Netilla Security Platform Administrator Manual

Version 4.2

Third Edition

Netilla®

Secure Application Access Management

ICSA Labs CERTIFIED
WWW.ICSALabs.com
SSL-TLS (VPN)

Netilla Networks, Inc.
347 Elizabeth Avenue Somerset, NJ 08873
Phone: 732.652.5200 Fax: 732.764.8862
www.netilla.com

Part No.480-0001-002

Netilla Networks, Inc.
347 Elizabeth Avenue
Suite 100
Somerset, NJ 08873
Phone: 1.877.NETILLA
732-652-5200
Fax: 732.764.8862

TABLE OF CONTENTS

About this Manual

This Administrator Manual assists with high-level configuration of the Netilla Security Platform (NSP), and is intended for administrators who possess advanced networking experience. This experience should include TCP/IP, routing/subnetting, DNS, and network security, as well as experience in operating system installation and configuration, such as Microsoft Windows 2000, UNIX/Linux, X11, and character-based applications. The individual should also have successfully completed the Netilla Certified Engineer Program.

All configuration instructions presented in this guide assume that you are logged in as radmin *(the account reserved for reseller administration) unless otherwise stated.*

NSP Documentation Set

The NSP documentation set consists of the following.

- *Netilla Security Platform QuickStart Guide:* Provides step-by-step instructions for getting your NSP up and running using the most common configuration.
- *Netilla Security Platform Administrator Manual:* Provides detailed information and step-by-step instructions for configuring the NSP.
- *Netilla Security Platform End User Manual*: Contains general end user instructions including how to use the NSP services as well as troubleshooting information.

Additional Information

Additional information, including Application Notes, FAQs, the Certificate Site Management Guide as well as the latest version of this manual, is available in the online Integrator Suite. Access the Integrator Suite by choosing the Provider Login link on the Netilla Website (www.netilla.com). Contact your local Channel Manager for an Integrator Suite login and password.

How to Use this Guide

Table 1 shows where to find specific information in this guide.

Table 1 How to Find Information

If you are looking for...	Turn to...
Overview of the NSP	Chapter 1
How to configure DNS and Ethernet settings, install licenses & certs	Chapter 2
Authentication configuration	Chapter 3
How to configure the Thin service	Chapter 4
How to configure the Web service	Chapter 5

Table 1 How to Find Information

How to configure the Tunnel service	Chapter 6
Information on User Accounts	Chapter 7
How to set up application load balancing	Chapter 8
How to monitor the NSP	Chapter 9
How to shadow user sessions	Chapter 9
How to configure the NSP Services	Chapter 10
How to configure the Netilla firewall	Chapter 11
Customizing the NSP's interface	Chapter 12
Configuring the Netilla Hot Standby system	Chapter 13
Troubleshooting the NSP	Appendix A
Firewall port requirements for using the NSP	Appendix B
APL key list for 3270 applications	Appendix C
Using the serial console	Appendix D
Hardware specifications	Appendix E

Conventions

Table 2 lists conventions that are used throughout this guide.

Table 2 Notice Icons

Icon	Notice Type	Description
	Information note	Information that describes important features or instructions
	Warning	Information that alerts you to important information regarding applications or data

1 Netilla Security Platform Overview

This chapter presents an overview of the Netilla Security Platform (NSP). The following topics are discussed.

- How the NSP Works
- NSP Access Requirements
- Understanding NSP Administrative Accounts
- Logging in to the Administrator Site

How the NSP Works

The NSP is a clientless, SSL VPN appliance that enables secure, Web-browser access to a wide range of data center resources. As a dedicated network device, the NSP integrates seamlessly into existing network and security infrastructures, offering rapid deployment, easy installation, minimal maintenance, and network protection.

The NSP is installed into the corporate network behind the Internet access router. It connects to both the Internet and the private network using one or two separate Ethernet ports. When accessing remote applications and Web-based intranet applications, users enter the URL of the NSP in their browser through an SSL encrypted session; the NSP terminates the SSL session and communicates directly to the application servers as appropriate:

- Remote Desktop Protocol (RDP) for Microsoft Windows servers
- UNIX/Linux X Windows and character-based applications (telnet, ssh, rexec, rcmd, or rlogin)
- 3270 over telnet for mainframes
- HTTP/HTTPS for Web servers
- SSL tunneling for client/server applications

An example of a typical NSP deployment is shown in Figure 1.

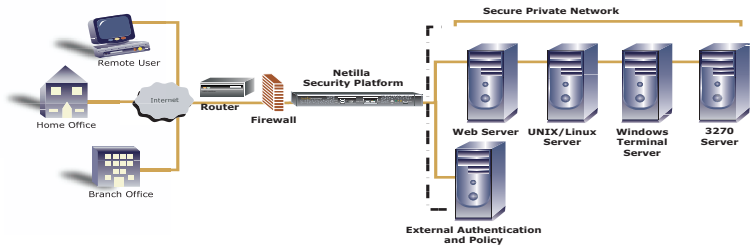


Figure 1 Typical NSP Deployment

Dependable Security with the dynaTRUST™ Operating System

Netilla's security features keep business-critical resources safe from potential risks. With browser-embedded SSL encryption to the Netilla SecureRealm Framework and multi-layer authentication engine, the NSP can leverage security solutions already in place, such as leading 2-factor authentication systems and the prevailing policy engines used in today's enterprise environment.

An extension of the Netilla SecureRealm framework, dynaTRUST™ is Netilla's hardened proprietary operating system that is optimized for policy enforcement and API integration. The dynaTRUST operating system promotes network processing efficiency by leveraging state-of-the-art hardware acceleration components, while maintaining session-aware state information and policy compliance checking.

To further guard private network resources, the NSP incorporates a dynamic, session-based and stateful inspection firewall, along with application-layer proxy technology that prevents exposure of information to unauthorized users. In addition, the Netilla Upgrade GeNIE ensures fast deployment of security and feature updates.

Versatility: Three Ways to Access Your Network

The NSP incorporates three SSL access technologies in a single appliance, providing a full-spectrum remote-access solution that meets a range of application access types:

- Thin client access to applications
- Web access to intranet Web-based applications and portals
- Tunnel access to local client/server applications

Thin Client Access

The Thin client application access mode enabled by the NSP is for remote applications residing on a centralized servers. With no application client software required, and with just a Java-enabled Web browser, users interact with the actual application running within a browser window, securely over the Web. Any program, running on any operating system - Windows, UNIX, Linux or 3270 mainframe and AS/400 with 3270 terminal emulation- can be made available to users.

In this remote application access model, both the client and server portions of an application are centrally hosted in the corporate data center. When a user requests a remote application, the NSP functions as an application-layer proxy, taking the native protocols that reside within these server-based applications - RDP for Windows, X11 for UNIX, and Telnet for mainframes - and translating them into the NSP’s built-in remote application protocol, which then presents the remote application in the user’s Web browser. This remote application protocol also provides dynamic bandwidth optimization between the remote user and the NSP.

The NSP supports these capabilities through a small Java applet that’s downloaded to the user's browser upon requesting a remote application for the first time. The applet routes application information (screen, keystrokes, and mouse clicks) between the remote user’s browser and the network's application server over compressed HTTPS data streams. The NSP monitors, measures, and adapts to the ways that data is transferred between the user and the network.

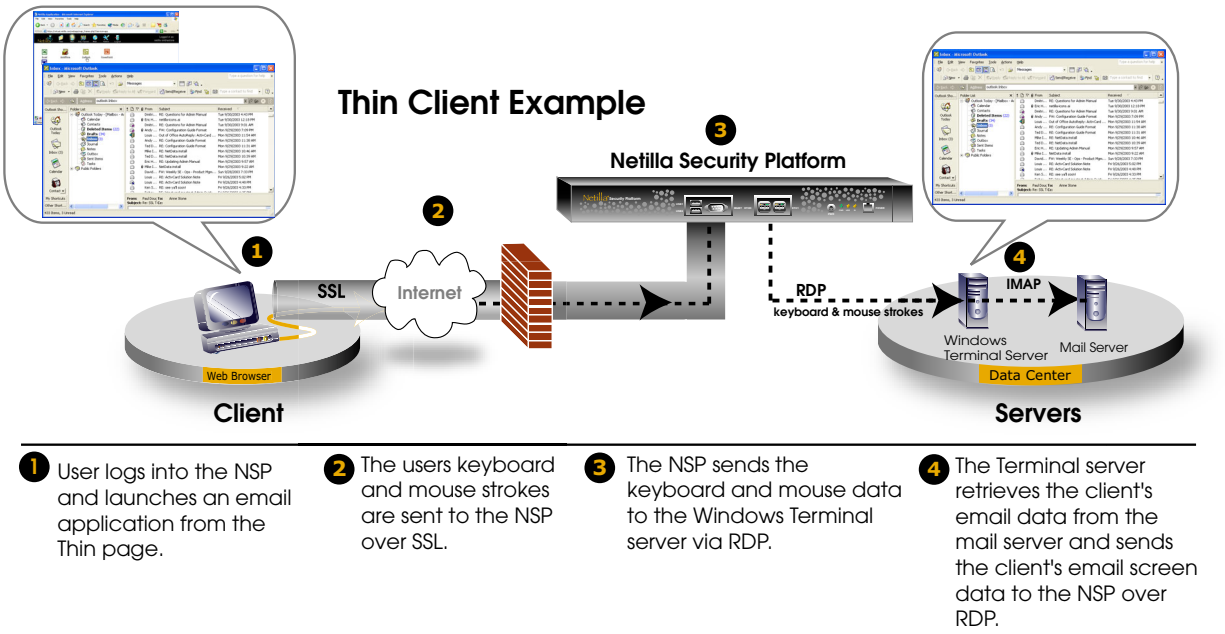


Figure 2 How Thin Client Works

In this way, users gain access to full-featured versions of applications, running on the remote application server, requiring no configuration of the user's computer. The application itself has the same resources available in the office, including server-based files, client drive mapping, and local and remote printing. Likewise, the remotely-located application can fetch files from the client PC and print at the client's site, creating a truly seamless branch or home office experience.

Web Application Access

The Web application access mode supported by the NSP is secure access to internal Web-based applications, intranet sites and portals through HTTP reverse proxy technology. In this application-layer proxy model, the NSP's built-in HTML translation engine dynamically rewrites all user requested Web pages - even those containing complex JavaScript - obscuring the URL, network topology, and source code of the originating Web application. Because all requested pages are re-written by the NSP, the opportunity also exists to filter potentially malicious Web components on an as-needed basis.

By using the NSP, all HTTP traffic is encrypted over SSL even for servers that the NSP connects to that are not SSL enabled.

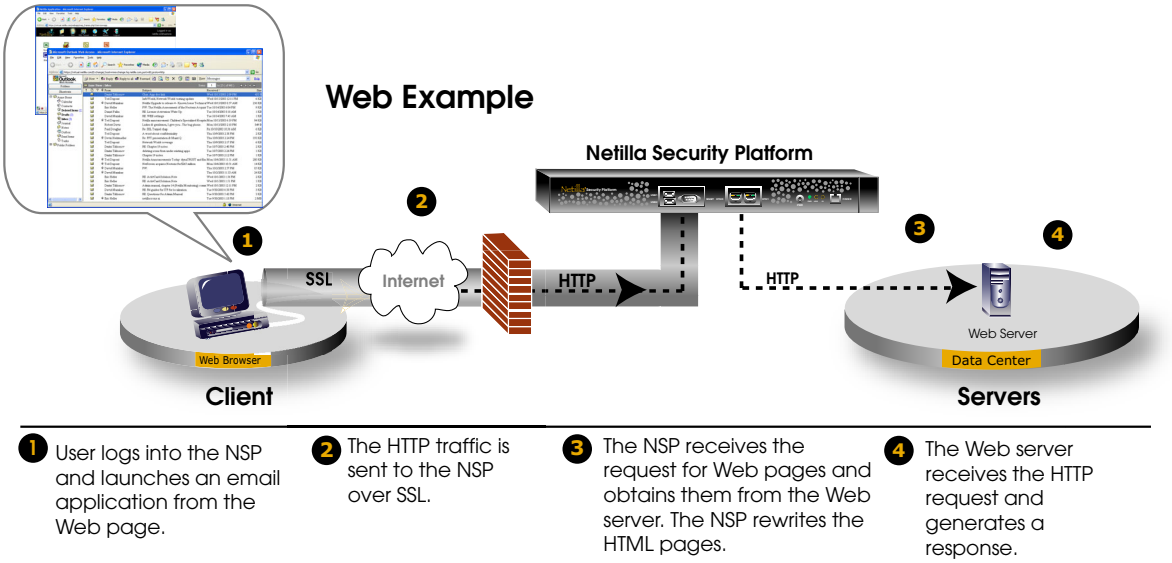


Figure 3 How HTTP/HTTPS Reverse Proxy Works

This approach allows organizations to deploy intranet-based Web applications without exposing Web servers to the public Internet. Authorized remote users gain instant, clientless access to internal Web applications from any location, without the cost and maintenance of locking each server down for public access.

Tunnel Access

The Tunnel application access mode supported by the NSP is client/server access over Tunneling. This feature allows users to work off line with local clients and “synch up” with remote servers over a secure Tunnel.

Netilla facilitates the secure SSL tunnel with a Virtual Adapter, an ActiveX component seamlessly downloaded the first time a user initiates the tunnel. The Netilla Virtual Adapter offers the broad application support of an IPSec-based VPN, including both TCP and UDP based applications, with the benefits of policy-based tunneling, dynamic session-based firewalling, and seamless installation, requiring no end-user configuration. Additionally, no changes to the client/server applications themselves are required.

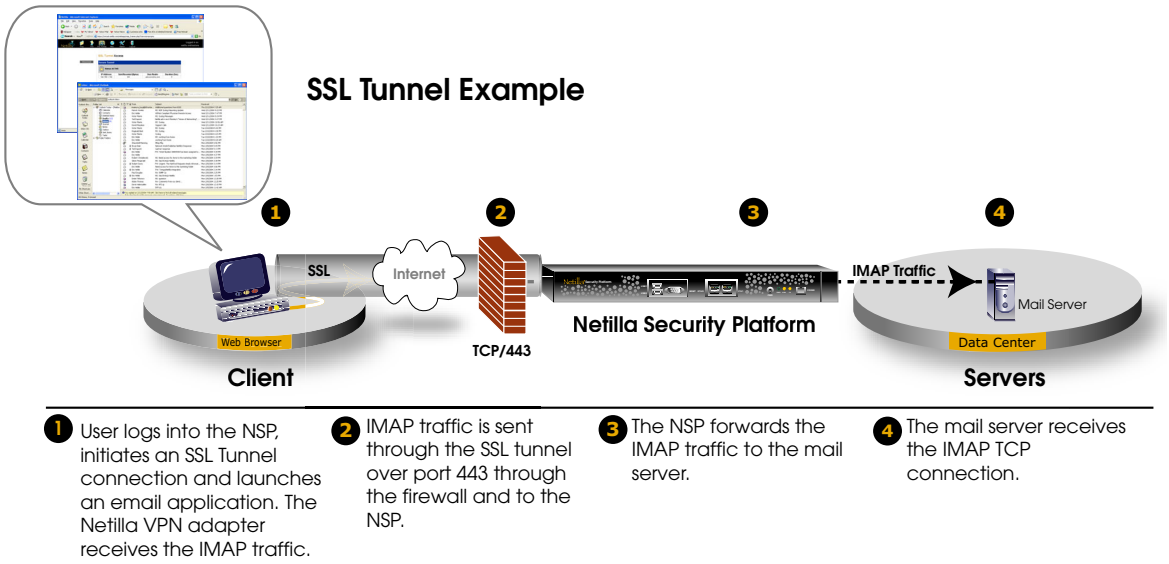


Figure 4 How SSL Tunneling Works

With a single perimeter firewall port open to the Internet, the NSP SSL Tunnel delivers a robust, low maintenance alternative to traditional VPN deployments.

NSP Access Requirements

The requirements for accessing the NSP site are different depending on whether you are an administrator or an end user. To access and use the NSP's administrator site, the Web browser requirements are described in "Administrator Requirements". To access and use the NSP's GUI for remote application access, client Web browser requirements vary depending on the type of applications being accessed. Refer to "End-User Requirements" for details.

Administrator Requirements

To access the NSP's Administrator Site, you will need the following:

- A computer capable of running a compatible Web browser. Compatible Web browsers are as follows:
  - Microsoft Internet Explorer 6.0 and higher (Win 32)
  - Netscape Navigator 6.0 and higher (Win 32 and Linux clients)
  - Mozilla 1.3 (Win 32 and Linux clients)
- A valid username and password, and the URL of your NSP.

End-User Requirements

For Thin Application Access:

- Web browser (128-bit SSL recommended) with Java Virtual Machine
  - Microsoft Internet Explorer 6.0 and higher for Windows
    - *Sun JVM 1.4 or higher or MS JVM 5.0.0.3805 or higher*
  - Netscape Navigator 6.0 and higher (Win32 and Linux clients)
    - *Sun JVM 1.4 or higher*
  - Mozilla 1.3 (Win32 and Linux clients)

- *Sun JVM 1.4 or higher*
- Configure Web browser to support Secure Socket Layer (SSL) version 3.0 or Transport Layer Security (TLS) 1.0
- Configure Web browser to allow plug-ins or Java access

Note that end users cannot access your NSP until you have activated your default licenses. Refer to *"Installing Licenses" on page 24* *for more information.*

For Web Application Access:

- Web Browser (128-bit SSL recommended)
  - Microsoft Internet Explorer 6.0 and higher (Win32 only)
  - Netscape Navigator 6.0 and higher (Win32 and Linux clients)
  - Mozilla 1.3 (Win32 and Linux clients)
  - Configure Web browser to support Secure Socket Layer (SSL) version 3.0 or Transport Layer Security (TLS) 1.0
  - Configure Web browser to allow plug-ins or Java access

For Tunnel Access

- Web browser (128-bit SSL recommended)
  - Microsoft Internet Explorer 6.0 and higher (Windows 2000 and XP clients)
  - ActiveX-enabled to allow Netilla Virtual Adapter to download
  - Configure Web browser to support Secure Socket Layer (SSL) version 3.0 or Transport Layer Security (TLS) 1.0
  - Configure Web browser to allow plug-ins or Java access

Files Service:

- Microsoft Internet Explorer 6.0 and higher with MS JVM 5.0.0.3805 or higher (Win32 only)

About your Internet connection

End users require a minimum connection of 28 Kbps for simple information transfers. When working with an application that includes multiple graphics, a cable modem or DSL connection is recommended. When using the Thin client service and working with large files, graphics, or applications, end users require at least 128 Kbps.

End User information on accessing and using the NSP features is provided in the Netilla Security Platform End User Manual.

Understanding NSP Administrative Accounts

The NSP ships with the following three default administrative accounts.

- *admin: The* admin account is the highest privilege level.
- *radmin* (or reseller administrator): An account created for managing the service in the field.
- *maint:* An account created for general maintenance and has the least number of privileges.

All configuration instructions presented in this guide can be performed as admin or radmin. Exceptions are noted.

Both admin and radmin provide the level of privileges necessary for configuring the NSP. Specifically, the rights each of the administrative accounts are listed in Table 3.

Table 3 Rights for NSP Administrative Accounts

NSP Administrator Rights	Admin	Radmin	Maint
Administer the Netilla licenses in the NSP	Yes	Yes	No
Backup and restore the NSP configuration settings	Yes	Yes	No
Create, modify and delete application objects	Yes	Yes	No
Access and change system configuration settings such as IP addresses	Yes	Yes	No
Activate and de-activate the Netilla firewall	Yes	Yes	No
Create, modify, and delete users	Yes	Yes	Yes
Customize the login screen (with the exception of changing the Menu Bar logo; this is reserved for *admin*)	Yes	Yes	Yes

To change the password for any of the administrative accounts, refer to "Modifying an Administrator Profile" on page 151.

Logging in to the Administrator Site

To access the Administrator Site of the NSP, do the following.

1 Initiate a connection to the Internet and launch a Web browser.

2 Enter the fully qualified domain name, for example, https://hostname.netillavo.com.

If you do not have this configuration information in your NSP packing materials please call contact your reseller.

The NSP log in window is displayed, as shown in Figure 5.

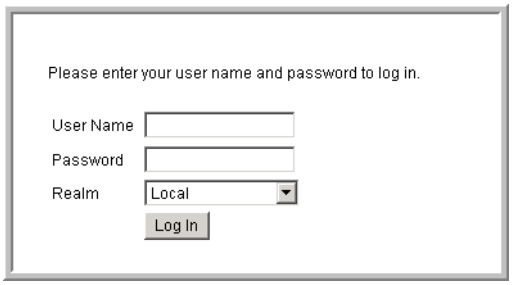


Figure 5 The NSP Login Screen for Radmin

3 For User Name, enter *admin or radmin*.

The User Name and Password fields are case-sensitive.

4 Enter your password. The default password was provided with your NSP.

The NSP can be configured to remove the Password field from the log in page. This is helpful for RADIUS challenge response scenarios. Refer to "Removing Password Field from Log In Page" on page 59 for details.

5 Make sure the Realm field is set to *Local (*or type *Local* in the Realm field if the Realm drop-down list is box is not displayed).

6 Click *Log In*.

The NSP License agreement is displayed when you log in for the first time as *radmin*. Accept the license agreement by clicking *Yes*.

The NSP Administrator Site is displayed.

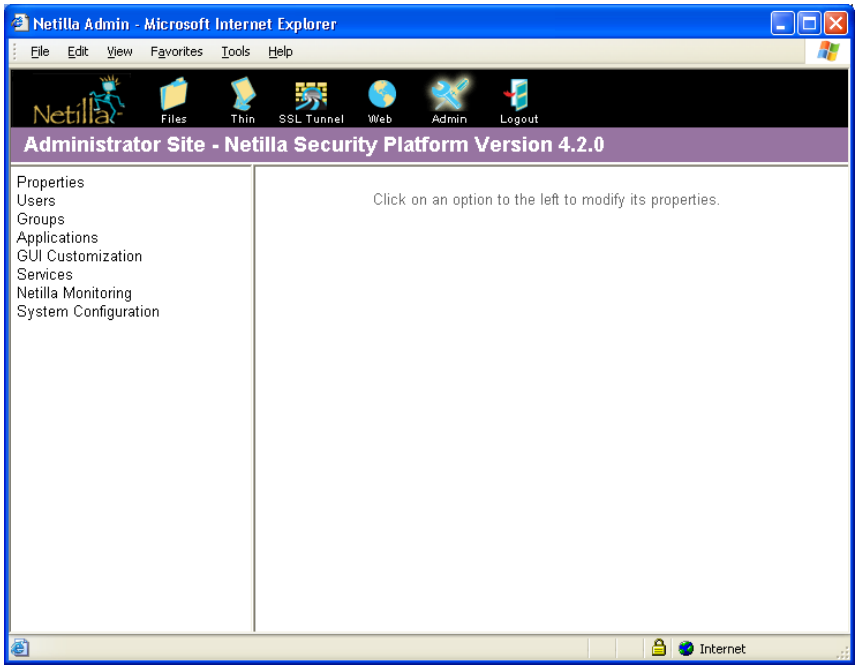


Figure 6 The Administrator Site

7 Change the default passwords for the administrator accounts. Refer to “Modifying an Administrator Profile” on page 151.

NSP Administrator Site Overview

This section lists and describes the Administrator Site main menu.

- **Properties**: Allows you to change the password and start up service for the currently logged in NSP administrator.
- **Users**: Allows you to add users to the NSP, and assign applications to users.
- **Groups**: Allows you to add groups to the NSP.
- **Applications**: Allows you to create pointers on the NSP to the applications that you want users to be able to access.
- **GUI Customization**: Allows you to customize the NSP GUI with your company’s name and logo.
- **Services**: Allows you to configure system-wide settings for each of the NSP services (that is, Web, Tunnel, Thin, Files)
- **Netilla Monitoring**: Allows you to gather and review NSP statistics some of which are based on time periods you specify.
- **System Configuration**: Allows you to configure network settings such as Ethernet and DNS settings, as well as install licenses, manage digital certificates, backup system settings and restore system settings.

2 System Configuration

This chapter describes how to configure the various system parameters, such as network connections, licenses, digital certificates and authentication settings. These settings allow you to manage the higher-level configuration options for the Netilla Security Platform (NSP), and will most likely not require frequent modifications.

The following items are discussed.

- About System Configuration Settings
- Configuring Network Connection Settings
- Installing Licenses
- Managing Certificates
- Backing up and Restoring NSP Profiles

About System Configuration Settings

This section describes how to access the system configuration menu and describes the available settings.

Accessing System Configuration Settings

To access the system configuration menu do the following.

1 From the Administrator Site, select *System Configuration*. The following subheadings appear.

For instructions on how to access the Administrator Site, refer to "Logging in to the Administrator Site" on page 15.

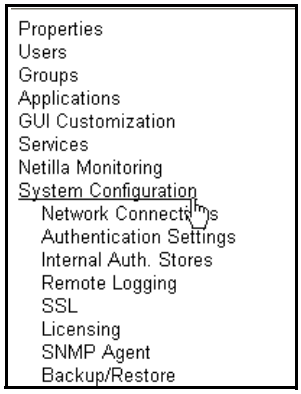


Figure 7 System Configuration Submenu

System Configuration Submenu

Table 4 lists the system configuration submenu items. Not all of the items listed are described in this chapter. References to other sections of this guide and other documents are noted.

Table 4 System Configuration Settings

Menu Name	Description
Network Connections	Allows you to configure network settings such as IP addresses for DNS servers and NSP Ethernet interfaces. For details refer to “Configuring Network Connection Settings” on page 18.
Authentication Settings	Allows you to create realms and configure authentication stages within those realms. For details refer to “Managing Authentication Settings” on page 43.
Internal Auth Stores	Allows you to create a database of users on the NSP that uses the NSP’s internal authentication. For details, refer to “Creating an Internal Authentication Data Store” on page 63.
Remote Logging	Allows the NSP to send syslog messages to a syslog server. For details, refer to “Remote Logging” on page 172.
SSH	SSH fields should be left at default settings unless instructed otherwise by Netilla Support personnel.
Licensing	Allows you to install Netilla licenses which enable you to use Netilla services. For details, refer to “Installing Licenses” on page 24.
SSL	Allows to request and install server and client digital certificates. For details, refer to “Managing Certificates” on page 25.
SNMP Agent	Allows the NSP to send SNMP traps to an SNMP manager. For details, refer to “Setting Up SNMP Reporting” on page 173.
Backup/Restore	Backup allows you to save your NSP configuration profile. Restore allows you to restore a previously saved configuration profile. For details, refer to “Managing Certificates” on page 25.
Software Upgrade	Allows you to upgrade the NSP’s software. These instructions are not included in this manual. They are detailed in a separate document that is provided with the software.
Locale	Allows the NSP’s end user GUI to be localized in Japanese. For details refer to
Failover	Allows you to configure the optional HotStandby optional feature. These instructions are covered in a separate document called the Netilla Hot Standby Manual an is located in the Integrator Suite Reference Library.
Shutdown	Allows you to shut down the NSP which includes turning off the power.

Configuring Network Connection Settings

The following options are available in the Network Connections submenu.

- **General**: Contains settings for NSP hostname, DNS servers, default gateway and the Ethernet interfaces.
- **IP Forwarding and Network Address Translation (NAT):** Allows you to enable or disable IP Forwarding and NAT features.
- **NTP**: Allows you to configure the NSP with an external time server.

- **Routing**: Allows you to configure static IP routes.
- **Firewall**: Allows you to use to NSP's built in firewall.

Configuring General Settings

The General Settings page, shown in Figure 8, is used to configure the general network information, including setting the Host name of the box, the Primary and Secondary DNS, the Default Gateway and the Ethernet interfaces.

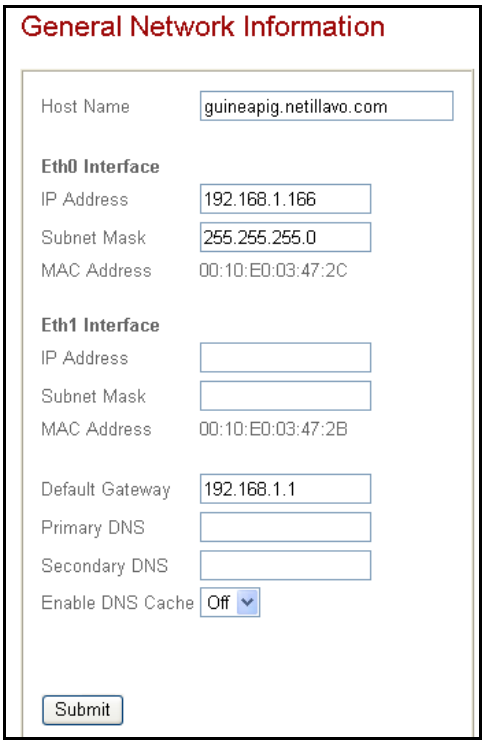


Figure 8 General Settings Page

To configure the General Network information, do the following.

1. For **Host Name**, you can change the host name of the NSP. The host name must match the common name on the digital certificate that is installed on the NSP. Whenever you change the host name, ensure that you also have a matching digital certificate to install on the NSP. If the digital certificate and the hostname of the NSP do not match, the end-user receives an error.
2. For the **Eth0 Interface**, enter the IP address and subnet mask of the primary Ethernet interface. Note that the MAC address of this interface is displayed.
3. For the **Eth1 Interface** (optional), enter the IP address and subnet mask of the secondary Ethernet interface. Leave these fields blank if you are not configuring a secondary Ethernet interface.
4. For **Default Gateway**, this is usually the address of the router that is used to reach the Internet.
5. For **Primary and Secondary DNS**, enter the IP address of your DNS servers. These are generally the current DNS servers provided by your ISP.

At least one DNS entry MUST be configured in order to use the Web service of the NSP. For details, refer to *"Configuring the Web Service" on page 101.*

6 If you configured a DNS server in step 5, you can **Enable DNS Cache**. Select *On* to enable the results of a DNS lookup to be cached. Alternatively you can disable caching by selecting *Off*. Note that when cached is enabled, performance is improved.

7 Click *Submit*.

Configuring IP Forwarding and NAT

This section describes how to configure IP forwarding and network address translation (NAT).

- **IP Forwarding:** IP Forwarding allows the NSP to forward packets from the two internal interfaces, as well as to the Virtual adapter when using the Tunnel service.
- **NAT:** Network Address Translation (NAT) allows users on a private network to access the Internet by using only one public IP address. This eliminates the need to assign a public IP address to every private machine on the internal network.

In order to use the Tunnel service, IP Forwarding MUST be set to Yes. Also as indicated on the screen, to implement NAT, IP Forwarding must be set to Yes.

Configuring IP Forwarding

To enable or disable IP Forwarding, do the following.

1 From the System Configuration submenu, click *IP Forwarding and NAT.*

2 Enable IP Forwarding by selecting *Yes* from the drop down menu shown in Figure 9.

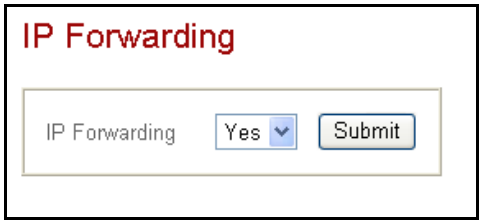


Figure 9 IP Forwarding Page

3 Click *Submit*.

The page refreshes.

Configuring NAT

This section describes how to configure network address translation (NAT) and set up the NSP as a gateway. NAT allows users on a private network to access the Internet by using only one public IP address. This eliminates the need to assign a public IP address to every private machine on the internal network.

Setting Up the NSP as a Gateway

To set up the NSP to be the gateway on your network, do the following.

1 From the System Configuration submenu, click *IP Forwarding and NAT.*

2 Enable **IP Forwarding** by selecting *Yes* from the drop down list box shown in Figure 10.

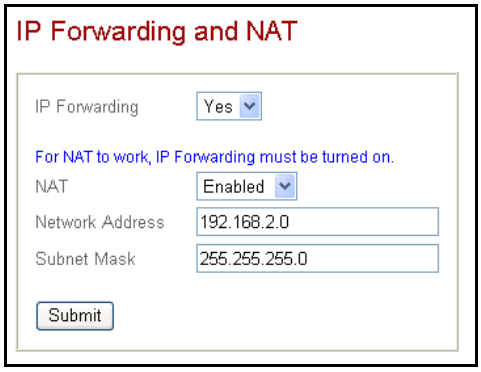


Figure 10 IP Forwarding Drop-down List Box

3 Select *Enabled* from the **NAT** drop-down menu.

4 For **Network Address**, enter the network address of the internal or private network.

For example, *192.168.2.0*.

5 For **Subnet Mask**, enter the subnet mask of the segment for the internal or private network.

6 Click *Submit*.

The page refreshes.

Configuring Network Time Service (NTP)

This section describes the steps required to configure the NSP with an external time server. An external time server is used by the NSP to keep accurate time and is highly recommended for Kerberos authentication to prevent authentication failures relating to clock skew.

It is recommended that a time server entry be used when setting up the optional HotStandby feature, to ensure proper synchronization of each NSP. For installation and configuration instructions for using the NSP failover feature, refer to "Configuring the Hot Standby System" on page 135.

To configure the NSP to use an external time server, do the following.

1 Click *NTP* from the Network Connections submenu. The NTP Settings page appears as shown in Figure 11.

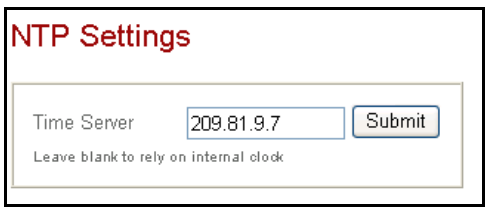


Figure 11 NTP Settings

2 Enter the appropriate server information in the Time Server field.

Many external time servers are available and can be found by searching for NTP Servers using any search engine. It is recommended that you choose a time server that is close to your location.

http://www.boulder.nist.gov/timefreq/service/time-servers.html *has a list of many public time servers available worldwide.*

3 Click *Submit*.

The page refreshes. Once complete, verify the new parameters.

How to Configure a Static Route

A static route is a manually configured route that specifies a transmission path to another network. Static routes essentially allow the NSP to see other networks that are not physically connected to the NSP via its Ethernet ports. A static route might be implemented in a situation where a site uses more than two subnets locally, but each needs to see the resources of the NSP. This section explains the procedure for adding a static route to the NSP system configuration.

About Static Routes

For an example of a static route, imagine a site that has an NSP connected to the public network on the primary interface, with an IP address of *208.206.100.1*, and the secondary interface with an IP address of *192.168.1.20* connected to a network where only servers reside. This network has segregated some servers from the end user network, and this server-only network is assigned the IP address *192.168.1.0*. At this point, the only application servers the NSP can access are those on the *192.168.1.0* network. However, there is an application server on another network with an IP address of 10.1.1.0, separated by a router. This router has an IP address of 192.168.1.10, and is on the 192.168.1.0 network.

An example of this network scenario is shown Figure 12.

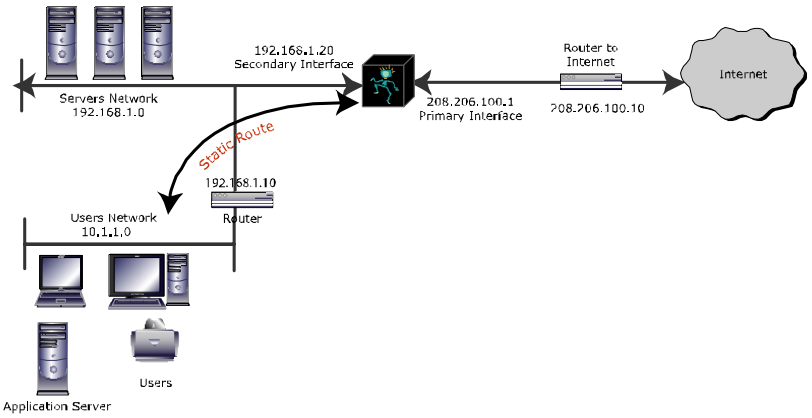


Figure 12 Static Route Network Example

What is needed is a method to allow the NSP to see the *10.1.1.0* network and application server, to allow the NSP to host applications for end users. This is accomplished by adding a static route to the NSP.

Adding a Static Route to the NSP

To add a static route, do the following.

1 From the Administrator Site, click *System Configuration*.

2 From the System Configuration submenu, click *Network Connections,* and then click *Routing*.

The Static Routes page appears as shown in Figure 13.

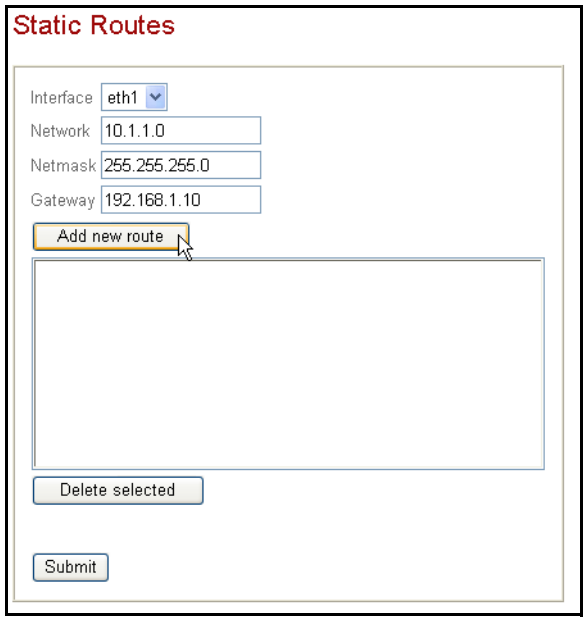


Figure 13 Static Route Screen

3 For **Interface**, select *eth0* or *eth1* from the Interface drop-down menu.

4 For the **Network** and **Netmask** fields, enter the IP address and subnet mask of the static route. In the previous example, the Network interface is 10.1.1.0.

5 For **Gateway**, enter the gateway IP address of the router between the NSP and your network.

In the previous example, the Gateway is *192.168.1.10*. The Gateway address is the IP address of the side of the router that is directly connected to the secondary interface of NSP.

6 Click *Add new route*. The route appears in the text field as shown in Figure 14.

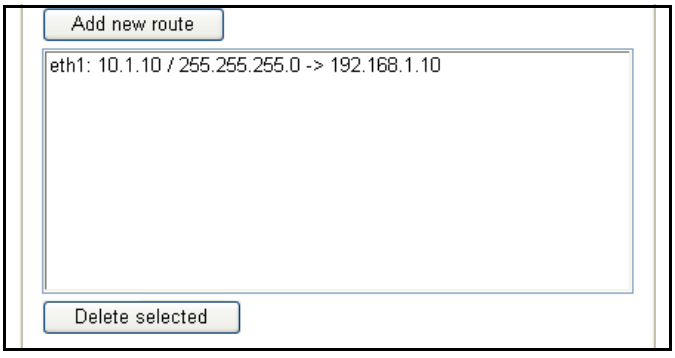


Figure 14 Add New Static Route Page

Deleting a Static Route

1 To delete a static route, select the route from the text field and click *Delete selected*.

Multiple static routes can be selected with the Shift or Control keys.

2 Click *Submit*.

Configuring the NSP Firewall

The firewall configuration is accessed by clicking *System Configuration*, *Network Connections*, and then *Firewall*. In order to use the firewall it must first be turned on by choosing *On* from the drop down list, then clicking *Submit*, found at the bottom of the firewall page.

A full description of the configuration of the firewall can be found in "The Netilla Firewall" on page 185.

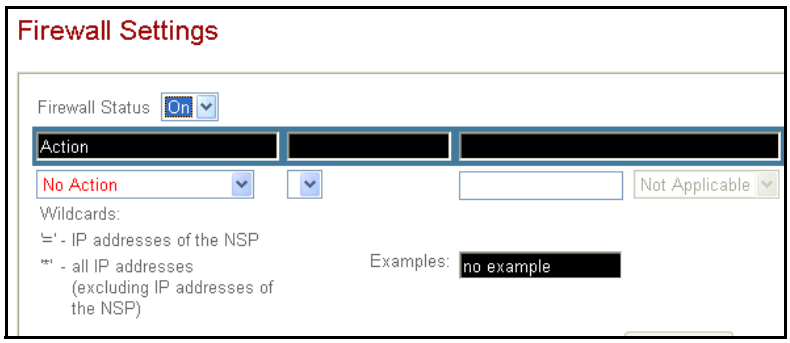


Figure 15 Firewall Settings Page

Installing Licenses

This section describes how to install a Netilla license. To complete this process, you will need the license key from your integrator or distributor.

To install an NSP license, do the following.

1 From the Administrator Site, click *System Configuration*, and then click *Licensing*, as shown in Figure 16.

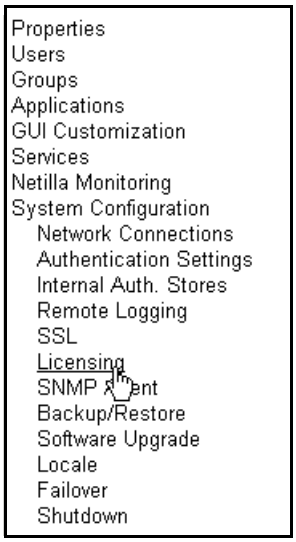


Figure 16 Licensing Menu Location

The Netilla License Management page appears as shown in Figure 17.

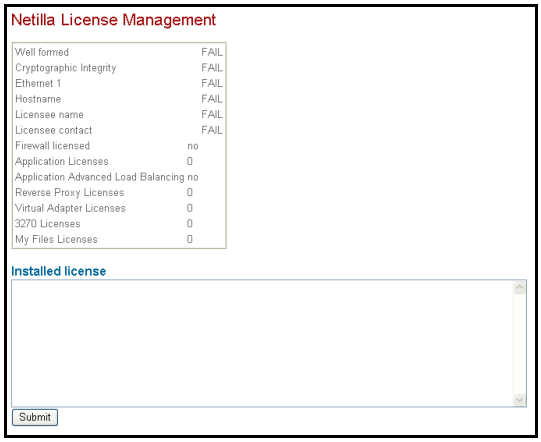


Figure 17 Netilla License Management Page

2 Copy the encoded text and paste it in the text box labeled **Installed License**.

3 Click *Submit*.

The Netilla License Management page with an installed license is shown in Figure 18.

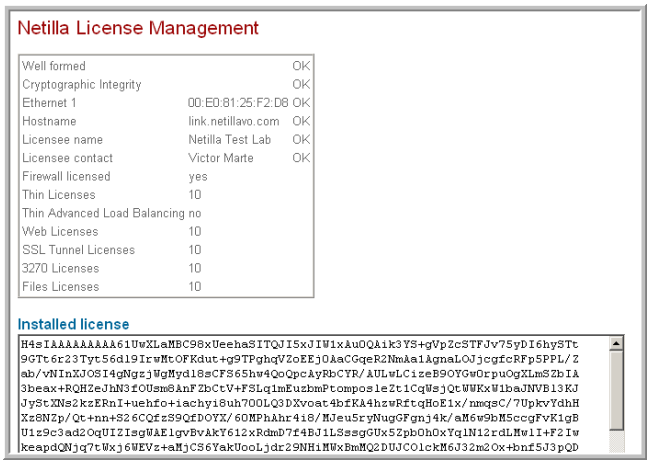


Figure 18 Netilla License Management Page

Managing Certificates

This section describes the digital certificate options available on the NSP.

It is assumed that the reader has some basic knowledge of public key infrastructure (PKI) and SSL.

If you have not already done so, the first step is to install a certificate from a Certificate Authority (CA) on the NSP.

- **Install a Certificate from a Certificate Authority on the NSP**

There are two ways you can do so depending on whether you need to request a certificate from a CA or whether you already have a certificate from a CA.

- If you already have a certificate from a CA that was generated on a server other than the NSP, refer to “Importing an Existing Server Certificate from a CA” on page 30 for instructions on how to install it.
- To obtain a certificate from a CA, refer to “Generating a Server Certificate Request from a CA” on page 26.

In addition to installing CA certificates, you can do the following using the NSP Certificates menu.

- **Require a Certificate for Client Verification**
- **Import a Root Certificate**
- **Set Browser Cryptographic Level Checking**

Accessing the NSP Certificates Page

To access the certificates page, do the following.

1. From the Administrator Site, click *System Configuration*.
2. Click *SSL*.

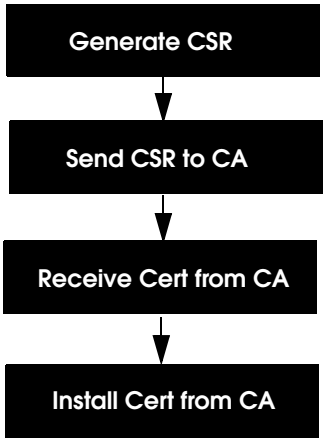
The following options are available.

- **Certs from CA** provides the following submenus.
  - **Generate CSR** allows you to generate a Certificate Signing Request (CSR) for the Certificate Authority. The CSR is used by the Certificate Authority to generate a new digital certificate.
  - **Upload Cert** allows you to install the digital certificate once it is received from the Certificate Authority.
- **Load Existing Cert** allows you to install a Digital Certificate and Key that were generated on a server other than the NSP.
- **Generate Self-Signed** generates a self-signed certificate on your NSP.
- **CA Certificates** provides options that allow you to upload new CA root certificate, view existing certificates and set up client verification.
- **Browser Settings** allows you to specify what occurs if the user’s Web browser does not support 128-bit encryption.

Generating a Server Certificate Request from a CA

This option allows you to generate a Certificate Signing Request (CSR) for the Certificate Authority. Once the CSR is generated, you send it in to the CA of your choice. The CA will send you a new digital certificates based on the information in the CSR.

The main steps for obtaining and installing a CA certificate are:



If a chain has been used to sign, the ROOT CAs must be added before the certificate from the CA is installed. Refer to "Installing a Server Certificate from a CA" on page 29 for details.

To generate a new CSR for the CA, do the following.

1. From the Administrator Site, click *System Configuration* and then click *SSL*.
2. From the SSL menu, click *Cert from CA* and then click *Request New Certificate*.

   The New Certificate Signing Request page displays.
3. Complete the required information as described in Table 5 and then click *Generate New* as shown in Figure 19.

Figure 19 New Certificate Signing Request Page

Table 5 New CSR Fields and Descriptions

Field Name	Description
Country	The two-letter ISO abbreviation for your country (for example, *US* for the United States). For the ISO country list, see http://www.iso.org/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.html
State	The state or province in which your organization is headquartered. Enter the full name of the state or providence; abbreviations are not allowed.
Locality	City in which your organization is headquartered.

Table 5 New CSR Fields and Descriptions

Field Name	Description
Organization	The name under which your organization is registered. This organization must own the domain name that appears in the common name of your NSP. Abbreviations and the following characters are not allowed < > ~ ! @ # $ % ^ * / \ ( ) ?.
Org. Unit	The name of the department or group that will be using the NSP.
Common Name	The name of your NSP as it appears in the server's URL (for example, *companyname.netillavo.com*). The Common Name must be identical to the fully qualified domain name of the NSP for which you are requesting a certificate. If the NSP name does not match the common name in the certificate, some services will fail to work. Do not include the protocol specifier (http://) or any port numbers or pathnames in the common name. Wildcards such as * or?, or IP addresses are not allowed.
Email	Email address of the contact person for the department or group using the NSP.

The newly-generated CSR is displayed. An example is shown in Figure 20. A matching private key is also generated and stored in the NSP.

Figure 20 Current CSR Page

4 After verifying that all data is correct you can submit this CSR to a CA of your choice.

5 Copy and save the Certificate Request to a text file.

Make sure you include the full BEGIN and END lines and all of the dashes.

6 Submit the new certificate request to your Certificate Authority.

Upon the receipt of the certificate from your certificate authority you may import it into the NSP as described in the next section, "Installing a Server Certificate from a CA".

Installing a Server Certificate from a CA

This section describes how to install a signed server certificate from a Certificate Authority.

Prerequisite

- **Verify Installation of Root CA and Intermediate Root CA Certs.** Before installing a server certificate from a CA, you will need to verify that the Root CA and any Intermediate Root CA certificates are installed on the box. Refer to "Installing a Root CA on the NSP" on page 33.

  Note that many certificates are signed by an Intermediate Certificate. Please check with you CA to determine whether the certificate you received is signed by one CA or a chain of CAs or Intermediate Root Certificate.

WARNING: If a chain has been used to sign, the ROOT CAs must be added in a specific order. Failure to add in this manner will cause the certificate to not function properly and may require access directly to the box via Netilla Support. Root CAs are added from the highest level down to the actual CA that signed the certificate. The server cert is then added after the ROOTs.

For example, if you have part of a certificate signing chain, you would install the certificates in the following order:

1. Top Level ROOT CA
2. Intermediate ROOT CA or Chain
3. Server certificate

If more than one Intermediate CA has been used, the Intermediate that signed the certificate must be the **last** one installed before installing the server cert.

Installing a Server Certificate

After receiving the signed certificate from the Certificate Authority, use the **Upload Cert from CA** option to install the certificate on the NSP as follows.

1. From the Administrator Site, click *System Configuration* and then click *SSL*. From the SSL menu, click *Certs from CA*, and then click *Upload Cert from CA*.
2. Open the newly-received certificate with a text editor. Copy and then paste the entire contents into the field provided by the NSP. An example is shown in Figure 21.

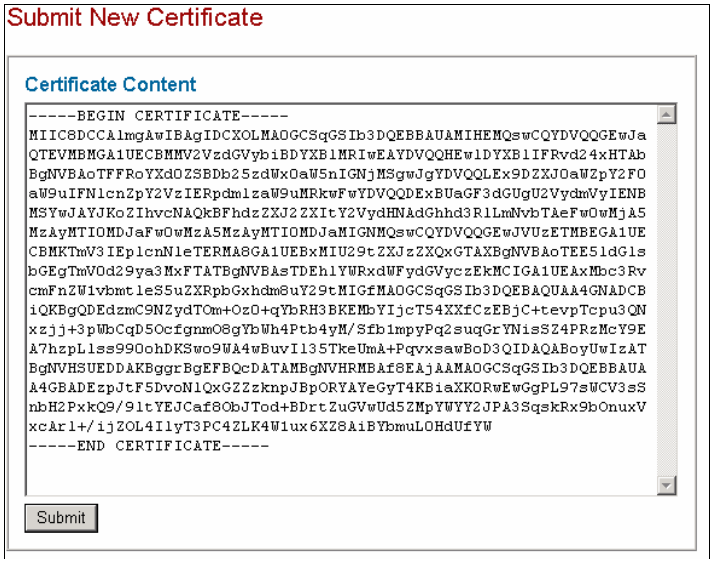


Figure 21 Certificate Content Field

3 Click *Submit*.

The Certificate Verification Window appears similar to the one shown in Figure 22.

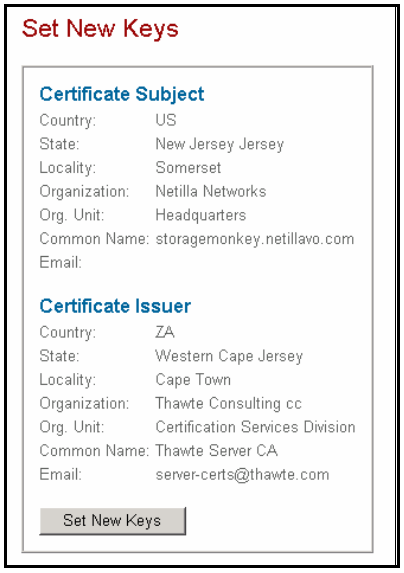


Figure 22 Certificate Verification Window

4 Click *Set New Keys* to install the certificate.

If you receive a "Check With Private Key" error message, refer to "Appendix A: Troubleshooting" on page 225.

Importing an Existing Server Certificate from a CA

This feature provides you with the tools needed to install a digital certificate and key that were generated on a server other than the NSP itself. Loading an Existing Cert is different from the previous portion in that the private key needs to also be uploaded since the original CSR was not generated from the NSP.

To load an existing certificate, do the following.

1 From the Administrator Site, click *System Configuration*, and then click *SSL*. From the SSL menu, click *Load Existing Cert*.

2 Copy the private key and certificate into the fields provided.

Figure 23 Private Key and Certificate Fields

3 Click *Submit*. The Certificate Verification page appears.

4 Click *Set New Keys* to install the certificate.

If you receive a "Check With Private Key" error message, refer to "Appendix A: Troubleshooting" on page 225.

Generating a Self-Signed Certificate

You can generate a self-signed certificate on the NSP. A self-signed certificate is not automatically recognized by users' browsers. If you connect to an NSP without a CA-signed certificate, a warning message informs you that the certificate has not been signed by a recognized authority.

It is highly recommended that you do not use self-signed certificates in a production environment as they represent a significant security risk. A valid certificate should be obtained from a recognized CA.

Figure 24 Security Warning Message

To generate a self-signed certificate on your NSP, do the following.

1 From the Administrator Site, click *SSL* and then *Generate Self-Signed*.

The only option available is the *Generate* button as shown in Figure 25.

Figure 25 Generate Self-Signed Certificate Page

2 Click *Generate* to create a new private key and certificate set.

WARNING: *Take extreme caution when using this feature. If your NSP already has a valid Private Key and Certificate installed, they will be overwritten by this action.*

Next you are presented with the information of the new key and certificate being generated.

3 Click *Set New Keys* to commit the changes.

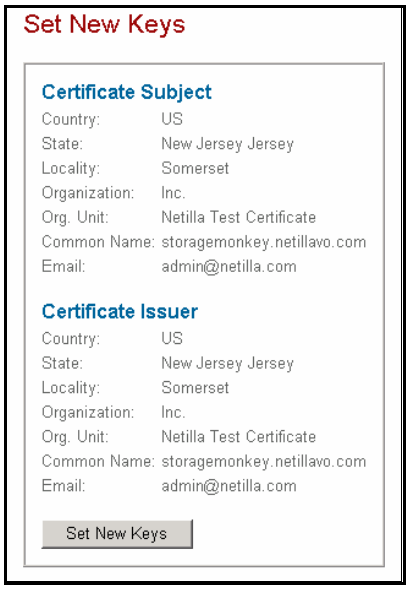


Figure 26 Set New Keys Page

Installing a Root CA

By default, the NSP has installed a list of CAs whose signatures it automatically accepts. The NSP prevents you from submitting and installing a certificate from an authorizing CA that is not in the list. To add a CA to the NSP's list, the root certificate of the issuing authority needs to be installed on the NSP before the server certificate is installed. If the NSP is being installed in an network that has its own private public key infrastructure, you will need to add that CA.

If the root CA that issued your certificate is not one of the CAs listed on the NSP, then you must install it. Also, if you are requiring client side certificate verification, then the root CA used for client verification must be installed on the NSP.

This section describes how to determine whether your root CA is installed on the NSP and if necessary, how to install the root CA. In addition, this section describes how to determine whether the client's root certificate is installed in the client's Web browser and, if necessary, how to install it.

Refer to the applicable section.

- **Installing a Root CA on the NSP**
- **Verifying Root CA is Installed in Web Browser**

Installing a Root CA on the NSP

To install a root CA on the NSP, follow the steps below.

1. From the Administrator Site, click *System Configuration* and then *SSL*.
2. From the SSL submenu, click *CA Certificates* and then click *View Existing*.
3. Verify that the root certificate of the CA that was used to sign the client-side certificates is installed.

4 If the Signing Authority is not listed, click *CA Certificates*, and then click *Upload New*.

5 Paste the contents of the CA root certificate in the field provided as shown in Figure 27.

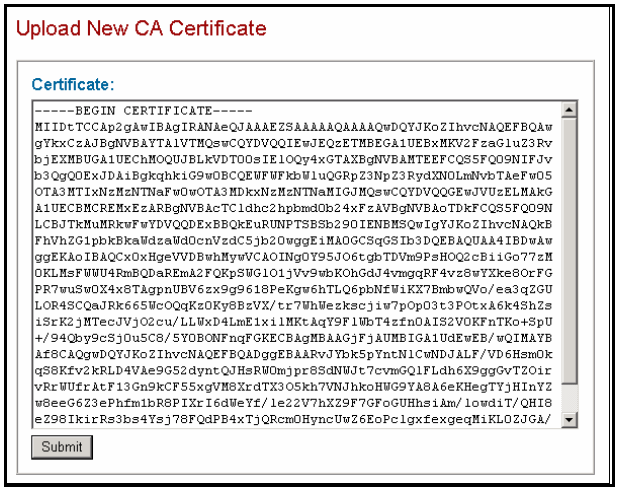


Figure 27 Upload New CA Certificate Page

6 Click *Submit*.

The new CA appears in the list of recognized authorities.

Setting Up Client Verification

The client verification via certificate option provides an additional layer of security. Client certificates are encrypted, digital files that contain personal identification. Similar to conventional forms of identification, client certificates enable the NSP to authenticate the identity of a user before letting that user log on.

For security purposes, the individual that administers client verification should posses a high level of PKI and SSL expertise.

About Client Verification

For each client session request, the server first asks the client to send its client certificate for verification. If the client certificate authenticates correctly against the server, then the session is granted. If not, the session is terminated and you will not see the log in page.

Client certificates are acquired from a CA. Before issuing a certificate, the CA requires you to provide identification information, such as a name, address, and organization. The extent of this information can vary with the identification assurance requirements of the certificate. If you need a certificate to provide absolute assurance about your identity, then the certificate authority may require further information. To obtain a list of identification assurance requirements contact your certificate authority.

Main Steps for Configuring Client Verification

- Verify that the root CA used for client verification is installed on the NSP.
- Verify that the root CA used for client verification is installed in the Web browser.

- Install client certificate in each Web browser that will attempt to connect to the NSP.

Verifying Root CA is Installed in Web Browser

This section describes how to verify that the CA for the client is listed as one of the trusted root certification authorities in the Web browser using Internet Explorer.

For Microsoft Internet Explorer Web Browsers (Versions 6.0 and higher for Win32)

Ensure that the CA for the client is listed as a one of the trusted root certification authorities in the browser as follows.

1 Launch Internet Explorer (IE) and then click *Tools*, and then *Internet options*.The Internet Properties window opens.

2 Click the *Content* tab.

3 Click *Certificates...*as shown in Figure 28.

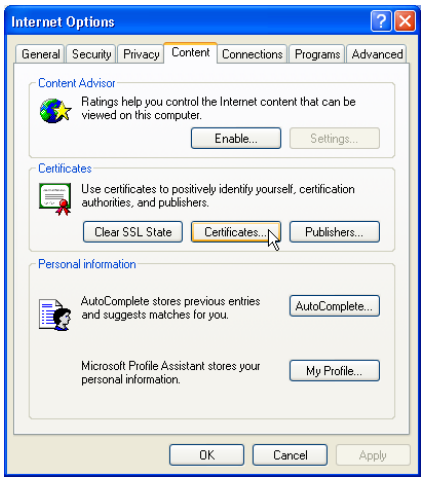


Figure 28 Internet Properties Content Tab

The Certificates window opens.

4 Click the Trusted Root Certification Authorities tab, as shown in Figure 29.

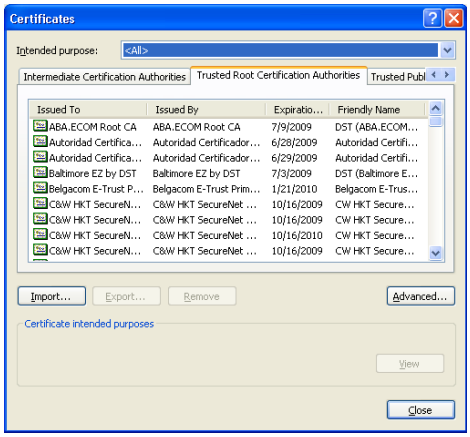


Figure 29 Trusted Root Certification Authorities

5 Scroll through the list and locate your CA.

If the CA that issued the client certificate is not listed, the root CA must be installed before proceeding to installing the client certificate.

Installing the Root CA For Internet Explorer Users

1 From the Tools menu, select *Internet Options* and then select the *Content* tab.

2 Click *Certificates* and then click *Trusted Root Certification Authorities*.

3 Click *Import…*

4 The Certificate Import Wizard guides you through the rest of the process for importing the root CA.

Go on to “Installing the Client Side Certificate For Internet Explorer Users” on page 36.

Installing the Client Side Certificate For Internet Explorer Users

After verifying that the CA issuing your client side certificate is listed as a trusted root certification authority, proceed to installing the client side certificate.

To install a client side certificate using Internet Explorer you must have the certificate file in a ".pfx" or “.p12” format.

1 From the Tools menu, select *Internet Options* and then select the *Content* tab.

2 Click *Certificates* and then click the *Personal* tab.

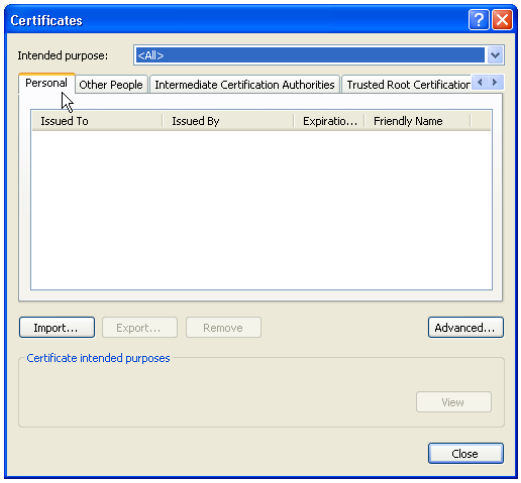


Figure 30 IE Properties Personal Tab

3 Click *Import*.

4 The Certificate Import Wizard guides you through the rest of the process for importing the root CA.

Upon a successful installation of the Root CA and the Client Side Certificate, proceed to “Verifying the Root CA on the NSP”.

Setting up Client Verification on the NSP

To set up client verification, do the following.

1 From the Administrator Site, click *System Configuration*, and then *SSL*.

2 From the SSL menu, click *CA Certificates*, and then click *Client Verification*.

3 Select the desired signing authority from the drop-down menu.

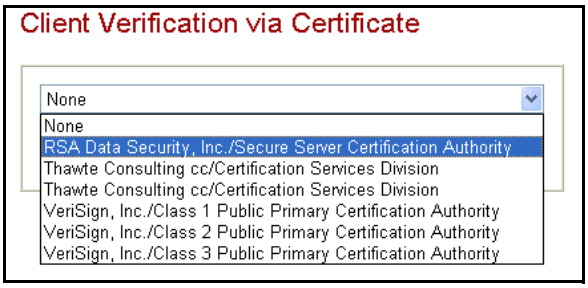


Figure 31 Client Verification Set Up Page

4 Click *Submit*.

***WARNING**: Do not close your browser or log out of the Netilla configuration site until you have verified that client verification via certificate is working properly. If you make an error and close the browser before testing, you could lock yourself out of the NSP. If this happens you will need to gain console access to the NSP. For details, refer to* *"Accessing the NSP's Serial Console" on page 261.*

Testing Client Verification via Certificate

1 Launch a separate browser window.

2 Access the NSP by entering the URL of your NSP (i.e., https://your-host-name.netillavo.com.

The Client Authentication window opens, as shown in Figure 30.

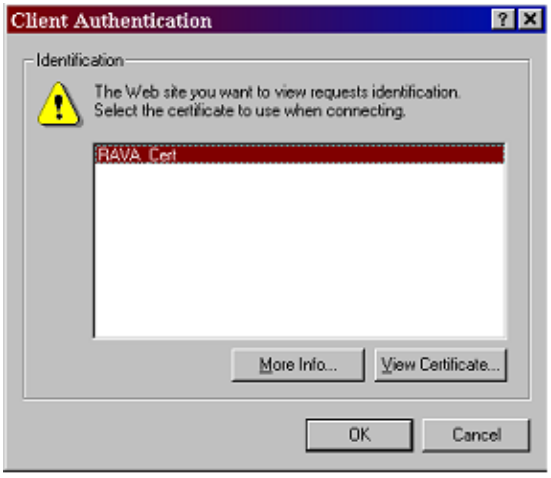


Figure 32 Client Authentication Window

3 Select the certificate for authentication and click *OK*.

The NSP Login Page opens.

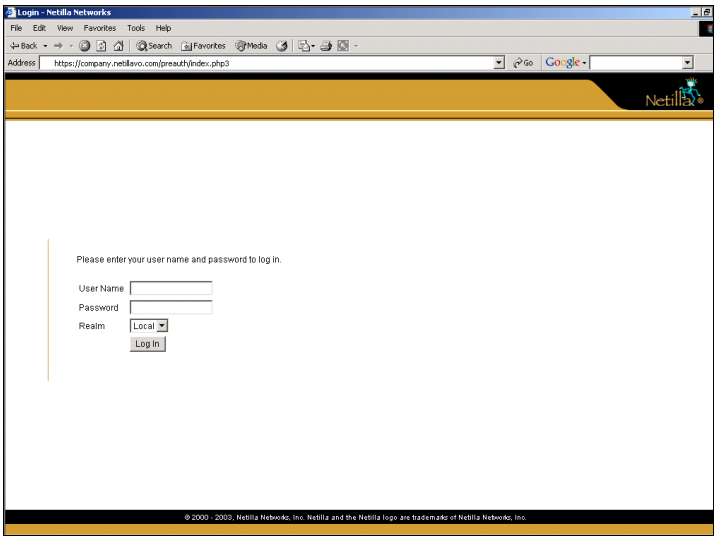


Figure 33 NSP Login Page

4 Enter your User name and Password and then select the appropriate Realm.

5 Click *Log In*.

Managing Certificates from Certificate Authorities

This section describes the procedures for removing Certificate Authorities (CA) from the list of existing CAs, and setting up Client Verification via Certificate.

To add a certificate authority, refer to "Installing a Root CA on the NSP" on page 33.

