method is called the Kiosk mode SSL VPN and the thin-client method is called the Enterprise mode SSL VPN.

In the Enterprise mode, all applications, including those on the desktop and the toolbar, are enabled for SSL, regardless of whether they were opened before or after connecting to SSL VPN. In this mode, a thin client is installed on the user's workstation, and the IP Forwarding feature is enabled by default. For more information on Enterprise mode, see [Section 1.3.1, "Enterprise Mode," on page 16](#).

In the Kiosk mode, only a limited set of applications are enabled for SSL VPN. In Kiosk mode, applications that were opened before the SSL VPN connection was established are not enabled for SSL. For more information on Kiosk mode, see [Section 1.3.2, "Kiosk Mode," on page 18](#).

As SSL VPN server administrators, you can decide which users can connect in Enterprise mode and which users can connect in Kiosk mode, depending on the role of the user. Or you can let the client select the mode in which the SSL VPN connection is made. For more information on how to do this, see [Chapter 4, "Configuring How Users Connect to SSL VPN," on page 47](#). Enterprise mode is available to a user who has the administrator right in a Windows workstation or a root user privilege on Linux or Macintosh workstations. If the user does not have administrator rights or root user privileges for that workstation, the SSL VPN connection is made in Kiosk mode.

Customized Home and Exit Pages for End Users

The home page and the exit page of the SSL VPN can be customized to suit the needs of different customers. For more information, see [Section 7.1, "Customizing SSL VPN User Interface," on page 83](#).

Clustering SSL VPN

The SSL VPN servers can be clustered to provide load balancing and fault tolerance. When you form a cluster of SSL VPN servers, they should all be running the high-bandwidth SSL VPN. For more information on SSL VPN clustering, see [Chapter 5, "Clustering the High-Bandwidth SSL VPN Servers," on page 59](#).

End-Point Security Checks

The SSL VPN has a set of policies that can be configured to protect your network and applications from clients that are using insufficient security restraints and also to restrict the traffic based on the role of the client.

You can configure a client integrity check policy to run a check on the client workstations before establishing a tunnel to the SSL VPN. This check ensures that the users have specified software installed and running in their systems. Each client is associated with a security level, depending on

the assessment of the client integrity check and the relevant traffic policies that are assigned. For more information on configuring end-point security, see [Chapter 3, “Configuring End-Point Security and Access Policies for SSL VPN,”](#) on page 31.

Ability to Order Rules

If you have configured more than one rule for a user’s role, the rule that is placed first is applied first. The NetIQ SSL VPN allows you to change the order of rules by dragging and dropping them, based on their priority. For more information on rule ordering in the SSL VPN, see [“Ordering Traffic Policies”](#) on page 43.

Ability to Import and Export Policies

The NetIQ SSL VPN allows you to export the existing configuration into an XML file through the Administration Console. You can reimport this configuration later. This is a very useful feature when you upgrade your servers from one version to another. For more information, see [“Exporting and Importing Traffic Policies”](#) on page 44

Desktop Cleanup Feature

When a user accesses the protected resource from outside by using the SSL VPN, it also means that the sites that the user visited are stored in the browser history, or some sensitive information is stored in the cache or cookies. This is a potential security threat if it is not properly dealt with. The NetIQ SSL VPN client comes with the desktop cleanup feature, so the user has the option to delete all the browser history, cache, cookies, and files from the system, before logging out of the SSL VPN connection.

If the user uses Firefox to connect to SSL VPN, the browsing data that was stored after the SSL VPN connection was made is deleted. In Internet Explorer, all the browser data is deleted, including the data that was stored before the SSL VPN session was established.

Sandbox Feature

When you connect to SSL VPN in either Kiosk mode or Enterprise mode, a folder named VPN-SANDBOX is created on your desktops. You can manually copy files to this folder, including files that you create or files that you download from your corporate network. This folder is automatically deleted along with its contents when you log out of the SSL VPN connection. This is a very useful feature if you are browsing from an Internet connection and you do not want any sensitive information to reach other persons. For more information on the sandbox feature of SSL VPN, see [“Using the Sandbox Feature”](#) in the *NetIQ Access Manager Appliance 4.0 SSL VPN User Guide*.

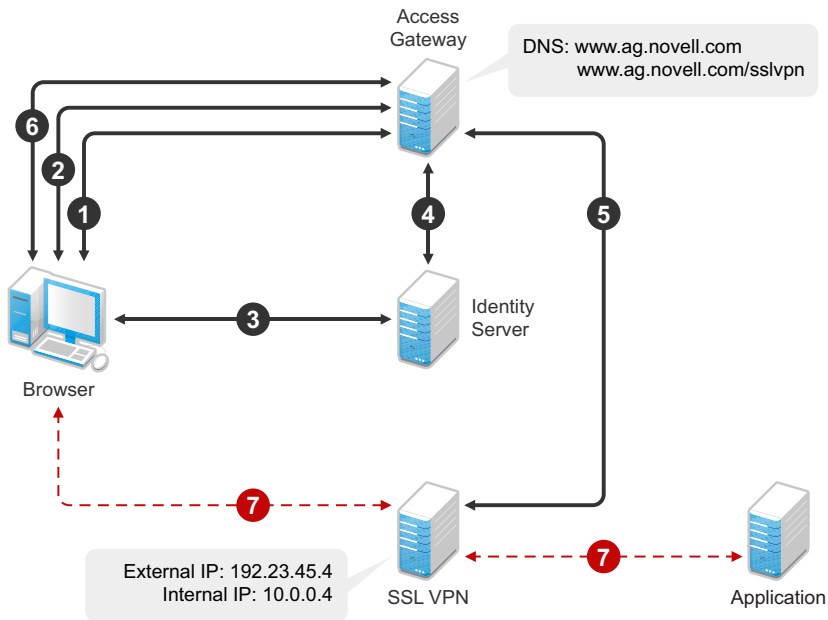
Custom Login Policy

When the custom login policy is configured, the SSL VPN redirects the custom login requests to different URLs based on the policy. This is a very useful feature when users want to access applications such as those on the Citrix application servers. For more information on how to configure a custom login policy, see [Section 4.2.5, “Configuring a Custom Login Policy for SSL VPN,”](#) on page 52.

1.2 NetIQ SSL VPNs

The following figure shows the Access Manager components and the process involved in establishing a secure connection between a client machine and the SSL VPN. In this deployment, the Access Gateway accelerates and protects the SSL VPN.

Figure 1-1 NetIQ SSL VPN



1. The user specifies the following URL to access the SSL VPN:

`https://<www.ag.novell.com>:8443/sslvpn/login`

`<www.ag.novell.com>` is the DNS name of the Access Gateway that accelerates the SSL VPN, and `/sslvpn/login` is the path of the SSL VPN.

2. The Access Gateway redirects the user to the Identity Server for authentication, because the URL is configured as a protected resource.
3. The Identity Server authenticates the user's identity.
4. The Identity Server propagates the session information to the Access Gateway through the Embedded Service Provider.
5. The Access Gateway injects the SSL VPN policy for that user into the SSL VPN servlet. The SSL VPN servlet processes the parameters and sends the policy information back to the Access Gateway.
6. The SSL VPN checks if the client machine has sufficient security restraints. For more information on client integrity checks, see [Chapter 3.1, "Configuring Policies to Check the Integrity of the Client Machine,"](#) on page 32.
7. One of the following actions takes place, depending on the mode of the SSL VPN connection:
 - ♦ In the Enterprise mode, a tunnel interface is created and is bound with the tunnel IP address assigned by the SSL VPN. A secure tunnel is established between the client machine and the SSL VPN, and the routing table is updated with the protected network configuration.
 - ♦ In the Kiosk mode, a secure tunnel is established between the client machine and the SSL VPN, and the protected network configuration is pushed to the client.

8. When the user accesses the applications behind the protected network, the connection goes through the secure tunnel formed with the SSL VPN and not through the Access Gateway.
 9. The browser stays open throughout the SSL VPN connection to allow the keep alive packets to go through the Access Gateway.
 10. When the user clicks the logout button to close the SSL VPN session, all the client components are automatically uninstalled from the workstation.
- ♦ If your organization has native applications that require secure Internet access and you do not need acceleration of Web applications.
 - ♦ You have implemented a different solution for Web SSO and need the SSL VPN for tunneling native applications.
 - ♦ You do not want Web SSO but you need secure access to the native applications or Web server.

Deploy the traditional SSL VPN if you implement Access Manager for Web SSO and want secure access to native applications.

1.2.1 High-Bandwidth and Low-Bandwidth SSL VPNs

NetIQ SSL VPN comes in high-bandwidth and low-bandwidth versions.

Low-Bandwidth Version: The default SSL VPN server is a low-bandwidth version. It is restricted to 249 simultaneous user connections and a transfer rate of 90 Mbits per second because of export restrictions.

High-Bandwidth Version: The high-bandwidth version does not have the connection and performance restrictions. It is essential to have the high-bandwidth SSL VPN installed if you want to cluster the SSL VPN servers.

If the export law permits, you can order the high-bandwidth SSL VPN RPM and get the high-bandwidth capabilities at no extra cost. After the export controls have been satisfied, the order will be fulfilled. You can install the high-bandwidth SSL VPN RPM on both the Traditional NetIQ SSL VPN server and on the ESP-enabled NetIQ SSL VPN server.

Your regular NetIQ sales channel can determine if the export law allows you to order the high-bandwidth version at no extra cost.

1.3 SSL VPN Client Modes

NetIQ SSL VPN has two client modes, Enterprise mode and Kiosk mode. In the Enterprise mode, which is available for users who have administrative privileges, all applications are enabled for SSL VPN. In the Kiosk mode, only a limited set of applications are enabled for SSL VPN.

Enterprise mode is available to users who have the administrator right in a Windows workstation or a root user privilege on Linux or Macintosh workstations. If a user does not have administrator rights or root user privileges for that workstation, the SSL VPN connection is made in Kiosk mode.

For more information on the client platforms and setups tested by NetIQ, see the [Access Manager 3.1 Support Pack 1 SSLVPN integration testing report](http://www.novell.com/support/viewContent.do?externalId=7004342&sliceId=1) (<http://www.novell.com/support/viewContent.do?externalId=7004342&sliceId=1>).

- ♦ [Section 1.3.1, “Enterprise Mode,” on page 16](#)
- ♦ [Section 1.3.2, “Kiosk Mode,” on page 18](#)

1.3.1 Enterprise Mode

In the Enterprise mode, all applications, including those on the desktop and the toolbar, are enabled for SSL, regardless of whether they were opened before or after connecting to SSL VPN. In this approach, a thin client is installed on the user's workstation. In the Enterprise mode, the IP Forwarding feature is enabled by default.

The Enterprise mode is recommended for devices that are managed by an organization, such as a laptop provided by the organization for its employees. The Enterprise mode supports the following:

- ♦ Protocols such as TCP, UDP, ICMP, and NetBIOS.
- ♦ Applications that open TCP connections on both sides, such as VoIP and FTP.
- ♦ Enterprise applications such as CRM and SAP*.
- ♦ Applications such as Windows File Sharing systems, the Novell Client™, and Novell SecureLogin.

You can configure a user to connect only in the Enterprise mode depending on the role of the user. For more information, see [Section 4.2.1, "Configuring Users to Connect Only in Enterprise Mode or Kiosk Mode," on page 48](#).

NOTE: If you have configured a user to connect in Enterprise mode only and that user does not meet the prerequisites, the SSL VPN connection fails with an appropriate error message if it is using the applet-based Web browser, or a blank screen if an ActiveX-based Web browser is used.

- ♦ ["Prerequisites" on page 16](#)
- ♦ ["User Scenarios" on page 16](#)

Prerequisites

A user can access the SSL VPN in the Enterprise mode if any one of the following prerequisites is in place:

- ♦ The user is an administrator or a root user of the machine, or a Super user or an Administrator user in Windows Vista user.
- ♦ The user is a non-admin or a non-root user who knows the credentials of the administrator or root user, or a standard user in Windows Vista.
- ♦ The SSL VPN client components are preinstalled on the user's machine.

User Scenarios

Depending on which prerequisites are in place, users have different login scenarios.

- ♦ ["Scenario 1: The User Is the Admin or Root User of the Machine" on page 17](#)
- ♦ ["Scenario 2: The User Is the Non-Admin or Non-Root User of Machine and Knows the Admin or Root Credentials" on page 17](#)
- ♦ ["Scenario 3: The User Is a Non-Admin or Non-Root User, but the Client Components Are Preinstalled on the Machine" on page 18](#)

Scenario 1: The User Is the Admin or Root User of the Machine

When the user is an administrator or a root user of the machine, the tool identifies the user as the admin or root user and Enterprise mode is enabled by default after the user specifies credentials in the Access Manager Appliance page. An admin or a root user can connect to SSL VPN only in the Enterprise mode unless the system administrator configures the user to connect in the Kiosk mode only. For more information on how to configure users for Kiosk mode only, see [Section 4.2.1, “Configuring Users to Connect Only in Enterprise Mode or Kiosk Mode,”](#) on page 48.

Scenario 2: The User Is the Non-Admin or Non-Root User of Machine and Knows the Admin or Root Credentials

A non-admin or a non-root user can access SSL VPN in Enterprise mode if the user knows the administrator or root user credentials. When a non-admin or a non-root user connects to SSL VPN, the user is prompted to specify the credentials on the Access Manager Appliance page. The tool identifies that the credentials supplied are those of the non-admin or a non-root user and displays the following dialog box.

Figure 1-2 SSL VPN Dialog box



The user must specify the username and password of the administrator or the root user of the machine in the dialog box, then click **OK** to enable the Enterprise mode.

The Enterprise mode is enabled by default in the subsequent sessions and the user is not prompted again for the administrator or root username and password.

Non-admin or non-root users who have connected to SSL VPN in Enterprise mode can connect to SSL VPN in Kiosk mode on the same machine. For more information, see [“Switching from Enterprise Mode to Kiosk Mode”](#) in the *NetIQ Access Manager Appliance 4.0 SSL VPN User Guide*.

NOTE: Users cannot switch from one mode to another if you have configured them to connect in one mode only.

Scenario 3: The User Is a Non-Admin or Non-Root User, but the Client Components Are Preinstalled on the Machine

If a non-admin or a non-root user wants to install SSL VPN in Enterprise mode, you can preinstall the SSL VPN client components on the user's machine. For more information, see [Section 4.1, "Preinstalling the SSL VPN Client Components," on page 47](#). When non-admin or non-root users access the client components from a workstation that has the SSL VPN client components preinstalled, the users are not prompted to enter the credentials of the admin user or root user.

The users are connected to SSL VPN in Enterprise mode after they specify their credentials on the Access Manager Appliance login page.

1.3.2 Kiosk Mode

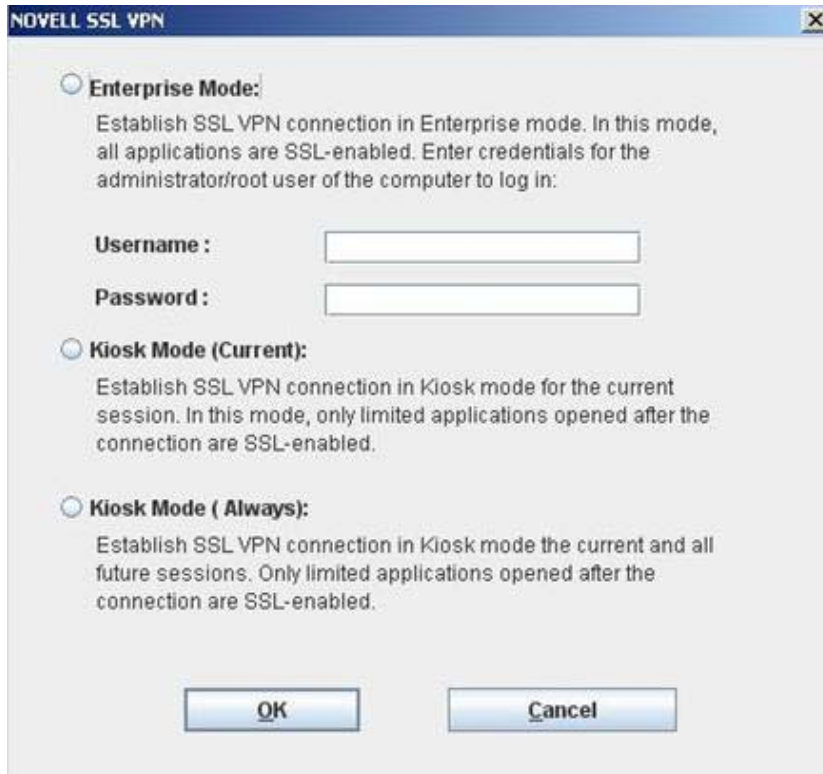
In the Kiosk mode, only a limited set of applications are enabled for the SSL VPN. A non-admin user, a non-root user, or a standard user in Windows Vista can connect to SSL VPN in Kiosk mode if he or she does not have administrator access. In the Kiosk mode, applications that were opened before the SSL VPN connection was established are not SSL-enabled.

The Kiosk mode supports TCP and UDP applications only. This mode is better suited for machines that are not managed by an organization, such as home computers and computers in Web browsing kiosks.

You can configure a user to connect in the Kiosk mode only. When you have done so, a user is connected to the SSL VPN in the Kiosk mode after the user provides credentials in the Access Manager Appliance login page. For more information, see [Section 4.2.1, "Configuring Users to Connect Only in Enterprise Mode or Kiosk Mode," on page 48](#).

If you have left the mode selection to the client and a user logs in to the SSL VPN client as a non-admin or non-root user, the following dialog box is displayed:

Figure 1-3 SSL VPN Dialog Box



The user can do one of the following to load the Kiosk mode:

- ♦ Click *Ignore* to connect to SSL VPN in Kiosk mode for that particular session. The user is prompted again to provide the administrator or the `root` username and password during the next login.
- ♦ Click *Ignore Forever* to connect to SSL VPN in Kiosk mode in the current session, as well as in subsequent sessions.

A user who has clicked *Ignore Forever* can still switch to SSL VPN in Enterprise mode in the next session. For more information, see [“Switching from Kiosk Mode to Enterprise Mode”](#) in the *NetIQ Access Manager Appliance 4.0 SSL VPN User Guide*.

NOTE: When a non-admin user uses Internet Explorer to establish an SSL VPN connection, the ActiveX download fails. This happens because ActiveX requires admin rights to download. This issue might also occur if you have upgraded from an older version. If a user wants to access SSL VPN with Internet Explorer, use the following URL:

`https:<DNS-Name>/sslvpn/login?forcejre=true`

For more information, see [Section 4.2.4, “Configuring SSL VPN to Download the Java Applet on Internet Explorer,”](#) on page 51.

2 Basic Configuration for SSL VPN

The SSL VPNs are auto-imported into the Administration Console during installation. You can use the SSL VPNs page in the Administration Console to view information about the current status of all SSL VPNs and to configure the SSL VPNs.

A path based service named as sslvpn is created to accelerate the SSL VPN while installing Novell Access Manager Appliance. You will find this service in the Access Gateway configuration in the Administration Console.

The following images displays the sslvpn service in the Access Gateway configuration:

Proxy Service List				
New...	Delete	Rename...	Enable	Disable
<input type="checkbox"/>	Name	Enabled	Multi-Homing	Published DNS Name
<input type="checkbox"/>	NAM-Service	✓		labs.blr.novell.com
<input type="checkbox"/>	sslvpn	✓	Path-Based	labs.blr.novell.com / ... (1) path(s) ▼

This section has the following information:

- [Section 2.1, “Configuring the IP Address, Port, and Network Address Translation,” on page 21](#)
- [Section 2.2, “Configuring Route and Source NAT for Enterprise Mode,” on page 26](#)
- [Section 2.3, “Configuring DNS Servers,” on page 28](#)
- [Section 2.4, “Configuring Certificate Settings,” on page 29](#)

2.1 Configuring the IP Address, Port, and Network Address Translation

The Gateway Configuration page displays the current configuration of the SSL VPN, such as the external IP address if the SSL VPN is behind Network Address Translation (NAT), the listening IP address, TCP encryption port, Connection Manager port, and the type of encryption used.

This section describes how to configure the IP addresses, port, subnet address and subnet mask, and protocol for SSL VPN.

- [Section 2.1.1, “Configuring the SSL VPN Gateway behind NAT or L4,” on page 22](#)
- [Section 2.1.2, “Configuring the SSL VPN Gateway without NAT or an L4 Switch,” on page 24](#)

2.1.1 Configuring the SSL VPN Gateway behind NAT or L4

To configure the SSL VPN behind NAT or by using an L4 switch:

- 1 In the Administration Console, click *Devices > SSL VPNs > Edit*.
The Server configuration page is displayed.
- 2 Select *Basic Configuration* from the *Gateway Configuration* section.

NAT/L4 related configuration

☒ Behind NAT / L4

L4 Listener Details

	Public IP Address	Port	Protocol
Kiosk Mode:	<input type="text" value="192.168.1.255"/>	<input type="text" value="443"/>	<input type="text" value="TCP"/>
Enterprise Mode:	<input type="text" value="N/A"/>	<input type="text" value="443"/>	<input type="text" value="UDP"/>

Server Listener Details

	Listening IP Address	Port	Protocol
Kiosk Mode:	<input type="text" value="192.168.1.255"/>	<input type="text" value="7777"/>	<input type="text" value="TCP"/>
Enterprise Mode:	<input type="text" value="192.168.1.255"/>	<input type="text" value="7777"/>	<input type="text" value="UDP"/>

Assigned IP Address Pool For Enterprise Mode

Subnet Address	<input type="text" value="12.8.0.0"/>
Subnet Mask	<input type="text" value="255.255.0.0"/>

Other Configuration

Identity Provider Address:	<input type="text" value="10.1.16.5"/>
Access Gateway Address:	<input type="text" value="10.1.16.5"/>
Inactivity Timeout (Minutes):	<input type="text" value="30"/>
Encryption:	<input type="text" value="AES256"/>
Enterprise Mode Compression:	<input type="text" value="Off"/>
Authentication Hardening :	<input type="text" value="On"/>
Server Debug Level:	<input type="text" value="Off"/>
Client Debug Level:	<input type="text" value="Off"/>

Re-generate

Last Modified at:Nov 23, 2009 11:53 AM

Security warning: Read this ?

Server(s) must be updated before changes made on this panel will be used. See [Configuration](#) Panel for summary of changes.

