
NMCI Deployable Seat

TimeStep (PERMIT/client) VPN Procedures Document

For



Prepared By



Task Number

0107-1053

Date

12/16/2002

TABLE OF CONTENTS

Paragraph & Description	Page
Title Page	i
Distribution List.....	ii
Revision History	ii
Table of Contents.....	iii
1.0 Introduction	1
1.1 NMCI CLIN 004AC Seat:.....	1
1.2 NMCI Environment.....	1
1.3 NMCI Deployed Environment	2
1.4 Background and Overview	2
2.0 TimeStep (Permit/Client) VPN software.....	4
2.1 Is TimeStep Installed.....	4
2.1.1 Determine if TimeStep is loaded on the machine.	4
2.1.2 Copy Certificate File to the CERT Directory on the NMCI Seat.....	5
2.1.3 Login your Certificate	6
2.1.4 Enter the password for your certificate	7
2.1.5 Certificate has been logged into TimeStep.....	8
Appendix Description	Page

1.0 Introduction

The NMCI enterprise Operating System environment is Microsoft Windows 2000 Active Directory. However, Windows NT is used in the USMC deployed environment. In preparation for the Marine Corps' transition to NMCI, MCTSSA has been tasked to perform a pilot implementation of an NMCI Seat in a deployed environment and document the procedure to accomplish this task. Dialin access to the NMCI Network is a requirement for Marine Corps units when deployed. As a result of this requirement, MCTSSA has been tasked to produce a TimeStep (PERMIT/client) VPN Procedures Document for distribution to the Fleet. This will be used as a guide to assist users with the process that is required in order to remotely access the NMCI Network. This document is intended as a supplement to the NMCI ISF document titled Remote Access Service Getting Started (Steps 3 and 4) and is intended to minimize the need for external assistance should a user encounter problems accessing the NMCI network from a remote location. This document describes the procedure of accessing the NMCI Network from a NMCI Seat that has been deployed into a tactical environment.

1.1 NMCI CLIN 004AC Seat:

Pentium III 1 GHz Processor
256MB of RAM
Integrated Ethernet 10/100 Adapter
Integrated V.90 56K Dialup Adapter

1.2 NMCI Environment

Access to the NMCI network will be accomplished via authentication through either Remote Access Service (RAS) or High Speed VPN (Virtual Private Network). The NMCI ISF (Internet Strike Force) has created a document titled Remote Access Service Getting Started Guide. You can obtain a copy of the NMCI ISF document by going to <http://www.nmci-isf.com/RASStartGuide.pdf>

The following document is intended to be a supplement to the NMCI ISF document and contains the procedures necessary to connect to the NMCI Network once a RAS connection to UUNET has been established. Connecting to the NMCI Network via RAS connectivity requires that a user connect via dialup to UUNET and connect to the NMCI network with TimeStep's VPN software (PERMIT/client). In order to accomplish this, a user must have:

- PKI Certificate
- Personal Security Password (PSP) for their Certificate
- The PaL and the PERMIT/Client software applications loaded on their laptops

-
- UUNET (WorldCom) account login information for MCI/UUNET (including your user name, host realm and password)

If you do not have these items you must call the NMCI Helpdesk (1-866-843-6624) to obtain them.

1.3 NMCI Deployed Environment

The Marine Corps' TDN environment consists of a Windows NT Operating System. Procedure development and assessment of the operability of NMCI Seats in a deployed environment has been conducted at MCTSSA in the SIF MEF Node consisting of Windows NT PDC and BDC, Cisco Routers and Checkpoint's Meta IP DNS.

1.4 Background and Overview

The NMCI Internet Strike Force (ISF)'s Site Manager conducted all initial hardware build and configurations on the NMCI Seats. The builds were modified in order to include the software and configurations necessary to connect to the NMCI Network via RAS.

The following is a step-by-step guide for launching TimeStep PERMIT/Client to access NMCI Network resources from a RAS Dialin connection once the connection has been established.