Deleting a Root Certificate

You can also remove unnecessary CAs from the NSP. If you install a CA and later find out that the particular CA already exists you can delete the duplicate to eliminate confusion. Alternatively, you may decide to keep only the CAs that are useful and delete all others.

To delete a root certificate, do the following

1 From the Administrator Site, click *System Configuration*, and then click *SSL*.

2 From the SSL menu, click *CA Certificates*, and then click *View Existing*.

3 Select the certificates that you wish to delete by clicking on the check box next to the CAs name as shown in Figure 34.

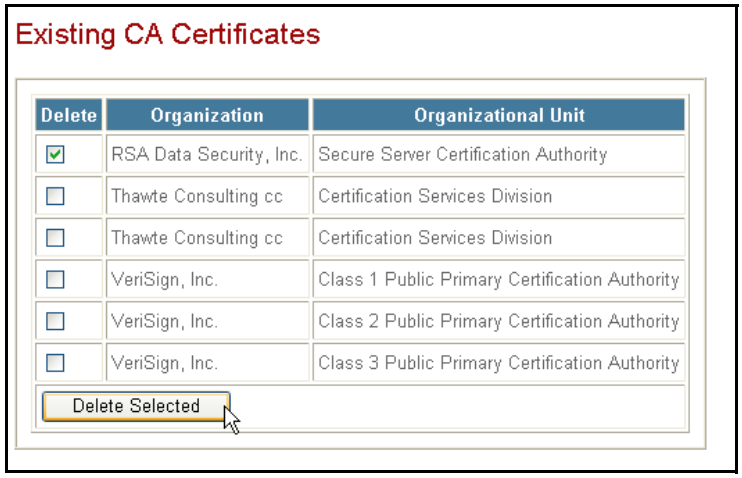


Figure 34 Existing CA Certificates Page

4 Click *Delete Selected* and the CA root certificate is deleted from the NSP.

You are not allowed to remove the Certificate Authority that issued the currently installed server certificate. For example, if the current certificate installed on the NSP is issued by Thawte Server you will not be able to delete Thawte Server CA.

SSL Browser Cryptographic Level Checking

You can specify what occurs if a client's web browser does not support 128-bit or higher encryption.

1 From the SSL submenu, click *Browser Settings*.

2 Select one of the following options.

- Warn user and let the user decide whether or not to proceed to the Web office
- Deny access to the Web office
- Do not ask the user to decide whether or not to proceed. Just allow access.

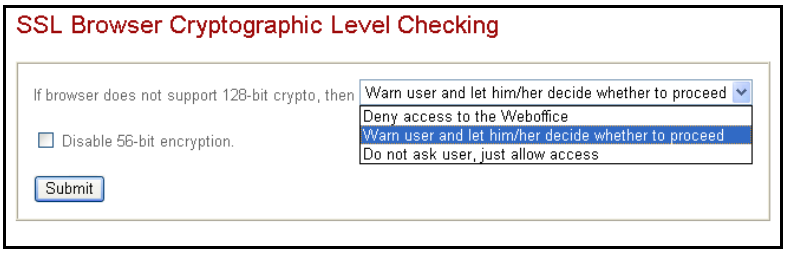


Figure 35 SSL Browser Cryptographic Level Checking Page

3 For **Disable 56-bit encryption**, check this box if you do not want the software to negotiate 56-bit encryption.

4 Click *Submit*.

Backing up and Restoring NSP Profiles

The Backup/Restore feature allows you to save the current NSP configuration settings and restore those settings at a future time. With the Backup/Restore feature, applications, application servers, user accounts and permissions, Netilla Licenses, and your customized GUI and logos can be safely backed-up and later restored.

You should back up the NSP configuration settings every time you make changes.

Backing Up and Restoring Your Current Settings

To backup and restore current settings, do the following.

1 From the Administrator Site, click *System Configuration* and then click *Backup/Restore*, as shown in Figure 36.

Figure 36 Backup / Restore Submenu

The Backup and Restore window opens, as shown in Figure 37.

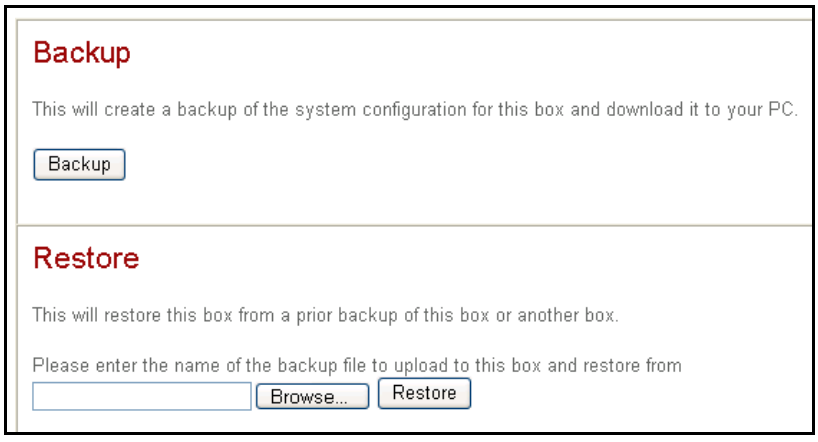


Figure 37 Backup and Restore Settings Window

2 Click *Backup*. You are prompted to either open or save the file.

3 Click *Save*.

This completes the Backup procedure.

Using the Restore Feature

To restore the configuration settings file that you have previously backed up, do the following.

1 From the Administrator Site, click *System Configuration* and then click *Backup/Restore*.

2 Click *Browse* to locate your previously created backup file. Select that file and then click *Open*.

The file is displayed in the Restore text box.

3 Verify the file path and name and click *Restore*.

The Restore process begins and is usually done within 5 minutes. However, this process may take longer depending on the type of NSP you have and the size of the data store. When complete, you are presented with a Restore Complete message.

4 Log out of the NSP completely.

5 Log in to the NSP to verify your restored changes.

Localizing the End User GUI

You can change the language that the end user GUI displays using the locale menu option. Currently, the end user GUI can be localized into Japanese. Note that this does not affect the language of the Administrator Site with the exception of the Properties menu where you can change the settings of the administrator account that you are currently logged in as (i.e., admin, radmin or maint).

To change the language of the end user GUI, do the following:

1 From the Administrator Site, click *System Configuration* and then click *Locale*.

The Locale Settings page appears as shown in Figure 38.

Figure 38 Local Settings Page

2 Select the preferred language and then click *Submit*.

3 Managing Authentication Settings

This section describes the procedures for managing authentication settings. The following topics are discussed.

- Understanding Realms on the NSP
- Creating a Realm
- Creating an Authentication Stage Within a Realm
- Managing Realms
- Creating an Internal Authentication Store

Understanding Realms on the NSP

This section presents a conceptual overview of realms and their implementation on the NSP. A realm is a means of grouping users with the same authentication and application policies. A user's association with a realm determines the user's method of authentication, and also determines the authentication server(s) against which a user's credentials are validated.

About the Local Realm

By default, the NSP is configured with a realm named local that uses internal authentication and contains the following administrative accounts.

- *admin: The* admin account is the highest privilege level.
- *radmin* (or reseller administrator): An account created for managing the service in the field.
- *maint:* An account created for general maintenance and has the least number of privileges.

For more information about NSP administrator accounts, refer to "Modifying NSP Administrator Accounts" on page 149.

Adding Authentication Stages to the Local Realm

For stronger administrator authentication, you can add more authentication stages to the local realm such as RADIUS or SMB. For details, refer to "Creating an Authentication Stage Within a Realm" on page 47.

Realm Considerations

Several items to consider when configuring realms with the NSP are listed below.

- To log in, every user must belong to one realm configured in the NSP.
- A user can only exist in one realm. Duplicate names in two realms are treated as unique users.
- You can create a maximum of 1000 authentication realms on one NSP.

- All members of the realm inherit all applications assigned to that realm.

Authentication Stages within Realms

Authentication stages are defined within a realm and are used to indicate the type of authentication server that validates a user's login credentials. Each defined authentication stage has two components, an authentication section and a policy section. The authentication section is required for any given stage. However, the policy definition is optional. Configuring policy enables the NSP to retrieve group membership information about users when they log in to the NSP.

Types of Authentication Stages within a Realm

Refer to Table 6 for a list of the types of authentication stages that can exist within a realm.

Table 6 Types of Authentication Stages within a Realm

Authentication Stage	Description
RADIUS	The user account is maintained on the RADIUS server.
SMB	The user account information is maintained in a Windows NT/2000 Domain Controller.
SecurID	The user account information is held on an RSA ACE server.
Kerberos	The user account information is held on a Windows 2000 Active Directory server.
Internal	The user account information is cryptographically maintained on the NSP itself. Internal user account information is hashed in a form where the original password cannot be recovered.

Multiple Authentication Stages Within a Realm

For added security, you can set up multiple authentication stages within the same realm. When a user logs in to a realm that has been set up with multiple authentication stages, successful authentication must occur at every stage within that realm before access to the NSP is allowed. This is an important consideration when creating different stages within a realm.

A maximum of 10 different authentication stages can exist within a realm.

Logging in as Multiple Users

By default, realms with multiple stages are configured so that users log in with the same username for every stage. The user is challenged for username and password for the first stage, and then prompted only for his password at each subsequent authentication stage (i.e., the username is carried forward from stage to stage). This default arrangement, when the user name is the same between stages, provides a level of user convenience.

Alternatively, realms can be configured to force users to log in using different user names as well as passwords for every stage. In effect, this allows a user to log in under different user names for the same session. There are several advantages to this arrangement, including:

- Users can access distinct systems (i.e., a UNIX server, and Windows terminal server, etc.) where they hold different accounts within the same Netilla session.
- Increased security.

- Administrators can log in with different administrative privilege levels for various administration needs, such as system testing.

This feature is configured when you create additional authentication stages within a realm. The Authentication Stage properties page has a check box labeled *Use same username as previous stage*, explained later in "Creating an Authentication Stage Within a Realm" on page 47.

Profiles and Multiple Users

Note that when a user logs in to the NSP with multiple user accounts, the profile associated with the first user account will be used to assign policies. This first user account will subsequently inherit the applications and group membership information from the accounts on the secondary stages, but only for the life of that session.

For example, if a user logs into the NSP as *user-one* for the first stage and as *user-two* for the second stage, *user-one* inherits all applications and group membership that has been assigned to *user-two*.

When viewed from the groups option on the NSP, the groups for the second user appear under the profile of the primary user.

About Policy

You have the option of configuring policy as part of an authentication stage within a realm. Configuring policy enables the NSP to retrieve group membership information about users when they log in to the NSP. For details on policy configuration related to authentication, refer to "Configuring Policy in an Authentication Stage" on page 56.

Creating a Realm

This section describes the steps required to create a realm. To create a new realm, do the following.

1 Log in to the NSP as the *radmin* user.

Make sure the realm name field is set to *Local*, or type *Local* in the Realm name field if your platform is configured to hide the realm drop-down list box.

To change the appearance of the Realm field, refer to "Changing the Realm Field Appearance" on page 62.

2 From the Administrator Site, click *System Configuration* and then click *Authentication Settings*, as shown in Figure 39.

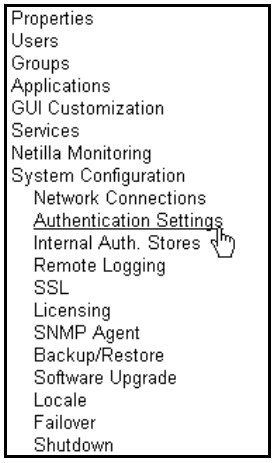


Figure 39 Authentication Settings Submenu

The Authentication Settings page opens.

Figure 40 Authentication Settings

3 Click *Create a New Realm*.

4 Enter a name to identify the authentication realm.

The default is *Realm* # where # is the number of existing realms plus one.

5 Click *Submit*.

The Authentication Realm window opens. The page refreshes. Verify your changes.

6 Once your changes are verified, click *Ready to commit changes* located at the bottom of the page.

Figure 41 Commit Changes

7 Click *Apply*.

The new realm appears in the drop-down menu at the log in page upon the next connection to the NSP.

To complete the creation of this realm, you must define at least one authentication stage within it. Go on to “Creating an Authentication Stage Within a Realm” on page 47.

About International Characters and Realms

The NSP provides support for international characters. In particular, the NSP supports Unicode (UTF-8) encoding.

Note that there are several considerations regarding the use of international characters and realm implementation, described in Table 7.

Table 7 Handling of International Characters on the NSP

Authentication Type	Handling of International Characters
RADIUS	International characters are supported if the RADIUS Server matches the language of the credentials forwarded by the NSP.
SecurID	International characters are supported if the ACE Server matches the language of the credentials forwarded by the NSP.
Kerberos	International characters are supported if the Kerberos server matches the language of the credentials forwarded by the NSP.
Local	User names on the NSP are required to be US ASCII text. Passwords with international characters are supported.

Creating an Authentication Stage Within a Realm

This section describes how to create an authentication stage within a realm. The steps for creating an authentication stage vary depending on what type of authentication you want to use. Refer to the appropriate section.

- “Creating a RADIUS Authentication Stage” on page 47
- “Creating an SMB Authentication Stage” on page 50
- “Creating a SecurID Authentication Stage” on page 51
- “Creating a Kerberos Authentication Stage” on page 53
- “Creating an Internal Authentication Stage” on page 55

Creating a RADIUS Authentication Stage

Before you begin, have the following RADIUS server information ready:

Table 8 RADIUS Field Information

RADIUS Field	Description
Primary RADIUS Server IP	IP address of RADIUS server.
Primary RADIUS Secret	Enter the Shared Secret configured on the RADIUS server in this field. The RADIUS Secret is case-sensitive and must match the RADIUS server secret exactly.
Primary RADIUS Port	Enter the port number of the RADIUS server. It is usually 1812 or 1645.
Primary RADIUS timeout	60 seconds is recommended.
Initial password	(Optional) If using challenge response, you can preconfigure an initial password for use until the RADIUS server sends the challenge. Alternatively, you can configure the Empty Password field.
Empty First Password	(Optional) If using challenge response, check this box to eliminate the use of the first password.
Secondary RADIUS Server IP	(Optional) IP address of backup RADIUS server.

Table 8 RADIUS Field Information

RADIUS Field	Description
Secondary RADIUS Port	(Optional) Port of backup RADIUS server.
Initial password	(Optional) If using challenge response, you can preconfigure an initial password for use until the RADIUS server sends the challenge. Alternatively, you can configure the Empty Password field.
Empty First Password	(Optional) If using challenge response, check this box to eliminate the use of the first password.

To create a RADIUS authentication stage, do the following.

1 Choose *RADIUS* from the Stage Type drop down list box located under *Create New Authentication Stage*.

2 Click *Submit*, as shown in Figure 42.

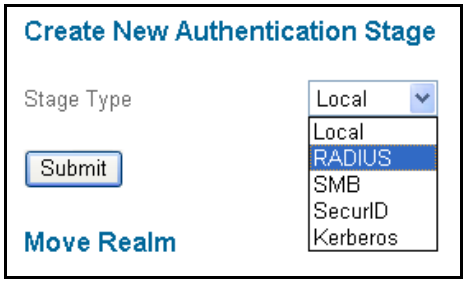


Figure 42 Create a New Authentication Stage

The Authentication Stage properties page opens, as shown in Figure 43.

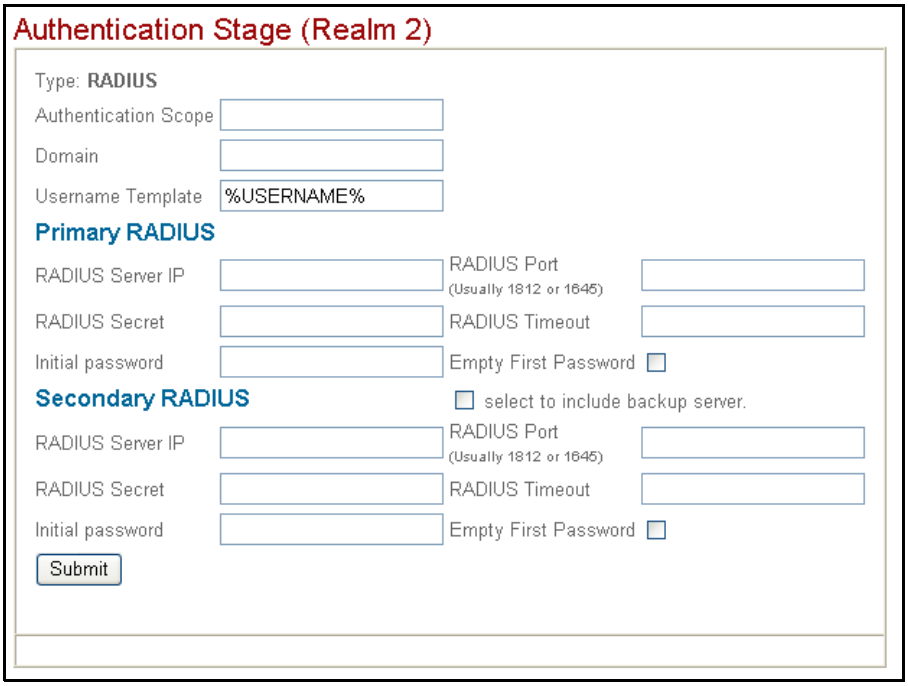


Figure 43 RADIUS Authentication Stage Properties

3 (Optional) Enter the **Authentication Scope** for the Local Authentication Stage. Use this field to create a label that will link these authentication stage credentials to the application that needs them.

After a user's credentials are validated against the authentication server as part of this authentication stage, the Authentication Scope feature will forward these credentials to the application that the user will subsequently access. This eliminates the user from being prompted for a username and password when launching an application.

To use this feature, enter an arbitrary name in the Authentication Scope field, such as the name of the realm. Note the exact name entered here must match the scope used when configuring applications.

If you do not define an Authentication Scope, all users assigned to this realm will be prompted for user credentials each time an application is launched.

4 (Optional) Enter the domain in the **Domain** field.

The value entered in the Domain field is sent in the RDP authentication request to the Terminal Server. This allows a user's account information to be passed from a trusted domain through to the terminal server, while adding the trusted domain name in the request. This is similar to the method of choosing a Domain name from the drop down menu when logging in directly to a server that has trusts with other domains.

If this field is not used, or has a value that doesn't match any domains associated with the Terminal Server, then the Terminal Server assumes the default domain that is associated with it.

5 The **Use same username as previous stage** check box is displayed when an authentication stage of any type has already been created for this realm. Check this box if you want the username entered in the previous authentication stage to be used for this authentication stage requiring users to enter only a password. Uncheck this box if you want users to enter a username as well as a password for this authentication stage.

6 The **Username template** field is used to prefix or postfix a string to the username. This removes the need for endusers to include this information when logging in.

For example, if users access a RADIUS server that requires postpending a Realm for authentication (i.e., **username@realm123**), the Username template field will concatenate the Realm name to the username automatically. In this case, you would add **@realm123** to the**%USERNAME%** field (i.e.,**%USERNAME%@realm123)**.

7 Enter the RADIUS information described in Table 8.

If you are using challenge response and have configured either the Initial Password or Empty Password fields, you can prevent the display of the Password field on the NSP's log in page. Refer to "Removing Password Field from Log In Page" on page 59 for details.

8 To configure a backup RADIUS server, check the box labeled **select to include backup server**.

9 (Optional) For **Secondary RADIUS**, enter the backup RADIUS information described in Table 8.

10 Click *Submit*.

The page refreshes. Verify your changes.

11 Once your changes are verified, click *Ready to commit changes* located at the bottom of the page.

Ready to commit changes *appears each time changes have been made but have not been committed.*

12 Click *Apply.*

If you want to configure policy in this authentication stage, go on to "Configuring Policy in an Authentication Stage" on page 56.

Creating an SMB Authentication Stage

Before you begin, have the following SMB server information ready.

- Primary Name: NetBIOS name of your primary SMB server
- Primary IP: IP address of your primary SMB server
- Secondary Name: Name of your secondary SMB server (optional)
- Secondary IP: IP address of your secondary SMB server (optional)

To create an SMB authentication stage, do the following.

1 Choose SMB from the Stage Type drop down list box located under *Create New Authentication Stage*.

2 Click *Submit,* as shown in Figure 44.

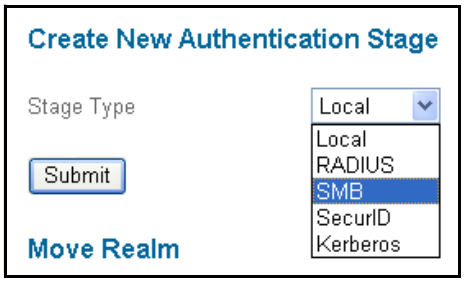


Figure 44 Create a New Authentication Stage

The Authentication Stage properties page opens, as shown in Figure 45.

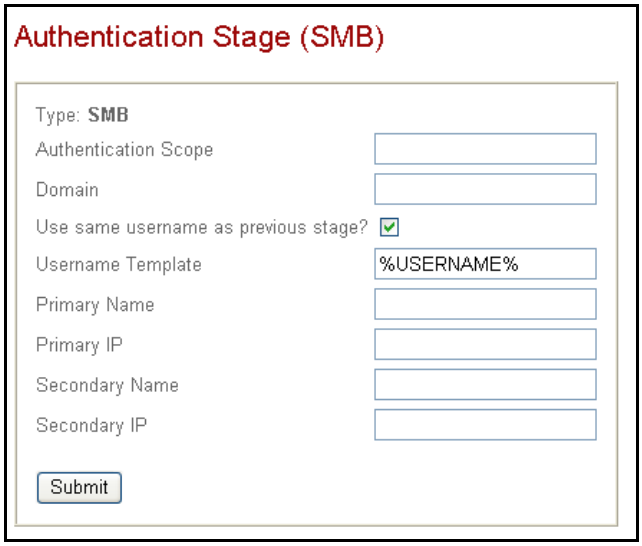


Figure 45 SMB Authentication Stage Properties

3 (Optional) Enter the **Authentication Scope** for the SMB authentication stage. Use this field to create a label that will link these authentication stage credentials to the application that needs them.

After a user's credentials are validated against the authentication server as part of this authentication stage, the Authentication Scope feature will forward these credentials to the application that the user will subsequently access. This eliminates the user from being prompted for a username and password when launching an application.

To use this feature, enter an arbitrary name in the Authentication Scope field, such as the name of the realm. Note the exact name entered here must match the scope used when configuring applications.

If you do not define an Authentication Scope, all users assigned to this realm will be prompted for user credentials each time an application is launched.

4 (Optional) Enter the domain in the **Domain** field.

The value entered in the Domain field is sent in the RDP authentication request to the Terminal Server. This allows a user's account information to be passed from a trusted domain through to the terminal server, while adding the trusted domain name in the request. This is similar to the method of choosing a Domain name from the drop down list when logging in directly to a server that has trusts with other domains.

If this field is not used, or has a value that doesn't match any domains associated with the Terminal Server, then the Terminal Server assumes the default domain that is associated with it.

5 The **Use same username as previous stage** check box is displayed when an authentication stage of any type has already been created for this realm. Check this box if you want the username entered in the previous authentication stage to be used for this authentication stage requiring users to enter only a password. Uncheck this box if you want users to enter a username as well as a password for this authentication stage.

6 The **Username template** field is used to prefix or postfix a string to the username. This removes the need for endusers to include this information when logging in.

For example, if users access a RADIUS server that requires postpending a Realm for authentication (i.e., **username@realm123**), the Username template field will concatenate the Realm name to the username automatically. In this case, you would add **@realm123** to the**%USERNAME%** field (i.e.,**%USERNAME%@realm123)**.

7 Enter the SMB information.

8 Click *Submit*.

The page refreshes. Verify your changes.

9 Once your changes are verified, click *Ready to commit changes* located at the bottom of the page.

Ready to commit changes *appears each time changes have been made but have not been committed*.

10 Click *Apply*.

If you want to configure policy in this authentication stage, go on to "Configuring Policy in an Authentication Stage" on page 56.

Creating a SecurID Authentication Stage

Before you begin, have the following SecurID information ready:

- ***ACE Config File***. You will need to know the location of this file. A browse button is provided.

To create a SecurID authentication stage, do the following.

1 Choose *SecurID* from the Stage Type drop down list box located under *Create New Authentication Stage*.

2 Click *Submit*, as shown in Figure 46.

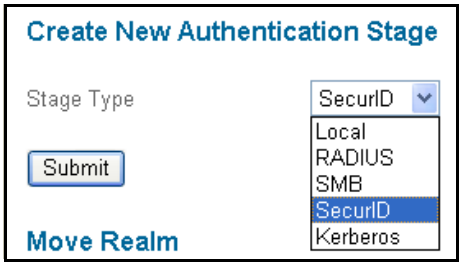


Figure 46 Create a New Authentication Stage

The Authentication Stage properties page opens, as shown in Figure 47.

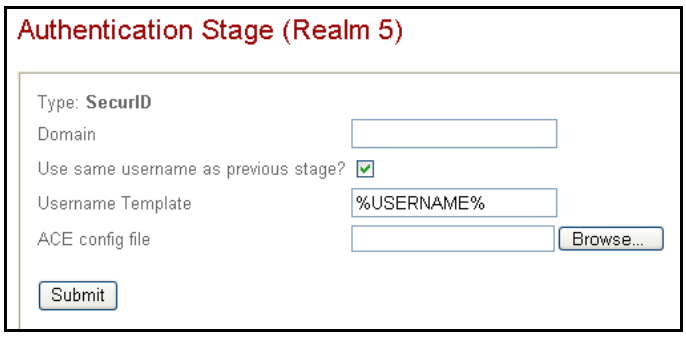


Figure 47 SecurID Authentication Stage Properties

3 (Optional) Enter the domain in the **Domain** field.

The value entered in the Domain field is sent in the RDP authentication request to the Terminal Server. This allows a user's account information to be passed from a trusted domain through to the terminal server, while adding the trusted domain name in the request. This is similar to the method of choosing a Domain name from the drop down menu when logging in directly to a server that has trusts with other domains.

If this field is not used, or has a value that does not match any domains associated with the Terminal Server, then the Terminal Server assumes the default domain that is associated with it.

4 The **Use same username as previous stage** check box is displayed when an authentication stage of any type has already been created for this realm. Check this box if you want the username entered in the previous authentication stage to be used for this authentication stage requiring users to enter only a password. Uncheck this box if you want users to enter a username as well as a password for this authentication stage.

5 The **Username template** field is used to prefix or postfix a string to the username. This removes the need for endusers to include this information when logging in.

For example, if users access a RADIUS server that requires postpending a Realm for authentication (i.e., **username@realm123**), the Username template field will concatenate the Realm name to the username

automatically. In this case, you would add **@realm123** to the **%USERNAME%** field (i.e.,**%USERNAME%@realm123)**.

6 Use the browse button to locate the ACE config file.

7 Click *Submit*.

The page refreshes. Verify your changes.

8 Once your changes are verified, click *Ready to commit changes* located at the bottom of the page.

Ready to commit changes *appears each time changes have been made but have not been committed.*

9 Click Apply.

If you want to configure policy in this authentication stage, go on to "Configuring Policy in an Authentication Stage" on page 56.

Creating a Kerberos Authentication Stage

Before you begin, have the following Kerberos information ready:

Table 9 Kerberos Field Descriptions

Kerberos Field	Description
Kerberos realm	Enter the realm name of the Kerberos Server. In Windows server environments, this entry must be capitalized. In Windows 2000, the realm would be the WIN2k Domain name (for example, *NETILLA.NET). See Microsoft Knowledge Base Article 248807 for more details.*
KDC server	Enter the IP address of the KDC server.
Kerberos Domain	Enter the domain name in which the Kerberos server exists. In Windows 2000 it would be the domain name (for example, netilla.net) and must be all lower case letters.
KDC port	Enter the UDP port that is used for communication between the NSP and the Kerberos Server.

The NTP Time Server parameter (located under the System Configuration menu) should be set to eliminate errors relating to clock skew. Refer to "Configuring Network Time Service (NTP)" on page 21 for details.

To create a Kerberos authentication stage, do the following.

1 Choose *Kerberos* from the Stage Type drop down list box located under *Create New Authentication Stage*.

2 Click *Submit*, as shown in Figure 48.

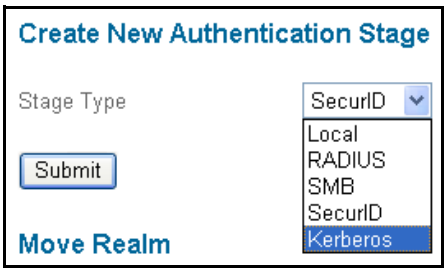


Figure 48 Create New Authentication Stage

The Authentication Stage properties page opens, as shown in Figure 49.

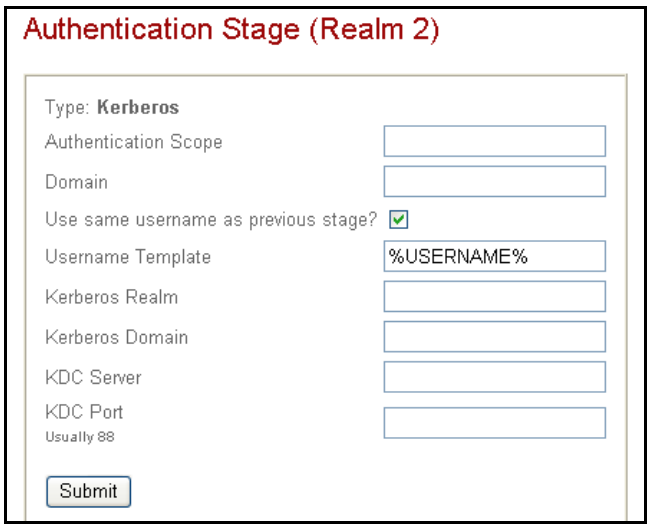


Figure 49 Kerberos Authentication Stage Properties

3 (Optional) Enter the **Authentication Scope** for the Kerberos authentication stage. Use this field to create a label that will link these authentication stage credentials to the application that needs them.

After a user's credentials are validated against the authentication server as part of this authentication stage, the Authentication Scope feature will forward these credentials to the application that the user will subsequently access. This eliminates the user from being prompted for a username and password when launching an application.

To use this feature, enter an arbitrary name in the Authentication Scope field, such as the name of the realm. Note the exact name entered here must match the scope used when configuring applications.

If you do not define an Authentication Scope, all users assigned to this realm will be prompted for user credentials each time an application is launched.

4 (Optional) Enter the domain in the **Domain** field.

The value entered in the Domain field is sent in the RDP authentication request to the Terminal Server. This allows a user's account information to be passed from a trusted domain through to the terminal server, while adding the trusted domain name in the request. This is similar to the method of choosing a Domain name from the drop down list when logging in directly to a server that has trusts with other domains.

If this field is not used, or has a value that doesn't match any domains associated with the Terminal Server, then the Terminal Server assumes the default domain that is associated with it.

5 The **Use same user name as previous stage** check box is displayed when an authentication stage of any type has already been created for this realm. Check this box if you want the username entered in the previous authentication stage to be used for this authentication stage requiring users to enter only a password. Uncheck this box if you want users to enter a username as well as a password for this authentication stage.

6 The **Username template** field is used to prefix or postfix a string to the username. This removes the need for endusers to include this information when logging in.

For example, if users access a RADIUS server that requires postpending a Realm for authentication (i.e., **username@realm123**), the Username template field will concatenate the Realm name to the username automatically. In this case, you would add **@realm123** to the**%USERNAME%** field (i.e.,**%USERNAME%@realm123)**.

7 Enter the Kerberos information described in Table 9.

8 Click *Submit*.

The page refreshes. Verify your changes.

9 Once your changes are verified, click *Ready to commit changes* located at the bottom of the page.

Ready to commit changes *appears each time changes have been made but have not been committed*.

10 Click *Apply*.

If you want to configure policy in this authentication stage, go on to "Configuring Policy in an Authentication Stage" on page 56.

Creating an Internal Authentication Stage

The authentication stage named Internal uses the NSP's authentication. Internal authentication is used for the NSP's administrator accounts and is useful for users that do not use an external authentication server.

To create an internal authentication stage, do the following.

1 Choose *Internal* from the Stage Type drop down list box located under *Create New Authentication Stage*.

2 Click *Submit*, as shown in Figure 50.

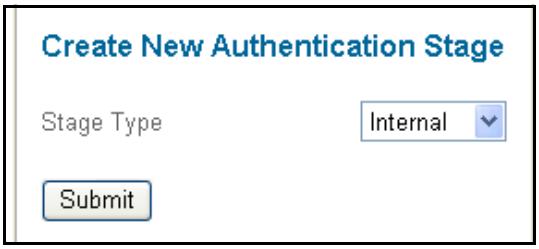


Figure 50 Create a New Internal Authentication Stage

The Authentication Stage properties page opens, as shown in Figure 51.

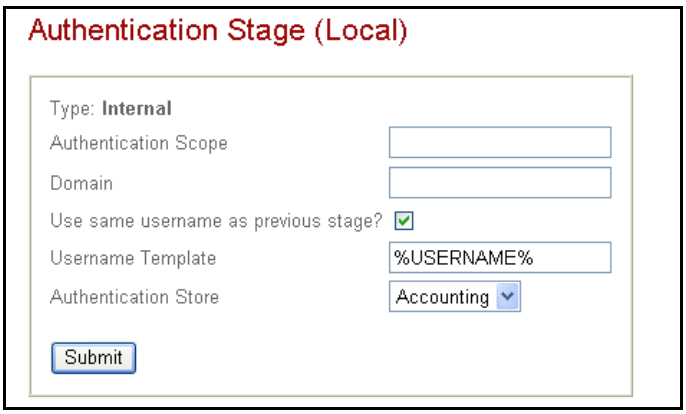


Figure 51 Authentication Stage Properties for Local Page

3 (Optional) Enter the **Authentication Scope** for the Local Authentication Stage. Use this field to create a label that will link these authentication stage credentials to the application that needs them.

After a user's credentials are validated against the authentication server as part of this authentication stage, the Authentication Scope feature will forward these credentials to the application that the user will subsequently access. This eliminates the user from being prompted for a username and password when launching an application.

To use this feature, enter an arbitrary name in the Authentication Scope field, such as the name of the realm. Note the exact name entered here must match the scope used when configuring applications.

If you do not define an Authentication Scope, all users assigned to this realm will be prompted for user credentials each time an application is launched.

4 (Optional) Enter the domain in the **Domain** field.

The value entered in the Domain field is sent in the RDP authentication request to the Terminal Server. This allows a user's account information to be passed from a trusted domain through to the terminal server, while adding the trusted domain name in the request. This is similar to the method of choosing a Domain name form the drop down list when logging in directly to a server that has trusts with other domains.

If this field is not used, or has a value that doesn't match any domains associated with the Terminal Server, then the Terminal Server assumes the default domain that is associated with it.

5 The **Username template** field is used to prefix or postfix a string to the username. This removes the need for endusers to include this information when logging in.

For example, if users access a RADIUS server that requires postpending a Realm for authentication (i.e., **username@realm123**), the Username template field will concatenate the Realm name to the username automatically. In this case, you would add **@realm123** to the**%USERNAME%** field (i.e.,**%USERNAME%@realm123)**.

6 For **Authentication Store**, select the name of the group of users that you want to associate with this authentication stage.

7 Click *Submit*.

The page refreshes. Verify your changes.

8 Once your changes are verified, click *Ready to commit changes* located at the bottom of the page.

9 Click *Apply.*

Configuring Policy in an Authentication Stage

You have the option of configuring policy in an authentication stage. Configuring policy enables the NSP to retrieve group membership information about users when they log in to the NSP. Group membership information can be used to determine which applications a user can access.

There are two types of policy you can add to an authentication stage, local or SMB.

To configure policy, do the following.

1 From the Administrator Site, click *System Configuration*.

2 Click *Authentication Settings* and then click the appropriate realm name.

3 From within that realm submenu, click the name of the authentication stage that you want to add policy to.

4 Click *Policy* as shown in Figure 52.

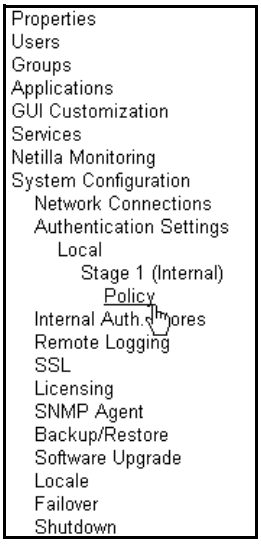


Figure 52 Authentication Stage Policy Configuration Location

5 The Policy Type drop-down menu shown in Figure 53 specifies the location of any policies to be applied to the user logging into the Realm.

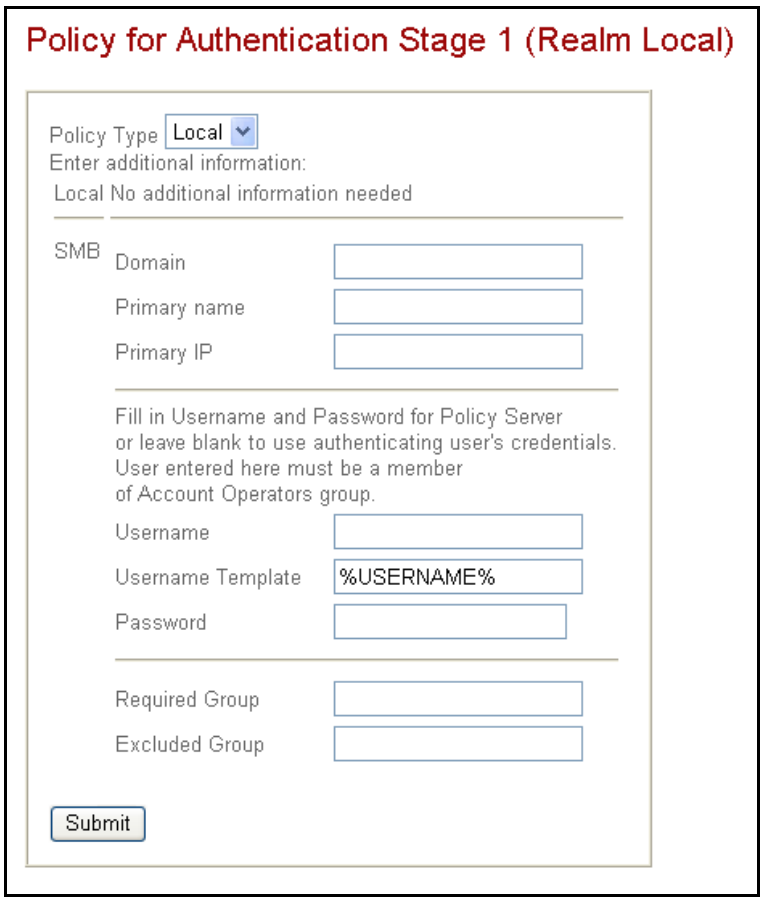


Figure 53 Authentication Policy Page

6 For SMB policy, indicate the **Domain** name.

7 Enter the **Primary name** (NetBIOS name of the Primary Domain Controller) and the **Primary IP** address (IP address of the Primary Domain Controller) in the appropriate fields.

8 The **Username** field allows you to select a user account that the NSP uses to access the user's group membership from the Domain Controller.

These fields are used when the user's NSP credentials are different than the credentials used to verify policy. The user account that you select should be created in the domain where the group membership information is stored.

9 The **Username template** field is used to prefix or postfix a string to the username. This removes the need for endusers to include this information when logging in.

For example, if users access a RADIUS server that requires postpending a Realm for authentication (i.e., **username@realm123**), the Username template field will concatenate the Realm name to the username automatically. In this case, you would add **@realm123** to the **%USERNAME%** field (i.e.,**%USERNAME%@realm123)**.

10 If you entered a Username as part of step 8, enter the **Password** associated with the username.

11 By default, domain authentication allows all domain users permission to log in to the NSP. Use the **Required Group** and **Excluded Group** fields to grant or deny access to the NSP.

Enter a group name in the Required Group field to allow only the domain users of a particular group to login.

Enter a group name in the Excluded Group field to allow all users permission to log into the NSP except members of the excluded group.

12 Click *Submit* to save the new settings to the authentication stage.

The page refreshes. Verify your changes.

13 Once your changes are verified, click *Ready to commit changes* located at the bottom of the page.

Ready to commit changes *appears each time changes have been made but have not been committed*.

14 Click *Apply*.

The new realm appears in the drop-down menu at the log in page upon the next connection to the NSP.

Removing Password Field from Log In Page

This section describes how to remove the password field from the login page.

Removing Password Field

To change prevent the password field from being displayed on the log in page, do the following.

1 From the Administration Site, click *System Configuration* and then click *Authentication Settings*.

2 Select *Password Input on Login Page*, as shown in Figure 56.

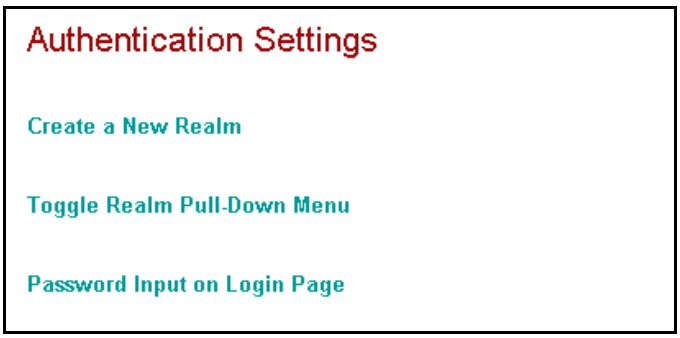


Figure 54 Authentication Realm Menu

3 The Password Input on Login Page appears, as shown in Figure 56.

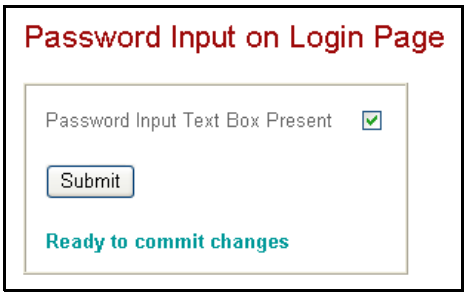


Figure 55 Password Input on Login Page Field

4 Click inside the check box to clear the check box.

5 Click *Submit*.

6 Click *Ready to Commit Changes* and then click the *Apply Changes* button.

Managing Realms

This section describes how to move realms, delete realms, and change the appearance of the Realm field. That is you can configure the NSP to present users with a text box to type in their realm name or present users with a drop down menu from which they select their realm name.

Moving Realms

To change the location of a realm in the list of realms, do the following.

1 From the Administration Site, click *System Configuration* and then click *Authentication Settings*.

2 Select the name of the realm that you want to move, as shown in Figure 56.

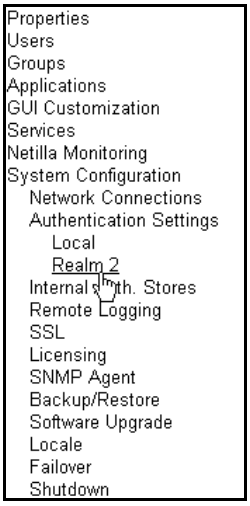


Figure 56 Authentication Realm Menu

The following page appears for that realm.

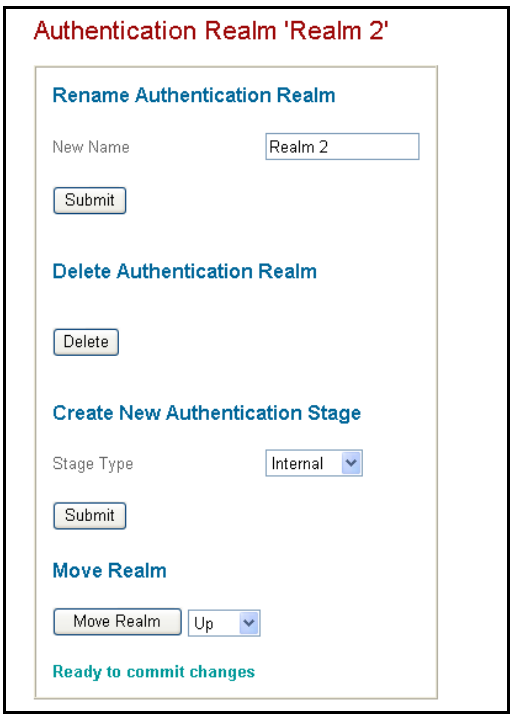


Figure 57 Authentication Realm Page

3 Under Move Realm, select either Up or Down from the drop down menu and then click *Move Realm* to move this realm either one place up or on place down in the realm list. Repeat as needed.

Deleting Realms

To delete a realm, do the following.

1 From the Administration Site, click *System Configuration* and then click *Authentication Settings*.

2 Select the name of the realm that you want to delete.

The following page appears for that realm.

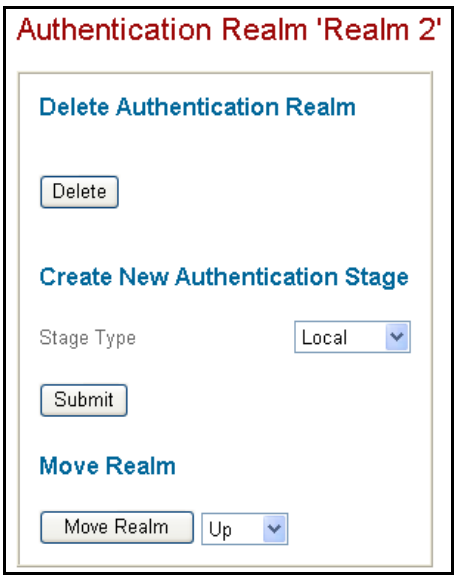


Figure 58 Authentication Realm Page

3 Under Delete Authentication Realm, click *Delete*.

Changing the Realm Field Appearance

By default, realms that you created are selected from the Realm drop down menu upon log in to the NSP. Alternatively, you can set the NSP to display the Realm Name field which requires end users to know their realm name and type it into the Realm Name field.

To change the realm field to a text box or to a drop down menu, do the following.

1 From the Administrator Site, select *System Configuration* and then select *Authentication Settings*.

2 Click *Toggle Realm Pull-Down Menu* as shown in Figure 59.

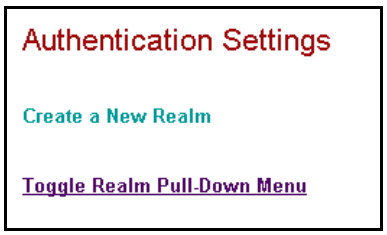


Figure 59 Toggle Realm Pull-Down Menu Location

3 For the Realm Menu Status field, select *Off* if you want a Realm list box. Select *On* if you want the Realm drop down menu.

4 Click *Submit* and then select *Ready to Commit Changes*.Click *Apply* changes.

For example, if you set the realm Menu Status to Off, the next time you log into the NSP the Realm field will be a text box as shown in Figure 59.

Figure 60 Realm Text Box

Using a Realm to Log in to the NSP

Once you have created a realm, users must choose that realm from the login page, as described here.

1 Enter your username and password.

2 Select the appropriate realm from the drop-down list menu or type in the realm name if your NSP is configured to hide the Realm drop-down list box.

3 Click *Log in*.

For Microsoft RADIUS Servers: *If you are logging into a domain in which the RADIUS server is a member, there is no need to precede the username with the domain name. If the RADIUS server authenticates across multiple domains, you*

may precede the username with the domain to which you wish to authenticate. See Microsoft Knowledge Base Article 197429 for more details.

Upon successful log in, the username appears in the list of users in the Administrator page.

Creating an Internal Authentication Data Store

You can create a database of users that are stored on the NSP. For instance, if you are not using another, external authentication server such as RADIUS, you can create a database of users on the NSP and use the NSP's internal authentication.

Adding a User

To create user accounts on the NSP, do the following.

1 From the Administrator Site, click *System Configuration* and then click I*nternal Auth. Stores*.

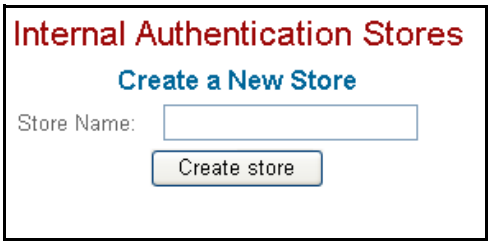


Figure 61 Create a New Store

2 **Store Name:** Enter a name for the group of users you want to add. Note that you can create multiple internal authentication stores.

3 Click *Create Store*.

The Add a New User page appears for the user group you just created.

Figure 62 Add a New User to an Authentication Store

4 **User Name**: Enter the user's name. Spaces are not permitted.

5 **Password**: Enter the user's password.

6 **Password Confirm**: Enter the user's password again.

7 Click *Add User.*

4 Configuring the Thin Service

This chapter describes how to configure the Thin service. Netilla's thin service allow users to remotely operate programs available on an application server via the thin-client protocol. When you "create" an application on the NSP you are actually creating a logical pointer to the real application on the Microsoft Windows 2000/Windows 2003 Terminal Server, UNIX, AS/400 or Mainframe computer.

The following topics are discussed.

- About Thin Applications
- Creating a New Application Server
- Creating a New Microsoft Windows Application
- Creating an X-Windows Application
- Creating a Character-Based UNIX Application
- Creating a 3270 Terminal Emulation Application
- Allowing Users to Access Thin Applications
- Modifying an Existing Application
- Deleting an Existing Thin Application
- Printing While Using the NSP's Thin Service
- Using Local Drive Mapping
- Microsoft Licensing and the NSP

Prerequisites

- **Install Applications on Your Application Server.** Before you create an application on the NSP, make sure the application has been installed on your application server.
- **Obtain a Thin License.** The Web service requires an additional Thin license to be purchased and installed on the NSP.

About Thin Applications

This section describes the types of thin applications that can be created and lists the main steps for creating a Thin client application.

Types of Thin Applications

This section lists the types of Thin client applications that can be configured on the NSP.

Table 10 Types of Remote Applications Supported on the NSP

Application Type	Important Notes
Microsoft	Windows applications created on the NSP must be installed on a Microsoft Windows 2000/2003 server with Terminal Services, and must be compatible with MS Terminal Server and the NSP. For a list of applications tested with the Netilla service, contact your Netilla representative.
X-Windows	The applications you create on the NSP must be installed on an X-Windows platform that uses the X11 Windowing Protocol. The appropriate daemon must also be running to allow connections from the NSP (i.e., telnet, ssh, rexec, rcmd, or rlogin).
3270 Terminal Emulation	The applications you create on the NSP must be installed on a mainframe computer that supports 3270 terminals.
5250 (AS/400)	Applications residing on IBM AS/400s, which use the 5250 protocol, are accessed over the NSP's built-in 3270 emulation. Note that this is not strict 5250 emulation, but an implementation that leverages the AS/400's ability to be accessed via a 3270 terminal that is emulating 5250. By defining the appropriate keymap, end users can access most of the features used in a 5250 terminal access session.
UNIX Character Based	The applications you create on the NSP must be installed on the UNIX-based host and the appropriate daemon must be running (i.e., telnet, ssh, rexec, rcmd, or rlogin).

Thin Service Configuration Main Steps

The following list details the main steps required to create an application.

1. Create Application Server
2. Create Application
3. Assign Application Servers to Application
4. Assign Authorized Users to Applications

Configuring Thin Service System-Wide Settings

This section describes how to configure system-wide settings for Thin applications via the thin client protocol as well as allow users to access Thin applications.

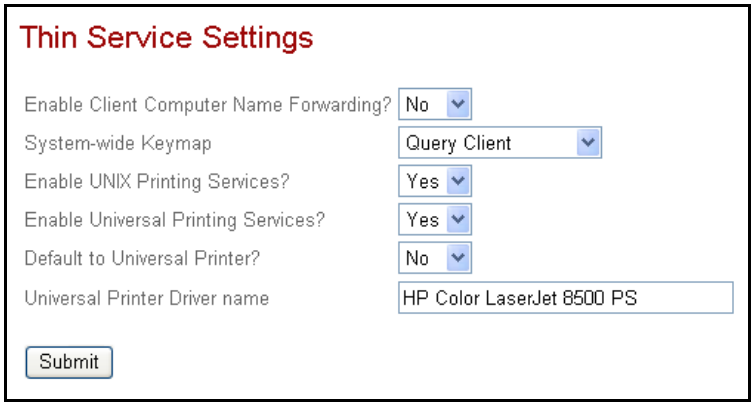


Figure 63 Thin Service System Wide Settings Page

Enable Client Computer Name Forwarding
When enabled, this field allows the NetBIOS name of the connecting client to be provided to Terminal Services sessions. For most situations, this field should be set to the default of *No*.

System-wide Keymap
This field provides support for international keyboards for clients connecting to the NSP. You can choose a particular language for all connecting users or select one of the following:

- Query Client: The NSP queries the client for its locale and uses it.
- Universal: US standard key mapping is used.

Enable Unix Printing Services
This setting enables and disables Unix printing. By default this field is set to *Yes*.

Enable Universal Printing Services
This setting enables and disables Universal printing which allows users to print files utilizing PDF. Printing via PDF does not require the print drivers needed for each end user to be installed on the remote server. Note that end users must have Adobe Acrobat version 4.0 or later on their computers to see and use this feature. By default this field is set to *Yes*.

Default to Universal Printer?
To specify the Universal PDF printer as the default, select *Yes*. Note that the Universal PDF printer may not support all of the printer properties as your native printer. By default, this field is set to No meaning that a native printer is used as the default printer.

Universal Printer Driver name
This setting tells the Terminal server which printer driver properties to use for universal printing. By default, this field is set to HP Color LaserJet 8500 PS. The default setting is recommended for most cases.

Once the service settings are configured, you must allow users to access the service. Refer to “Adding Members to the Thin Service”.

Adding Members to the Thin Service

To authorize users to access the Thin service, do the following.

1. From the Administration Site, click *Services* and then click *Thin*. The Thin Settings page appears.
2. Use the arrow keys to move users under the Members column that you want to allow access to Thin applications.

Changes are saved automatically.

Creating a New Application Server

Application servers appear as objects beneath the NSP’s application servers submenu. The application server object may be named independently of its network name. Note that you create an application server before you can create

applications. You also have the option of creating more than one application server, with each pointed at a different server.

To create a new application server, do the following.

1 From the Administrator Site, select *Applications*, and then *Application Servers*, as shown in Figure 64.

Figure 64 Application Servers Submenu

If no applications have been created, the Application Wizard appears and helps set up an application server and automatically creates Microsoft Word, Excel, PowerPoint, Notepad and Windows Desktop applications.

2 The *Add Application Server* page appears, as shown in Figure 65.

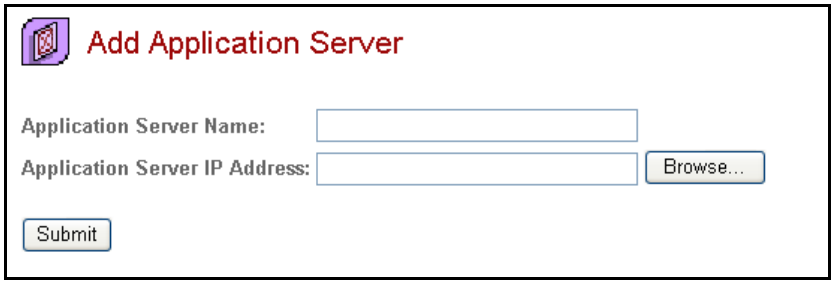


Figure 65 Add Application Server Page

3 Enter a name for the Application Server.

4 Browse to the server using the Browse button.

Creating the list of available servers may take a few seconds to display.

5 Click *Submit*.

The server is now available under Application Servers, as shown in Figure 66.

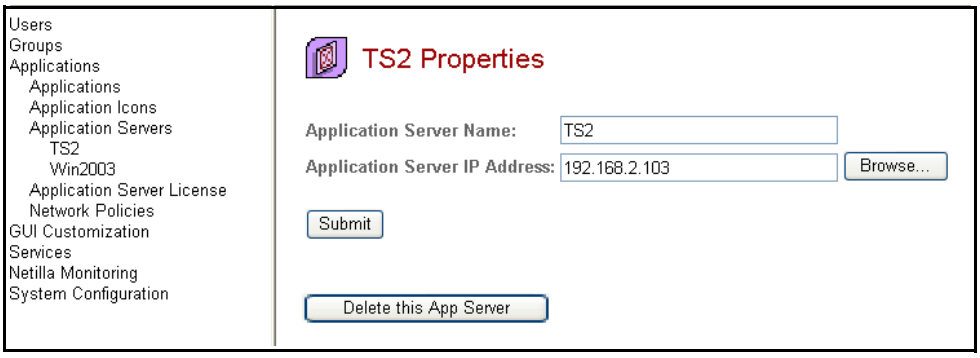


Figure 66 Properties for Application Server

Once you have created an application server, you can create applications that will be available to end users.

Creating a New Microsoft Windows Application

This section describes how to create a Microsoft Windows application. Note that you may have already installed some Microsoft Windows applications as part of the Application Wizard option that you see the first time you configure an application server. This section provides the steps for configuring a Windows application without using the Application Wizard.

To create a new Microsoft Windows application, do the following.

1 From the Administrator Site, click *Applications* and then click *Applications* in the submenu as shown in Figure 67.

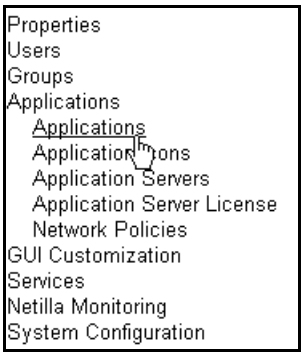


Figure 67 Applications Submenu

If this is the first application to be installed, the NSP prompts you to identify your application server.

The Create New Application window opens, as shown in Figure 68.

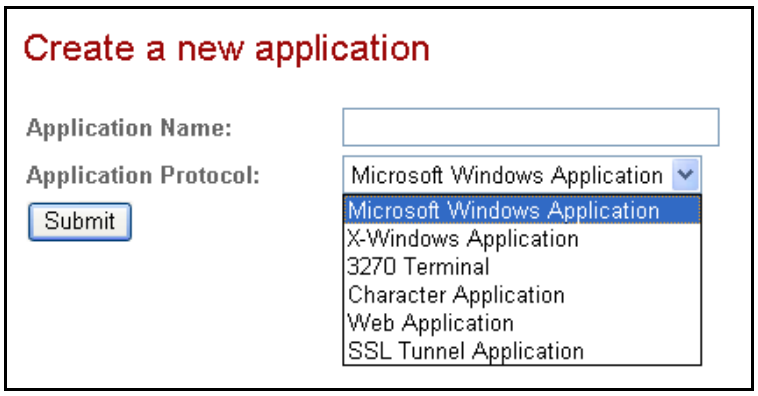


Figure 68 Create New Application Window

2 Enter the application name in the Application Name field.

This name appears beneath the application icon on your users' desktops.

3 Select *Microsoft Windows Application* from the Application Protocol drop-down menu.

4 Click *Submit*.

The General properties screen for the new application is displayed.

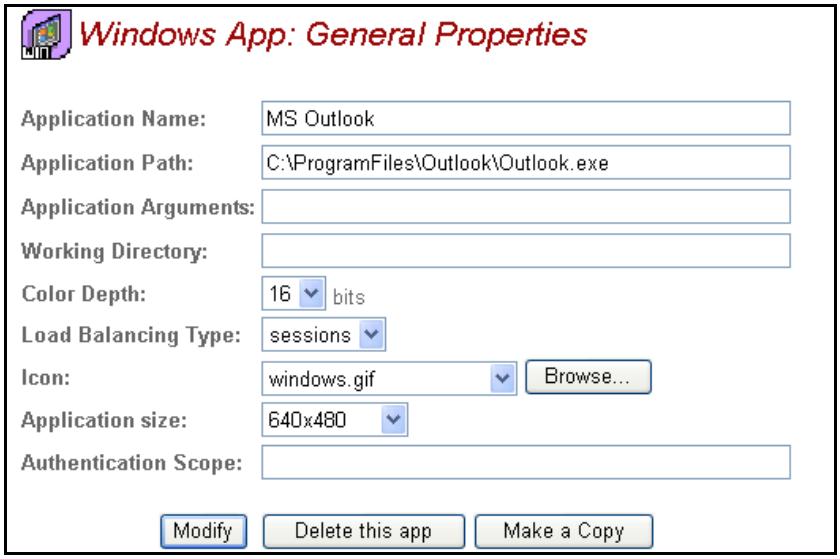


Figure 69 Windows Application General Properties Window

The property screen that you see varies; its contents depend upon the application protocol selected.

5 For **Application Path**, enter the full path of the application on its server. For example, **c:\Program Files\WordProcessingApp\word.exe**.

6 (Optional) For **Application Arguments**, enter the arguments that are passed to the Windows executable each time the application is started.

7 (Optional) For **Working Directory,** enter the location of the folder that contains the application or related information.

8 For **Color Depth**, select the color depth for this application. Choose from 8, 16 or 24 bits. Note that 24-bit should be selected only for applications that require this extensive color depth because of the added processing power required.

9 (Optional) For **Load Balancing Type**, select the type of load balancing you want to use. Choose from sessions, CPU or Memory. If unsure, leave the default set to sessions. For more information, refer to Chapter 8 on page 153.

10 For **Icon**, use the Browse button to locate the icon that you want to represent this application on users' webtops. Refer to "Working with Icons" on page 199 for more information.

11 For **Application Size**, enter the screen area in which the application operates. Choose *Kiosk Mode* to run the application in full screen mode without visible browser borders. When applications are set to *Kiosk Mode*, users must use the Alt+Tab keyboard combination to switch from their Netilla application to their local applications.

Each user's screen must be compatible with this screen size. If a user reports difficulty with their screen appearance, such as phantom or double-scroll bars, instruct that user to modify their screen display properties to match the Application Size field entered here.

12 (Optional) If you created an **Authentication Scope** as part of authentication configuration (see "Creating an Authentication Stage Within a Realm" on page 47) enter the same name that was entered in the authentication configuration in this field.

The name entered here must match the scope configured as part of the authentication stage. This label will be used to link the authentication stage credentials and pass them through to the application that needs them.

13 Click *Modify* to save your changes.

The new application is added to the system.

14 Choose *Application Servers* and select the Server to be associated with this Application.

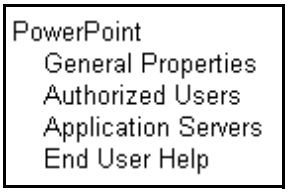


Figure 70 Application Servers Submenu

15 Press the arrow button to move the server to the Members column, as shown in Figure 71.

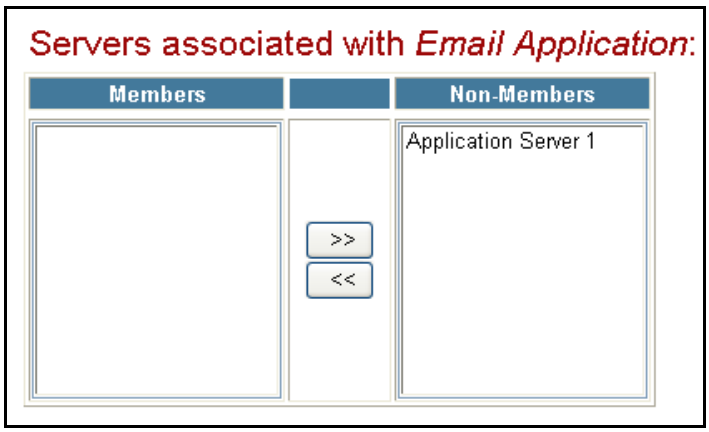


Figure 71 Application Servers Members Window

If you add more than one server, session load balancing will be used between the two servers.

Each server must have the application installed in the same exact location for load balancing to function properly.

16 Choose *End User Help* to create a Help file to be displayed when a user hovers the mouse pointer over the Application Icon.

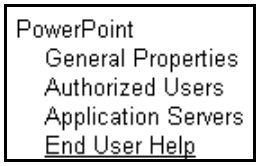


Figure 72 End User Help Submenu

You can upload an HTML file or type in your own text.

17 Scroll down and select *Commit Changes* when finished adding help text.

The last step for configuring applications is to allow users to access the applications. Refer to “Allowing Users to Access Thin Applications” on page 87.

Make a Copy of an Application

The Make a Copy button located on the General Properties page of an application allows you to copy an application. This function is useful for publishing the same application with different screen resolutions or for ease of configuration for creating another application.

Creating an X-Windows Application

Before you begin, the X-Windows applications you create on the NSP must first be installed on an X-Windows platform that uses the X11 Windowing Protocol. The appropriate daemon must also be running to allow connection from the NSP (i.e., telnet, ssh, rexec, rcmd, or rlogin).

To create an X-Windows application, do the following.

1 From the Administrator Site, click *Applications* and then click *Applications* in the submenu as shown in Figure 73.

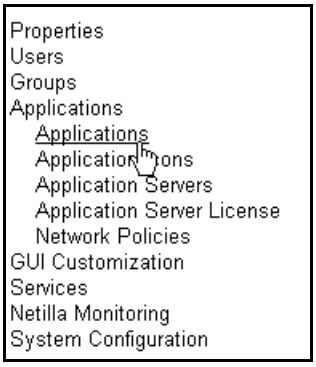


Figure 73 Applications Submenu

If this is the first application to be installed, the NSP prompts you to identify your application server.

The Create a New Application Window opens, as shown in Figure 74.

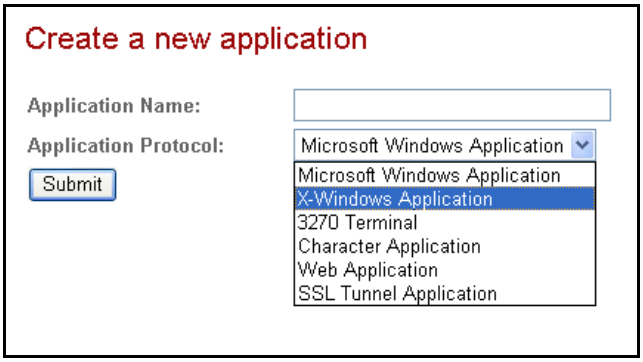


Figure 74 Create a New Application Window

2 Enter the application name in the Application Name field. This name appears beneath the application icon on your users' desktops.

