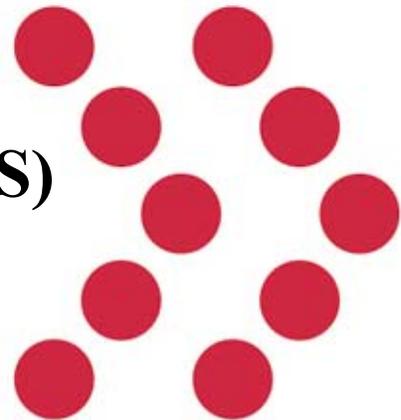


Remote Access Service (RAS) User Guide



Update

Version 1.8

12 December 2003

NMCI.60016.01.U+8.E

Revision History

The Revision History table below lists in chronological order each minor revision of this document. A minor revision is defined as a set of changes affecting fewer than 30 percent of the pages in the document.

-1- Date	-2- Author	-3- Revision Number	-4- Change(s) Made	-5- Affected Page(s)
19 May 2003	DMC		Formatted and edited for publication.	All
9 May 2003	Rose Tajvidi		Replaced Timestep with Alcatel screens and instructions.	All
16 June 2003	Karen Poncina		Formatted and edited for publication.	All
12 December 2003	Karen Poncina		Formatted and edited for publication to include new VPN information.	All

¹**Date:** date of the revision, listed on the cover page (format: MM/DD/YY)

²**Author:** person(s) responsible for revising the document (first and last name)

³**Revision Number:** version number, as listed on the cover page

⁴**Change(s) Made:** list of modifications (e.g., section added, exhibit revised, paragraph deleted, etc.)

⁵**Affected Page(s):** list of pages that were revised (e.g., 1, 2, 4-6, etc.)

Entries in the Revision History table are deleted when a document undergoes a major revision, called a document update. A document update is defined as a set of changes affecting more than 30 percent of the pages in the document. Document updates do not need to be listed in the Revision History table.

For more information about Navy Marine Corps Intranet (NMCI) documentation, contact the manager of the Document Management Center (DMC) (Sandra Ward, 703-742-1164, ISFDOCSMailbox@eds.com).

Document Storage

The NMCI Operations Library assigns identification (ID) numbers for NMCI documents and stores the master editions. To contact the library, telephone or e-mail the Operations Librarian (James R. Taylor, 703-742-1940, ISFOPSLibrary@eds.com).

Table of Contents

1. INTRODUCTION.....	1
2. PREPARATION	2
3. ESTABLISHING A RAS CONNECTION	3
3.1 Connecting to An Analog Telephone Line	3
3.2 Logging on to the NMCI Laptop.....	4
3.3 Local Access Number	5
3.4 Establishing An Internet Connection	11
3.5 Logging on to the VPN Client – Timestep and Alcatel	12
3.6 Logging on to the VPN Client – Netscreen Remote	14
3.7 Confirming the PKI Certificate was Imported Successfully	19
3.8 Loading the PKI Identity Certificate into NetScreen Remote.....	20
3.9 Creating a Secure Connection with NetScreen Remote.....	21
4. EXPECTATIONS	24
5. ACCESSING THE NMCI H: DRIVE.....	25
5.1 Viewing the H: Drive.....	25
5.2 Connecting To the NMCI H: Drive.....	26
6. DISCONNECTING FROM THE NMIC NETWORK.....	28
7. RESETTING OR CHANGING THE PAL HOST PASSWORD.....	30
8. IMPORTANT REMINDERS	31
8.1 PKI Certificate.....	31
8.2 NMCI RAS.....	31

Exhibit

Exhibit 1 – Analog Telephone Cable	3
--	---

Appendix

Appendix A - Acronyms	A-1
-----------------------------	-----

1. INTRODUCTION

Welcome to the *NMCI Remote Access Service (RAS) User Guide*. RAS allows NMCI laptop users to connect to the NMCI network while working away from the user's assigned site. It allows the user to access the NMCI account including NMCI Microsoft (MS) Outlook e-mail, as well as the H: and S: drives. The instructions in this guide outline step-by-step procedures for a configured, undocked NMCI laptop to be connected to the NMCI network through an analog telephone line.

2. PREPARATION

To prepare to successfully dial in to the NMCI network, perform the following steps:

1. The laptop must have been logged into the NMCI network through the local area network (LAN) connection at the user's site at least once. This enables a network profile to be established allowing the remote connection.
2. Obtain a Public Key Infrastructure (PKI) certificate. The PKI certificate is used to authenticate the user's identity allowing remote access to the NMCI network. To obtain a PKI certificate, contact the Information Systems Security Officer (ISSO) or Contract Technical Representative (CTR).
3. Place a copy of the PKI certificate on the laptop (refer to the *PKI Certificate Download Quick Reference Guide* in the PKI/CAC section at <http://www.nmci-isf.com/userinfo.htm> or through the user information section available on the NMCI Homeport Web site, Services tab).
4. Contact the NMCI Help Desk (1-866-THE-NMCI or 1-866-843-6624) to obtain the host password used with the Phone Access Line (PaL) dial-up application.