- 3 Specify the following NAT/L4 configuration as follows:

Behind NAT/L4: Select the check box to specify that the SSL VPN Gateway is behind NAT.

Public IP Address: This field is enabled when the *Behind NAT* check box is selected. Specify the public IP address (that is, the address exposed to the Internet user) that translates into the SSL VPN Gateway IP address. This is the IP address where the external user on the Internet must be able to access the SSL VPN.

Port: Specify a port number for Kiosk mode as well as for Enterprise mode when the SSL VPN is behind an L4 switch or a behind NAT.

Protocol: Specify a protocol for Kiosk mode as well as for Enterprise mode, when the SSL VPN is behind an L4 switch or behind NAT. The protocol is TCP for Kiosk mode and UDP for Enterprise mode.

4 Specify the device-specific configuration as follows:

Cluster Member: Select the cluster member from a list of IP addresses.

Listening IP Address: Specify the IP address that the SSL VPN listens on.

Port: Specify a port number for Kiosk mode as well as for Enterprise mode when the SSL VPN is behind an L4 switch or behind NAT. Make sure that the port you specify here is free.

Protocol: Specify a protocol for Kiosk mode as well as for Enterprise mode, when the SSL VPN is behind an L4 switch or behind NAT. The protocol is TCP for Kiosk mode, but it can either be TCP or UDP for Enterprise mode.

5 Specify the following information to configure the assigned IP address pool for Enterprise mode:

Subnet Address: Specify the IP address of the subnet pool where SSL VPN assigns the IP address to each client in Enterprise mode. For this assigned IP address pool to work properly, you must configure the routing table and source NAT. For more information, see [Section 2.2, “Configuring Route and Source NAT for Enterprise Mode,”](#) on page 26.

Subnet Mask: Specify the subnet mask for Enterprise mode.

The values specified in the *Subnet Address* and *Subnet Mask* fields determine the IP addresses that are assigned to the clients. Make sure that the assigned IP address and the IP address of the client do not match.

NOTE: IP pooling is not applicable for Kiosk mode. In Enterprise mode, if you have only one SSL VPN installed, then you can configure only one IP pool. However, if you have multiple SSL VPNs in a cluster, then each SSL VPN must have separately defined IP pools. In the Enterprise mode, each connection requires two IP addresses. Make sure that the IP pool has two IP addresses for each connection.

6 Specify the other configuration as follows:

Cluster Communications Port: Specify the port that is used for communication between the cluster members.

Identity Provider Address: Specify the public IP addresses or the public DNS name of the Identity Server if you are configuring SSL VPN for the full tunneling mode. This configuration is required to split the management traffic from the tunneled traffic. For more information on full tunneling, see [Section 3.4, “Configuring Full Tunneling,”](#) on page 44.

Access Gateway Address: Specify the IP address or DNS name of the Access Gateway if your server is accelerated by the Access Gateway. This field is not present if you have installed the ESP-enabled SSL VPN. This configuration is required to split the management traffic from the tunneled traffic. For more information on full tunneling, see [Section 3.4, “Configuring Full Tunneling,”](#) on page 44.

Inactivity Timeout (Minutes): You can configure the time in minutes. If no data exchange takes place during the stipulated time, the connection is closed so that the resources are freed to allow additional incoming connections. The inactivity timeout period can be one minute to 1800 minutes. The default inactive timeout period is 30 minutes.

Encryption: Select the type of encryption. It can be either AES128 or AES 256.

Enterprise Mode Compression: Specify if you want to enable compression in Enterprise mode in order to reduce the time taken to establish connection.

Authentication Hardenings: This option is applicable to Enterprise mode clients only. When this option is enabled, it provides protection against active attacks by using a keyed Hash Message Authentication Code (HMAC) cryptographic hash such as SHA1 to sign and verify packets. When this option is enabled, a packet is examined by a stateless filter and dropped if the HMAC signature does not match.

To enable *Authentication Hardening*, select *On*. To manually regenerate the key click *Re-generate*. This option uses random number generation to regenerate the key.

Server Debug Level: Set this option to *On* if you want to get more debug information from the server. This option is set to *Off* by default.

Client Debug Level: Set this option to *On* if you want to get more debug information from the client. This option is set to *Off* by default.

- 7 To save your modifications, click *OK*, then click *Update* on the Configuration page.

2.1.2 Configuring the SSL VPN Gateway without NAT or an L4 Switch

- 1 In the Administration Console, click *Devices > SSL VPNs > Edit*.

The Server configuration page is displayed.

- 2 Select *Basic Configuration* from the *Gateway Configuration* section.

NetIQ Access Manager
ADMIN
PRIVACY/AGB_TREE

Access Manager | Devices | Policies | Auditing | Security

NAT/L4 related configuration
☒ Behind NAT / L4

L4 Listener Details

	Public IP Address	Port	Protocol
Kiosk Mode:	10.10.40.42	7777	TCP
Enterprise Mode:	10.10.40.42	7778	TCP

Server Listener Details

	Listening IP Address	Port	Protocol
Kiosk Mode:	164.99.184.42	7777	TCP
Enterprise Mode:	164.99.184.42	7778	TCP

Assigned IP Address Pool For Enterprise Mode

Subnet Address	42.42.0.0
Subnet Mask	255.255.0.0

Other Configuration

Identity Provider Address: 10.1.16.5
 Access Gateway Address: 10.1.16.5
 Inactivity Timeout (Minutes): 30
 Encryption: AES256
 Enterprise Mode Compression: Off
 Authentication Hardening: On **Re-generate Key** Last Modified at: May 5, 2010 3:16 PM
 Server Debug Level: Off
 Client Debug Level: Off Security warning: Read this ?

Server(s) must be updated before changes made on this panel will be used. See [Configuration](#) Panel for summary of changes.

OK Cancel

Diagram: A network diagram showing a Workstation connected to a Firewall. The Firewall has an 'Enterprise Listening IP address' and an 'Enterprise Ext. IP'. The Firewall is connected to a NAT device, which is connected to an 'Ext. IP' and an 'SSLVPN' device. The SSLVPN device has an 'Enterprise port' and a 'Servlet Port'. The SSLVPN device is connected to a 'Servlet' device, which is labeled '(Same or different computer)'. The SSLVPN device also has a 'Listening IP address'.

- 3 Specify the device-specific configuration as follows:

Cluster Member: Select the cluster member from a list of IP addresses.

Listening IP Address: Specify the IP address that the SSL VPN listens on.

Port: Specify a port number for Kiosk mode as well as for Enterprise mode when the SSL VPN is behind an L4 switch or behind NAT. Make sure that the port you specify here is free.

Protocol: Specify a protocol for Kiosk mode as well as for Enterprise mode, when the SSL VPN is behind an L4 switch or behind NAT. The protocol is TCP for Kiosk mode, but it can either be TCP or UDP for Enterprise mode.

- 4 Specify the following information to configure the assigned IP address pool for Enterprise mode:

Subnet Address: Specify the IP address of the subnet pool where SSL VPN assigns the IP address to each client in Enterprise mode. For this assigned IP address pool to work properly, you must configure the routing table and source NAT. For more information, see [Section 2.2, “Configuring Route and Source NAT for Enterprise Mode,”](#) on page 26.

Subnet Mask: Specify the subnet mask for Enterprise mode.

The values specified in the *Subnet Address* and *Subnet Mask* fields determine the IP addresses that are assigned to the clients. Make sure that the assigned IP address and the IP address of the client do not match.

- 5 Specify the other configuration as follows:

Cluster Communications Port: Specify the port that is used for communication between the cluster members.

Identity Provider Address: Specify the IP addresses or the DNS name of the Identity Server if you are configuring SSL VPN for the full tunneling mode. For more information on full tunneling, see [Section 3.4, “Configuring Full Tunneling,”](#) on page 44.

Access Gateway Address: Specify the IP address or DNS name of the Access Gateway if your server is accelerated by the Access Gateway and if you are configuring SSL VPN for the full tunneling mode. This field is not present if you have installed the ESP-enabled SSL VPN. For more information on full tunneling, see [Section 3.4, “Configuring Full Tunneling,”](#) on page 44.

Inactivity Timeout (Minutes): You can configure the time in minutes. If no data exchange takes place during the stipulated time, the connection is closed so that the resources are freed to allow additional incoming connections. The inactivity timeout period can be one minute to 1800 minutes. The default inactive timeout period is 30 minutes.

Encryption: Select the type of encryption. It can be either AES128 or AES 256.

Enterprise Mode Compression: Specify if you want to enable compression in Enterprise mode in order to reduce the time taken to establish connection.

Authentication Hardening: This option is applicable to Enterprise mode clients only. When this option is enabled, it provides protection against active attacks, by using a keyed Hash Message Authentication Code (HMAC) cryptographic hash such as SHA1 to sign and verify packets. When this option is enabled, a packet is examined by a stateless filter and dropped if the HMAC signature does not match.

To enable *Authentication Hardening*, select *On*. To manually regenerate the key click *Re-generate Key*. This option uses random number generation to regenerate the key

Server Debug Level: Set this option to *On* if you want to get more debug information from the server. This option is set to *Off* by default.

Client Debug Level: Set this option to *On* if you want to get more debug information from the client. This option is set to *Off* by default.

- 6 To save your modifications, click *OK*, then click *Update* on the Configuration page.

2.2 Configuring Route and Source NAT for Enterprise Mode

In the Enterprise mode, the SSL VPN assigns IP addresses to each client from the subnet specified in the configuration. The values specified in the *OpenVPN Subnet Address* and *OpenVPN Subnet Mask* fields determine the IP addresses that are assigned to the clients. Make sure that the assigned IP address and the IP address of the client do not match.

For more information on configuring the IP address, see [Section 2.1, “Configuring the IP Address, Port, and Network Address Translation,” on page 21](#).

The packets from these clients reach the application server with the IP address of the client as the source address. The response packets need to be routed back to the SSL VPN, which sends them on to the clients. You can solve this routing problem in one of the following ways:

- [Section 2.2.1, “Configuring the OpenVPN Subnet in Routing Tables,” on page 26](#)
- [Section 2.2.2, “Configuring Source NAT,” on page 26](#)
- [Section 2.2.3, “Configuring Source NAT for SSL VPN,” on page 26](#)

2.2.1 Configuring the OpenVPN Subnet in Routing Tables

If you have a gateway for your network between the application server and the SSL VPN, you can configure the gateway to send the dynamically assigned IP addresses from the OpenVPN address pool to the SSL VPN. This is the best routing approach because most applications, including ActiveFTP and TFTP, can work in this type of environment. To establish this type of routing, you need to add a static route to your network's routing infrastructure so that traffic to the OpenVPN subnet pool of addresses is sent via the SSL VPN gateway.

2.2.2 Configuring Source NAT

You can configure Source NAT to change the dynamically assigned client addresses to the address of the SSL VPN before sending them to the application server. The application server can then use the source address in the packets to send them back to the SSL VPN, which can then reassign the client address and send the packets on to the client. This is the best approach if you are using the SSL VPN for TCP and UDP applications. Other applications, such as ActiveFTP and TFTP, cannot work in this type of environment. To establish this type of routing, you need to create an entry in the *iptables* file on the SSL VPN. If the *OpenVPN Subnet Address* option is set to 10.8.0.0/16 and the IP address of the SSL VPN is 10.16.12.247, the entry should be similar to the following:

```
iptables -t nat -A POSTROUTING -s 10.8.0.0/16 -j SNAT --to 10.16.12.247
```

Restart the SSL VPN services after the *iptables* file has been modified.

IMPORTANT: This simple solution only works if you are not using *iptables* to translate ports of other applications or Access Manager components. For a solution that works with multiple components, see [Configuring SUSE Firewall for the SSL VPN Component in Access Manager \(http://www.novell.com/coolsolutions/appnote/19939.html\)](http://www.novell.com/coolsolutions/appnote/19939.html).

2.2.3 Configuring Source NAT for SSL VPN

You can configure the source NAT (SNAT) for the SSL VPN Enterprise mode to change the dynamically assigned client addresses to the address of the SSL VPN before sending them to the application server. The application server can then use the source address in the packets to send them

back to the SSL VPN, which can then reassign the client address and send the packets on to the client. This is the best approach if you are using SSL VPN for TCP and UDP applications. Other applications, such as ActiveFTP and TFTP, cannot work in this type of environment.

To establish this type of routing, you need to create an entry in the iptables rule on the SSL VPN.

- ♦ “Configuring SNAT for Enterprise Mode” on page 27
- ♦ “Ordering SNAT Entries” on page 28

Configuring SNAT for Enterprise Mode

- 1 In the Administration Console, click *Devices > SSL VPNs > Edit*.
The Server configuration page is displayed.
- 2 Select *Advanced Configuration* from the *Gateway Configuration* section.

SNAT Configuration		
New... Delete Enable Disable		
<input type="checkbox"/>	SNAT Entry	Enabled
<input type="checkbox"/>	iptables -t nat -A POSTROUTING -s 12.8.0.0/255.255.0.0 -j SNAT --to 11.11.11.161	✓
<input type="checkbox"/>	iptables -t nat -A POSTROUTING -s 12.8.0.0/255.255.0.0 -j SNAT --to 11.11.11.162	✓
<input type="checkbox"/>	iptables -t nat -A POSTROUTING -s 12.8.0.0/255.255.0.0 -j SNAT --to 11.11.11.163	✓
Server(s) must be updated before changes made on this panel will be used. See Configuration		
OK Cancel		

- 3 If the SSL VPN is a member of a cluster, the *Cluster Member* option is displayed. The SNAT Entry configuration is specific to different cluster members. Select the IP address of the cluster member for which you want to configure the SNAT entry.
- 4 To configure a new SNAT entry, click *New*.

New	
iptables -t nat -A POSTROUTING	
--protocol (-p)	ANY
--source (-s)	12.8.0.0/255.255.0.0
--destination (-d)	0.0.0.0
--destination-port (--dport)	0
-j SNAT --to-source (--to)	
Provide additional parameters (Will be appended to command)	
OK Cancel	

5 Specify the information in the following format:

--protocol (-p): This is an optional parameter. To specify a protocol, select a protocol from the list. The protocol can be ANY, UDP, TCP or ICMP. By default, the ANY option is selected.

--source (-s): Specifies the IP address of the subnet pool where SSL VPN assigns the IP address to each client in Enterprise mode.

NOTE: This field is populated by the Enterprise mode IP address by default. However, you can edit the value in this field if you want to use this field to add iptables SNAT entries for other cases in Kiosk mode, such as for full tunneling.

--destination (-d): This is an optional parameter. You can either specify the host IP address or the destination IP address or specify the IP address and the network mask combination in the following format:

<destination>/<SubnetMask>

The network mask should be in the dotted decimal format only.

--destination-port (--dport): This is an optional parameter. You can specify the destination port.

-j SNAT --to-source (--to): This is a mandatory parameter. Specify a valid IP address of SSL VPN.

Provide additional parameters (Will be appended to command): You can add any other parameters, depending on your requirements. However, these parameters are not validated.

Click OK.







The new SNAT entry is displayed in the following format:

```
iptables -t nat -A POSTROUTING -p <Any> s <openVPNSubnetIP> -d <destinationIP> --dport <destinationPort> -j SNAT --to <privateIPSSLVPN> <additional parameters>
```

6 To save your modifications, click *OK*, then click *Update* on the Configuration page.

Ordering SNAT Entries

You can configure SNAT rules for a user's role. However, the SNAT entries are processed based on their order in the list. If you want to change the order of the rules, you can click the up-arrow or down-arrow to move them up or down.

<input type="checkbox"/> SNAT Entry	Enabled
<input type="checkbox"/> iptables -t nat -A POSTROUTING -s 12.8.0.0/255.255.0.0 -j SNAT --to 11.11.11.161	<input checked="" type="checkbox"/>  
<input type="checkbox"/> iptables -t nat -A POSTROUTING -s 12.8.0.0/255.255.0.0 -j SNAT --to 11.11.11.162	<input checked="" type="checkbox"/>  
<input type="checkbox"/> iptables -t nat -A POSTROUTING -s 12.8.0.0/255.255.0.0 -j SNAT --to 11.11.11.163	<input checked="" type="checkbox"/>  

2.3 Configuring DNS Servers

The DNS servers configured in the SSL VPN are pushed to the client during the connection. When a Linux or Windows client connects to the SSL VPN, the existing DNS entry on the client is pushed as the secondary entry and the DNS entry configured on the SSL VPN is pushed as the primary DNS entry.

However, on a Mac client, the DNS entry configured on the SSL VPN acts as the secondary DNS. After the SSL VPN connection, name resolution is done through the DNS entry configured before the SSL VPN connection. However, when the primary DNS server is not available, the DNS entry configured by the SSL VPN takes care of DNS resolution for the client.

You can configure DNS servers for the Enterprise mode through the Administration Console. The DNS servers can be configured for the Kiosk mode either during the installation if you are installing the Access Gateway and SSL VPN on the same machine, or by using YaST® after the installation.

- 1 In the Administration Console, click *Devices > SSL VPNs > Edit*.
The Server configuration page is displayed.
- 2 Select *DNS Server List* from the *Basic Gateway Configuration* section.

The screenshot shows two sections: 'DNS Servers' and 'Domains'. The 'DNS Servers' section has a 'New...' button, a 'Delete' button, a checkbox, and a text field containing '10.1.1.1'. The 'Domains' section has a 'New...' button, a 'Delete' button, a checkbox, and a text field containing 'abc.com'. Below these sections is a message: 'Server(s) must be updated before changes made on this panel will be used. See [Configuration](#) Panel for summary of changes.' At the bottom are 'OK' and 'Cancel' buttons.

- 3 To configure a DNS server, click *New* in the *DNS Servers* section, specify the IP address of the server, then click *OK*.
- 4 To configure a domain, click *New* in the *Domains* section, specify the domain name, then click *OK*.
- 5 To delete a DNS server or a domain, select the check box next to the field and click *Delete* in the section.
- 6 To save your modifications, click *OK*, then click *Update* on the Configuration page.

2.4 Configuring Certificate Settings

Access Manager Appliance components and agents can access the keystore to retrieve certificates, keys, and trusted roots as needed.

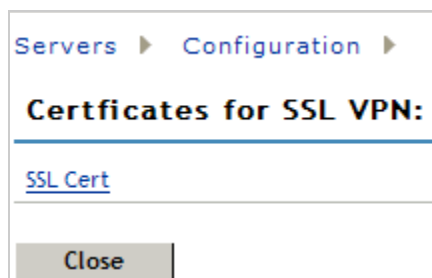
When SSL VPN is installed, it creates a test-connector certificate with the default DNS name of the SSL VPN. However, if you have changed the default DNS name of the SSL VPN, then you must create a new certificate and replace the test-connector.

The following instructions assume that you have already created a certificate. For more information on creating certificates, see “[Security and Certificate Management](#)” in the *NetIQ Access Manager Appliance 4.0 Administration Console Guide*.

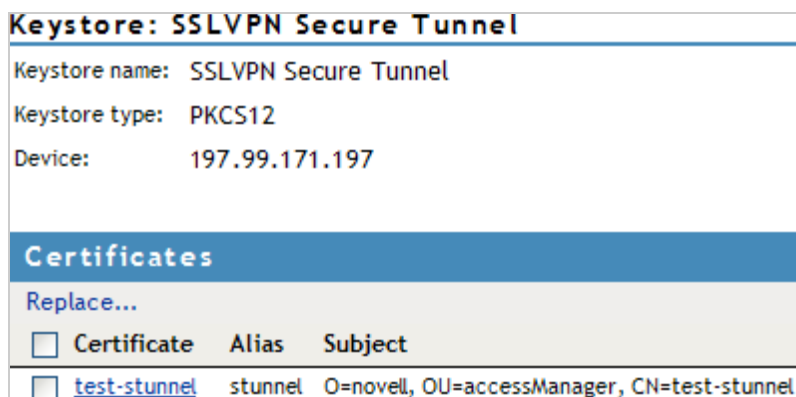
Before you proceed with the configuration, log in to the Administration Console, select *Security > Trusted Roots*, click the down arrow for the trusted root that you are interested in. Make sure that two SSL VPN trust stores are displayed. If they do not exist, you must manually push the certificates to the trust store.

NOTE: Make sure that SSL VPN certificate names contain only alphanumeric characters, space, underscore (_), hyphen (-), the at symbol @, and the dot (.).

- 1 In the Administration Console, select *Devices > SSL VPN > Edit*.
- 2 Select *SSL VPN Certificates* from the *Security settings* section.



- 3 Click *SSL Cert*.



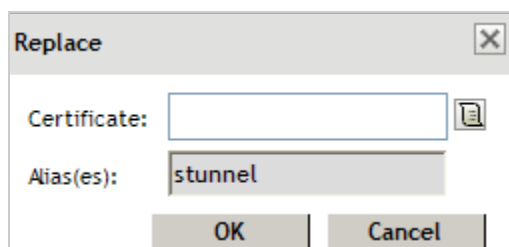
Certificates in the SSL VPN STunnel are used by SSL VPN services for encryption. This page contains the following information:

Keystore name: Displays the name of the keystore to which the certificate belongs.

Keystore type: Displays the type of keystore. It can be Java, PEM, or PKCS12.

Device: Displays the IP address of the SSL VPN device.

- 4 To replace the default certificate, click *Replace*.



Fill in the following fields:

Certificates: Click the *Select Certificate* icon to browse and select the certificate that you want to associate with SSL VPN.

Alias(es): You can provide an alternate name for the certificate you are importing.

- 5 Click *OK* to save changes.
- 6 To save your modifications, click *OK*, then click *Update* on the Configuration page

3 Configuring End-Point Security and Access Policies for SSL VPN

The SSL VPN has a set of client integrity check policies to protect your network and applications from clients that are using insufficient security restraints. You can configure a client integrity check policy to run on the client workstations before establishing a tunnel to the SSL VPN gateway. This check ensures that the users have specified software installed and running in their systems.

SSL VPN also allows you to configure traffic policies to control access to resources based on the role of the client. You can then configure different levels of security and assign them to traffic policies.

The traffic policies are a set of rules and regulations, administered to regulate user access to the protected network resources based on the role of the user and the security level adhered to by the client machine. The policies ensure that certain actions take place when the user tries to establish an SSL VPN connection.