3 Select *X-Windows Application* from the Application Protocol drop-down menu.

4 Click *Submit*.

The General properties screen for the new application is displayed.

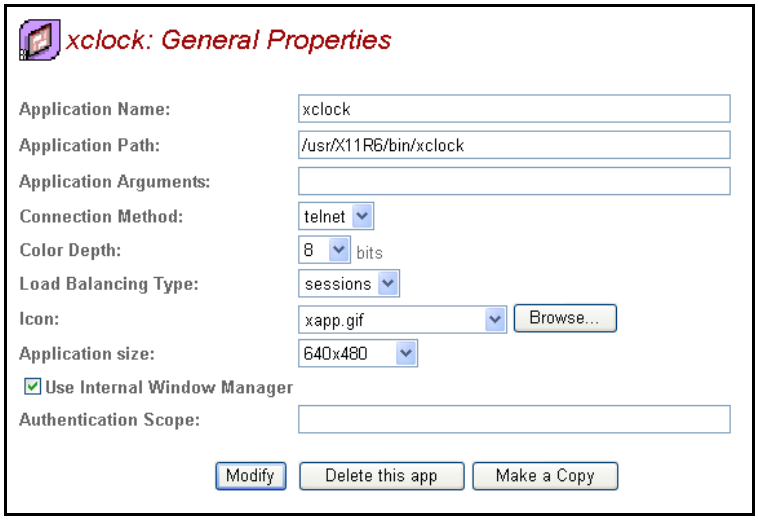


Figure 75 X-Windows Application General Properties Window

The property screen that you see varies; its contents depend upon the application protocol selected.

5 Define the properties that are associated with this new application. The following options are provided.

Table 11 X Windows Application Properties

Field Name	Description
Application Path	This is the full path of the application on its server. This should follow standard UNIX path, i.e.: /usr/X11R6/bin/xterm
Application Arguments	These are the arguments that are passed each time the application is started.
Connection Method	This defines the protocol that the NSP uses to connect to the X-Window Server. This protocol must be supported on the Unix host.
Load Balancing Type	Select the type of load balancing you want to use, sessions, CPU or Memory. For more information, refer to Chapter 8 on page 153.
Icon	This is the icon that represents this application on users' desktops. Use browse to select. Refer to Chapter 4 "Working with Icons" for more information.
Application Size	This is the screen area in which the application operates.Each user's screen must be compatible with this screen size. If a user reports a difficulty with their screen appearance, such as phantom or double-scroll bars, instruct that user to modify their screen display properties to match the Application Size field entered here.
Authentication Scope	If you created an Authentication Scope as part of authentication configuration (see "Creating an Authentication Stage Within a Realm" on page 47) enter the same name that was entered in the authentication configuration in this field. The name entered here must match the scope configured as part of the authentication stage. This label will be used to link the authentication stage credentials and pass them through to the application that needs them.
Use Internal Window Manager	If you are publishing a new application that has its own Window Manager Program (e.g., KDE, GNOME desktop), uncheck this box. Otherwise leave it checked.

6 Click *Modify*. (If you do not click Modify your changes are lost.)

The new application is added to the system.

7 Choose *Application Servers*, and select the server to be associated with this Application.

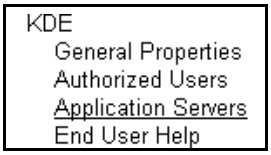


Figure 76 Application Servers Submenu

8 Press the arrow button to move the server to the Members column.

Changes are saved automatically.

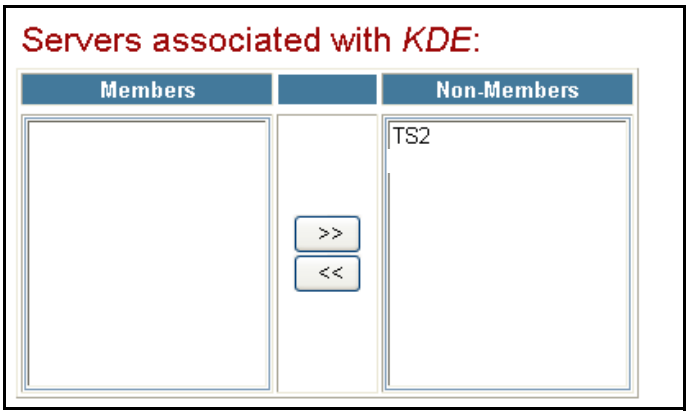


Figure 77 X Application Servers Window

If you add more than one server, the application is load balanced between the servers. Each server must have the application installed in the same exact location for load balancing to function properly.

9 Choose *End User Help* to create a Help file to be displayed when a user hovers the mouse pointer over the Application Icon.

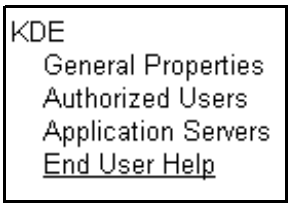


Figure 78 End User Help Submenu

You can upload an HTML file or Type in your own text.

10 Scroll down and select *Commit Changes* when finished adding help text.

The next step is to allow users to access the applications. Refer to “Allowing Users to Access Thin Applications” on page 87.

Make a Copy of an Application

The Make a Copy button located on the General Properties page of an application allows you to copy an application. This function is useful for publishing the same application with different screen resolutions or for ease of configuration for creating another application.

Creating a 3270 Terminal Emulation Application

Before you begin, the 3270 terminal emulation applications that you create on the NSP must be installed on a mainframe computer that supports 3270 terminals.

Applications residing on IBM AS/400s, which use the 5250 protocol, are accessed over the NSP's built-in 3270 emulation. Note that this is not strict 5250 emulation, but an implementation that leverages the AS/400's ability to be accessed via a 3270 terminal that is emulating 5250. By defining the appropriate keymap, end users can access most of the features used in a 5250 terminal access session. When using 3270 emulation to access a 5250 machine, the 3270 display does not support 5250 keyboard shift and validation. This means that a user's input in an uppercase-only field appears exactly as entered. The *Field Exit*, *Field +* and *Field -* keys are not supported by the AS/400's emulation, so key mappings must simulate this by erasing to the end of the field then tabbing to the next field.

To create a 3270 terminal emulation application, do the following.

1. From the Administrator Site, click *Applications*.
2. *Applications* from the Applications submenu, as shown in Figure 79.

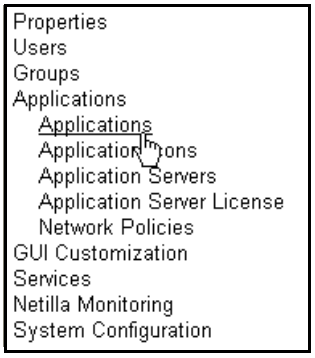


Figure 79 Applications Submenu

If this is the first application to be installed, the NSP prompts you to identify your application server.

The Create a New Application Window opens, as shown in Figure 80.

3. Type the application name in the **Application Name** field. This name appears beneath the application icon on your users' desktops.
4. Select *3270 Terminal* from the **Application Protocol** drop-down menu as shown in Figure 80.

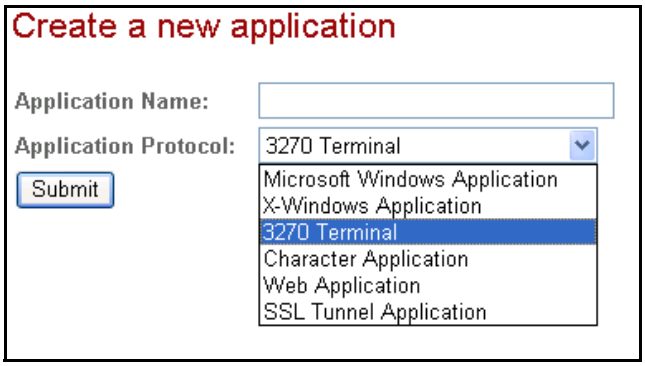


Figure 80 Create a New 3270 Application Window

5 Click *Submit*.

The General properties screen for the new application is displayed.

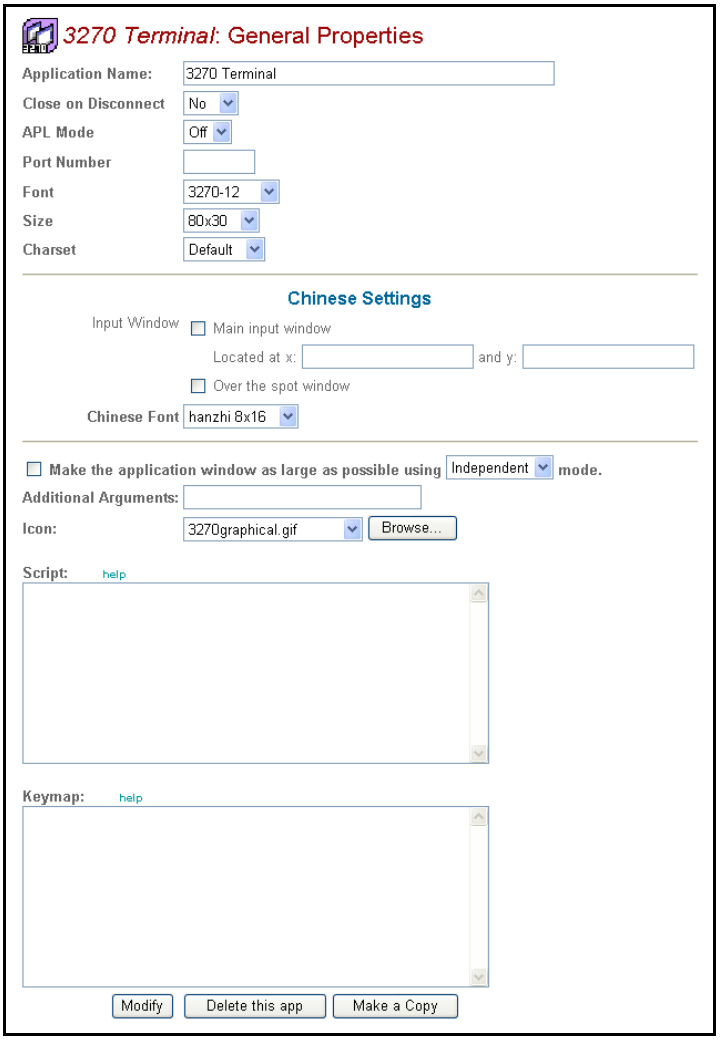


Figure 81 3270 General Properties Page

The property screen that you see varies; its contents depend upon the application protocol you selected.

6 Define the properties that are associated with this new application. The following options are provided.

Table 12 3270 Application Field Descriptions

3270 Application Field	Description
Close on Disconnect	Determines whether the session window is closed upon disconnect.
APL Mode	Enables or disables APL mode. This modifier defines the *Alt* key as an APL key, with a typical APL keyboard layout. For example, choosing *Alt* plus the *A* key results in the APL *alpha* symbol. For reference, the complete list of special APL keys is shown in "Appendix C: APL Key List for 3270 Applications" on page 257.
Port Number	Designates the TCP/IP port used to connect to the Mainframe from the NSP.
Font	Used to select the font displayed in the terminal window.
Size	This is the screen area in which the application operates.
Charset	Sets the character set to the default (US), or Chinese.
Make the application window as large as possible	Sets the application window larger than the default size. Choose from the following: **Kiosk**: When set to kiosk, the application runs without visible browser borders, completely filling the screen. **Independent**: When set to independent, the application window has borders, a title bar and can occupy the entire screen.
Additional Arguments	Allows you to add additional arguments such as screen size, etc.
Icon	This is the icon that represents this application on users' desktops. Use browse to select. Refer to "Working with Icons" on page 199 for more information.

Script	Allows the admin/radmin to specify a script to run upon connection to the server. For example, to create a script that will wait for a connection, enter a string in an input field, and then enter the F3 key. The following script would be entered into the script field:
	`Wait(5, InputField)`
	`String("some string")`
	`Wait(5, Output)`
	`Enter()`
	`Wait(5, Output)`
	`PF(3)`
	`Wait(5, Output)`
	`CloseScript(0)`

Keymap	The Keymap field is used to remap keystrokes from within a 3270 session. An example would be using a 3270 emulation to connect to a 5250 (AS/400) Mainframe. In this case, the default 3270 keystrokes could be replaced with a keymapping relevant to the 5250 Mainframe connection. Copy and paste the contents of your keymap file into the Keymap field. Refer to "Keymapping Details" on page 79 for more information.
Chinese Settings	
Input Window	Checking the Main input window checkbox sets the Chinese Character input screen to the specified X and Y co-ordinates within the session. Checking the Over the Spot Window causes the Chinese Character input screen to appear at the location of the potential input.
Chinese Font	Sets the Chinese font for the session (8x16 or 12x24).

For help creating a script or for keymapping assistance, click the Help hyperlink above the field.

7 Click *Modify*. (If you do not click Modify your changes are lost.)

The new application is added to the system.

8 Choose *Application Servers*, and then select the server to be associated with this application as shown in Figure 82.

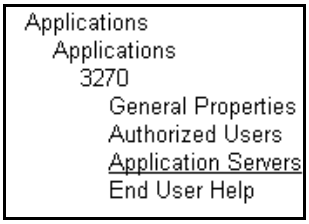


Figure 82 Application Servers Submenu

9 Press the arrow button to move the server to the Members column.

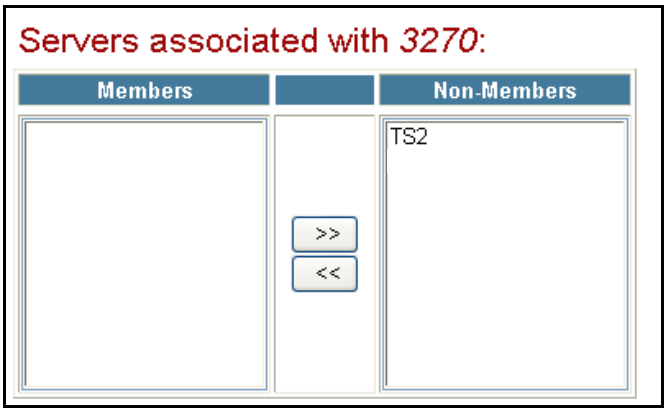


Figure 83 Application Servers Members and Non-Members Window

Changes are saved automatically.

If you add more than one server, the application will be load balanced between the servers. Each server must have the application installed in the same exact location for this to function properly.

10 Choose *End User Help* to create a Help file to be displayed when a User hovers the mouse pointer over the Application Icon.

You can upload an HTML file or Type in your own text.

11 Scroll down and Select *Commit Changes* when finished adding help text.

The next step is to allow users to access the applications. Refer to “Allowing Users to Access Thin Applications” on page 87.

12 Click *Help* to display the conventions used to create your own Custom Key mapping file in a text editor.

Make a Copy of an Application

The Make a Copy button located on the General Properties page of an application allows you to copy an application. This function is useful for publishing the same application with different screen resolutions or for ease of configuration for creating another application.

Keymapping Details

This section provides more details for changing keymap settings. The Keymap field on the 3270 Terminal General Properties page is used to remap keystrokes from within a 3270 session.

Changing the Keymap Settings

To remap keystrokes from within a 3270 session, do the following.

1 Copy and paste the contents of your keymap file into the Keymap field of the application's General Properties page, as shown in Figure 84.

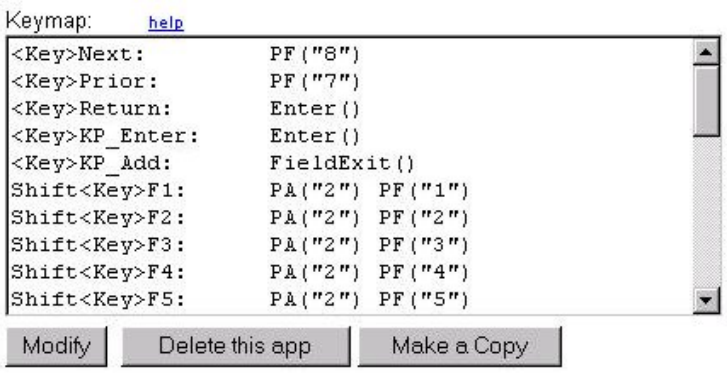


Figure 84 Keymap Field Example

2 Click *Modify*.

Changing the Keymap Default

If you are using the keymap feature, you can change the default keymap setting to the one specified in the Keymap field.

1 To use the Keymap field specified on the General Properties page as the default key mapping when initiating the application, enter *-keymap custom* in the application's Additional Arguments field, as shown below in Figure 85.

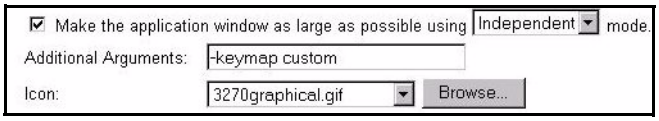


Figure 85 Additional Arguments Field

2 Click *Modify*.

Once launched, the application now uses the custom key mapping.

View Current Key Mappings

1 To view the current key mappings that are available from within the application, select *Options* from within the launched application, and choose *Display Current Keymap*, as shown in Figure 86.

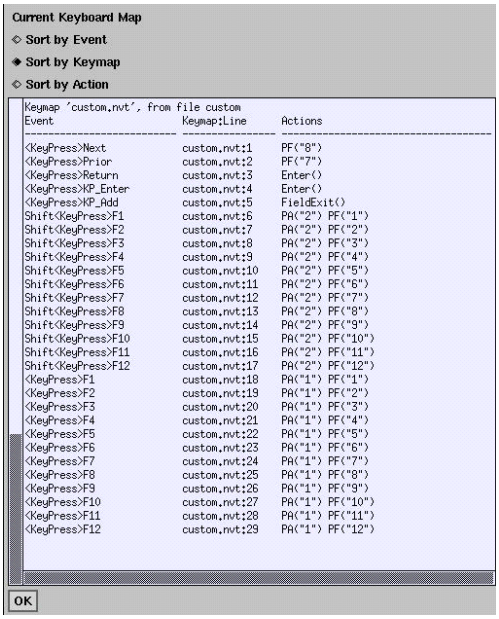


Figure 86 Custom Keymap Display

Within a 3270 application, the available key mappings are "base", "base.3270", and "5250". Any mapping that is specified within the application's properties is saved under the "custom" heading.

If key mappings are changed within the session, and the user would like to go back to the specified (custom) mapping, then "custom" must be entered in the 3270 application's Keymap field, access by choosing Options *and selecting* Change Keymap, *as shown in Figure 87.*

Figure 87 Change Keymap Field

Creating a Character-Based UNIX Application

To create a character-based UNIX application, do the following.

1 From the Administrator Site, click *Applications* and then click *Applications* as shown in Figure 88.

Figure 88 Applications Submenu

If this is the first application to be installed, the NSP prompts you to identify your application server.

The Create a New Application Page opens, as shown in Figure 89.

2 Type a name for the application in the **Application Name** field. This name appears beneath the application icon on your users' desktops.

3 Select *Character Application* from the **Application Protocol** drop-down menu as shown in Figure 89.

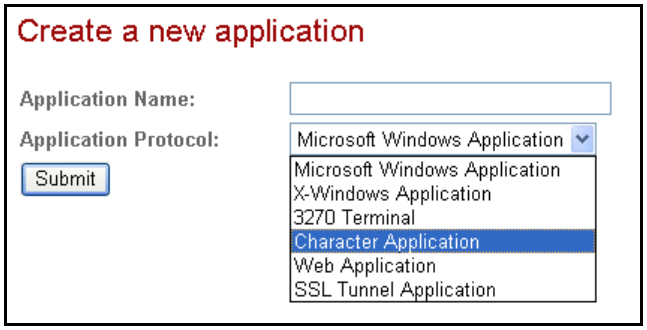


Figure 89 Create a New Character Application

4 Click *Submit*.

The General properties screen for the new application is displayed.

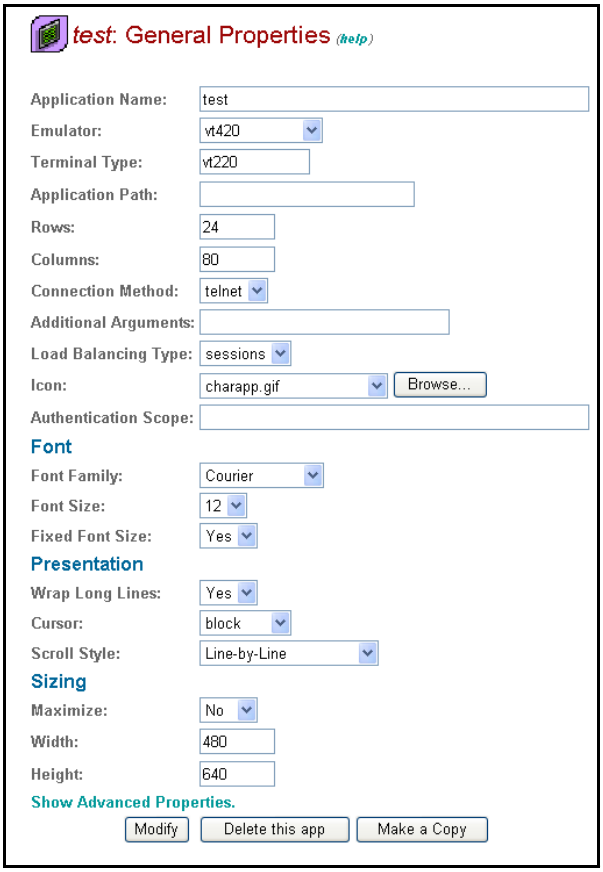


Figure 90 Character Application General Properties Page

5 Define the properties that are associated with this new application:

Based on the Emulator type selected, the remaining fields in the General Properties page vary.

Table 13 Character-Based UNIX Application Fields

Field Name	Description
Emulator	Identifies the type of emulation required for the application, (i.e. SCO Console, vt420, or Wyse 60) as appropriate based on the Terminal Type that you set.
Terminal Type	Specifies the terminal type required for the application. Set appropriately for the emulation type.
Application Path	The full pathname to the application.
Rows	Specify the number of lines of text that fit in the terminal.
Columns	Specify the number of columns of text that fit in the terminal.
Connection Method	Specify the connection protocol that the NSP uses to connect to the UNIX server. You can choose from telnet, ssh, rexec, rcmd, and rlogin.
Additional Arguments	Specify command line arguments for the application.
Load Balancing Type	Select the type of load balancing you want to use, sessions, CPU or Memory. For more information, refer to Chapter 8 on page 153.

Table 13 Character-Based UNIX Application Fields

Field Name	Description
Icon	Select an icon to represent this application on users' desktops. Use browse to select. Refer to Chapter 4 "Working with Icons" for more information.
Authentication Scope	If you created an Authentication Scope as part of authentication configuration (see "Creating an Authentication Stage Within a Realm" on page 47) enter the same name that was entered in the authentication configuration in this field.
	The name entered here must match the scope configured as part of the authentication stage. This label will be used to link the authentication stage credentials and pass them through to the application that needs them.
Font Parameters	
Font Family	Select Courier, Helvetica, or Times Roman.
Font Size	Specify the point size from 2-20 points.
Fixed Font Size	Specify *True* or *False*.
	If true, the font size attribute is used, and scrollbars appear when necessary. If false, the emulator chooses a font size that fits the defined number of columns and lines into the width and height defined for the application. The font size attribute is used as the minimum value.
Presentation	
Wrap Long Lines	Choose either *Yes* or *No*. This attribute determines the emulator behavior when the user enters characters extending beyond the right edge of the emulator window. If set to true, the characters are wrapped onto the next line. If set to false, the characters are placed in the keyboard buffer.
Cursor	Specify whether you want the cursor off, or to appear in either block, or underline format.
	Specifies the method used for terminal window scrolling. Select line-by-line, several lines at once or smoothly.
Sizing Parameters	
Maximize	Choose either *Yes* or *No*. If *Yes*, the fixed font size attribute should be set to No. If set to No, then the Width and Height attributes can be used to set the width.
Width	From 10 to 2000 pixels; only used if Maximize is set to No.
Height	From 10 to 2000 pixels; only used if Maximize is set to No.

Advanced Properties

To access advanced properties, click the *Show Advanced Properties* link. The fields that you see vary depending on the type of terminal emulation you selected for the Emulator field. Terminal dependencies are noted in the descriptions that follow.

An example of the advanced properties section for vt420 terminals is shown in Figure 91.

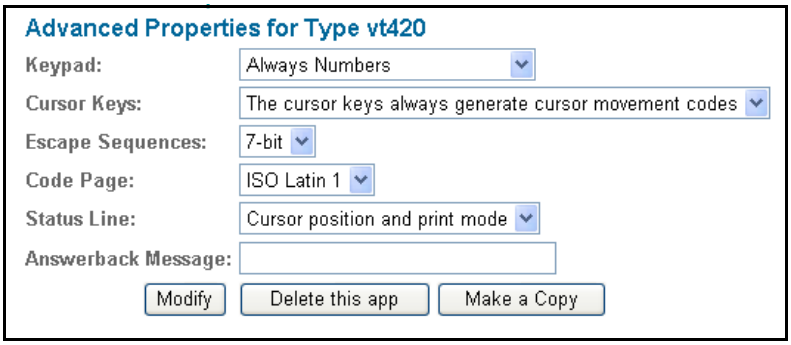


Figure 91 Advanced Properties Fields for Emulation Type vt420

6 Define the properties that are associated with this new application:

Table 14 Advanced Parameters Description

Field Name	Applicable Terminal	Description
Keypad	vt420	Applies to vt420 only. Specifies the behavior of the numeric keypad - whether it always generates numbers or whether you want the application to change the codes generated by the keypad.
Cursor Keys	vt420	Applies to vt420 only. Specifies the behavior of the cursor keys - whether they always generate cursor movement codes, or whether you want the application to change the codes generated by the cursor keys.
Escape Sequences	vt420	Applies to vt420 only. Specifies how escape sequences are sent from the emulator to the application server. Can be set for 7-bit or 8-bit control codes.
Code Page	vt420 wyse 60 SCO console	Specifies the code page you want to use for the emulator. ▪ SCO Console: International, Multilingual, Central Europe, Portuguese, Canadian-French, Danish-Norwegian. ▪ VT420: ISO Latin 1 and ISO Latin 2. ▪ Wyse 60: Multinational, Mazovia, CP852.
Status Line	vt420 wyse 60	Specifies the type of status line to show for the application. ▪ vt420: Choose None, Cursor position and print mode or Messages from the host. ▪ Wyse 60:Choose None, Standard or Extended.
Answerback Message	vt420 wyse 60	Applies to vt420 and wyse 60 only: Provide the text message to return when a query is sent from the application server to the emulator.
Application Key Mode	wyse 60	Applies to wyse 60 only. Specifies whether the application may change the codes generated by keys on the keyboard. Select *True* or *False*.

7 Click *Modify*. (If you do not click Modify your changes are lost.)

The new application is added to the system.

8 Choose *Application Servers*, and then select the Server to be associated with this Application.

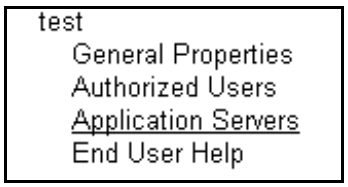


Figure 92 Application Servers Submenu

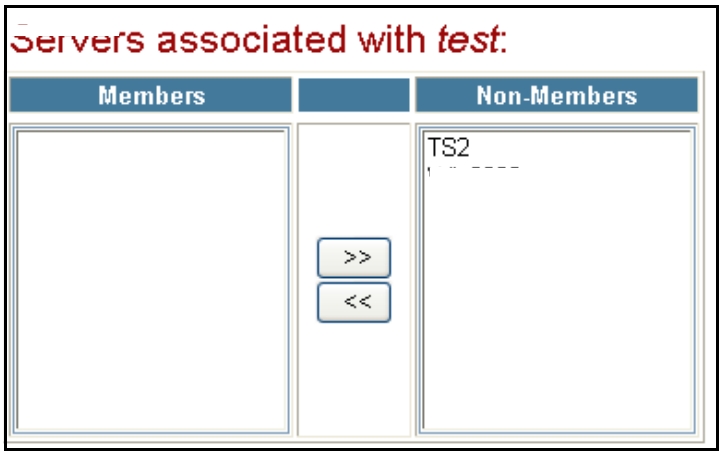


Figure 93 Application Servers Members and Non-Members Window

9 Press the arrow button to move the server to the Members column.

If you add more than one server, the application is load balanced between the servers. Each server must have the application installed in the same exact location for this to function properly.

10 Choose *End User Help* to create a Help file to be displayed when a user hovers the mouse pointer over the Application Icon.

11 You can upload an HTML file or Type in your own text.

12 Scroll down and Select *Commit Changes* when finished adding help text.

The next step is to allow users to access the applications. Refer to “Allowing Users to Access Thin Applications” on page 87.

Make a Copy of an Application

The Make a Copy button located on the General Properties page of an application allows you to copy an application. This function is useful for publishing the same application with different screen resolutions or for ease of configuration when creating another application.

Allowing Users to Access Thin Applications

There are two ways you can allow users to access the Thin applications you configured, via the Applications menu or the Users menu. This section describes how to authorize users to access applications using the Applications menu.

For details on allowing users to access application using the Users menu, refer to "Creating Users on the NSP" on page 139.

1 From the Administrator Site, select *Applications* and then select *Applications*.

2 Select the name of the application that you want to assign users to.

3 Choose *Authorized Users*.

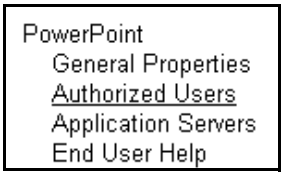


Figure 94 Authorized Users Submenu

4 Choose the users you want to grant access to this application from the Non-Members column, and then click the arrow to move them to the Members column.

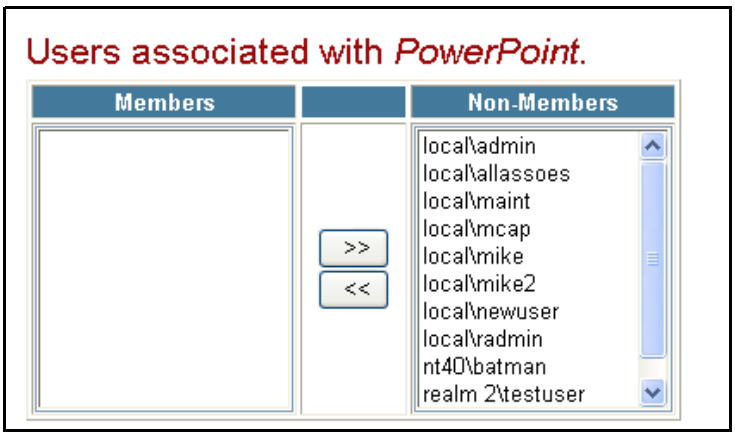


Figure 95 Authorized Users Members and Non-Members Window

Changes are saved automatically.

You can use Control+Click to select multiple members, or Shift+Click to select a range of members.

Modifying an Existing Application

To modify an existing application, do the following.

1 Under *Applications*, click the name of the application, as shown in Figure 96.

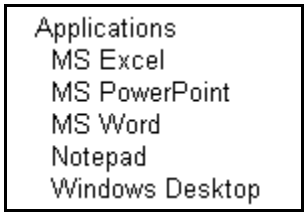


Figure 96 Application List Submenu

2 Select the application you want to modify.

Figure 97 Application Submenu

The Application Properties page opens, as shown in Figure 98.

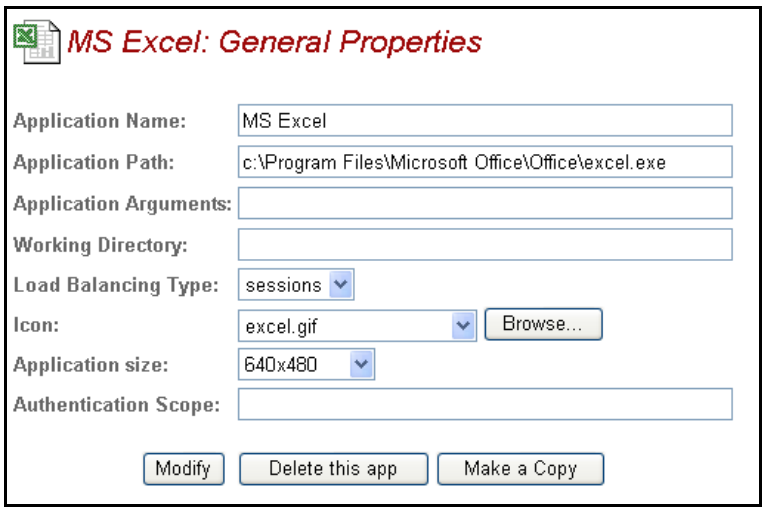


Figure 98 Application General Properties Window

The properties screen that you see varies; its contents depend upon the protocol used by the application.

3 Make the appropriate modifications to the properties associated with this application.

4 Click *Modify*. (If you do not click Modify your changes are lost.)

The modified application properties are saved.

Changes to authorized users and authorized servers take place immediately.

Deleting an Existing Thin Application

To delete an existing application, do the following.

1 Under *Applications*, click the name of the application.

2 Choose *General Properties* and click *Delete this app*.

The application is deleted.

Printing While Using the NSP's Thin Service

The NSP supports the following types of printing for use with the Thin service.

- **Universal Printing**

  The NSP supports universal printing which allows users to print locally without having the necessary print drivers installed on the remote server. With universal printing, users can print documents locally that they are accessing from the remote server regardless of printer type.

  End users must have Adobe Acrobat version 4.0 or later on their computers to see the Universal PDF printer listed in the Printer name drop down menu.

The Universal PDF printer may not support all of the printer properties as your native printer.

- **Native Printing**

  The NSP supports the automatic redirection of printed output to locally-attached client printers. When a user connects to the NSP, printers that are locally attached to the client workstation are automatically made available for the redirection of printed output from remote applications. This process is achieved through Windows 2000/2003 Terminal Server and the Microsoft Plug and Play architecture.

How to Set Up Universal Printing

Setting up universal printing simply requires the following.

Prerequisites for Universal Printing

- **Adobe Acrobat Reader on Client Workstation.** Each workstation must have Adobe Acrobat Reader version 4.0 or higher installed.

How Universal Printing Works

Universal printing works as follows on the NSP.

1 The client selects Universal printing from the printer control panel and prints a document.

2 The NSP connects to the Terminal server and tells the Terminal server that the client is using a postscript printer.

3 The Terminal server sends the document in postscript format to the NSP.

4 The NSP converts the postscript file to PDF and sends it to the client.

5 The client's Acrobat Reader program enables the document to be printed.

How to Set Up Native Printing for Microsoft Applications

Once a local printer is created and output is redirected to it, a user can send printed output from any NSP application, to the locally-attached printer. The print queue that is created can be paused and restarted, or pending jobs can be deleted if needed, just as if the user is running the application on a local machine. The default local printer may be changed to a different local printer or remote network printer as needed.

Prerequisites

For the operation to be seamless the following items must be completed.

- **Local Printer Must be Supported.** The default printer must be a natively supported printer under Windows 2000. If it is not, the printer must be installed locally on the Terminal Services machine with a Windows 2000 compatible driver. To check if the printer is supported visit the following URL: http://www.microsoft.com/windows2000/server/howtobuy/upgrading/compat/search/devices.asp
- **Manually Add Print Driver for Windows 98 or Windows NT clients.** Windows 98 or Windows NT clients require that the driver be manually added to the Terminal Server machine. After creating the printer using the Windows 2000 driver, right click the printer icon and select *Sharing*. Click *Additional Drivers*. Check the appropriate client(s). You will be prompted for the Windows 2000/2003 server disk. If the driver does not exist, you will need to get the driver from the manufacturer.

Once these steps are completed, log into the NSP service. When the *Thin* icon is selected, the printer is scanned. A printer icon appears in the left edge of the Application icons. Hover the mouse pointer over the printer and the printer name will be displayed at the bottom of the browser screen. There are also buttons for pausing the printer and deleting the print job.

How printer mapping works with the NSP

The following steps present an overview of remote printing through the NSP.

1. A user logs in to the NSP with a printer defined.
2. The Netilla print spooler queries the remote computer for the name of the default printer driver designated on the user's computer.

   You can verify that the printer was properly detected by hovering the mouse pointer on the printer icon on the user's WebTop to see if the driver's name appears on the status bar of the browser.
3. When the user launches a Windows application, the name of the print driver is forwarded to the Windows Terminal Server.
4. The Terminal server uses the name of the print driver to create a printer for the user by looking up the driver locally and creating a temporary default printer, which in turn prints to the end user's default printer.
5. In the application server's Printers folder, users see a printer named in the format **<Printer Driver Name>/Netilla/Session <#>** Where <Printer Driver Name> is the client's default printer driver (not the printer's name); Tarantella is the name of the application service and <#> is a sequential number used to identify the users session. For example:

   "HP 4050 PCL6/Netilla/Session 5"

Users see only the session printers that have been created for them, while administrators can see all of the current session printers.

The first time a printer is defined for a user on the application server, the printer settings use the application server's default parameters for the appropriate printer driver. The current settings of the client printer are not used. Note that this is a limitation of Windows Terminal Services.

Any printer options that are set on the local printer will remain the same for any applications that do not send formatting information such as page layout with the print job. Applications such as the Microsoft® Office Suite (Word, Excel, PowerPoint) and others that send page-formatting information in the print stream will override the default printer settings. For example, if the local printer is set to print portrait, but the MS Word page set-up is for landscape, the page prints landscape.

Printing Considerations

Pausing the printer pauses output from the NSP to the local printer. It does not pause the local printer from being used with local applications.

Deleting print jobs deletes only the print job output from the NSP service to the local printer. It will not delete any local jobs that have not printed.

Once a print job is passed from NSP's Thin service to the local printer, the pause and delete have no effect. To delete or pause local printing, open the Printers folder and double click the default printer. Select the job, choose the document menu, and choose pause or delete.

How to Set Up Printing For UNIX Applications

The NSP allows you to access and print from UNIX applications residing on a UNIX server. This section presents step-by-step instructions for doing so.

To print from an application residing on a UNIX server, do the following.

1. Log in to the NSP as either the admin or radmin administrative account.
2. Once logged in, append */extras/x-print-install* to the URL. For instance,

   http://[FQDN-of-platform]/extras/x-print-install
3. Copy and then paste the contents onto your UNIX host.
4. Log in to the UNIX application as user *root*.
5. Execute the script on the UNIX application server, as shown in Figure 99.

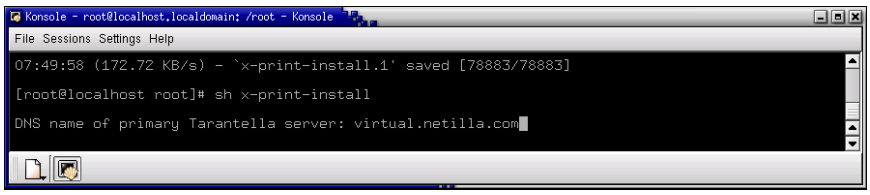


Figure 99 Print Script Execution Window

   For example: *sh x-print-install*

6. When prompted, enter the DNS name of the NSP, as follows.

   For example: *companyname.netillavo.com*
7. Restart the printing services on the UNIX application server.

   For example: */etc/rc.d/init.d/lpd restart*

The specifics of this procedure differ depending on the particular brand of UNIX; the example above is *Linux-specific*. If this example does not work, ask the UNIX application server system administrator for assistance with restarting printing services.

8 Access the NSP by pointing your browser to your company URL (for example, http://company-name.netilla.com).

9 Launch an application via the Thin service of the NSP.

10 Once an application is opened, print a test page.

For example, enter the following command from xterm:
echo "This is a test page." | lpr

The address of the NSP must be resolvable from the application server by the DNS server(s) specified. Refer to "Configuring General Settings" on page 19 for DNS configuration details.

Using Local Drive Mapping

Local Drive Mapping is a feature of the NSP that provides direct access to devices or folders when using Microsoft applications. Through its integration with the NSP, Local Drive Mapping mimics the mapping of local drives, offering the user easy access to local drives from within remote applications. This feature allows you to save, copy and move files between your local PC and your network server seamlessly. When saving a file within any remote application using the Save or Save As dialog box, the local drives of the user's PC are automatically available. These locally-mapped drives are transparent to the user and the network administrator.

Prerequisites

The following changes must be made to your Terminal Server in order to enable Local Drive Mapping through the NSP.

- **Install the Enhancement Module.** The service requires the installation of the Enhancement Module on the Terminal Server that runs the shared applications. To install the module you must first log in to the NSP. Once logged in, download the module from the following location: https://<*address_of_netilla_platform*>/extras/temwin32.exe. Download the installation file to the Terminal Server and install the program via the add/remover program applet under control panel.
- **Verify Ability of Terminal Server to Resolve NSP Name.** The Terminal Server must be able to resolve the name of the NSP to the internal IP address assigned to the NSP. This can be done either via internal DNS Server or by modifying the HOSTS file on the Terminal Server.
- **Allow NetBIOS traffic.** NetBIOS traffic (port 139) must not be blocked between NSP and the Terminal Server. Access rules might need to be made on the firewall if NSP sits inside a DMZ.
- **Enable LAN Manager Compatibility.**
- **Enable NetBIOS over TCP on the interface.**

LAN Manager compatibility and NetBIOS over TCP are enabled by default. However, if either of these functions have been disabled, you will need to re-enable them on the Terminal Server before client drive mapping will work. See the troubleshooting chapter for more information.

Understanding Local Drive Mapping

When the Local Drive Mapping service is enabled, all users are granted access to the service by default. Each user is subsequently given access to his floppy drives, all fixed drives, and all network drives with read and write access as defined on their client device. The drives are mapped using the same drive letter already used by the client, unless the drive letters are already in use.

When the drives on the client device conflict with the drive letters on the application server, the drives will be mapped in a descending order beginning with the letter "Z:"

For example, User A connects to the NSP using a client with local drives mapped in the following manner:

- Local drive *A:* is mapped to the floppy drive
- Drive *C:* is mapped to the local hard disk
- Drive *D:* is mapped to the local CD-ROM
- *E:* is mapped to another hard drive
- The client also has the following network-mapped drives: *H:* (home), *P:* (Public) and *G:* (Accounting).

Given this scenario, when User A connects to a terminal server with drives A:, C: and D:, the client drives are mapped as follows:

- Floppy drive *A:* would conflict with drive *A:* on the Terminal Server. In this case, the local drive *A:* will fall back and be renamed *Z:*
- The same would happen with drives *C:* and *D:*. They are remapped to *Y:* and *X:*, respectively.
- The rest of the drives would be mapped using the same drive letter as on the client device, since no conflict exists (i.e., drive *E:* is be mapped as *E:*, *H:* as *H:*, etc.

Once mapped, a user saving a file within any remotely accessed application using the Save or Save As dialog box can choose between the local drives on their computer and drives located on the remote network.

For example, consider a user who would like to save a file to their local C:\ drive from within a shared application accessed through the NSP. After choosing the Save or Save As dialog box, the user would scroll to the newly mapped Y:\ drive, and the file would be saved on their local machine.

In the example in Figure 100, A:\, C:\, and D:\ are the drives on the Terminal Server, while X:\, Y:\, and Z:\ are the local drives on the client side.

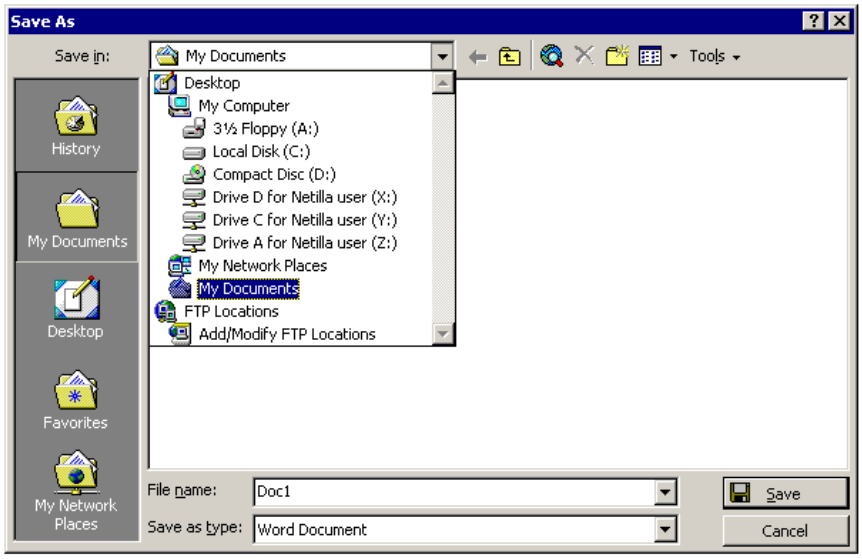


Figure 100 Local Drive Mapping Example

Note that to access the local floppy and CD-ROM drives via Advanced Find, appropriate media must be inserted **prior to launching a NSP session**. When an application is opened, (for example, Word), the local drives are checked for available media in which to write. The absence of media results in the following error message when attempting to access the drive(s): "You do not have access to the folder *x*; see your administrator for access to this folder."

Configuring Drive Mapping

This section describes how to change the local drive mapping default settings. You can change these default settings on a realm or user basis. Changing settings by realm allows you to apply the changes to all users logging into that realm. Alternatively, policies can be applied to the individual user's profile on the NSP. In this case, settings only apply to that particular user. Note that realm default settings take precedence over user default settings.

Changing Client Drive Mapping Settings Per Realm

To change client drive mapping access permissions for a realm, do the following.

1 From the Administrator Site, click *Users* to expand the tree and display the list of realms.

2 Click the name of the realm to configure.

The properties for the realm display on the right hand pane.

3 Scroll down to the Drive Mapping section, shown in Figure 101.

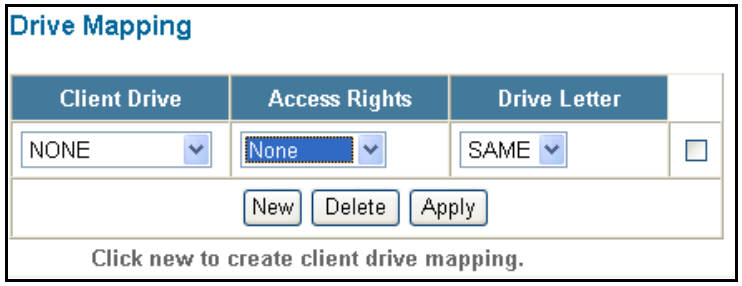


Figure 101 Drive Mapping Window

4 Click *New*.

5 For **Client Drive**, you can either select the type of client drive device or mapped based on the drive letter. If you configure client drive mapping based on client drive type, your choices are:

- Read/Write drives which are typically floppy drives
- Fixed Drives which are typically hard drives
- Read Only drives which are can be CD-ROM/DVD drives
- Network Drives which are typically network mapped

6 For **Access Rights**, select None, Read-Only or Read-Write for the selected Client Drive.

Permissions are set to each group of drives separately. For example, if fixed drives are set to *Read Only*, the client will have read-only access to all of his hard drives when accessed from a remote session.

Note that these permissions override the write permissions that users have on the local machine. This means that if the drives are set to read-only on the NSP, and the user has read-write permissions on the local client, the users will only have only read access to the drives when accessing them through the NSP.

Also, the NSP will not grant user permissions that do not already exist on the client. If a user has read-only permissions on the client machine, he cannot get write permissions via the NSP.

The following options are provided.

Table 15 Read/Write Permission Options

Field Name	Description
Read/Write	Sets read-write access to the group of drives.
Read/Only	Sets read-only access to the group of drives.
None	No access to the group of drives.

7 For **Drive Letter**, specify whether you want to use the same letter that is already set for this drive or select an alternative letter.

8 Click *New*. The client drive you configured appears in the Client Drive Mapping table.

9 Repeat steps 4 through 8 to configure other client drives.

Changes apply to users that login after the settings are applied. Users who are already logged in will maintain their current settings until they log off and back on again.

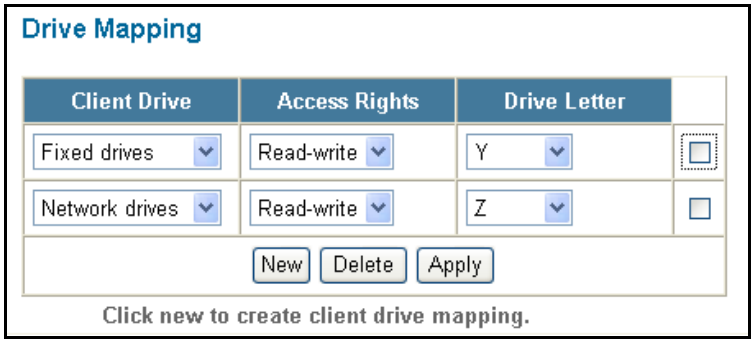


Figure 102 Drive Mapping Configuration Example

Changing Client Drive Mapping Settings Per User

To change the client drive mapping settings for a specific user, do the following.

1. From the Administrator Site, click *Users* to expand the tree and display the list of realms.
2. Expand the realm of the user you wish to modify by clicking on the name of the realm.
3. Click on the name of the user that you want to work with.
4. Click *Drive Mapping* under the user's properties.

   The drive mapping properties for the user are displayed on the right hand pane, as shown in Figure 103.

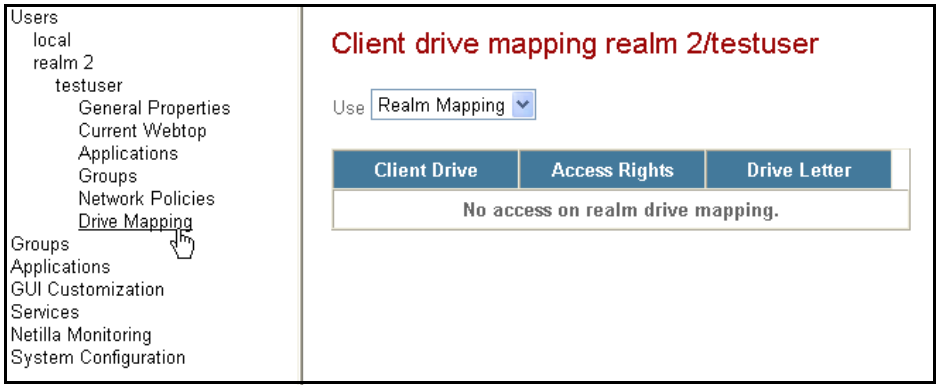


Figure 103 Client Drive Mapping Settings by User

   By default, users are set to inherit their client drive mapping permissions from the ream that they log into, as shown via the *Local Mapping* drop-down list box.

5. To configure this user's drive mappings preferences individually, select *User Mapping* from the Use drop-down list.

   The Client Drive Mappings table is activated.

6. For **Client Drive**, you can either select the type of client drive device or mapped based on the drive letter. If you configure client drive mapping based on client drive type, your choices are:
   - Read/Write drives which are typically floppy drives
   - Fixed Drives which are typically hard drives
   - Read Only drives which are can be CD-ROM/DVD drives

- Network Drives which are typically network mapped

7 For **Access Rights**, select None, Read-Only or Read-Write for the selected Client Drive.

Permissions are set to each group of drives separately. For example, if fixed drives are set to *Read Only*, the client will have read-only access to all of his hard drives when accessed from a remote session.

Note that these permissions override the write permissions that users have on the local machine. This means that if the drives are set to read-only on the NSP, and the user has read-write permissions on the local client, the users will only have only read access to the drives when accessing them through the NSP.

Also the NSP will not grant user permissions that do not already exist on the client. If a user has read-only permissions on the client machine, he cannot get write permissions via the NSP.

The following options are provided.

Table 16 Read/Write Permission Options

Field Name	Description
Read/Write	Sets read-write access to the group of drives.
Read/Only	Sets read-only access to the group of drives.
None	No access to the group of drives.

8 For **Drive Letter**, specify whether you want to use the same letter that is already set for this drive or select an alternative letter.

9 Click *New*. The client drive you configured appears in the Client Drive Mapping table.

10 Repeat steps 1 through 3 to configure other client drive types. When done, go on to step 5 to apply the changes.

11 Click *Apply* to have the changes take affect.

Changes will apply to users that login after the settings are applied. Users who are already logged in will maintain their current settings until they log off and back on again.

Drive Mapping with the Office Suite

When the NSP is first installed, and an initial connection to the Windows 2000 Terminal Server is made, the NSP automatically generates icons for the Office Suite that will be available to NSP clients.

Microsoft Licensing and the NSP

Microsoft Licensing is invoked when an NSP user launches an application that is configured to run from a Microsoft Terminal Server. Each application that is launched initiates a new terminal server session. Users are required to follow the licensing requirements as set forth by Microsoft.

TS CALS and the NSP

Due to a change in Microsoft licensing requirements, the Terminal Server now queries end users for compliance. The manner by which the NSP handles TS CALS varies depending on the Microsoft server operating system and client operating system as shown in Figure 104.

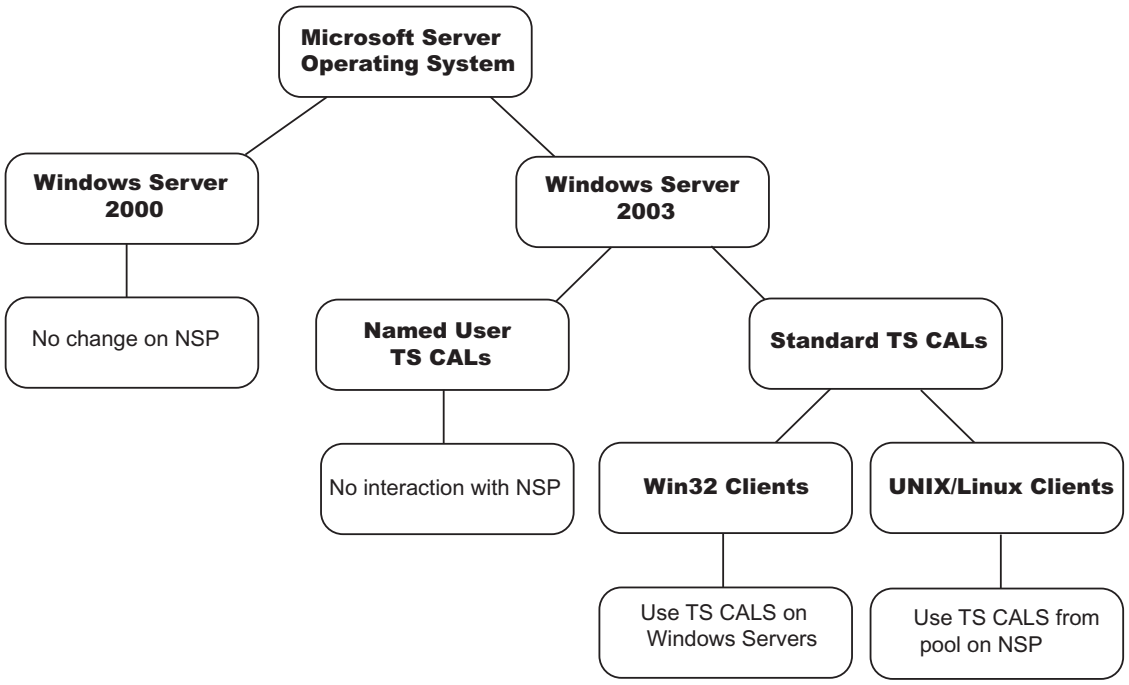


Figure 104 Microsoft Licensing and the NSP

License enforcement also applies to non-Windows machines, such as UNIX or Linux users who access Terminal Server applications via Netilla. For these users, a pool of TSCALs will be maintained on the Netilla platform.

Connecting to Windows 2000 Servers

When using the NSP to connect to Windows 2000 servers from either Windows clients or non-windows clients, the model is unchanged as compared with previous releases of the NSP.

Connecting to Windows 2003 Servers from Windows Clients

If the connecting client is Windows, then the process is as follows:

1. The Windows client logs in to the NSP.
2. A Windows 2003 Terminal Services application is launched.
3. The Windows client is checked to see whether a TS CAL is installed on the client.
4. If a TS CAL is already present on the Windows client, then it is sent to the Terminal Server. If a TS CAL is not already present on the Windows client, the NSP asks the Microsoft License Server for a TS CAL, and that license is installed on the Windows client PC.

TS CALS that are unused for 90 days will be automatically reclaimed by the server for re use.

Connecting to Windows 2003 Servers from Non-Windows Clients

If the connecting client is not Windows based, then a pool of TS CALs are maintained on the NSP, to handle the maximum number of concurrent NSP

users running Terminal Server applications at any given time. The process is as follows:

1 The non-Windows client logs into the NSP.

2 A Windows 2003 Terminal Services application is launched.

3 The NSP checks to see whether there are any available TS CALs in its license pool.

4 If there is a TS CAL available in the RDP license pool, that TS CAL is marked as “in use” and the session is established to the Terminal Server using that TS CAL.

5 If all the TS CALs in the RDP license pool are in use, then the NSP requests a TS CAL from the Microsoft License Server, and that TS CAL is stored in the RDP license pool. It is then marked as “in use” and used to connect to the Terminal Server for that user.

6 If the user proceeds to bring up a second Terminal Services session, the same TS CAL is used as the first session. If the user closes down all Terminal Services sessions, then the TS CAL becomes available, and can be used by another user.

Connecting to Windows 2003 Servers Using Named Users TS CALs

If the customer has purchased “named user” TS CALs, neither the NSP nor the connecting client have any interaction with the TS CAL.

This approach is recommended for roaming users who connect from Windows based kiosks, such as airports or Internet cafes. Because the license is associated with the user, not the client computer, the licenses never leave the Terminal Server eliminating the need to recycle licenses.

For more information on Microsoft TSCAL licensing policy, visit http://www.microsoft.com/licensing.

Netilla Networks, Inc. assumes no responsibility for customer compliance with Microsoft licensing policy and suggests that the customer consult with Microsoft directly in regards to license practices.

Netilla Networks suggests that the Terminal Server be configured in Per Seat mode for Client Access Licenses. Configuring the Terminal Server otherwise may result in operational inconsistencies.

About the NSP’s TS CAL Pool

You can view the TS CALS that are currently in use on the NSP as follows.

1 From the Administrator Site, select *Services*.

2 Select *Thin* and then select *Licensing*. You will see the NSP’s page for the TS CALs it issues to non-Windows clients as shown in Figure 105.

Figure 105 NSP TS CAL License Page

This page lists all TS CALs currently assigned by the NSP to non-Windows users. By default, one TS CAL is always listed and shown as “in use”.

Removing TS CALS from the NSP’s Pool

The TS CALs listed in the NSP pool are assigned to non-Windows clients requesting access to Windows 2003 terminal services. You have the option of removing TS CALS from the NSP’s pool. You may want to do this if you find that you have extra TS CALs that are part of the NSP’s pool and you want to use them for Windows users.

Removing TS CALs from the NSP’s pool does not implicitly make them available. Contact Microsoft for details regarding recovering TS CALs.

To take TS CALs from the NSP’s pool, do the following.

1. Select the license(s) that you want to remove.
2. Click the *Remove Licenses Not in Use* button.

5 Configuring the Web Service

The Netilla Security Platform (NSP) provides secure access to Web-based intranet applications and portals via HTTP reverse proxy technology. This means that end users can access secure Web servers that remain protected within the private intranet, while policies on the NSP limit access to paths, directories, servers, and web components on a user or group basis.

This following topics are discussed.

- Understanding the Web Service
- Configuring Web Service System-Wide Settings
- Adding Members to the Web Service
- Creating a Web Application
- Configuring Web Policy
- Allow Users to Access a Web Application
- Advanced Web Services Configuration

Prerequisites

Before you begin to configure the Web service, do the following.

- **Obtain a Web License**. The Web service requires an additional Web license to be purchased and installed on the NSP.
- **Configure a DNS server**. Refer to “Configuring General Settings” on page 19 for details.

Understanding the Web Service

Netilla’s Web service uses HTTP reverse proxy technology to allow remote users to access intranet Web applications from the Internet. To understand how a reverse proxy operates, consider the way a forward proxy operates. A forward proxy acts as a gateway for a client's browser, sending HTTP requests to the Internet on the client's behalf. When the external HTTP server receives the request, it sees the IP address originating from the proxy, not the actual client. This is a common method for protecting the internal network.

Alternatively, a reverse proxy operates on behalf of an internal web server, rather than the remote client. The reverse proxy acts as a gateway to the internal web servers, and is the last IP address that the client sees. In this way, the proxy protects the web server.

HTTP Reverse Proxy Main Steps

The following list details the main steps required to configure the Web service.

1. Configure Web Service System Wide Settings
2. Create Web Applications
3. Configure Web Policy
4. Add Members to the Web Service

Configuring Web Service System-Wide Settings

This section describes system-wide settings for the Web service. For most Web service configurations you can leave the system-wide settings at their default values. However, you should review this section to determine whether there are any changes you would like to make.

Settings that cover advanced configurations are described in “Advanced Web Services Configuration” and do not need to be changed for most scenarios.

To configure system-wide Web service parameters, do the following.

WARNING: *Changes to these fields take effect immediately.*

1. From the Administrator Site, click *Services* and then click *Web*.
2. Click *General Properties*. The Web settings page appears.

Refer to the fields under System Settings.

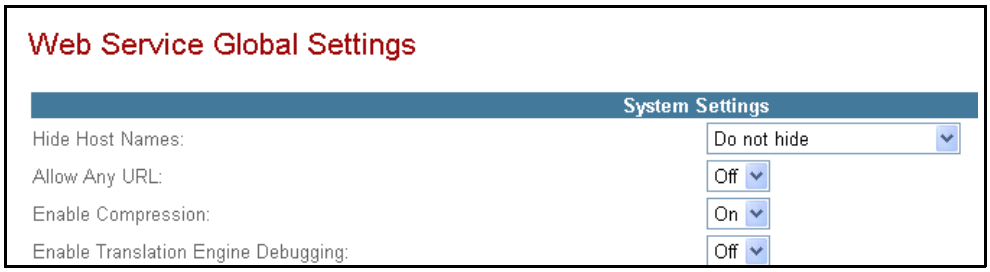


Figure 106 Web Service System Parameters

The fields are described in Table 17

Table 17 Web Service System-Wide Settings Description

Field Name	Description
Hide Host Names	Provides the following options for hiding internal web server's hostnames and IP addresses. ▪ **Do not hide**: Internal web server's hostnames and IP addresses are not hidden. (Default) ▪ **Hide-unique per URL**: Obscures the hostname differently per URL. Because this option involves significant processing, performance may become noticeably slower. However, this option is the most secure. ▪ **Hide-unique per page**: Obscures the hostname differently per web page. ▪ **Hide-unique per session**: Obscures the hostname differently per session. Because this option involves the least amount of processing of the three hide choices, performance is affected the least. However, this option is the least secure.
Allow Any URL	Allows you to add a field to the NSP's Web services page that users can use to enter an internal URL. Note that this simply adds a URL field to the Web services page and does not provide access unless a user has been granted access via NSP policy settings.
Enable Compression	Set this option to *On* if you have users dialing in with slow links. Otherwise, set this option to *Off*. By default this field is set to *On*.
Enable Translation Engine Debugging	This option allows you to save untranslated HTML, JavaScript and other web resources for isolating issues that you may encounter while using the Web service. Select *O*n only for the amount of time necessary to capture the untranslated information. Do not leave this option turned on for extended periods of time. Refer to "Web Service Monitoring" on page 164 for details on accessing the untranslated information.

3 Configure the advanced fields as appropriate.

4 Click *Submit*.

Changes take affect immediately.

Adding Members to the Web Service

To authorize users to access the Web service, do the following.

1 From the Administration Site, click *Services* and then click *Web*.

2 Click *Membership*. The Web Settings page appears.

3 Use the arrow keys to move users under the Members column that you want to allow access to Web applications.

Changes are saved automatically.

Creating a Web Application

This section describes how to create a Web application on the NSP. When you "create" an application on the NSP you are actually creating a logical pointer to the real application.

Note that configuration of all fields is not required. Optional fields are noted. Advanced fields should be left at their default values unless you are instructed otherwise.

To create a Web Application, do the following.

1 From the Administrator Site, click *Applications* and then click *Applications* as shown in Figure 107.

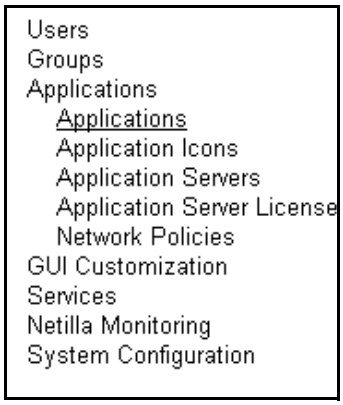


Figure 107 Applications Sub Menu

2 The Create a New Application page appears.

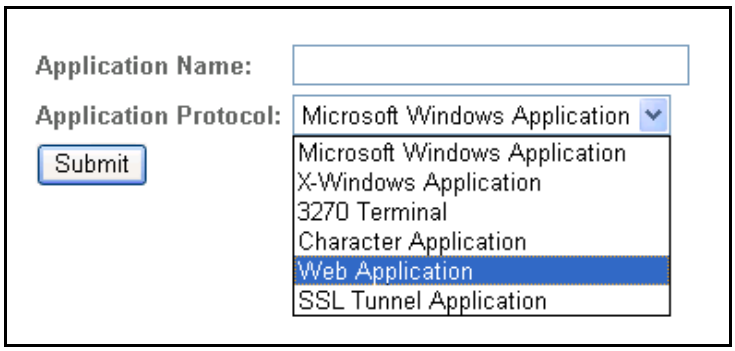


Figure 108 Create a New Application Page

3 Enter a name for your new Web-based application, and then choose *Web Application* as the Application Protocol.

4 Click *Submit*.

The General Properties page appears.