3. ESTABLISHING A RAS CONNECTION

To remotely access the NMCI network, perform the following steps:

1. Connect the laptop to an analog telephone line.
2. Log in to the laptop.
3. Locate a local access number.
4. Enter the dialing prefix information, if applicable.
5. Save the local access number.
6. Connect to the NMCI network using PaL and the Virtual Private Network (VPN) client.

3.1 CONNECTING TO AN ANALOG TELEPHONE LINE

Before attempting to connect to the NMCI network, the following items are needed:

- NMCI laptop
- A telephone (analog) wall jack. (**DO NOT** use a digital line.)

NOTE: If you do not know if the telephone jack is digital or analog, ask someone who is familiar with the telephone connections at that location. Connecting the NMCI laptop to a digital line causes damage to the modem.

- An analog telephone cable (Exhibit 1).



Exhibit 1: Analog Telephone Cable

To establish a remote connection, perform the following steps:

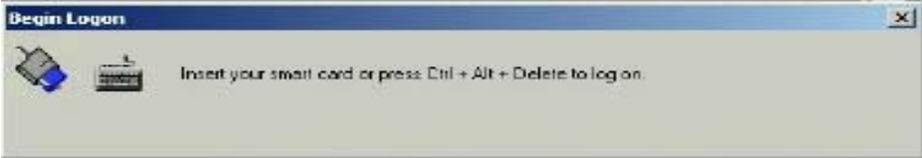
Step	Action
1.	Connect one end of the telephone cable to the modem connection on the side of the laptop. <div style="text-align: center;">  </div>

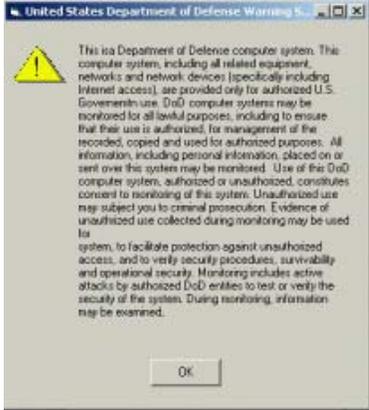
Step	Action
2.	<p>Plug the other end of the telephone cable into an analog telephone wall jack.</p> 
3.	<p>The complete cable connection from the laptop to a telephone wall jack is shown below.</p> 

NOTE: If RAS is required outside of the United States, the following countries require a country-specific telephone cable adapter: Austria, Belgium, Denmark, Finland, France, Germany, Holland, Ireland, Italy, New Zealand, Norway, Poland, Spain, South Africa, Sweden, Switzerland, and the United Kingdom. For more information, call the NMCI Help Desk at 1-866-THE-NMCI or 1-866-843-6624.

3.2 LOGGING ON TO THE NMCI LAPTOP

Logging on to the NMCI laptop is the same process that is completed when it is in the docking station. To log in to the NMCI laptop, perform the following steps:

Step	Action
1.	<p>Press the Power button. Microsoft Windows 2000 loads and the Begin Logon window appears.</p> 

Step	Action
2.	<p>Press Ctrl + Alt + Delete. The U.S. Department of Defense (DoD) Warning Statement window appears.</p> 
3.	<p>Click OK. The Logon Information window appears.</p> 
4.	<p>In the User Name field, type the NMCI network user name. (For example, Jack Smith.)</p>
5.	<p>In the Password field, type the NMCI network password.</p>
6.	<p>In the Log on to: field, verify that the correct domain is selected. If not, in the drop-down list, click the correct domain. If the domain unknown, contact the NMCI Help Desk at 1-866-THE-NMCI or 1-866-843-6624.</p>
7.	<p>After typing the NMCI user name, network password, and domain, click OK. The workstation will complete the logon process.</p>

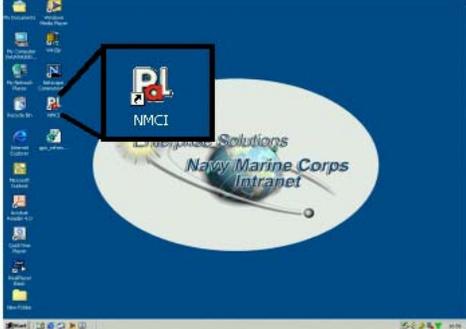
NOTE: If the user logs on to the laptop without using an NMCI network connection, a *Loss of Profile* message may appear. Click **OK**. The desktop appears.