- ♦ A client integrity check (CIC) is performed on the client machine to determine if the client has the required firewall or antivirus installed on the machine. For more information on how to CIC, see [“Configuring Applications for a Category” on page 34](#). If the client fails the integrity check, one of the following actions occurs:
 - ♦ If there is a traffic policy configured for that user’s role and the security level is None, the SSL VPN connection is established with minimal access to that client.
 - ♦ If there is no traffic policy configured for that user’s role and the security level is None, the SSL VPN connection fails.
- ♦ If the client passes the CIC, the level of security at the client machine is determined, depending on the requirements for the different levels configured and the software installed in the client machine. For more information on how to configure security levels, see [Section 3.2.1, “Client Security Levels,” on page 39](#).
- ♦ If the client adheres to the accepted security level, the SSL VPN connection is made and the secure tunnel is established between the SSL VPN client and server.
 - ♦ When the tunnel is up, if some changes are made to the client integrity check policy, the client policy, or the traffic policy, and the changes alter the security level of the client, you must restart the server to force the clients to reconnect with the new security level that applies to them.
 - ♦ When the tunnel is up, if the user installs a new software that enhances the security level of the client, the SSL VPN connection continues without the tunnel being disconnected. But if the security level of the client is changed to a lower level because the client deleted some of the CIC resources, the SSL VPN connection is disconnected. When the user logs in again, new policies applicable to the changed level are imposed on the user.
- ♦ The user is then given access to different resources based on the traffic policies configured for the role of the user and the security levels adhered to by the user. For more information on how to configure traffic policies for different roles, see [Section 3.3, “Configuring Traffic Policies,” on page 40](#).

NOTE: All configurations done while the tunnel is up affect users who connect after the changes are applied. To apply the configuration changes to all users immediately, disconnect the active connections from the statistics page. For more information, see [Section 6.4, “Disconnecting Active SSL VPN Connections,”](#) on page 74.

3.1 Configuring Policies to Check the Integrity of the Client Machine

You can configure a CIC policy to verify if the prescribed software (such as firewall and antivirus software) is installed on the client machine. You can configure different policies for Windows, Linux, and Macintosh machines, then specify applications that must be present in the client machines in order to pass the client integrity check.

A category that you have configured can be deleted only if it is not assigned to any of the security levels.

- [Section 3.1.1, “Selecting the Operating System,”](#) on page 32
- [Section 3.1.2, “Configuring the Category,”](#) on page 33
- [Section 3.1.3, “Configuring Applications for a Category,”](#) on page 34
- [Section 3.1.4, “Configuring Attributes for an Application,”](#) on page 34
- [Section 3.1.5, “Exporting and Importing Client Integrity Check Policies,”](#) on page 38

3.1.1 Selecting the Operating System

- 1 In the Administration Console, click *Devices > SSL VPNs > Edit*.
- 2 Select *Client Integrity Check Policies* from the *Policies* section.

CIC policies for all Operating Systems			
Import... Export...			
Operating System	Category	Application	Enabled
Linux	Antivirus Linux	AntiVir	
	Firewall Linux	FireStarter	
	Antivirus Mac	Mcafee Virex	
	Antivirus Windows	Symantec AntiVirus 10.0	
Macintosh	Antivirus Windows	Zone Alarm Personal Firewall 6.0.631.003	
	Firewall Windows		
	Antivirus Linux		
Server(s) must be updated before changes made on this panel will be used. See Configuration Panel for summary of c			
OK Cancel			

- 3 Select the operating system.
Next, you must configure a category of software that needs to be present in the client machine.

- 4 Continue with “Configuring the Category” on page 33.

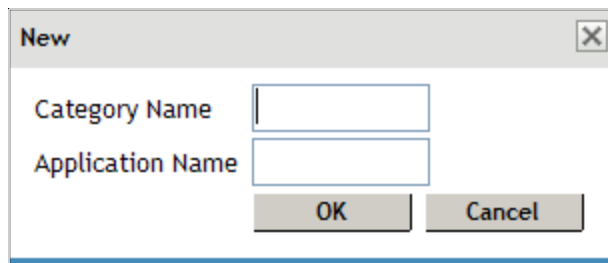
For more information on exporting and importing client integrity check policies, see [Section 3.1.5, “Exporting and Importing Client Integrity Check Policies,”](#) on page 38.

3.1.2 Configuring the Category

A category is a group of similar software. For example, a firewall category can contain a list of firewalls such as the Windows Firewall and ZoneAlarm firewall. You can configure multiple software categories for a single CIC policy.

When multiple categories are configured for an operating system, if one of the enabled category does not exist on the client, the client integrity check fails.

- 1 To add a new category, click *New*.



A dialog box titled "New" with a close button (X) in the top right corner. It contains two text input fields: "Category Name" and "Application Name". Below the fields are two buttons: "OK" and "Cancel".

- 2 Specify a name for category and a name for the application in the *Category Name* and the *Application Name* fields, then click *OK*.
- 3 Select the newly added category, then click *Enable*.

CIC policies for all Operating Systems			
Import... Export...			
Operating System	Category	Application	Enabled
Linux	Antivirus Linux	Antivir	
	Firewall Linux	FireStarter	
	Antivirus Mac	Mcafee Virex	
	Antivirus Windows	Symantec AntiVirus 10.0	
Macintosh	Antivirus Windows	Zone Alarm Personal Firewall 6.0.631.003	
	Antivirus Linux		
	Antivirus Mac		
Windows	Antivirus Linux		
	Antivirus Mac		
	Antivirus Windows		
Server(s) must be updated before changes made on this panel will be used. See Configuration Panel for summary of c			
OK Cancel			

- 4 To disable a category that is already enabled, select the category, then click *Disable*.
- 5 To delete a category, select the category, then click *Delete*.
- 6 Click *OK* to save your modifications, then click *Update* on the Configuration page.
- 7 Continue with “Configuring Applications for a Category” on page 34.

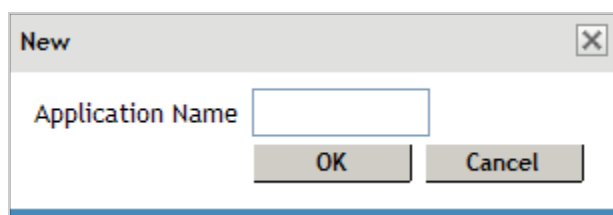
3.1.3 Configuring Applications for a Category

A category consists of group of applications. You can add more than one application under a category. A client workstation is checked for the presence of any one of the software items in the category. If at least one of the enabled application definition exists on the system, the client integrity check passes.

- 1 To configure or add applications to a category, click the category.



- 2 To add a new application, click *New*.



- 3 Specify an application name, then click *OK*.
- 4 Select the newly added application, then click *Enable*.

NOTE: To enable an application you must have already enabled the category that the application is part of.

- 5 To disable an application that is already enabled, select the application, then click *Disable*.
- 6 To delete an application, select the application, then click *Delete*.
- 7 Click *OK* to save your modifications, then click *Update* on the Configuration page.
- 8 Continue with [“Configuring Attributes for an Application” on page 34](#).

3.1.4 Configuring Attributes for an Application

After you have added an application to a category, you must configure the attributes for each of these applications. These attributes can be in the form of RPMs, processes, registry keys, or executable files. The client integrity check detects the presence of these attributes.

- 1 To add a new attribute, click *New*, specify an attribute name, then click *OK*.
- 2 Click the application to add application details and attributes.

Operating System: Linux					
Category: Firewall_Linux					
Application:	FireStarter				
Definition of the Application					
New... Delete					
<input type="checkbox"/> Attribute Type	Attribute				
<input type="checkbox"/> AbsoluteFile	<table border="1"> <tr> <td>Name</td> <td>/var/lock/subsys/firestarter</td> </tr> <tr> <td>HashMD5</td> <td><input type="text"/> Select file...</td> </tr> </table>	Name	/var/lock/subsys/firestarter	HashMD5	<input type="text"/> Select file...
Name	/var/lock/subsys/firestarter				
HashMD5	<input type="text"/> Select file...				
<input type="checkbox"/> RPM	<table border="1"> <tr> <td>Name</td> <td>FireStarter</td> </tr> <tr> <td>Version</td> <td>0.9.3</td> </tr> </table>	Name	FireStarter	Version	0.9.3
Name	FireStarter				
Version	0.9.3				
Server(s) must be updated before changes made on this panel will be used. See Configuration Panel for summary of changes.					
<input type="button" value="OK"/>	<input type="button" value="Cancel"/>				

- 3 Specify details for the attributes. The following table lists the attributes for applications on different operating systems:

Operating System	Attribute Type	Attribute Name
Linux	RPM	<p>Name: Specify the name of the RPM that must be present on the client machine.</p> <p>Version: Specify the version of the RPM that must be present on the client machine.</p>
	Process	<p>Name: Specify the name of the process that must be present on the client machine.</p> <p>Owner: Specify the owner of the process.</p>
	Absolute File	<p>Name: Specify the name and absolute path of the file that must be present on the client machine.</p> <p>HashMD5: Specify the MD5 checksum value of the absolute file. To calculate the MD5 checksum value of an absolute file located in your local system, click <i>Select File</i> to select the file. The MD5 checksum value of the selected file is displayed.</p> <p>To calculate the MD5 checksum value for an absolute file that is on another system, remotely connect to that system, calculate the MD5 value, then copy the value in the <i>HasMD5</i> field.</p> <p>NOTE: You can also copy the file from the remote system to the local system, then calculate the MD5 checksum by using the <i>Select File</i> option. However, this might change the MD5 value of the file during the process. If you want to use this method, then ensure that the file size and file contents did not change during the process.</p>

Operating System	Attribute Type	Attribute Name
Macintosh	Package	<p>Name: Specify the name of the software package that must be present on the client machine.</p> <p>Version Specify the version of the software package.</p>
	Process	<p>Name: Specify the name of the executable file that must be present on the client machine.</p> <p>Owner: Specify the owner of the process.</p>
	Absolute File	<p>Name: Specify the name and absolute path of the file that must be present on the client machine.</p> <p>HashMD5: Specify the MD5 checksum value of the absolute file. To calculate the MD5 checksum value of an absolute file located in your local system, click <i>Select File</i> to select the file. The MD5 checksum value of the selected file is displayed.</p> <p>To calculate the MD5 checksum value for an absolute file that is on another system, remotely connect to that system, calculate the MD5 value, then copy the value in the <i>HasMD5</i> field.</p> <p>NOTE: You can also copy the file from the remote system to the local system, then calculate the MD5 checksum by using the <i>Select File</i> option. However, this might change the MD5 value of the file during the process. If you want to use this method, then ensure that the file size and file contents did not change during the process.</p>
Windows	Process	<p>Name: Specify the name of the executable file that must be present on the client machine.</p> <p>RegistryKeyName: Specify the registry key name. When you add this name, make sure that you also specify a value for <i>RegistryKey Value</i>.</p> <p>ValueName: Specifies the value for RegistryKey configured. The data found in this key value should be the absolute path of the folder where the process file is present.</p> <p>Version: Specify the version of the software process that must be running in the client machine.</p> <p>NOTE: The version attribute specifies the Windows Explorer file version number.</p>

Operating System	Attribute Type	Attribute Name
	RegistryKey	<p>Name: Specify the name and absolute path of the registry key that must be present on the client machine.</p> <p>Value Name: Specify the name of the registry key value.</p> <p>Value Data: Specify a data for the registry key value. This data can be for registry type REG_BINARY, REG_DWORD, REG_DWORD_LITTLE_ENDIAN, REG_MULTI_SZ, or REG_SZ. The value for REG_DWORD and REG_DWORD_LITTLE_ENDIAN is hexadecimal or decimal. The value of a REG_MULTI_SZ or REG_SZ can be a string value or, numeric or alphanumeric. The value of REG_BINARY can be binary or hexadecimal.</p> <p>The Value name and Value data are separated by a comparison operator such as =, >, <, <=, >=. You must always use = with a string or with the registry type REG_BINARY. You can use any comparison operator with other registry types</p> <p>For example, if the registry key name is specified as <code>RegKey</code> with a Value Name of <code>RegValue</code>, a comparison operator of <code>=</code>, and a Value Data of <code>RegData</code>, the client integrity check process looks for the presence of <code>RegKey</code> with a value name <code>RegValue = value data RegData</code> on the client machine. If the registry is present with the specified values, the client passes the client integrity check.</p> <p>NOTE: Registry keys are not case sensitive, and they can contain either a single backslash (\) or double backslash (\\).</p> <p>For example: One of the registry key descriptions is <code>HKEY_Local_Machine\\Software\\Symantec</code>. It can also be written as <code>HKEY_Local_Machine\\Software\\Symantec</code>.</p>
	Absolute File	<p>Name: Specify the name and absolute path of the file that must be present on the client machine.</p> <p>Version: Specify the version of the absolute file that must be running on the client machine.</p> <p>HashMD5: Specify the MD5 checksum value of the absolute file. To calculate the MD5 checksum value of an absolute file located in your local system, click <i>Select File</i> to select the file. The MD5 checksum value of the selected file is displayed.</p> <p>To calculate the MD5 checksum value for an absolute file that is on another system, remotely connect to that system, calculate the MD5 value, then copy the value in the <i>HasMD5</i> field.</p> <p>NOTE: You can also copy the file from the remote system to the local system, then calculate the MD5 checksum by using the <i>Select File</i> option. However, this might change the MD5 value of the file during the process. If you want to use this method, then ensure that the file size and file contents did not change during the process.</p>
	Service	<p>Name: Specify the display name of the service.</p> <p>Status: Specify the status of the process in the client machine. The status of the process can be <i>Running</i> or <i>Stopped</i>.</p>

- 4 To delete an attribute, select the attribute, then click *Delete*.

- 5 Click *OK* to save your modifications, then click *Update* on the Configuration page.
- 6 To continue with configuring a connection and traffic policy for a client, proceed with [Section 3.2, “Configuring Client Security Levels,” on page 39](#).

3.1.5 Exporting and Importing Client Integrity Check Policies

You can export the client integrity check policy configuration into an XML file and import it back into the server.

You can modify the exported file without violating the schema format to include anew configuration. The new configuration is included when the file is imported.

- ♦ [“Exporting Client Integrity Check Policies” on page 38](#)
- ♦ [“Importing Client Integrity Check Policies” on page 38](#)

Exporting Client Integrity Check Policies

- 1 In the Administration Console, click *Devices > SSL VPNs > Edit*.
- 2 Click *Client Integrity Check Policies* in the Policies section. The Client Integrity Check Policies page is displayed.
- 3 Select the policies that you want to export, then click *Export*. This exports the configuration for all the platforms, categories, and applications.
- 4 Specify a filename for the XML document that saves the configuration.
- 5 Specify a location to save the XML file.
- 6 Click *OK* to save.

Importing Client Integrity Check Policies

- 1 In the Administration Console, click *Devices > SSL VPNs*.
- 2 Do one of the following:
 - ♦ If you want to import the client integrity check policy configuration to an individual server, select the server, then click *Edit*.
 - ♦ If you want to import the client integrity check policy configuration of a cluster, select the cluster, then click *Edit*.
- 3 Click *Client Integrity Check Policies* in the Policies section.
- 4 Click *Import*.
- 5 Browse and select the XML file that contains the saved client integrity check policies configuration.
- 6 Click *OK*.
- 7 To save your modifications, click *OK*, then click *Update* on the Configuration page.

3.2 Configuring Client Security Levels

You can configure the SSL VPN to send traffic on the SSL VPN tunnel based on the level of security configured at the client machine. You can decide the categories of software that you want to be present for each level.

- ♦ [Section 3.2.1, “Client Security Levels,” on page 39](#)
- ♦ [Section 3.2.2, “Configuring a Security Level,” on page 39](#)

3.2.1 Client Security Levels

You can configure the following security levels:

- ♦ **Least Secure:** Specifies the minimum categories of software that must be present on a client machine for the client to be at the lowest secure level. When a client is at a least secure level, you can configure the traffic policies so that the client has access to limited set of resources.
- ♦ **Moderately Secure:** Specifies the categories of software that must be present on a client machine for the client to be at a moderately secure level. When a client is at a moderately secure level, you can configure the traffic policies accordingly.
- ♦ **Secure:** Specifies the software categories that must be present on a client machine for the client to be secure. When a client is at a secure, the traffic policies can be configured so that the client has access to all or most of the protected resources, depending on the role of the client.
- ♦ **None:** If a client does not have any of the software such as firewall or antivirus specified in the client integrity check policy, then the security level of that client is None. When a client is at this level, the SSL VPN connection is established, but the client is given access to only a minimal set of resources.

In some circumstances you cannot configure a custom security level of a client:

- ♦ If, during the client integrity check, a client is found to have a certain level of security, then all the policies under that level as well as the policies under the lower security levels are imposed on the client. For example, if the client passes the security level check as Moderately Secure, then all the policies for this level as well as policies for Least Secure and None are imposed on the client.
- ♦ If you change the requirements for a particular security level, the changes are applied only to new user connections. For example, a client that has established the SSL VPN connection is currently at the Secure level. You now add a new the requirement for the Secure level, so the client that is already connected at the Secure level now does not meet the requirements for the new Secure level. In this scenario, the client that is already connected continues to be connected to the server. The new policies are applicable only to new connections.

NOTE: If you want to impose the new policies for clients that are already connected, you must force the clients to reconnect by restarting the SSL VPN.

3.2.2 Configuring a Security Level

To configure a client security level:

- 1 In the Administration Console, click *Devices > SSL VPNs > Edit*.
- 2 Select *Client Security Levels* from the *Policies* section.

Client Security Levels: 152cluster	
SecurityLevel	Message
Least Secure	Your workstation is at Least Secure Level
Moderately Secure	Your workstation is at Moderately Secure Level
Secure	Your workstation is at Secure Level
None	Client Integrity failed !!!

Server(s) must be updated before changes made on this panel will be used. See [Configuration](#) Panel for summary of changes.

OK Cancel

- Click a security level to configure it.

Edit Security Level Definition : 152cluster - Secure	
Security Level:	Secure
Display Message At Client :	Your workstation is at Secure Level
Level Definition	
Assign Remove	
Categories	Assigned
<input type="checkbox"/> Linux	
<input type="checkbox"/> Firewall_Linux	<input checked="" type="checkbox"/>
<input type="checkbox"/> Antivirus_Linux	<input checked="" type="checkbox"/>
<input type="checkbox"/> Windows	
<input type="checkbox"/> Firewall_Windows	<input checked="" type="checkbox"/>
<input type="checkbox"/> Antivirus_Windows	<input checked="" type="checkbox"/>
<input type="checkbox"/> Macintosh	
<input type="checkbox"/> Antivirus_Mac	<input checked="" type="checkbox"/>

Server(s) must be updated before changes made on this panel will be used. See [Configuration](#) Panel for summary of changes.

OK Cancel

Any category that is not enabled in the client integrity check policy appears as dimmed.

- To assign a category for a level, select categories under each operating system, then click *Assign*.
- To remove a category for a level, select the category, then click *Remove*.
- Click *OK* to save your modifications, then click *Update* on the Configuration page.

3.3 Configuring Traffic Policies

You can configure a maximum of 250 traffic rules per role, depending on the length of the policy name. If you have configured multiple traffic policies, the policies are prioritized based on the order of their creation.

The roles for a user are created in the Identity Server. These roles are displayed in the traffic policies page by default. In scenarios such as a federated setup where the role can be injected from another Identity Server, you can add or remove the user-configured roles while creating the traffic policies.

- [Section 3.3.1, "Configuring Policies," on page 41](#)
- [Section 3.3.2, "Ordering Traffic Policies," on page 43](#)
- [Section 3.3.3, "Exporting and Importing Traffic Policies," on page 44](#)

3.3.1 Configuring Policies

You can configure a different set of traffic policies for different roles as follows:

- 1 In the Administration Console, click *Devices > SSL VPNs > Edit*.
- 2 Select *Traffic Policies* from the *Policies* section.

List of Traffic Policies										Sort On: Policy Name ▾
New... Delete Enable Disable Import... Export...										
<input type="checkbox"/>	Policy Name	Enabled	Role(s)	Dst. Network	Protocol	Application	Port	Action	Security Level	Priority
<input type="checkbox"/>	Any_Role_TCP_Modify_Network		Any	10.0.0.0/255.0.0.0	TCP	AnyTCP	0	Encrypt	Secure	1
<input type="checkbox"/>	Any_Role_UDP_Modify_Network		Any	10.0.0.0/255.0.0.0	UDP	AnyUDP	0	Encrypt	None	2
<input type="checkbox"/>	FT		Any	0.0.0.0	ANY	dummyApp	0	Encrypt	None	4

- 3 Click *New*. The New dialog box is displayed.
- 4 Specify the traffic policy name in the *Traffic Policy Name* field, then click *OK*.
- 5 (Optional) To enable the full tunneling mode, select *Enabling Full Tunneling*.
For more information, see [Section 3.4, “Configuring Full Tunneling,” on page 44](#)
- 6 Click the newly added traffic policy.

Traffic Policy

Policy Name:

Any_Role_UDP_Modify_Network

Scope of Policy

Role(s):

Available Roles

001
002
003
004

Assigned Roles

[Any]

Manage Roles...

Destination Addresses:

10.0.0.0/255.0.0.0

Predefined Applications:

Name:

AnyUDP

Protocol:

UDP

Port:

0

Security Level:

None

Action

Action:

Encrypt

Server(s) must be updated before changes made on this panel will be used. See [Configuration](#) Panel for summary of changes.

OK

Cancel

Fill in the following fields:

Policy Name: Displays the name that you have specified for the traffic policy.

Role (s): The role to which the traffic rule applies. If the role was created in the Identity Server, it is displayed in *Available Roles* by default. Select the role you want to assign the traffic policy to and click the forward arrow to send it to *Assigned Roles*. If you want to assign a traffic policy to multiple roles, press the Ctrl key when selecting the roles.

To assign a traffic policy to user-defined roles, click the *Manage Roles* button.

Manage Roles

OK

Cancel

Click the *Add Role* icon to add the roles and click the *Remove selected roles* icon to delete the roles. Click *OK* to confirm your changes, or click *Cancel* to discard the changes.

The role is case-sensitive. If the role configured is `Employee` and the Identity Server sends a request for `employee`, the rule is not pushed to the client. You cannot change the role name after you have configured a traffic rule. If you do so, the changes are not reflected in the associated traffic rule.