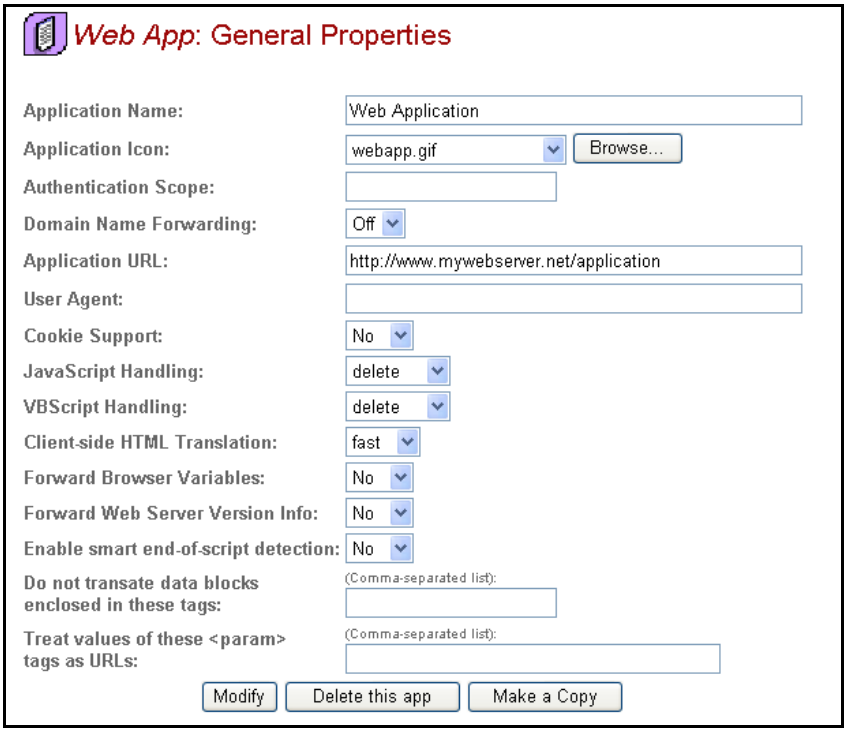


Figure 109 Web Application General Properties

5 (Optional) For the **Application Icon** field, click Browse to choose an icon for the application (or leave the default).

6 (Optional) **Authentication Scope**. If you created an Authentication Scope as part of authentication configuration (see “Creating an Authentication Stage Within a Realm” on page 47) enter the same name that was entered in the authentication configuration in this field.

The name entered here must match the scope configured as part of the authentication stage. This label will be used to link the authentication stage credentials and pass them through to the application that needs them.

Your web server dictates the type of authentication that is allowed. If an authentication type other than basic is required by the web server, the user is prompted for their username and password.

7 (Optional) **Domain Name Forwarding**. This field applies if you configured an Authentication Scope. You can include the NT domain name associated with the authentication stage of the specified Authentication Scope for this Web application. When set to *On*, the NT domain name and the user name are sent to the remote Web server. When set to *Off*, only the username is sent.

8 In the **Application URL** field, enter the starting URL for the webpage (for example, http://www.website.com).

The required convention for this field is **http://** *or* **https://** *preceding the URL.*

9 (Optional) **User Agent** allows you to spoof a particular browser and version for display. This information is sent to the remote Web site instead of the information provided by the browser in the HTTP request headers.

For example, to emulate Internet Explorer 6.0 for Windows, enter ***Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)***

10 For **Cookie Support**, specify whether cookies are permitted (Yes) or not (No).

Cookies are stored temporarily in the NSP's memory and are deleted when the user logs out of the NSP.

11 For **JavaScript Handling**, it is recommended that you select *Translate* if your Web application uses JavaScript. The choices are as follows:

- **Delete**: Removes JavaScript from proxied web pages.
- **Translate**: Translates JavaScript in proxied Web pages.
- **Passthru**: Web proxy does not do translation.

12 For **VBScript Handling**, it is recommended that you select *Passthru* if your Web application uses VBScript. The choices are as follows:

- **Delete**: Removes VBScript from proxied web pages.
- **Passthru**: Web proxy does not do translation.

13 For **Client-side HTML Translation**, specify *Fast*, *Full* or *None*. Fast is recommended for most Web applications. Because HTML translation is inherently slow, Netilla provides a *Fast* option that quickly processes Web pages and works with the majority of Web applications. Should you notice malfunctioning links or images not loading in your Web application, change this setting to *Full*. There are also rare cases when no translation is required. For these situations, select *None*.

14 For **Forward Browser Variable**, specify whether or not you want to prevent the server from receiving information about a client such as user agent and language preferences. Select *Yes* to allow the server to see browser variables or *No* to keep browser variable information private.

15 For **Forward Web Server Info**, specify whether or not you want to prevent clients from seeing information about the Web server. Select *Yes* to allow the clients to see Web server information or *No* to keep Web server information secure.

16 (Advanced) For **Smart end-of-script detection**, specify whether to enable advanced checking for Java script code embedded in HTML. For most cases, this option can be left at the default setting of No.

17 (Advanced) For **Do not translate data blocks enclosed in these tags**, enter tags that you do not want to be translated. For most cases, this option can be left at the default setting.

18 (Advanced) For **Treat values of these <param> tags as URLs**, enter tags that you should be translated URLs. For most cases, this option can be left at the default setting.

19 Click *Modify*.

At least one policy must be defined to allow users to access Web applications. Go on to "Configuring Application Policy" on page 107.

Configuring Web Policy

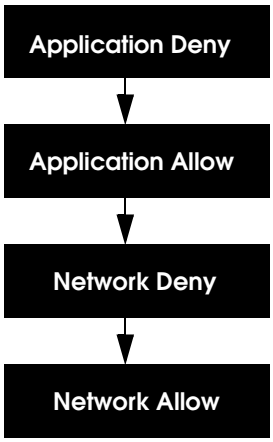
Unlike Thin applications, Web and Tunnel applications require the client computer to have access via the NSP to the back-end server. After a Web or Tunnel application is created on the NSP, at least one policy rule must be created for each application to allow users to access the application. This section describes how to configure policy for Web-based applications.

About Application and Network Policy

There are two types of policies that can be created for a Web application, application-level policy and network policy. With application policy, you can greatly control user access by directing users to specific locations on a server to which you want to allow access. Network policies are more general and typically allow users to have wider access. As such, network policies do not provide as stringent policy as application policies and, if configured, should only be done so sparingly. Network policy can be useful in situations where multiple servers do not need restriction. That is, only a couple of applications on a particular server need restrictions.

Application and Network Policy Processing

When the NSP receives an HTTP request, all application and network policies are evaluated and processed in the following order:



First, the NSP checks to see if there are any application rules that deny access to this user. If there are no application policy rules that deny access to this user, application allow rules are checked.

If an Application Allow rule grants access to this user, the subsequent network polices are not checked. If there were not any application rules that allowed access to this user, network policies would be checked. If there are no network policy rules that deny access to this user, network policy allow rules are checked.

To activate policy changes made during an active session, the user must log out and in again for the change to take affect.

Best Practices for Web Policy Configuration

- Application policy is preferred over network policy because network policy tends to be more liberal and therefore less secure.
- Use network policy carefully and sparingly.

Configuring Application Policy

This section explains how to configure application-level policy for Web applications.

All Web applications must have a policy that specifies that the connection to the Web application is allowed otherwise users will be denied access.

The following example describes how to create a rule that allows the protocol **HTTP** over port **80** to www.mywebserver.net/applications/myapp.asp and all subdirectories.

1 Click *Applications* and then click *Applications* as shown in Figure 107.

2 Select the name of the application to which you want to add policy.

3 Click *Policy Rules* located below the application name as shown in Figure 110.

Figure 110 Web Application Policy Rules Menu

The Policy page for Web applications appears as shown in Figure 111.

Figure 111 Web Application Policy Page

4 Select *Allow* from the **Allow/Deny** drop-down menu.

5 Specify the **Host Type** as *DNS*, since we will be entering the FQDN of the site, not the IP address.

Alternatively, **Host Type** can be set to **IP** which allows you to specify an IP address in the Host Address. For example, to create a rule that applies to subnet C under 192.168.1.0, set Host Type to IP and for Host Address, enter 192.168.1.0/24.

6 For **Protocol,** select *http*.

Other options are https and Any which allows either protocol.

7 Because the protocol (http://) is specified, the **Host Address** starts with *www* (www.mywebserver.net), or just the domain name (mywebserver.net). Entries with a protocol preceding the URL will NOT be accepted (for example: http://www.mywebserver.net).

8 For **Port**, enter the TCP port to be used (for this example, it is 80 which is also the default).

9 For **Path**, enter the allowed path on the target Web server. The default is /, which allows access to the entire domain. If you want this policy to apply to an application residing at www.mywebserver.net/application, you would enter */application* in the Path field. This policy would then allow the connection ONLY to the specified path.

10 Click *Create*.

The policy appears above the policy creation fields.

11 Create additional rules as needed.

Although the Netilla policy allows the connection, you must ensure that nothing blocks the traffic outside of the NSP, such as the NSP Firewall or DMZ Firewall.

Configuring Network Policy for Web applications

To configure network policy for Web applications, do the following.

1 From the Administrator Site, click *Applications*, and then click *Network Policies*.

The Create a New Network Policy page appears.

Figure 112 Create New Network Policy Page

2 Enter a **Name** for the network policy that you are creating.

Use a descriptive name to make it easier to identify when it comes time to apply the policies.

3 Select Web from the **Network Policy Type** drop down list box and then click *Submit*.

The General Properties page for a network policy for a Web application is shown in Figure 113.

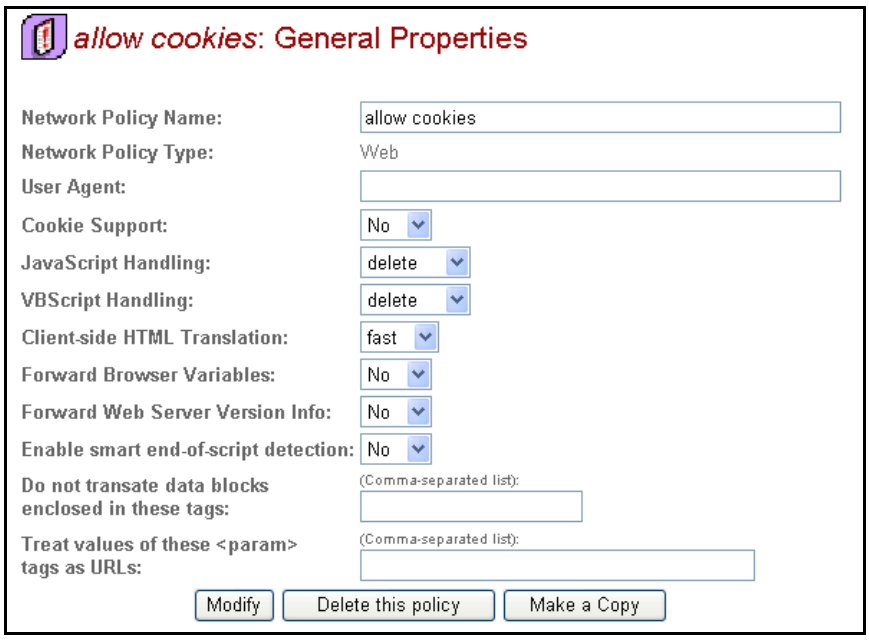


Figure 113 General Properties for a Network Policy for a Web Application

4 Configure the general properties fields.

For security reasons, the password forwarding feature (i.e., Authentication Scope field) is not configurable as part of a network policy. If you want to configure a policy for password policy, you can create an application policy. For details, refer to "Configuring Application Policy" on page 107.

5 Refer to Table 18 for descriptions of the fields.

Table 18 Web Policy Fields and Descriptions

General Properties Field	Description
User Agent	Allows you to spoof a particular browser and version for display. This information is sent to the remote Web site instead of the information provided by the browser in the HTTP request headers. For example, to emulate Internet Explorer 6.0 for Windows, enter ***Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)***
Cookie Support	Specifies whether cookies are permitted (Yes) or not permitted (No).
JavaScript Handling	It is recommended that you select *Translate* if your Web application uses JavaScript. The choices are as follows: **Delete**: Removes JavaScript from proxied web pages. **Translate**: Translates JavaScript in proxied Web pages. **Passthru**: Web proxy does not do translation.
Client Side HTML Translation	Specify Fast, Full or None. Fast is appropriate for most pages.
VBScript Handling	It is recommended that you select *Passthru* if your Web application uses VBScript. The choices are as follows: **Delete**: Removes VBScript from proxied web pages. **Passthru**: Web proxy does not do translation.
Forward Browser Variables	Specifies whether or not you want to prevent the server from receiving information about a client such as user agent and language preferences. Select *Yes* to allow the server to see browser variables or *No* to keep browser variable information private.

General Properties Field	Description
Forward Web Server Info	Specifies whether or not you want to prevent clients from seeing information about the Web server. Select *Yes* to allow the clients to see Web server information or *No* to keep Web server information private.
Enable smart end-of-script detection	Specifies whether to enable advanced checking for Java script code embedded in HTML. For most cases, this option can be left at the default setting of No.
Do not translate data blocks enclosed in these tags	Enter tags that you do not want to be translated. For most cases, this option can be left at the default setting.
Treat values of these <param> tags as URLs	Enter tags that you should be translated URLs. For most cases, this option can be left at the default setting.

6 Click *Modify*.

Once you have created network policies, you must apply these policies to users to make them effective.

When Policies Collide

When an HTTP request comes in to the NSP, the NSP does not know which application policy to apply because there is no application information provided in the request message. Therefore, the NSP performs a "reverse lookup" to determine which application policy to apply. A reverse lookup means the following:

- **Hostname**: For hostnames, the NSP checks for a matching hostname starting from the right. For instance, **webserver.com** matches **applications.webserver.com**
- **Path**: For paths, the NSP checks for a matching path from the left. For instance, **/webserver** matches any path that starts with **/webserver** such as **/webserver/applications**

The Application URL field on the Web Application General Properties page does not apply to policy and cannot be used as part of the matching criteria since it is simply a bookmark.

If the NSP finds multiple hostname matches, then the corresponding policies are merged and the least restrictive policies are applied by default.

For example, there are two Web applications, an email and a word processing application that have been configured on the NSP as shown in Figure 114. While these two applications appear to be quite different, they have the same policies with one exception, one allows cookies and the other denies cookies.

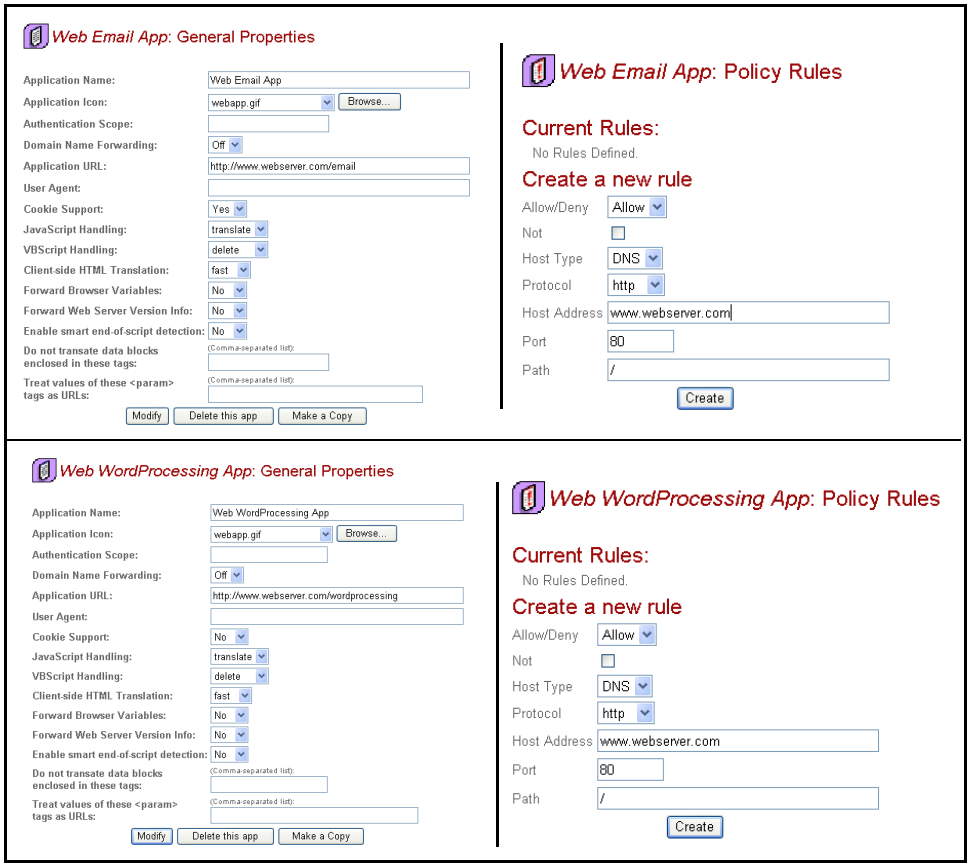


Figure 114 Multiple Web Policy Example

When an HTTP request comes in to the NSP, the NSP checks the hostnames from the right for a match. Because the policies for both of these Web applications have the same Host Address, the NSP must now break the tie between the two sets of policy rules.

In this example, the only determination to be made is whether or not to allow cookies since all other policy rules are the same. Because the least restrictive policy applies, cookies will be allowed.

One of the tie breaking rules is configurable, the rule for determining Client-Side HTML Translation. For details, refer to "Advanced Web Services Configuration" on page 114.

Applying Network Policies to Users

To apply network policies to users, do the following.

Alternatively, you can apply network policies via the Users or Group menu. For details, refer to "Managing User Accounts" on page 137.

1. From the Administrator Site, select *Applications*, and then *Network Policies*.
2. Under *Network Policies*, select the name of the network policy you want to apply.
3. Click *Authorized users*. In the Non-Members column, locate the name(s) of the users to which you want to assign the network policy.

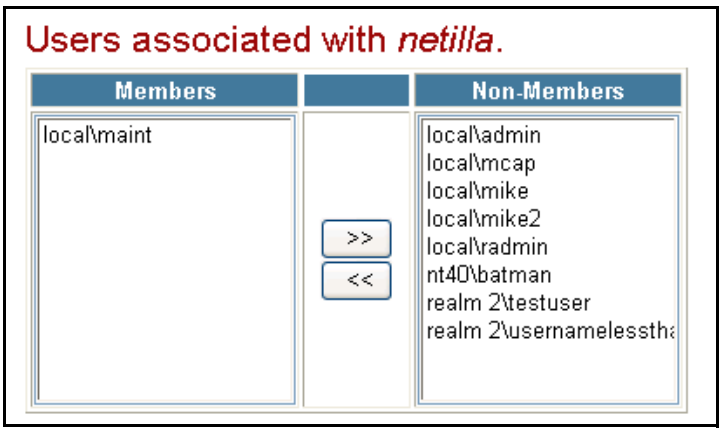


Figure 115 Network Policy Authorized Users Page

4 Click on the arrow button to move to the user name from the Non-Members column to the Members Column. Once the user is moved to the Members column, that user becomes a member. Changes take affect automatically.

Testing a Web Application

Once you have created a Web application you can test it to ensure that it works properly.

To test a newly-created application, do the following.

1 Log in as admin or radmin and then select the *Web* icon.

The application icon appears.

2 Click the icon. A separate browser window opens, initiating the connection through the NSP to the URL specified within the application's configuration.

Note the URL that appears in the Address field of the browser. The URL of the NSP precedes the URL of the internal web server, connection protocol, and the port number.

If the Web-based application does not open properly, refer to "Appendix A: Troubleshooting" on page 225.

Allow Users to Access a Web Application

Once created, Web applications are not accessible by end users until access to them is allowed.

Alternatively, you can assign applications to users via the Users or Group menu. For details, refer to "Managing User Accounts" on page 137.

To allow users to access Web applications, do the following.

1 From the Administrator Site, click *Applications* and then click *Applications*.

2 Select the name of the application that you want to allow users to access.

3 From the submenu of that application, select *Authorized Users* as shown in Figure 116.

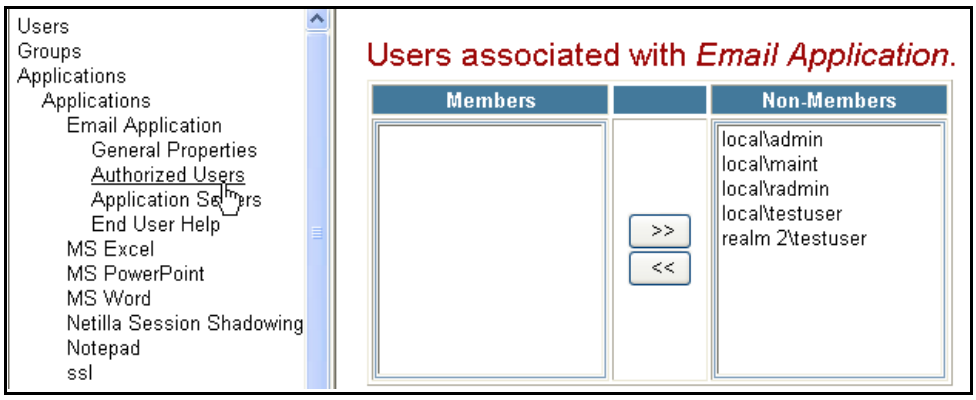


Figure 116 Authorizing Users to Access a Web Application

4 Use the arrow keys to move the users that you want to allow access to this application from the Non-Members column to the Members column.

Changes are saved automatically.

Advanced Web Services Configuration

This section describes advanced configuration parameters for Web services. It is recommended that you leave these fields set to their default values unless instructed otherwise by Netilla. Note that these are system-wide parameters. As such, they affect all Web application users.

Changes to these fields take effect immediately.

To configure advanced system-wide Web service parameters, do the following.

1 From the Administrator Site, click *Services* and then click *Web*.

2 Click *General Properties*. The Web settings page appears.

The advanced settings fields are shown in Figure 117.

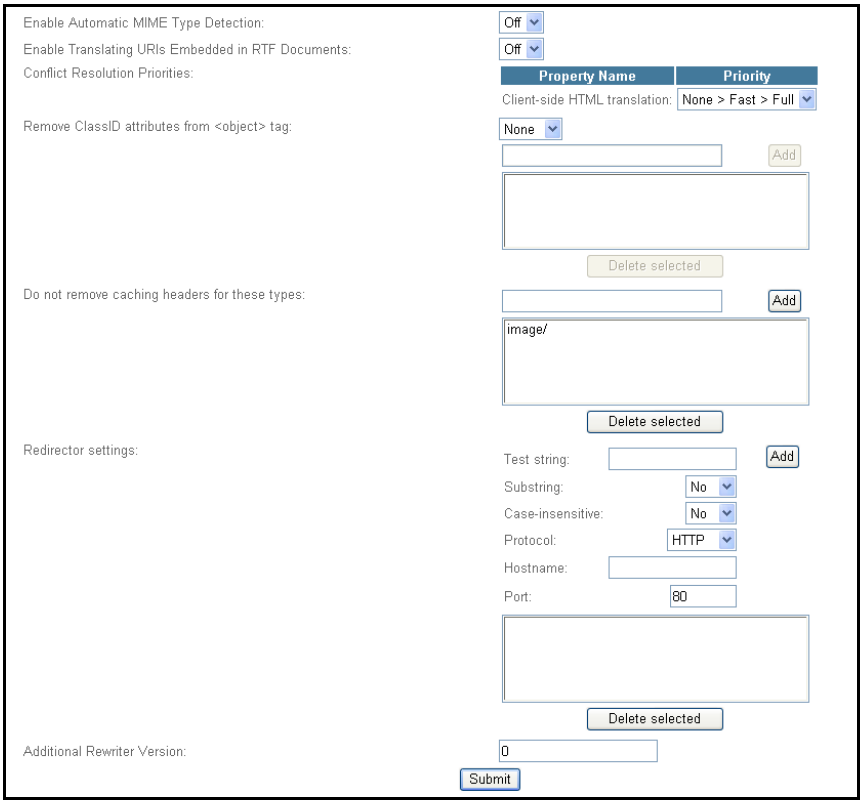


Figure 117 Web Service Advanced Parameters

The fields are described in Table 19.

Table 19 Advanced Web System Settings Fields

Field Name	Description
Enable Automatic MIME Type Detection	If a web server is providing inaccurate content type information, you can enable the NSP to automatically detect the correct MIME type. By default this field is set to *Off*. Select *On* if a web server is providing inaccurate content types.
Enable Translating URIs Embedded in RTF documents	If you have applications with RTF documents that contain links to resources located on a server behind the NSP, select *On* to enable these links to be translated. By default this field is set to *Off*. Leave this field set to Off unless you are certain that you have URIs embedded in RTF documents.
Conflict Resolution Priorities	If more than one policy rule matches a request for a Web resource, the least restrictive policy is used by default. This field allows you to override the least restrictive default and specify exactly how multiple policies are merged for the Client-Side HTML field. Choices are as follows: ▪ None>Fast>Full: None overrides Fast which overrides Full. ▪ Full>Fast>None: Full overrides Fast which overrides None.
Remove Class ID Attributes from <subject> tag	Some situations require the removal of references to ActiveX components. To do so, enter the class ID identifying the ActiveX component in this field.

Table 19 Advanced Web System Settings Fields

Field Name	Description
Do not remove caching headers for these types	For security reasons, web resources are not cached on users's computers. This requires the NSP to get the resource each time it is referenced. Because this process can slow down performance, you can set this field to MIME types of web resources that may be cached on a client's browser in order to improve performance. Note that the NSP never allows HTML pages to be cached.
Redirector Settings	This feature allows the NSP to intercept and redirect requests to the NSP that would otherwise be bypassed. Bypassing occurs when, for example, the HTTP request was issued by a Java applet or ActiveX component that had not been translated yet. ■ **Text string**: Enter the string that will be matched against a URL request. For example, if the request begins with**'/Exchange'** enter**'/exchange'**. ■ **Substring**: Select *Yes* to expand the test string search to include substrings. If set to *No*, the search only checks whether the URL starts with the text string. ■ **Case-insensitive**: Select *Yes* if you do not want case considered in the search for a match between the specified text string and URL request. ■ **Protocol**: Specify the protocol of the web server to which the request is redirected when a match occurs. ■ **Hostname**: Specify the hostname of the web server to which the request is redirected when a match occurs. ■ **Port**: Specify the port of the web server to which the request is redirected when a match occurs.
Additional Rewriter Version	For internal use only. Do not change the value in this field unless instructed to do so by Netilla Technical Support.

3 Configure the advanced fields as appropriate.

4 Click *Submit*.

Changes take effect immediately.

Java Applet Rewriting Module Configuration

If you are using web applications that use signed applets, these applets must be signed again as part of the NSP's HTML translation process. For security reasons, in order for the NSP to get the applets signed again, the NSP's administrator must approve the re-signing of the applets and a code signing certificate must be issued.

Setting up the Java applet rewriting module (JARM) involves the following main steps:

- Importing a Code Signing Certificate from a CA
- Configuring JARM
- Approving Applets for Rewriting

Also, additional information regarding code signing certificates is in “Code Signing Certificate Management” on page 118.

Importing a Code Signing Certificate from a CA

The NSP comes with a self-signed code signing certificate installed. While a self-signed certificate may be useful for initial set up and testing, it should not be used in a production environment. You should obtain a code signing certificate from a certificate authority.

Code Signing Certificate Type

When you request a code signing certification from a CA, make sure it meets the following specifications:

- **Format of the certificate**: Microsoft Authenticode (Multi-Purpose)
- **Certificate file extension:** SPC (Software publisher certificate)
- **Private key file extension**: PVK
- **Passphrase used to encrypt PVK file (when generating private key)**: empty(no encryption/password protection; JARM does not support using encrypted private keys)

It is highly recommended that you do not use self-signed certificates in a production environment as they represent a security risk. A valid code signing certificate should be obtained from a recognized CA.

Once you receive your code signing certificate, import it to the NSP as follows:

1. From the Administrator Site, click *Services*, and then click *Web*.
2. Click *JARM* and then click *Certificates*.

Figure 118 Import Code Signing Certificate Page

3. For Certificate, click *Browse* to locate the file containing the certificate you want to import.
4. For Private Key, click *Browse* to locate the file containing the private key for the certificate you want to import.
5. Click *Import*.

Configuring JARM

Configuring JARM requires notifying the NSP administrator of applets that need approval for resigning. To enter the contact information for the NSP administrator, do the following.

1. From the Administration Site, click *Services* and then click *Web*.
2. Click *JARM* and then click *General Settings*.

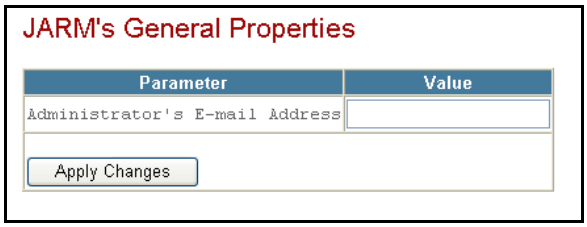


Figure 119 JARM General Properties Page

3. Enter the email address of the NSP administrator who will approve any applet resigning that is required.
4. Click *Apply Changes*.

Approving Applets for Rewriting

Once the NSP is set up, log in as a user and test your Web applications. If any of your Web applications have Java applets that require re-writing, you will receive an email notification.

To approve Java applets for re-writing, do the following.

1. From the Administration Site, click *Services* and then click *Web*.
2. Click *JARM* and then click *To be approved*.

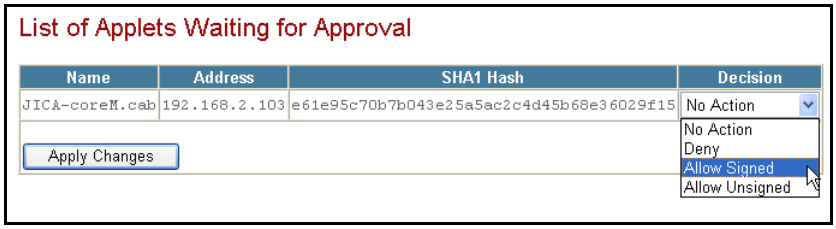


Figure 120 JARM Applet Approval Page

3. Under the Decision column, approve the applets for rewriting.
4. Once the applets are approved, test the Web application.

Code Signing Certificate Management

Although the NSP comes with a self-signed code signing certificate pre-installed, you should use a code signing certificate from a certificate authority.

This section describes the following:

- Code Signing Certificate Type
- Import a Code Signing Certificate from a Certificate Authority
- Generate a Self-Signed Certificate

Code Signing Certificate Type

When you request a code signing certification from a CA, make sure it meets the following specifications:

- **Format of the certificate**: Microsoft Authenticode (Multi-Purpose)
- **Certificate file extension:** SPC (Software publisher certificate)
- **Private key file extension**: PVK
- **Passphrase used to encrypt PVK file (when generating private key)**: empty(no encryption/password protection; JARM does not support using encrypted private keys)

Import a Code Signing Certificate from a Certificate Authority

To import a code signing certificate, do the following.

1 From the Administrator Site, click *Services*, and then click *Web*.

2 Click *JARM* and then click *Certificates*.

Figure 121 Import Code Signing Certificate Page

3 For Certificate, click *Browse* to locate the file containing the certificate you want to import.

4 For Private Key, click *Browse* to locate the file containing the private key for the certificate you want to import.

5 Click *Import*.

Generate a Self-Signed Certificate

You can generate a self-signed certificate on the NSP for code signing. A self-signed certificate is not automatically recognized by users' browsers. If you connect to an NSP without a CA-signed certificate, a warning message informs you that the certificate has not been signed by a recognized authority.

It is highly recommended that you do not use self-signed certificates in a production environment as they represent a security risk. A valid certificate should be obtained from a recognized CA.

To generate a self-signed certificate, do the following.

1 From the Administrator Site, click *Services*, *Web* and then click *JARM*.

2 Click *Certificates* and then click *Self-Signed*.

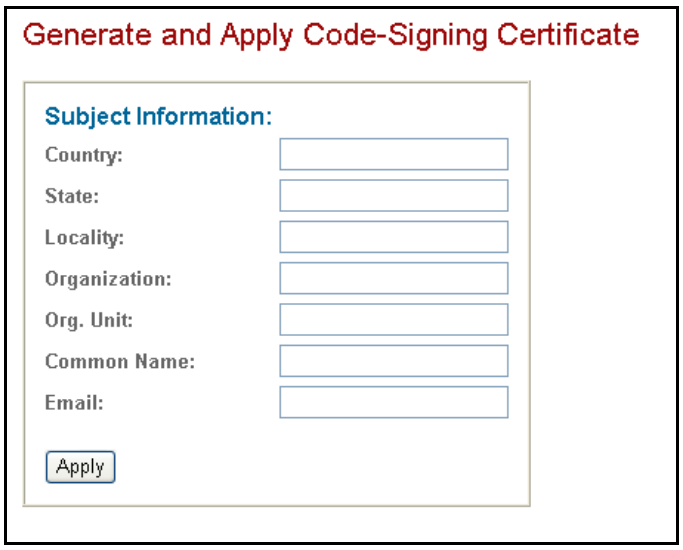


Figure 122 Self Signed Certificate Page

3 Enter the following information:

Table 20 Self-Signed Code Signing Certificate Fields and Descriptions

Field Name	Description
Country	The two-letter ISO abbreviation for your country (for example, *US* for the United States). For the ISO country list, see http://www.iso.org/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.html
State	The state or province in which your organization is headquartered. Enter the full name of the state or providence; abbreviations are not allowed.
Locality	City in which your organization is headquartered.
Organization	The name under which your organization is registered. This organization must own the domain name that appears in the common name of your NSP. Abbreviations and the following characters are not allowed < > ~*!* @ # $ % ^ * / \ ( ) ?.
Org. Unit	The name of the department or group that will be using the NSP.
Common Name	The name of your NSP as it appears in the server's URL (for example, *companyname.netillavo.com*). The Common Name must be identical to the fully qualified domain name of the NSP for which you are requesting a certificate. If the NSP name does not match the common name in the certificate, some services will fail to work. Do not include the protocol specifier (http://) or any port numbers or pathnames in the common name. Wildcards such as * or?, or IP addresses are not allowed.
Email	Email address of the contact person for the department or group using the NSP.

4 Click *Apply*.

Java Applet Sockets Network Policy

The Java Applet Sockets network policy applies to Web applications that contain Java applets that require making another connection (UPD or TCP) beyond the NSP. To ensure the that this second connection is secure, a network policy must be configured on the NSP that defines which of the servers located behind the NSP this applet can access.

To define a Java Applet Socket network policy, do the following.

1 From the Administrator Site, click *Applications*, and then click *Network Policies*.

The Create a New Network Policy page appears.

Figure 123 Create New Network Policy Page

2 Enter a **Name** for the network policy that you are creating.

Use a descriptive name to make it easier to identify when it comes time to apply the policies.

3 Select Java Applet Sockets from the **Network Policy Type** drop down list box and then click *Submit*. This policy appears in the Network Policy submenu.

4 Select the policy name from the menu to expand the sub menu and then select *General Properties*.

The General Properties page for network policy for TPD is shown in Figure 124.

Figure 124 Policy Rules Page for TPD Network Policy

5 For **Allow/Deny** select *Allow*.

6 For **Address**, specify the IP **Address** of the back end server the applet will be accessing.

7 For **Port**, enter the TCP or UDP port number to be used.

8 For **Protocol,** select *TCP, UDP* or *Any* which allows either protocol. Also, you can allow all ports by entering zero.

9 *Ranges are also supported. Use a colon or dash as a separator.*

10 Click *Create*.

The policy appears above the policy creation fields.

11 Create additional rules as needed.

6 Configuring the Tunnel Service

The Netilla Security Platform (NSP) supports locally installed client/server applications allowing users to work live between applications that reside both locally and on a server over the Tunnel. In addition, this functionality enables users to work offline with their local PC-based applications - such as Outlook mail clients, CRM, sales tools or productivity applications - and update their files and data when an Internet connection becomes available. This provides functionality that is similar to an IPSec tunnel, but with much less complexity required.

This section describes how to configure Tunnel applications. There following topics are covered.

- Understanding the Tunnel Service
- Configuring the Tunnel Service
- Adding Members to the Tunnel Service
- Creating an Tunnel Application
- Configuring Tunnel Policy
- Allow Users to Access an Tunnel Application
- Example Tunnel Configuration

Prerequisites

Before you begin to configure the Tunnel service, do the following.

- **Obtain an Tunnel License**. The Tunnel service requires an additional license to be purchased and installed on the NSP.
- **Enable IP Forwarding**. IP forwarding must be enabled for Tunnel applications to work. Refer to "Configuring IP Forwarding and NAT" on page 20.
- **Check for potential IP address conflicts**. If you have a home network on 192.168.0.X or 192.168.1.X and your company uses the same IP address range, you may experience routing problems and be unable to communicate with the corporate network over the SSL VPN Tunnel. It is recommended that you change your home network to another IP segment such as 192.168.3.X. Refer to the instructions that came with your home router or cable modem for details.

Understanding the Tunnel Service

Configuring the Tunnel service involves enabling the service and then setting up user access controls. User access controls are configured and enforced using Tunnel policy settings. Policy settings are rules or instructions that you create to dictate the manner in which the NSP handles user requests for access.

Specifically, the VPN policy settings define dynamic Netilla firewall rules that allow input or output ports to be opened for a range of protocols. Rules also control traffic to and from the remote computer and the corporate network. The

Netilla dynamic firewall opens the application-specific back end ports each time a user initiates an Tunnel. These ports are subsequently closed when the user exits their Tunnel session.

Multiple rules can be created that dictate the client/server applications that the user is allowed to use. For example, if using a POP3 mail client, you might create rules that allow the POP3 protocol for retrieving mail, and SMTP for sending mail. If a user attempts to launch an application that uses a port that has not been allowed, traffic to that port will be blocked. This effectively denies a user the ability to access a client/server application, even if the application resides on the user's local device.

While Tunnel policy uses the same underlying infrastructure as the Netilla firewall, Tunnel policy rules are independent of Netilla firewall rules. The Netilla firewall controls traffic on the NSP's primary and secondary Ethernet interfaces (i.e., eth0, and eth1) whereas Tunnel policy controls traffic on the NSP's PPP interface. For example, if the Netilla firewall is turned off, Tunnel policy is not affected.

Configuring the Tunnel Service

To access client/server applications via an Tunnel, you must enable the Tunnel service and configure client IP address information.

Make sure that IP Forwarding is enabled as described in "Configuring IP Forwarding and NAT" on page 20.

To enable the Tunnel service, do the following.

1. From the *Administrator* site, click *Services* and then click *Tunnel*.
2. From the Tunnel submenu, select *General Properties*. The Tunnel Settings page appears as shown in Figure 125.

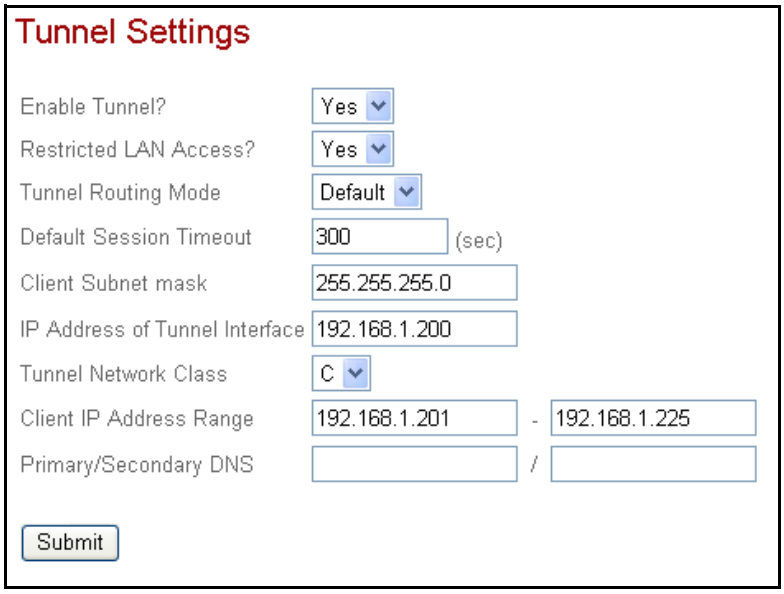


Figure 125 Tunnel Settings Page

3. For **Enable Tunnel**, select *Yes*.

4 **Restricted LAN Access** indicates whether or not Tunnel policy is enforced. Select Yes or No as appropriate. It is strongly recommended that you select *Yes* to prevent unauthorized client applications from accessing any resource on a private network.

Selecting *Yes* enables you to control which local applications a particular user is allowed to use over the tunnel.

Selecting *No* allows ANY type of connection through the tunnel (such as FTP, SMTP) as well as a connection from the server to the client.

If you select Yes for Restricted LAN Access*, you must configure the applications users may access and the policies that allow users to access only those applications. Refer to "Creating an Tunnel Application" on page 128 for details. If you select No, the user has access to all local client/server applications they have on their computer. Therefore, no application configuration is required.*

5 (Optional) **Tunnel Routing Mode** allows you to specify the Tunnel as the client's default gateway by selecting *Default*. Alternatively, you can select *Split* to specify that only traffic destined for the company's internal network and any additional subnets that are specified are accessible during a Tunnel session.

6 (Optional) **Default Session Timeout** sets the time that the NSP keeps the Tunneling connection open with non-activity. Any activity results in the connection being re-established transparently to the client application. The default is 5 minutes. Note that this timeout does not affect the users's session. The user remains connected unless disconnected for other reasons.

7 For **Client Subnet Mask**, type the subnet mask that will be assigned to the remote user when he/she is given an IP address from the specified range of IP addresses described in step 8.

8 For **IP Address of the PPP interface**, type the IP address that is given to the NSP's PPP interface. This should be an available IP address on the internal LAN and must be different than the internal IP address already assigned to the NSP. All remote users will go through this interface to get to the specified segment.

9 For **PPP Network Class** specify the number of addresses that the NSP recognizes as available. This configuration validates the range of IP addresses configured in the Client IP Address Range field. Setting this field to C acknowledges the first 3 octets of the subnet mask. Setting this field to B acknowledges the first two octets.

10 For **Client IP Address Range**, type the range (scope) of IP addresses that the NSP gives to the remote users. The range entered here must be an available range of IP addresses on the target LAN.

11 (Optional) For the **Primary/Secondary DNS** fields, specify the DNS servers that the remote clients will use after initiating the SSL session. If left blank, then DNS server(s) on your company's network will not be available.

12 Click *Submit*.

If you need to specify another network that users can access during an Tunnel connection, refer to "Adding Another Network Accessible by the Tunnel" on page 126. Otherwise, go on to "Adding Members to the Tunnel Service" on page 127.

Adding Another Network Accessible by the Tunnel

To specify another network that users can access during an Tunnel connection, do the following:

1. From the Administrator Site, click *Services* and then click *Tunnel*.
2. From the Tunnel submenu, select *General Properties*.
3. For Tunnel Routing Mode, select *Split* and then click *Submit*.
4. Under Additional Networks Accessible by Tunnel (as shown in Figure 126), enter the IP address in the field on the left and the subnet mask in the field on the right.

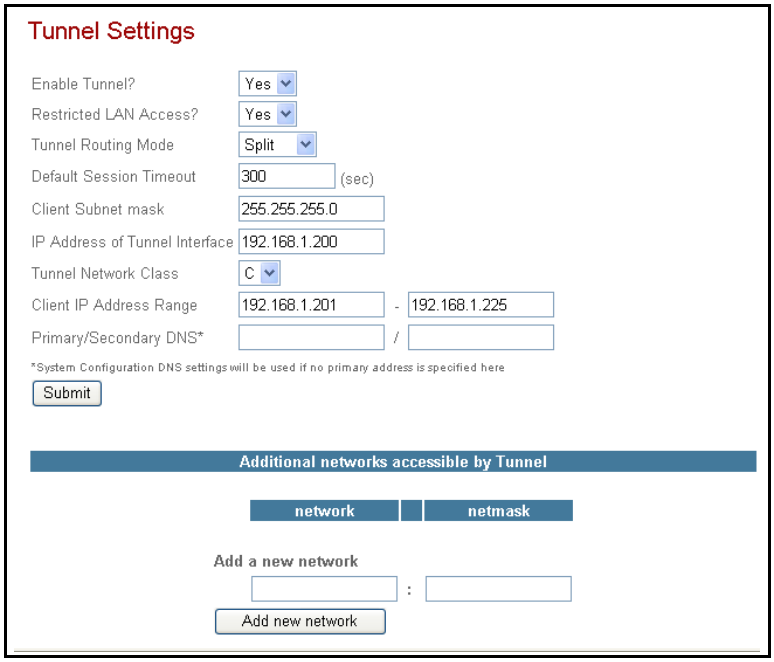


Figure 126 Accessing Additional Networks via Tunnel Page

5. Click *Add new network*.

Accessing Another Network by the Tunnel Example

The following network diagram shows an example of a network where the NSP is connected to the public network on the primary interface, with an IP address of *208.206.100.1*, and the secondary interface with an IP address of *192.168.1.300* connected to a network where only servers reside. This network has segregated some servers from the end user network, and this server-only network is assigned the IP address *192.168.1.310*. At this point, the only application servers the NSP can access are those on the *192.168.1.310* network. However, there is an application server on another network with an IP address of 10.1.1.0, separated by a router. This router has an IP address of 192.168.1.301, and is on the 192.168.1.300 network.

An example of this network scenario is shown Figure 127.

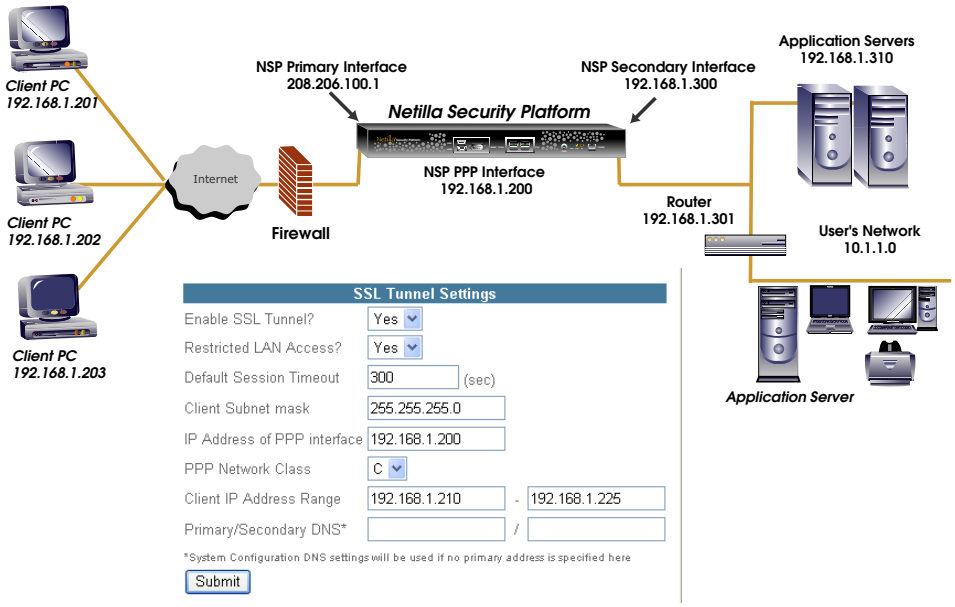


Figure 127 Adding Another Network for Tunnel Access Example

What is needed is a method to allow the NSP to see the *10.1.1.0* network and application server, to allow the NSP to host Tunnel sessions for end users who need to access that application server. This is accomplished by adding that network route (10.1.1.0 in this example) to the NSP using the Add a New Network field as shown in Figure 128.

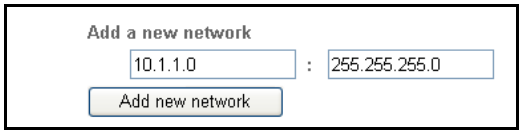


Figure 128 Add a New Tunnel Network Example

In this example, the User's Network, 10.1.1.0 may have to be added to the NSP's static route table depending on the configuration of the NSP's default route. Refer to "How to Configure a Static Route" on page 22 for details.

Go on to "Adding Members to the Tunnel Service" on page 127.

Adding Members to the Tunnel Service

To authorize users to access the Tunnel service, do the following.

1 From the Administration Site, click *Services* and then click *Tunnel*. The Tunnel Settings page appears.

2 Use the arrow keys to move users under the Members column that you want to allow access to Tunnel applications.

Changes are saved automatically.

If you select Yes for Restricted LAN Access (via he Tunnel Settings page shown in Figure 125), you must configure the applications users may access and the policies that allow users to access only those applications. Refer to "Creating an Tunnel Application" on page 128 for details. If you select No, the user has access to all local client/server applications they have on their computer. Therefore, no application configuration is required.

Creating an Tunnel Application

Creating an Tunnel application is required when you select *Yes* for the Restricted LAN Access field which provides maximum security by controlling which local applications a user is allowed to use over the Tunnel.

To create an Tunnel application, do the following.

1 From the Administrator Site, click *Applications* and then click *Applications* as shown in Figure 129.

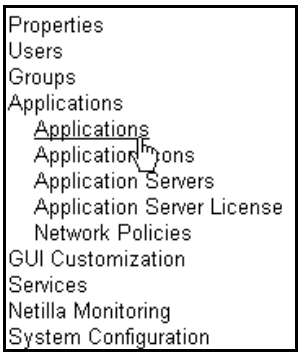


Figure 129 Applications Sub Menu

The create a new application page appears.

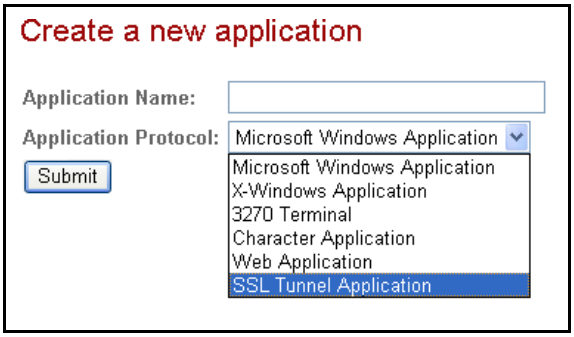


Figure 130 Create a New Application Page

2 Enter a name for your new Tunnel application, and then choose *Tunnel Application* as the Application Protocol.

3 Click *Submit*.

You are then presented with the new application's General Properties page. An example is shown in Figure 131.

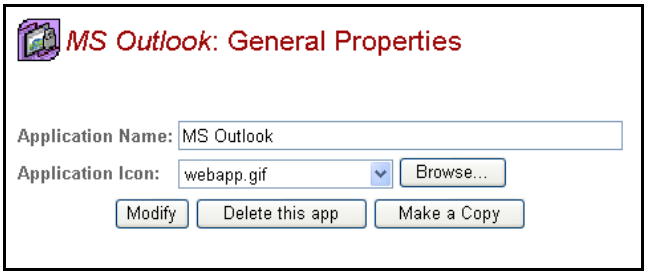


Figure 131 Application General Properties Page

4 Choose an icon for the application (or leave the default).

5 Click *Modify*, and the page refreshes.

Go on to "Configuring Tunnel Policy" on page 129.

Configuring Tunnel Policy

Unlike Thin applications, Web and Tunnel applications require the client computer to have access via the NSP to the back-end server. After a Web or Tunnel application is created on the NSP, at least one policy rule must be created for each application to allow users to access the application. This section describes how to configure policy for Tunnel applications.

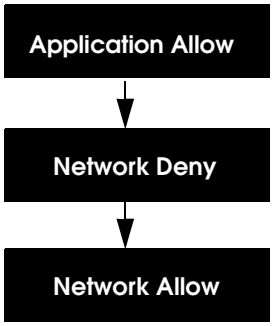
About Application and Network Policy

There are two types of policy that can be created for an Tunnel application, application policy and network policy. With application policy, you can greatly control user access by directing users to specific locations on a server to which you want to allow access. Network policies are more general and typically allow users to have wider access. As such, network policies do not provide as stringent policy as application policies and, if configured, should only be done so sparingly.

A typical policy configuration would prevent users from accessing a particular subnet yet allow users to access a couple of applications that reside on the subnet. To configure this scenario, a network policy rule is created to deny access to the subnet. Then, an application rule is created that allows access to a particular application. With this configuration, the user can only access the application and cannot access any other resources on the subnet.

Application and Network Policy Processing

When a user tries to connect to the NSP's Tunnel service, all application and network policies are evaluated and processed in the following order:



Based on the typical scenario where a network policy rule is created to deny access to a subnet and an application rule is created that allows access to a particular application on that subnet, the policy processing would work as follows.

First, the NSP checks to see if there are any application rules that allow access to this user. Based on the typical scenario, there is an application rule that allows access to a particular application. The user is granted access to the application and no further checking is performed by the NSP. The NSP takes the first rule that matches.

If there were not any application policy rules that allowed access to this user, network deny rules would be checked. If a network deny rule exists, the user is not granted access and no further checking is required. If there are no network deny rules for this user, network allow rules are checked.

To activate policy changes made during an active session, the user must log out and in again for the change to take affect.

Best Practices for Tunnel Policy Configuration

- Set the Restricted LAN Access setting to *Yes* to enable policy enforcement.
- Application policy is preferred over network policy because network policy tends to be more liberal and therefore less secure.
- Use network policy carefully and sparingly.

Adding Policy to an Tunnel Application

This section describes how to add policy to an Tunnel application. Depending on the type of policy you want to create, the configuration steps will vary.

If you add policy to Tunnel applications, Restricted LAN Access must be set to Yes *as described in "Creating an Tunnel Application" on page 128.*

Creating a Rule to Allow Access to an Tunnel Email Application

For example, to add a rule that allows access to an email server (IMAP) with an IP address of 192.168.1.22 on eth0, do the following.

1. From the Administrator Site, click *Applications* and then click *Applications*.
2. Click the name of the Tunnel application to which you want to add policy.
3. Below the name of the Tunnel application, on the left hand side, click *Policy Rules*.

   The Policy Rules page for the Tunnel application appears.

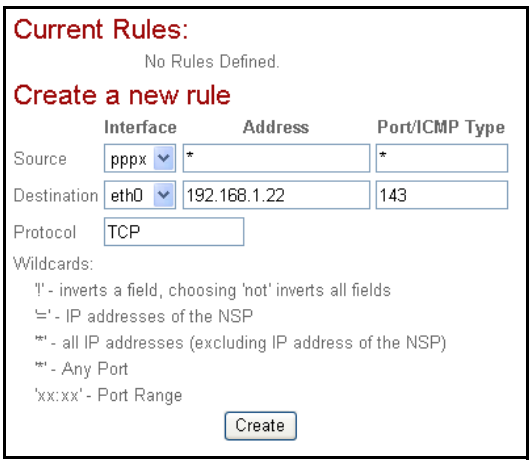


Figure 132 Policy Rules Page for Tunnel Applications

Depending on the type of policy you want to create, the configuration steps will vary. Specify the allowed **Source**.

- **Interface:** Select from the following source interfaces: pppx, eth0, eth1, lo (local which is the NSP itself) or Any (any includes pppx, eth0, and eth1. Local is not included when Any is selected). For this example, select *pppx*.

Source will always be set to "pppx" (the name of Netilla Virtual Adapter) for incoming connections. When "pppx" is the Source interface the Address and Port/ICMP Type fields are configured with asterisks (*).

- **Address**: Insert an asterisk (*) to have the rule pertain to all Netilla Virtual Adapter connections. Alternatively, a specific address may be entered.
- **Port/ICMP Type**: Insert an asterisk (*) to allow a connection from the Netilla Virtual Adapter. Alternatively, a particular incoming port could be specified.

4 Specify the **Destination**.

- **Interface:** Select from the following destination interfaces: pppx, eth0, eth1, lo (local which is the NSP itself) or Any (any includes pppx, eth0, and eth1. Local is not included when Any is selected).
- **Address**: Enter the IP address of the server you want to connect to.
- **Port/ICMP Type:** Enter the common port number for the server (143).

5 For **Protocol**, enter the appropriate protocol.

6 Click *Create*. The new rule appears.

Some applications may require another rule to be created that the server to access the client.

Creating Network Policy for Tunnel Applications

To configure network policy for Tunnel applications, do the following.

1 From the Administrator Site, click *Applications*, and then click *Network Policies*.

The Create New Network Policy page appears.

Figure 133 Create New Network Policy Page

2 Enter a **Name** for the network policy that you are creating.

3 Select Tunnel from the **Network Policy Type** drop down list box.

Use a descriptive name to make it easier to identify when it comes time to apply the policies.

4 Click *Submit*.

The Tunnel General Properties page appears.

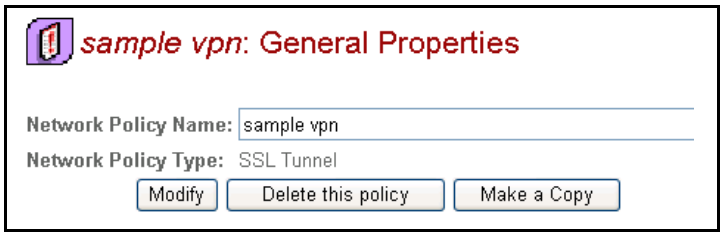


Figure 134 Tunnel General Properties Page

5 From the menu on the left, under the Network Policy Name you just created, select *Policy Rules*. The Rules page appears as shown in Figure 135.

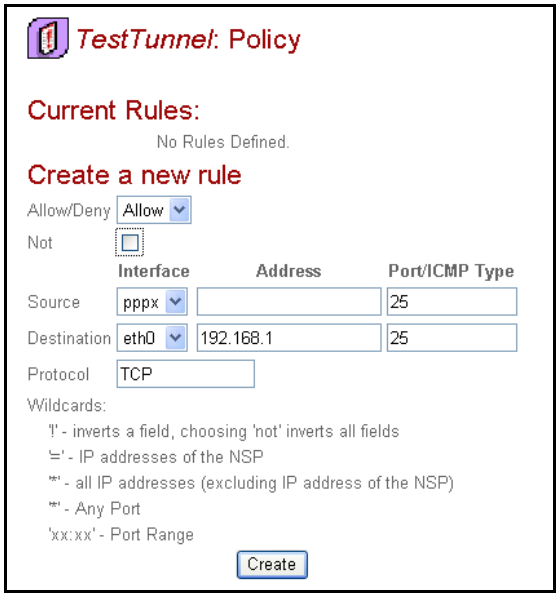


Figure 135 Create a New Rule Page

6 For Allow/Deny, select *Allow*.

7 Specify the allowed **Source**.

- **Interface:** Select from the following source interfaces: pppx, eth0, eth1, lo (local which is the NSP itself) or Any (any includes pppx, eth0, and eth1. Local

is not included when Any is selected). For this example, select *pppx* which is the Netilla Virtual Adapter.

Source will always be set to "pppx" (the name of Netilla Virtual Adapter) for incoming connections. When "pppx" is the Source interface the Address and Port/ICMP Type fields are configured with asterisks (*).

- **Address**: Insert an asterisk (*) to have the rule pertain to all Netilla Virtual Adapter connections. Alternatively, a specific address could be entered.
- **Port/ICMP Type**: Insert an asterisk (*) to allow a connection from the Netilla Virtual Adapter. Alternatively, a particular incoming port could be specified.

8 Set the **Destination Interface** to eth0 to allow the connection to come in over the primary interface of the NSP.

- **Address**: Enter the IP address of the IMAP server.
- **Port/ICMP Type:** Enter the common port number for the IMAP server (143).

9 For **Protocol**, enter *TCP*.

10 Click *Create*. The new rule appears.

Changes are saved automatically.

Go on to "Example Tunnel Configuration" on page 134 to add members to the Tunnel service.

Applying Network Policies to Users

Once you have created network policies, you must apply these policies to users in order to make them effective.

To apply network policies to users, do the following.

Alternatively, you can apply network policies to a realm, individual user or a group. For details, refer to "Managing User Accounts" on page 137.

1 Select *Applications*, and then *Network Policies*.

2 Under *Network Policies*, select the name of the policy object.

3 Click *Authorized users*. In the Non-Members column, locate the name(s) of the users to which you want to assign the network policy.

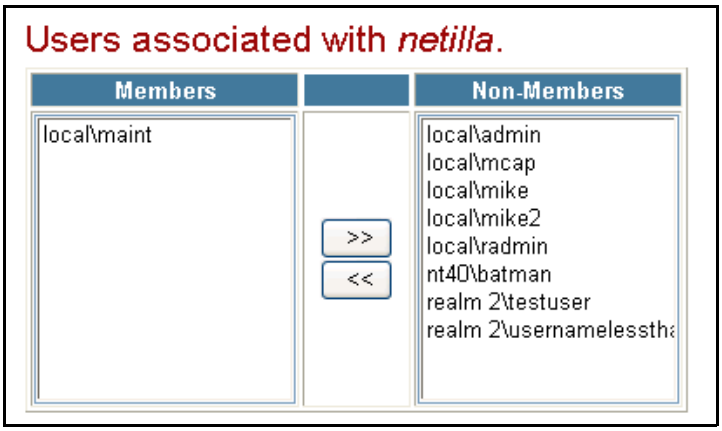


Figure 136 Network Policy Authorized Users Page

4 Click on the arrow button to move to the user name from the Non-Members column to the Members Column. Once the user is moved to the Members column, that user becomes a member. Changes take affect automatically.

Allow Users to Access an Tunnel Application

Once created, Tunnel applications are not accessible by end users until access to them is allowed.

Alternatively, you can assign applications to users via the Users or Group menu. For details, refer to "Managing User Accounts" on page 137.

To allow users to access Tunnel applications, do the following.

1 From the Administrator Site, click *Applications* and then click *Applications*.

2 Select the name of the application that you want to allow users to access.

3 From the submenu of that application, select *Authorized Users* as shown in Figure 137.

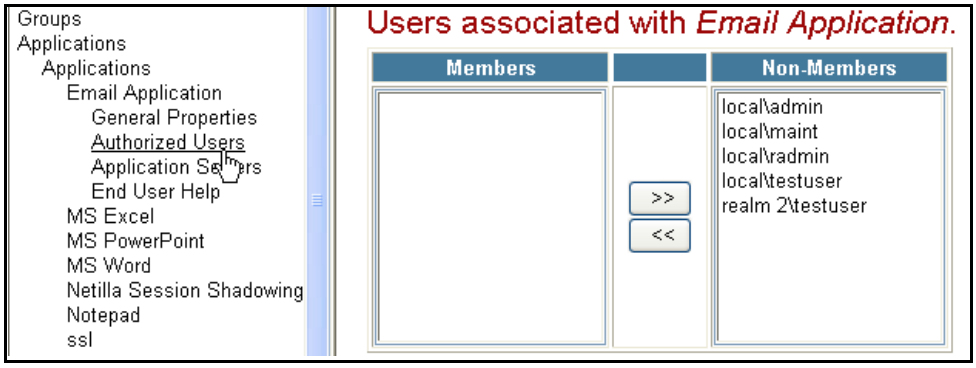


Figure 137 Authorizing Users to Access an Tunnel Application

4 Use the arrow keys to move the users that you want to allow access to this application from the Non-Members column to the Members column.

Changes are saved automatically.

Example Tunnel Configuration

This section provides an example network scenario and lists the configuration steps. For this example, the Tunnel service is configured based on the network set up shown in Figure 138. Users will be allowed to access only the applications that they need.

The main steps for configuring this Tunnel configuration example are as follows:

1 **Enable the Tunnel Service**

2 **Add Members to the Tunnel Service**

3 **Create Tunnel Applications**

4 **Create Rules to Allow Access to the Tunnel Applications**

5 **Allow Users to Access Tunnel Applications**

1. Enable the Tunnel Service

The first step for configuring this scenario is to configure the Tunnel Settings which include enabling the service and configuring the client IP addresses. The sample network scenario and the Tunnel service settings for the sample network are shown in Figure 138.

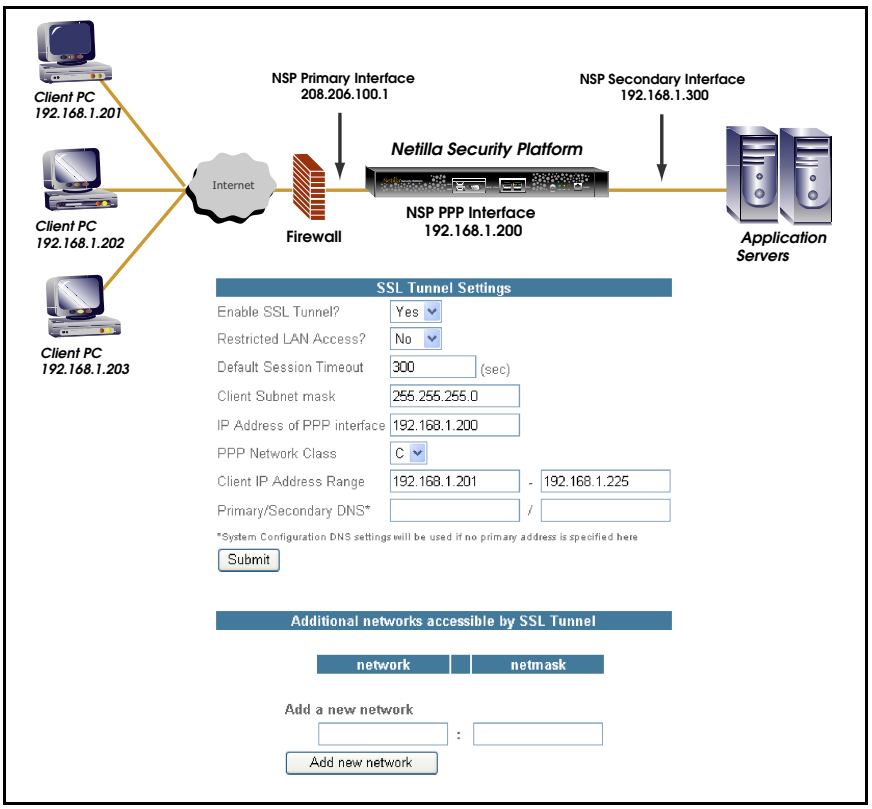


Figure 138 Sample Tunnel Configuration

2. Add Members to the Tunnel Service

Click *Services* and then click *Tunnel*. From the Tunnel Settings page, use the arrow keys to move users under the Members column that you want to allow access to Tunnel applications.