3.3 LOCAL ACCESS NUMBER

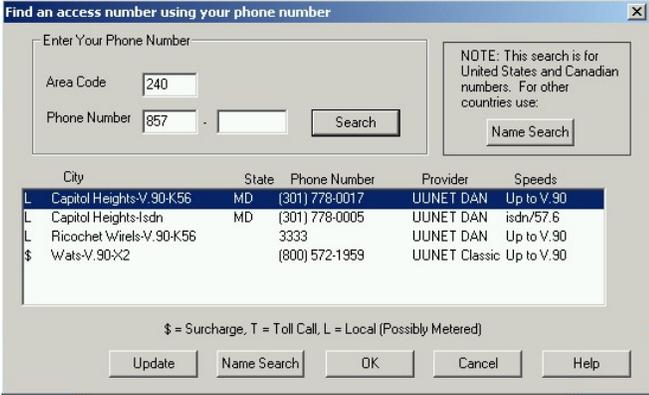
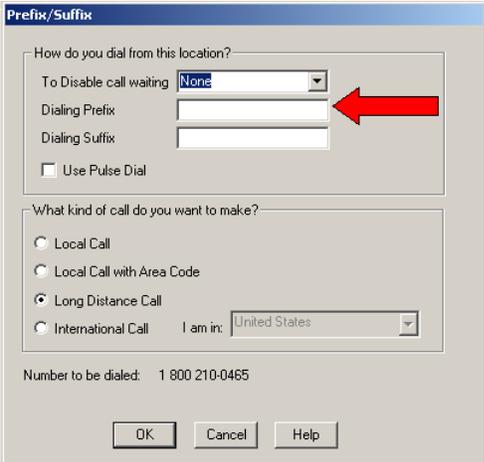
The user is ready to begin using the NMCI dial-up software (PaL) to establish a remote connection. The PaL icon is located on the desktop. The first step is to locate a local or toll-free

access number. Using a local access number associated with the user's location ensures that long distance telephone charges are not incurred. To locate a local access number, perform the following steps:

NOTE: A toll-free access number is available at any time; however, it is strongly recommended to use a local access number when possible. The toll-free access number should only be used when a local access number is not available at the user's location.

Step	Action
1.	Double-click the PaL icon. 
2.	The main PaL window appears. 
3.	Click Phone Book .

Step	Action
4.	<p>If the Name Search window appears, click Number Search. The Number Search window appears.</p>  <p>NOTE: To locate a local access number, perform either a name search (type the city and state) or a number search (type the area code and the first three digits of the location).</p> 
5.	To perform a number search, in the Area Code field, type the location area code.
6.	In the first Phone Number field, type the first three digits of the location.

Step	Action
7.	<p>Click Search. The bottom portion of the window displays a list of local access numbers (and the toll free number).</p> 
8.	Click a number from the list.
9.	<p>Click OK. The Prefix/Suffix window appears.</p> 
10.	If dialing prefix information is not required, leave those fields blank and click OK .
11.	If additional dialing information is needed, type the applicable information. (For example, if 9 must be dialed to access an outside line, in the Dialing Prefix field, type 9 .) If needed, change any additional fields and click OK .

Step	Action
12.	<p>The access number and prefix, if required, displays in the Phone Number field.</p> 

After selecting a local access number, save that number as a Favorite. This allows easy access from the Show Favorites feature if needed in the future. This is also helpful for traveling to the same location repeatedly. To save a local access number, perform the following steps:

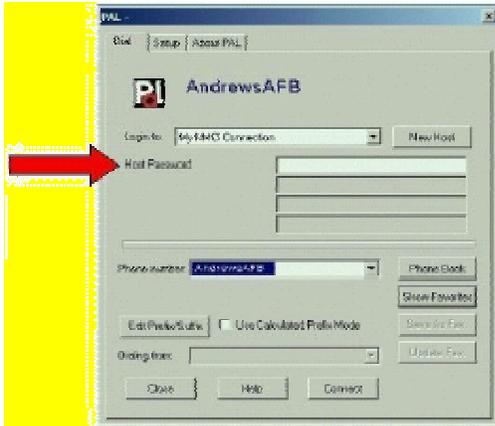
Step	Action
1.	<p>In the main PaL window, click Save As Fav.</p> 

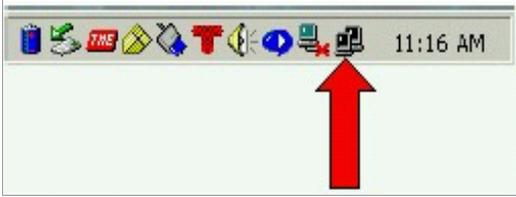
Step	Action
2.	<p>The Save Call Setup window appears.</p> 
3.	<p>In the Enter a name for this setup field, type a name to help identify the selected local access number (for example: San Diego Dial In).</p>
4.	<p>Click OK.</p>

3.4 ESTABLISHING AN INTERNET CONNECTION

The following steps outline the process to log into the PaL dial up application and establish an Internet connection. To access the NMCI network, after establishing an Internet connection, the steps in *Logging on to the VPN Client* **must** be completed. To establish an Internet connection, perform the following steps:

NOTE: Contact the NMCI Help Desk at 1-866-THE-NMCI or 1-866-843-6624 to obtain the host password for logging on to the PaL application.