Destination Addresses: Specify the destination IP address entries in any of the following formats:

- ♦ A single host IP address. For example, 192.168.1.1
- ♦ A range of IP addresses in the same subnet. For example, 192.168.1.1-192.168.1.10
- ♦ A combination of host address and network mask. For example, 192.168.1.0/255.255.255.0
- ♦ A full tunneling IP address 0.0.0.0.

NOTE: You can configure a traffic policy with a maximum of 20 IP address entries. However, in Enterprise Mode, the OpenVPN client can add a maximum of 100 routes.

To add an IP address, click the + icon. To delete an IP address, select the address that you want to delete, then click the - icon. You can also edit the existing IP address.

NOTE: If the traffic policy includes a host entry, you cannot change the subnet mask.

Predefined Application: Select a predefined application from the drop-down list.

Name: Specify a name for the application. This information is optional.

Protocol: Select a protocol from the drop-down list. You can select TCP, UDP, ICMP, or Any.

Port: Specify the port number on which the service is available. You can also specify a range of port numbers. You can specify a port range separated by a comma or a hyphen. For example 8, 10, 11-15.

Specify 0 to allow all ports depending on the protocol. You can configure a maximum of 20 port entries for a traffic policy.

Action: Specify if a service can be allowed or denied. Select *Encrypt* to allow the service in encrypted form. Select *Deny* if you do not want to allow the service.

Security Level: Specify the minimum level of security to be adhered to by the client machine in order to apply this traffic policy. For more information on how to configure security levels, see [Section 3.2, “Configuring Client Security Levels,” on page 39](#).

- 7 To delete a traffic policy, select the policy, then click *Delete*.
- 8 To enable a traffic policy, select the policy, then click *Enable*.
- 9 To disable a traffic policy, select the policy, then click *Disable*.
- 10 To save your modifications, click *OK*, then click *Update* on the Configuration page.

3.3.2 Ordering Traffic Policies

You can configure multiple traffic policies for a user’s role. These traffic policies can be sorted either based on their priority or alphabetically. Use the *Sort On* option in the traffic policies page to sort the traffic policies either based on the policy name or based on the priority of policies.

However, for a user, traffic policies are applied based on the order of the traffic policies. For example, the first traffic policy is applied to the user, followed by the second traffic policy, and so on. The rules set in the first traffic policy takes precedence over the next. For example, if you want to allow a user access to an application, and you place the policy as the third policy, the policy would work provided the first and second policy do not deny access to that particular application.

If you want to order the policies based on their priority, you can drag and drop the policies in the order that you want them to be placed. The *Sort On* option must be set to *Priority* in order to drag and drop the policies.

3.3.3 Exporting and Importing Traffic Policies

You can export the traffic policies that you have created and save them on your local machine as an XML file. This file can be imported when you want to copy the policies into a new setup or into an existing setup, for example, if you want to add to or duplicate the traffic policies. This feature is also useful when you want to reinstall a setup.

- 1 In the Administration Console, click *Devices > SSL VPNs > Edit*.
- 2 Select *Traffic Policies* from the *Policies* section. The SSL VPN Traffic Policies page is displayed.
- 3 Select the policies that you want to export, then click *Export*.
- 4 Specify a filename for the XML document that saves the configuration.
- 5 Specify a location to save the XML file.
- 6 To import the exported XML file, select the server into which you want to import the traffic policies.
- 7 Click *Import* in the traffic policies page.
- 8 Browse and select the XML file that contains the saved traffic policies.
- 9 To save your modifications, click *OK*, then click *Update* on the Configuration page.

3.4 Configuring Full Tunneling

The SSL VPN is configured for split tunneling by default. This means that only the traffic that is enabled to go through the protected network, such as items meant for the corporate network, goes through the VPN tunnel. Traffic to public networks does not go through the tunnel. However, if you want all traffic in the client machine to go through the tunnel, you must configure the SSL VPN for full tunneling.

When you configure the SSL VPN for full tunneling, all traffic to the protected network as well as the public network passes through the tunnel, thereby making the SSL VPN connection more secure. Any session management information between the client and the Identity server, Access Gateway (for Traditional SSL VPN), and the SSL VPN is exchanged outside the SSL VPN tunnel. You can configure full tunneling for both Kiosk mode as well as Enterprise mode.

You must configure traffic policies for both split tunneling and full tunneling in your organization in order to permit access to specific internal hosts as well as prevent a hacker from controlling the machine via a connection external to the tunnel. The split tunneling policies must be ordered at the top of the policy list and the full tunneling policy must be placed as the last policy.

3.4.1 Creating a Full Tunneling Policy

- 1 In the Administration Console, click *Devices > SSL VPNs > Edit*.
- 2 Click *New* to create a new traffic policy.
- 3 Specify a name for the traffic policy.
- 4 Select *Enable Full Tunneling*.
- 5 Select *Encrypt* to allow the service in encrypted form.
- 6 Click *OK*.

7 Select *Gateway Configuration* from the *Basic Gateway Configuration* section.

NetIQ Access Manager
ADMIN
PHYAHAGB_TREE

Access Manager | Devices | Policies | Auditing | Security

NAT/L4 related configuration
☒ Behind NAT / L4

L4 Listener Details

	Public IP Address	Port	Protocol
Kiosk Mode:	10.10.40.42	7777	TCP
Enterprise Mode:	10.10.40.42	7778	TCP

Server Listener Details

	Listening IP Address	Port	Protocol
Kiosk Mode:	164.99.184.42	7777	TCP
Enterprise Mode:	164.99.184.42	7778	TCP

Assigned IP Address Pool For Enterprise Mode

Subnet Address: 42.42.0.0
Subnet Mask: 255.255.0.0

Other Configuration

Identity Provider Address: 10.1.16.5
Access Gateway Address: 10.1.16.5
Inactivity Timeout (Minutes): 30
Encryption: AES256
Enterprise Mode Compression: Off
Authentication Hardening: On **Re-generate Key** Last Modified at: May 5, 2010 3:16 PM
Server Debug Level: Off
Client Debug Level: Off Security warning: Read this ?

Server(s) must be updated before changes made on this panel will be used. See [Configuration](#) Panel for summary of changes.

OK Cancel

8 Specify the following information in the *Other Configuration* section:

Identity Provider Address: Specify the public IP addresses or the public DNS name of the Identity Server if you are configuring the SSL VPN for the full tunneling mode. This configuration is required to split the management traffic from the tunneled traffic.

Access Gateway Address: Specify the IP address or DNS name of the Access Gateway if your server is accelerated by the Access Gateway. This field is not present if you have installed the ESP-enabled SSL VPN. This configuration is required to split the management traffic from the tunneled traffic.

NOTE: This server requires a split DNS if a DNS address is used.

9 To save your modifications, click *OK*, then click *Update* on the Configuration page.

4 Configuring How Users Connect to SSL VPN

You can configure client machines to control how users connect to the SSL VPN.

- ♦ [Section 4.1, “Preinstalling the SSL VPN Client Components,” on page 47](#)
- ♦ [Section 4.2, “Configuring Client Policies,” on page 48](#)
- ♦ [Section 4.3, “Configuring SSL VPN to Connect through a Forward Proxy,” on page 53](#)
- ♦ [Section 4.4, “Configuring SSL VPN for Citrix Clients,” on page 54](#)

4.1 Preinstalling the SSL VPN Client Components

You can preinstall the SSL VPN client components on the client machine, so that the users can access the SSL VPN in the Enterprise mode.

- ♦ [Section 4.1.1, “Installing Client Components for Linux,” on page 47](#)
- ♦ [Section 4.1.2, “Installing Client Components for Macintosh,” on page 47](#)
- ♦ [Section 4.1.3, “Installing Client Components for Windows,” on page 48](#)

4.1.1 Installing Client Components for Linux

- 1 On the client machine, download the following RPM from the `/var/opt/novell/tomcat7/webapps/sslvpn/linux` directory:

`novell-sslvpn-serv.tar.gz`

- 2 Enter the following command to untar the file:

```
tar -zxvf <filename>
```

- 3 Enter the following command to install `novl-sslvpn-service-xxx-xx.i586.rpm`:

```
rpm -ivh <rpm_name>
```

4.1.2 Installing Client Components for Macintosh

- 1 On the client machine, download the following package for the PPC platform from the `/var/opt/novell/tomcat7/webapps/sslvpn/MacOS` directory:

`novell-sslvpn-serv.tar.gz`

- 2 On the client machine, download the following package for the Intel* platform from the `/var/opt/novell/tomcat7/webapps/sslvpn/Maci386` directory:

`novell-sslvpn-serv.tar.gz`

- 3 Enter the following command to untar the file:

```
tar -zxvf novell-sslvpn-serv.tar.gz
```

- 4 Enter the following command to install the novl-sslvpn-service.pkg package extracted from the tar ball:

```
installer -pkg novl-sslvpn-service.pkg -target "/"
```

4.1.3 Installing Client Components for Windows

- 1 On the client machine, download the following file from /var/opt/novell/tomcat7/webapps/sslvpn/windows:

```
novl-sslvpn-service-install.exe
```

- 2 Run the .exe file to install the client components.

NOTE: If the Internet Explorer 7 fails to detect the ActiveX component that you have installed and tries to install it again, then it is due to some security level set in the Internet Explorer. Hence *Select Force JRE for all Clients Using Internet Browser* or modify firefox properties to avoid the failure.

4.2 Configuring Client Policies

You can configure the SSL VPN so that a client can be forced to connect in either Kiosk mode only or Enterprise mode only, depending on the role of a client. You can also configure the SSL VPN to let the client select the SSL VPN mode based on the client privileges, or you can configure the SSL VPN to download the applet client when the Internet Explorer browser is used to establish the SSL VPN connection.

- ♦ [Section 4.2.1, "Configuring Users to Connect Only in Enterprise Mode or Kiosk Mode," on page 48](#)
- ♦ [Section 4.2.2, "Allowing Users to Select the SSL VPN Mode," on page 50](#)
- ♦ [Section 4.2.3, "Configuring Client Cleanup Options," on page 50](#)
- ♦ [Section 4.2.4, "Configuring SSL VPN to Download the Java Applet on Internet Explorer," on page 51](#)
- ♦ [Section 4.2.5, "Configuring a Custom Login Policy for SSL VPN," on page 52](#)

4.2.1 Configuring Users to Connect Only in Enterprise Mode or Kiosk Mode

You can configure client policies to user roles so that they can connect only in Enterprise mode or only in Kiosk mode.

- 1 In the Administration Console, click *Devices > SSL VPNs > Edit*.
- 2 Select *Client Policies* from the policies section.

3 Select one of the following options:

Always Kiosk Mode: Select this option to force the SSL VPN users to connect in Kiosk mode only, depending on the role of the user.

Always Enterprise Mode: Select this option to force the SSL VPN users to connect in Enterprise mode only, depending on the role of the user.

Client Privilege Based Mode: Select this option to allow users to connect in either Enterprise mode or Kiosk mode, depending on their privileges. If you do not select any client modes for roles, the roles are by default configured for the *Client Privilege Based Mode* option.

NOTE: You cannot configure some roles to connect in *Always Kiosk Mode* and other roles to connect in *Always Enterprise Mode*. The two modes are mutually exclusive. However, if you configure some roles for one of these modes, and do not configure the other roles for any mode, the roles without a specific configuration are by default assigned to the *Client Privilege Based Mode*.

For example, you cannot configure the Sales role for the *Always Kiosk Mode* and the Finance role for the *Always Enterprise Mode*. However, if you configure the Sales role for the *Always Kiosk Mode* and do not configure the Finance role for any mode, the Finance role is by default configured for the *Client Privilege Based Mode*.

4 To configure the role for the client policy, specify the following information:

Role (s): The role to which the client policy applies. If the role is created in the Identity Server, it is displayed in *Available Roles* by default.

The role is case-sensitive. If the role configured is `Employee` and the Identity Server sends a request for `employee`, the rule is not pushed to the client.

Manage Roles: To assign a client policy to user-defined roles, click the *Manage Roles* button. Click the *Add Role* icon to add roles or click the *Remove selected role* icon to delete roles. Click *OK* to confirm your changes, or click *Cancel* to discard them.

Available Roles: Select the role for which you want to assign the client policy and click the forward arrow to send it to *Assigned Roles*. If you want to assign a client policy to multiple roles, press the `Ctrl` key when selecting the roles.

Assign Roles: Lists the roles for which a client policy is assigned.

If some roles are not explicitly configured for a mode, they are assigned to the Client Privileged mode by default.

5 To save your modifications, click *OK*, then click *Update* on the Configuration page.

4.2.2 Allowing Users to Select the SSL VPN Mode

To configure users to connect in either Enterprise mode or Kiosk mode, depending on their privileges, you assign them to the *Client Privilege Based Mode* option.

- 1 In the Administration Console, click *Devices > SSL VPNs > Edit*.
- 2 Select *Client Policies* from the policies section.
- 3 The Client Policies page is displayed. Select the *Client Privilege Based Mode* option to allow users to select the SSL VPN connection mode. If the client has admin privileges, it can connect in Enterprise mode; otherwise, it can connect in Kiosk mode.
- 4 To save your modifications, click *OK*, then click *Update* on the Configuration page.

If you do not configure any client modes for roles, then the roles are by default configured for the *Client Privilege Based Mode* option.

4.2.3 Configuring Client Cleanup Options

You can configure the cleanup options that are displayed to the user while disconnecting the SSL VPN connection.

- 1 In the Administration Console, click *Devices > SSL VPNs > Edit*.
- 2 Select *Client Policies* from the policies section.

Client Cleanup Options		
Cleanup Option	Default Option	Allow User to Override
Clear Browser Private Data	Yes ▼	Yes ▼
Clear Java Cache	Yes ▼	Yes ▼
Uninstall Enterprise Mode	No ▼	Yes ▼
Leave Behind the Client Components	No ▼	Yes ▼
Uninstall ActiveX control (for IE users only)	No ▼	Yes ▼

- 3 Select any of the following options:

Clear Browser Private Data: Select this option to clear the browser history and cache, saved password, authenticated sessions and auto form-fill data when the client logs out. When this option is selected, all the data and information that were saved after the SSL VPN connection was made are cleared from the client machine. In the Firefox browser, any previous browsing history or data that was present before the SSL VPN connection was made is not cleared.

Clear Java Cache: Select this option to clear the Java cache when the client logs out. This clears not just the files and applets used by the SSL VPN, but all files and applets in the cache. The Java cache is cleared when the browser window is closed.

Uninstall Enterprise Mode: Select this option to uninstall the Enterprise mode client when the client logs out.

Leave Behind the Client Components: Select this option to reduce the connection time when the client logs in again. When this option is selected, some of the SSL VPN components are left on the client and the connecting time is reduced because these components are not downloaded again.

If this option is not enabled:

- ♦ All client components downloaded for the connection are removed in Kiosk mode.
- ♦ All client components other than the service RPM or service MSI are removed in Enterprise mode. This is because the service RPM or service MSI is mandatory for operation in this mode.

Uninstall ActiveX control (for IE users only): When a user connects to the SSL VPN through Internet Explorer, ActiveX is downloaded to the client machine to enable the SSL VPN connection. You can select this option to remove the ActiveX control when the client logs out.

To select any of these options, set *Default Option* to *Yes*.

If you set *Allow User to Override* to *Yes*, users can change any of the cleanup options set by you. To require users to retain the cleanup options you configured, set *Allow User to Override* to *No*.

- 4 To save your modifications, click *OK*, then click *Update* on the Configuration page

4.2.4 Configuring SSL VPN to Download the Java Applet on Internet Explorer

The SSL VPN client components are downloaded on the client machine through a Java applet or through ActiveX, depending on the browsers they use. The Internet Explorer browser uses the ActiveX control by default to download the SSL VPN client components. However, some Windows clients do not allow ActiveX controls to run in Internet Explorer.

In such scenarios, the you can force the Windows client to load the Java applet instead of the ActiveX control.

- 1 In the Administration Console, click *Devices > SSL VPNs > Edit*.
- 2 Select *Client Policies* from the policies section.

Client Mode

☐ Always Kiosk Mode

☐ Always Enterprise Mode

☒ Client Privilege Based Mode

JRE in IE

☒ Force JRE for all clients using Internet Explorer browser

Custom Login

[New...](#) | [Delete](#)

☐ Custom Action

☐ [modify firefox properties](#)

Default URL:

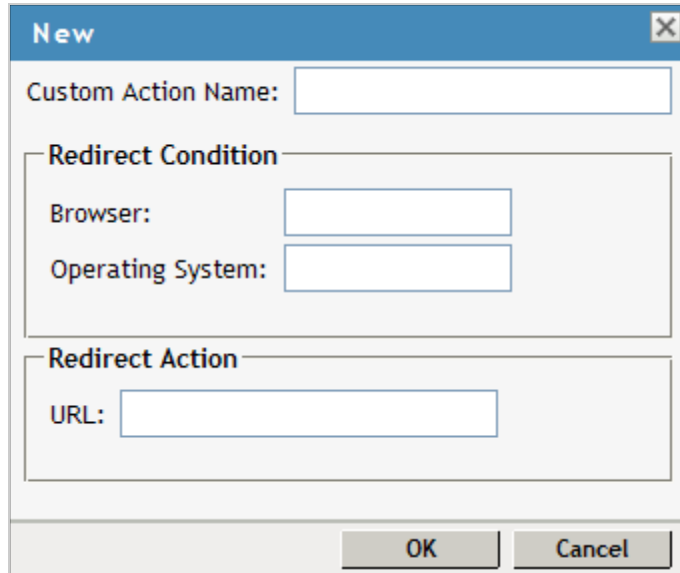
Server(s) must be updated before changes made on this panel will be used. See [Configuration](#) Panel for summary of changes.

- 3 Select *Force JRE for all Clients Using Internet Browser*.
- 4 To save your modifications, click *OK*, then click *Update* on the Configuration page.

4.2.5 Configuring a Custom Login Policy for SSL VPN

When you configure a custom login policy for SSL VPN, the SSL VPN server redirects the login requests to different URLs based on the policy configuration.

- 1 In the Administration Console, click *Devices > SSL VPNs > Edit*.
- 2 Select *Client Policies* from the policies section.
- 3 Click *New* in the *Custom Login* section.



The screenshot shows a 'New' dialog box with the following fields:

- Custom Action Name:** A text input field.
- Redirect Condition:** A section containing two text input fields: 'Browser' and 'Operating System'.
- Redirect Action:** A section containing a text input field labeled 'URL'.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

- 4 Specify the following information:

Custom Action Name: Specify a name for the custom login policy.

Redirect Condition: Specify the redirect condition in terms of the browser and the operating system. The conditions configured for the workstation platform and the browser platform are verified against the user agent HTTP header of the browser.

For an example of a custom-login policy configured for Citrix clients, see [Section 4.4.3, “Configuring a Custom Login Policy for Citrix Clients,”](#) on page 56.

- ♦ The browser can be Firefox, Safari*, Internet Explorer, or any other. You can specify more than one browser, separated by commas.
- ♦ The operating software can be Windows, Linux, Macintosh, or Any. When you configure this attribute to Any, the custom-login policy becomes platform independent.

Redirect URL: Specify the URL to which a user is redirected if the redirection conditions match.

- 5 Click *OK*.
- 6 Specify a URL as the default URL. The user is redirected to this URL if none of the conditions are met.
- 7 To save your modifications, click *OK*, then click *Update* on the Configuration page.

4.3 Configuring SSL VPN to Connect through a Forward Proxy

The SSL VPN can be configured to detect and connect through a forward proxy in both Kiosk and Enterprise modes after authenticating to the Identity Server. To establish the SSL VPN connection through a forward proxy, you can either configure the browser or create a `proxy.conf` file in the user's home directory. You must also ensure that the SSL VPN server is listening on the TCP port and not on the UDP port.

NOTE: The SSL VPN client ignores the use of dynamic proxy configuration either by assigning a `proxy.pac` JavaScript to the browser client or by using the WPAD protocol. In such a scenario, use the `proxy.conf` file.

- ♦ [Section 4.3.1, “Understanding How SSL VPN Connects through a Forward Proxy,” on page 53](#)
- ♦ [Section 4.3.2, “Creating the proxy.conf File,” on page 53](#)

4.3.1 Understanding How SSL VPN Connects through a Forward Proxy

When a user initiates a connection to the SSL VPN server through a browser, the SSL VPN uses the following process to connect:

1. the SSL VPN checks to see if the browser is configured to use a proxy.
2. If it is, the SSL VPN checks for the `proxy.conf` file in the user's home directory.
3. If a proxy configuration file is present, the following occurs:
 - ♦ the SSL VPN checks for the format of the file. If the information provided in the file is not in the correct format, the SSL VPN proceeds with step 4.
 - ♦ If the configuration information is in the correct format, the SSL VPN reads the proxy information from the `proxy.conf` file, then proceeds with Step 6.
4. If the proxy configuration file is not present or if the information is not in the correct format, the SSL VPN checks for proxy configuration information from the browser registry or profile.
5. If the SSL VPN is unable to get the proxy configuration information either through the `proxy.conf` file or through the registry, it throws an error asking the user to edit the `proxy.conf` and tries to establish a direct connection.
6. the SSL VPN reads the connection order information in the configuration file and connects either directly or through the proxy.

4.3.2 Creating the proxy.conf File

- 1 Create a text file and save it as `proxy.conf` in the following location:

`C:\Documents and Settings\<username>` in Windows.

`/home/<username>` in Linux.

- ♦ `$home/` in Macintosh.

- 2 Specify the IP address and the port number of the forward proxy in the following format:

`proxyHost=<IPaddress>:<port number>`

For example,

`proxyHost=192.10.0.0:8080`

- 3 Add one of the following lines to specify the connection order:
 - ♦ To configure the SSL VPN to connect through the proxy first, specify
`ConnectionOrder=direct:proxy`
 - ♦ To configure the SSL VPN to try a direct connection, specify
`ConnectionOrder=proxy:direct`

If the connection order is not specified in the configuration file, the SSL VPN connects directly without the proxy.

- 4 (Optional) If the Basic authentication method is used for the forward proxy, the SSL VPN can connect in Kiosk mode as well as Enterprise mode. To enable the SSL VPN connection when authentication is enabled, specify the username and password of the forward proxy administrator in the following format:

```
proxyAuth=<username>:<password>
```

This is not a recommended method because you need to specify the credentials of the forward proxy in the configuration file and this might be a security vulnerability.

- 5 Save and close the file.