3. Create Tunnel Applications

Because *User Access Restrictions* is enabled, applications that users are allowed to access must be created. For this example, an email application will be created.

From the Administrator Site, click *Applications* and then click *Applications. Select Tunnel Application.* A name and an icon is selected for the application object. For this example, the following was entered.

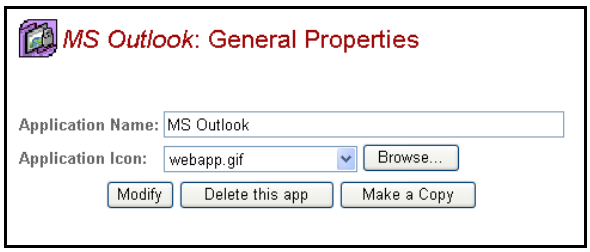


Figure 139 Tunnel Application Creation Example

4. Create a Rule to Allow Users to Access this Application

The previous step created an application object on the NSP. A rule must be created that allows users to connect to the email server. For instance, a rule is added that allows access to an email server (IMAP) with an IP address of 192.168.1.22 on eth0, as follows.

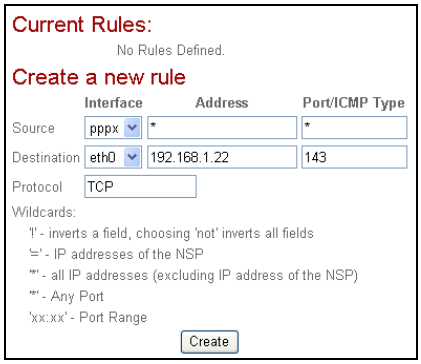


Figure 140 Rule Configuration Example

5. Allow Users to Access Tunnel Applications

Click *Applications*, *Applications* and then select the name of the application that you want to allow users to access. From the submenu of that application, select *Authorized Users*. Use the arrow keys to move users under the Members column.

7 Managing User Accounts

This chapter describes how to configure and manage user accounts on the Netilla Security Platform (NSP). The following topics are discussed.

- User Accounts on the NSP
- User Profiles and Policies
- Creating Users on the NSP
- Creating Groups on the NSP
- Creating an External NT Global Group
- Modifying NSP Administrator Accounts

User Accounts on the NSP

There are two main ways of adding users to the NSP, either individually or in groups for ease of configuration. Groups provide an easy way to publish applications to many users simultaneously. This is accomplished by applying policy settings to the group rather than each individual user. All applications published for the group will be subsequently inherited by the group members.

Because NT global groups are automatically created when the user logs in, it is recommended that you create a user on the Domain Controller that is a member of all the groups you wish to work with. Then, log in to the NSP as that user to automatically create the groups on the NSP.

There are two types of users, local and external.

- **Local Users**

  Local Users have accounts that are created and stored on the NSP. The NSP Administrative accounts are listed under the local users menu.

- **External Users**

  External Users are accounts that exist outside the NSP and are stored in an external account database, such as a Windows NT or 2000 Domain Controller. Currently supported authentication servers are RADIUS, SecurID, Kerberos, SMB (Windows domain).

All user accounts also have a profile associated with them, regardless of their type. The profile contains configuration information used by the NSP to customize what the user sees when logged in.

Profiles for local users are created when the local user is configured on the NSP. Profiles for external users, can be pre-created, or the NSP will create one the first time the user logs in.

User profiles are based on the following information.

- The realm the user is authenticated to, including applications, network policies and client drive mapping policies assigned to the realm.
- Group membership of the user, and applications, network policies and client drive mapping policies associated with that group.
- User properties including the settings in the Services menu, such as the Default Startup Service and network policies defined and applied to the user's object.

User Profiles and Policies

NSP policy management allows an administrator to control who can log in to the NSP and which applications and services users can access once they are logged in.

About User Profiles and Groups

Unlike a login account, which can be stored either internally or externally, a user's profile is always stored and maintained locally on the NSP, regardless of the authentication employed for that user.

A profile is automatically created for each new user that logs in for the first time. It is also possible to create and configure a user's profile prior to initial login. User profiles are located under the realm into which they login; the profile name is a combination of the realm plus the user name. For instance, **local/jsmith**. Profiles are made up of a combination of user settings that are used to create the user's webtop.

About Policy Management

Policy management allows the Netilla Administrator to manage a user's login permissions and to control access to the available applications and services of the NSP.

Policies are used to provide a common set of applications and network access restrictions for groups or individuals. Netilla policies preclude a user from accessing applications and resources for which they have not been authorized. A user is presented only with the applications they have been assigned to use, allowing a Netilla administrator to streamline application resources by job, role or departmental needs.

User Profile Configuration options

The following list details the various options available when configuring a user's profile.

- Publish applications to the user
- Assign the services that will be available to the user
- Assign the start-up service for the user
- Reset password (Local groups only)
- Set group membership (Local groups only)
- Restrict access to the Service Tabs (i.e., Files, Apps, Web, Tunnel, Admin)
- Assign network policies to Tunnel and Web applications
- Assign client drive mapping policy to users (applies to Thin applications only)

Creating Users on the NSP

This section explains how to create and modify local users/local user profiles. This section may also be used to create external user profiles.

If you created an internal authentication store (as described in "Creating an Internal Authentication Data Store" on page 63), then the users you configure will not appear in the appropriate realm in the Users menu until they log in for the first time.

1 From the Administrator Site, click *Users* as shown in Figure 141. The realms that have been created are listed.

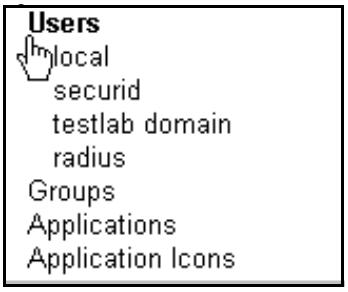


Figure 141 Users Submenu

The local realm is always shown and cannot be deleted because it contains the NSP administrator accounts.While you can add users to the local realm, it is typically used for administrators only. Note that adding a user to the local realm does not grant administrator rights to that user.

2 Choose the name of the realm in which you want to create a user profile.

The New User dialog box opens.

3 Type in a name for the User or Profile.

4 Click *Create User,* as shown in Figure 142.

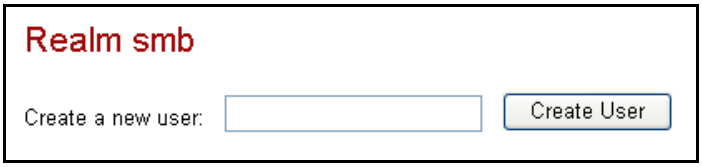


Figure 142 New User Window

The new user is added to the realm.

5 Click the name of the realm you just created. For the example in Figure 143, click *newuser* to expand the configuration page for this user.

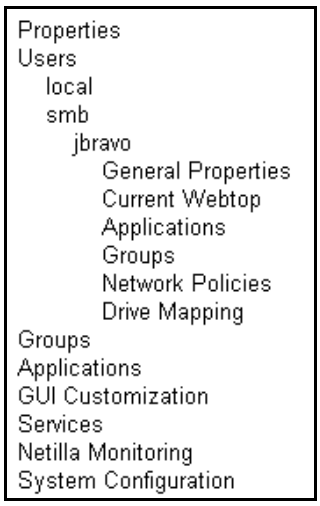


Figure 143 User Submenu

The Properties window for *newuser* opens, as shown in Figure 144.

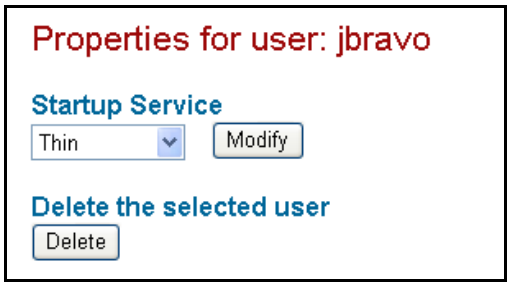


Figure 144 User Properties Window

6 Select the Startup Service to set the default service that will be displayed at initial login.

7 Click *Modify* to save the changes.

8 If you want to change the password, type the identical password in the New Password and New Password Confirm fields.

You may or may not see a **Change Password** section depending on the type of authentication used in this user's realm. Password changing is permitted for SMB and local authentication stage types. Password changing is not permitted for RADIUS, SecureID and Kerberos authentication stage types.

Also note that there may be more than one Change password field if multiple authentication stages are used in this user's realm and the authentication types allow password changing.

These fields are case-sensitive.

9 Click *Update Password* to save the changes.

If you changed the password, log out and log in again using the new password.

10 Choose *Current Webtop* from the left pane to view applications assigned for this user.

The applications that are currently assigned to this user are displayed, as shown in Figure 145.

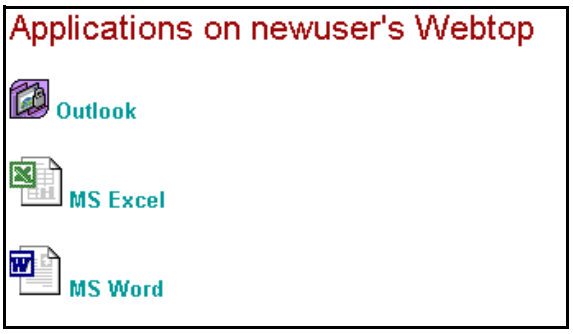


Figure 145 Applications Assigned for Webtop Window

11 Choose *Applications* from the left hand pane to manage applications for the user.

The Applications Associated with *newuser* window are displayed, as shown in Figure 146.

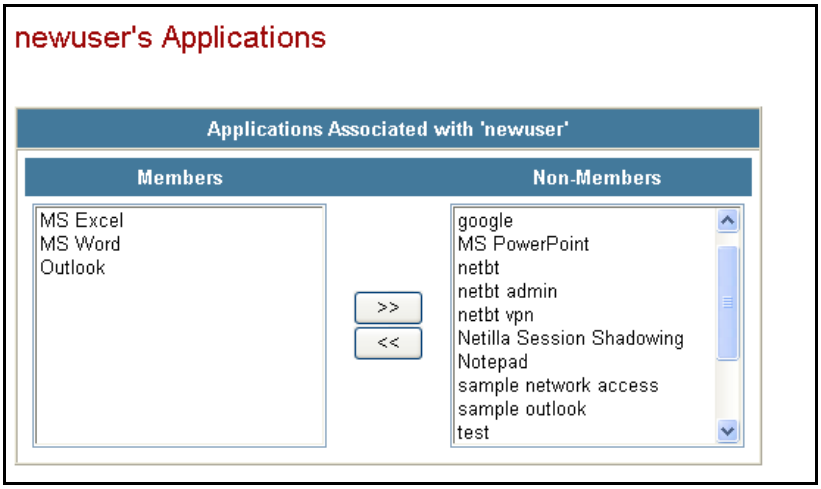


Figure 146 Applications Associated with User Window

12 Use the arrow keys to move the applications that you want this user to be able to access to the Members column.

13 Choose *Groups* from the left hand pane to add the user to a group.

The Local Groups window are displayed, as shown in Figure 147.

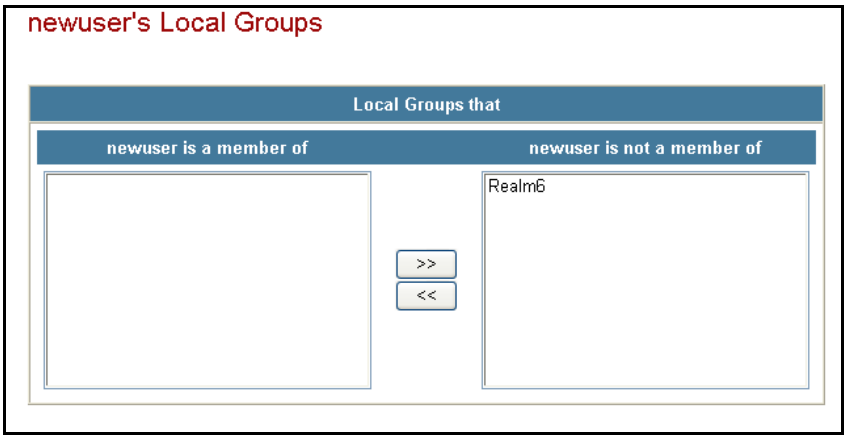


Figure 147 User's Groups Page

14 To add this user to a group, move the name of the group to the *User is a Member of* column.

15 Choose *Network Policies* from the left hand pane to associate network policies with this user. The Network Policies Associated with User window, shown in Figure 148.

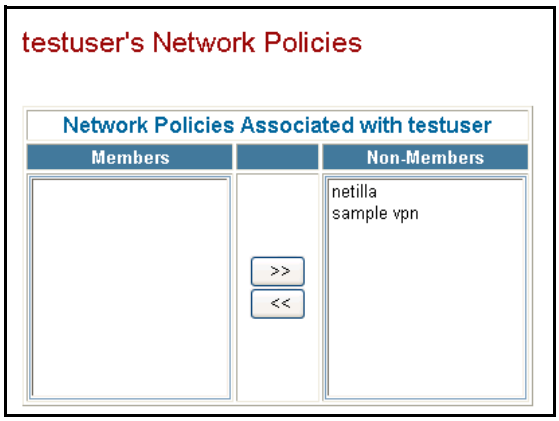


Figure 148 Network Policies Associated with Groups Window

16 Select the desired policies from the Non-Members window and use the arrows to move the policies to the Members window.

Changes take affect immediately.

Setting up Client Drive Mapping

If you are using Thin applications, you can set up client drive mapping. To set up client drive mapping, refer to “Using Local Drive Mapping” on page 92. Note that client drive mapping only applies to remote applications.

Creating Groups on the NSP

Groups provide an easy way to publish applications to many users simultaneously. This is accomplished by applying policy settings to the group rather than each individual user. All applications published for the group will be subsequently inherited by the group members.

The NSP supports two types of groups, local groups and NT Global Groups. Local groups are stored and defined in the NSP database. NT Global Groups are Microsoft Windows Domain Groups, which are defined and stored on the Domain Controller. A user’s group membership is determined during the login process. For local groups, the information is retrieved from the local database. For NT domain users, the user’s group membership credentials are retrieved from the Domain Controller.

During the login process a profile is created for the user by gathering information about the realm that the user logs into as well as any global settings that have been defined on the NSP, such as restricting access to any of the service tabs.

Group Configuration Options

The following list details the various options available when configuring local and remote groups.

Local Groups

- Can be nested (i.e., can contain other local groups).
- Groups inherit applications and policies from parent groups.
- Local groups cannot contain NT Global Groups.
- Can contain local and remote users.
- SecurID and RADIUS users are managed with local groups.

NT Global Groups

- Can contain only NT users.
- Cannot be nested.
- Can be manually defined prior to log in to the NSP.
- If not pre-defined, are created automatically when the NSP queries the NT server to determine a user's group membership.

Creating Local Groups

This section describes the how to create a local group on the NSP.

To create a local group, do the following.

1 From the Administrator Site, click *Groups*, and then click *Local*, as shown in Figure 149.

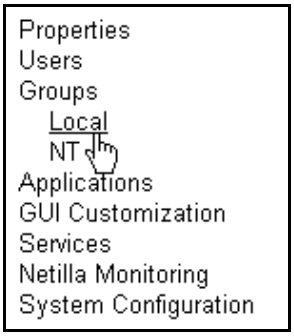


Figure 149 Local Groups Submenu

All existing groups are displayed, as shown in Figure 150.

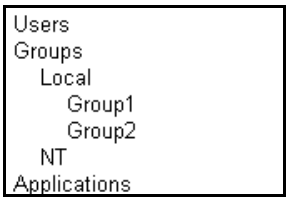


Figure 150 Local Groups Window

2 Create a group by entering a name for the new local group in the Local Groups page and then click *Submit*, as shown in Figure 151.

Figure 151 Create a New Group Window

The properties for the new group are displayed.

Configuring Policies for a Local Groups

Once you have created a new local group, you can configure the policies that are inherited by the users who are members of the group.

Note the available options for Local Groups.

- Rename the group
- Add or remove users to the group
- Assign applications to the group
- Assign network policies to the group
- Join the local group to other local groups
- Delete the group

To configure policy for groups, do the following.

1 From the Administrator Site, click *Group* and then select the name of the group you want to configure policies for.

To rename the group, enter the new name in the Rename the Group text box and click Submit.

The Group Properties page opens.

2 Scroll to the Users Associated With page, as shown in Figure 152.

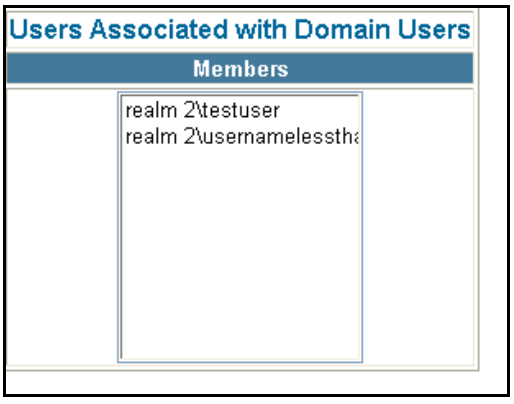


Figure 152 Group Properties Window

The existing user profiles appear in the Non-Members window.

3 To add users to the group, select the profile from the Non-Members window and use the arrows to move the user to the Members window.

The user inherits any applications that are assigned to this group.

4 To remove users from the group, click the profile from the Members window and use the arrows to move the user to the Non-Members window.

Unlike NT groups, local groups can contain all types of users (local, RADIUS, SecurID or Domain users).

5 Scroll to the Applications Associated window to assign applications to be inherited by the members of this group.

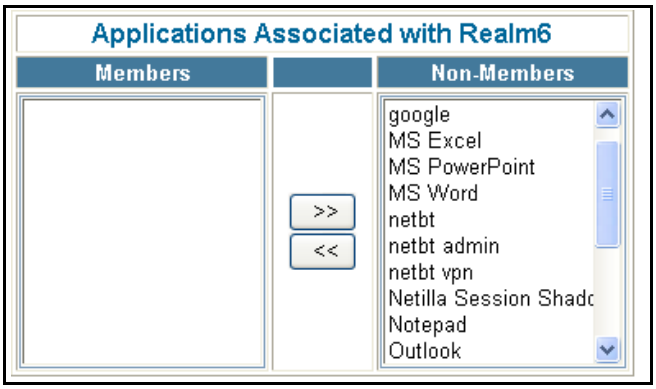


Figure 153 Applications Associated with Group Window

6 Select the desired application from the Non-Members window and use the arrows to add the application to the Members window.

7 To associate network policy with this group, scroll down to the Network Policies Associated with Group window. An example is shown in Figure 155.

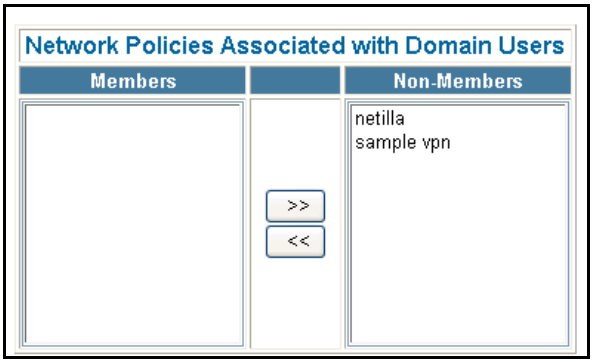


Figure 154 Network Policies Associated with Groups Window

8 Select the desired policies from the Non-Members window and use the arrows to move the policies to the Members window.

Changes take affect immediately.

9 To join the group to other groups, scroll to the Groups Associated with Group list box, shown in Figure 155.

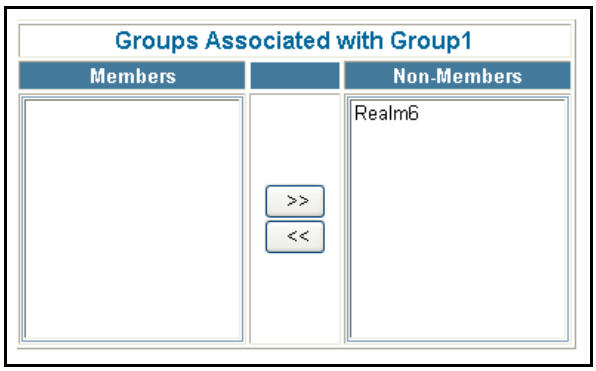


Figure 155 Groups Associated with Group List Box

10 Select the desired groups from the Non-Members window and use the arrows to move the group to the Members window.

Members of the newly created group inherit applications assigned to this group.

Changes to the Members and Non Members columns are saved automatically.

Deleting Groups

To delete a group, do the following.

1 Select *Groups* and then select the name of the group you want to delete.

2 Delete the group by clicking *Delete Group* located at the bottom of the Group Properties page, as shown in Figure 156.

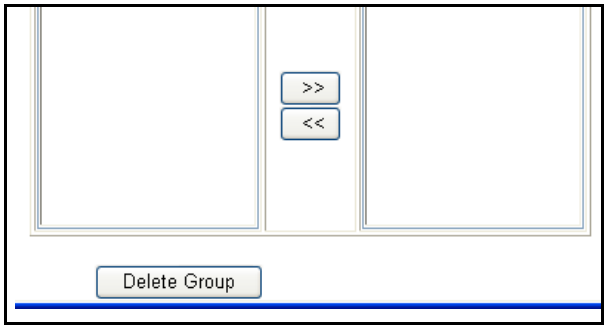


Figure 156 Delete Group Button

Creating an External NT Global Group

NT global groups are not created or stored on the NSP. Instead, NT groups reside on a Microsoft Windows Domain Controller, and a profile of the domain and the group is stored on the NSP. The Netilla Administrator uses these profiles to manage application policies that apply to NT groups.

Normally, there is no need to create NT groups. The group profiles are created automatically when a user logs into the NSP.

Because NT global groups are automatically created when the user logs in, it is recommended that you create a user who is a member of all the groups you wish to work with. Then, log in as that user to automatically create the groups on the platform.

If you want to manually create a profile for an NT Global group, follow these steps:

1 From the Administrator Site, click *Groups*, *NT*, and then click the name of the domain that the user belongs to. For example, the domain in Figure 157 is *test*.

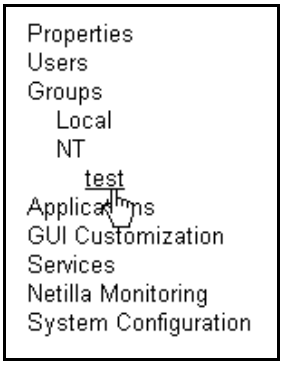


Figure 157 NT Groups Submenu

2 If the domain profile has not been created, enter the name of the domain and click *Submit*, as shown in Figure 158.

Figure 158 Domain Name Field Box

The domain name appears in the submenu.

3 Click the newly-created domain name to edit its properties.

4 The Domain Properties window opens, as shown in Figure 159.

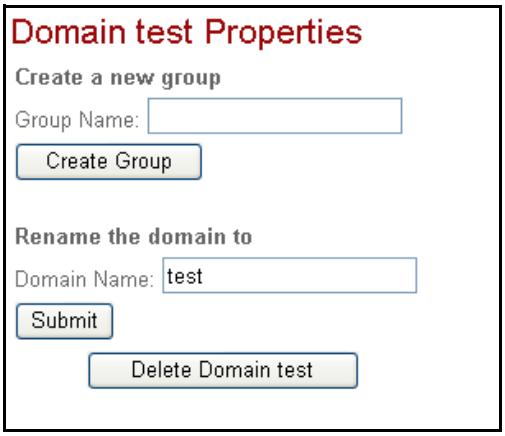


Figure 159 Domain Properties Page

5 To define a new group, enter the name in the Group Name field. Use the Rename the Domain to field to rename the domain profile.

The group name appears under the newly created domain in the submenu.

The name of the domain's profile must match the name of the actual domain in order for policy propagation to work.

The properties for the NT new group are displayed on the right hand pane.

Configuring Policies for NT Groups

This section describes the steps to configure policies that are inherited by users who are members of the group.

Configuration options for NT groups are as follows:

- Rename the group
- Assign applications to the group
- Delete Group

To configure policies for NT Groups, do the following.

1 Click *Groups* and then click *NT.* From the NT menu, click the name of the domain, and then click *Domain Users* as shown in Figure 160.

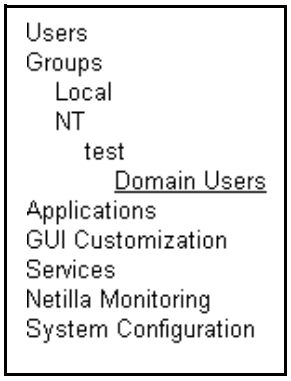


Figure 160 Domain Users Location

You can rename the domain by entering the new name on the Rename the domain to field and then clicking Submit*, as shown in Figure 161.*

Figure 161 Rename the Group Field

2 Scroll to the Applications Associated with Domain Users window.

3 Select the desired application from the Non-Members window and use the arrows to add the application to the Members window, as shown in Figure 162.

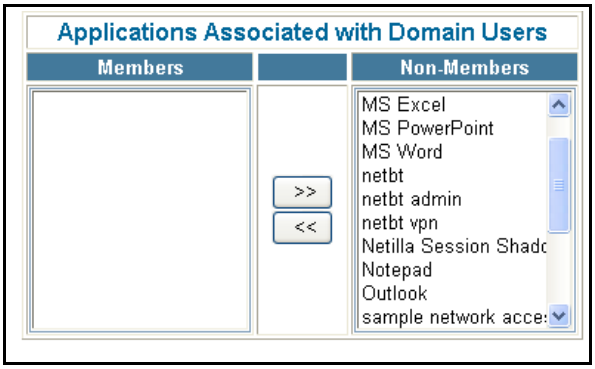


Figure 162 Applications Associated Group Members and Non-Members Window

4 (Optional) Associate network policies with these domain users.

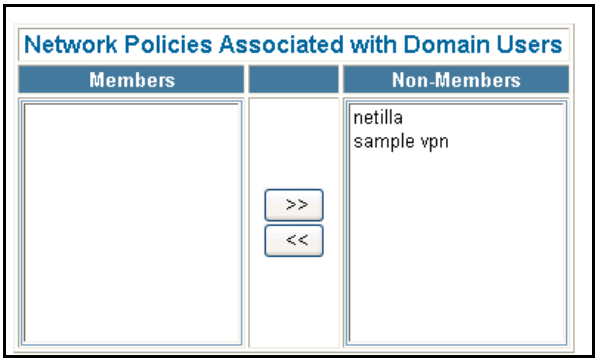


Figure 163 Network Policies Associated with Domain Users Window

Changes take affect immediately.

Changes to the Members and Non Members columns are saved automatically.

Deleting Groups

To delete a group, do the following.

1 Select *Groups* and then select the name of the group you want to delete.

2 Delete the group by clicking *Delete Group* located at the bottom of the Group Domain User Properties page underneath the Network Policies Associated with Domain Users page, shown in Figure 163.

Modifying NSP Administrator Accounts

This section describes how to change passwords and the start up service for the NSP's administrator accounts as well as assign applications, network policies and customize client drive mapping.

Refer to the preferred section.

About the NSP's Administrator Accounts

The NSP ships with the following three default administrative accounts.

- *admin:* The admin account is the highest privilege level.
- *radmin* (or reseller administrator): An account created for managing the service in the field.

- *maint*: An account created for general maintenance and has the least number of privileges.

All configuration instructions presented in this guide assume that you are logged in as radmin unless otherwise stated.

Both admin and radmin provide the level of privileges necessary for configuring the NSP. Specifically, the rights each of the administrative accounts are listed in Table 21:

Table 21 Rights for NSP Administrative Accounts

NSP Administrator Rights	Admin	Radmin	Maint
Administer the Netilla licenses in the NSP	Yes	Yes	No
Backup and restore the NSP configuration settings	Yes	Yes	Yes
Create, modify and delete application objects	Yes	Yes	Yes
Access and change system configuration settings such as IP addresses, and services such as NAT and DHCP	Yes	Yes	No
Activate and de-activate the Netilla firewall	Yes	Yes	No
Create, modify, and delete users	Yes	Yes	Yes
Customize the login screen (with the exception of changing the Menu Bar logo; this is reserved for *admin*)	Yes	Yes	Yes

When you log in to the NSP as an *admin* or *radmin* user you will be able to see administrative features that are hidden from normal users.

If the feature you want is not visible, log out and back in as the admin user, if applicable.

Changing an Administrator's Password

To change the password of your administrator account, do the following.

1 From the Administrator Site, select *System Configuration* and then select *Internal Auth Stores*.

WARNING: *If you change the password for the admin account, be sure to document the new password and keep it in a safe location. If you forget the password you will not be able to access the NSP and there is no other way to gain access.*

2 Click *Admins* and then select the admin account for which you want to change the password.

Figure 164 Properties Page for Administrator Account

3 Enter a new password in the New Password field and then type the identical password in the New Password Confirm field.

The Password field is case-sensitive.

4 Click *Update Password* to save the changes.

If you changed the password, log out and then log in again using the new password.

Modifying an Administrator Profile

This section describes how to change the start up service, assign applications, network policies and change drive mapping defaults for the NSP administrative profiles, *admin*, *radmin* and *maint*.

1 Log in as the administrative account that you want to change, *admin, radmin*, or *maint*.

2 Click *Users* and then click *local*. From local, choose the name of the account you want to change *admin, radmin*, or *maint* as shown in Figure 165.

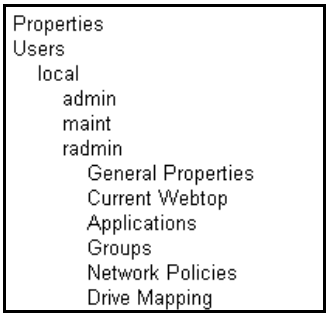


Figure 165 Radmin Submenu

The Properties for the administrative user you selected opens. An example using the radmin account is shown in Figure 166.

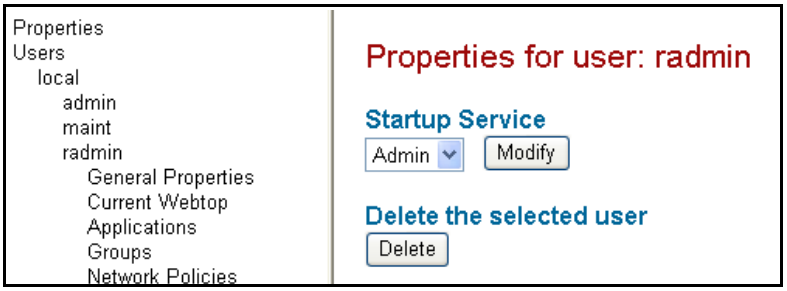


Figure 166 Radmin User Properties Page

3 Select the option you would like to change. You can choose from the following.

- **General Properties**: Allows you to change the start up service for this user.
- **Current Webtop**: Allows you to view the applications currently assigned to this user.
- **Applications:** Allows you to manage applications for this user.
- **Groups:** Allows you to manage group membership for this user.
- **Network Policies**: Allows you to manage network policies for this user.
- **Drive Mapping**: Allows you to change client drive mapping default settings for this user for use with Thin applications.

4 Click *Modify* to save the changes to the General Properties page. Changes to the remaining options are saved automatically.

This page intentionally left blank.

8 Application Server Load Balancing

Application Server Load Balancing allows the NSP to determine which application server is best suited for an end user's application request. The NSP provides two types of application load balancing, session-based and advanced. Advanced Load Balancing is an optional feature and requires the purchase of an Advanced Load Balancing license.

Refer to the preferred section for configuration details.

- Configuring Session-based Load Balancing
- Configuring Advanced Load Balancing

Configuring Session-based Load Balancing

Session-based load balancing is the NSP's default load balancing mode, and is available on every NSP. This approach employs an algorithm that the NSP uses to determine the appropriate application server based on the number sessions running on each server. Each time an application is launched, the NSP directs the session to the server with the fewest active sessions.

To configure an application for session-based load balancing, do the following.

1. From the Administrator Site, click *Applications* and then click *Applications*.
2. Locate the application to configure for session-based load balancing and then click the name of the application.
3. Click *General Properties* as shown in Figure 167.

Figure 167 Applications Sub Menu

The General Properties page appears as shown in Figure 168.

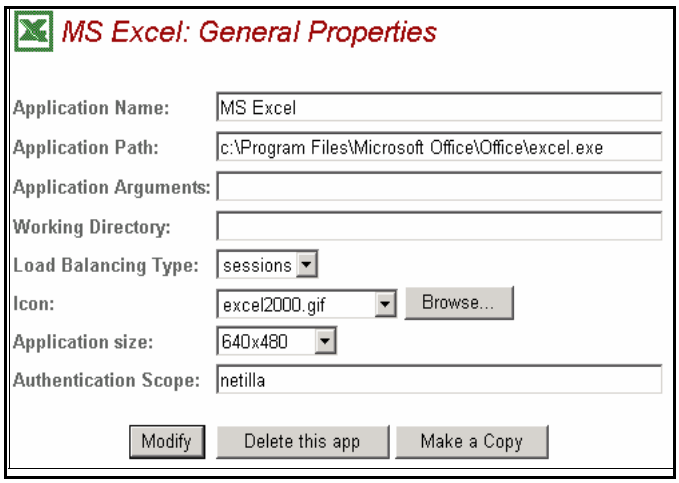


Figure 168 Application General Properties Page

4 Set Load Balancing Type to *sessions*.

Sessions load balancing is the default.

5 Click *Modify*.

Next, the application server must be configured.

6 To configure the application servers to be load balanced for this application, select *Application Servers* from beneath the application name, as shown in Figure 169.

Figure 169 Application Servers for a Particular Application

The Servers Associated with this Application page appears.

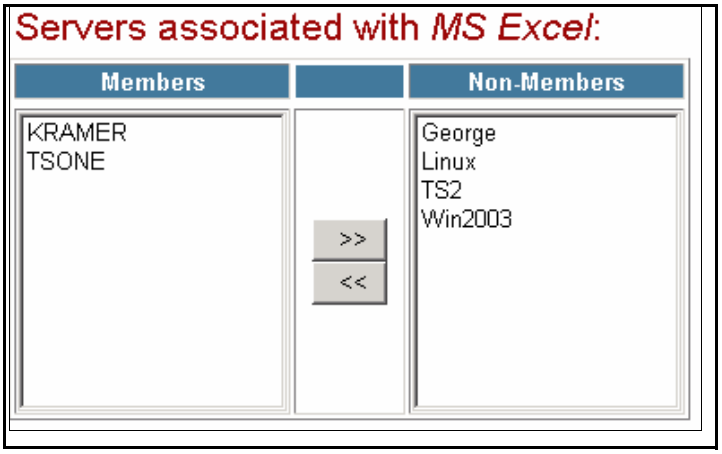


Figure 170 Servers Associated with an Application Page

7 Select the group of servers to be load balanced from the Non-Members column and move them to the Members column.

To do so, highlight and move using the arrow buttons. To select multiple servers, hold the shift or control keys as you click each selection.

8 Once the application has two or more server assigned in the Members column, load balancing will begin.

Configuring Advanced Load Balancing

Advanced Load Balancing, an optional feature, provides more intelligent algorithms for load balancing application servers. When advanced load balancing is employed, the decision-making criteria is based either on the application server's available amount of free CPU or memory capacity. Netilla Advanced Load Balancing supports Windows Terminal Server applications, X11 applications, and UNIX character-based applications.

The NSP supports this feature by downloading a small software program called the Enhancement Module onto each application server to be load balanced. This module provides a load balancing service which gives the NSP real time information about the application server's CPU/memory load. It also allows the load balancing service to determine whether an application server is available, or unavailable for a reboot.

Advanced Load Balancing requires the purchase of an additional license.

Installing the Enhancement Module

The installation instructions vary depending on which operating system you are using. Refer to the appropriate section.

- Installing the Enhancement Module on Windows Servers
- Installing the Enhancement Module on UNIX/Linux Servers

Installing the Enhancement Module on Windows Servers

The Enhancement Module for Windows provides client drive mapping and advanced application server load balancing services for Microsoft Windows 2000 application servers.

To install the Enhancement Module for Windows, do the following.

1. Log in to the Windows 2000/2003 server as a user with administrator privileges.
2. Download the Enhancement Module Setup program, temwin32.exe, by logging in to the NSP and appending the NSP's URL with **/extras/temwin32.exe**.
3. Press *Enter*.
4. Save the program to a temporary directory on the Windows 2000 application server.
5. Double-click **temwin32.exe** to install the Enhancement Module.
6. Follow the instructions on your screen.
7. You have the option of installing the drive mapping or the load balancing components or both.

Installing the Enhancement Module on UNIX/Linux Servers

To install the Enhancement Module for UNIX/Linux, do the following.

1. Log in as root on the application server.
2. Download the Enhancement Module Setup program, temi3li.shx, by logging in to the NSP and appending the NSP's URL with **/extras/temi3li.shx**.
3. Press *Enter*.
4. Save the program to a temporary directory on the application server. The file is:

```
tempahp.shx for HP-UX 11+
temrsai.shx for IBM AIX 5.1+
temi3li.shx for Red Hat Linux 7.1+, Sun Linux 5.0+ and UnitedLinux
1.0+
temspso.shx for SPARC Solaris 2.8+
```

5. Type `sh shx_file`.
6. Follow the instructions on your screen.

Starting and Stopping the Enhancement Module

When you install the Enhancement Module, the services that it provides start immediately. The services also automatically start whenever the server is rebooted. You can also manually stop and start the load balancing service. This section explains how this is done.

The instructions vary depending on which operating system you are using. Refer to the appropriate section.

- Stopping and Starting Load Balancing on a Windows Application Server
- Stopping and Starting Load Balancing on a UNIX Application Server

Stopping and Starting Load Balancing on a Windows Application Server

To manually stop/start the load balancing service on a Windows 2000 application server, do the following.

1. Log in to the Windows 2000/2003 server as a user with administrator privileges.
2. Go to Control Panel, open Administrative Tools and then click *Computer Management*.
3. In the tree, open Services and Applications and then click *Services*.
4. Select the Load Balancing Service and right-mouse click.
5. Select Stop or Start.

Stopping and Starting Load Balancing on a UNIX Application Server

To manually stop/start the load balancing service on a UNIX application server, do the following.

1 Log in as root on the application server.

2 Type **install_dir/bin/tem stop** or **install_dir/bin/tem start**. By default, install_dir is /opt/tta-tem.

Configure an Application for Advanced Load Balancing

To configure an application for advanced load balancing, do the following.

1 From the Administrator Site, click *Applications* and then click *Applications*.

2 Locate the name of the application you want to configure for session-based load balancing, as shown in Figure 171.

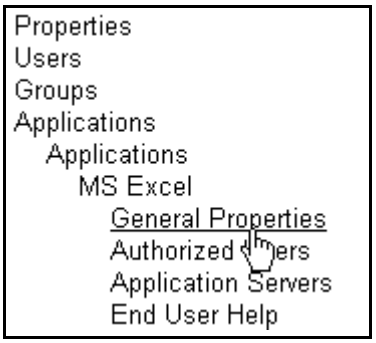


Figure 171 Applications Sub Menu

The General Properties page appears as shown in Figure 172.

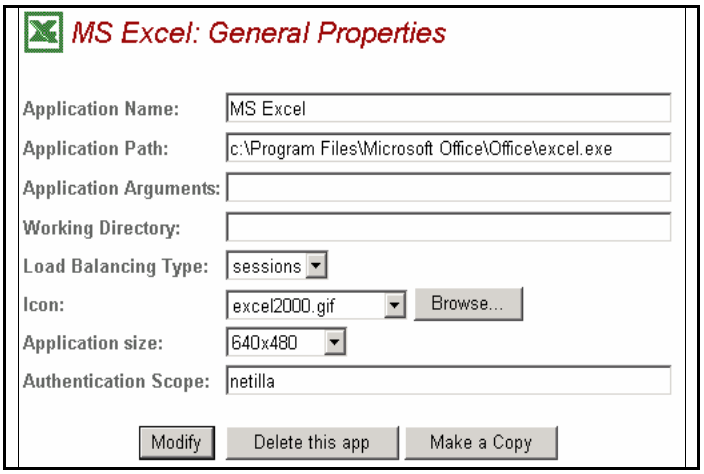


Figure 172 General Properties Page

3 Set Load Balancing Type to either *CPU* or *Memory*.

CPU:

Analyzes the application server's CPU processing capacity to determine which server is best suited for an end user's application request.

Memory

Analyzes the application server's amount of free memory to determine which server is best suited for an end user's application request.

4 Click *Modify*.

Next, the application server must be configured.

5 To configure the application servers to be load balanced for this application, select *Application Servers* from beneath the application name, as shown in Figure 167.

The Servers Associated with this application page appears.

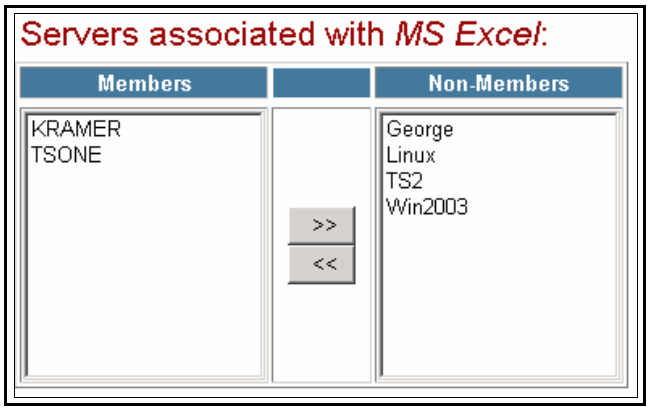


Figure 173 Servers Associated with an Application Page

6 Select the group of servers to be load balanced from the Non-Members column and move them to the Members column. To do so, first highlight and then move them between columns using the arrow buttons. To select multiple servers at once by holding down the shift or control keys as you click each of the servers.

Load balancing begins once the application has two or more servers assigned in the Members column.

9 Monitoring and Reporting

This chapter describes how to configure and use the Netilla Security Platform's (NSP) monitoring and reporting features.

Monitoring Features

The NSP provides the following monitoring features:

- **Netilla Monitoring** allows you to gather and review system statistics about the NSP such as system performance, application usage, Web service and the Netilla firewall.
- **Session Shadowing** allows NSP administrators to interact with user sessions which can be helpful for training or troubleshooting assistance.

Reporting Features

The NSP provides the following reporting features:

- **Remote Logging** allows syslog messages of a facility and severity you define to be sent to a syslog server.
- **Setting Up SNMP Reporting** allows SNMP traps to be sent to an SNMP manager.

Netilla Monitoring

Netilla Monitoring provides you with tools to monitor system performance, Netilla firewall activity, and track end user application usage. System statistics, which are stored for one year, are accessed through the Web-based Netilla monitoring utility. You can create customized queries to receive timely service information. Results are available as graphs, which can be "drilled down" for greater granularity, or as screen-based text reports.

There are four main areas to the Netilla Monitoring feature.

- System Performance
- Application Usage
- HTTP Reverse Proxy Policy
- Netilla Firewall Monitoring

Accessing Netilla Monitoring

To access Netilla Monitoring, do the following.

1 From the Administrative Site, click *Netilla Monitoring* as shown in Figure 174. Current System Information is displayed.

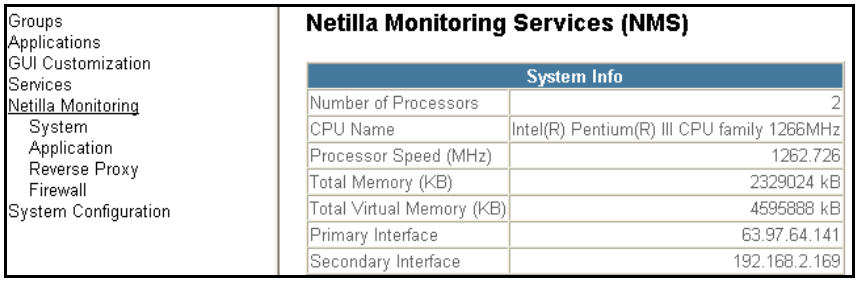


Figure 174 Netilla System Information Window

System Performance Monitoring

System Monitoring provides the following data:

- CPU utilization
- Memory utilization
- Disk utilization
- The top five processes utilizing the processor and the relevant amounts
- The top five processes that are utilizing memory and the relevant amounts

Accessing System Monitoring

To access System Monitoring, do the following.

1 Click *Netilla Monitoring*.

2 Click *System*. The System Monitoring page appears as shown in Figure 175.

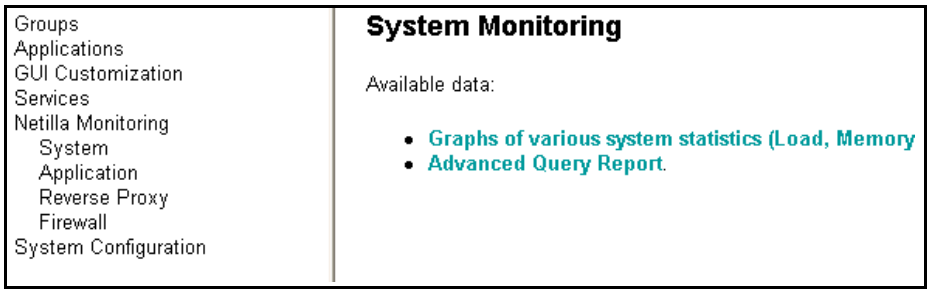


Figure 175 System Monitoring Window

System Statistics Graphs

To view system statistics in graphical form, do the following.

1 To view a graph, click *Graphs of various system statistics*.

The Graph of System Stats opens, as shown in Figure 176.

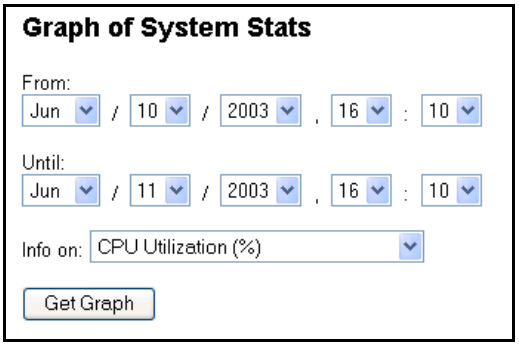


Figure 176 Graph of System Statistics

2 Specify a time frame by selecting a starting date from the *From:* field and ending date in the *Until*: field.

One year of historical data is always available.

3 For *Info on*, select a counter type.

4 Click *Get Graph* to see the graph. An example of load average is shown in Figure 177.

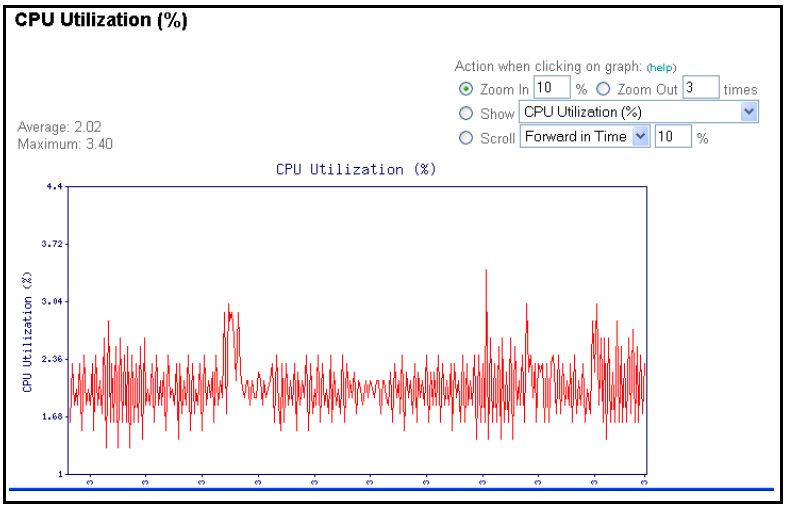


Figure 177 Load Average Example

Action When Clicking on Graph

You can control what action occurs when clicking on a generated graph by making selections from the Action area in the upper right-hand corner. Once a selection is made, click on the graph to change the parameters as selected.

System Monitoring (Advanced Query Report)

From the main System Monitoring page, choose *Advanced Query Report* to enter parameters for a custom report.

Application Usage Monitoring

This section describes how to create application reports for Thin applications. Note that this section does not apply to Tunnel or HTTP Reverse Proxy applications.

Application Usage reports can be created from among the following variables:

- Application usage history by individual user
- Historical user activity per application
- Total number of concurrent users by application

Accessing Application Monitoring

To access Application Monitoring, click *Netilla Monitoring* and then click *Application*. The Application Monitoring page appears.

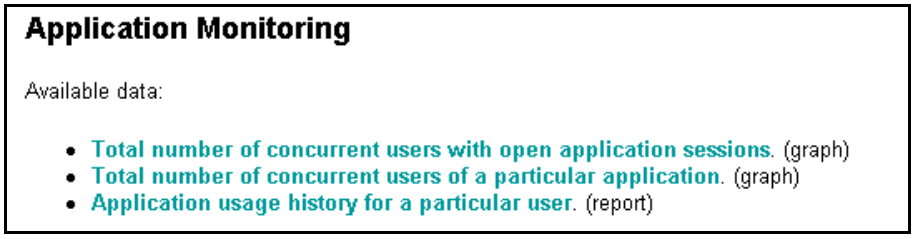


Figure 178 Application Monitoring Options

Application Monitoring (Total Number of Concurrent Users With Open Application Sessions)

1. Click *Application* to retrieve statistics regarding Applications.
2. Choose *Total Number of Concurrent Users with Open Application sessions*
3. Select a date range using the From and Until fields.
4. Choose the resolution.
5. Click *Get Graph*.

   An example is shown in Figure 179.

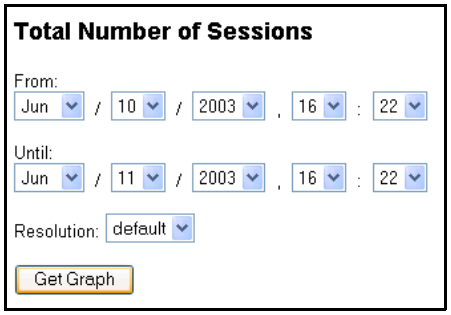


Figure 179 Total Number of Sessions Example

6. Follow the procedure for “Action When Clicking on Graph” on page 161.

Application Monitoring (Total Number of Concurrent Users of a Particular Application)

1 Click Application to retrieve statistics regarding Applications.

2 Choose *Total Number of Concurrent Users of a Particular Application*.

3 Select a date range using the From and Until fields.

4 Choose the resolution.

5 Press *Get Graph*.

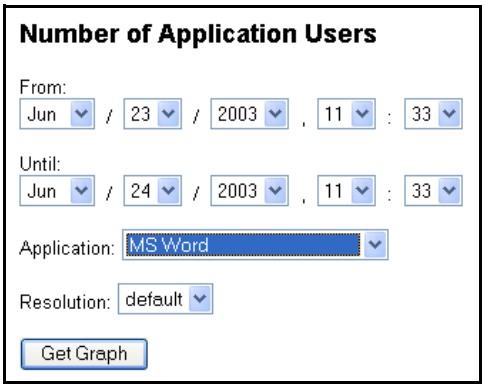


Figure 180 Number of Application Users Example

6 Follow the procedure for "Action When Clicking on Graph" on page 161.

Application Monitoring (Application Usage History for a Particular User)

1 Click *Application* to retrieve statistics regarding Applications

2 Click *Application usage History for a Particular User.*

3 Choose a date range using the *From:* field and the *To:* field.

4 Select the type of applications you want to monitor for this user.

5 For *User*, select the name of the user.

6 Click *Get Report* to display a report for that user.

An example is shown in Figure 181.

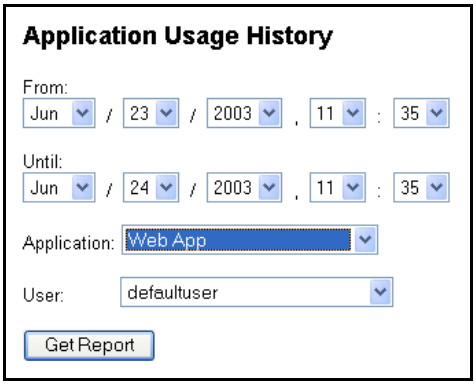


Figure 181 Application Usage History Example

7 You can generate a new report by making new selections at the top and choosing *Change Parameters*, as shown in *Figure 182*.

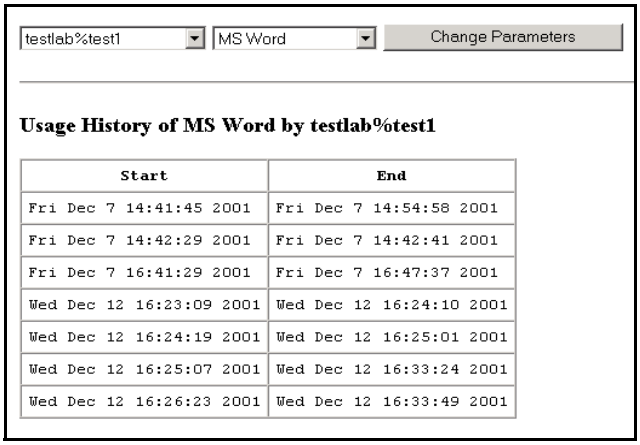


Figure 182 Change Parameters Example

Web Service Monitoring

With Web service monitoring, reverse proxy policy logs are created for analysis. Reports can be created from among the following variables as shown in Figure 183:

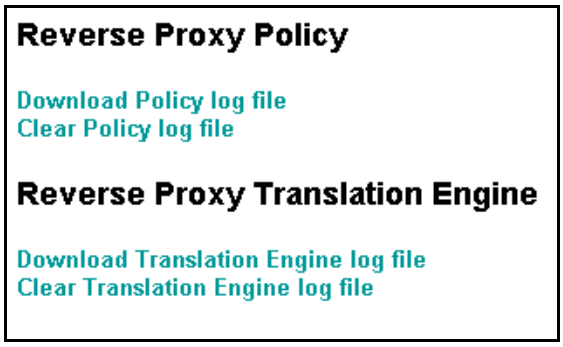


Figure 183 Reverse Proxy Policy Options

Reverse Proxy Policy

The Reverse proxy policy option allows you to view all requests that have been made to access the NSP Web service. This may be useful for auditing purposes.

Download Policy log file

To download the Reverse Proxy log file, do the following.

1 Click *Download Policy Log File*.

2 The File Download Window opens, as shown in Figure 184.

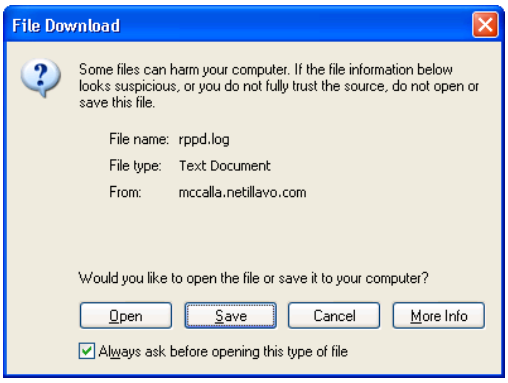


Figure 184 Policy Log File

3 Click *Save*.

4 Use Notepad or another text editor to open the log file for analysis.

Clear Policy Log File

To clear the policy log file, select *Clear Policy log file*.The log is cleared right after you click Clear Policy log file.

Reverse Proxy Translation Engine

This option allows you to view untranslated HTML, JavaScript and other web resources for isolating issues with the HTTP reverse proxy feature. You must first enable the Enable Translation Engine Debugging field that allows this information to be stored. For details, refer to “Configuring Web Service System-Wide Settings” on page 102.

Download the Translation Engine log file

To download the translation engine log file, do the following.

1 Click *Download Translation Engine Log File*.

2 The File Download Window opens, as shown in Figure 184.

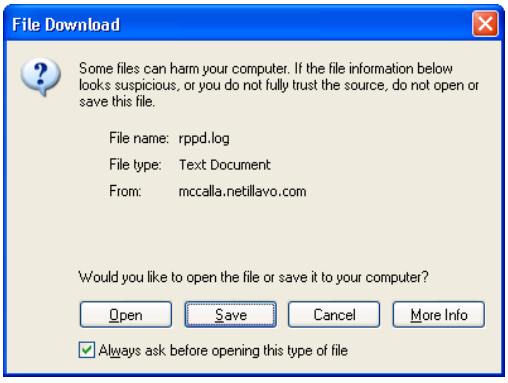


Figure 185 Policy Log File

3 Click *Save*.

4 Use Notepad or another text editor to open the log file for analysis.

Clear Translation Engine Log File

To clear the policy log file, select *Clear Policy log file*.The log is cleared right after you click Clear Policy log file.

Netilla Firewall Monitoring

This section describes how to view statistics regarding the Netilla firewall.

Firewall Monitoring provides the following statistics:

- Total unauthorized firewall requests
- Unauthorized firewall requests by detail:
  - Interface of request
  - Protocol employed by the request
  - IP address of request
  - Port that rejected request
  - Packet size
  - Analysis of packets rejected by the firewall

Accessing Firewall Monitoring

To access Firewall Monitoring, do the following.

1. Click *Netilla Monitoring*.
2. Click *Firewall*. The Firewall Monitoring page appears.

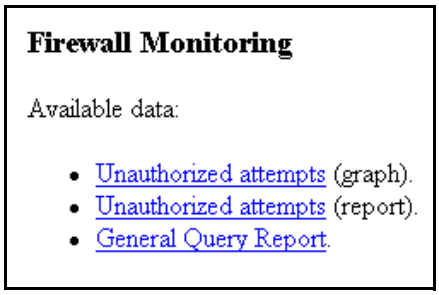


Figure 186 Firewall Monitoring Example

Firewall Monitoring Unauthorized Attempts Graph

1. Choose *Unauthorized attempts* graph.
2. Specify a time frame by entering a start date in the To: field and an end date in the From: field.
3. For Granularity, specify the level of detail.
4. Click *Get Graph*, as shown in Figure 187.

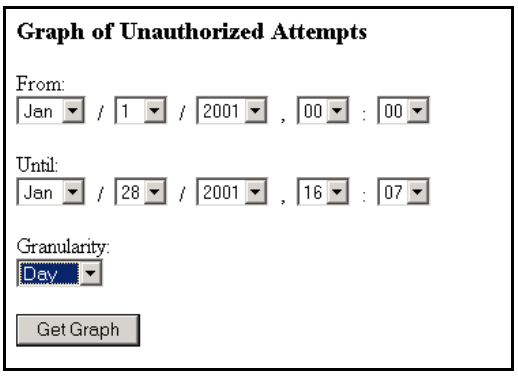


Figure 187 Unauthorized Firewall Attempts Screen

Follow the procedure for "Action When Clicking on Graph" on page 161.

Firewall Monitoring Unauthorized Attempts Report

1. Choose Unauthorized attempts report.
2. Choose a date range and click *Get Report* to generate a report.

Firewall Monitoring General Query Report

1. Choose *General Query* report.
2. Choose a date range and the query parameters.
3. Click *Get Report* to generate a report.

Session Shadowing

Session Shadowing allows you to view and interact with NSP user sessions, as long as the user grants permission to be shadowed. Session Shadowing is a way to assist with training or on-the-spot troubleshooting needs.

Session Shadowing is available for Thin applications only.

By default, only the *admin* user has permission to assign the Session Shadowing application to users, including assigning the application to the *admin* user himself. Once the *admin* user has assigned the Session Shadowing user to himself, shadowing can be granted to other accounts as needed.

The Session Shadowing application is limited to 10 simultaneous users.

Session shadowing is managed as a shared application. You set access permissions for Session Shadowing in several ways:

Realm Level (not recommended)
All users logging into the realm have access to Session Shadowing.

Application Level
You can specify which users can access Session Shadowing through the application's properties.

Group Level
All users with membership to the specified group have permission to use Session Shadowing.

User Level

You can publish access to Session Shadowing through the user's General Properties.

Using Session Shadowing

This section describes how Session Shadowing is used with the NSP.

By default, radmin, and admin accounts have access to Session Shadowing.

1 Log in as one of the default administrative accounts (i.e., radmin, or admin), and then click the *Thin* icon. There you will see the Netilla Session Shadowing icon.

The Netilla Session Shadowing icon is displayed, as shown in Figure 188.

Figure 188 Netilla Session Shadowing Icon

2 Click the Session Shadowing icon to launch the application.

3 Select the realm in which the user resides, and select the current session(s) that you would like to view, as shown in Figure 189.

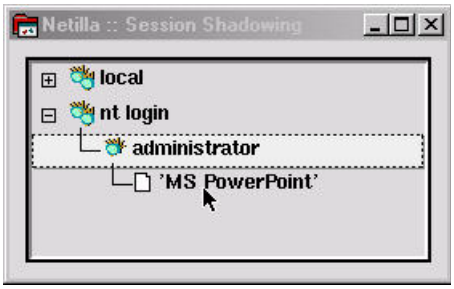


Figure 189 Choosing a User's Session to Shadow

Clicking on a realm displays all user accounts that currently reside in that realm. To see if the user has an application session open, click the individual account name as described in the following steps.

4 Double-click the user's session that you would like to shadow.

The following message appears, indicating that the Shadowing Application is waiting for acceptance from the user.

Figure 190 Shadow Status Window

At the same time, the following message appears within the user's application session:

Figure 191 User's Shadowing Message

If the user clicks *No*, the Shadowing session ends, and the user trying to view the session is presented with the following dialogue box:

Figure 192 Shadow Status Window

If the user clicked *Yes* to allow the Shadow request, a shadowing session appears, allowing the shadow account to interact and/or view the remote user's session.

5 To end the Shadowing session, close the Shadow Session window.

The remote user is presented with the Shadowing Has Ended window, as in Figure 193.

Figure 193 Shadowing Has Ended Window

6 To return the remote user to their application session, click *OK*.

Assigning Shadowing Permissions to Users

By default, only the administrative accounts (i.e., radmin, and admin) have permissions to Shadow users' session. However, this permission can be granted to specific users by either radmin or admin.

You can choose to assign permission in three ways: By realm (not recommended), by User, and by Application.

Assigning Shadowing Permissions by Realm (not recommended)

1 From the Administrator Site, click *Users*, and select the Realm to which you want to publish Session Shadowing.

The Applications Associated with User window opens, as shown in Figure 194 (NT Login, in this example).

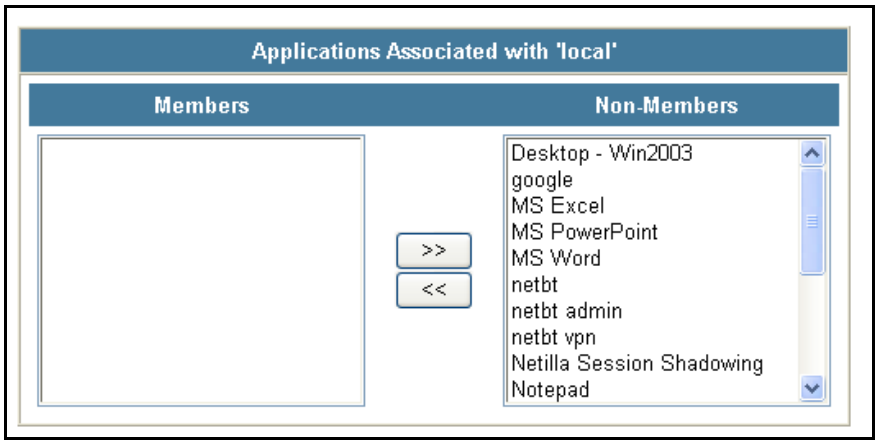


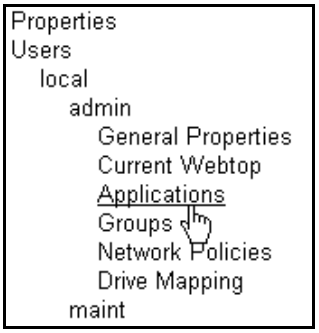
Figure 194 Applications Associated with User Window

2 Select the Session Shadowing application, and click the left arrow button to move it to the Members panel.

All users logging into the *NT Login* realm now have the ability to shadow any user's sessions.

Assigning Shadowing Permission by User

1 From the Administrator Site, click *Users* from the left links menu, select the realm the individual user resides in, choose the individual user (admin, in this example), and select *Applications* under the Users menu.



The Applications Associated with *administrator* window opens.

2 Select the Session Shadowing application, and click the left arrow button to move it to the Members pane, as shown in Figure 195.

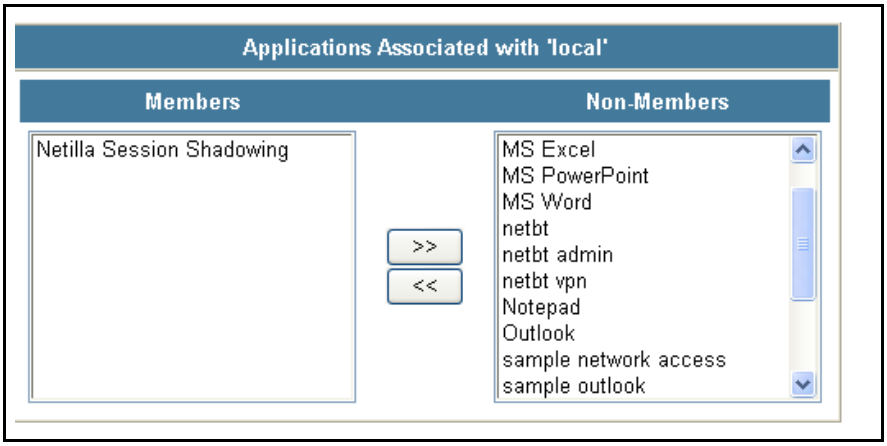


Figure 195 Applications Associated with Administrator Window

Now, the *administrator* user has permission to run the Session Shadowing application, once logged in.