This page intentionally left blank

2.0 TimeStep (Permit/Client) VPN software

2.1 Is TimeStep Installed

2.1.1 Determine if TimeStep is loaded on the machine.

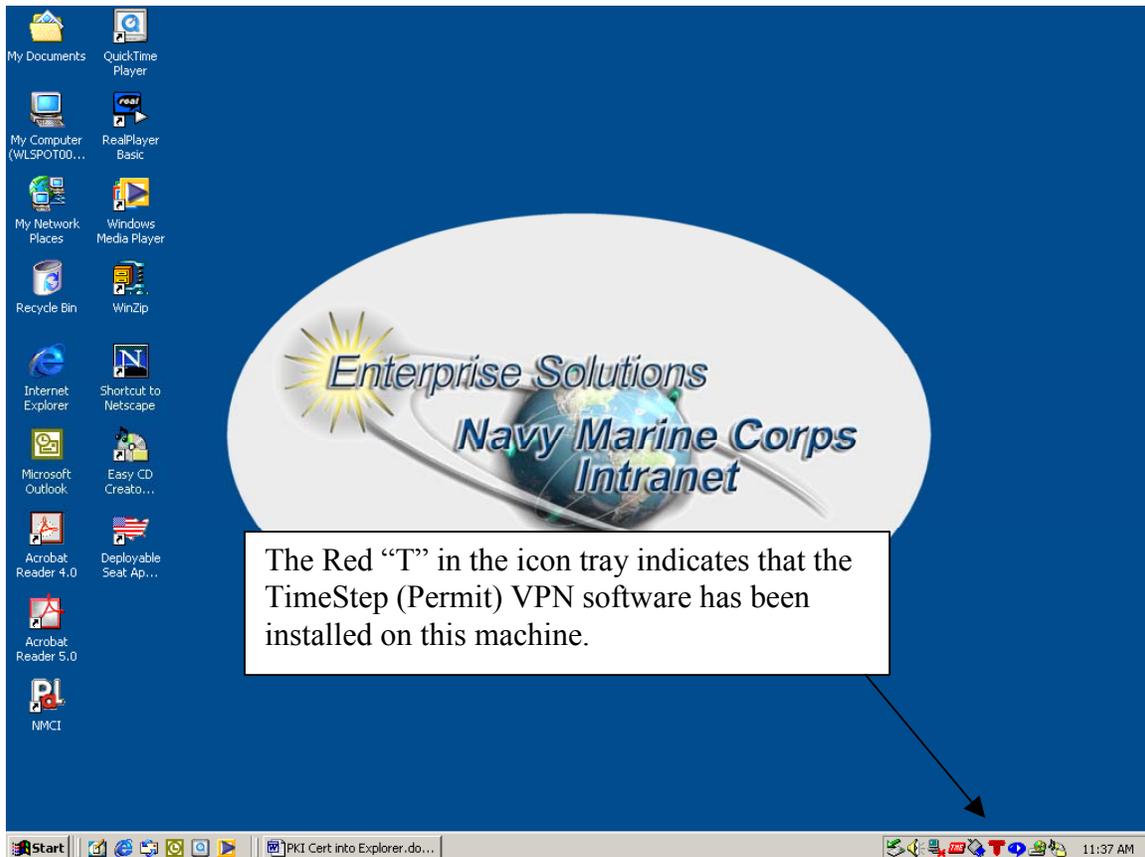


Figure 2.1-1

- 2.1.1.1 *Figure 2.1-1 above shows a Red "T" on the Icon Tray, if this does not appear on your screen you must install TimeStep.*
- 2.1.1.2 *If TimeStep is already loaded (see Figure 2.1-1) proceed with the following installation steps, **otherwise, contact the NMCI Help Desk to have the TimeStep Application loaded on the Seat before you can proceed.***