4.4 Configuring SSL VPN for Citrix Clients

You can configure a user to enable the single sign-on feature of Access Manager Appliance when accessing published Citrix applications through the SSL VPN. To enable single sign-on, you must configure a custom login policy and protect the Citrix Application Server with the Access Gateway. If you are using the ESP-enabled SSL VPN, you must install an Access Gateway in order to protect the Citrix server. The following sections discuss the configuration process:

- ♦ [Section 4.4.1, “Prerequisites,” on page 54](#)
- ♦ [Section 4.4.2, “How It Works,” on page 55](#)
- ♦ [Section 4.4.3, “Configuring a Custom Login Policy for Citrix Clients,” on page 56](#)
- ♦ [Section 4.4.4, “Configuring the Access Gateway to Protect the Citrix Server,” on page 56](#)
- ♦ [Section 4.4.5, “Configuring Single Sign-On between Citrix and SSL VPN,” on page 57](#)

4.4.1 Prerequisites

- ☐ NFuse server
- ☐ MetaFrame server
- ☐ Identity Server

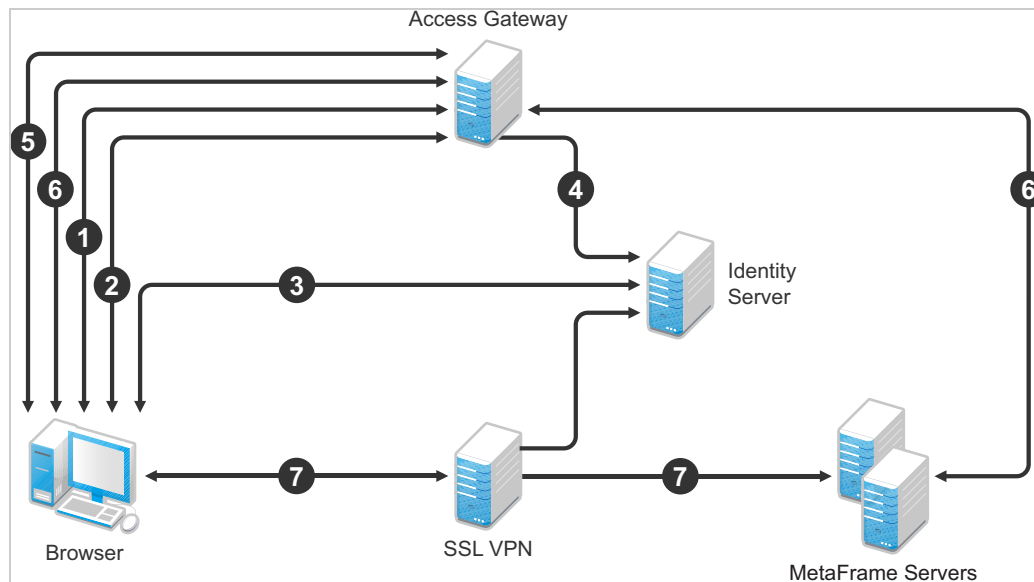
The MetaFrame server must be placed in the protected network. The SSL VPN server must use its private network interface adapter to communicate with the network interface of the MetaFrame server.

- ☐ Access Gateway
- ☐ Configure the SSL VPN to use the same Identity Server as the Access Gateway.
- ☐ Download the `Citrix_Script.js` file from the [Additional Resources \(http://www.novell.com/documentation/novellaccessmanager31/index.html\)](http://www.novell.com/documentation/novellaccessmanager31/index.html) section on the NetIQ Documentation site and copy it to a Web server that is protected by the Access Gateway.

4.4.2 How It Works

Access Manager Appliance can be configured to provide single sign-on for the Citrix clients. [Figure 4-1](#) illustrates this process for the Citrix Web client.

Figure 4-1 Citrix Client Configuration



1. The client specifies the public DNS name of the Access Gateway that accelerates the Web Interface login page of the Citrix MetaFrame Presentation Server.
2. The Access Gateway redirects the user to the Identity Server for authentication, because the URL is configured as a protected resource.
3. The Identity Server authenticates the user's identity.
4. The Identity Server propagates the session information to the Access Gateway through the Embedded Service Provider.
5. The Access Gateway has been configured with a Form Fill policy, which invokes the SSL VPN servlet along with the corresponding policy information for that user. The SSL VPN servlet creates a secure tunnel between the client and the SSL VPN server.
6. On successful SSL VPN connection, the Access Gateway performs a single sign-on to the Citrix MetaFrame Presentation Server. The user is authenticated to both the Citrix Presentation Server and to the SSL VPN server.
7. The Web session containing the list of published applications in the Citrix Presentation server is served to the client through the Access Gateway.
8. When the user connects to the published application, the data goes through the secure tunnel that is formed between the client and the SSL VPN server.

4.4.3 Configuring a Custom Login Policy for Citrix Clients

A custom login policy must be configured to enable users to use a browser to access Citrix applications protected by Access Manager Appliance. This is because the browser settings of the client need to be modified so that connections to Citrix applications can happen through the SSL VPN.

The following procedure configures a sample custom login policy for Citrix where all Linux users connecting from the Firefox browser on Linux are redirected to a page that modifies the browser settings and then redirects the user to the SSL VPN/login URL:

- 1 In the Administration Console, click *Devices > SSL VPNs > Edit*.
- 2 Select *Client Policies* from the policies section.
- 3 Click *New* in the *Custom Login* section.
- 4 Specify the following information in the *New* dialog box.
 - Custom Action Name:** Specify a name for the custom login policy. For example, `modify_firefox_properties`
 - Redirect Condition:**
 - ◆ Specify Firefox as the browser.
 - ◆ Specify Linux as the Operating Software.
 - Redirect URL:** Specify the redirect URL as `http://<sslvpn-url>/sslvpn/pages/sslvpn-citrix.jar!configure_browser.html`.
- 5 Click *OK*.
- 6 Specify `/login` as the default URL. The user is redirected to this URL if none of the conditions are met.
- 7 To save your modifications, click *OK*, then click *Update* on the Configuration page.

4.4.4 Configuring the Access Gateway to Protect the Citrix Server

To enable users to access Citrix applications through the SSL VPN, you must create a protected resource to protect the Citrix login page.

- 1 In the Administration Console, click *Devices > Access Gateways > Edit > [Name of Reverse Proxy]*.
The reverse proxy can be set up to require SSL or not.
- 2 Click *Name of Proxy Service > Protected Resources > New*.
- 3 When you configure the protected resource, set up the following:
 - ◆ Select a contract that requires authentication. Usually this is a Name/Password contract, but it can be a certificate contract if your NFuse server is configured to use certificates.
 - ◆ For the URL Path List, specify the URL to the Citrix login page. This URL should include the filename of this login page.

For more information, see “[Configuring Protected Resources](#)” in the *NetIQ Access Manager Appliance 4.0 Access Gateway Guide*

- 4 On the Server Configuration page, click *OK*, then click *Update*.

4.4.5 Configuring Single Sign-On between Citrix and SSL VPN

You need to create a Form Fill policy and assign it to the protected resource for the Citrix login page.

- 1 In the Administration Console, click *Devices > Access Gateways > Edit > [Name of Reverse Proxy]*.
- 2 Click *Form Fill > Manage Policies > New*.
- 3 Name the Citrix policy, select *Access Gateway: Form Fill* as the type, then click *OK*.
- 4 In the *Actions* section, click *New > Form Fill*.
- 5 In the *Form Selection* section, identify the form on the Citrix login page.
- 6 In the *Fill Options* section, create the following:
 - ♦ Username input field
 - ♦ Password input field
 - ♦ (Optional) If your login page requires a domain, add a domain input field.
- 7 Configure the following *Submit* options:
 - 7a Select *Auto Submit*.
 - 7b Select *Enable JavaScript Handling*.
 - 7c Click *Statements to Execute on Post*. Copy the Citrix Script found in the [Additional Resources](http://www.novell.com/documentation/novellaccessmanager31/index.html) (<http://www.novell.com/documentation/novellaccessmanager31/index.html>) section in the NetIQ Documentation site.
 - 7d In the script, replace `<ag-url>` with the following:
 - ♦ For a Traditional SSL VPN, use the hostname of the Access Gateway that is accelerating the SSL VPN server.
 - ♦ For an ESP-enabled SSL VPN, use the hostname of the SSL VPN server.
 - 7e Change the protocol to HTTPS if the secure protocol is used.
 - 7f Replace `<Webserver-path>` with the location of the Web server on which the `Citrix_Script.js` JavaScript file is located. When this JavaScript file is used, it connects users from the outside through the SSL VPN.
 - 7g Change the URL as follows, if you want to use the custom login method:
`http://<ag-url>/sslvpn/custom-login`
- 8 Configure any other options to match your form and your network.

For more information, see “[Creating Form Fill Policies](#)” in the *NetIQ Access Manager Appliance 4.0 Policy Guide*.
- 9 In the *Actions* section, click *New > Form Login Failure*.
- 10 Specify the procedures you want followed when login fails.

For more information, see *Login Failure Policy* in the *Novell Access Manager 3.1 SP4 Policy Management Guide* (<https://www.netiq.com/documentation/novellaccessmanager31/policyhelp/data/bookinfo.html>).

Citrix displays login failures via the query string, so you need to use CGI matching
- 11 Click *OK*, then click *Apply Changes*.
- 12 Click *Close*.

You should return to the Form Fill page for the protected resource.
- 13 Select the policy you just created, then click *Enable*.
- 14 Click *Configuration Panel*, then click *OK*.
- 15 On the Server Configuration page, click *OK*, then click *Update*.

5 Clustering the High-Bandwidth SSL VPN Servers

You can cluster the high-bandwidth SSL VPN servers to provide load balancing and fault tolerance capabilities and act as a single server. The SSL VPN servers in a cluster share a common configuration and are managed on a single Administration Console. The servers are configured to balance load and failover. When a member of the SSL VPN cluster fails, the user sessions are failed over to another SSL VPN server that is healthy.

Even though the SSL VPN authentication connection to the cluster remains unaffected during the session failover, the SSL VPN tunnel goes down and a new tunnel is established with the new SSL VPN server. This might affect applications such as FTP that were being accessed through the tunnel at the time of failover.

A cluster can be set up to function with an L4 switch or the Access Gateway to handle load balancing. A cluster can be set up to function with an L4 switch or by using the Access Gateway. You can have a cluster of servers in both HTTP and HTTPS.

Clients access the virtual IP address of the cluster presented on the L4 switch, and the L4 switch alleviates server load by balancing traffic across the cluster. Whenever a user accesses the virtual IP address (port 8080) assigned to the L4 switch, the system routes the user to one of the SSL VPN servers in the cluster, as traffic necessitates.

Using L4 for Clustering: In this approach, the SSL VPN cluster is placed behind an L4 switch. If the tunnel IP address configured in the administration console is the virtual IP address of an L4 switch, additional load balancing is done at this level. When a user is authenticated, all the members of the cluster are informed, so that the cluster members can handle failover. For more information on configuring the L4 switch, see [“Configuration Tips for the L4 Switch”](#) in the *NetIQ Access Manager Appliance 4.0 Setup Guide*.

Using Access Gateway for Clustering: In a direct connection, the client directly establishes contact with the tunneling component, which could be a NAT IP address and not the L4 switch. This approach ensures that the load balancing of SSL VPN servers is achieved with the help of Access Gateway clusters. The client establishes connection with the first tunnel.

For more information, see [Chapter 5.5, “Clustering SSL VPNs by Using the Access Gateway without an L4 Switch,”](#) on page 64.

This section has the following information:

- ♦ [Section 5.1, “Prerequisites,”](#) on page 60
- ♦ [Section 5.2, “Limitations,”](#) on page 60
- ♦ [Section 5.3, “Creating a Cluster of SSL VPN Servers,”](#) on page 60
- ♦ [Section 5.4, “Clustering SSL VPN by Using an L4 Switch,”](#) on page 63
- ♦ [Section 5.5, “Clustering SSL VPNs by Using the Access Gateway without an L4 Switch,”](#) on page 64
- ♦ [Section 5.6, “Configuring SSL VPN to Monitor the Health of the Cluster,”](#) on page 66

5.1 Prerequisites

- ☐ An L4 switch is installed. The LB algorithm can be anything (hash/sticky bit) defined at the Real server level.
- ☐ Persistence (sticky) sessions are enabled on the L4 switch. You usually define this at the virtual server level.
- ☐ SSL VPN servers are installed and imported into the same administration console. The health status of all the imported servers must be green or yellow.
- ☐ The traffic policies must be imported into the SSL VPN servers before they are clustered.
- ☐ An SSL VPN Server configuration is created for the cluster, and all the SSL VPN servers are assigned to this configuration.

The base URL DNS name of this configuration must be the virtual IP address of the L4 server. The L4 switch balances the load between the SSL VPN servers in the cluster.

- ☐ The following ports are open on the L4 switch for SSL VPN communication:
 - ♦ 8443 (for HTTPS communication)
 - ♦ 7777 (for Stunnel over TCP and OpenVPN over UDP)
 - ♦ 7778 (for OpenVPN over TCP)

5.2 Limitations

When you are clustering the SSL VPN servers, all SSL VPN servers must be running the high-bandwidth version of SSL VPN.

5.3 Creating a Cluster of SSL VPN Servers

The system automatically enables clustering when multiple SSL VPN servers exist in a group. To create an SSL VPN cluster, you must create a cluster of SSL VPNs after you install an SSL VPN server, then assign one or more SSL VPN servers to that cluster. The Access Manager software configuration process is the same whether there is one server or multiple servers in a cluster.

This section describes how to set up and manage a cluster of SSL VPN servers:

- ♦ [Section 5.3.1, “Creating a Cluster of SSL VPN Servers,” on page 60](#)
- ♦ [Section 5.3.2, “Adding an SSL VPN Server to a Cluster,” on page 62](#)
- ♦ [Section 5.3.3, “Removing an SSL VPN Server from a Cluster,” on page 62](#)

5.3.1 Creating a Cluster of SSL VPN Servers

To create a new SSL VPN server cluster, you start by creating a cluster configuration with a primary server.

- 1 In the Administration Console, click *Devices > SSL VPN*.
- 2 Select the SSL VPN server that you want to add to the cluster, then click *New Cluster*.



- 3 Specify a name for the cluster configuration. If you selected the server in the previous step, the IP address of the server is displayed in the *Primary Server* drop-down list. If you have not selected a server in the previous step, you can now select the server or servers that you want to assign to this configuration.
- 4 Click OK.
- 5 Click the cluster configuration name that you created.
- 6 On the Cluster Details page, click *Edit*.

Cluster Detail Edit: sslclstr

Name:

Description:

Primary Server:

- 7 Fill in the following fields as required:
 - Name:** Specifies the name of the SSL VPN server cluster configuration. You can modify the name of the cluster if you want.
 - Description:** Specify a brief description of the SSL VPN cluster.
 - Primary Server:** Specify the IP address of the primary server in the SSL VPN server cluster. The *Cluster Members* section displays the IP address and other details of the SSL VPN servers that are assigned to the cluster.
- 8 Click OK.

The status icons for the configuration and the SSL VPN Server should turn green. It might take several seconds for the SSL VPN server to start and for the system to display a green light.

5.3.2 Adding an SSL VPN Server to a Cluster

After you create a cluster and identify the primary member, you can add other SSL VPN servers to the cluster. You can add more than one SSL VPN server to the SSL VPN cluster.

- 1 In the Administration Console, click *Devices > SSL VPNs*.
- 2 On the Servers page, select the server, then click *Actions > Assign to Cluster*.



To select all the servers in the list, select the top-level Server check box.

- 3 Select the name of the cluster that you want to add the SSL VPN server to.

The health status of the SSL VPN server turns green, if the server is already configured and the trust relationship is established with the Identity Servers. Otherwise, the health status is displayed as yellow. It might take several seconds for the SSL VPN server to start and for the system to display the health icon.

5.3.3 Removing an SSL VPN Server from a Cluster

Removing an SSL VPN server from a cluster disassociates the SSL VPN server from the cluster configuration. You can either remove servers individually or remove all the clusters at the same time.

When you remove a server from a cluster, all of the configuration except the trust relationship remains unchanged and can be reassigned later or assigned to another server. The trust relationship established with the Identity Server is lost when a server is removed from the cluster.

- 1 In the Administration Console, click *Devices > SSL VPNs*.
- 2 Select the server, then click *Stop*. Wait for the *Health* tab to show a red icon, indicating that the server has stopped.
- 3 Select the server, then choose *Actions > Remove from Cluster*.



- 4 Click *OK*.

5.4 Clustering SSL VPN by Using an L4 Switch

You configure the SSL VPN cluster to be behind a Layer 4 (L4) switch because it is essential in order to assign multiple SSL VPN servers to the same configuration. You can use the same L4 switch for SSL VPN server clustering, Identity Server clustering, and Access Gateway clustering, provided that you use different virtual IP addresses.

You can either have a cluster of traditional SSL VPN servers by using L4 switches and Access Gateways or you can have a cluster of ESP-enabled SSL VPNs by using the L4 switch. In a cluster, policies such as the client integrity check policies, traffic policies, and client policies are common to all the cluster members. However, each of the secondary members of the cluster must have specific listening IP addresses for Kiosk mode and Enterprise modes and a specific subnet mask and subnet addresses configured for Enterprise mode.

Make sure that the base URL of SSL VPN is resolvable with its own IP address as well as the public IP address of the L4 switch. The Identity Server should be able to resolve the base URL of SSL VPN to the virtual IP address of the SSL VPN cluster.

5.4.1 Configuring a Cluster of Traditional SSL VPNs by Using an L4 Switch

To configure a cluster of traditional SSL VPNs

- 1 Install the SSL VPN servers and import them into the same administration console.
- 2 Verify that the health of all the imported SSL VPNs is displayed as green or yellow.
- 3 Configure the L4 switch, gateway details, and Audit events in the SSL VPN server that you want to mark as primary.

For more information on configuring the L4 switch and gateway details, see [Section 2.1, “Configuring the IP Address, Port, and Network Address Translation,” on page 21](#). For more information on configuring the Audit events, see [Section 6.2, “Enabling SSL VPN Audit Events,” on page 70](#).

- 4 Import the traffic policies into the server.

For more information on importing the traffic policies, see [“Exporting and Importing Traffic Policies” on page 44](#).

- 5 Create a cluster of SSL VPNs.

For more information on creating a cluster, see [Section 5.3.1, “Creating a Cluster of SSL VPN Servers,” on page 60](#).

- 6 Assign all SSL VPN servers to the cluster.

For more information, see [Section 5.3.2, “Adding an SSL VPN Server to a Cluster,” on page 62](#).

- 7 In the Administration Console, click *Devices > SSL VPNs > Edit*, then select the Gateway configuration page. Configure specific listening IP addresses for Kiosk mode and Enterprise modes. Configure specific listening IP addresses for Kiosk mode and Enterprise modes. Make sure that each of the cluster members are assigned to different IP pools for Enterprise mode. For more information, see [Section 2.1, “Configuring the IP Address, Port, and Network Address Translation,” on page 21](#).
- 8 Accelerate the SSL VPN server by using the Access Gateway.
- 9 To save your modifications, click *OK*, then click *Update* on the Configuration page.

5.5 Clustering SSL VPNs by Using the Access Gateway without an L4 Switch

You can install and run the SSL VPN self-monitoring and failover scripts on each SSL VPN server in order to provide automatic monitoring and failover support for the SSL VPN servers that are behind a 3.1 SP4 Access Gateway.

When the health status of an SSL VPN server is bad, these scripts modify the iptables entries on that server to stop the Access Gateway from sending connection requests to that particular SSL VPN server. When the SSL VPN server health status returns to normal, the scripts remove the iptables entries and allow the Access Gateway to communicate with the SSL VPN server. You must perform the following tasks to configure load balancing and fault tolerance through the Access Gateway:

- ♦ [Section 5.5.1, “Configuring the Access Gateway,” on page 64](#)
- ♦ [Section 5.5.2, “Installing the Scripts,” on page 65](#)
- ♦ [Section 5.5.3, “Testing the Scripts,” on page 65](#)

5.5.1 Configuring the Access Gateway

- 1 In the Administration Console, click *Access Gateways > Edit > [Name of Reverse Proxy] > [Name of Proxy Service] > Web Servers*.
- 2 Add all the SSL VPN servers that are part of the failover group as origin Web servers to the proxy service that you have defined.
- 3 Click *TCP Connect Options*.
- 4 Select *Round Robin* in the *Policy for Multiple Destination IP Addresses* field.
- 5 Select *Enable Persistent Connections*.
- 6 Save your changes and update the Access Gateway.

5.5.2 Installing the Scripts

- 1 Download the tar file containing scripts for SSL VPN automatic monitoring and failover from the Additional Resources section on the [NetIQ Access Manager documentation page \(http://www.netiq.com/documentation/novellaccessmanager32/index.html\)](http://www.netiq.com/documentation/novellaccessmanager32/index.html). The tar file contains `sslvpn-heartbeat.sh` and `sslvpn-heartbeat`.
- 2 Copy the `sslvpn-heartbeat.sh` script to the `/opt/novell/sslvpn/bin` directory in each of the SSL VPN servers.
- 3 Copy the `sslvpn-heartbeat` file to the `/etc/init.d/` directory.
- 4 Enter the following commands to change `sslvpn-heartbeat.sh` and `sslvpn-heartbeat` into executable files:

```
chmod +x sslvpn-heartbeat.sh
chmod +x sslvpn-heartbeat
```
- 5 Enter the following command to run the script every time the Access Gateway is started:

```
insserv /etc/init.d/sslvpn-heartbeat
```

5.5.3 Testing the Scripts

- 1 Enter the following command to stop the SSL VPN server:

```
/etc/init.d/novell-sslvpn stop OR rcnovell-sslvpn stop
```
- 2 Enter the following command to verify if the scripts have blocked port 8080:

```
iptables -L
```

The following lines are displayed if port 8080 is blocked:

```
Chain      sslvpn-heartbeat-chain (1 reference)
target     prot opt source          destination
REJECT     tcp  --  anywhere        anywhere        tcp
dpt:http-alt reject-with icmp-port-unreachable
```
- 3 In the Administration Console, click *Access Gateways* > *[Name of Server]* > *Health*. The following message is displayed if the SSL VPN server is down:


```
The HTTP Reverse Proxy service <reverse proxy name> might not be functioning properly. Few of the Web servers being accelerated are unreachable <sslvpn server IP Address>:8080
```
- 4 Click *Update from Server* to get the latest health status of the Access Gateway.
- 5 Connect to SSL VPN. Verify that your connection was sent to the SSL VPN that is running and not to the one that is marked as down by the Access Gateway.
- 6 Enter the following command to start the SSL VPN server:

```
/etc/init.d/novell-sslvpn start
OR rcnovell-sslvpn start
```
- 7 Enter the following command to verify if the script has removed the block on port 8080:

```
iptables -L
```

The following lines are displayed if the block on port 8080 is removed:

```
Chain sslvpn-heartbeat-chain (1 references)
target     prot opt source          destination
```
- 8 In the Administration Console, click *Access Gateways* > *[Name of Server]* > *Health*, then check to make sure that the SSL VPN server is up.