Step	Action
<p>1.</p>	<p>Verify that the correct access number displays in the Phone number field. If not, in the Favorites list, click Show Favorites and select the number.</p> <p>In the Host Password field, type the host password supplied by the NMCI Help Desk.</p> 
<p>2.</p>	<p>Click Connect. As the system is establishing the connection, the Network Call Status window appears.</p> 

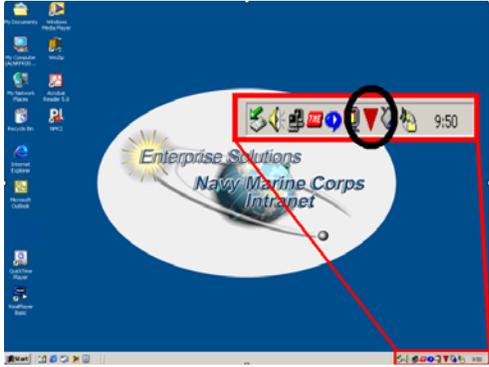
Step	Action
3.	<p>After the connection is established, the PaL status window minimizes. A set of computer icons appears in the lower right corner of the taskbar.</p> 

3.5 LOGGING ON TO THE VPN CLIENT – TIMESTEP AND ALCATEL

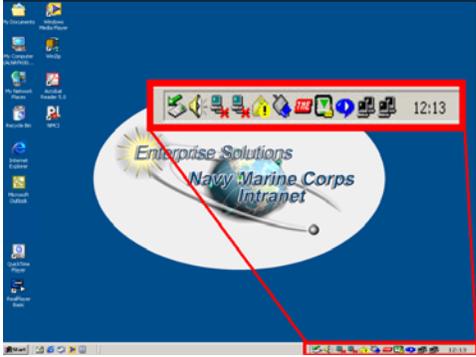
This section describes the inverted red triangle icon that is associated with a software version used to create a secure connection. If the workstation currently displays a red T, instead of a red triangle, the steps in this section apply for both software versions.

NOTE: For USMC NMCI laptop users, refer to the section *Logging on to the VPN Client – NetScreen Remote* for instructions.

After establishing the dial-up connection, to access the NMCI network, the user must log in to the VPN client by logging on to the PKI certificate stored on the hard drive. If the PKI is not stored on the hard drive, contact the NMCI Help Desk at 1-866-THE-NMCI or 1-866-843-6624 for assistance. To log in to the VPN client, perform the following steps:

Step	Action
1.	<p>In the lower right corner of the desktop, right-click the red inverted triangle.</p> 

Step	Action
2.	<p>The VPN client menu appears.</p> 
3.	<p>Click Login Certificate. The VPN Client Login window appears.</p>  <p>NOTE: The first time a user logs on to the VPN client, click Browse to locate the PKI certificate. After successfully logging into the PKI certificate, the User File field defaults to the certificate name. Contact the NMCI Help Desk at 1-866-THE-NMCI or 1-866-843-6624 for assistance.</p>
4.	<p>In the Password field, type the personal security password (the password created when the PKI certificate was downloaded).</p>
5.	<p>Click OK. A message window appears reporting that a secure tunnel is being created and a status message appears.</p>

Step	Action
6.	After the connection process completes, the red inverted triangle becomes green. (The PaL window minimizes automatically.)
7.	<p>When the secure connection is established, a second set of computer icons appears in the lower right corner and a black box with a padlock displays around the green inverted triangle.</p> 

NOTE: Do not attempt to access network applications, drives, or folders until the red inverted triangle becomes green and the second set of computer icons appears in the taskbar.

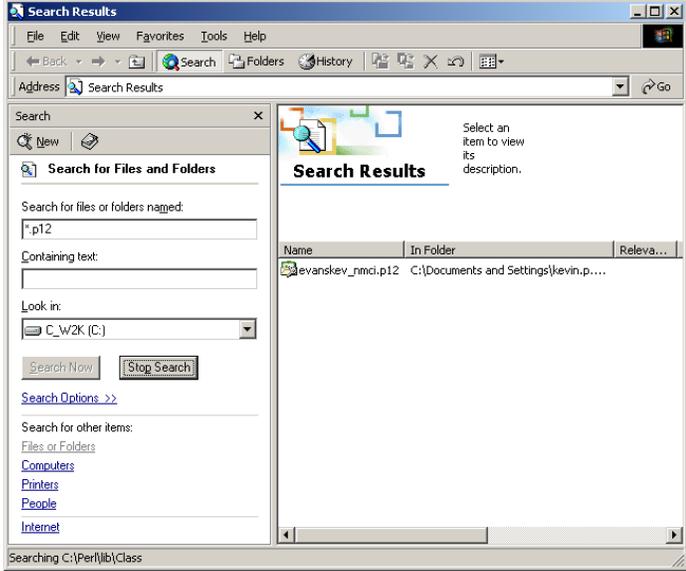
NOTE: Because the NMCI network has not been logged in to directly, and before attempting to open MS Outlook or access the H: or S: drives, reinitiate the mappings for these drives. To perform this, on the desktop, click **Mapshare** or **Mappings.bat**. If the H: drive needs to be remapped, complete the steps in *Connecting to the NMCI H: Drive*. Contact the NMCI Help Desk at 1-866-THE-NMCI or 1-866-843-6624 for assistance.