2.1.2 Copy Certificate File to the CERT Directory on the NMCI Seat

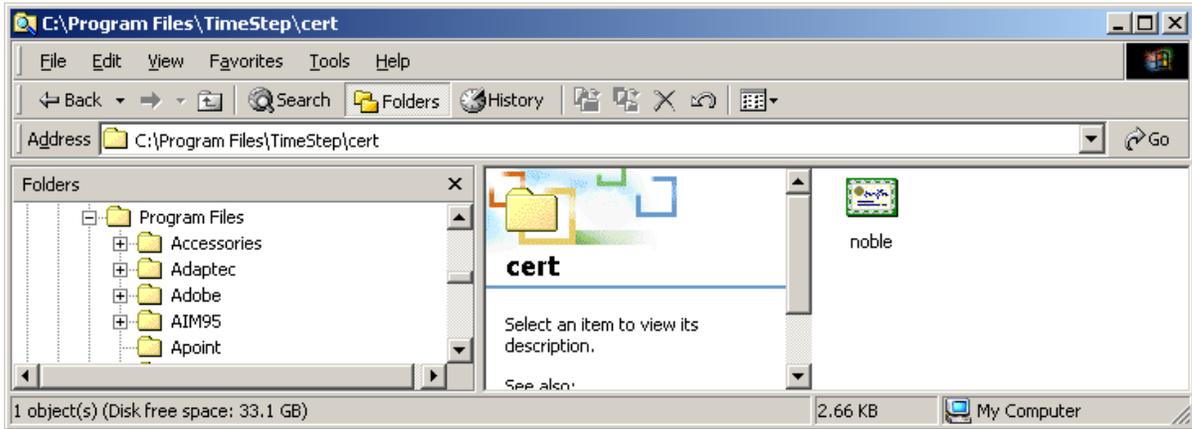


Figure 2.1-2

- 2.1.2.1 *Certificate files must be copied from your diskette to a folder on the NMCI Seat. The folder is located in c:\Program Files\TimeStep\cert as shown in Figure 2.1-2*
- 2.1.2.2 *The user will need to create the "cert" folder if it does not exist and copy their certificate to the cert folder.*