- 9 Click *Update from Server* to get the latest health status of the Access Gateway.
- 10 Connect to SSL VPN. Verify if your connection was sent to the SSL VPN server that was restarted. It might require several attempts before you can connect to the desired Access Gateway.
- 11 Repeat [Step 1](#) to [Step 8](#) to verify if the SSL VPN health scripts are working on all the SSL VPN servers.

5.6 Configuring SSL VPN to Monitor the Health of the Cluster

The L4 switches use health checks to determine which cluster members are ready to receive requests and which cluster members are unhealthy and should not receive requests. You need to configure the L4 switch to monitor the heartbeat URL of the Identity Servers and Access Gateways, so that the L4 switch can use this information to accurately update the health status of each cluster member.

- ♦ [Section 5.6.1, “Services of the Real Server,” on page 66](#)
- ♦ [Section 5.6.2, “Monitoring the SSL VPN Server Health,” on page 67](#)

5.6.1 Services of the Real Server

A user’s authentication resides on the real (authentication) server cluster member that originally handled the user’s authentication. If this server malfunctions, all users whose authentication data resides on this cluster member must reauthenticate.

Requests that require user authentication information are processed on this server. When the system identifies a server as not being the real server, the HTTP request is forwarded to the appropriate cluster member, which processes the request and returns it to the requesting server.

- ♦ [“A Note about Alteon Switches” on page 66](#)
- ♦ [“Real Server Settings Example” on page 67](#)
- ♦ [“Virtual Server Settings Example” on page 67](#)

A Note about Alteon Switches

When you configure an Alteon* switch for clustering, direct communication between real servers must be enabled. If direct access mode is not enabled and one of the real servers tries to proxy another real server, the connection fails and times out.

To enable direct communication on an Alteon switch:

- 1 Go to `cfg > slb > adv > direct`.
- 2 Specify `e` to enable direct access mode.

With some L4 switches, you should configure only the services that you are using. For example, if you configure the SSL service for the L4 switch and you have not configured SSL in Access Manager, then the HTTP service on the L4 switch does not work. If the health check for the SSL service fails, the L4 switch assumes that all the services configured to use the same virtual IP are down.

Real Server Settings Example



Virtual Server Settings Example



5.6.2 Monitoring the SSL VPN Server Health

The health status of the SSL VPN server can be monitored by using the heartbeat URL. The heartbeat URL uses the DNS name of the SSL VPN server as follows:

```
https://<SSLVPN DNS NAME>/sslvpn/heartbeat
```

L4 switches require you to use the IP address rather than the DNS name. If the IP address of the SSL VPN server is 10.10.16.50, and you have configured it for HTTPS, the heartbeat URL is:

```
https://10.10.16.50:8443/sslvpn/heartbeat
```

You must configure the L4 switch to use this heartbeat to perform a health check. If you have configured SSL on the SSL VPN servers and your L4 switch has the ability to do an SSL L7 health check, you can use HTTPS. The SSL L7 health check returns a value of 200 OK, indicating everything is healthy. Any other status code indicates an unhealthy state.

For a Foundry* switch, the L7 health check script string should look similar to the following when the hostname is sslvpn1 and the IP address is 10.10.16.50:

```
healthchk sslvpn1ssl tcp
  dest-ip 10.10.16.50
  port ssl
  protocol ssl
  protocol ssl url "GET /sslvpn/heartbeat HTTP/1.1\r\nHost: st160.lab.tst"
  protocol ssl status-code 200 200
  l7-check
```

If your switch does not support an SSL L7 health check, the HTTPS URL returns an error, usually a 404 error. The SSL VPN Server heartbeat URL listens on both HTTPS and HTTP, so you can use an HTTP URL for switches that do not support the SSL L7 health check. For example:

```
http://10.10.16.50:8080/sslvpn/heartbeat
```

An Alteon switch does not support the L7 health check, so the string for the health check should look similar to the following:

```
open 8080,tcp
send GET /sslvpn/heartbeat HTTP/1.1\r\nHOST:heartbeat.lab.tst \r\n\r\n
expect HTTP/1.1 200
close
```

6 Monitoring the SSL VPN Servers

This section describes the various ways you can determine whether the SSL VPN server is functioning normally and whether an Internet attack is in progress.

- ♦ [Section 6.1, “Viewing and Editing SSL VPN Server Details,” on page 69](#)
- ♦ [Section 6.2, “Enabling SSL VPN Audit Events,” on page 70](#)
- ♦ [Section 6.3, “Viewing SSL VPN Statistics,” on page 71](#)
- ♦ [Section 6.4, “Disconnecting Active SSL VPN Connections,” on page 74](#)
- ♦ [Section 6.5, “Monitoring the Health of SSL VPN Servers,” on page 75](#)
- ♦ [Section 6.6, “Viewing the Command Status of SSL VPN Server,” on page 77](#)
- ♦ [Section 6.7, “Monitoring SSL VPN Alerts,” on page 79](#)

6.1 Viewing and Editing SSL VPN Server Details

- 1 In the Administration Console, click *Devices > SSL VPNs*.
- 2 Click the server whose information you want to view. The following information about the server is displayed:

Edit: Click this option to modify the general details of the selected SSL VPN server. For more information, see [Section 8.3, “Modifying SSL VPN Server Details,” on page 88](#).

The General page displays information about the selected server. If the field is empty, click *Edit* to add a value. The fields that contain links transfer you to another page where you can edit the information.

Name: Specifies the Administration Console display name of the server. This field is mandatory. Click the link or click *Edit* to edit the name.

Management IP Address: Specifies the IP address used to manage the server. This field is mandatory.

Port: Specifies the port used for management. This field is mandatory.

Location: Specifies the location of the SSL VPN server. This information is optional, but useful if your network contains multiple SSL VPN servers.

Server Version: Specifies the version of the installed server RPM.

Description: Provides a brief description of the SSL VPN server. This information is optional, but useful if your network contains multiple SSL VPN servers.

- 3 Click *Close* to save and close the General page.

6.2 Enabling SSL VPN Audit Events

The *Novell Audit Settings* option allows you to configure the events you want audited. The following steps assume that you have already set up Novell Audit on your network. For more information, see *Configuring the Administration Console* in the “[Configuring the Administration Console](#)” in the *NetIQ Access Manager Appliance 4.0 Administration Console Guide*.

- 1 In the Administration Console, click *Devices > SSL VPNs > Edit*.
- 2 Select *Novell Audit Settings* from the *Novell Audit and Alerts* section.

Novell Audit Settings for SSL VPN:	
Events	
<input type="checkbox"/> Select All	
<input checked="" type="checkbox"/> Authentication Logs	<input type="checkbox"/> Command Line Interface Logs
<input type="checkbox"/> Command Line Interface Debug Logs	<input type="checkbox"/> Servlet Communications Logs
<input type="checkbox"/> Connection Manager Logs	<input type="checkbox"/> Certificate Management Logs
<input type="checkbox"/> Certificate Management Debug Logs	<input type="checkbox"/> SSL VPN Incoming Connections Logs
<input type="checkbox"/> SSL VPN Incoming Connections Debug Logs	<input checked="" type="checkbox"/> Other SSL VPN Gateway Logs
<input type="checkbox"/> Cluster Logs	
Server(s) must be updated before changes made on this panel will be used. See Configuration Panel for summary of changes.	
<input type="button" value="OK"/>	<input type="button" value="Cancel"/>

- 3 Select the *Select All* option to receive logs for all the events.
Or, select one or more of the following:

Event	Description
Authentication Logs	Generates a log file containing the authentication details.
Command Line Interface Logs	Generates a log file containing command line actions.
Command Line Interface Debug Logs	Generates a log file containing command line actions. These logs help in debugging errors.
Servlet Communications Logs	Generates a log file containing information on servlet communication.
Connection Manager Logs	Generates a log file containing information on the connection activity.
Certificate Management Logs	Generates a log file containing certificate management information.
Certificate Management Debug Logs	Generates a log file containing certificate management information.
SSL VPN Incoming Connections Logs	Generates a log file containing information on the incoming connection.
SSL VPN Incoming Connections Debug Logs	Generates a log file containing debug information on the incoming connection.
Other SSL VPN Gateway Logs	Generates a log file containing miscellaneous information.
Cluster Logs	Generates a log file containing information about the SSL VPN cluster.

- 4 To save your modifications, click *OK*, then click *Apply Changes* on the Configuration page.

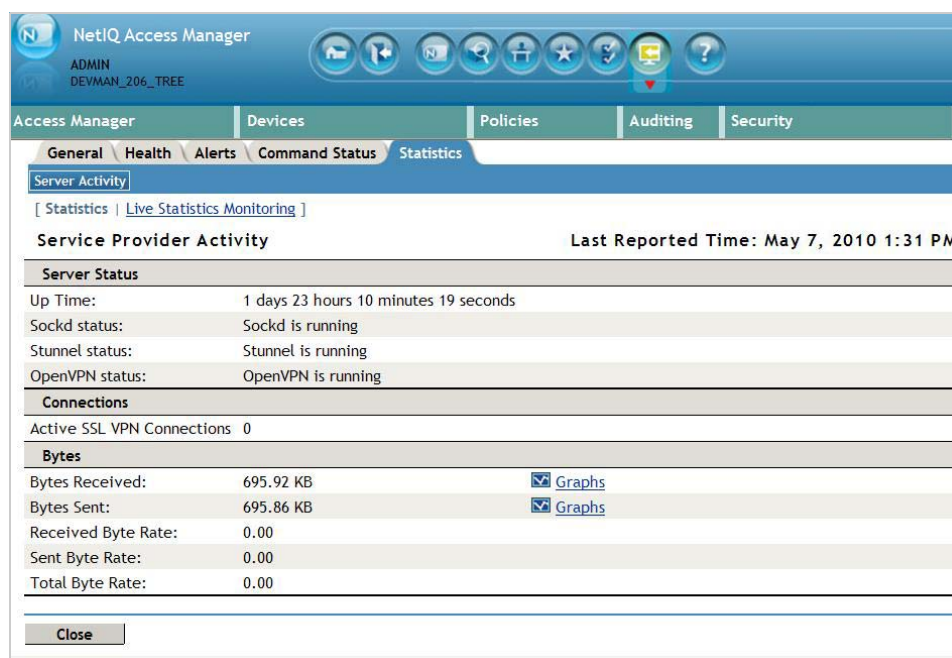
6.3 Viewing SSL VPN Statistics

The Statistics page allows you to view information such as the number of active client connections and the time when the SSL VPN server was started.

- ♦ [Section 6.3.1, “Viewing the SSL VPN Server Statistics,” on page 71](#)
- ♦ [Section 6.3.2, “Viewing SSL VPN Server Statistics for the Cluster,” on page 73](#)
- ♦ [Section 6.3.3, “Viewing the Bytes Graphs,” on page 73](#)

6.3.1 Viewing the SSL VPN Server Statistics

- 1 In the Administration Console, click *Devices > SSL VPNs > [Server Name] > Statistics*.



Server Status information is gathered in the following sections:

Column	Description
Up Time	Displays the duration for which the server has been up and running.
Sockd Status	Displays if the sockd is running or not.
Stunnel Status	Displays if the Stunnel is running or not.
OpenVPN Status	Displays if the OpenVPN is running or not.

Connection information is gathered in the following sections:

Column	Description
Active SSL VPN Connections	Displays the number of active SSL VPN connections. Also displays the username, role of the user, and uptime of each user for each active connection.

Bytes information is gathered in the following sections:

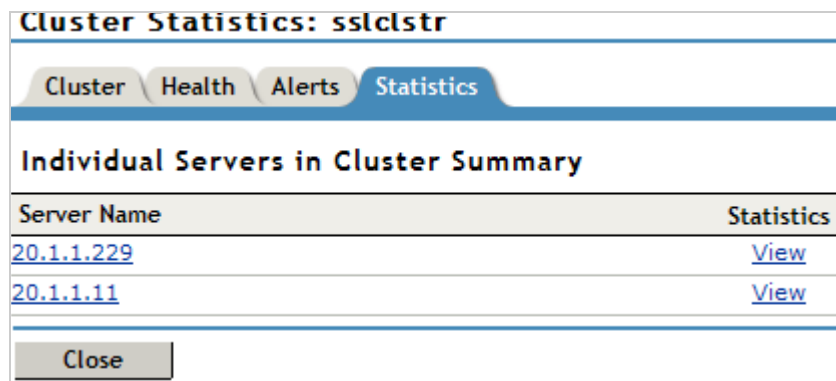
Column	Description
Bytes Received	Displays the number of bytes received. You can also view a graph, which lists the number of bytes sent for fixed intervals. For more information, see Section 6.3.3, "Viewing the Bytes Graphs," on page 73.

Column	Description
Bytes Sent	Displays the number of bytes sent. You can also view a graph, which lists the number of bytes sent for fixed intervals. For more information, see Section 6.3.3, “Viewing the Bytes Graphs,” on page 73.
Received Byte Rate	Displays the percentage of bytes received.
Sent Byte Rate	Displays the percentage of bytes sent.
Total Byte Rate	Displays the total percentage of bytes transferred.

- 2 Select one of the following options:
 - ♦ **Statistics:** To display the number of active client connections and the time when the server was started, click *Statistics*.
 - ♦ **Live Statistics Monitoring:** To refresh the statistics for a specified interval, click *Live Statistics Monitoring*. You can select the refresh interval from the *Refresh Rate* drop-down list.
- 3 Click *Close* to close the *Statistics* tab.

6.3.2 Viewing SSL VPN Server Statistics for the Cluster

- 1 In the Administration Console, click *Devices > SSL VPNs > [Cluster Name] > Statistics*.



- 2 The Statistics page has the following information:

Server Name: The IP address identifying the SSL VPNs in the cluster. Click the *Edit* link to edit server information.

Statistics: Click the *View* link to get a summary of the statistics of individual servers in a cluster. For more information on viewing the statistics details of individual servers, see [Section 6.3, “Viewing SSL VPN Statistics,”](#) on page 71.
- 3 Click *Close* to close the *Statistics* tab.

6.3.3 Viewing the Bytes Graphs

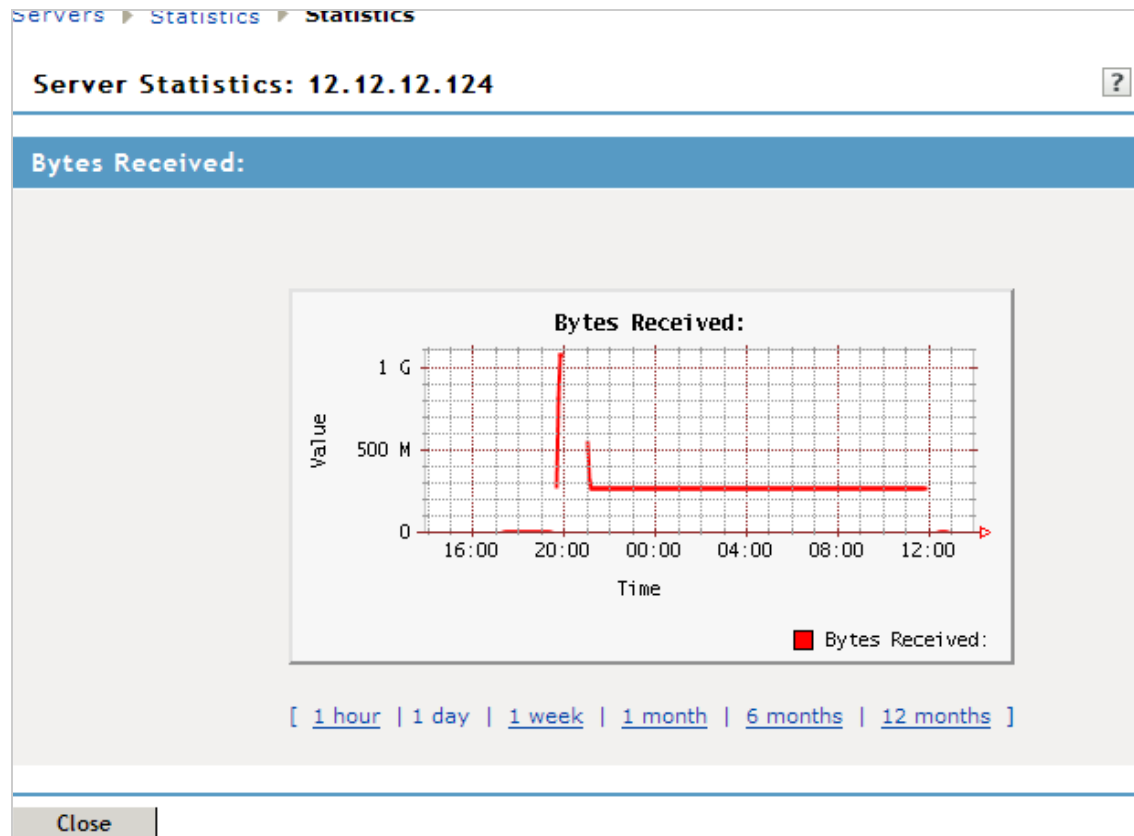
The number of bytes sent and bytes received can be viewed in the form of graphs. You can view graphs for the following time frames:

- ♦ **1 Hour:** The number of bytes sent or received every ten minutes.
- ♦ **1 Day:** The number of bytes sent or received every four hours.

- ♦ **1 Week:** The number of bytes sent or received every day.
- ♦ **1 Month:** The number of bytes sent or received every week.
- ♦ **6 Months:** The number of bytes sent or received every month for six months.
- ♦ **12 Months:** The number of bytes sent or received every month for one year.

To view graphs:

- 1 In the Administration Console, click *Devices > SSL VPNs > [Server Name] > Statistics*.
- 2 Select *Graphs* from either the *Bytes Received* or *Bytes Sent* section, depending on your needs.



- 3 Click *Close* to close the Graphs page.

6.4 Disconnecting Active SSL VPN Connections

You can use the Administration Console to disconnect users who are connected to the SSL VPN. You can disconnect one user at a time or select and delete multiple users.

- 1 In the Administration Console, click *Devices > SSL VPNs > [Server Name] > Statistics*.
The Server Statistics page is displayed.
- 2 Click *Live Statistics Monitoring*.



- 3 Select the users that you want to disconnect, then click *Disconnect*.
- 4 Click *OK* to confirm your action.

6.5 Monitoring the Health of SSL VPN Servers

You can monitor the health of an SSL VPN Server through the Health page, which displays the current status of the server.

- ♦ [Section 6.5.1, “Monitoring the Health of a Single Server,” on page 75](#)
- ♦ [Section 6.5.2, “Monitoring the Health of an SSL VPN Cluster,” on page 76](#)


6.5.1 Monitoring the Health of a Single Server

- 1 In the Administration Console, click *Devices* > *SSL VPNs* > *[Server Name]* > *Health*.





General Health Alerts Command Status Statistics

Refresh | Update from Server

Status Description

 Server is operational (Passed)

Services Detail

Type	Status	Message
Socks		(Passed) Socks Server is up and running.
Stunnel		(Passed) Stunnel Server is running properly
OpenVPN		(Passed) OpenVPN service is running properly
Servlet		(Passed) Servlet is running and registered with Connection Manager

Close

The *Status* column displays the current state, and the *Description* column explains the significance of the current state.

The *Services Details* section provides the following information:

Type: Displays the type of service.

Status: Displays the status of the service.




Message: Displays a description of the status of the service.

- 2 To reload the current page with the latest status, click *Refresh*.
- 3 To send a request to the agent to update its status information, click *Update from Server*. Click *OK* in the confirmation dialog box. This can take a few minutes.
- 4 To close the Health page, click *Close*.

6.5.2 Monitoring the Health of an SSL VPN Cluster

You can monitor the health of an SSL VPN Server through the Health page, which displays the current status of the server.

- 1 In the Administration Console, click *Devices > SSL VPNs > [Cluster Name] > Health*.







Servers		
Cluster Health: sslclstr		
Cluster Health Alerts Statistics		
Cluster Health 		
Server Name	Health	Description
20.1.1.11		Server is operational (Passed)
20.1.1.229		Server is operational (Passed)
Refresh Close		

The *Cluster Health* section displays the current state, and the *Description* column explains the significance of the current state.

The *Services Details* section provides the following information:

Server Name: Displays the name of the SSL VPN server in the cluster.

Health: Displays the health status of the server. The following health states are possible:

Icon	Description
	A green status indicates that the server has not detected any problems.
	A red status with a bar indicates that the server is stopped.
	A white status with disconnected bars indicates that the server is not communicating with the Administration Console.
	A yellow status indicates that the server might be functioning suboptimally because of configuration discrepancies.
	A yellow status with a question mark indicates that the server has not been configured.
	A red status with an x mark indicates that the server configuration might be incomplete or wrong, a dependent service might not be running or functional, or that the server is having a runtime error.

Click the icon to get the health status of individual servers.

Description: Displays a description of the status of the server.

- 2 To reload the current page with the latest status, click *Refresh*.
- 3 To send a request to the agent to update its status information, click *Update from Server*. Click *OK* in the confirmation dialog box. This can take a few minutes.
- 4 To close the Health page, click *Close*.

6.6 Viewing the Command Status of SSL VPN Server

Use the Command Status page to view the command status of the selected SSL VPN server.