Assigning Session Shadowing By Application

The Session Shadowing application can also be published to a user on a Group or Application level. Refer to "Allowing Users to Access Thin Applications" on page 87 for more details.

Remote Logging

You can set up the NSP to send syslog messages to a syslog server based on the subsystems and corresponding priorities that you configure.

The subsystems you will find most important are listed and described in Table 22.

Table 22 Remote Logging Message Content

Facility	Message Content
Kernel	Logs Ethernet status (link up/down) and speed for eth1 and eth0.
Auth	Logs authentication attempts to the NSP including failed attempts.
Tunnel	Logs session initiation and termination and includes user and realm and length of session.
Thin	Logs application launch and close and includes name of application, user name, realm, application server name, and security method (SSL) and length of session.
Web	Logs application launch, close and includes user name, realm and path. Logs access allow and deny messages and indicates realm, user name and path.
Failover	Logs information related to the HotStandby system similar to the information that is sent in the HotStandby email alerts. For details about email messages, refer to “Email Alerts” on page 223.

Setting Up Remote Logging

Setting up remote logging requires defining the severity and type of syslog messages to be sent to a syslog server.

To define the types of messages to be sent, do the following. Note that you can create multiple rules. Because rules are mutually exclusive, they may overlap.

1 From the Administrative Site, click *System Configuration* and then click *Remote Logging*.

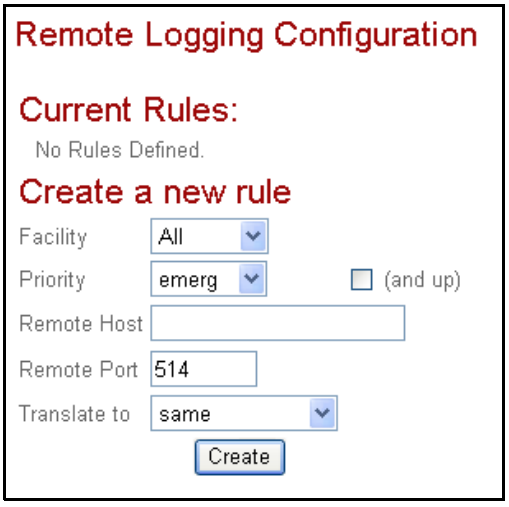


Figure 196 Remote Logging Configuration Page

2 **Facility**: Select the application or operating system component for which you want generate log messages.

3 **Priority**: Select the severity to be assigned to this classification of messages. Note that the list is ordered from most severe (i.e., emerg) to least severe (debug).

Debug level is for Netilla support personnel and is intended for internal use.

And up check box: Check this box if you want include the priority selected as well as all other higher priorities.

4 **Remote Host**: Enter either the host name or the IP address of the destination syslog server.

5 (Optional) **Remote Port**: By default, this field lists the common UDP port number for syslog. If necessary, you can change the port number.

6 (Optional) **Translate to**: This field allows you to receive messages on the destination syslog server under a different facility rather than what is specified in the NSP's Facility field. Use this field to translate NSP subsystems that are not standard syslog facilities to any syslog facility that your syslog listener can understand. By default, this field is set to *same* meaning the facility of the messages is not changed.

If All *was selected for Facility, then set* Translate to *to the preferred type for the non-standard syslog facilities that are not listed in the* Translate to *drop down menu such as such as sysmon and JARMpd. For example, if* Translate to *is set to uucp, then messages from JARMpd and sysmon will be displayed on the remote syslog server as if they came from UUCP while messages from the Thin subsystem still show up as Local2.*

7 Click *Create*.

Setting Up SNMP Reporting

The NSP provides support for the simple network management protocol (SNMP). The main steps for configuring the NSP to send SNMP traps to an SNMP manager are as follows:

- Define General Settings
- Defining SNMP Users
- Configuring SNMP Traps

Define General Settings

Setting up SNMP requires defining the SNMP agent (NSP) settings and users who are authorized to query the NSP.

General Settings

The general settings page defines basic information about the NSP for the SNMP manager.

1 From the Administrative Site, click *System Configuration* and then click *SNMP Agent*.

2 Click *General*.

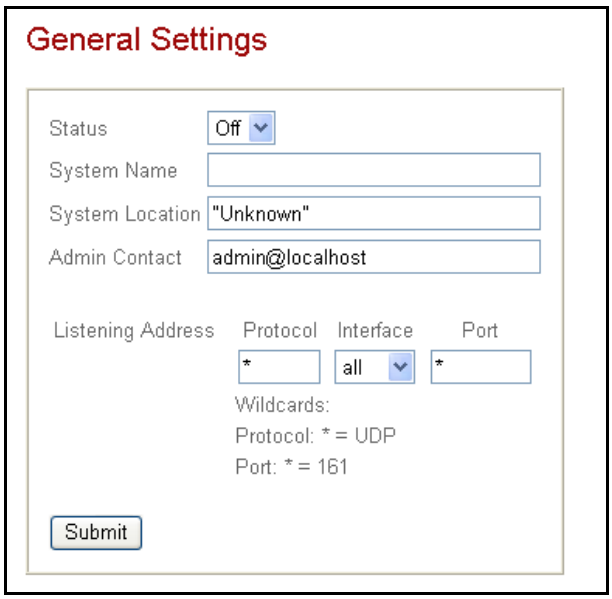


Figure 197 SNMP General Settings Page

3 **Status**: To enable the SNMP feature, select *On*.

4 **System Name**: Enter the fully qualified domain name (FQDN) or host name of the NSP.

5 **System Location**: Enter the physical location of the NSP (e.g., 2nd floor IT center).

6 **Admin Contact**: Enter the email address of the contact person for the NSP.

7 (Optional) **Listening Address**: By default, this field is set to listen to UDP on all interfaces over port 161, the common port number for sending and receiving requests via SNMP. Make changes as preferred. For instance, you may want to configure the NSP to listen on one interface.

8 Click *Submit*.

Defining SNMP Users

The NSP supports three types of SNMP users, version 1, version 2c, and version 3 (user-based security model). A user is an SNMP manager that will be querying the NSP.

Add a Version 1 or Version 2 SNMP User

1 From the Administrative Site, click *System Configuration* and then click *SNMP Agent*.

2 Click *Users*.

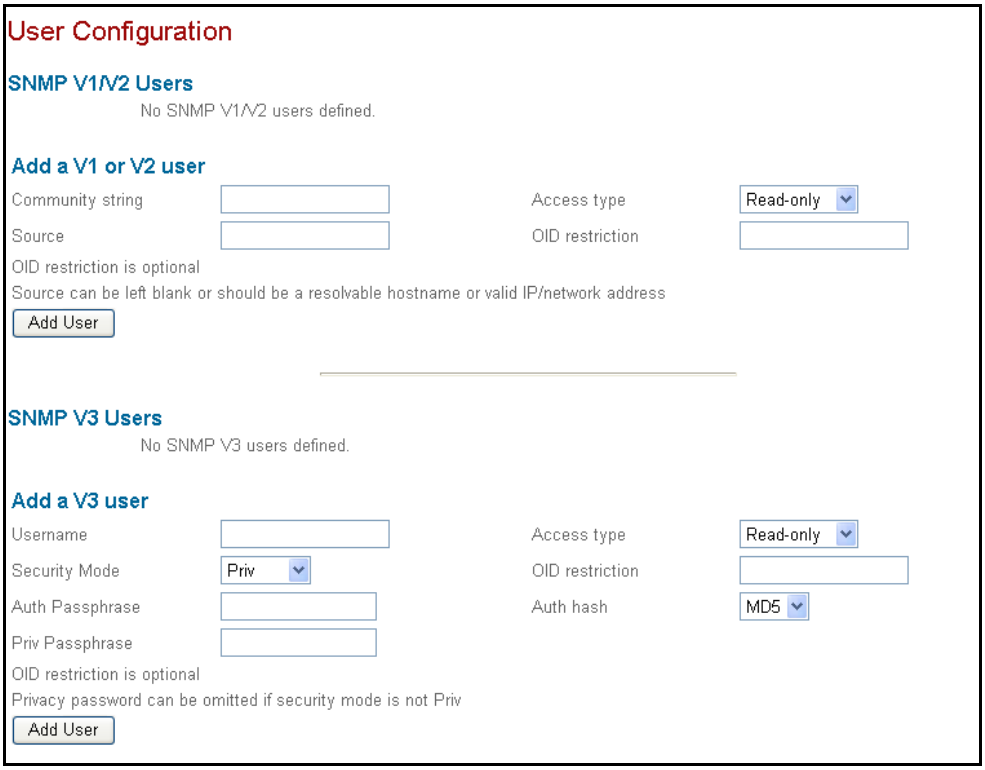


Figure 198 SNMP Users Configuration Page

Under Add a V1 or V2 user, enter the following:

3 **Community string**: Enter the password that allows the SNMP manager to poll the NSP.

4 **(Optional) Source**: Use this field to restrict the location from which an SNMP manager can query the NSP. Enter the IP address or resolvable host name of the location. For instance, if you enter 192.168.10.4, only queries to the NSP from 192.168.10.4 with the appropriate community string will be allowed.

5 **Access type**: Select the rights you want to allow this user to have. Choose either Read-only or Read-Write.

6 **(Optional) OID Restriction**: Use this field to restrict access to certain sections of the MIB. Enter either the object identifier or type in the name of the sub tree you want to restrict access to. For instance, if you enter **System**, this user can access only the System branch and anything below.

7 Click *Add User*.

Add a Version 3 SNMP User

To configure a version 3 user, do the following.

1 From the Administrative Site, click *System Configuration* and then click *SNMP Agent*.

Under Add a V3 user, enter the following:

2 **User**: Enter a name for this user.

3 **Security Mode**: Select the type of security for this user. Choices are:

- Priv: Private mode requires this user to be authenticated and it requires encryption to be used. Encryption type supported is DES.

- Auth: Authentication mode requires this user to be authenticated but does not required encryption to be used.
- No Auth: No Authentication mode does not require authentication for this user nor encryption.

4 **Auth Passphrase**: Enter the password to be used for authentication.

5 **Auth Hash**: Enter the hash algorithm to be used for this user's credentials.

6 **Priv Passphrase**: If you selected Privacy as the Security Mode type, enter the password to be used for the encryption/decryption key.

7 **Access type**: Select the rights you want to allow this user to have. Choose either Read-only or Read-Write.

8 **(Optional) OID Restriction**: Use this field to restrict access to certain sections of the MIB. Enter either the object identifier or type in the name of the sub tree you want to restrict access to. For instance, if you enter **System**, this user can access only the System branch and anything below.

9 Click *Add User.*

Configuring SNMP Traps

This section lists the traps supported by the NSP and describes how to configure the server information to which you want to send SNMP traps.

Supported TRAPS

The NSP supports the following SNMP traps:

Table 23

SNMP Trap	Description
Cold Start	A Cold Start trap is sent when the NSP reboots.
Warm Start	A Warm Start trap is sent when the NSP reinitializes itself
Link Down	A Link Down trap is sent when an interface on the NSP goes down.
Link Up	A Link Up trap is sent when an interface on the NSP comes back up.
Authentication Failure	An Authentication Failure trap is sent when someone has tried to query the NSP with an incorrect community string. Note that this setting must be set to Yes in the NSP's Trap Configuration page.

Configuring TRAPs

1 From the Administrative Site, click *System Configuration* and then click *SNMP Agent*.

2 Click *Traps*.

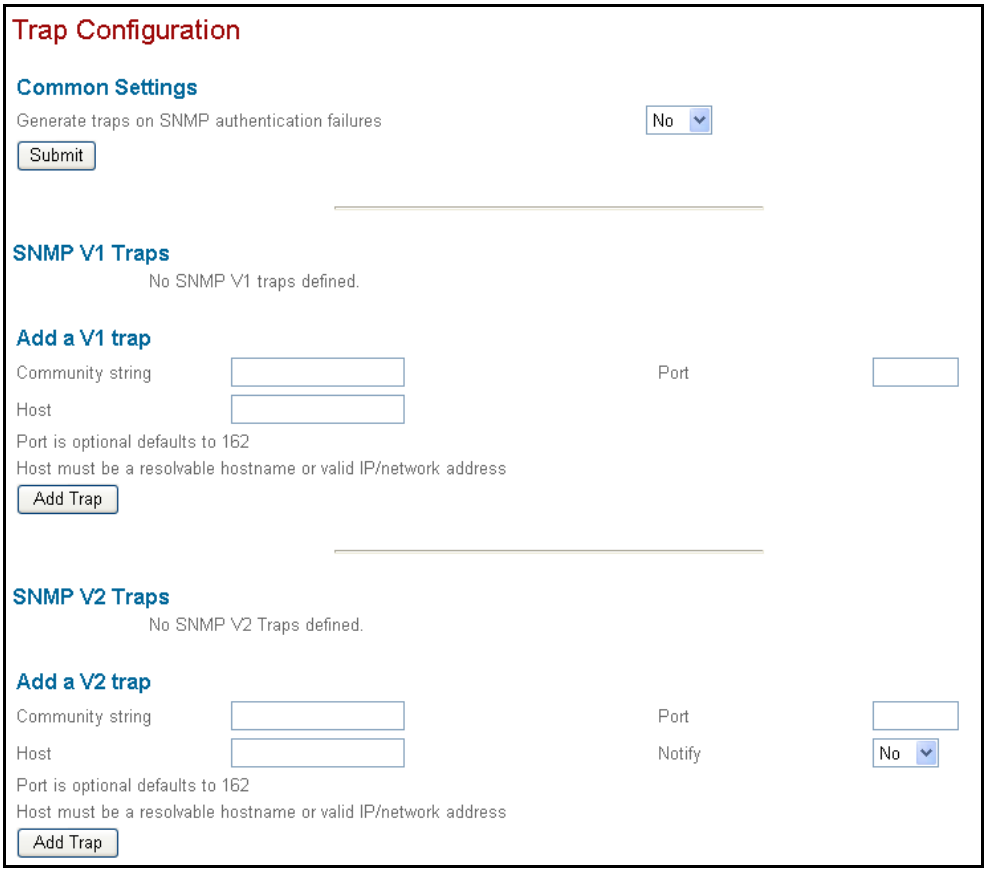


Figure 199 SNMP Users Configuration Page

3 Under **Common Settings**, select *Yes* if you want to send a trap to the remote server when an attempt to query the NSP fails. This can be helpful in determining unauthorized access attempts.

Under Add a V1 or V2 user, enter the following:

4 **Community string**: Enter the password that allows the SNMP manager to receive traps from the NSP.

5 **Host**: Enter the SNMP manager's IP address or resolvable host name.

6 **(Optional) Port**: The port is set to 162, the common port number for SNMP traps. If you want to use a different port number, enter the preferred port number.

7 Click *Add Trap*.

Add a Version 2 SNMP Trap

1 From the Administrative Site, click *System Configuration* and then click *SNMP Agent*.

2 Click *Traps*.

Under Add a V2 trap, enter the following:

3 **Community string: Enter** the password that allows the SNMP manager to receive traps from the NSP.

4 **Host**: This field defines the location where the traps are sent. Enter the SNMP manager's IP address or resolvable host name.

5 **(Optional) Port**: This field defines the port the traps are sent on. By default, the port is set to 162, the common port number for SNMP traps. If you want to use a different port number, enter the preferred port number.

6 **Notify**: Select *Yes* if you want the SNMP manager the NSP that the trap was received. By the default this field is set to *No*.

7 Click *Add Trap*.

10 Configuring NSP Services

The Services menu of the Netilla Security Platform (NSP) provides system-wide settings for each NSP service (Files, Thin, Tunnel, Web) as well as settings for general customization of the services icons that reside in the NSP GUI.

This section describes the following:

- Changing Default Service Settings for Users
- Configuring the Files Service
- Allowing Users to Access a Service
- Allowing Users to Access a Service
- Allowing Users to Access the Administrator Site

Changing Default Service Settings for Users

This section describes how to change the following default settings.

- Changing the Default Services Settings for Users
- Setting the Default Startup Service for Users

Changing the Default Services Settings for Users

The services tabs shown in Figure 200 can be re-sorted or hidden, allowing you to change the default appearance of the NSP seen by your users.

Figure 200 The NSP Services Tabs

To change the default Netilla services, do the following.

1 From the Administrator Site, click *Services* as shown in Figure 201.

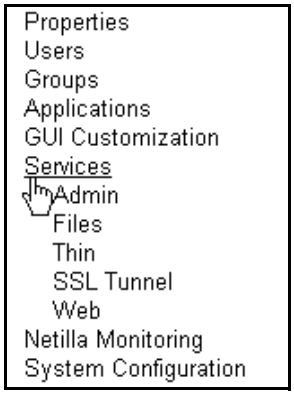


Figure 201 Services Submenu

The Default Service Setting for Users page opens.

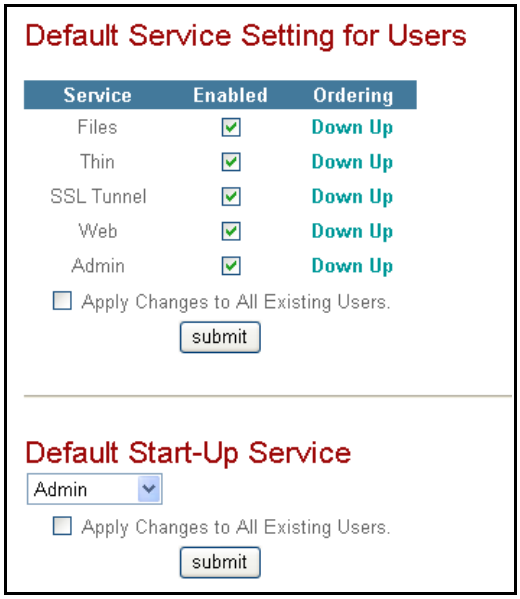


Figure 202 Default Settings for New Users Window

2 Remove a service from the Netilla GUI by un-checking the box next to its name.

Note that changes apply to all new users created from this point on.

3 To include these changes to existing users as well as new users check *Apply Changes to All Existing Users*.

4 To change the order in which the services tabs appear click the Down/Up controls to the right of the interface.

5 Click *Submit*.

Setting the Default Startup Service for Users

The default startup service is used to configure the default service that a user sees the first time they log into the NSP, if a profile has not already been created. For instance, if the user primarily uses Web applications, you can specify that the Web applications appear each time the user logs into the NSP.

To specify a default start up service, do the following.

1 With the Default Service Setting for Users window open, shown in Figure 202, select a service from the Default Start-up Service drop-down list box.

2 To include these changes to existing users as well as new users check *Apply Changes to All Existing Users*.

3 Click *Submit*.

Configuring the Files Service

This section describes how to configure the location of the server to be used for file sharing as well as how to allow users to use this service.

Configuring File Sharing Server Location

To specify the location of the server to be accessed for file sharing, do the following.

1 From the Administrator Site, click *Services* and then click *Files*.

2 Click General Properties. The Files Sharing Configuration page appears.

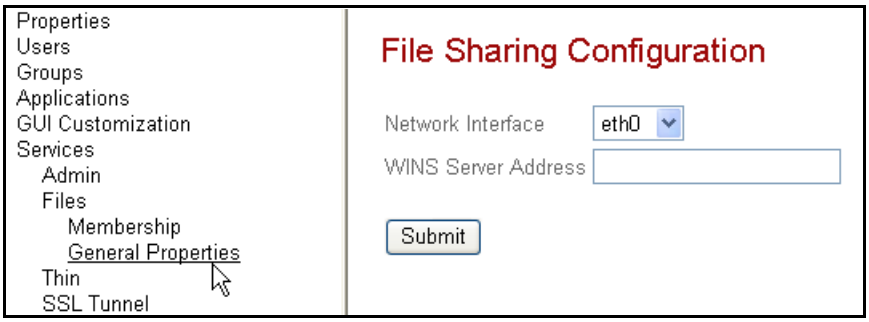


Figure 203 Files Settings Page

Network Interface
Specify whether the file server is connected to the NSP's eth0 or eth1 Ethernet interface.

WINS Server Address
Enter the IP address of the file server.

3 Click *Submit*.

Once the service settings are configured, you must allow users to access the service. Refer to "Allowing Users to Access a Service".

Allowing Users to Access a Service

To allow a user to access a service, do the following.

1. From the Administrator Site, click *Services* and then click the name of the service that you want to allow access to from the Services submenu (that is, Files, Thin, Tunnel, Web or the Administrator Site).
2. Click *Membership*.
3. Use the arrow buttons to move the users to the Members column who you want to be able to use the service. An example using the Thin service is shown in Figure 204.

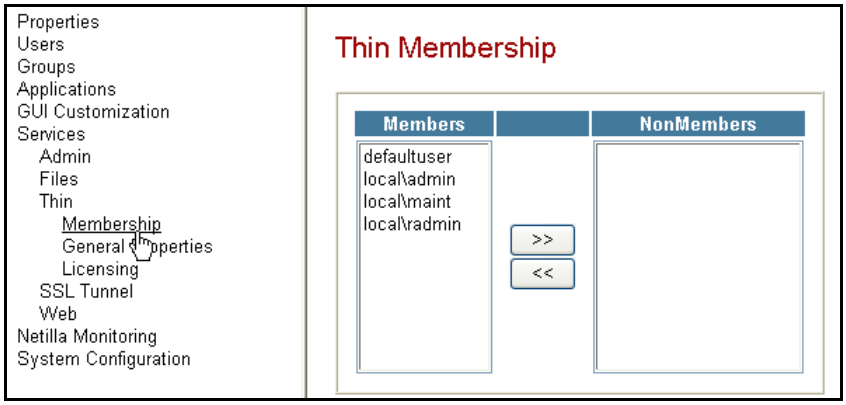


Figure 204 Thin Service Membership Page

You can use Control+Click to select multiple members, or Shift+Click to select a range of members. Changes are applied automatically.

Changes take affect immediately.

Allowing Users to Access the Administrator Site

This section describes how to allow users to access their Administrator Site. The Administrator Site for end users is quite different than the admin, radmin and maint Administrator Site. The Administrator Site for end users only allows a user to change their own password and start up service.

An example of the Administrator Site for end users is shown in Figure 205.

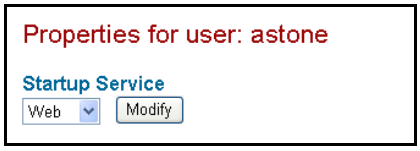


Figure 205 Administrator Site for End Users

Refer to "Creating Users on the NSP" on page 139 for details on configuring the Startup Service and changing passwords for end users.

To add members to the NSP administrator group, do the following.

1 From *Administrator Site*, click *Services* and then select *Admin* as shown in Figure 206.

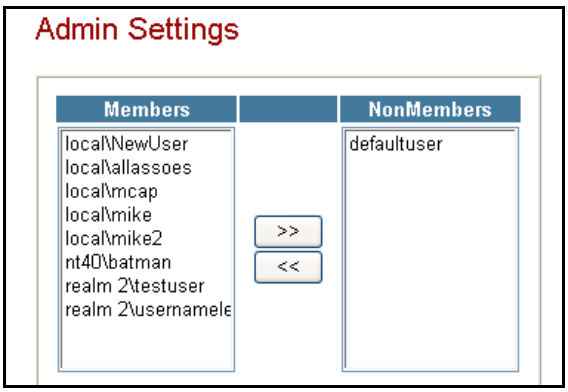


Figure 206 Configuring Services for Users Window

2 The Admin Settings page appears.

3 Select a user and click the arrow buttons to add or remove the user from the service.

If removed, the user no longer sees the Admin icon on their webtop.

This page intentionally left blank.

11 The Netilla Firewall

The Netilla firewall intercepts, analyzes, and implements security decisions on every network packet that travels through the NSP, regardless of the point of entry. The stateful inspection technology allows the Netilla firewall to extract state-related information from each network packet and use that information to make security decisions. This information, which is dynamically stored in memory and recalled for future analysis upon subsequent connections, offers a more robust level of performance and security than alternative proxy and packet filtering security measures.

This chapter presents the configuration options for the Netilla Security Platform (NSP) firewall. The following topics are discussed.

- Accessing the Firewall Settings
- Activating the Firewall
- Creating Rules

Accessing the Firewall Settings

To access the Netilla firewall settings, do the following.

1. From the Administrator Site, click *System Configuration*.
2. From the *System Configuration* submenu, click *Network Connections* and then *Firewall*. The Firewall Settings window opens, as shown in Figure 207.

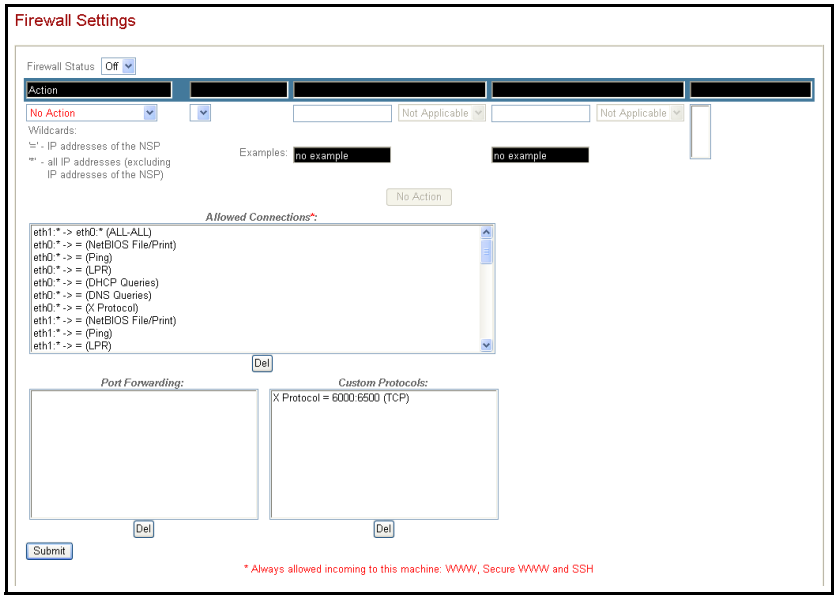


Figure 207 Firewall Settings Window

Note the following options.

Table 24 Firewall Settings and Description

Firewall Setting	Description
Firewall Status	Enables or disables the firewall.
Action	Allows you to choose the type of protocol or type of rule you would like to configure. The drop down menu provides three options. **Allow Connections:** Create rules to allow connections to a particular service or port. **Port Forwarding:** Create rules to map service requests on a particular port to a private host behind the Netilla firewall. **Create Custom Protocol:** Allows you to define names for non-standard ports so that they can be used later to create rules.
Context Fields	These fields allow you to enter parameters for new rules. Note that these fields vary depending on the action selected from the Actions drop down menu.
Commit Button	Allows you to commit the rules or protocols being created. Rules are not active until they are committed (and the firewall is enabled). The label and function of this button are context sensitive; they change depending on the action chosen from the Action drop-down menu.
Allowed Connections	For your convenience, a number of firewall rules come pre-configured. These pre-configured rules and any additional rules you create are displayed in this window. For a list of the pre-configured rules, refer to Table 25.
Port Forwarding	This window displays all of the port forwarding rules that you create.
Custom Protocols	This window displays all of the custom protocols that you create.

Activating the Firewall

The firewall service is pre-installed but not enabled by default. Enable the firewall service by changing the Firewall Status to *ON*, as shown in Figure 208.

Figure 208 Enabling the Firewall

Creating Rules

Rules are instructions that you create to dictate the manner in which the firewall handles network traffic trying to traverse the NSP.

Once the firewall has been activated, you are ready to define rules and/or set port forwarding using the Action parameters located on the firewall configuration interface.

Understanding Conventions

Before you can successfully create a rule for the Netilla firewall, an understanding of firewall conventions is required.

The following symbols are used as parameters for the rules you create using the actions menu.

Netilla Firewall Conventions

eth0	The external (public) interface of the NSP.
eth1	The internal (private) interface of the NSP.
=	The IP addresses of the NSP.
*	All IP addresses excluding the addresses of the NSP.
:	Use this to indicate a range of IP addresses or to indicate an ipaddress:port socket

For G-class NSPs, eth1 is the Gigabit Ethernet interface.

Context-sensitive Fields

Context-sensitive fields are used to enter the parameters for new rules. The functions of the fields will change depending on the type of rule you are trying to create. The default state of the action menu is *No Action* and the context fields are blank, as shown in Figure 209.

Figure 209 Default Firewall Settings

Creating an Allow Connections Rule

For maximum security, the Netilla firewall is *restrictive*. This means that the firewall automatically blocks all inbound traffic *unless a rule has been created* to allow access for each specific type of traffic or protocol.

For example, once the firewall is enabled, all inbound IRC Chat traffic is blocked to the NSP, as well as the LAN. This state continues until a rule has been created to allow incoming connections of type IRC on port 531 to the LAN.

For your convenience all of the rules listed below are pre-configured and are available once the firewall has been activated. It is highly recommended that you review these rules and remove the rules that you do not need.

Some rules cannot be changed or deleted because they are required by the NSP.

Table 25 Netilla Firewall Rules

Rule	Protocol	Effect
eth1:*->eth0:*	(ALL-ALL)	Allows traffic of all common[1] or well-known protocol types to travel from any host in the internal network (LAN) to any host in the public network (Internet) but not to the NSP itself.
eth0:*->=	(NetBIOS File/Print)	Allows NetBIOS File and Print traffic to travel from any host in the public network (Internet) to the NSP but not to the private network (LAN).
eth0:*->=	(Ping)	Allows ICMP traffic to travel from any host in the public network (Internet) to the NSP but not to the private network (LAN).
eth0:*->=	(LPR)	Allows LPR traffic to travel from any host in the public network (Internet) to the NSP but not to the private Network (LAN).
eth0:*->=	(DHCP Queries)	Allows DHCP Queries to travel through public interface to the NSP from any host but not to the LAN.
eth0:*->=	(DNS Queries)	Allows DNS Queries from any host coming in through public interface to the NSP itself but not to the LAN.
eth0:*->=	(X Protocol)	Allows X11 traffic to travel from any host in the public network (Internet) to the NSP but not to the LAN.
eth1:*->=	(NetBIOS File/Print)	Allows NetBIOS File and Print traffic to travel from any host in the private network (LAN) to the NSP but not to the public network.
eth1:*->=	(Ping)	Allows ICMP traffic to travel from any host in the private network (LAN) to the NSP but not to the public network (Internet).
eth1:*->=	(LPR)	Allows LPR traffic to travel from any host in the private network (LAN) to the NSP but not to the public network (Internet).
eth1:*->=	(DHCP Queries)	Allows DHCP Queries from any host in the private network to the NSP but not to hosts in the public network (Internet)
eth1:*->=	(DNS Queries)	Allows DNS Queries from any host in the private network to the NSP but not to hosts in the public network (Internet).
eth1:*->=	(X Protocol)	Allows X11 traffic from any host in the private network to the NSP but not to hosts in the public network (Internet).
=->eth0:*	(IMAPv4)	Allows IMAPv4 traffic from the NSP to any host in the public network (Internet).
=->eth0:*	(SMTP)	Allows SMTP traffic from the NSP to any host in the public network (Internet).
=->eth0:*	(NetBIOS Name)	Allows NetBIOS Name traffic from the NSP to any host in the public network (Internet).
=->eth0:*	(NetBIOS File/Print)	Allows NetBIOS traffic from the NSP to any host in the public network (Internet).
=->eth0:*	(DNS Queries)	Allows DNS queries from the NSP to any host in the public network (Internet).
=->eth0.*	(RDP)	Allows RDP traffic from the NSP to any host in the public network (Internet).
=->eth0:*	(SSH)	Allows SSH traffic from the NSP to any host in the public network (Internet).
=->eth0:*	(Telnet)	Allows Telnet traffic from the NSP to any host in the public network (Internet).
=->eth0:*	(DHCP Responses)	Allows DHCP responses from the NSP to any host in the public network (Internet).
=->eth0:*	(NTP)	Allows NTP traffic from the NSP to any host in the public network (Internet).
=->eth0:*	(RADIUS)	Allows RADIUS traffic from the NSP to any host in the public network (Internet).
=->eth1:*	(IMAPv4)	Allows IMAPv4 traffic from the NSP to any host in the private network (LAN).
=->eth1:*	(SMTP)	Allows SMTP traffic from the NSP to any host in the private network (LAN).
=->eth1:*	(NetBIOS Name)	Allows NetBIOS-Name traffic from the NSP to any host in the private network (LAN).
=->eth1:*	(NetBIOS File/Print	Allows NetBIOS-File and Print traffic from the NSP to any host in the private network (LAN).
=->eth1:*	(DNS Queries)	Allows DNS Queries from the NSP to any host in the private network (LAN).
=->eth1:*	(RDP)	Allows RDP traffic from the NSP to any host in the private network (LAN).
=->eth1:*	(SSH)	Allows SSH traffic from the NSP to any host in the private network (LAN).
=->eth1:*	(Telnet)	Allows Telnet traffic from the NSP to any host in the private network (LAN).
=->eth1:*	(DHCP Responses)	Allows DHCP Responses from the NSP to any host in the private network (LAN).

Table 25 Netilla Firewall Rules

=->eth1:*	(NTP)	Allows NTP from the NSP to any host in the private network (LAN).
=->eth1:*	(RADIUS)	Allows RADIUS traffic from the NSP to any host in the private network (LAN).

The following rules are not configurable, because they are required for the NSP.

Firewall Rules Not Allowed

eth0:*->=	HTTP on port 80	Allows WWW traffic on port 80 from the public network (Internet) to the NSP but not to the private network (LAN).
eth0:*->=	HTTPS on Port 443	Allows SSL traffic on port 443 from the public network (Internet) to the NSP but not to the private network (LAN).
eth0:*->=	SSH on Port 22	Allows SSH traffic on port 22 from the public network (Internet) to the NSP but not to the private network (LAN).
eth1:*->=	HTTP on port 80	Allows WWW traffic on port 80 from the private network (LAN) to the NSP but not to the public network (Internet).
eth1:*->=	HTTPS on Port 443	Allows SSL traffic on port 443 from the private network (LAN) to the NSP but not to the public network (Internet).
eth1:*->=	SSH on Port 22	Allows SSH traffic on port 22 from the private network (LAN) to the NSP but not to the public network (Internet).

For a complete list of all of the common protocols refer to "Table of Common Protocols" on page 192.

Creating an Allow Rule

To create a new allow rule, do the following.

1 From the Actions drop-down menu select *Allow Connections*, as shown in Figure 210.

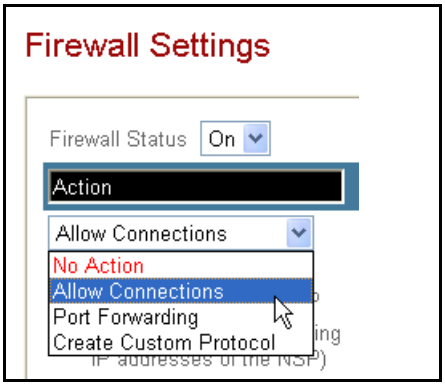


Figure 210 Allow Connections Rule Window

2 Select the type of network traffic for which you want to create a rule.

Type refers to a group of related protocols. For example, *WWW protocols* include HTTP, HTTPS, and Gopher.

3 Enter the source address and interface.

Source address refers to the address from where the traffic originates. The interface is the interface where the traffic will be arriving into the firewall.

- To allow traffic originating from any host use an asterisk "*"
- To allow traffic originating from the virtual office use an equal sign "="
- To allow traffic originating from a specific address, use the IP address of the host

- To allow traffic originating from a range of possible IP addresses, enter the beginning and ending addresses separated by a colon "**:**".
- Alternatively you can use the CIDR addressing scheme to refer to a group of computers in a network.

4 Enter the destination address and interface.

The destination address is the destination IP address where the traffic is permitted to travel. The destination interface is the interface from which the traffic is permitted to exit the firewall to go to its destination.

5 Select the protocol.

Depending on the type of protocol you choose, you will have one or more choices. Choose the protocol for which you are creating the rule. Note that it is possible to choose more than one protocol. To select multiple protocols, hold down the control key and click on each of the protocols.

6 Click *Allow Connections*.

7 Click *Submit*.

Creating Port Forwarding Rules

Port forwarding is used to redirect specific traffic to a specified destination IP or another port on your network.

Prerequisite

Before you can use Port Forwarding, you must first enable IP Forwarding on the NSP. To enable IP Forwarding, do the following.

1 Click *System Configuration*.

2 Click *IP Forwarding and NAT*.

3 Choose *Yes* from the IP Forwarding drop down list box.

4 Click S*ubmit*.

5 To test the rule for validity after the page has refreshed, scroll to the bottom of the Configuration page and click *Set* to apply the values written in this procedure.

Creating a Port Forwarding Rule

To set up a port-forwarding rule, do the following.

1 From the Action drop-down menu, choose *Port Forwarding*.

The context menu changes to provide all the options needed to create a port forwarding rule.

2 Choose a protocol *TCP or UDP* from the Protocol drop down menu.

3 In the Incoming Address: Port field, enter the IP Address to which incoming traffic would be headed, as well as the port.

In most cases, this would be the external IP address of the NSP and the port for the service being requested.

The following example displays the external IP address and the DNS service as the incoming address:

port 63.97.64.254:53

4 In the Destination Address: Port field, enter the IP address of the network host to which you want to forward the request, as well as the port.

5 To continue with the previous example, forward the DNS request to an internal host with IP address 192.168.2.133 listening on port 53.

In this case the entry would look like this:

192.168.2.133:53.

Any DNS request that arrives on the public interface 63.97.64.254 would be redirected to the internal interface 192.168.2.133.

6 To accept these changes, click *Forward Port*.

The new rule definition appears in the *Port Forwarding* box.

7 Click *Submit*.

Creating a Custom Protocol Rule

Custom rules are intended for adding Allow rules for protocols that are not in the default "Common Protocols" set. Refer to Table 26 for a list of common protocols.

For example, before you can create an "allow rule" for Microsoft SQL Server, you need to create a custom protocol named MSSQLSRV and assign it port 1433.

To create custom protocols, do the following.

1 Choose *Create Custom Protocol* from the Action drop-down list box.

2 Choose the type of connection protocol, either *UDP* or *TCP*.

3 Enter a name for the protocol. Note that you are not required to assign the actual name of the protocol, but it is recommended that you choose a descriptive name for ease of identification.

4 Enter a port to assign to the custom protocol.

5 Click *Create Custom Rule*.

The Custom Rule appears in the Custom Protocols box.

6 Click *Submit*.

Table of Common Protocols

The following table lists common protocols and their port numbers.

Table 26 Table of Common Protocols

Name	Protocol	Port Number
FTP	tcp	21
SSH	tcp	22
Telnet	tcp	23
SMTP	tcp	25
DNS TCP	tcp	53
Gopher	tcp	70
WWW	tcp	80
POP-2	tcp	109
POP-3	tcp	110
IMAPv4	tcp	143
NNTP	tcp	119
NetBIOS File/Print	tcp	139
IMAPv3	tcp	220
Secure WWW	tcp	443
LPR	tcp	515
RDP	tcp	3389
X11-0.0	tcp	6000
X11-1.0	tcp	6001
X11-2.0	tcp	6002
DNS Queries	udp	53
DHCP Queries	udp	67
DHCP Responses	udp	68
NTP	udp	123
NetBIOS Name	udp	137
NetBIOS Browse	udp	138
XDM	udp	177
RADIUS	udp	1812
Ping	icmp	8
Traceroute	icmp	8

12 Customizing the NSP

The NSP provides administrators with tools to customize your NSP. Specifically, you can add and remove graphics such as logos and edit text as well as create custom messages.

The following topics are discussed.

- Customizing the Graphical User Interface (GUI)
- Changing the Menu Bar Logo and Text
- Changing the Company Name Field on the Login Page
- Customizing the NSP Login Page
- Working with Icons

Customizing the Graphical User Interface (GUI)

The following GUI customizations are allowed.

- Upload an image of your company's logo for display on the login page
- Change various logos and icons that appear within the NSP
- Display customized identification text on the login screen, such as Integrator or company-specific information
- Design a customized login page using HTML to replace the default login page

The first four options allow you to easily customize the Netilla GUI by adding your own custom images and text while maintaining the Netilla look and feel. The last option allows you to remove the Netilla login theme entirely and replace it with your own design. Replacing the login theme requires knowledge of HTML.

To use the GUI customization tools you must be logged in as radmin.

Changing the Integrator Logo

To change the logo that appears on the login page of the NSP, login as *radmin* and do the following.

1 Click *GUI Customization*.

The GUI Customization submenu opens, as shown in Figure 211.

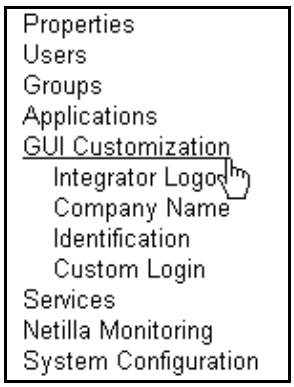
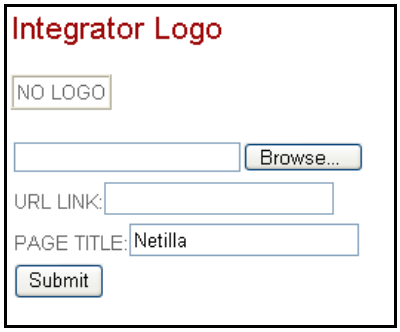


Figure 211 GUI Customization Submenu

2 Click *Integrator Logo*.



3 Browse to a logo of your choice using the browse button.

The logo must be in the form of gif, jpeg, or png.

The logo is uploaded to the NSP.

4 Enter a URL in the *URL Link* text box to point to a Web site of your choice, such as your company's home page on the Internet. *URL Link* redirects to a Web site or e-mail address when a user clicks on the logo.

The logo is displayed in the login screen, as shown in Figure 212.

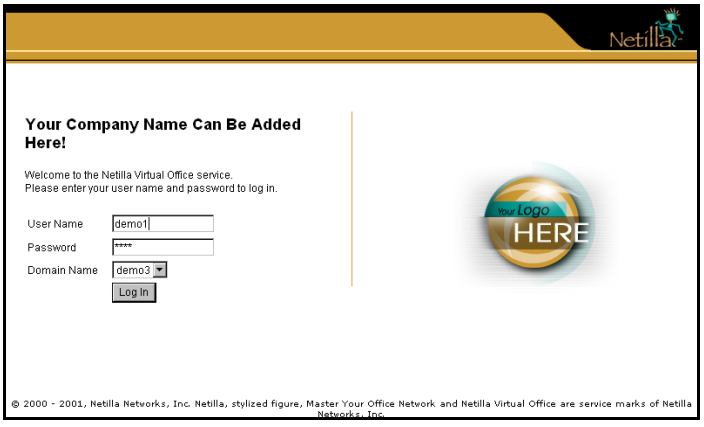


Figure 212 NSP Login Screen with Custom Logo

5 To change the title name of the page, enter a name in the Page Title field.

6 Click *Submit*.

Changing the Menu Bar Logo and Text

The Identification submenu of the GUI Customization tools allows you to change the menu bar logo and text that is displayed once users are logged in. These changes appear on the menu bar.

Changing the Menu Bar Text

The text that is displayed on the upper right side of the menu bar can be replaced with your own custom text. To do so, follow these steps.

1 Click *Identification* from the GUI Customization submenu, as shown in Figure 213.

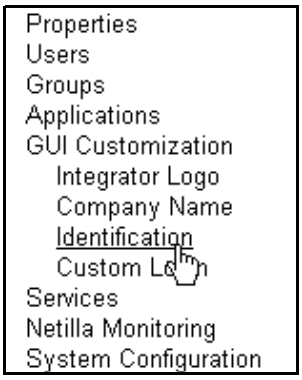


Figure 213 Identification Submenu

The Customer and Integrator Identification window opens, as shown in Figure 214.

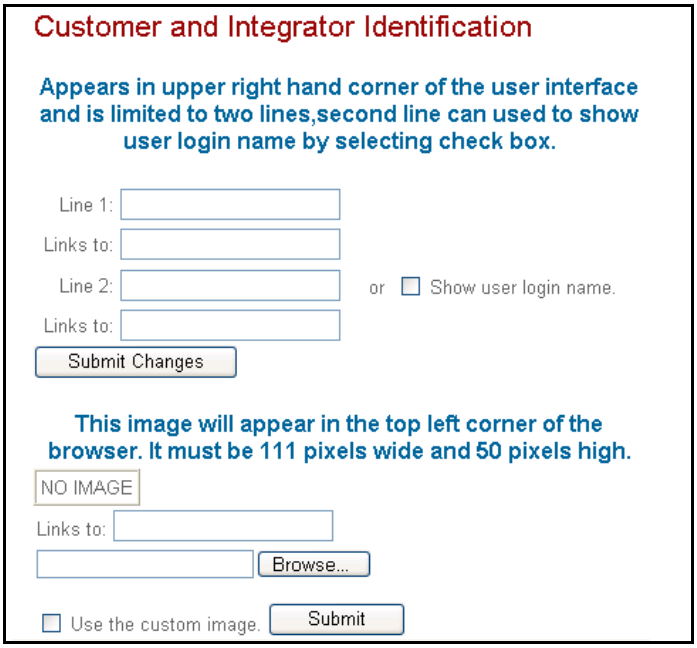


Figure 214 Customer and Integrator Identification Window

The top panel displays controls to change the text that appears in the right corner of the user interface, as well as the link associated with it. Alternatively, you can choose to show the user login name, instead of custom text.

2 Change the text in the fields *Line 1* and *Links to:* as you want them to appear.

Links to redirects to a Web site or e-mail address when a user clicks on the text (specified in Line 1) in the user interface.

3 Add a second line in *Line 2* and *Links to:* if you desire a second line of text to appear.

4 To show the user login name instead of custom text, check *Show User Login Name*.

5 Click *Submit Changes* when finished.

Changing the Menu Bar Logo

Use the controls in the bottom panel of the Customer and Integrator Identification window to change the logo that is displayed in the top right corner of the menu bar.

Note the following guidelines.

- The image must be saved in gif format
- The image must be 111 pixels wide and 50 pixels high
- The image should be set against a black background (not required)

To change the menu bar logo, do the following.

1 Click *Browse*.

2 Navigate to the location of your custom logo.

The logo is attached.

3 Enter an address in the Links To text box to link the icon to a URL.

4 Check *Use Custom Image*.

5 Click *Save*.

To see your company's logo, refresh the page. To revert back to the default Netilla logo, clear the check mark from *Use Custom Image* and click *Save*. Refresh the page and to see changes.

Changing the Company Name Field on the Login Page

This section describes how to modify the company name field that appears above the login fields on the login page.

To change the Company Name field, do the following.

1 Select *Company Name* from the GUI Customization submenu, as shown in Figure 215.

Figure 215 GUI Customization Submenu

2 Enter a name and then click *New Name*.

Customizing the NSP Login Page

The GUI Customization tools allow you to customize the messages and text pertinent to the login process, such as customizing the Netilla login page.

Note the following guidelines.

- Your HTML page must be contained in a file named *index.html*.
- Your HTML page must contain the word LOGIN on a line by itself. The Netilla software uses this word as a placeholder to display the Login and Password fields.
- Images cannot be larger than 100K.
- The *src* attribute of the <*img*> tags in your HTML source must begin with */ngui/custom*. For example, if the source image is named *background.gif*, it must be referenced as */ngui/custom/background.gif*.
- Your HTML cannot contain any Java Script or VBScript.

Uploading your custom login page

Once you have created your custom login HTML page, upload the file to the NSP.

To upload your custom HTML login page, do the following.

1 Select *Custom Login* from the GUI Customization submenu, as shown in Figure 216.

If you have previously uploaded a file, it is listed here.

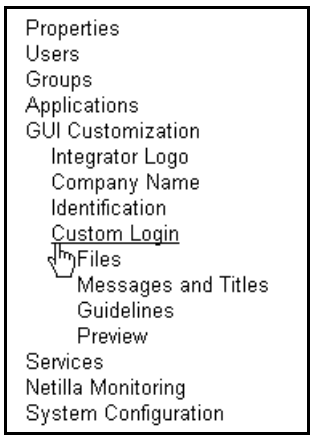


Figure 216 Custom Login Submenu and Page

2 Click *Files* and then browse to your HTML file as shown in Figure 217.

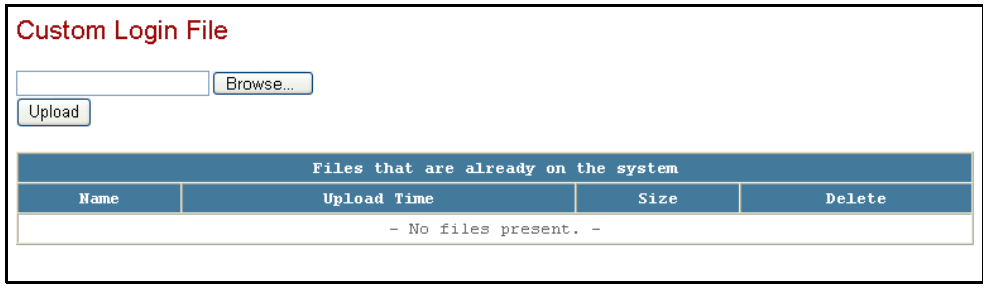


Figure 217 Custom Login Browse to File Page

3 Preview the file by clicking *Preview* from the GUI Customization submenu.

4 Once you are satisfied with the page, click Custom Login from the GUI Customization submenu and then activate the page by clicking *Use Custom Login Page*.

All users will now see your custom login page upon accessing then NSP.

Note that once you have applied a custom page the function of the Use Custom Login button changes and will allow you to revert to the default Netilla log in page. This is useful if you encounter problems with your custom page.

Troubleshooting the Custom Login Page

If you are unable to login after changing the page, append the following text to the end of the URL that is displayed in the browser's Address toolbar:

?logintheme=default.

This forces the display of the default Netilla login page to allow you to log in and correct the problem with your custom page.

The NSP automatically reverts to the default login page whenever a new index.html file or any image files are added or deleted. This allows you to use the Preview *link to see potential errors. Once you are satisfied with the preview, make the page effective by clicking* Use Custom Login Page.*Creating Custom Messages*

By creating custom messages, you can customize the information and error messages that users see when using the NSP. There are a total of 27 messages that can be customized, including four customizable titles. These titles are User name, Password, Realm, and the text displayed on the Log-in button.

Titles are the labels that identify fields, such as Username, Password and Realm, as shown in Figure 218.

Custom login messages only display when using a custom login page.

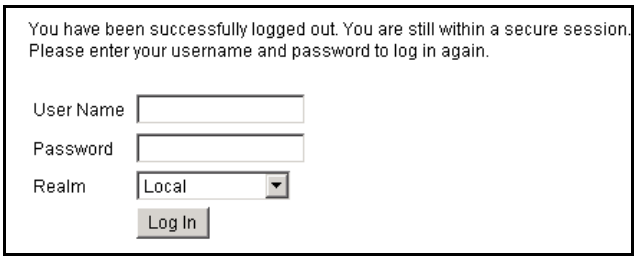


Figure 218 Titles and Fields Example

An example of a message is the text above the login fields that state that the users have successfully logged out but are still in a secure session.

Custom messages and titles apply only to custom login pages. The messages on the default login page are static and are not affected by custom messages.

To create custom messages, do the following.

1. Log in to the NSP as the *admin* user. The radmin administrative account does not have authority to change these settings.
2. Click *GUI Customization,* then *Custom Login* and choose *Messages and Title*.

   The messages properties window opens.
3. Enter your custom messages as needed. Note that HTML tags are permitted with your custom text.
4. After you've made all of the changes, scroll to the bottom of the page and click *Submit Changes*.

   Users will now see the custom messages and titles.
5. To revert back to the default messages, click *Set All Default Values* located on the top of the page.

Working with Icons

When you create an application on the NSP, you assign an icon to graphically represent the application on the end user's Webtop. By default, the NSP comes with a set of standard icons. However, you can also install additional icons as needed.

To install icons on the NSP, you must upload a 32 x 32 pixel image of the icon in gif format via the Application Icons tools. This section describes how this is done.

Creating Icons

If the icon you want to upload to the NSP is in non-gif format or is not set at 32 x 32 pixels, you can use any standard image capture program to create and/or resize the images. There are also several popular programs available that allow you to extract the icon files that reside inside an executable or.dll file. In this case, you must convert the icon file to gif format prior to uploading. Most icon programs provide this functionality.

Uploading Icons to the NSP

To upload gif files to the NSP, log in as *radmin* and follow the instructions below.

1 Click *Application* and then click *Application Icons*, as shown in Figure 219.

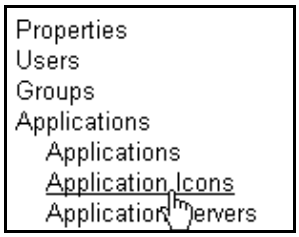


Figure 219 Application Icons Submenu

The Custom Icons tools is displayed, as shown in Figure 220.

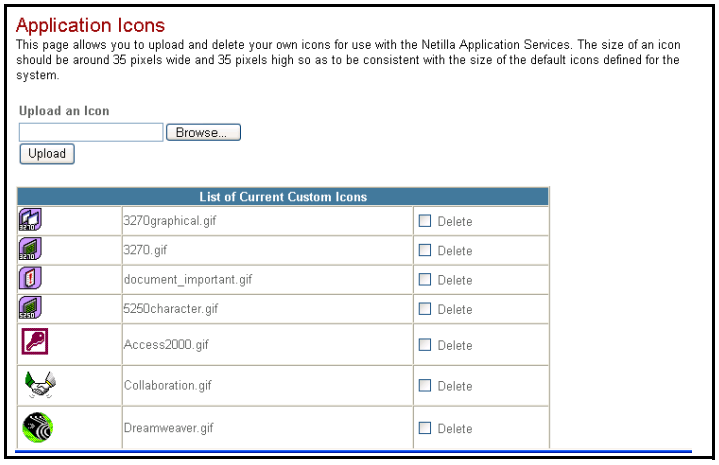


Figure 220 Custom Icon Tools Window

2 Click *Browse*, and locate the icon you want to upload.

3 Once located, click *Upload*. The icon now appears on the list of available icons for publishing applications.

Deleting Icons

To remove an icon, do the following.

1 Click *Application Icons*. The Icons window is displayed.

2 Locate the icon(s) to delete and then click the *Delete* checkbox.

3 Scroll to the bottom of the screen and click *Delete Selected Icons*.

13 Configuring the Hot Standby System

This chapter describes how to set up and configure the HotStandby system, an optional failover feature that provides redundancy. The following main topics are discussed:

- About the Hot Standby system
- Pre-Installation Configuration
- Installing the HotStandby Hardware
- Configuring the HotStandby System
- Running the HotStandby System

About the Hot Standby system

The Netilla Hot Standby System, also referred to as Failover, consists of two Netilla Security Platform (NSP) appliances: a “Master” and a “Backup”. Each NSP (both Master and Backup) receives an individual hostname and IP address (e.g., master.netillavo.com - 172.16.0.11, backup.netillavo.com - 172.16.0.12). Each appliance is subsequently configured to respond to a single, common virtual hostname and IP address.(e.g., office.netillavo.com - 172.16.0.10). Note that all three IP addresses must reside on the same network.

Both NSPs are connected via the secondary interface (ETH1) for replication and keep-alive status advertisement. The Remote Power Switch (RPS) is connected via the Netilla failover cable to the Hot Standby port (FOVER) located on the front of the NSP designated as Backup. The Master power cable is plugged into the remote power switch. This allows the Backup machine to power cycle the Master when it initiates a failover routine.

If you have a G-class NSP with a Gigabit Ethernet interface, ETH1 of the NSP is the Gigabit interface. Therefore, reverse these instructions and connect to the network using ETH1 and connect to the secondary interface with ETH0.

About the Heartbeat Process

Monitoring between the two units is implemented via encrypted keep-alive messages, referred to as a heartbeat. Heartbeat messages are sent every two seconds over both Ethernet interfaces. The heartbeat process has two primary functions. First, it allows each node (Master and Backup) to monitor each other’s existence or health. Second, it manages the takeover procedure and migration of shared resources.

One consequence of this implementation is that the second Ethernet (ETH1) interface on each NSP, if not previously used, should be configured to a private subnet address (for example, 10.10.10.x), with a crossover cable used to connect the NSPs.

Each of the two NSPs monitors heartbeat messages from the other NSP. If the heartbeat from one NSP is missing for more then 10 seconds, the other NSP declares that unit "dead." At this point, any shared resources belonging to the dead NSP are migrated to the active unit.

The shared resources that are migrated include the public NSP name (i.e. office.netilla.com) and the Virtual IP address (VIP, also referred to as the public IP address). E-mails are sent to a designated IP address alerting the pre-configured contact admin that these resources have migrated or have been taken over.

About Replication

The Backup NSP must be ready to assume the role of the Master at any time. Therefore, the Backup NSP must be a clone of the Master. Any NSP configuration changes are replicated on the Backup machine. (Exceptions include changes that are host specific, such as host name, IP address, etc.)

About System Assurance

In failover mode the system assurance process on the Backup machine determines whether the application service on the Master is responding to external requests on the Virtual IP address. After two consecutive failed attempts to elicit a response from the Master's applications service (90 seconds apart), the Backup machine's system assurance process induces a failover by forcing a power cycle of the Master. Note that the system assurance process monitors the Master unit at a slower rate than the heartbeat process. This reduces the likelihood interaction between the two processes.

The system assurance process on the Backup machine also monitors the replication client and generates a warning e-mail if the client dies. If there is network connectivity to the Master unit, the system assurance process also stops the Backup's heartbeat process.

Hot Standby Roles

There are three configurations required for a Hot Standby system. Each unit is configured with a unique host name and a unique IP address, and configuration is shared between the Master and Backup. This third configuration is called the Virtual Address, and it determines how users access the resources of their NSP.

The Master unit assumes the identity of the virtual address and responds to all requests for the NSP. The Backup waits passively, monitoring the health of the Master. If the Backup detects that the application service on the Master has failed, or detects that the Master is unavailable, it will take over the role of Master for the site and will issue a restart to the Master unit. The Backup unit needs to power cycle the Master to avoid any shared resource contention issues and remove the possibility of two NSPs acting as Master simultaneously.

To ensure that there are never two simultaneous Masters, the role assumed by the NSP after a reboot is dependent on its state prior to the reboot. The state of the NSP is defined as the combination of its current role and its previous role. When a failure occurs, the units toggle operations. The Backup becomes the Master, but the Master that was previously a stand alone will never re-designate itself from "Master" to "Backup;" instead, the Master reboots as a stand-alone system.

The table below describes the change of states after a reboot. The state within the brackets indicates the role the unit had prior the current one. Note that once a Master is power cycled it cannot become a Master again. Also note that the Hot Standby feature does not allow for any states not listed in the table. For example,

it is never possible for a Master to change roles to a Backup without first changing to stand-alone mode.

State before reboot	Prior State	State after reboot
Master	[Stand-alone]	Stand-alone [Master]
Backup	[Stand-alone]	Backup [Stand-alone]
Master	[Backup]	Master [Backup]
Stand-alone	[Master]	Stand-alone [Master]

In the case of a power failure, both units will reboot, and the Master [a stand-alone in its prior state] will return as stand-alone [Master], while the Backup [Stand-alone in its prior state] will return as Backup. The Backup will detect that the Master in no longer available, and switch its role to Master [Backup].

About E-mail Alerts

Each time a change occurs in a Hot Standby installation, an e-mail alert is generated to a pre-defined e-mail address. Refer to “Appendix A: Troubleshooting” on page 225 for a list of email alerts and descriptions

Pre-Configuration Checklist

Before you begin configuration of the HotStandby feature, ensure that the following items have been completed.

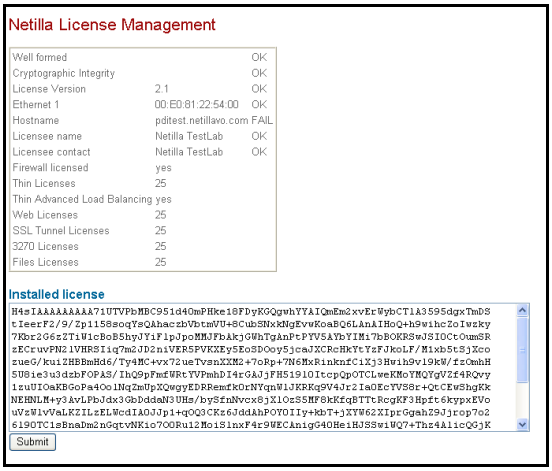
- ❑**Synchronize Date and Time**. Confirm that the date, time and time zone settings are in sync with both Master and Backup NSPs. Access each NSP’s serial console to check the date, time and time zone settings. For detailed steps, refer to *Appendix D* of the *Netilla Security Platform Administration Manual*.
- ❑**Configure a Time Server**. It is recommended that you configure a Time Server on the Master and the Backup NSPs. To do so, log in to each NSP. From the Administrator Site, select *System Configuration* and then select *Network Connections*. Enter the location of the time server in the field provided.

Variations in time between the Master and Backup NSPs that are greater than two minutes will cause a replication failure.

- ❑**Complete the Worksheet**. Fill in the following configuration worksheet with the appropriate information for your network.

	Name	IP Address (Primary)	IP Address (Secondary)
Virtual			N/A
Virtual Gateway			
Master			
Backup			

- ❑**Install Each NSP License**. You should have received two licenses, one for each of your NSPs. Install the appropriate license on each NSP. Ensure that both the Master and Backup NSPs have a license installed that references the virtual hostname. Once you install the license, you may notice that the Hostname field indicates **Failed** as shown.



This is the correct status for this stage. Once the HotStandby system is running (that is, replication occurs) the Hostname field becomes valid.

❑**For SecurID Users**. If SecurID is being used, before you configure HotStandby, authenticate to a SecurID server as follows.

- Create a SecurID authentication stage on each stand-alone system with the same realm name and in the same realm order.
- Authenticate each NSP individually to a SecurID server prior to Master/Backup configuration, as a stand alone platform. Before doing so, ensure that the secondary interface (eth1) is disabled (without settings and un-configured).
- After each NSP has successfully authenticated against a SecurID server, enable the secondary interface, which is necessary for Failover.

❑**Network Configuration**.

- Configure the secondary interface on both Master and Backup NSPs to a common network (different from the primary interface) to allow both NSPs to communicate with each other for replication and state messages exchange.
- Configure both Master and Backup primary interface to the same physical subnet.

❑**Physical Hostname Configuration for each NSP**. Configure the physical host name of both the Master and Backup NSP via each NSP's serial console port as described in *Appendix D of the Netilla Security Platform Administrator Manual*. No other site-specific configuration is needed, since the Backup will receive all of the site's configuration information when it synchronizes with the Master.

❑**Backup Each NSP's Configuration Profile.** Backup each NSP's configuration prior to configuring Hot Standby settings. For details, refer to the *NSP Administration Manual*.

❑**Netilla Software Version Must be the Same**: The Master and Backup NSP appliances must run the same version of Netilla software. To check the current version of software, log in to each NSP. From the Administrator Site, select *System Configuration*, *Software Upgrade* and then select *Server Status*. Under Local Upgrade, click *Continue*. Refer to the Current Release field.

❑**Firewall Settings**. If there is a firewall between the Master NSP and the server you designate in the Failover's Network Verification Address field, then the firewall must have a port open to allow ICMP messages from the NSP to the previously mentioned server. If you are using the Netilla firewall, here are

more detailed instructions. Add the following firewall rule in the Firewall Settings page of the NSP's Administrator Site:

- Action: Allow Connections
- Type: Unix
- Source Address: =
- Source Interface = Local
- Destination Address = IP Address of Network Verification Address
- Destination Interface = Interface that the Network Verification Address server is on
- Unix Protocol: ping

Only one server certificate is needed for both the Master and Backup NSPs because the certificate is associated with the virtual name of the Netilla HotStandby system which is seen as a single entity even though there are actually two NSPs.The server certificate that is applied to the Master will be copied over to the Backup during replication

HotStandby Hardware Installation

This section describes how to setup the Netilla Hot Standby hardware components.

Package Contents

The Netilla Hot Standby system includes the following items.

- Two Netilla Security Platforms (NSP) that will be installed in a redundant configuration (Master and Backup)
- A Remote Power Switch (RPS-10
- A Netilla Failover cable used to connect the Backup unit to the remote power switch

Remote Power Switch Description

This section describes the Remote Power Switch (RPS-10) which is included with the Hot Standby system.

An illustration of the front panel is shown in Figure 221.

Figure 221 RPS Front Panel

The following options are provided.

- **AC ON**: Lights when power to the Switched Outlet is ON.
- **LINK**: Flashes when command data is received

- **RDY**: Lights when AC Power is applied and the module is ready to receive commands. Note that this LED does not indicate the ON/OFF condition of the Switched Outlet.

An illustration of the RPS back panel is shown in Figure 222.