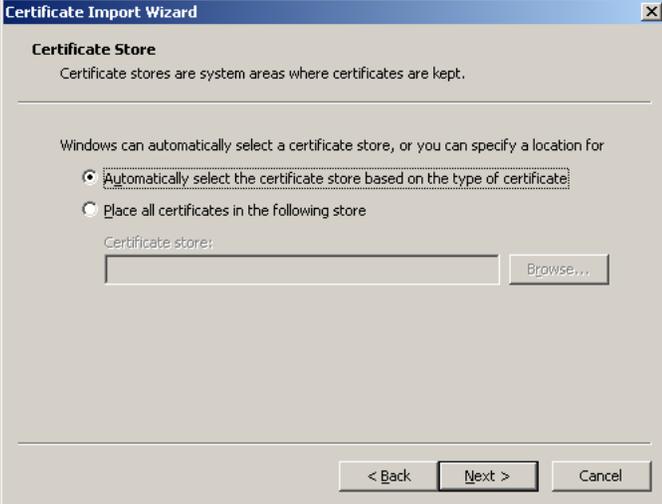
3.6 LOGGING ON TO THE VPN CLIENT – NETSCREEN REMOTE

After establishing the dial-up connection, to access the NMCI network, log in to the VPN client. This is performed by logging on to the PKI certificate on the hard drive, importing into the certificate store of the workstation, and loading into the NetScreen Remote application. If the PKI certificate has not been stored on the hard drive, imported the certificate into the certificate store, and loaded into the NetScreen Remote application, contact the NMCI Help Desk at 1-866-THE-NMCI or 1-866-843-6624 for assistance. The steps in this section outline how to import the PKI certificate into the certificate store on the workstation and to create a secure connection using the VPN client.

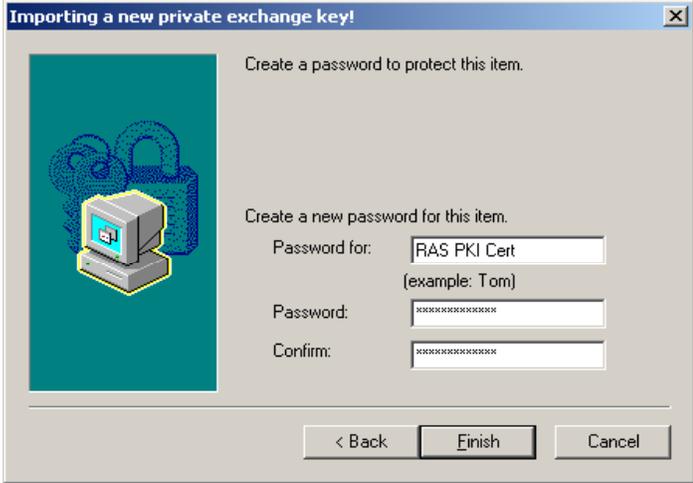
NOTE: Before beginning these steps, a copy of the PKI certificate must be placed on the laptop hard drive. Also, if multiple NMCI laptops are used, the user’s PKI certificate must be imported in to NetScreen Remote on to each laptop that is used remotely. The import and loading process only needs to be completed once on each laptop.

To import the PKI certificate into the Certificate Store, perform the following steps:

Step	Action
1.	From Windows Explorer, click Search .
2.	In the Search for Files or Folders Named field, type *.p12 . This file extension corresponds with the PKI certificate.
3.	In the Search Results window, click Search Now . The system locates the PKI certificate. 
4.	Double-click the PKI certificate. The Certificate Import Wizard window appears. Review the information and click Next .

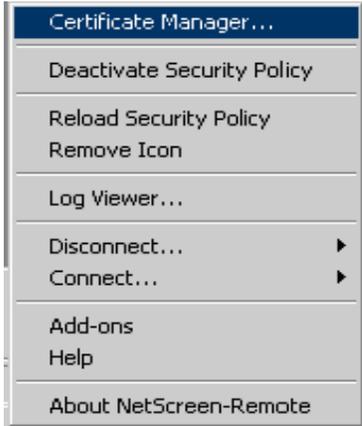
Step	Action
5.	<p>In the Certificate Import Wizard window, in the Password field, type the correct PKI password (the password created after downloading the PKI certificate). Ensure that both boxes are checked and click Next.</p> 
6.	<p>In the Certificate Import Wizard – Certificate Store window, ensure that Automatically select the certificate store based on the type of certificate is selected. Click Next.</p> 
7.	<p>A screen appears indicating that the Certificate Import has been completed. Click Finish.</p>