- 1 In the Administration Console, click *Devices > SSL VPNs > [Server Name] > Command Status*.

servers ▾ Command Status					
SSL VPNs: 12.12.12.124					
<div>General</div> <div>Health</div> <div>Alerts</div> <div>Command Status</div> <div>Statistics</div>					
Delete Refresh					
<input type="checkbox"/>	Name	Status	Type	Admin	Date & Time (Note)
<input type="checkbox"/>	12.12.12.124 Configuration	SUCCEEDED	Device Configuration	cn=admin,o=novell	Jun 19, 2006 5:34 PM
<input type="checkbox"/>	12.12.12.124 Configuration	SUCCEEDED	Device Configuration	cn=admin,o=novell	Jun 19, 2006 5:19 PM
<input type="checkbox"/>	12.12.12.124 Configuration	SUCCEEDED	Device Configuration	cn=admin,o=novell	Jun 19, 2006 4:26 PM
<input type="checkbox"/>	12.12.12.124 Configuration	SUCCEEDED	Device Configuration	cn=admin,o=novell	Jun 19, 2006 3:43 PM
<input type="checkbox"/>	12.12.12.124 Configuration	SUCCEEDED	Device Configuration	cn=admin,o=novell	Jun 19, 2006 3:42 PM
<input type="checkbox"/>	12.12.12.124 Configuration	SUCCEEDED	Device Configuration	cn=admin,o=novell	Jun 19, 2006 3:41 PM
<input type="checkbox"/>	12.12.12.124 Start	SUCCEEDED	SSL VPN Start	cn=admin,o=novell	Jun 19, 2006 3:40 PM
<input type="checkbox"/>	12.12.12.124 Configuration	SUCCEEDED	Device Configuration	cn=admin,o=novell	Jun 19, 2006 3:40 PM
<input type="checkbox"/>	12.12.12.124 Start	SUCCEEDED	SSL VPN Start	cn=admin,o=novell	Jun 19, 2006 3:38 PM
<input type="checkbox"/>	12.12.12.124 Configuration	EXECUTING	Device Configuration	cn=admin,o=novell	Jun 19, 2006 3:28 PM

This page lists the command and the following information about the command:

Name: Contains the display name of the command. Click the link to view additional details about the command. For more information, see [Section 6.6, “Viewing the Command Status of SSL VPN Server,”](#) on page 77.

Status: Displays the status of the command. Some of the possible states include *Pending*, *Incomplete*, *Executing*, and *Succeeded*.

Type: Displays the type of command.

Admin: Indicates if the system or a user issued the command. If a user issued the command, the DN of the user is displayed.

Date & Time: Displays the local date and time the command was issued.

- 2 To delete a command, select the check box for the command, then click *Delete*. The selected command is cleared.
- 3 To update the current cache of recently executed commands, click *Refresh*.
- 4 Click *Close* to close the Command Status page.

6.6.1 Viewing Command Information

To view configuration of individual commands:

- 1 In the Administration Console, click *Devices > SSL VPNs > [Server Name] > Command Status > [Individual Command]*. The command status page is displayed.
- 2 Click the command to get a detailed information on the command.

Servers ▸ **Server Scheduled Command**

Server Details Edit: Server Configuration Scheduled Command

Note: Date and time entries are specified in local time.

Command Information	
Delete Refresh	
Name:	12.12.12.124 Configuration
Type:	Device Configuration
Admin:	cn=admin,o=novell
Description:	12.12.12.124 Configuration
Status:	SUCCEEDED
Last Executed On:	Jun 19, 2006 5:34 PM
Aggregate Command Result:	Success

Command Execution Details	
Command	Command Result
Cancel	

You can perform the following actions:

Delete: To delete a command, click *Delete*. Click *OK* in the confirmation dialog box.

Refresh: To update the current cache of recently executed commands, click *Refresh*.

- 3 Click *Close* to return to the command status page.

6.7 Monitoring SSL VPN Alerts

The Alerts page allows you to view information about current system alerts and to clear the alerts. An alert is generated whenever the SSL VPN Gateway detects a condition that prevents it from performing normal system services.

- ♦ [Section 6.7.1, “Configuring SSL VPN Alerts,” on page 79](#)
- ♦ [Section 6.7.2, “Viewing SSL VPN Alerts,” on page 80](#)
- ♦ [Section 6.7.3, “Viewing SSL VPN Cluster Alerts,” on page 81](#)

6.7.1 Configuring SSL VPN Alerts

- 1 In the Administration Console, click *Devices* > *SSL VPNs* > *[Server Name]* > *Alert Settings*.

Alerts	
<input type="checkbox"/> Select All	
<input type="checkbox"/> SSL VPN Gateway UP	<input type="checkbox"/> SSL VPN Gateway DOWN
<input type="checkbox"/> Concurrent Connections Reached 200	<input type="checkbox"/> Concurrent Connections Reached Maximum Limit (249)
<input type="checkbox"/> Invalid Configuration	<input type="checkbox"/> Invalid Certificate
<input type="checkbox"/> Webserver Servlet Down	<input type="checkbox"/> Application SSL Encryptor Down
<input type="checkbox"/> Socks Protocol Daemon Down	<input type="checkbox"/> Cluster Alerts
<p>Server(s) must be updated before changes made on this panel will be used. See Configuration Panel for summary of changes.</p>	
OK	Cancel

- 2 Select the *Select All* option to send alerts for all the events, or select one or more of the following:

Alert	Description
SSL VPN Gateway up	Sends an alert when the SSL VPN server is up and running.
SSL VPN Gateway down	Sends an alert when the SSL VPN server is down and is not functional.
Concurrent connections reached 200	Sends an alert when the number of concurrent connection reaches 200. The maximum is 249.
Concurrent connections reached maximum limit (249)	Sends an alert when the number of concurrent connections reaches 249.
Invalid configuration	Sends an alert when the configuration is not valid.
Invalid certificate	Sends an alert when the SSL VPN certificate used for encryption and communication is invalid.
Web Server servlet down	Sends an alert whenever a Web Server servlet is down.
Application SSL encryptor down	Sends an alert whenever the SSL encryptor is down.
Socks Protocol Daemon down	Sends an alert whenever the socket protocol daemon is down.
Cluster Alerts	Sends alerts whenever the cluster node is up, down, or restarted.

6.7.2 Viewing SSL VPN Alerts

- 1 In the Administration Console, click *Devices > SSL VPNs > [Server Name] > Health*.

Servers ▸ Alerts		
Server Alert Detail: 10.10.12.123		
General Health Alerts Command Status Statistics		
Acknowledge Alert(s)		
<input type="checkbox"/> Severity	Date & Time	Message
<input type="checkbox"/> Information	Aug 16, 2006 3:09 PM	SSLVPN Servlet is registered
<input type="checkbox"/> Information	Aug 16, 2006 5:46 PM	VCC Started
<input type="checkbox"/> Information	Aug 16, 2006 5:47 PM	SSLVPN Servlet is registered
<input type="checkbox"/> Information	Aug 17, 2006 4:19 PM	VCC Started
<input type="checkbox"/> Information	Aug 17, 2006 4:20 PM	SSLVPN Servlet is registered
<input type="checkbox"/> Information	Aug 17, 2006 6:27 PM	VCC Started
<input type="checkbox"/> Information	Aug 17, 2006 6:28 PM	SSLVPN Servlet is registered
<input type="checkbox"/> Information	Aug 18, 2006 2:43 PM	SSLVPN Servlet is registered
<input type="checkbox"/> Information	Aug 21, 2006 4:44 PM	SSLVPN Servlet is registered
<input type="checkbox"/> Information	Aug 21, 2006 5:29 PM	SSLVPN Servlet is registered
Close		

The following information is displayed:

Severity: Describes the type of alert. An alert can be informational, critical, or a warning.

Date & Time: Indicates the date and time when an alert was issued. The date and time are given in the local time.

Message: Displays the message that was sent with the alert. This information is optional.

- 2 To send an acknowledgement, select the check box next to the alert, then click *Acknowledge Alert(s)*. When you acknowledge an alert, the alert is cleared from the list.
- 3 Click *Close* to close the Alerts page.

6.7.3 Viewing SSL VPN Cluster Alerts

To view information about current alerts for all members of a cluster:

- 1 In the Administration Console, click *Devices > SSL VPNs > [Name of Cluster] > Alerts*.

Cluster Health Alerts Statistics				
<input type="checkbox"/>	Server Name	Severe	Warning	Information
<input type="checkbox"/>	10.10.16.140	2	2	0
<input type="checkbox"/>	10.10.16.141	2	4	0
Acknowledge Alert(s)				

- 2 Analyze the data that is displayed.

Column	Description
Server Name	Lists the name of the SSL VPN server that sent the alert. To view additional information about the alerts for a specific SSL VPN, click the specific SSL VPN.
Severe	Lists the number of critical alerts that have been sent and not acknowledged.
Warning	Lists the number of warning alerts that have been sent and not acknowledged.
Information	Lists the number of informational alerts that have been sent and not acknowledged.

- 3 To acknowledge all alerts for an SSL VPN server, select the check box next to the SSL VPN server, then click *Acknowledge Alert(s)*. When you acknowledge an alert, you clear the alert from the list.
- 4 To view information about a particular alert, click the server name.

7 Additional Configurations

The following sections describe additional configurations for the SSL VPN server:

- ♦ [Section 7.1, “Customizing SSL VPN User Interface,” on page 83](#)
- ♦ [Section 7.2, “Creating DH Certificates with Different Key Sizes,” on page 84](#)
- ♦ [Section 7.3, “Creating a Configuration File to Add Additional Configuration Changes,” on page 84](#)

7.1 Customizing SSL VPN User Interface

You can customize the contents of the SSL VPN home page, the exit page, and the error messages, depending on your organization’s requirements.

- ♦ [Section 7.1.1, “Customizing the Home Page and Exit Page,” on page 83](#)
- ♦ [Section 7.1.2, “Customizing Error Messages,” on page 83](#)

7.1.1 Customizing the Home Page and Exit Page

To customize the home page, modify the `/var/opt/novell/tomcat7/webapps/sslvpn/sslvpnclient.jsp` file.

The home page content is displayed within the `<div id="homecontent">` tags.

To customize the Exit page, modify the `/var/opt/novell/tomcat7/webapps/sslvpn/logout.jsp` file.

7.1.2 Customizing Error Messages

To customize the error messages:

- 1 Browse and open the following file:
`/var/opt/novell/tomcat7/webapps/sslvpn/Applet/properties/BrowserAgentMessages.properties`
- 2 Edit the file to modify existing error messages and to add new messages as necessary.
- 3 Save and close the file.

7.2 Creating DH Certificates with Different Key Sizes

The Enterprise mode of the SSL VPN uses DH certificates for encryption. These certificates are created automatically during the installation or upgrade, with a default key size of 1024. You can create DH certificates with key sizes of your choice up to a maximum key size of 4096.

To create a DH certificate with a key size of your choice, enter the following command:

```
sslvpn -k <keysize>
```

Replace <keysize> with the key size of your choice.

7.3 Creating a Configuration File to Add Additional Configuration Changes

You can use a configuration file to create and execute many extended configuration options for both the SSL VPN Enterprise client and the Enterprise server.

- 1 Browse to `/etc/opt/novell/sslvpn`.
- 2 Open the following files, depending on the changes you want to make:
 - ♦ Open `openvpn-client.conf` if you want to push configuration changes to the Enterprise mode client.
 - ♦ Open `openvpn-server.conf.tpl` if you want to push configuration changes to the Enterprise server.
- 3 Add the commands for additional OpenVPN configuration to these files. For example, to decrease the MTU size of the TUN interface, specify the command in the following format in both files:

```
link-mtu 1200
```
- 4 Save your changes.
- 5 Restart the server.

8 Server Configuration Settings

This section describes the configuration settings that affect SSL VPN servers.

- ♦ [Section 8.1, “Managing SSL VPN Servers,” on page 85](#)
- ♦ [Section 8.2, “Configuring SSL VPN Servers,” on page 87](#)
- ♦ [Section 8.3, “Modifying SSL VPN Server Details,” on page 88](#)

8.1 Managing SSL VPN Servers

Use the Servers page to view the status of SSL VPN servers, to modify their configuration, to create or delete clusters, or to stop and start the server.

1 In the Administration Console, click *Devices > SSLVPNs*.

2 Select one of the following options:

New Cluster: Displays the New Cluster dialog box, where you can specify a name for your SSL VPN configuration and assign an Identity Server. When you click *OK*, the system displays the Create Cluster Configuration page, which lets you configure how your Identity Servers operate in an Access Manager Appliance configuration.

Stop: To stop the SSL VPN server so that the power can be turned off, select the SSL VPN Server, then click *Stop*.

Start: To start the SSL VPN server, select the SSL VPN server, then click *Start*.

Refresh: Use this option to update the list of servers and their health status.

3 To perform an action available in the *Actions* drop-down menu, select an SSL VPN server, then select one of the following:

Assign to Cluster: To add the selected SSL VPN server to a cluster, select *Assign to Cluster*, then select the cluster. This SSL VPN is reconfigured with the configuration of the primary cluster server.

Remove from Cluster: To remove the selected SSL VPN server from a cluster, select *Remove from Cluster*. The SSL VPN server retains its configuration from the cluster, but no traffic is sent to it until it is reconfigured. You can assign it to a different cluster and have it updated with the new cluster’s configuration, or you can delete all of its reverse proxies and start a new configuration.

Delete: To remove the selected SSL VPN server from the list of servers that can be managed from this Administration Console, select *Delete*. If the SSL VPN server is a member of a cluster, you must first remove it from the cluster before you can delete it.

IMPORTANT: When an SSL VPN server is deleted from the Administration Console, you can no longer manage it. To access it again, you must manually trigger an auto-import, which causes it to import into an Administration Console.

Update Health from Server: Click this action to send a request to the server for updated health information. If you have selected multiple servers, a request is sent to each one. The health status changes to an animated circle until the reply returns.

Service Provider: Select one of the following actions:

- ♦ **Start Service Provider:** To start the Embedded Service Provider associated with the selected SSL VPN, click *Start Service Provider*. The Embedded Service Provider is the module within the SSL VPN that communicates with the Identity Server.

The Embedded Service Provider should be restarted whenever you enable or modify logging on the Identity Server.

- ♦ **Stop Service Provider:** To stop the Embedded Service Provider associated with the selected SSL VPN, click *Stop Service Provider*. The Embedded Service Provider is the module within the SSL VPN that communicates with the Identity Server.

When an SSL VPN is not functioning correctly, you should always try stopping and starting the service provider before stopping and starting the SSL VPN.

- ♦ **Restart Service Provider:** To restart the Embedded Service Provider associated with the selected SSL VPN, click *Restart Service Provider*. This command stops the Embedded Service Provider and then starts it. The Embedded Service Provider is the module within the ESP-enabled SSL VPN that communicates with the Identity Server.

When an Access Gateway is not functioning correctly, you should always try restarting the Embedded Service Provider before stopping and starting the Access Gateway.

4 Use the following links to manage a cluster or an SSL VPN server:

Name: Displays a list of servers that can be managed from this administration console. This also displays the name of the cluster, if you have configured one. Click the link of a particular server to view or modify its configuration. For more information, see [Viewing and Editing SSL VPN Server Details](#).

Status: Indicates the configuration status of the SSL VPN server. Possible states are pending, update, and current.

- ♦ *Current* indicates that all configuration changes have been applied.
- ♦ *Update* indicates that a configuration change has been made, but not applied. Click this link to apply the changes.
- ♦ *Pending* indicates that the server is processing a configuration change, but has not completed the process.

Health: Indicates the health of the SSL VPN server. Click the icon to view additional information about the functional status of an SSL VPN server.

Alerts: Indicates whether any alerts have been sent. Click the link to view additional information about alerts. This option is not available to you if the alert count is 0. For more information, see [Viewing SSL VPN Alerts](#).

Commands: Indicates the status of commands issued to servers. For more information, see [Viewing the Command Status of SSL VPN Server](#).

Statistics: Indicates the number of active client connections and the time when the Gateway was started. Click *View* to get the statistics information. For more information, see [Viewing the SSL VPN Server Statistics](#).

Type: Indicates the type of SSL VPN that is installed. This section indicates whether the SSL VPN server installed is an SSL VPN protected by the Access Gateway or if it is a standalone SSL VPN. It also indicates if the SSL VPN version is high-bandwidth or low-bandwidth. For example, if the high-bandwidth version of SSL VPN protected by the Access Gateway is installed, then the *Type* displayed is *High (non-ESP)*.

Configuration: Indicates the date and time when the last modification was made. It also indicates the fully distinguished name of the user who made the last modification. Click *Edit* to view and modify the SSL VPN configuration. For more information, see [Configuring SSL VPN Servers](#).

8.2 Configuring SSL VPN Servers

The Configuration page allows you to view the configuration status and to configure the features of a cluster or a single SSL VPN server.

All configuration changes are applied from the SSL VPNs page. The links from this page allow you to accept or cancel any changes, but the changes are not sent to the SSL VPN server from the other pages.

- 1 In the Administration Console, *Devices > SSLVPNs > Edit*.

To edit an SSL VPN server that is not a member of a cluster, click the *Edit* button next to the server that you want to edit.

To edit the configuration of a cluster, click the *Edit* button next to the cluster.

The Server configuration page is displayed with the following information:

Services: A list of the services available for configuration.

Last Changed: The date and time the service was last modified.

Change By: The distinguished name of the user who made the last modification.

- 2 Select one of the following configuration options:

- ♦ The Gateway configuration section allows you to configure the SSL VPN gateway and DNS server list information. You can select one of the following options:

Basic Configuration: Allows you to configure the gateway. For more information, see [Configuring the IP Address, Port, and Network Address Translation](#).

Advanced Configuration: Allows you to configure SNAT entries for the SSL VPN server. For more information, see [Configuring Route and Source NAT for Enterprise Mode](#).

DNS Servers List: Allows you to configure the DNS server list. For more information, see [Configuring DNS Servers](#).

- ♦ The policies section allows you to configure policies that determine the resources a client can access, depending on the role and the security measures adhered to by the client.

Client Integrity Check Policies: Allows you to configure the client integrity check policies. For more information, see [Configuring Policies to Check the Integrity of the Client Machine](#).

Client Security Levels: Allows you to configure different security levels for different client roles. For more information see [Client Security Levels](#).

Traffic Policies: Allows you to configure traffic policies. For more information, see [Configuring Traffic Policies](#).

Client policies: Allows you to configure policies that determine if clients should access SSL VPN in Kiosk mode only, or in Enterprise mode only, or if the mode selection can be done by the clients. For more information, see [Configuring Full Tunneling](#).

- ♦ The Novell Audit and Alerts section allows you to set up alerts so that notifications are sent when specified events occur.

Novell Audit Settings: Allows you to configure Novell Audit settings. For more information, see [Enabling SSL VPN Audit Events](#).

Alerts Settings: Allows you to configure alerts settings. For more information, see [Configuring SSL VPN Alerts](#).

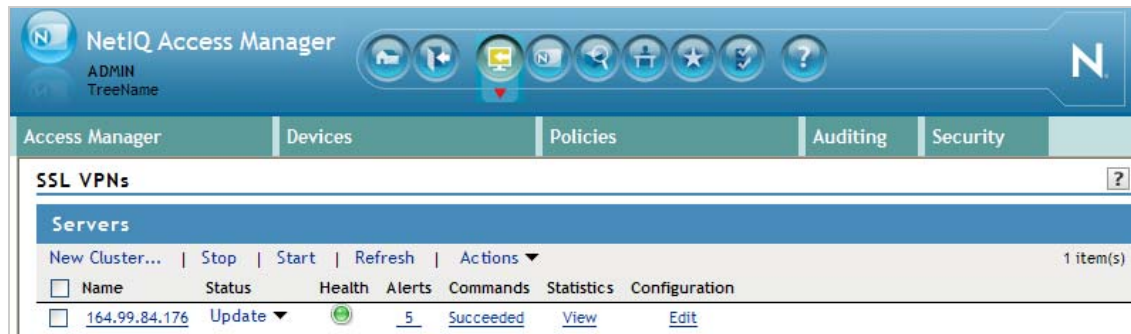
- ♦ The security settings section allows you to view and modify the current security configuration for the SSL VPN server.

SSL VPN Certificates: Allows you to configure certificate details for SSL VPN. For more information, see [Configuring Certificate Settings](#).

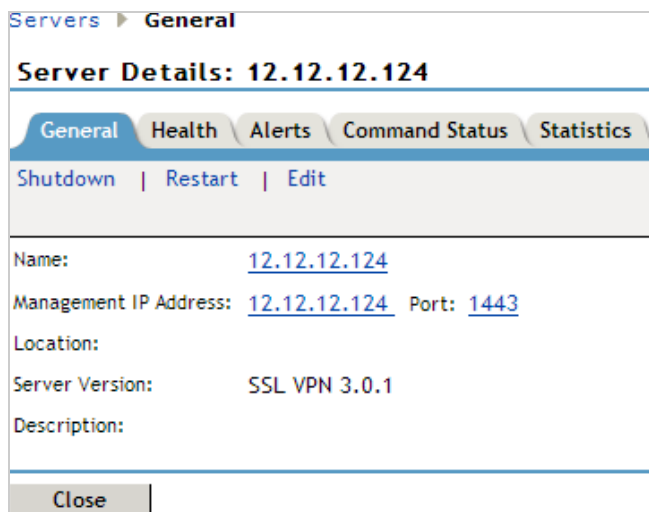
- 3 To apply and save changes, select one of the following actions:
 - ♦ **OK:** To save all the configuration changes that have been made, click *OK*. When you leave this page, the changes are accepted and the SSL VPN server is scheduled for an update.
 - ♦ **Cancel:** To close without saving any pending changes, click *Cancel*, then click *OK* at the confirmation dialog box.
 - ♦ **Revert:** To cancel configuration changes that you have already accepted and return to the previous configuration, click *Revert*.

8.3 Modifying SSL VPN Server Details

- 1 In the Administration Console, click *Devices* > *SSL VPNs*.



- 2 Click the server.



The *General* tab of the Server Details page displays information such as name, management IP address, port, location, and the server version of the selected server.

- 3 Click *Edit*.

Servers > General > Edit

Server Details Edit: 12.12.12.123

Name: 12.12.12.123

Management IP Address: 12.12.12.123 Port: 1443

Location:

Description:

OK Cancel

- 4 Verify the information and make any necessary changes.

Name: Specify the IP address of the server. This field is mandatory.

Management IP Address: Specify the IP address used to manage the server. If the system on which the agent is installed has multiple IP addresses, you can select one from the drop-down list.

Port: Specify the port used for management. This field is mandatory.

Description: (Optional) Provide a brief description of the purpose of this SSL VPN Gateway or any other relevant information.

- 5 Click *OK* to save changes or click *Cancel* to discard the changes.