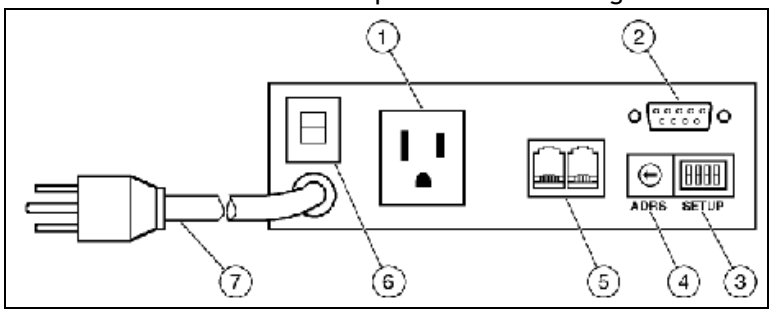


Figure 222 RPS Back Panel

The following options are provided.

1 Switched Outlet
2 RS232 Control Port
3 Setup Switches
4 Rotary Address Switch
5 RJ11 Link Ports
6 Circuit Breaker (10 Amps)
7 Power Cable

Netilla Hot Standby Physical Installation

This section describes the physical installation procedure for the Netilla Hot Standby system. An overview of the hardware setup is shown in Figure 223.

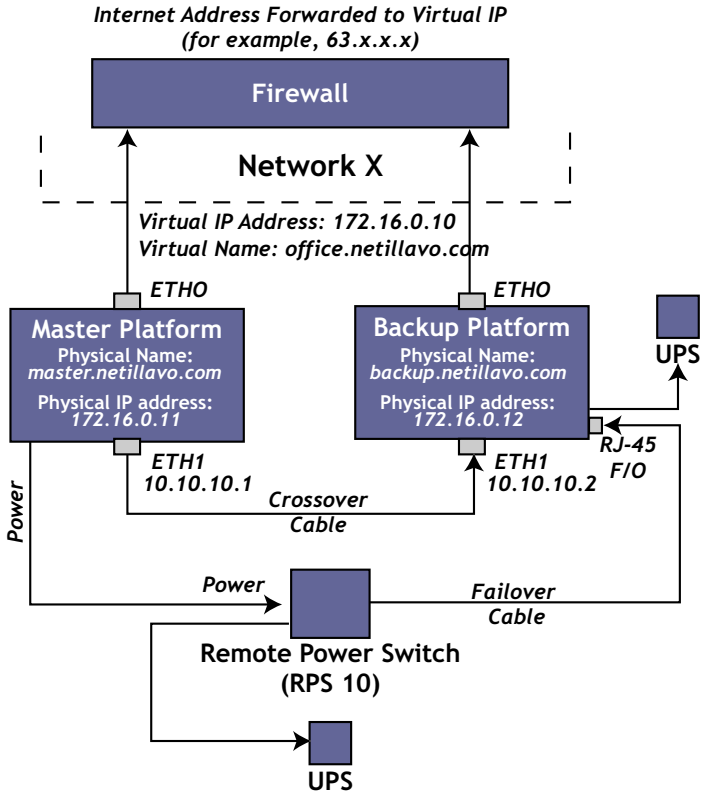


Figure 223 Hot Standby System Overview

The following configuration work sheet applies to the example shown in Figure 223.

Table 27 Example Configuration Work Sheet

	Name	Primary IP Address (ETH0)	Secondary IP Address (ETH1)
Virtual	office.netillavo.com	172.16.0.10	N/A
Master	master.netillavo.com	172.16.0.11	10.10.10.1
Backup	backup.netillavo.com	172.16.0.12	10.10.10.2

The Netilla Hot Standby System consists of two NSP appliances: a “Master” and a “Backup”. Each NSP appliance (both Master and Backup) ships with an individual hostname and IP address (e.g., master.netillavo.com - 172.16.0.11, backup.netillavo.com - 172.16.0.12). Each NSP appliance is subsequently configured to respond to a common virtual hostname and IP address.(e.g., office.netillavo.com - 172.16.0.10). Note that all three IP addresses must reside on the same network.

Both NSPs are connected via their secondary interface (ETH1) for replication and keep-alive status advertisement.

If you have a G-class NSP with a Gigabit Ethernet interface, ETH1 of the NSP is the Gigabit interface. Therefore, reverse these instructions and connect to the network using ETH1 and use the crossover cable with ETH0.

The Remote Power Switch (RPS) is connected via the Netilla failover cable to the Hot Standby port (FOVER) located on the front of the platform designated as Backup.

The Master power cable is plugged into the remote power switch. This allows the Backup machine to power cycle the Master when it initiates a failover routine.

It is recommended that the NSP be installed in a private network with an address that has been translated via NAT to the virtual IP address.

An example configuration worksheet is provided below, which can be used as a guide. Complete the worksheet with your particular network's parameters before you begin your hardware setup.

Table 28 Sample Configuration Worksheet

	Name	IP Address (Primary)	IP Address (Secondary)
Virtual			N/A
Master			
Backup			

Installing the Remote Power Switch (RPS10)

To install the RPS10, do the following.

1. Locate the section labeled Setup. Set switch 3 to the "up" position (i.e., "off"). All remaining switches remain in the "down" position.
2. Connect the provided power cable to a power source (preferably a UPS).
3. Connect one end of the provided Netilla HotStandby cable to the RJ45 port labeled FOVER on the Backup NSP and the other end to the RS232 port on the Remote Power Switch.

Installing the Master

To install the Master platform, do the following.

1. Connect the power cable from the back of the Master NSP to the switched outlet on back of the Remote Power Supply.
2. Connect the primary Ethernet port (ETH0) to the network through which the Master NSP will be accessed.

If you have a G-class NSP with a Gigabit Ethernet interface, ETH1 of the NSP is the Gigabit interface. Therefore, reverse these instructions and connect to the network using ETH1 and use the crossover cable with ETH0.

3. Connect the secondary Ethernet port (ETH1) to ETH1 on the Backup using a crossover cable. Alternatively, you can connect to a network that is common to ETH1.

   It is necessary for the two NSPs to communicate via ETH1 for heartbeat keep-alive message exchange and for synchronization of configuration changes.

***WARNING**: Do not connect the primary ETH0 and Secondary ETH1 interfaces on the same network. Doing so will cause a number of services to stop functioning.*

Installing the Backup

To install the Backup platform, do the following.

1. Connect the power cable to a power source separate from the one used for the Master (preferably a UPS).

Never connect the Backup unit's power cable to the Remote Power Switch.

2. Connect the RS232 end of the Netilla Failover cable to the Remote Power Switch (RPS-10) and connect the opposite end to the failover port on Backup (FOVER).
3. Connect the primary Ethernet ports (ETH0) the network through which the NSP will accessed.

If you have a G-class NSP with a Gigabit Ethernet interface, ETH1 of the NSP is the Gigabit interface. Therefore, reverse these instructions and connect to the network using ETH1 and use the crossover cable with ETH0.

4. Connect the crossover cable from ETH1 on Master to ETH1 on Backup. Alternatively, you can connect to a network that is common to ETH1.

   It is necessary for the two Netilla Security Platforms to communicate via ETH1 for heartbeat keep-alive message exchange and for synchronization of configuration changes.

***WARNING**: Do not connect the primary ETH0 and Secondary ETH1 interfaces on the same network. Doing so causes a number of services to stop functioning.*

Configuring the Master NSP

To configure the Hot Standby system, begin by configuring the Master. The first step is to fully configure the Master NSP as a stand-alone unit, as described in the *NSP Administration Manual*. This includes configuring all of the network parameters, application and application server creation, realm configuration, etc., and following the guidelines in the pre-installation section of this manual. Note the following:

- ❑When you name the Master, the physical name must be different from the virtual name.
- ❑Ensure a certificate that matches the virtual name is installed on the Master.

If you are setting up a SecurID authentication stage, refer to "For SecurID Users. If SecurID is being used, before you configure HotStandby, authenticate to a SecurID server as follows." on page 204 prior to configuring the Hot Standby system.

Do not configure the Backup until **AFTER** the email confirmation from Master has been received, as explained later in this section.

Configuring the Hot Standby Settings for the Master

To configure the Hot Standby settings on the Master NSP, do the following.

1. Log in to the NSP that will be used as the Master.
2. From the *Administrator Site*, click *System Configuration* and then click *Failover.*

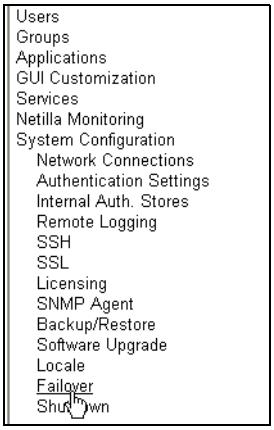


Figure 224 Failover Menu Location

3 For **Role**, select *Master* and then click *Change*, as shown in Figure 225.

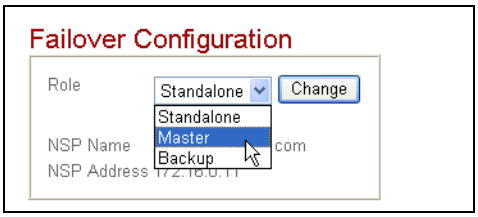


Figure 225 Failover Role Selection for Master NSP

After changing the role, the Failover Configuration page appears with the current details about the Master NSP, as shown in Figure 226.

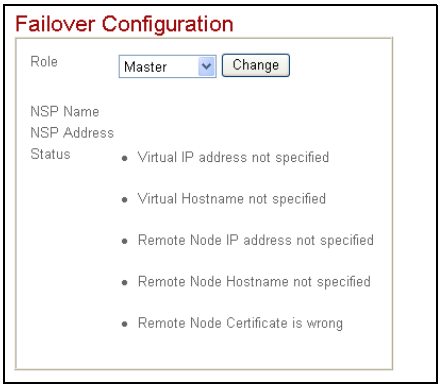


Figure 226 Failover Configuration Page for Master NSP

4 Go on to “Configuring the Virtual Settings on the Master” on page 210.

Configuring the Virtual Settings on the Master

This section describes how to configure the virtual NSP settings. These virtual settings are common to both the Master and Backup NSPs but are only configured on the Master NSP.

To configure the NSP settings, you will need the following information.

Table 29 NSP Settings Page Field Descriptions

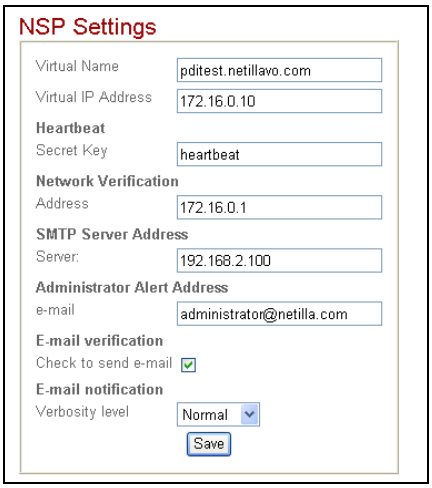
Field Name	Description

Virtual Name	The name of the NSP site. This is the address that will be used to access the NSP by end users.
Virtual IP Address	The IP address that will be used to access the site. Ownership of this address changes between NSP when a Hot Standby event occurs.
Heartbeat Secret Key	Enter any word or string to be used as a shared secret used to link both NSP for replication. The key can be any combination of characters and is case sensitive.
Network Verification Address	Enter the IP address of a server that responds to ICMP messages. For instance, the gateway for the Primary network. The Backup unit uses this IP address to verify network connectivity.
SMTP Server Address	Enter the IP address of your SMTP server.
Administration Alert Address	E-mail address that will receive system alerts related to Hot Standby.
Email Verification	Check to have system alerts sent via Email relating to Hot Standby.
Email Notification	Choose Email verbosity level. With *Normal* mode, only notifications about the shared resource migration and starting and stopping the failover service are sent. With *Verbose* mode, in addition to the notifications send in normal mode, notifications are sent about each fail over subsystem.

To configure the NSP settings for the virtual site, follow these steps.

1 From the Administration Site of the Master NSP, click *NSP Settings*.

The NSP Settings page appears.



2 Configure the appropriate information as described in Table 29.

3 Click *Save* to apply the changes.

4 Confirm that the assigned Netilla administrator receives an email with the subject *[Failover] The Email Verification* before going any further.

Do not continue with the next step until you confirm that the assigned Netilla administrator has received the Failover Verification email. If this email is not successfully received, verify that the SMTP server will allow the IP address of the NSP to use its SMTP gateway to relay messages to the email address you entered in the NSP Settings page. If you still do not receive an email, review your configuration steps.

5 Click *Replication Settings* from the Failover submenu of the Master NSP and then enter the Backup hostname (physical peer name).

6 Enter the Backup IP address (physical peer IP address of ETH0).

7 Highlight the certificate, right-click and choose *Copy* to copy the certificate to the Windows Clipboard buffer, as shown in Figure 227.

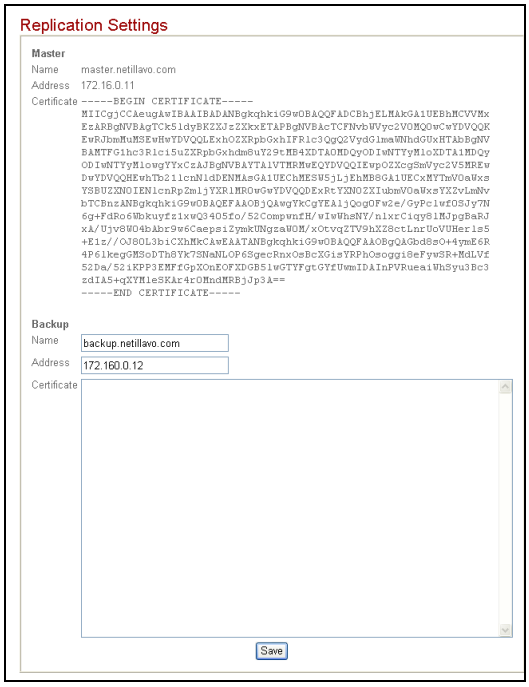


Figure 227 Digital Certificate Page for Master NSP

Note that using Control +C *does function properly when copying the certificate to the clipboard.*

You will paste the certificate into the Backup platform during its configuration, as explained in “Configuring the Backup NSP” on page 212.

8 Go on to “Configuring the Backup NSP”.

Configuring the Backup NSP

To configure the NSP that will function as the Backup, do the following.

1 Launch a new browser window to begin configuration of Backup.

2 Log into the NSP that will be designated as the Backup.

3 From the Administration Site, click *System Configuration*, and then click *Failover*.

4 For **Role,** select *Backup* and then click *Change*, as shown in Figure 228.

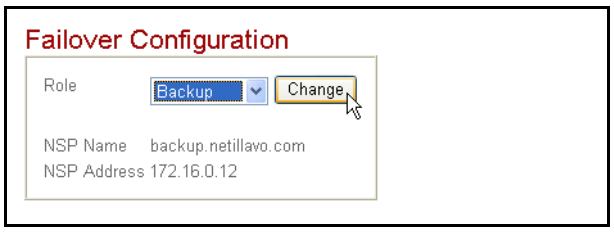


Figure 228 Failover Role Selection for Backup NSP

The Failover Settings window opens, as shown in Figure 229.

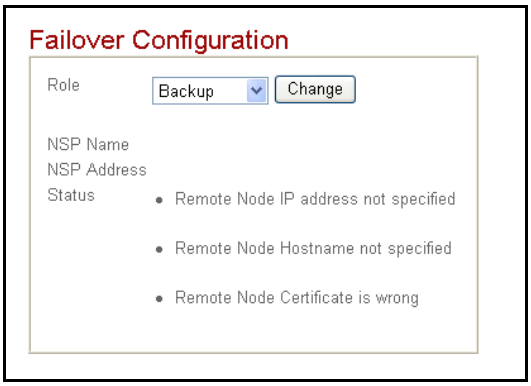


Figure 229 Failover Configuration Settings for Backup NSP

5 Click *Replication Settings* from the Failover submenu of the Backup NSP.

Because you are configuring the Backup NSP, "Remote Node" refers to the Master.

To make configuration easier, you can click the Task bar and click Tile Vertically to view the Master and Backup Configuration pages side-by-side as shown in Figure 230.

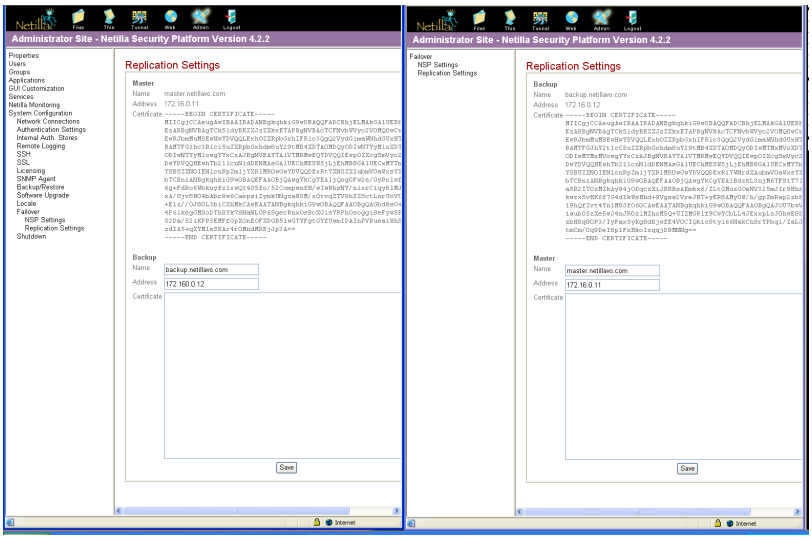


Figure 230 Side-by-Side Master and Backup Pages

6 From the Replication Settings page of the Backup NSP, enter the Physical IP address (actual IP), not the virtual IP address of the Master.

7 Paste in the certificate that you copied to the Windows Clipboard when configuring the Master.

8 Click *Save* to apply the changes, as shown in Figure 231.

Figure 231 Save Replication Settings Page for Backup NSP

9 Highlight and then copy the certificate (from the Backup) and paste it into the certificate field of the Master Replication Settings window.

This window should still be open if you launched a new browser window to configure the Backup.

10 Click *Save* on the Master as shown in Figure 232.

Figure 232 Save Replication Settings Page for Master NSP

11 Return to the Backup Replication Settings window.

12 Click *Save*.

This concludes the Netilla Hot Standby system configuration. To start the HotStandby system, go on to the next section.

Starting the HotStandby System

This section describes how to start the failover process.

1 From the Master NSP, click *Failover* from the System Configuration submenu.

2 Click *Start Failover* as shown in Figure 233.

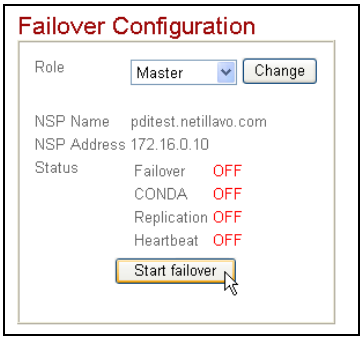


Figure 233 Start Failover Button for Master NSP

The heartbeat and replication processes begin. Status messages are displayed, as shown in Figure 234.

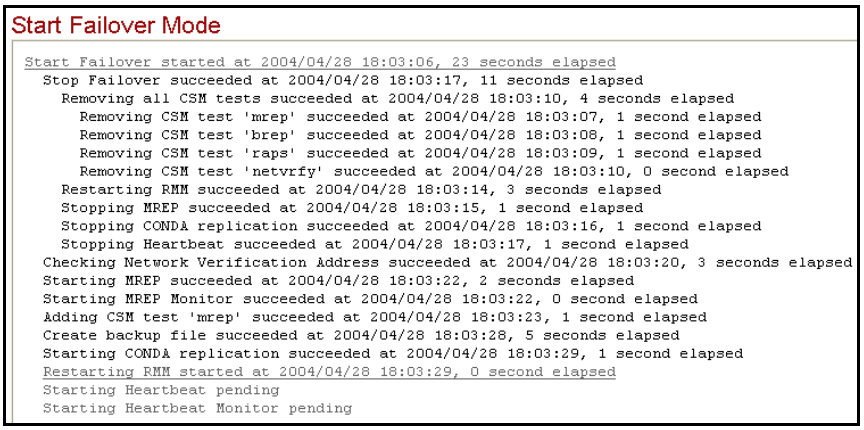


Figure 234 Initialization Status Messages on Master NSP

Once the process is complete, the first line indicates Start Failover Succeeded and the *Back* link appears at the bottom of the page. Click the *Back* link, as shown in Figure 235, to return to the Failover Configuration page.

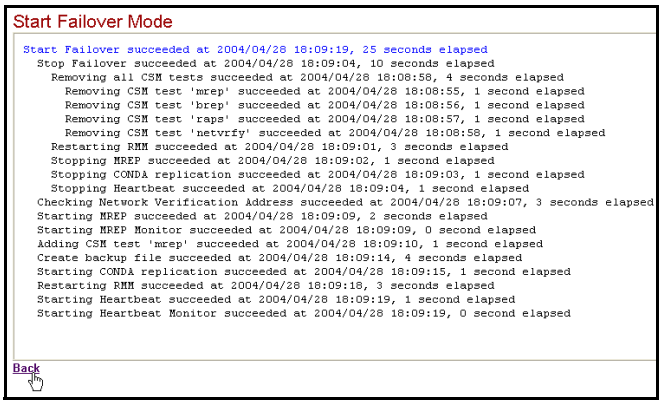


Figure 235 Initialization Status Message End with Back Link on Master NSP

3 Verify that the replication client has started by viewing the Failover Settings window on the Master as shown in Figure 236.

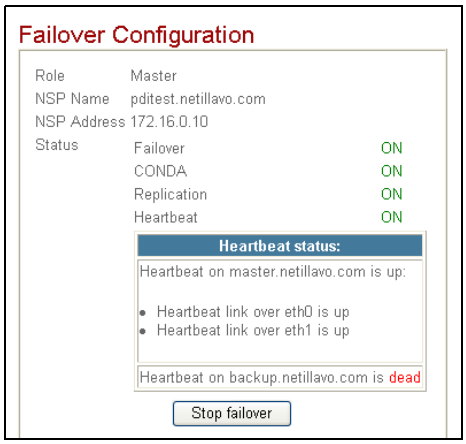


Figure 236 Failover Settings Status Window for Master NSP

4 From the Backup NSP, click *Failover* from the System Configuration submenu.

5 Click *Start Failover* from the Backup NSP as shown in Figure 237.

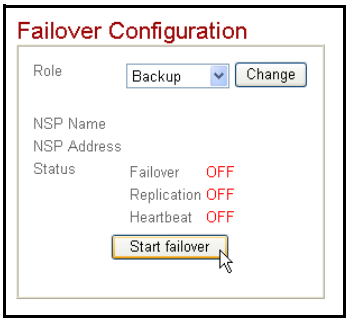


Figure 237 Start Failover Button on Backup NSP

6 The heartbeat and replication processes begin. Status messages are displayed, as shown in Figure 238.

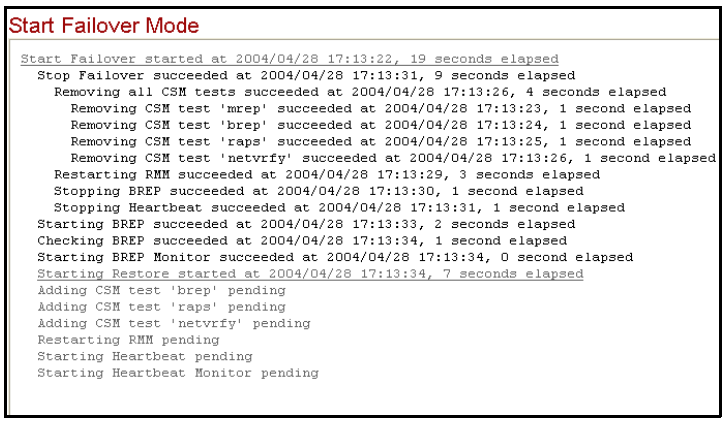


Figure 238 Initialization Status Messages

Once the process is complete, the first line indicates Start Failover Succeeded and the *Back* link appears at the bottom of the page. Click the *Back* link, as shown in Figure 235, to return to the Failover Configuration page.

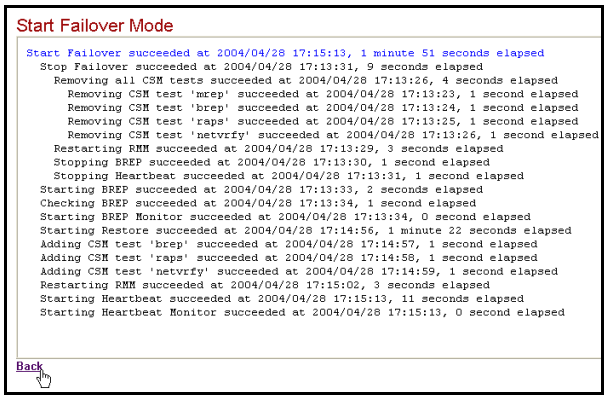


Figure 239 Initialization Status Message End with Back Link on Backup NSP

7 Verify that the replication client has started by viewing the Failover Settings window on the Backup NSP as shown in Figure 240.

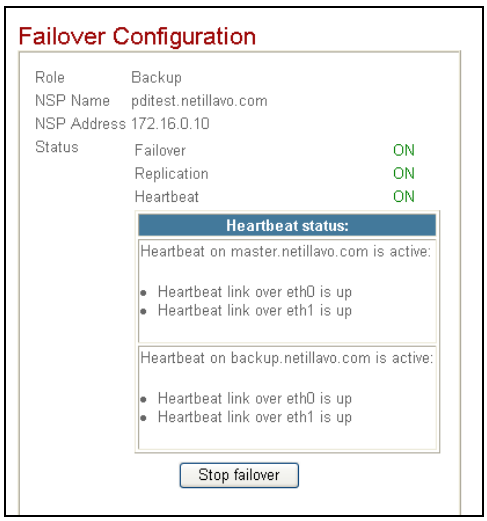


Figure 240 Failover Settings Status Window for the Backup NSP

8 Review the Status section to ensure that each process is On.

You may need to refresh the browser window on each NSP to display updated failover status.

Stopping the Hot Standby System

To manually stop the Hot Standby system **you must first stop the failover process on the Backup NSP and then stop the failover process on the Master NSP**. To do so, follow these instructions.

1 Connect to the physical IP address of the Backup NSP.

2 From the *Administrator Site*, click *System Configuration* and then click *Failover*.

3 Click *Stop Failover*, as shown in Figure 241.

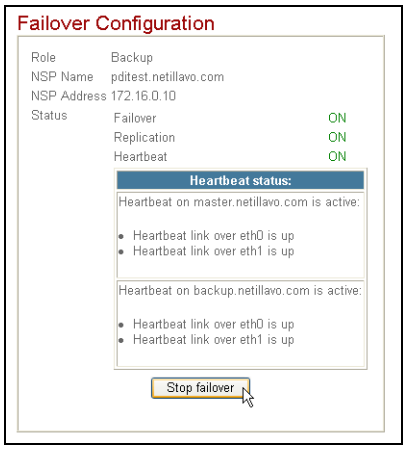


Figure 241 Stop Failover Button on the Backup NSP

This stops the Hot Standby service on the Backup NSP. You will see status messages similar to the following.

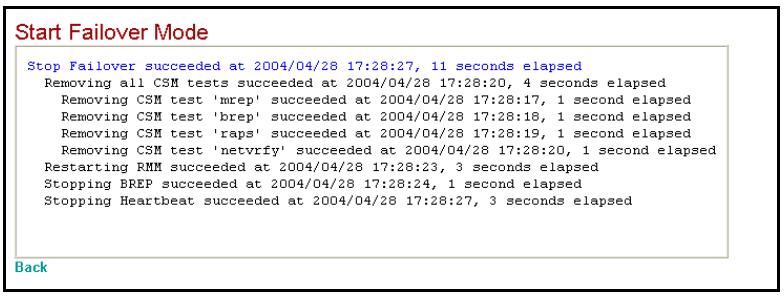


Figure 242 Stop Failover Status Messages on Backup NSP

4 Connect to the physical IP address of the Master NSP.

5 From the *Administrator Site*, click *System Configuration* and then click *Failover.*

6 Click *Stop Failover* as shown in Figure 243.

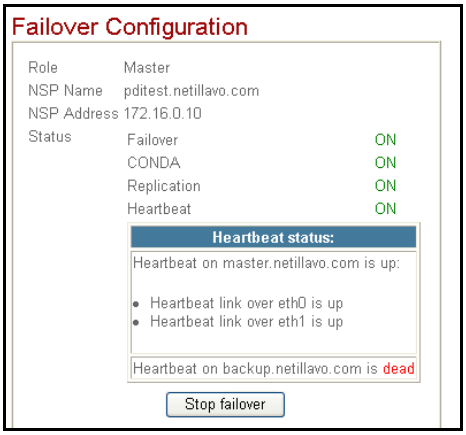


Figure 243 Stop Failover Button on Master NSP

This stops the Hot Standby service. You will see status messages similar to the following.

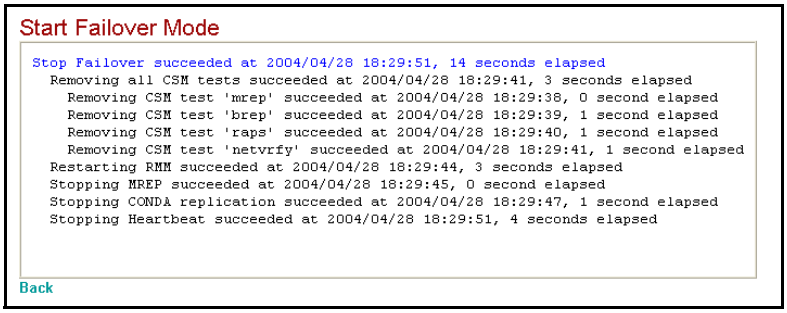


Figure 244 Stop Failover Status Messages on Master NSP

What to do If Failover Occurs

If failover occurs, the first step is to determine what caused the failover. There are variety of reasons why a fault is detected on a Master NSP causing the system

to revert to a Backup NSP. Contact your reseller for help in determining what caused the failover to occur.

Resetting Failover

Once you determine the cause and are ready to reset Failover, do the following.

1 Stop failover on the NSP currently acting as Master as shown in

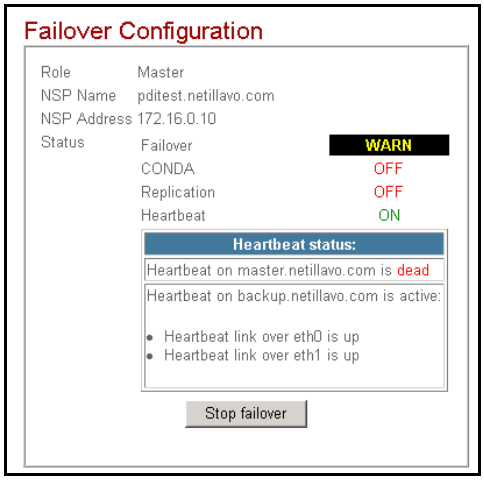


Figure 245 Stop Failover Page

2 Change the role of the NSP currently acting as Master to Standalone.

3 Log in to the NSP that you want to become Master.

4 Click *System Configuration* and then click *Failover*. For **Role**, select *Master* and then click *Change*, as shown in Figure 225.

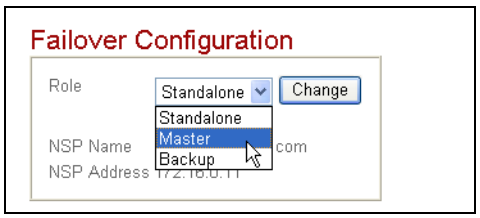


Figure 246 Failover Role Selection for Master NSP

5 Open another browser window and then log in to the NSP that you want to be the Backup.

6 Click *System Confutation* and then click *Failover*. For **Role**, select Standalone and then click *Change*. You will now see Backup as an option under Role. Select *Backup* and then click *Change*, as shown in Figure 228.

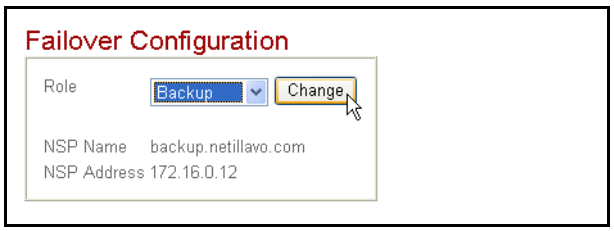


Figure 247 Failover Role Selection for Backup NSP

7 From the Master NSP, click *Start Failover* as shown in Figure 233.

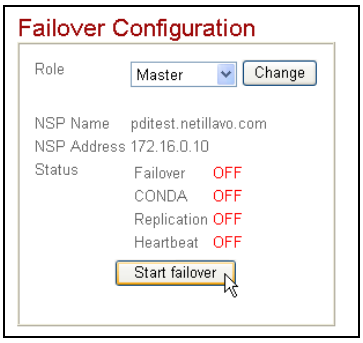


Figure 248 Start Failover Button for Master NSP

The heartbeat and replication processes begin. Once the process is complete, the first line indicates Start Failover Succeeded and the *Back* link appears at the bottom of the page. Click the *Back* link, as shown in Figure 235, to return to the Failover Configuration page.

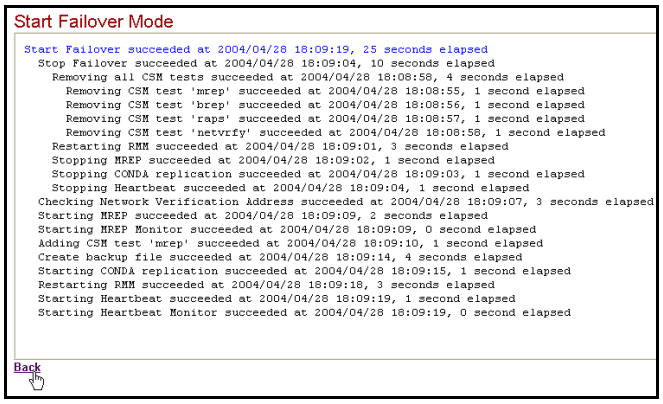


Figure 249 Initialization Status Message End with Back Link on Master NSP

8 Verify that the replication client has started by viewing the Failover Settings window on the Master as shown in Figure 236.

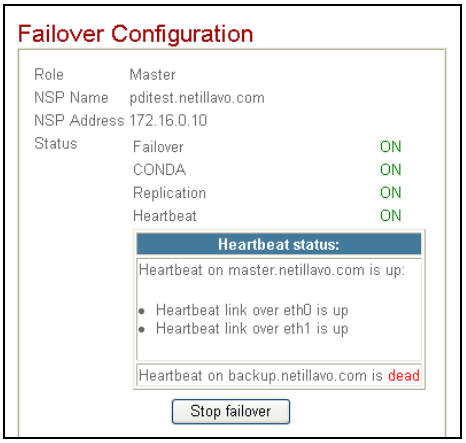


Figure 250 Failover Settings Status Window for Master NSP

9 From the Backup NSP, click *Failover* from the System Configuration submenu.

10 Click *Start Failover* from the Backup NSP as shown in Figure 237.

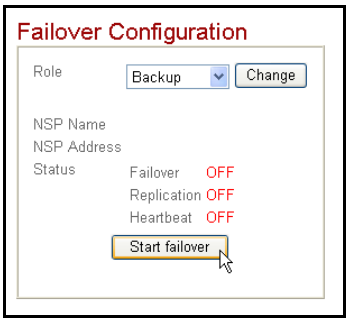


Figure 251 Start Failover Button on Backup NSP

The heartbeat and replication processes begin. Status messages are displayed.Once the process is complete, the first line reads *Start Failover Succeeded* and the *Back* link appears at the bottom of the page. Click the *Back* link, as shown in Figure 252, to return to the Failover Configuration page.

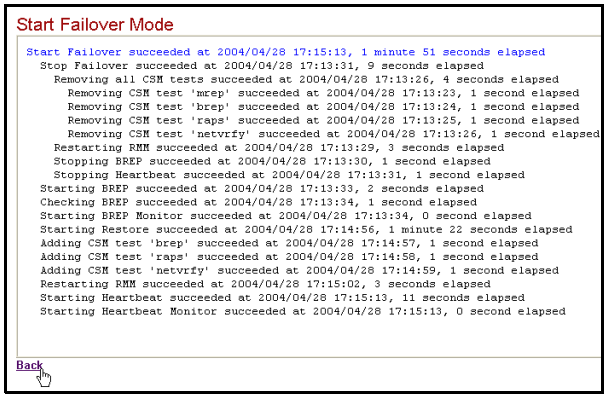


Figure 252 Initialization Status Message End with Back Link on Backup NSP

11 Verify that the replication client has started by viewing the Failover Settings window on the Backup NSP as shown in Figure 253.

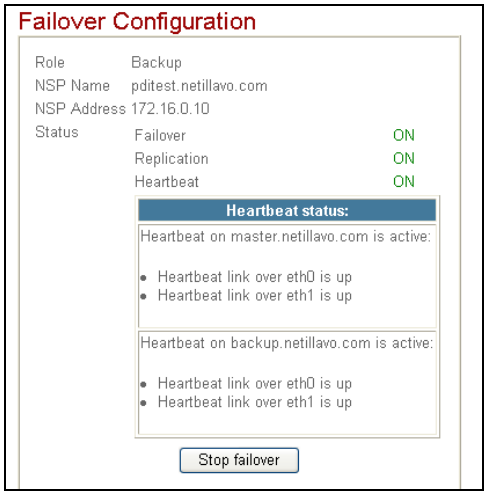


Figure 253 Failover Settings Status Window for the Backup NSP

12 Review the Status section to ensure that each process is On.

You may need to refresh the browser window on each NSP to display updated failover status.

Email Alerts

The following table lists and describes some of the email messages that you may receive regarding the HotStandby Service.

The following table lists and describes many of the possible e-mail alert messages that administrators can receive. The host's names used in this example are "master.netillavo.com" and "backup.netillavo.com".

Table 30 E-mail Message Description Table

Message Subject	Message Body	Description
[Failover] The e-mail verification	This test e-mail has been sent to verify the failover e-mail settings.	Indicates that no configuration errors have been detected in the NSP Settings page. You can proceed by starting the failover process on the Master NSP.
[FAILOVER] Start Failover initiated on the master	Start Failover initiated at 2004/04/28 18:03:06.	Indicates the date and time failover was initiated on the master NSP.
[FAILOVER] Start Failover succeeded on the master	Start Failover succeeded at 2004/04/28 18:03:33.	Indicates failover initiation was successful.
[FAILOVER] Shared resource takeover by 'master.netillavo.com'.	The public NSP name and virtual IP address now reside on 'master.netillavo.com'.	Master.netillavo.com has control of the Virtual IP address and the public name of the system
[FAILOVER] Stop Failover initiated on the master	Stop Failover initiated at 2004/04/28 18:06:54.	Indicates the process for stopping failover has begun.
[FAILOVER] Stop Failover succeeded on the master	Stop Failover succeeded at 2004/04/28 18:07:08.	Indicates failover has been stopped.
[Failover] Heartbeat status changed	Interface 'eth1' on host 'master.netillavo.com' changed status from 'dead' to 'up'.	Indicates the eth1 interface is now up. Heartbeat status messages are sent when the status (up or down) changes for Ethernet interfaces as well as when the status changes for the backup and master NSP.
[Failover] CONDA replication mode has been enabled	The CONDA replication mode has been enabled on the master.	The master NSP is preparing to replicate its settings to the Backup NSP.
[Failover] Replication server started	The replication server has been started on the master NSP	The master NSP is preparing to replicate its settings to the Backup NSP.
[FAILOVER] Shared resource migration from 'master.netillavo.com'.	The public NSP name and virtual IP address no longer belong to 'master.netillavo.com'.	Master.netillavo.com has surrendered the virtual IP and public name
[FAILOVER] CSM: INITIATING HOT STANDBY TO BACKUP SERVER	REMOTE APP SERVICE FAILURE detected	The Backup system assurance process has detected that the Master's app service isn't running and has initiated a fail over as a result
[FAILOVER] CSM: REPLICATION SERVER FAILURE	REPLICATION SERVER FAILURE detected	The system assurance process has detected that at least one of the replication processes on the Master has died
[FAILOVER] CSM: REPLICATION CLIENT FAILURE	REPLICATION CLIENT FAILURE detected	The system assurance process has detected that the replication client on the Backup machine has died

Table 30 E-mail Message Description Table

[FAILOVER] Start Failover failed on the backup	Start Failover failed: Replication:Installer:BREPException: tlsv1 alert **unknown ca**	Indicates there's a certificate error. Repeat the certificate replication process and then start failover again. For details, begin with "Configuring the Master NSP" on page 143.

A Appendix A: Troubleshooting

This chapter presents general troubleshooting suggestions to overcome common problems you may experience with the Netilla Security Platform (NSP).

The following topics are discussed.

- Troubleshooting Realms
- Troubleshooting the Thin Service
- Troubleshooting the Web Service
- Troubleshooting the Tunnel Service
- Troubleshooting Certificate Errors
- Troubleshooting End User Access
- Troubleshooting the HotStandby System

Troubleshooting Realms

This section describes how to resolve problems you may experience with realms. Refer to the appropriate section.

- Troubleshooting a Local Authentication Realm
- Troubleshooting SecurID Realm

Troubleshooting a Local Authentication Realm

This section provides answers to common questions that may arise when setting up a local authentication realm.

Problem:

Users can successfully login to a local realm, but are presented with the Windows 2000 login screen each time they launch an application.

Possible solution:

1. Log in to the Windows Terminal Server that hosts your applications.
2. Choose *Administrative Tools*, *Terminal Services Configuration*, and then double click *RDP-TCP*, located under *Connections*.
3. Click *Logon Settings* and clear the *Always Prompt for Password* checkbox.
4. Have the users log out and then log in again.

   If users are still prompted to enter a username and password, then continue with the next step.
5. Check to see that the Authentication Scope name that you entered while creating your local realm is spelled exactly as the Scope Label text that is entered when setting up your Application Server in the NSP Administrator Site.
6. Log in to the NSP as *radmin*.

7 Click *System Configuration*, and then choose *Authentication Settings*.

Find the name of the authentication stage that authenticates for local users. Note the spelling of the Local Authentication Realm that you assigned.

8 Click *Application Servers* and choose the name of your Terminal Server. The properties of the Terminal Server are displayed in the right-hand side window.

Make sure the spelling of the Application Server Authentication Scope exactly matches the name of the Authentication Realm Scope that you looked up. If they don't match, change the Application Server Authentication Scope to exactly match the Authentication Realm Scope. This should be the domain name of the application server.

9 Click *Submit*.

Troubleshooting SecurID Realm

This section provides answers to common questions that may arise when setting up a SecurID authentication realm.

Problem:

You setup a SecurID Realm but users are not able to authenticate.

Possible solution

Verify that the user's SecurID key fob, PIN code, and server side configuration are functioning properly.

1 Verify that the user can successfully log into the ACE server from another ACE client on the network.

Refer to the ACE Server instruction manuals for information on using the ACE Server Windows/UNIX client.

2 Confirm that the user has not been blocked from authenticating to the realm that contains the SecurID authentication stage.

When you configured the policy for the SecurID authentication stage during its initial configuration, you may have placed a group in the Exclude field. Ensure that the user is not a member of the excluded group.

3 Next, check that the user is entering their NT username and their 4 digit pin number followed by the SecurID six digit number.

4 Verify that the user is selecting the SecurID Realm from the Realm drop down box on the login screen.

5 If the user has done everything correctly, check to see if a sub-realm was created within the SecurID realm for NT SMB authentication.

When you stack authentication realms, if any part of the authentication is wrong, then the user is sent back to the beginning of the first stage.

For example, if a user authenticates to a SecurID server, and then incorrectly enters their NT password when prompted, they are subsequently returned beginning to re-authenticate with SecurID.

6 Ensure that the NT username is the same as the SecurID username.

The NSP takes the username supplied at the time of log in to the SecurID server, and passes this username to the NT authentication stage, if it is present. Note that you cannot have a different username for SMB when using stacked realms.

Troubleshooting the Thin Service

This section provides troubleshooting information for the Thin service which covers remote application configuration and usage. The following information is provided.

- Troubleshooting Client Drive Mapping
- Thin Applications Error Messages Explained
- Printing Problems with Thin Applications
- Troubleshooting End User Remote Application Access
- Troubleshooting the Applet Download
- Troubleshooting Proxy Server and Other Connection Problems

Troubleshooting Client Drive Mapping

Although Local Drive mapping is very simple to setup, sometimes problems arise. If local drive mapping does not work, try the following.

Prerequisites

Verify that you have met the following prerequisites for local drive mapping.

- Local drive mapping uses port 139/tcp on the NSP. Verify that port 139 is open between the NSP and the Terminal Server
- Local drive mapping works only with Microsoft Internet Explorer running on a Windows client.
- The Enhancement module must be installed on the Terminal Server. Refer to “Installing the Enhancement Module” on page 227 for details.
- If the NSP is installed as a bastion host, edit the host file on the Terminal Server so that it resolves the URL of the NSP to the private (LAN) IP address. Refer to “Adding a Host File Entry for the NSP” on page 229.

If you have met these prerequisites and are still having trouble with local drive mapping, go on to “Ensure that the NSP can be resolved by the Terminal Server by URL.” on page 228.

Installing the Enhancement Module

1. Access the Add/Remove Programs control panel.
2. Ensure the Enhancement Module for Windows is installed, as shown in Figure 254.

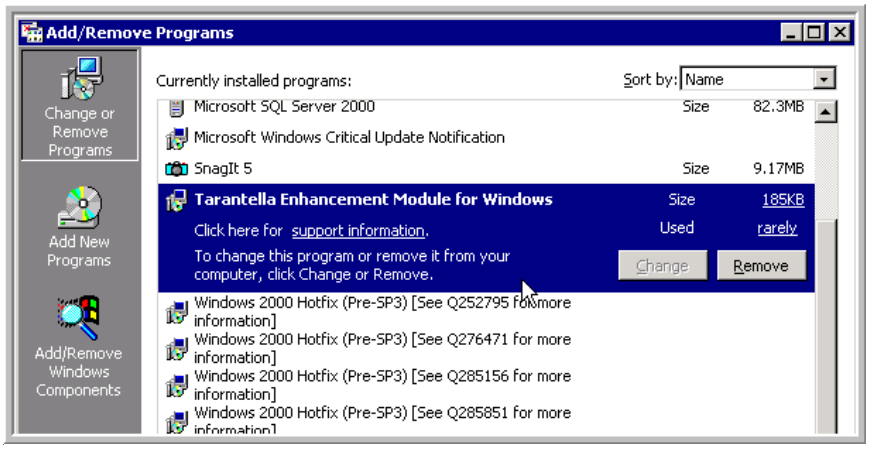


Figure 254 Add Remove Programs Control Panel

If the Enhancement Module for Windows is installed, go on to “Ensure that the NSP can be resolved by the Terminal Server by URL.”

If not, reload the module by browsing to the following URL of your NSP:

company.netillavo.com/extras/temwin32.exe

Ensure that the NSP can be resolved by the Terminal Server by URL.

1 Open a DOS prompt on the Terminal Server and ping the full URL of the NSP. For example **ping yourcompany.netillavo.com**, as shown in Figure 255.

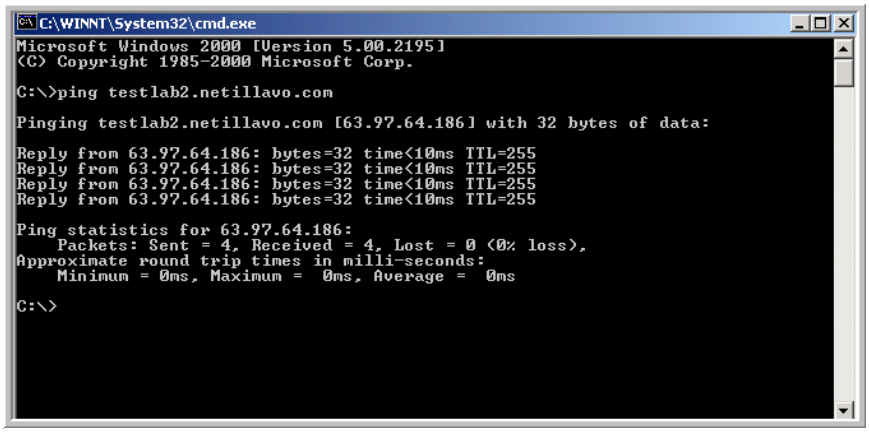


Figure 255 DOS Prompt Ping Windows

Ensure that the response is coming from the internal IP address and not from the public address of the NSP. If the NSP responds from a public IP address, it is very likely that it is sitting behind a firewall or router device and that device is blocking NetBIOS traffic. If this is the case, see “Adding a Host File Entry for the NSP” on page 229 to edit your host file to resolve the URL of the NSP to a private IP address.

2 If the ping receives a successful reply, the Terminal Server can see the NSP.

3 If the pings time out, the Terminal Server cannot resolve the NSP correctly. In this case, add a host file on the Terminal Server, as explained in “Adding a Host File Entry for the NSP” on page 229.

Adding a Host File Entry for the NSP

1 Open Notepad.

2 Click *File*, and choose *Open*.

3 Browse to the file C:\Winnt\System32\Drivers\ETC\hosts and open this file.

4 Add a line to the Hosts file that starts with the Internal IP address of the Netilla Service Appliance.

5 Press the TAB key on your keyboard, and then enter the URL of the NSP.

For example: “192.168.100.10 companyname.netillavo.com”

6 Save the file.

7 Test to see if the corrected file works by pinging the NSP by its URL from a DOS prompt. If you receive a successful reply retry Local Drive Mapping.

8 If you still cannot ping the NSP by its URL, confirm the IP address and the spelling of the URL entered in the Hosts file.

9 Open Terminal Server Manager and check to see if the TTATDM.exe runs under “Processes” when the user connects, as shown in Figure 256.

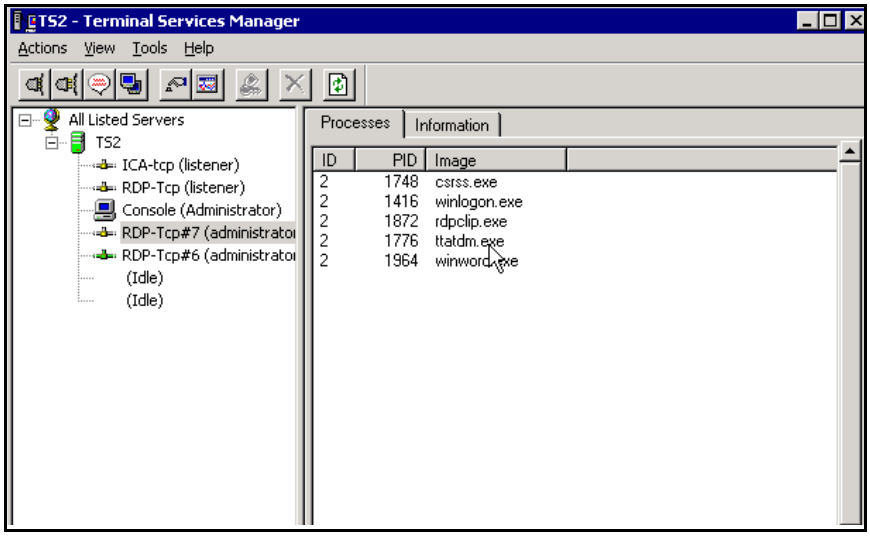


Figure 256 Terminal Server Manager

Doing so immediately reveals whether the local drive mappings are functioning.

10 If not, remove the Tarantella Enhancement Module and re-install the temwin32.exe file.

11 If problems persist, go on to “Additional Troubleshooting Tips”.

Additional Troubleshooting Tips

Collect the following information and then contact Netilla Technical support.

1 From the Terminal Server, run the net view command again to the fully qualified domain name of the NSP.

I.e. ***net view comapny.netillavo.com***

The command should return error 5.

If you receiver an error 5, this means that the terminal server can resolve the URL to IP address of the NSP successfully and it also confirms that the port 139 is not being blocked.

All other errors indicate the opposite; either the terminal server is unable to resolve the fully qualified domain name of the NSP to the internal address or the name is being resolved correctly but NetBIOS traffic is blocked between the NSP and the terminal server.

2 To test that the name is being resolved correctly, ping the fully qualified domain name of the NSP and make sure that it is responding from the private interface.

3 To test that NetBIOS traffic is not being blocked, telnet to the NSP from the Terminal Server via port 139. That is, c:\>telnet company.netillavo.com 139. A successful connection results in a black screen with a blinking cursor on the top left of the screen.

4 Press “Ctrl+]” to exit from telnet. If the port is being blocked, a trying to connect message is displayed for a few seconds followed by another message that the system cannot open a connection to the host on port 139.

Thin Applications Error Messages Explained

This section explains the various error messages that may be presented to users when launching an application icon on the Thin services page of the NSP.

The Launch Details Window

Selecting the Show Launch Details checkbox displays the Launch Details window each time an application is requested. The example in Figure 257 details a successful connection.

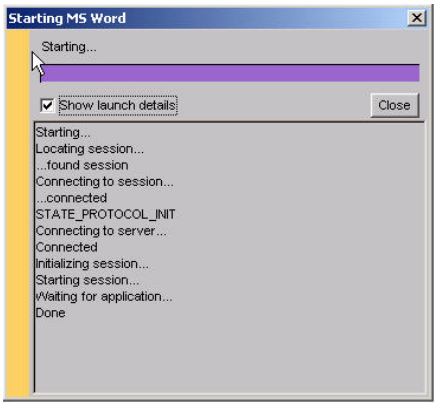


Figure 257 Launch Details Window

Refer to the preferred section.

- Microsoft Windows Application Messages
- 3270 Mainframe Application Messages
- X Windows Connection Application Messages
- Unix Character-Based Error Messages

Microsoft Windows Application Messages

Table 31 lists the various error messages that may be presented to end users when launching a Microsoft Windows application.

Table 31 Error Messages for Microsoft Windows Applications

Message	Description
No Terminal Services Licenses Available	The *No Terminal Services Licenses Available* error appears when there are no available TSCALs from a License Server to allow a connection to the application server.
Application Server Not Specified	The *Application Server Not Specified* error appears if an application server has not been specified within the individual application's properties. This is a common error that is made when creating a new application. Ensure that an application server has been specified in the application parameters.
Connection Failed: No Route to Host	The *Connection Failed: No Route to Host* error appears during launch if an application server address is not correctly specified, or if there is no physical path for the NSP to reach the server. In this case, you may need to configure a static route. Refer to Chapter 2 "How to Configure a Static Route" on page 22 for more information.
Connection Failed: Connection Refused	The *Connection Failed: Connection Refused* error message appears when a connection is attempted to a server that is not running Terminal Services, or a server where the Terminal Services service has stopped.
Protocol Engine "xxx_xxx" Has Rejected the Request	The error message *Protocol Engine "xxx_xxx" has rejected the request* appears when there is an error in the application's configuration fields (e.g., reversed fields, netbios name instead of IP address).

3270 Mainframe Application Messages

Table 32 details the 3270 emulation (mainframe) messages that might appear when launching a 3270 application.

Table 32 Error Messages for 3270 Mainframe Applications

Message	Description
Connect to* >IP Address of NSP<, *port xx: Connection refused	The message *Connect to* >IP Address of NSP<, *port xx: Connection refused* appears if there an application server has not been specified within the application's configuration. This might occur if the application is attempting to connect to the NSP's IP address rather than the application server's IP address.
Connect to >IP Address of Host<, port xx: No route to Host:	The message *Connect to >IP Address of Host<, port xx: No route to Host* appears if a valid host for the application is not found at the specified IP address.
Connect to >IP Address of Host<, port xx: Connection refused:	The message *Connect to >IP Address of Host>, port xx: Connection refused* appears if the connection method specified within the application's properties is not supported by or is not available to the host. For example, this scenario might occur if telnet is the specified connection protocol, but telnet access to the host is blocked on the Netilla Firewall.

Table 32 Error Messages for 3270 Mainframe Applications

Message	Description
3270 "INV-DEVICE-TYPE" Error	This error is generated if the 3270 mainframe does not support the terminal type sent by the NSP, which dictates whether to act as a 3278 or 3279 terminal, how many columns and rows to render, and whether or not to support printing. These parameters are set via the Arguments field for the 3270 Application General Properties. If you this error upon connecting to the 3270 server, add the text *-model 3279-2-E* to the Arguments field. This suggested text is made up of three parts, any of which can be omitted. The first part is the base model, which is either 3278 or 3279. 3278 specifies a monochrome 3270 display; 3279 specifies a color 3270 display. When 3278 emulation is specified for a color X display, fields are displayed using pseudo-colors. The second part is the model number, which specifies the number of rows and columns. Model 4 is the default. The third part specifies the Extended 3270 Data Stream, and is given as -E. It sends a signal to the host that the 3270 display is capable of displaying extended field attributes, and supports structured fields and query replies. A 3279 always uses the Extended Data Stream (whether or not -E is specified); for a 3278 it is optional. The default model for a color X display is 3279-4-E. For a monochrome X display, it is 3278-4-E.

X Windows Connection Application Messages

Table 33 details the error messages that might appear when launching an X Windows application.

Table 33 Error Messages for X Windows Applications

Message	Description
Authentication for >FQDN of NSP<:	The error message *Authentication for >domain name of NSP<* appears if a host for the application is not specified within the application's properties.
Error: ErrTransport Not Available (No route to Host):	The *Error: ErrTransportNotAvailable (No route to host)* message appears if the host specified within the application's properties does not exist. For example, this message might be generated if an incorrect IP address of the application server (host) has been specified, or if no route is available to the host. If this is the case, you may need to configure a static route. Refer to Chapter 2 "How to Configure a Static Route" on page 22 for more information.
Error: ErrTransport NotAvailable (Connection Refused):	The error message *Error: ErrTransportNotAvailable (Connection refused)* appears if the protocol specified within the application's properties is not available or supported on the Host. For example, this message is generated if telnet is the specified connection protocol, but telnet is being blocked by the NSP firewall, of if the telnet daemon is not running on the server.
Error: ErrThirdTierRead:	The error message *Error: ErrThirdTierRead* appears when connecting to a server that does not have the X protocol activated.

Unix Character-Based Error Messages

This section details the messages that might appear when launching a UNIX character-based application.

Table 34 Error Messages for UNIX Character-Based Applications

Message	Description
Authentication for >Domain Name of NSP<	The *Authentication for >domain name of NSP<* dialog box appears if a supported server is not specified within the application's properties.
Error: ErrTransportNotAvailable (No route to host):	The message *Error: ErrTransportNotAvailable (No route to host)* appears if the server specified within the application's properties does not exist at the specified IP address, or if there is no physical path for the NSP to reach the server. In this case, you may need to configure a static route. Refer to Chapter 2 "How to Configure a Static Route" on page 22 for more information.
Error: ErrTransportNotAvailable (Connection refused)	The message *Error: ErrTransportNotAvailable (Connection refused)* appears if the connection method (e.g., telnet) is supported by the server, but the application does not exist on the server. For example, this might be caused by erroneously connecting to a Windows server with telnet enabled, but the application does not exist on the server.
No such file or directory	The error message *No such file or directory* appears if the server is correctly specified within the application's properties but the application path is not correctly specified.

Printing Problems with Thin Applications

If you experience any difficulties while trying to print while using Thin applications, refer to Table 35.

Table 35 Remote Application Printing Problems and Solutions

Problem	Solution
While printing to a local printer, my session was disconnection.	When you print from a remote application, the output is sent back to the local printer through the Netilla Application Service Print Queue software. If the session is disconnected and the print job has not been fully sent to the local machine, it will remain in the Netilla Application Service print queue. When the user reconnects and opens a Thin application, the printer will show that the queue is paused and list the number of jobs still left. Simply click the pause button and the print job will start again. There is no time limit to how long the job will remain in the queue.
The session printer does not get created on the application server	The user may not have a default printer defined locally. Verify by looking at the printer icon on the user's desktop and confirm that a green check mark appears on the printer. If the green check mark is present, verify that the correct printer driver has been detected by viewing the browser's status bar while hovering the mouse pointer over the printer icon. If the icon is red, then define a default local printer for the user.
Cannot see the printer being created after installing the printer driver on the application server.	Contact the printer's manufacturer to determine if a driver is available for your printer that is compatible with Windows Terminal Server. Note that not all printers are supported for remote session printing. Some printers use proprietary print spoolers and monitoring programs that do not work with Microsoft's RDP protocol. These printers must be attached directly to the computer running the application to allow bi-directional communication. This is common on low-end printers, also known as Win Printers, that do not have the necessary hardware to simultaneously render print jobs and rely on software running on a client computer for processing.
Print jobs never reach my local printer even though the printer is on the application server.	Make sure that the printer is not paused on the NSP webtop. Go to the Thin icon of the NSP and verify that a green check mark appears on the printer icon on the left had of the screen. If there is not a green check mark, is likely that the printer queue has been paused. Click once on the pause button to un-pause the queue.

Table 35 Remote Application Printing Problems and Solutions

Problem	Solution
Cannot print	Make sure that the clients' printer is not paused. If it is not paused, it is possible that there is a configuration error with the your NSP. Contact Netilla technical support for assistance.
Print jobs take a long time to print.	The print process has three steps: 1.)The job is processed and spooled on the application server. 2).The processed job is transferred from the application server to the NSP's print queue, 3.)The job is transferred from the NSP's queue to the client's local queue Because the job is processed and spooled remotely, it can take anywhere from a few seconds to several minutes to begin printing. The size of the document being printed and the bandwidth availability of the user's connection also affect the speed of remote printing.
Printer is being detected by the NSP (there's a green check mark on the WebTop printer icon), but the session printer is not being created on the application server	The print driver is not installed on the application server. The printer driver must be installed on the Terminal server. If the print driver is not installed, an event will be registered on the Terminal Server's event viewer. Look for an event titled "TemServDevices". Once opened, it should read "Driver Unknown required for printer," or simply "Printer could not be installed." Install the driver on the terminal server. Obtain the print driver from the media that came with the printer or download it from the manufacturer's website. Once installed, delete the printer form the printer folder. Only the driver is necessary for remote printing.
Cannot switch between two printers connected to a PC locally when using local printing	Open the local printers folder, right click the printer you would like to set as the default, and choose Set As Default Printer. From the Thin page, refresh your browser by choosing View- Refresh (F5 may work, but not on all platforms). The printer port will be scanned, and the new default printer will be listed at the bottom of the browser. To change printers follow the same procedure. When printing from applications such as Notepad or Mail, you are offered the option to choose your printer. The default printer selected will also be the machine's default printer, but you will also see the prior default print queue(s). This may cause confusion especially when the printers are different languages and the wrong one is chosen. To help avoid confusion, before changing the default printer, logout, change the printer, and log in again.

Troubleshooting End User Remote Application Access

If end users are unable to access Thin applications, check the following:

- **Browser Check:** The NSP requires Netscape Version 6.0 or above, Internet Explorer 5.5 or above, or Mozilla 1.3 or above.
- **Proxy Server:** It is possible that some proxy servers will block your access to the Netilla Security Platform. Refer to "Troubleshooting Proxy Server and Other Connection Problems" for more information.
- **Browser Security Settings:** Your browser Security Settings must be set to Medium or Low. Setting your browser security settings to High will prevent the Java Applet and Netilla SSL adapter from executing. This is detailed in the section Verifying Browser Security Settings.

Troubleshooting the Applet Download

If end users are unable to launch applications, verify that the thin-client applet has been successfully downloaded. Instructions vary depending on the type of Web browser and Java Virtual Machine (JVM) you are using. Refer to the appropriate section.

- Troubleshooting the Applet Download using Internet Explorer & MS JVM
- Troubleshooting the Applet Download using Internet Explorer & SUN JVM

Troubleshooting the Applet Download using Internet Explorer & MS JVM

To verify a successful applet download using Internet Explorer and Microsoft's JVM, do the following.

1 Open your Web browser.

2 Choose *Tools*, and select *Internet Options*. The Internet Properties page opens.

3 Choose the *General Tab* and select *Settings*, as shown in Figure 258.

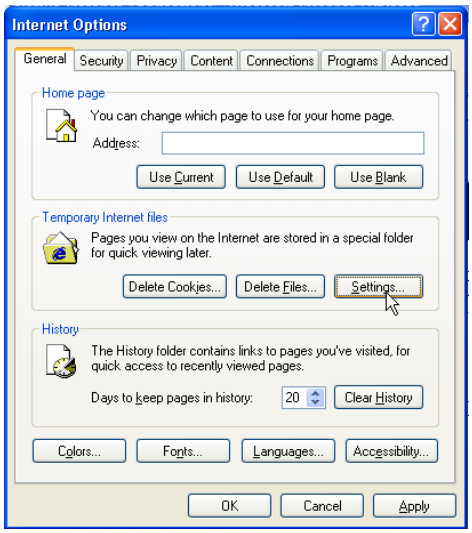


Figure 258 Internet Explorer Settings Location

The Settings page opens.

4 Choose *View Objects*, as shown in Figure 259.

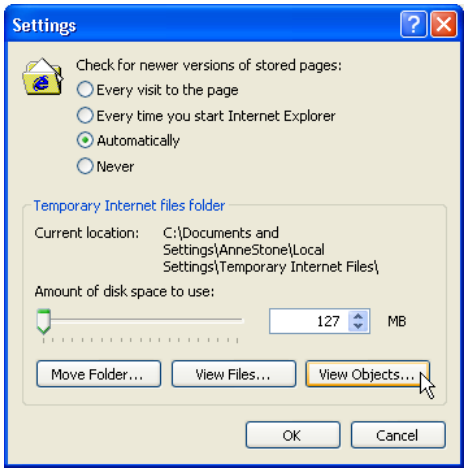


Figure 259 Internet Explorer Setting Page

The Downloaded Program Files page opens. There you should see the downloaded applet, as shown in Figure 260.