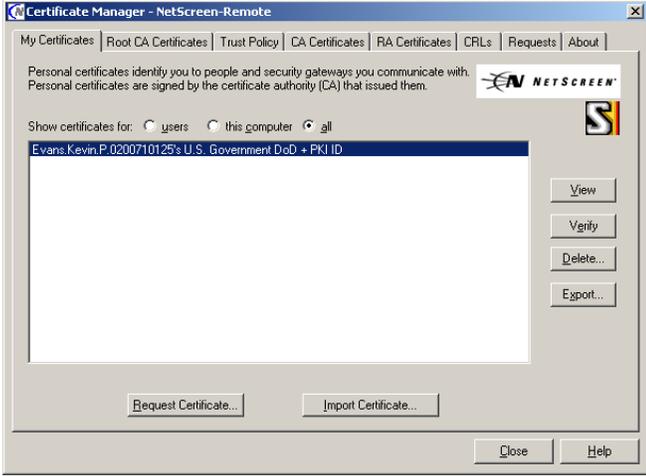
Step	Action
8.	<p>The Importing a New Private Exchange Key window appears. Click Set Security Level.</p> 
9.	<p>In the Importing a New Private Exchange Key window, click High and Next.</p> 

Step	Action
10.	<p>The Importing a New Private Exchange Key – Creating a Password window appears. In the Password for field, type a short description of how the certificate is used (For example, RAS PKI Cert). In the Password and Confirm fields, type the password created when downloading the PKI certificate. Click Finish.</p> 
11.	<p>The Importing a New Private Exchange Key window appears. Click OK.</p> 
12.	<p>A dialog box indicating that the certificate import was successful appears. Click OK.</p>

3.7 CONFIRMING THE PKI CERTIFICATE WAS IMPORTED SUCCESSFULLY

To confirm that the PKI certificate was imported into the Certificate Store successfully, perform the following steps:

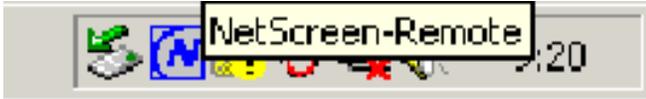
Step	Action
1.	<p>From the desktop, in the lower right corner, right-click the blue box with the red X.</p> 
2.	<p>The NetScreen Remote dialog box appears. Click Certificate Manager.</p> 

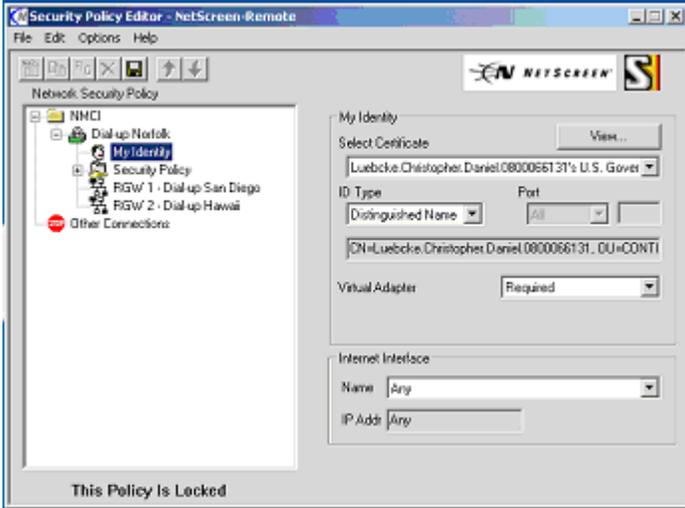
Step	Action
3.	<p>In the Certificate Manager – NetScreen-Remote window, on the My Certificates tab, the PKI certificate is listed. Click Close.</p> 

3.8 LOADING THE PKI IDENTITY CERTIFICATE INTO NETSCREEN REMOTE

To load the PKI identity certificate into NetScreen-Remote, perform the following steps:

NOTE: These steps only need to be completed once during setup. They do not need to be completed each time a user remotely connects to the NMCI network. If additional laptops are used, this process must be completed for each laptop.

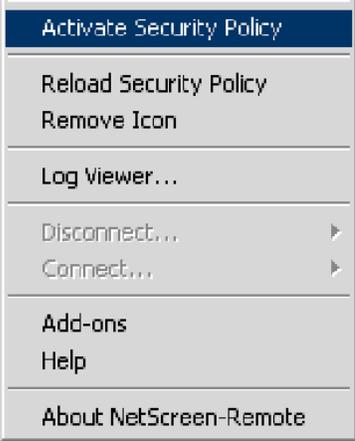
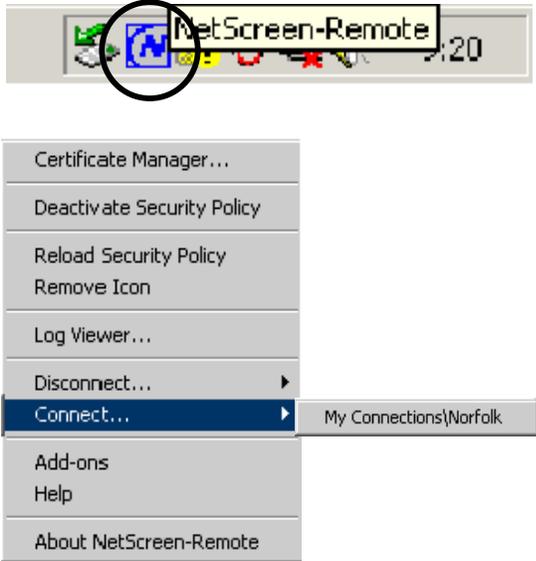
Step	Action
1.	<p>On the desktop, in the taskbar, right-click the red X and click Activate Security Policy. Double-click the blue N.</p> 