2.1.3 Login your Certificate

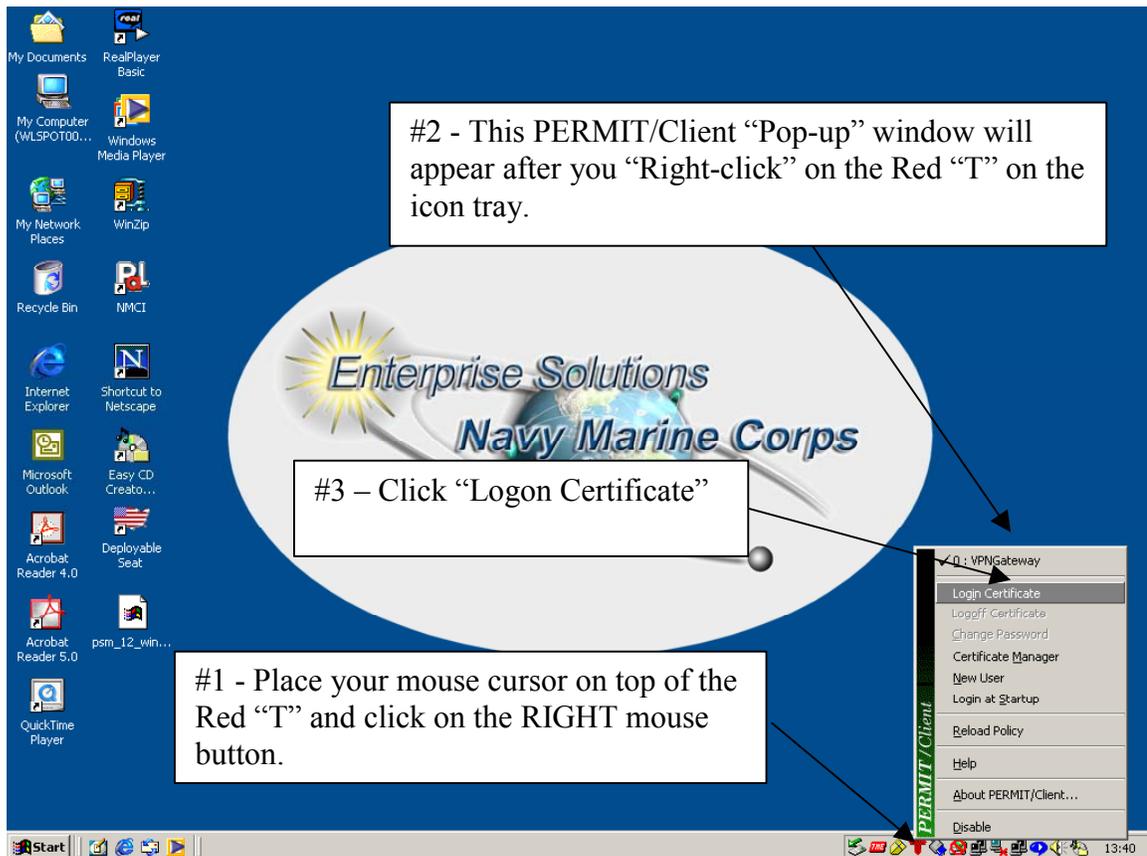


Figure 2.1-3

2.1.3.1 *Right click on the Red T in the Icon Tray and the screen shown in Figure 2.1-3 above will be displayed.*

2.1.4 Enter the password for your certificate

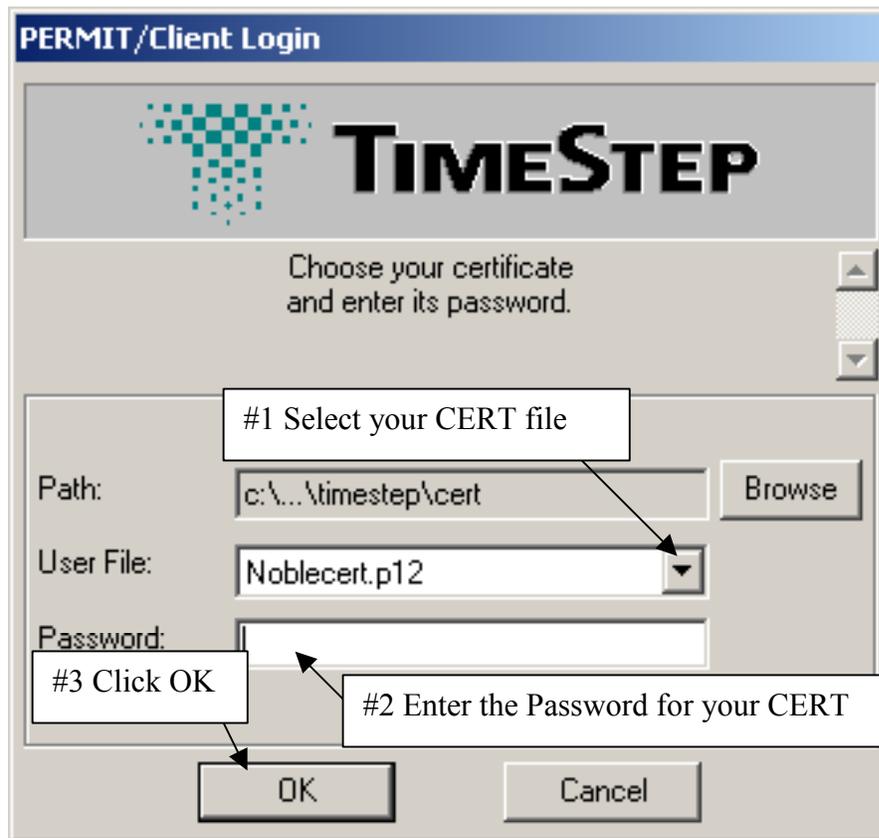


Figure 2.1-4

2.1.4.1 *Figure 2.1-4 appears when you select Login Certificate.*

2.1.4.2 *If you do not see your CERT file listed in the User File block, click the Browse button and select the path to your CERT (c:\Program Files\timestep\cert)*

2.1.4.3 *Select your CERT, then enter your password and click the **OK** button.*

2.1.5 Certificate has been logged into TimeStep.



Figure 2.1-5

- 2.1.5.1 *The Red "T" has now turned green and is ready to connect to the NMCI network. This indicates that the Certificate has been logged in and TimeStep is awaiting a network connection (PaL Dialin).*