A Troubleshooting SSL VPN Configuration

You might sometimes encounter issues while installing or configuring the SSL VPN servers. The SSL VPN server might not work the way you intended because of problems encountered during installation or configuration. The following sections list some of the scenarios that you might encounter and the steps to troubleshoot such issues:

This section provides various troubleshooting scenarios that you might encounter while configuring SSL VPN.

- ♦ [Section A.1, “Successfully Connecting to the Server,” on page 92](#)
- ♦ [Section A.2, “The SSL VPN Server Is in a Pending State,” on page 93](#)
- ♦ [Section A.3, “SSL VPN Connects in Kiosk Mode, But There Is No Data Transfer,” on page 94](#)
- ♦ [Section A.4, “The TFTP Application and GroupWise Notify Do Not Work in Enterprise Mode,” on page 94](#)
- ♦ [Section A.5, “SSL VPN Does Not Report,” on page 94](#)
- ♦ [Section A.6, “Verifying SSL VPN Components,” on page 95](#)
- ♦ [Section A.7, “Unable to Contact the SSL VPN Server,” on page 96](#)
- ♦ [Section A.8, “Unable to Get Authentication Headers,” on page 96](#)
- ♦ [Section A.9, “The SSL VPN Connection Is Successful But There Is No Data Transfer,” on page 96](#)
- ♦ [Section A.10, “Unable to Connect to SSL VPN Gateway,” on page 97](#)
- ♦ [Section A.11, “Multiple Instances of SSL VPN Are Running,” on page 97](#)
- ♦ [Section A.12, “Issue with the Preinstalled Enterprise Mode Client,” on page 97](#)
- ♦ [Section A.13, “Socket Exception Error After Upgrading SSL VPN,” on page 97](#)
- ♦ [Section A.14, “SSL VPN Server Is Unable to Handle the Session,” on page 98](#)
- ♦ [Section A.15, “Embedded Service Provider Status Is Red,” on page 98](#)
- ♦ [Section A.16, “Connection Manager Log Does Not Display the Client IP Address,” on page 98](#)
- ♦ [Section A.17, “SSL VPN Full Tunnel Connection Disconnects on VMware,” on page 98](#)
- ♦ [Section A.18, “Clustering Issues,” on page 98](#)
- ♦ [Section A.19, “On Windows XP and 7, Loading ActiveX Takes More than Three Minutes to Connect to SSL VPN,” on page 99](#)
- ♦ [Section A.20, “If There Is An Install Log Error, SSL VPN Client In Kiosk Mode Fails To Start,” on page 100](#)

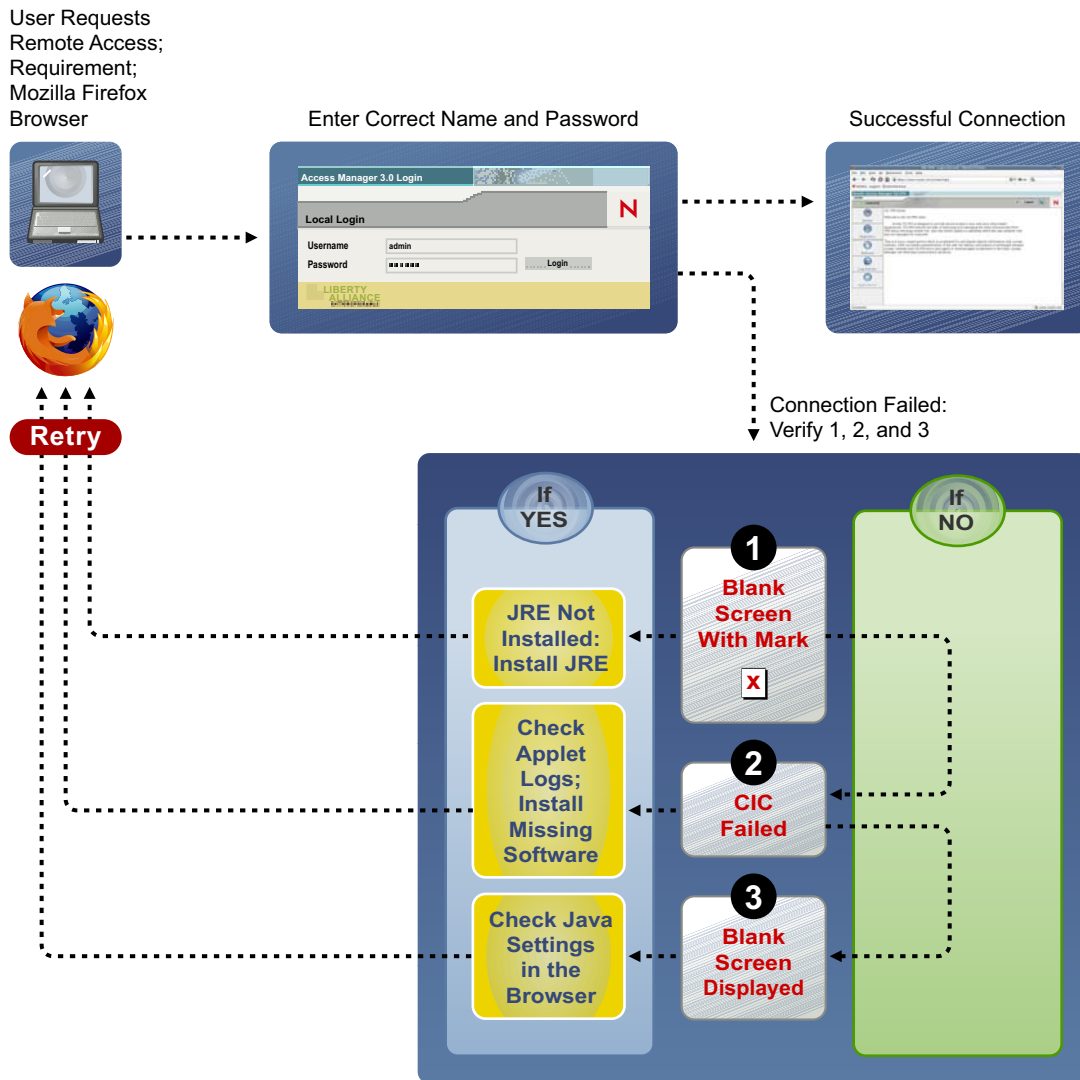
A.1 Successfully Connecting to the Server

You can access the protected resources that are using SSL VPN by authenticating to the proxy server. The proxy server loads the SSL VPN client on your browser. The following sections describe some of the problems that clients might encounter:

- ♦ [“Connection Problems with Mozilla Firefox” on page 92](#)
- ♦ [“Connection Problems with Internet Explorer” on page 93](#)

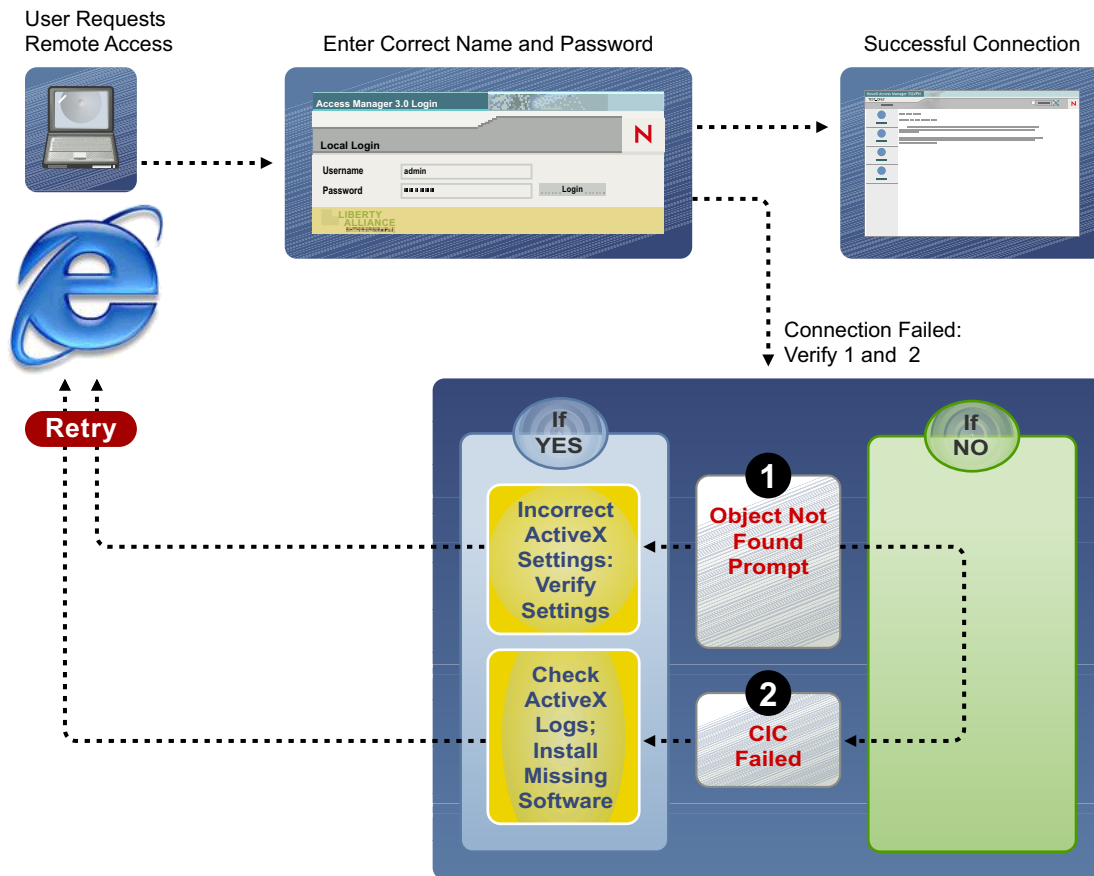
A.1.1 Connection Problems with Mozilla Firefox

Figure A-1 Using Mozilla Firefox to Connect to the SSL VPN Server



A.1.2 Connection Problems with Internet Explorer

Figure A-2 Using Internet Explorer to Connect to the SSL VPN Server



A.2 The SSL VPN Server Is in a Pending State

The SSL VPN server sometimes gets into a pending state even when all of its commands have been successful.

To work around this problem:

- 1 In the Administration Console, click *Devices > SSL VPNs*.
- 2 Click the *Commands* link.
- 3 Select all the pending commands, then click *Delete > Close*.
- 4 If the device is still in a pending state, click *Auditing > Troubleshooting*.
- 5 In the *Device Pending with No Commands* section, select the SSL VPN server and remove the pending state.

A.3 SSL VPN Connects in Kiosk Mode, But There Is No Data Transfer

If the user successfully gets connected in the Kiosk mode but the data transfer does not happen, verify if the user is configured to connect through a forward proxy. Then verify that the entries in the `proxy.conf` file are correct. For more information, see [Chapter 4.3, “Configuring SSL VPN to Connect through a Forward Proxy,” on page 53](#).

A.4 The TFTP Application and GroupWise Notify Do Not Work in Enterprise Mode

If the TFTP application and GroupWise® Notify do not work in the Enterprise mode, make sure you have done the following:

- ♦ You have configured a route using the default gateway. For more information, see [Section 2.2, “Configuring Route and Source NAT for Enterprise Mode,” on page 26](#).
- ♦ You are not using source NAT to route packets.

A.5 SSL VPN Does Not Report

If the SSL VPN is not reporting, you must verify the status of JCC and the SSL VPN and restart them if they are down. If restarting any of these components does not work, reconfigure the SSL VPN. If none of these work, you must delete and reimport the SSL VPN server.

- ♦ [Section A.5.1, “Verifying and Restarting JCC,” on page 94](#)
- ♦ [Section A.5.2, “Verifying and Restarting the SSL VPN Server,” on page 94](#)

A.5.1 Verifying and Restarting JCC

To check the status of JCC, enter the following command:

```
/etc/init.d/novell-jcc status
```

```
OR rcnovell-jcc status
```

If it is not running, enter the following command to restart JCC:

```
/etc/init.d/novell-jcc restart
```

```
OR rcnovell-jcc restart
```

A.5.2 Verifying and Restarting the SSL VPN Server

To verify the status of the SSL VPN server, enter the following command:

```
/etc/init.d/novell-sslvpn status
```

```
OR rcnovell-sslvpn status
```

If any component is down, stop and start the SSL VPN server by using the following commands:

```
novell-sslvpn stop
novell-sslvpn start
```

A.6 Verifying SSL VPN Components

Use the commands and processes described in the following sections to verify that the SSL VPN components are running:

- ♦ [Section A.6.1, “SSL VPN Server,” on page 95](#)
- ♦ [Section A.6.2, “SSL VPN Linux Client,” on page 95](#)
- ♦ [Section A.6.3, “SSL VPN Macintosh Client,” on page 95](#)
- ♦ [Section A.6.4, “SSL VPN Windows Client,” on page 96](#)

A.6.1 SSL VPN Server

To verify the status of the SSL VPN components, use the commands listed in the table below:

Component	Command
Connection Manager	<code>pgrep connman</code>
Sock Daemon	<code>pgrep sockd</code>
Secure Tunnel	<code>pgrep stunnel</code>
OpenVPN	<code>pgrep openvpn</code>

A.6.2 SSL VPN Linux Client

Component	Command
Policy Resolver for Kiosk mode	<code>pgrep polresolver</code>
Secure Tunnel for Kiosk mode	<code>pgrep stunnel</code>
OpenVPN for Enterprise mode	<code>pgrep openvpn</code>

A.6.3 SSL VPN Macintosh Client

Component	Command
Policy Resolver for Kiosk mode	<code>ps -A grep polresolver grep -v grep</code>
Secure Tunnel for Kiosk mode	<code>ps -A grep stunnel grep -v grep</code>
OpenVPN for Enterprise mode	<code>ps -A grep openvpn grep -v grep</code>

A.6.4 SSL VPN Windows Client

Check to see if the stunnel and polresolver processes are up and running if SSL VPN is in Kiosk mode, and check openVPN if SSL VPN is in Enterprise mode.

A.7 Unable to Contact the SSL VPN Server

In the client browser, verify the following if you encounter any of these messages:

SSLVPN Gateway is in bad state

SSLVPN Gateway is not available:

- ♦ **Error Status:** Check the status at `/var/log/messages`, `/var/log/stunnel.log`, and `/var/log/novell-openvpn.log`.
- ♦ **SSL VPN Status:** At the command prompt, enter the following command:
`/etc/init.d/novell-sslvpn status`
Usage: novell-sslvpn {start | stop | restart}
- ♦ **Message Log:** Check the `/var/log/messages` file for more information.

A.8 Unable to Get Authentication Headers

If the browser displays the Unable to Get Authentication Headers error while accessing the SSL VPN URL, check whether the custom HTTP headers required for SSL VPN are configured and enabled in the Access Gateway. In the Administration Console, click *Access Gateways* > *[Configuration Link]* > *[Name of Reverse Proxy]* > *[Name of SSL VPN Proxy Service]* > *[Name of SSL VPN Protected Resource]* > *Identity Injection*.

The SSLVPN_Default policy should be enabled. This policy injects an authentication header and two custom headers (X-SSLVPN-PROXY-SESSION-COOKIE and X-SSLVPN-ROLE).

A.9 The SSL VPN Connection Is Successful But There Is No Data Transfer

Possible Cause: This issue might occur in both Kiosk and Enterprise modes of the SSL VPN. If the SSL VPN server is behind a NAT, the public IP address specified during server configuration might be incorrect.

Action: In the Administration Console, click *Devices* > *SSL VPNs* > *Edit* > *Gateway Configuration*. Make sure that the Public IP address is configured to be the IP address of a NAT through which the external user on the Internet can access the SSL VPN server.

Possible Cause: If this issue appears in the Enterprise mode, it could be because the NAT configuration is wrong.

Action: At the command prompt, enter `iptables -L` to check the configuration details. For more information, see [Section 2.1, “Configuring the IP Address, Port, and Network Address Translation,” on page 21](#).

Possible Cause: If this issue appears in the Enterprise mode, it could be because the router configuration is wrong.

Action: Check the router configuration. For more information, see [Section 2.1, “Configuring the IP Address, Port, and Network Address Translation,” on page 21.](#)

Possible Cause: If this issue appears in the Enterprise mode, the TUN interface might be down.

Action: At the command prompt, enter `ifconfig` to check if the TUN0 interface is down. If it is down, enter the `etc/init.d/novell-sslvpn restart` OR `rcnovell-sslvpn restart` command to restart the SSL VPN services.

Action: If you are using a 64-bit machine and have changed the TUN interface, check to make sure the interface is up. If it is down, enter the `etc/init.d/novell-sslvpn restart` OR `rcnovell-sslvpn restart` command to restart the SSL VPN services.

A.10 Unable to Connect to SSL VPN Gateway

Possible Cause: A forward proxy is enabled in Internet Explorer.

Action: In the Administration Console, select *Devices > Access Gateways > Edit > Reverse Proxy > Proxy List > Path-Based Multi-Homing > HTTP Options*. Select the *Allow Pages to Be Cached by the Browser* check box.

A.11 Multiple Instances of SSL VPN Are Running

If you get this error while trying to connect to the SSL VPN, it could be because there was an improper logout in the previous session and some of the processes did not close properly. Verify if any of the SSL VPN processes are running. For more information on how to verify this, see [Section A.6, “Verifying SSL VPN Components,” on page 95.](#)

When this error occurs, manually kill the process if you are an admin or a root user of the machine. If you are a non-admin or non-root user of the machine, restart the machine.

A.12 Issue with the Preinstalled Enterprise Mode Client

If you preinstalled the Enterprise mode client for a non-admin or a non-root user of the machine, the user should be connected to the SSL VPN without being prompted to enter the credentials of the admin user. If the user is still prompted to specify the credentials of the admin user, make sure the SSL VPN service is running. For more information on how to check the SSL VPN service, see [Section A.6, “Verifying SSL VPN Components,” on page 95.](#)

A.13 Socket Exception Error After Upgrading SSL VPN

You might randomly get a socket exception error after upgrading the ESP-enabled SSL VPN cluster if the SSL certificate is configured in the HTTPS mode. You are getting this error because the SSL VPN certificate is missing from the keystore. To work around this problem, you must reinstall the SSL VPN server and configure a new SSL certificate.

A.14 SSL VPN Server Is Unable to Handle the Session

If the SSL VPN server failed because of SSL VPN component failure and you restarted the server by using the `novell-sslvpn start` command, the server cannot handle the subsequent sessions. To work around this issue, restart Tomcat by using the `novell-sslvpn restart` command.

A.15 Embedded Service Provider Status Is Red

If the status of the Embedded Service Provider is red or if the Embedded Service Provider does not start after installation, restart Tomcat by entering the following command:

```
novell-sslvpn restart
```

A.16 Connection Manager Log Does Not Display the Client IP Address

When the ESP-enabled SSL VPN is installed, you might see `UNKNOWN HOST` displayed in the Connection Manager logs instead of the IP address of the client. This is because this information is provided by the Access Gateway and is available only if the Traditional NetIQ SSL VPN server is deployed.

A.17 SSL VPN Full Tunnel Connection Disconnects on VMware

Possible Cause: An SSL VPN full tunnel connection might disconnect because of no keepalive response if the Access Manager Appliance setup is on a host-only network, on a VMware interface of the client.

Explanation: After full tunnel is enabled, a new route entry is added to the client routing table to route the keepalive packet to the SSL VPN server through the default gateway. Because the SSL VPN gateway is on a host-only network on a VMware, the keepalive packet might not reach the SSL VPN server through the default gateway.

Action:

- 1 Add a virtual address to the SSL VPN gateway.
For example, if the primary address is 200.200.200.140, add 200.200.200.141.
- 2 Disconnect the physical network from the client to make sure that there is no default gateway to the Internet.
- 3 Manually add a default route.
For example, `route add 0.0.0.0 mask 0.0.0.0 200.200.200.141 metric 5`.

A.18 Clustering Issues

- [Section A.18.1, “Bringing Up the Server If a Cluster Member Is Down,” on page 99](#)
- [Section A.18.2, “Bringing Up a Binary If It Is Down,” on page 99](#)
- [Section A.18.3, “Debugging a Cluster If Session Sharing Doesn’t Properly Happen,” on page 99](#)

A.18.1 Bringing Up the Server If a Cluster Member Is Down

Action: Check the Administration Console for the component that is down in the cluster member. If the component is `openvpn`, `stunnel`, or `sockd`, restart SSL VPN by using the following command:

```
/etc/init.d/novell-sslvpn restart
```

OR `rcnovell-sslvpn restart`

You can check for the status by using the following command:

```
/etc/init.d/novell-sslvpn status
```

OR `rcnovell-sslvpn status`

A.18.2 Bringing Up a Binary If It Is Down

Action: If the `openvpn`, `stunnel`, or `sockd` binaries are not running:

- 1 Stop the server by using the following command:

```
/etc/init.d/novell-sslvpn stop
```

OR `rcnovell-sslvpn stop`

- 2 Use the `ps` command to check whether the `openvpn`, `stunnel`, and `sockd` binaries are still running.

If the binaries are running, kill the processes and start the server.

- 3 Restart Tomcat if it is not responding.
- 4 Check the status of the SSL VPN server.

A.18.3 Debugging a Cluster If Session Sharing Doesn't Properly Happen

Action: Check the connectivity among the cluster members by using the following command:

```
netstat -anp | grep 8900
```

Restart Tomcat on all of the machines if each cluster member doesn't have a TCP connection with other members.

When a user is added, you can see the username in `/var/log/messages` of all cluster members.

NOTE: 8900 is the default port used for session sharing among cluster members. If a different port is configured, `grep` for session sharing.

A.19 On Windows XP and 7, Loading ActiveX Takes More than Three Minutes to Connect to SSL VPN

The ActiveX component which is enabled at web browser, is not detected in the forward proxy. Hence, on Windows 7, the forward proxy connections were not through.

To workaround this issue, enter the `UseThisConfigurationAnyway=true` parameter in `proxy.conf` file, which forces the ActiveX component to use the forward proxy configuration in this file.

A.20 If There Is An Install Log Error, SSL VPN Client In Kiosk Mode Fails To Start

If there is an error in the install log as *RegOpenKey failed with error code*, then the SSL VPN client in the Kiosk mode fails.

To work around this issue, enter the registry key manually.

- 1 Go to run command.
- 2 Type *regedit*. The Registry Editor window displays.
- 3 Go to *My Computer > HKEY_CURRENT_USER*.
- 4 Right-click on *HKEY_CURRENT_USER > New > Key*.
- 5 Enter the new key name as *Environment*.