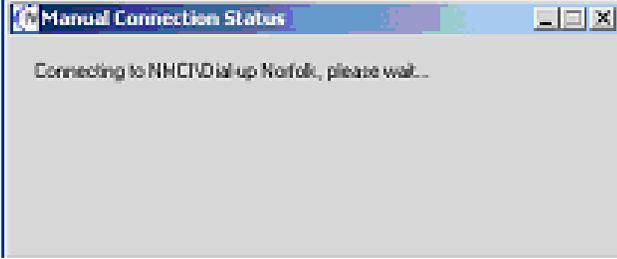
Step	Action
2.	<p>The Security Policy Editor – NetScreen-Remote screen appears. Click + to expand NMCI, + to expand Dial Up Network, and click My Identity.</p> 
3.	<p>In the Select Certificate field, in the drop-down list, click the correct PKI identity certificate and View to confirm that the correct PKI identity certificate has been selected. Close the box. After selecting the correct PKI identity certificate, save this function. The certificate is now loaded into the NetScreen Remote application.</p>
4.	<p>From the desktop, in the lower right corner, click the blue N. Click Deactivate Security Policy.</p>

3.9 CREATING A SECURE CONNECTION WITH NETSCREEN REMOTE

To create a secure connection with NetScreen Remote, perform the following steps:

Step	Action
1.	<p>From the desktop, in the lower right corner, right-click the red X.</p> 

Step	Action
2.	<p>In the following dialog box, click Activate Security Policy. This activates the security policy that allows a secure connection to be established. After selecting this option, the dialog box will close and the red X will change to a blue N.</p> 
3.	<p>In the taskbar, right-click the blue N and click Connect. Click the connection closest to the user's location (for users on the East coast of the United States, click My Connections/Norfolk).</p> 

Step	Action
4.	<p>The Manual Connection Status window appears indicating the connection. A dialog box appears prompting the user for the PKI identity certificate password. Type the PKI identity certificate password and click OK.</p> <p>NOTE: The system may require the user to type the PKI identity certificate password more than once for verification. NetScreen Remote completes the connection.</p>  <p>The screenshot shows a dialog box titled "Manual Connection Status" with a progress bar and the text "Connecting to NMCI/Dial-up Norfolk, please wait..."</p>
5.	<p>After establishing the connection, in the lower right corner of the screen, a gold key with the NetScreen Remote icon and a second set of computer icons appear.</p>  <p>The screenshot shows a notification area in the system tray. A yellow notification box displays "SafeNet Virtual Adapter Interface" and "Speed: 10.4 Mbps". Below it, a gold key icon and a second set of computer icons are visible, both circled in black. The system clock shows 14:17.</p>

4. EXPECTATIONS

After establishing a remote connection to the NMCI network, the following functionalities are available:

- Access to the NMCI MS Outlook account (send and receive e-mails, calendar items, and public folders).
- Access to the H: and S: drives.

NOTE: If the H: and S: drives are not accessible, to reconnect, click the **Mapshare** or **Mappings.bat** icon on the desktop or follow the instructions in *Connecting to the NMCI H: Drive*.

- Access to the Internet.
- Access to the NMCI Portal.
- Access to the Navy and Marine Corps white pages to search for people and commands.

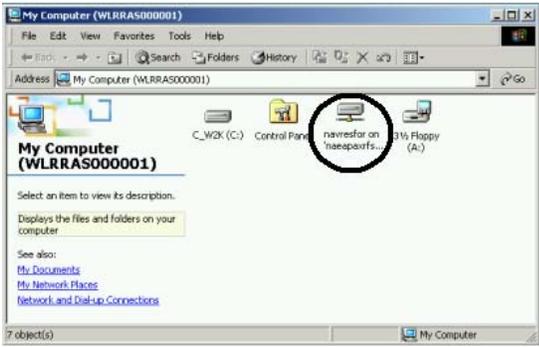
NOTE: Laptop performance is slower when using RAS (especially when sending and receiving large documents through e-mail and accessing the public folders in MS Outlook) because the network is being accessed through telephone cables.

5. ACCESSING THE NMCI H: DRIVE

This section describes how to access the NMCI H: drive when connecting to the NMCI network remotely. If the H: drive is not accessible, follow the instructions *Connecting to the NMCI H: Drive*.