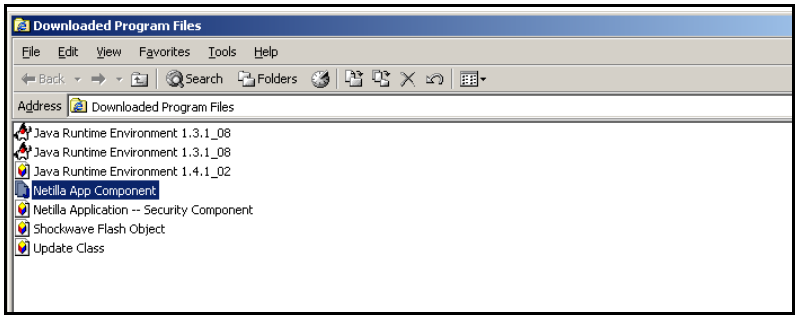


Figure 260 Internet Explorer Downloaded Program Files Page

You will likely see more than the Netilla applet if you have other files that have been downloaded from other web sites.

Troubleshooting the Applet Download using Internet Explorer & SUN JVM

To verify a successful applet download using Internet Explorer and Sun Microsystem's JVM, do the following.

1 From the MS Window's Start menu, select *Control Panel*.

2 Locate your Java plug in and double click it.

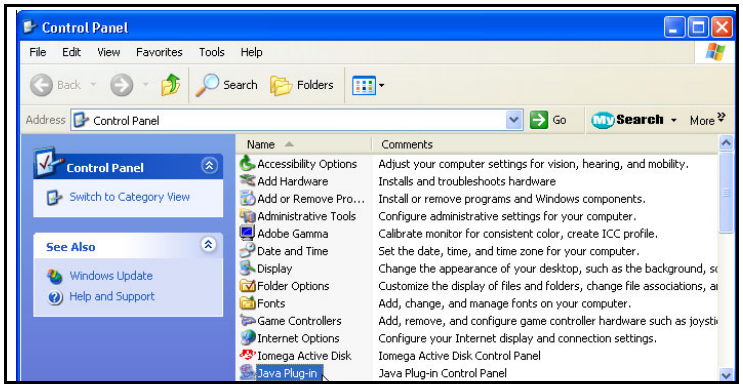


Figure 261 Java Plug In Location

The Java Plug-in Control Panel appears.

3 Click the Cache tab and then click View as shown in Figure 262.

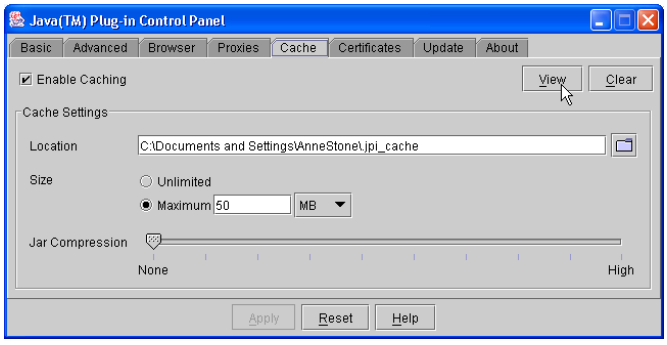


Figure 262 Java Plug-in Control Panel

4 Locate the Netilla applet as shown in Figure 263.

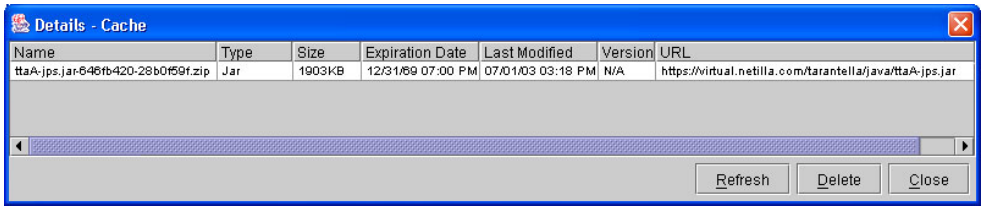


Figure 263 Netilla Applet Location

If the applet does not appear correctly, you can delete it from this page and re-download it. Alternatively, if the applet does not appear at all, it can also be re-downloaded.

Re-downloading the Java Applets

To re-download the applets, re-connect to the NSP, and then click the Thin icon to download the applets.

Troubleshooting Proxy Server and Other Connection Problems

If you receive proxy server errors or other connection difficulties when attempting to launch the Thin page, do the following.

To troubleshoot the procedure using Netscape, refer to "Troubleshooting Using Netscape".

Troubleshooting Proxy Server Problems with Internet Explorer and MS JVM

If you are using Internet Explorer with Microsoft's JVM, then instructions for troubleshooting proxy server and other connection problems are as follows.

1 With the browser open, select *Tools* and choose *Internet Options*, as shown in Figure 264.

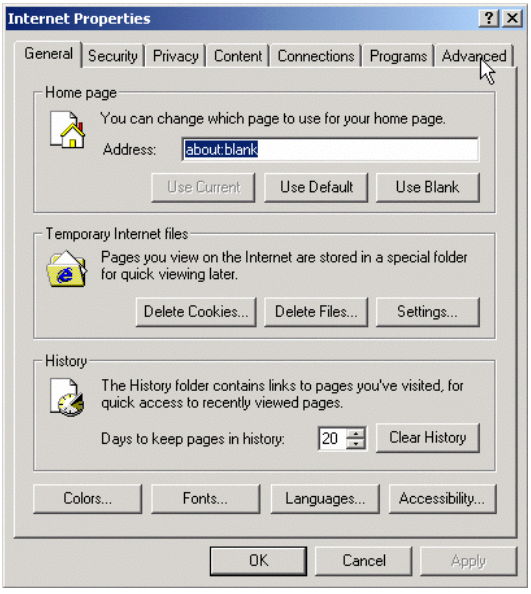


Figure 264 Internet Explorer Internet Properties Page

2 Select the *Advanced* tab.

3 Scroll to Microsoft VM, as shown in Figure 265.

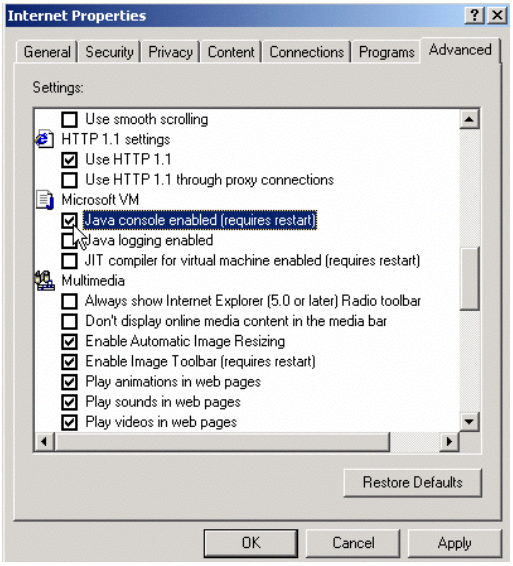


Figure 265 Internet Explorer Java Settings Page

4 Check the box marked Java Console Enabled (requires restart).

5 Click *OK*.

6 Exit the browser and then restart the browser.

7 Before connecting to the Netilla Security Platform site, choose *View*, and then choose *Java Console*, as shown in Figure 266.

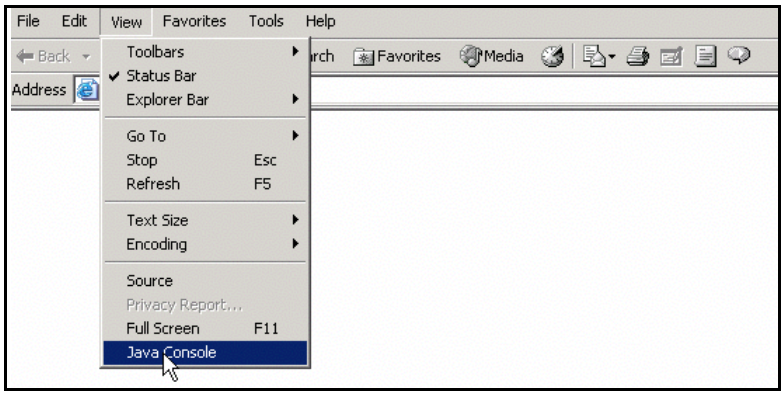


Figure 266 MS Java Console Location

8 The Java Console screen opens, as shown in Figure 267.

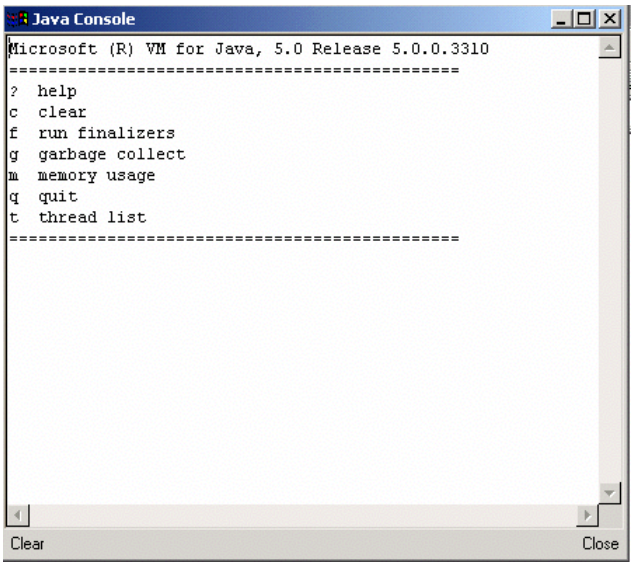


Figure 267 MS Java Console

9 Reconnect to the Netilla Security Platform site.

The Apps page attempts to connect, and messages appear on the console.

The Java Console may be hidden behind the browser.

A successful connection displays a screen similar to the one shown in Figure 268.

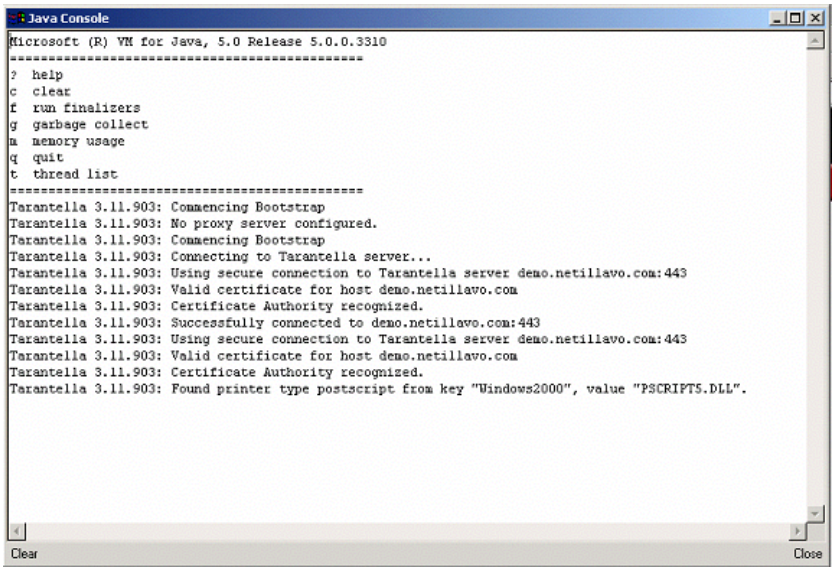


Figure 268 MS Java Console Showing Successful Connection to Remote Applications

Note that for this connection, no proxy was found, a secure connection was made, the certificate was verified, and the local printer driver was loaded.

Troubleshooting Proxy Server Problems with Internet Explorer and Sun JVM

If you are using Internet Explorer with Sun Microsystem's JVM, then instructions for troubleshooting proxy server and other connection problems are as follows.

1 With the browser open, select *Tools* and choose *Sun Java Console* as shown.

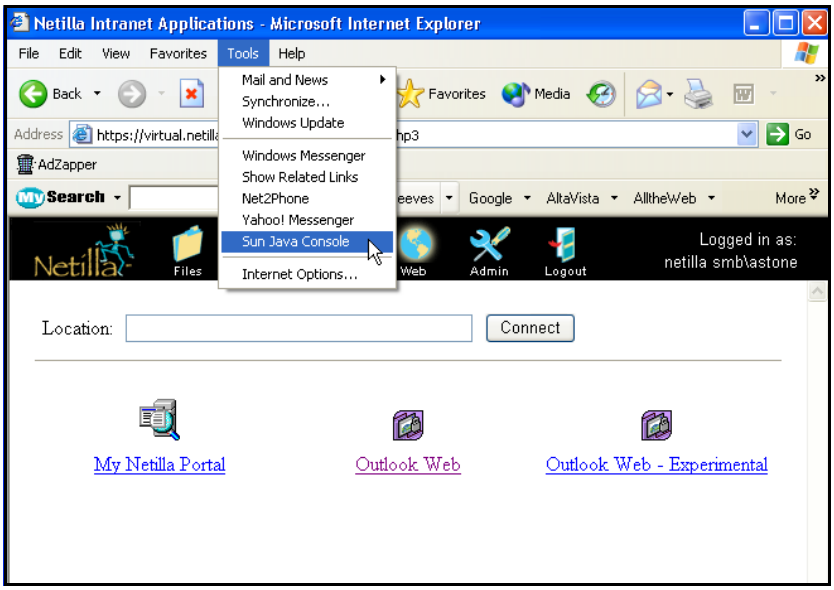


Figure 269 Internet Explorer Sun Java Console Location

The Java Console screen opens, as shown.

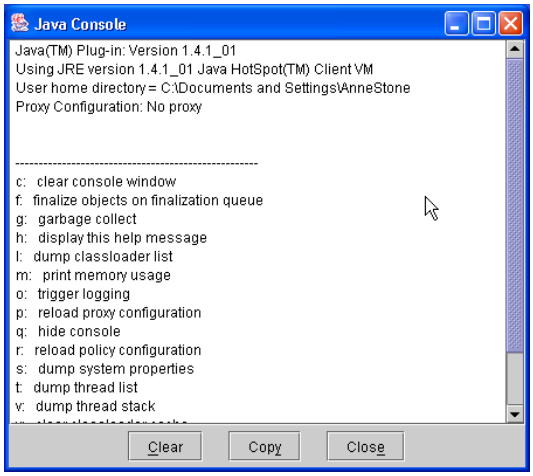


Figure 270 Sun Java Console

2 Reconnect to the NSP remote applications site by clicking the Thin icon.

The Thin page attempts to connect, and messages appear on the console.

The Java Console may be hidden behind the browser.

A successful connection displays a screen similar to the one shown in Figure 271.

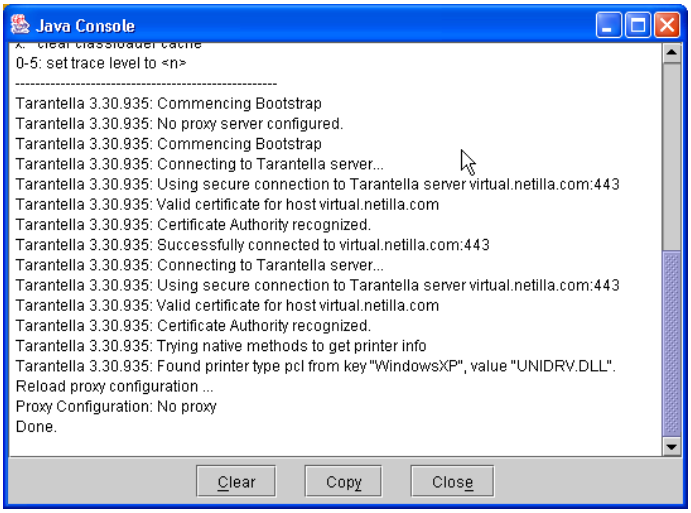


Figure 271 Sun Java Console Showing Successful Connection to Remote Applications

Getting Additional Help

If you are still unable to connect to the site, do following.

1. Highlight the messages in the console.
2. Press Ctrl-C to save the text to your computer's clipboard.
3. Open Notepad or Word, and select Edit and then choose Paste.
4. Save the file and email to support@netilla.com.
5. Alternatively, you can simply paste the contents of the Java Console directly into the body of an email message.

Verifying Browser Security Settings

To successfully download the applet that is necessary to access the Netilla Security Platform, your browser's security settings must be set to allow the download. This section describes how this is done.

1. With your Web browser open, select Tools and then choose Internet Options.
2. Choose the Security tab, as shown.

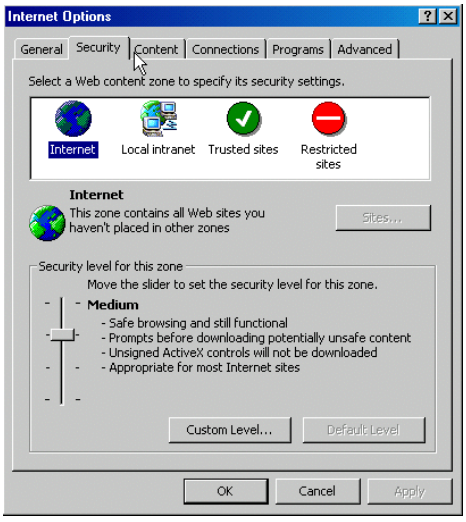


Figure 272 Web Browser Security Settings Page

3 Verify that your browser's Security Settings are set to either Medium or Low.

4 Click *Apply* and then click *OK*.

This completes the Browser Security Settings setup.

Troubleshooting the Applet Download Using Netscape

This section describes the procedure for troubleshooting connection problems when using Netscape.

Removing and reinstalling the Netilla Applets

1 From the MS Window's Start menu, select Control Panel.

2 Locate your Java plug in and double click it.

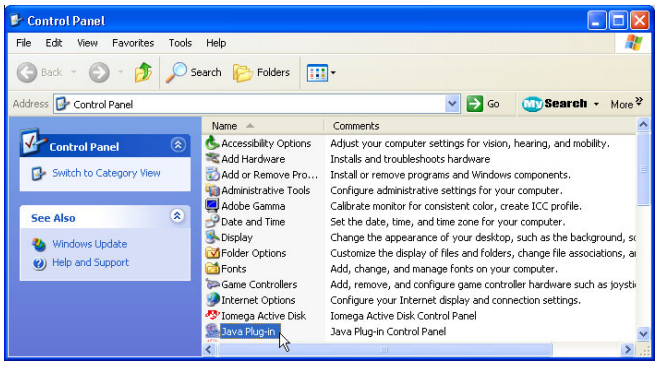


Figure 273 Java Plug In Location

The Java Plug-in Control Panel appears.

3 Click the Cache tab and then click View as shown in Figure 274.

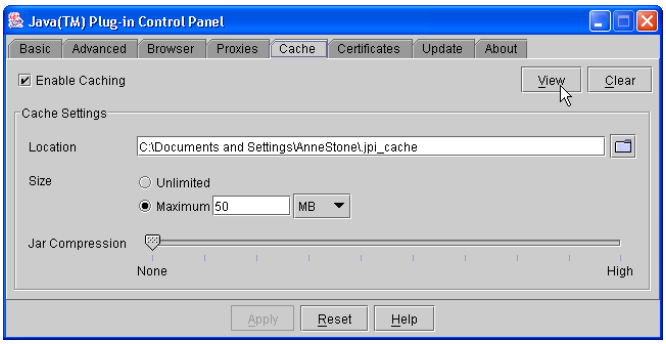


Figure 274 Java Plug-in Control Panel

4 Locate the Netilla applet as shown in Figure 275.

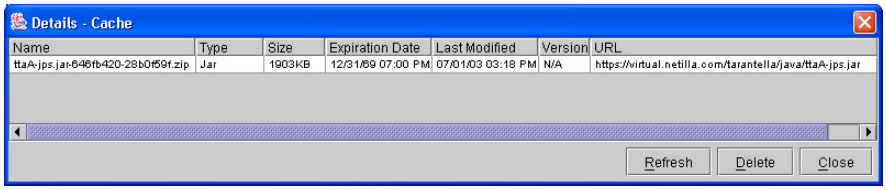


Figure 275 Netilla Applet Location

If the applet does not appear correctly, delete it from this page and re-download it. Alternatively, if the applet does not appear at all, it can also be re-downloaded.

5 Reconnect to the Netilla Security Platform URL to download the applet again.

6 Once logged in to the NSP, click the *Thin* icon.

7 After the applet downloads, try accessing an application.

8 If you are still having trouble, enable the Java Console and email the output to Netilla Networks as described in “Enabling the Java Console”.

Enabling the Java Console

1 From the Navigator menu, choose *Tools*, *Web Development* and then select *Java Console* as shown in Figure 276.

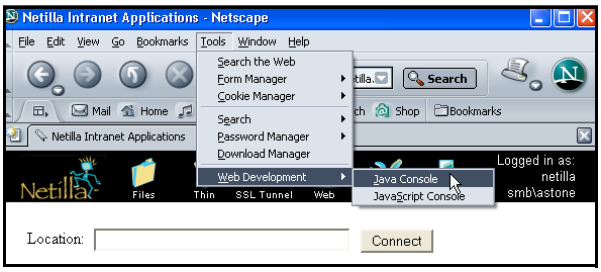


Figure 276 Netscape Java Console Location

The Java Console opens.

2 Click the *Thin* icon.

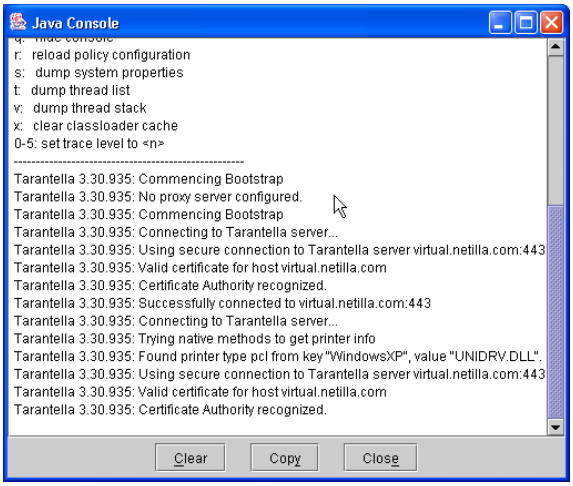


Figure 277 Java Console

3 Highlight the messages in the console.

4 Press Ctrl-C to save the text to your computer’s clipboard.

5 Open Notepad or Word, and select Edit and then choose Paste.

6 Save the file and email to support@netilla.com. Alternatively, you can simply paste the contents of the Java Console directly into the body of an email message.

Troubleshooting the Web Service

If you are having using the Web service, refer to the section which best describes the problem.

- Cannot Access Web Applications
- Web Applications Do Not Work

Cannot Access Web Applications

If you cannot access any of the Web-based applications, check the following.

1. **Check the DNS settings** on the NSP. If you are accessing internal web servers, ensure the name/URL will resolve correctly on the server(s) specified. Also, if you will be accessing external sites, ensure DNS forwarding is enabled on the internal DNS Server (if specified).
2. **Ensure the syntax of the URL is correct** in the URL fields. On the Policy Rules page, a protocol specification is required (http://, https://). On the General Properties page for the application, a protocol is already specified, so www.domain.com, or domain.com will suffice.
3. **Check port requirements.** Make sure the specified protocol is open from the NSP to the web server through additional firewalls, etc.

Web Applications Do Not Work

If a Web-based application has broken links and does not appear properly, check the following:

1. **Check Web Application Settings**. From the Administrator Site, navigate to the General Properties page for the Web application and then check the following settings.
   - **HTML Translation**: If this field is set to Fast, change it to *Full* and then save changes and try the Web application again.
   - **JavaScript Handling**: Set this field to *Translate* and then save changes and try the Web application again.
2. **Configure JARM.** Web applications may contain Java applets that require making another connection (UPD or TCP) beyond the NSP or they may contain signed applets that require re-signing. For configuration details, refer to “Java Applet Rewriting Module Configuration” on page 116.
3. **Download Policy Log File.** From the Administrator Site, select Netilla Monitoring and then select Reverse Proxy. Under the Reverse Proxy Policy section, click Download Policy Log File. Check the contents of the log file for any Deny statements that may be preventing access to a Web application. Correct Web application or network policies or add policies as needed.
4. **Avoid using cached settings**. When adding or removing policies, it is important to remember to close your browser(s) between tests. Cached settings in the browser may prevent the application from opening, even if the offending rules are corrected.
5. **Send Web Log File to Netilla**. If you are still having trouble, download the HTML translation log file as follows: From the Administrator Site, select Netilla Monitoring and then select Reverse Proxy. Under the Reverse Proxy Translation Engine section, click Download Translation Engine Log File. Email this log file to **support@netilla.com**.

Troubleshooting Web Application End User Access

If end users are having trouble accessing applications via the Web service, and you have verified that there are no conflicts as described in the previous section, then do the following.

1. Check the user's Web browser settings. For the Web service, the Web browser requirements are as follows:
   - Web browser (128-bit SSL recommended)
   - Microsoft Internet Explorer 6.0 and higher (any platform)
   - Netscape Navigator 6.0 and higher (any platform)
   - Mozilla 1.3 and higher (any platform)

Troubleshooting the Tunnel Service

If Tunnel applications do not work properly, check the following:

1. **Enable IP Forwarding**. IP forwarding must be enabled for Tunnel applications to work. Refer to Chapter 2 "Configuring IP Forwarding and NAT" on page 20.
2. **Check for IP address conflicts**. If you have a home network on 192.168.0.X or 192.168.1.X and your company uses the same IP address range, you may experience routing problems and be unable to communicate with the corporate network over the SSL VPN Tunnel. It is recommended that you change your home network to another IP segment such as 192.168.3.X. Refer to the instructions that came with your home router or cable modem for details.
3. **Check Policy Settings**. If you are still experiencing problems, temporarily disable policy settings as follows. From the Administrator Site, click *Services*, and then click *Tunnel*. For Restricted LAN Access, select *No* to disable policy settings and then click *Submit*. Log in the NSP and then click the *Tunnel* icon. Click *Connect* and then launch an application. If successful, then there is a policy configuration error. Review your application and network policy settings.
4. **Check the DNS settings** on the NSP. Perform a DNS lookup of the NSP and confirm that it is the external IP address of the NSP.

Troubleshooting Tunnel End User Access

If end users are having trouble accessing applications via the Tunnel service, and you have verified that there are no conflicts as described in the previous section, then do the following.

1. Check the user's Web browser settings. For the Tunnel service, the Web browser requirements are as follows:
   - Microsoft Internet Explorer 6.0 and higher; Windows 2000 and XP clients
   - 128-bit SSL recommended
   - ActiveX-enabled
2. If the Web browser settings are correct, uninstall and then reinstall the VPN adapter on the client's computer as described in "Uninstalling the Tunnel Adapter".

Uninstalling the Tunnel Adapter

To uninstall the Tunnel adapter, do the following.

1. Close the Web browser you were using to access the Tunnel service.
2. From the Windows Start menu, select *Control Panel*.

3 From Control Panel, select *Add or Remove Programs*.

4 Locate and then select the *Netilla Tunnel Client*.

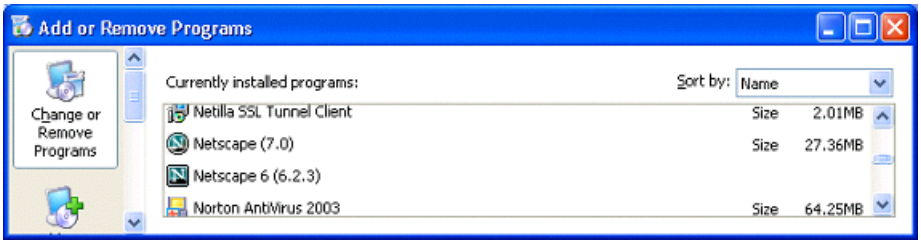


Figure 278 Add/Remove Programs Window

5 Click *Change/Remove*. You will a confirmation message.

6 Click Yes.

7 Go to *Start My Computer* and then double click Local Disc (C:)

8 Locate and then double click the *Program Files* folder.

9 Select the *Netilla VPN f*older and then select *Delete this folder* as shown in Figure 279.

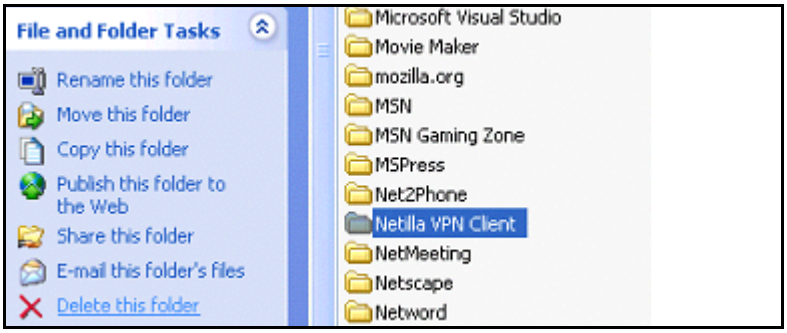


Figure 279 Add/Remove Netilla Tunnel Window

Reinstalling the Tunnel Adapter

To reinstall the Tunnel adapter, do the following.

1 Launch your Web browser and then connect to the NSP.

2 Select the *Tunnel* icon.

3 Click *Connect*.

4 Click *Yes*. Another message appears asking for confirmation.

5 Click *Yes*.

An installation progress bar appears.

A page appears indicating that you have established an Tunnel and are now ready to work with you locally applications in sync with your remote applications.

Troubleshooting Certificate Errors

This section describes how to troubleshoot server certificate errors and client certificate errors. Refer to the desired section.

Troubleshooting Server Certificate Errors

If you receive an error message, it is possible that the server certificate you are installing is either not valid or it does not belong to your particular NSP. To troubleshoot errors, do the following.

1. Ensure that you have copied the full content of the certificate prior to pasting it into the certificate content window.
2. Ensure that the certificate belongs to the NSP (i.e., the CSR that you used to obtain the certificate must have been generated from that NSP).
3. Ensure that a subsequent request for a CSR has not been made after submitting the original CSR request to the CA. Subsequent requests invalidate the certificate.
4. If a chain has been used to sign your server certificate, then the Root CAs must be added in a specific order. Root CAs are added from the highest level down to the actual CA that signed the certificate. The server certificate is then added after the ROOTs.For example, if you have part of a certificate signing chain, you would install the certificates in the following order:
   - •Top Level ROOT CA
   - •Intermediate ROOT CA or Chain
   - •Server certificate

   If more than one Intermediate CA has been used, the Intermediate that signed the certificate must be the **last** one installed before installing the server certificate.

Troubleshooting Client Side Certificate Errors

While configuring client side certificates you may inadvertently lock yourself out the NSP. This occurs when the browser is closed or the administrator logs out of the Netilla configuration site before verifying that client verification via certificate is working properly. If you make an error and close the browser before testing, you could lock yourself out of the NSP.

If this happens you must first gain console access to the NSP. For details, refer to Chapter “Accessing the NSP’s Serial Console” on page 261.

Once you gain console access, restore client verification to the default setting to regain access to your NSP as follows.

1. From the NSP serial console main menu, select *Reset Settings*.
2. Select *Client Verification*.
3. Select *Save* and then *Exit*.

Troubleshooting End User Access

This section presents tips and step-by-step procedures to overcome problems end users may experience when connecting to the NSP.

The following topics are discussed.

- Prerequisites
- Troubleshooting the Connection for End Users
- Web Browser Requirements for End Users

Prerequisites

Before users can successfully log in to the NSP and begin to access services, the following steps must be completed.

- ❑ **Netilla Licenses**: Ensure that you have not reached the concurrent users limit. When the maximum number of concurrent sessions has been reached, all subsequent attempts to log in to the NSP are denied.

  Note also that end users cannot log in to the NSP until the default licenses have been activated. Refer to “Installing Licenses” on page 24 for more information.
- ❑ **Browser Check: Web** browser requirements vary depending on the types of NSP services. Refer to for details
- ❑ **Firewall Ports**: If accessing the NSP from behind a firewall, users must open port 80 (HTTP) and port 443 (SSL) on the firewall to allow traffic in both directions.
- ❑ **Proxy Server**: It is possible that some proxy servers affect a user’s ability to access the platform. Refer to “Troubleshooting Proxy Server Problems with Internet Explorer and MS JVM” on page 237 or “Troubleshooting Proxy Server Problems with Internet Explorer and Sun JVM” on page 240.
- ❑ **Browser Security Settings**: Browser Security Settings must be set to *Medium* or *Low*. Setting browser security settings to *High* will prevent the Java Applets from executing. This is detailed in the section “Verifying Browser Security Settings” on page 241.
- ❑ **Connection Speed**: Connection speed should be at least 28.8 Kbps to demonstrate acceptable performance.

Troubleshooting the Connection for End Users

If end users are not able to see the login page for your site, they should try the following:

1. Check the spelling of the URL entered. Did they enter **https://** instead of **http://**?
2. Try connecting to the Netilla Demo site. http://demo.netillavo.com. Are end users able to see the login screen? If not, verify the Internet configuration. If end users are able to access the Netilla Demo site but not your own site, and have verified the URL, notify your network administrator.
3. If you are able to connect but are unable to see or launch applications, proceed to “Web Browser Requirements for End Users”.

Web Browser Requirements for End Users

Web browser requirements vary depending on the type of application end users are trying to access. Refer to Table 36 for a list of the Web browser requirements per application type.

Table 36 Web Browser Requirements

Application Type	Web Browser Requirements
Thin Applications 	■ Web browser (128-bit SSL recommended) with Java Virtual Machine ▪ Microsoft Internet Explorer 6.0 and higher for Windows ▪ *Sun JVM 1.4 or higher or MS JVM 5.0.0.3805 or higher* ▪ Netscape Navigator 6.0 and higher (Win32 and Linux clients) ▪ *Sun JVM 1.4 or higher* ▪ Mozilla 1.3 and higher (Win32 and Linux clients) ▪ *Sun JVM 1.4 or higher* ▪ Configure Web browser to support Secure Socket Layer (SSL) version 3.0 or higher or Transport Layer Security (TLS) 1.0 ▪ Configure Web browser to allow plug-ins or Java access
Web-based Applications 	■ Web Browser (128-bit SSL recommended) ▪ Microsoft Internet Explorer 6.0 and higher (Win32 only) ▪ Netscape Navigator 6.0 and higher (Win32 and Linux clients) ▪ Mozilla 1.3 and higher (Win32 and Linux clients) ▪ Configure Web browser to support Secure Socket Layer (SSL) version 3.0 or higher or Transport Layer Security (TLS) 1.0 ▪ Configure Web browser to allow plug-ins or Java access
Tunnel Applications 	■ Web browser (128-bit SSL recommended) ▪ Microsoft Internet Explorer 6.0 and higher (Windows 2000 and XP clients) ▪ ActiveX-enabled to allow Netilla Virtual Adapter to download ▪ Configure Web browser to support Secure Socket Layer (SSL) version 3.0 or higher or Transport Layer Security (TLS) 1.0 ▪ Configure Web browser to allow plug-ins or Java access
Files Service 	■ Microsoft Internet Explorer 6.0 and higher with MS JVM 5.0.0.3805 or higher (Win32 only)

To check the settings listed in Table 36, refer to the appropriate section based on the type of Web browser.

- Verifying Internet Explorer Browser Settings
- Verifying Netscape Navigator Browser Settings
- Verifying Mozilla Browser Settings

Verifying Internet Explorer Browser Settings

To verify your Microsoft Internet Explorer browser version and other settings, do the following.

1. Open your Internet Explorer browser.
2. From the Help menu, click *About Internet Explorer.*

   The version is listed in the first line.

3 Make sure the version number is 6.0 or higher.

If you have a version number prior to 6.0, go to http://www.windowsupdate.com to get version 6.0 or later.

4 From Tools menu, select *Internet Options*. The Internet Options window appears.

5 Select the *Advanced* tab and then scroll down to the Security section.

6 Make sure that Use SSL version 3.0 is checked.

7 Click *OK* and then click the *Security* tab.

8 Click *Custom Level*. The Security Settings windows appears.

9 Click *Default Level* to restore the security settings to the default values.

10 Click *OK* and then click *OK* again to exit Internet Options.

Verifying Netscape Navigator Browser Settings

To verify the browser settings for Netscape Navigator, do the following.

1 Open your Netscape Navigator browser.

2 From the Help menu, click *About Netscape*. A page appears showing the version number.

If you have a version number prior to 6.0, go to http://www.netscape.com/computing/download to get version 6.0 or later.

3 From the Edit menu, select *Preferences*.

4 Click *Privacy and Security* and then click *SSL*.

5 Under SSL Protocol Versions, make sure Enable SSL version 3 is checked.

6 Click *OK*.

Verifying Mozilla Browser Settings

To verify the browser settings for Mozilla, do the following.

1 Open your Mozilla browser.

2 From the Help menu, click *About Mozilla*. A page similar to the following appears showing the version number.

3 From the Edit menu, select *Preferences*.

4 Click *Privacy and Security* and then click *SSL*.

5 Under SSL Protocol Versions, make sure *Enable SSL version 3* is checked.

6 Click *OK*.

Troubleshooting the HotStandby System

This section provides troubleshooting information for the optional HotStandby system which provides redundancy should an NSP experience a failure. The following information is provided.

- Troubleshooting via E-mail Alerts
- Troubleshooting via GUI Messages

Troubleshooting via E-mail Alerts

Each time a change occurs that affects the Hot Standby system, an e-mail alert is generated to the e-mail address you specified. This section lists some of the emails that you may receive that indicate a failure and require troubleshooting.

For a list of informational email messages related to HotStandby, refer to “Email Alerts” on page 223.

Message Subject	Message Body	Description
[FAILOVER] Start Failover failed on the backup	Start Failover failed: Replication::Installer::BREPException : tlsv1 alert **unknown ca**	Indicates there’s a certificate error. Repeat the certificate replication process and then start failover again. For details, begin with “Configuring the Master NSP” on page 143.

Troubleshooting via GUI Messages

The Status field of the Failover Configuration page provides descriptions of errors as they occur. This section provides descriptions of some of those errors including the following:

- Remote Power Switch Error Message
- IP Address Configuration Error

Remote Power Switch Error Message

Should the Remote Power Switch not respond, a message appears in the Errors field of the Failover Settings window, as shown in Figure 280.

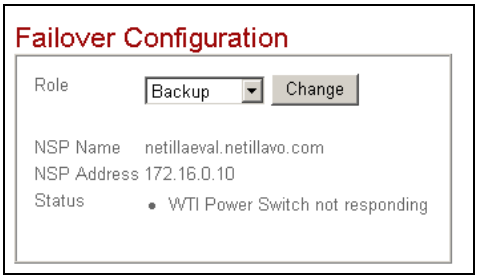


Figure 280 Remote Power Switch Error Message

This message displays if the switch becomes damaged, is malfunctioning or if it is not plugged in to the Backup NSP. Make sure the remote power switch is plugged in to the Backup NSP. If it is, check the switches located on the back of the NSP and labeled Setup to make sure that they are set correctly as described in “Installing the Remote Power Switch (RPS10)” on page 208.

IP Address Configuration Error

If the Start Failover button does not appear in the Failover Configuration page, refer to the Status field for a description of the problem. One example shown in Figure 281 indicates that the physical IP address of the Master was configured in the NSP Settings page instead of the virtual IP address.

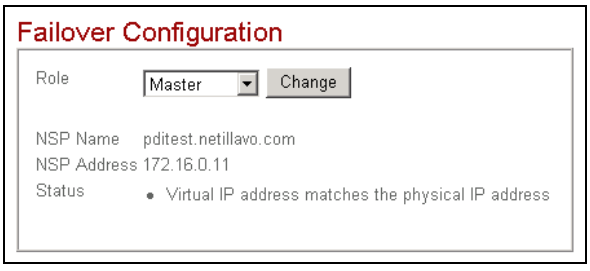


Figure 281 IP Address Configuration Error Message

B Appendix B: Netilla Port Requirements

This section presents common implementations of the Netilla Security Platform (NSP) and describes the various service NSP ports that must be open to allow traffic between the NSP, application hosts, and authenticating sources.

For a complete list of common ports and their usage, please see "The Netilla Firewall" section of the NSP Administration Manual.

The following topics are discussed.

- Background
- Public Interface Port Requirements
- Private Interface Port Requirements
- Common Architecture Port Requirement Scenarios

Background

If the NSP is deployed behind a firewall that sits between the NSP and an external server (either an application or authentication server), specific ports on the firewall must be open to allow successful communication between the devices.

Note, however, that if the NSP is deployed behind an existing firewall, it is possible to limit the open ports to the platform to 443 only, allowing all traffic to the platform over SSL.

Alternatively, Netilla administrators have the option to close Ports 80 (http), and 443(SSL) ports the NSP on *eth1* connection.

Port 22 (SSH) access to the NSP may occasionally be required, as stated in the "Remote Access Addendum". However, it is recommended that Port 22 be opened only when specifically requested by a Netilla Certified Engineer.

Public Interface Port Requirements

This section describes the public interface port requirements for accessing back resources.

- Port 443(SSL) inbound to the NSP
- (Optional) Port 80 (HTTP) inbound to the NSP if you want automatic redirection from HTTP to HTTPS. Note that opening this port only allows the redirection and does not expose resources.

Private Interface Port Requirements

This section describes the private interface port requirements for accessing internal servers that do not need to be exposed to the public Internet.

Authentication Port Requirements

This section describes the required ports that must be open for each authentication protocol.

SMB

- Port 139/TCP (NetBIOS) outbound from the NSP if the authentication server is running Microsoft NT 4.0.
- Port 445/TCP (NetBIOS) outbound from the NSP if connecting to a Windows 2000/2003 server.

RADIUS

- Port 1812/UDP (RADIUS) or 1645/UDP (RADIUS) outbound from the NSP (by default; may vary by location).

SecurID

- Port 5500/UDP (SecurID) and/or 5510/TCP (securidprop) outbound from the NSP (by default; may vary by location).

Kerberos

- UDP port 88 outbound from the NSP. The Kerberos port number is configuration via the NSP. For details, refer to “Creating a Kerberos Authentication Stage” on page 53.

Internal

- There are no port requirements for internal authentication.

Thin Service Port Requirements

This section describes the required ports that must be open for the various Thin service applications.

Microsoft Windows applications

- Port 3389/TCP (RDP) outbound to the Windows 2000/2003 server.
- (Optional) Port 139 inbound if you want to use client drive mapping.

X Windows applications

- Inbound TCP on all ports in the 6000-7000 range.
- Outbound port numbers per application type are as follows:
  - Telnet: Port 23/TCP outbound to the X Host.
  - SSH: Port 22/TCP outbound to the X Host.
  - Rexec: Port 512/TCP outbound to the X Host.
  - Rcmd: Port numbers vary (544 TCP).
  - Rlogin: Port numbers vary (221/541 TCP).

3270 applications

- Port 23/TCP (telnet) outbound to the mainframe (by default; may vary by location).

Character-Based UNIX applications via:

- Telnet: Port 23 (default) TCP (telnet) outbound to the UNIX Host.
- SSH: Port 22 (default) TCP (SSH) outbound to the UNIX Host.
- Rlogin: Port numbers vary; 221 or 541 TCP (by default; may vary by location).

Files Service Port Requirements

This section describes the required ports that must be open for the Files service.

- Port 139 (NetBIOS) inbound and outbound
- Port 137 UDP (WINS) outbound

Web Service Port Requirements

This section describes the required ports that must be open for the Web service.

- Port 80 outbound
- Port 443 outbound (by default; may vary by location)

Tunnel Service Port Requirements

The ports required for the Tunnel service are dictated by the Tunnel rules that are created. For each Tunnel rule that you create, the corresponding firewall ports must be open.

Common Architecture Port Requirement Scenarios

Netilla on the LAN behind an existing firewall

The following illustration describes the common layout when the NSP is deployed behind an existing firewall.

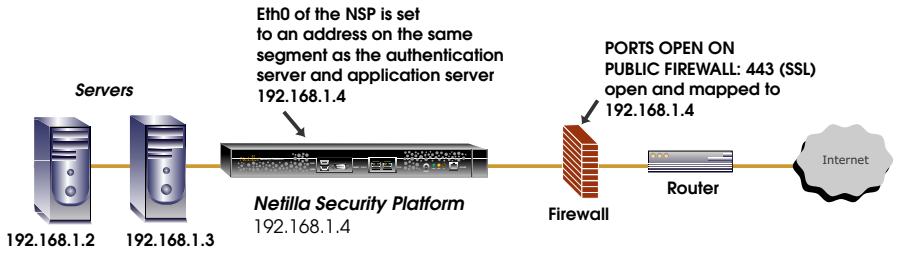


Figure 282 NSP Deployed Behind a Firewall

Requirements

- At a minimum, this type of deployment requires Port 443 (SSL) to be open on the firewall to the NSP.

Optional

- Port 80 (http) for the redirect to port 443 (SSL).

The NSP Deployed in a DMZ

The following illustration describes the port requirements when deploying the NSP in a DMZ.

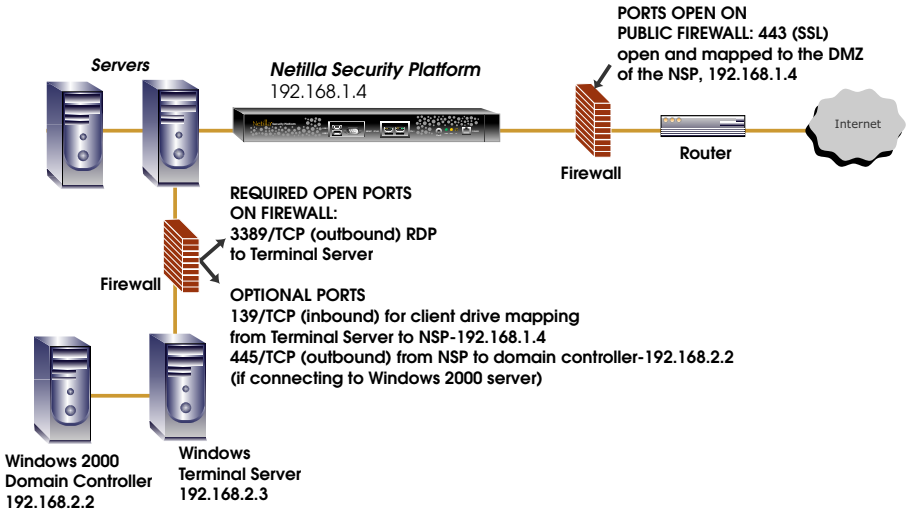


Figure 283 The NSP Deployed in a DMZ

Requires

- Port 443 (SSL) open on the firewall to the NSP at a minimum.
- Port 3389 (RDP) outbound to the 2000 Application Server.

Optional

- Port 80 (http) inbound for the redirect to port 443 (SSL).
- Port 139/TCP (NetBIOS) inbound for client drive mapping.
- Port 139/TCP (NetBIOS) outbound for SMB authentication to an external source.
- Port 445/TCP (NetBIOS) outbound for NT group membership information (for assignment of applications via group membership).
- Port 137 UDP (WINS) outbound for computers to be available under Network Neighborhood section of Files.
- Port 514/UDP outbound for syslog.
- Port 161 (UDP/TCP) inbound for SNMP messages.
- Port 162 (UDP/TCP) outbound for SNMP traps.

C

Appendix C: APL Key List for 3270 Applications

For reference, the complete list of special APL keys is shown in Table 37. Entries marked with an asterisk (*) represent simple aliases for standard EBCDIC characters. Entries marked with an (S) represent Sharp APL characters.

Table 37 APL Key List for 3270 Applications

APL Symbol	Hex	x3270 Keysym	X3270 Key	X3270 Composed Keys
A underbar	41	apl_Aunderbar	Alt-A	A + underbar
alpha	B0	apl_alpha	Alt-a	
B underbar	42	apl_Bunderbar	Alt-B	B + underbar
bar	60*	apl_bar	-	
brace left	C0	apl_braceleft	Alt-{	
brace right	D0	apl_braceright	Alt-}	
C underbar	43	apl_Cunderbar	Alt-C	C + underbar
circle	9D	apl_circle	Alt-o	
circle bar	ED	apl_circlebar		circle + bar
circle slope	CF	apl_circleslope		circle + slope
circle star	FD	apl_circlestar		circle + star
circle stile	CD	apl_circlestile		circle + stile
colon	7A*	apl_colon	:	
comma	6B*	apl_comma	,	
comma bar (S)	E5	apl_commabar		comma + bar
D underbar	44	apl_Dunderbar	Alt-D	D + underbar
del	BA	apl_del	Alt-g	
del stile	DC	apl_delstile		del + stile
del tilde	FB	apl_deltilde		del + tilde
delta	BB	apl_delta	Alt-h	
delta stile	DD	apl_deltastile		delta + stile
delta underbar	FC	apl_deltaunderbar		delta + underbar

diamond	70	apl_diamond		up caret + down caret
dieresis	72	apl_dieresis	Alt-1	
dieresis circle (S)	E5	apl_dieresiscircle		dieresis + circle
dieresis dot	EC	apl_dieresisdot		dieresis + dot
dieresis jot (S)	E4	apl_dieresisjot		dieresis + jot
divide	B8	apl_divide	Alt-+	
dot	4B*	apl_dot	.	
down arrow	8B	apl_downarrow	Alt-u	
down caret	78	apl_downcaret	Alt-9	
down caret tilde	CB	apl_downcarettilde		down caret + tilde
down shoe	AB	apl_downshoe	Alt-v	
down stile	8E	apl_downstile	Alt-d	
down tack	AC	apl_downtack	Alt-b	
down tack jot	FE	apl_downtackjot		down tack + jot
down tack up tack	DA	apl_downtackuptack		down tack + up tack
E underbar	45	apl_Eunderbar	Alt-E	E + underbar
epsilon	B1	apl_epsilon	Alt-e	
epsilon underbar	75	apl_epsilonunderbar		epsilon + underbar
equal	7E*	apl_equal	"="	
equal underbar	E1	apl_equalunderbar		equal + underbar
euro (S)	E7	apl_euro		C + =
F underbar	46	apl_Funderbar	Alt-F	F + underbar
G underbar	47	apl_Gunderbar	Alt-G	G + underbar
greater	6E*	apl_greater	>	
H underbar	48	apl_Hunderbar	Alt-H	H + underbar
I underbar	49	apl_Iunderbar	Alt-I	I + underbar
iota	B2	apl_iota	Alt-i	
iota underbar	74	apl_iotaunderbar		iota + underbar
J underbar	51	apl_Junderbar	Alt-J	J + underbar
jot	AF	apl_jot	alt-j	
K underbar	52	apl_Kunderbar	Alt-K	K + underbar

L underbar	53	apl_Lunderbar	Alt-L	L + underbar
left arrow	9F	apl_leftarrow	Alt-[	
left bracket	AD	apl_leftbracket	[	
left paren	4D *	apl_leftparen	(	
left shoe	9B	apl_leftshoe	Alt-z	
less	4C *	apl_less	<	
M underbar	54	apl_Munderbar	Alt-M	M + underbar
N underbar	55	apl_Nunderbar	Alt-N	N + underbar
not equal	BE	apl_notequal	Alt-8	equal + slash
not greater	8C	apl_notgreater	Alt-4	less + equal
not less	AE	apl_notless	Alt-6	greater + equal
O underbar	56	apl_Ounderbar	Alt-O	O + underbar
omega	B4	apl_omega	Alt-w	
overbar	A0	apl_overbar	Alt-2	
P underbar	57	apl_Punderbar	Alt-P	P + underbar
plus	4E*	apl_plus	+	
Q underbar	58	apl_Qunderbar	Alt-Q	Q + underbar
quad	90	apl_quad	Alt-l	
quad divide	EE	apl_quaddivide		quad + divide
quad jot	73	apl_quadjot		quad + jot
quad quote	DE	apl_quadquote		quad + quote
quad slope	CE	apl_quadslope		quad + slope
query	6F*	apl_query	?	
quote	7D *	apl_quote	'	
quote dot	DB	apl_quotedot		quote + dot
R underbar	59	apl_Runderbar	Alt-R	R + underbar
rho	B3	apl_rho	Alt-r	
right arrow	8F	apl_rightarrow	Alt-]	
right bracket	BD	apl_rightbracket	]	
right paren	5D *	apl_rightparen	)	
right shoe	9A	apl_rightshoe	Alt-x	
S underbar	62	apl_Sunderbar	Alt-S	S + underbar

semicolon	5E*	apl_semicolon	;	
slash	61*	apl_slash	/	
slash bar	EA	apl_slashbar		slash + bar
slope	B7	apl_slope	Alt-\	
slope bar	EB	apl_slopebar		slope + bar
squad	CC	apl_squad		quad + quad
star	5C *	apl_star	*	
stile	BF	apl_stile	Alt-|	
T underbar	63	apl_Tunderbar	Alt-T	T + underbar
tilde	80	apl_tilde	Alt-~	
times	B6	apl_times	Alt-=	
U underbar	64	apl_Uunderbar	Alt-U	U + underbar
underbar	6D *	apl_underbar	"_"	
up arrow	8A	apl_uparrow	Alt-y	
up caret	71	apl_upcaret	Alt-0	
up caret tilde	CA	apl_upcarettilde		up caret + tilde
up shoe	AA	apl_upshoe	Alt-c	
up shoe jot	DF	apl_upshoejot		up shoe + jot
up stile	8D	apl_upstile	Alt-s	
up tack	BC	apl_uptack	Alt-n	
up tack jot	EF	apl_uptackjot		up tack + jot
V underbar	65	apl_Vunderbar	Alt-V	V + underbar
W underbar	66	apl_Wunderbar	Alt-W	W + underbar
X underbar	67	apl_Xunderbar	Alt-X	X + underbar
Y underbar	68	apl_Yunderbar	Alt-Y	Y + underbar
Z underbar	69	apl_Zunderbar	Alt-Z	Z + underbar

D Appendix D: Using the Netilla Serial Console

This section describes how to connect to the NSP serial port and how to change settings. Note that these settings were configured as part of the initial installation. This section is provided should changes become necessary.

You will need the following:

- ❑Terminal emulation software, such as HyperTerminal.
- ❑A 9-pin DB9 null modem cable. (This cable is included in your NSP package.)

Accessing the NSP's Serial Console

To access the NSP's serial console, do the following.

1. Connect one end of a 9-pin DB9 null modem cable to the serial port of a computer running Windows® 95, 98, 2000 or XP, or Linux®.
2. Connect the other end to the serial port labeled *Mgmt* located on the front of the NSP as shown in Figure 284.

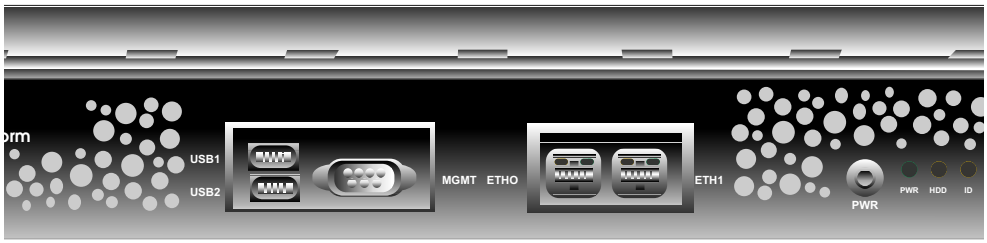


Figure 284 NSP Front Panel

3. From the computer that you are using to configure the NSP, use terminal emulation software or a utility such as HyperTerminal to connect to the NSP using an available Com port. Connection settings would be as follows:
   - Bits per second: 115200
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow Control: Hardware
4. Enter *sadmin* at the log in prompt and press *Enter*.

   You are prompted for your password.
5. Enter your password for accessing the serial console and press *Enter*.

Your serial console password is different than your password for accessing the NSP Administrator Site.

6 After logging in, you are presented with the Terminal Emulation menu, shown in Figure 285.

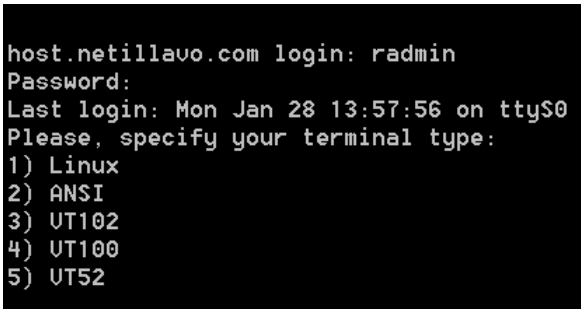


Figure 285 Terminal Emulation Window

7 Choose *ANSI* by typing 2 and then *Enter*.

Use the Tab key to move between fields.

You are connected to the NSP, and the configuration menu is displayed as shown in Figure 286.

Figure 286 NSP Serial Console Configuration Main Window

The following options are provided.

Network Settings

Network Settings allows you to change your TCP/IP configuration as shown in Figure 287.

Set Date & Time

Use this area to set the time/timezone and date. Entering this information correctly helps avoid digital certificate errors.

Change Password

Use this option to change the password for accessing the serial console menu. Note that this password is only for accessing the NSP's serial console menu and is independent of the administrator passwords that are used to access the NSP's Administrator Site.

SSH Configuration

By default, SSH is disabled on the NSP. Leave this field at its default setting unless instructed otherwise by Netilla Support personnel.

Reset Settings

Use this option to reset the following:

Client Verification: Resets client verification to its default state should you become locked out due to a misconfiguration.

Local Authentication Realm: Reverts the local realm to internal authentication only should you become locked out of the NSP because of a misconfiguration of an additional authentication stage. By selecting this option, you will be able to log in to the NSP with your current user name and password.

Shutdown Box

This option allows you to power down your NSP.

Reboot Box

This option allows you to reboot your NSP.

Changing Network Settings

To change network settings, do the following.

1 Select *Network Settings*.

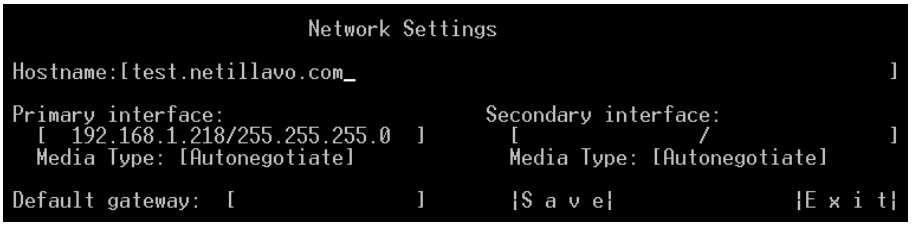


Figure 287 Network Settings Window

2 Type in the IP address of your Primary interface and Default gateway. If necessary, you can configure a Secondary interface.

Note that primary and secondary interfaces cannot be on the same network.

3 If necessary, change the Media Type.

The Media Type field provides the ability to configure the Ethernet link speed manually. By default, the Media Type field is set to "Autonegotiate" but if your device requires a specific link speed you can set it to one of the following:

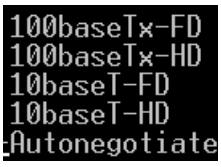


Figure 288 Media Type Choices

FD refers to Full Duplex; HD refers to Half Duplex.

4 Select *Save*.

5 Select *Exit*.

Changing Date and Time Settings

To change the date and time, do the following.

1. From the main menu, select *Set Date and Time*.
2. Enter the current date, time and time zone.
3. Select *Save*.
4. Select *Exit*.

Appendix E: NSP Features & Hardware Specifications

NSP Feature List

The NSP provides the following features.

Application Access Features

Thin Applications

- Windows 2000/2003 Terminal Services-compliant applications (RDP)
- UNIX/Linux X Windows and Character-based Applications (telnet, ssh, rexec, rcmd, or rlogin)
- Mainframe 3270
- AS/400 (5250 via key map overlay emulation over 3270)
- Java-based, integrated thin-client application protocol
- Proprietary data compression ensures optimal performance over any Internet connection, including dial-up
- Application Layer Proxy: Termination, policy and translation in the DMZ
- Single applications portal consolidates access into a single secure gateway, simplifying management

Web Features

- Browser-based, Internet access to intranet Web resources
- Application Layer Proxy: Termination, policy and translation in the DMZ
- Gateway portal protection hides network topology from unauthorized viewing
- Granular access controls to directories, servers, and paths
- Web-object filtering blocks unwanted Web components (JavaScript, cookies)

Tunneling Features

- Windows 2000 and Windows XP client/server applications
- UDP and TCP application support
- Dynamic session-based firewall controls egress application port availability on a session-by-session basis
- Netilla Virtual Adapter: Downloads automatically upon initial request

NSP Functionality

Email

- Securely access Outlook Web client or Web-based e-mail
- Real-time e-mail access (ability to synchronize via Tunnel)
- Client Drive Mapping: Save attachments to local drives

Printing

- Universal printing via PDF
- Utilizes Microsoft Windows 2000 printing platform
- Redirection of print output to local or network printers
- Session printer management

Performance

- Dynamic bandwidth optimization for remote access to client/server applications (with Remote applications)
- Application server load balancing (optional)
- Fail-over/redundant platform architecture (Netilla Hot Standby)

Netilla File Sharing

- Microsoft Windows SMB-compatible
- Manage files from server-based folders
- Transfer to and from local drive and remote server
- Files interface allows Web-based files and folders manipulation

Authentication Protocols:

- Internal (Shadow)
- RADIUS®
- Microsoft Windows® NT/2000 Active Directory
- Microsoft SMB
- Kerberos Version 5
- RSA SecurID® Ready
- RSA Ace 5 Server Ready
- VASCO Ready Partner
- Aladdin eToken™ Enabled Partner
- X.509 digital certificate support

Operating Architecture

- Hardened dynaTRUST O/S (Netilla's proprietary OS that is optimized for policy enforcement and API integration)
- Hardened Apache® Web-server

NSP Security

Encryption and PKI

- 128-bit secure socket layer (SSL)
- Support for standard X.509 server digital certificates, such as from Thawte/Verisign®
- Client-side certificate support
- Encryption-level browser control
- Secure HTTP (HTTPS) over Port 443
- SSL Security Confirmation

Secure Architecture

- Application-Layer Proxy: Security at the network edge
- Dual-interface firewall protects hacking from outside or inside the enterprise
- Granular control through dynamic policy-based authentication and authorization framework with multiple user-verification challenges
  - Internal authentication
  - External authentication via a pre-existing server, such as RADIUS, Windows NT/2000, Kerberos, or SecurID
- Automated security patches and system software updates (Netilla GeNIE)
- Single log in enforcement
- Multiple domain support

Netilla Firewall

- Internal dual-Ethernet protection option
- Stateful-inspection technology
- Firewall transversal to limit port openings
- Ideal for multi-layer firewall designs
- Session-based for controlling desktop application access

Netilla Management

Web-based GUI

- Customizable log in page
- Tailor service tabs (Files, Apps, etc.) to individual needs
- Full Desktop display (Kiosk Mode)
- Print controls to pause or stop printing
- Help and notification text area per application
- Run multiple applications simultaneously

User Management

- Local Group support
- Microsoft Active Directory Support
- Remote and local software update with the Netilla GeNIE
- Remote monitoring, configuration and diagnostic troubleshooting
- Session-based Monitoring
- No client software or local configuration of applications required for Remote and Web applications
- Non-intrusive deployment
- No new firewall ports to open - All traffic traverses Port 443
- Compatible with third-party access and authentication protocols

Networking & Routing

- Multiple domains
- Private subnets
- Static routing
- Dual Interface configuration

Monitoring/Reporting

- NSP appliance performance
- Application usage
- Internal firewall
- SNMP
- Remote logging to a syslog server

Hardware Specifications

Netilla-powered SSL VPN solutions are available in B, E, and G series models, depending on the capacity needs of your organization.

Hardware Specifications

Dimensions

- 17.75 in. x 15.25 in. x 1.75 in. (45.1 cm x 38.7 cm x 4.5 cm); fits in a standard single-unit (1U), 19-in. equipment rack.
- Weight: 15 lbs. (6.8 kg)
- Power Requirements
  - E-Class and B-Class: Input rating 100-240 V, 50/60 Hz
  - G-Class: Input rating 100-240 V, 47/63 Hz
- Power Consumption
  - E-Class and B-Class: 5.3 amps
  - G-Class: 6.0 amps

Ports

- Two RJ-45 10/100 Ethernet
- Nine pin serial console port

Operating Environment:

- 32°F to 95°F (0°C to 35°C)
- 10% to 90% humidity (non-condensing

Non-Operating Environment

- 14°F to 112oF (-10°C to 50°C)
- 5% to 93% humidity (non-condensing)

Regulatory Approvals

- CISPR 22B
- UL
- CE
- FCC Part 15 B
- CSA

F Appendix F: Third Party Licenses

GNU Public License

There may be provided with the Netilla products certain Open Source software that is governed by the GNU General Public License (GPL). A complete machine-readable copy of the corresponding source code is available by contacting Netilla at 732-652-5200 or info@netilla.com. There may be a nominal charge for delivering the media containing the Open Source software. This offer is valid for 3 years.

OpenSSL

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL. This library is free for commercial and non-commercial use as long as the following conditions are adheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)". The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

5. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-ocore@openssl.org.

6. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.

7. Redistributions of any form whatsoever must retain the following acknowledgement: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG AND THE OPENSSL PROJECT`AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENSSL PROJECT,AUTHOR OR THEIR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed, i.e., this code cannot simply be copied and put under another distribution licence, including the GNU Public License.

PostgreSQL

Portions Copyright © 1996-2004, The PostgreSQL Global Development Group
Portions Copyright © 1994, The Regents of the University of California Permission to use, copy, modify, and distribute this software and its documentation for any purpose, without fee, and without a written agreement is hereby granted, provided that the above copyright notice and this paragraph and the following two paragraphs appear in all copies.

IN NO EVENT SHALL THE UNIVERSITY OF CALIFORNIA BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS, ARISING OUT OF THE USE OF THIS SOFTWARE AND ITS DOCUMENTATION, EVEN IF THE UNIVERSITY OF CALIFORNIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE UNIVERSITY OF CALIFORNIA SPECIFICALLY DISCLAIMS ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE PROVIDED HEREUNDER IS ON AN “AS IS” BASIS, AND THE UNIVERSITY OF CALIFORNIA HAS NO OBLIGATIONS TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

Index