5.1 VIEWING THE H: DRIVE

To view the H: drive, perform the following steps:

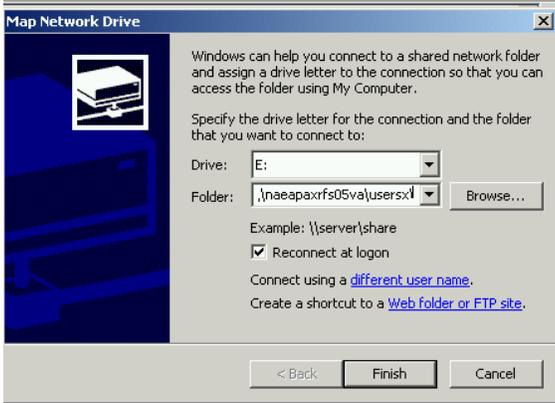
Step	Action
<p>1.</p>	<p>From the desktop, double-click the My Computer icon.</p> <div data-bbox="776 705 932 873" data-label="Image">  </div> <p>The My Computer window appears.</p> <div data-bbox="583 936 1122 1283" data-label="Image">  </div>
<p>2.</p>	<p>To access the H: drive, double-click the H: drive icon.</p> <p>NOTE: Remote connections to the NMCI network may slow down the process.</p>

5.2 CONNECTING TO THE NMCI H: DRIVE

After remotely connecting and opening the **My Computer** icon, if the NMCI H: drive is not visible, perform the following steps:

NOTE: Before beginning this process, the server name containing the H: drive must be known. If this information is not available, contact the NMCI Help Desk at 1-866-THE-NMCI or 1-866-843-6624 for assistance.

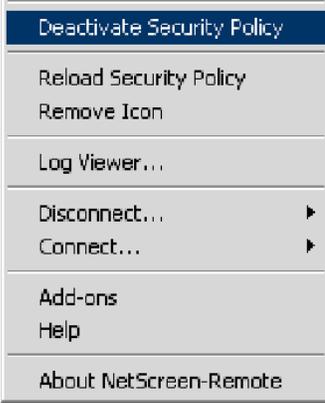
Step	Action
1.	<p>From the menu, in the My Computer window, click Tools.</p> 
2.	<p>Click Map Network Drive. The Map Network Drive window appears.</p> 
3.	<p>In the Drive field, in the drop-down list, click H:.</p>
4.	<p>In the Folder field, type two back slashes (\\), the server name that contains the H: drive, a single back slash (\), the user.name, and \$. (For example: \\naduseas\jack.smith\$.)</p>
5.	<p>Ensure that the Reconnect at logon checkbox is selected.</p>

Step	Action
6.	<p>Click Finish.</p> 
7.	<p>A message appears informing the user that the application is attempting to connect to the \\servername\user.name\$. After the mapping completes, the icon for the H: drive appears in the My Computer window.</p>

6. DISCONNECTING FROM THE NMIC NETWORK

To disconnect the RAS connection from the NMCI network, perform the following steps:

Step	Action
1.	Close all windows and applications using the RAS connection (e.g., MS Outlook, browser windows, etc.).
2.	On the taskbar, click Network Call Status . 
3.	The Network Call Status window appears. 
4.	Click Disconnect . The network is disconnected. (Some computer icons disappear from the taskbar.)
5.	In the Network Call Status window, click Cancel .
6.	To log out of the VPN client, right-click the green inverted triangle icon.
7.	From the VPN Client menu, click Logoff Certificate .

Step	Action
8.	<p>If using NetScreen Remote, right-click the blue N. Click Disconnect. Right-click the blue N and click Deactivate Security Policy. The connection terminates.</p>  <p>NOTE: If the security policy is not deactivated before reconnecting to a LAN network connection (i.e., the user's NMCI connection at the office), the network connection will not function.</p>

7. RESETTING OR CHANGING THE PAL HOST PASSWORD

The PaL Host Password can be changed. Complete one of the following to change the host password:

- Contact the NMCI Help Desk at 1-866-THE-NMCI or 1-866-843-6624.

Or

- Visit the Web site: <https://www.nmci.uu.net/english/default.asp>. Log on to the site using the NMCI user name (for example: Jack.Smith), NMCI network password, and complete the instructions.

NOTE: The PaL password is **NOT** the user's personal security password used to log in to the VPN Client login window.

8. IMPORTANT REMINDERS

This section provides important information when using the RAS process to connect to the NMCI network.

8.1 PKI CERTIFICATE

The following are some points to remember concerning the PKI certificate:

- If the floppy disk is lost or someone finds out a user's password, have the certificate revoked and a new certificate issued.
- The PKI certificate is valid for 3 years. (The PKI password does not expire during that 3-year timeframe.)
- If the PKI certificate is used on a non-military workstation (with the exception of the user's home computer) to access NMCI e-mail using MS Outlook Web Access, remove the certificate from that workstation after completing activities.

8.2 NMCI RAS

The following are some points to remember concerning NMCI RAS:

- Only use an analog line to connect to the NMCI network. A digital line will damage a modem.
- Use local access numbers when possible. Only use the toll-free number when local access numbers are not available at a user's location.
- If traveling frequently, place the NMCI laptop in the docking station at least monthly to receive periodic updates to applications, virus protection, etc. using the direct network connection.

APPENDIX A: ACRONYMS

Acronyms

RAS	Remote Access Service
NMCI	Navy Marine Corps Intranet
MS	Microsoft
LAN	Local Area Network
PKI	Public Key Infrastructure
ISSO	Information Systems Security Officer
CTR	Contract Technical Representative
PaL	Phone Access Lookup
VPN	Virtual Private Network
DoD	Department of Defense
DMC	Document Management Center