

CGDN+ Extranet Access Client Instructions for Windows 9x, Me, NT, 2000, and XP Updated 03/29/2005

Overview: The Nortel Networks Extranet Access Client will enable secure encrypted tunnels to Nortel Networks devices. You must load the client to your laptop or home computer. The client is free and can be used if your computer or laptop is connecting to the CG managed Extranet Switch and is being used for government work (i.e. Telecommuting Program).

What You Need: You will need some information prior to the actually setting up your connection profile. Please obtain your Workgroup/Domain and your Primary and Secondary WINS addresses from your servicing IRM or RSM Staff. It is assumed that you already have an Internet Service Provider (ISP) account. You must also already have an authentication token with a RADIUS username and password. If you do not have a token and would like one, please visit our Remote Access Page:

<http://cgweb.tiscom.uscg.mil/tsd1/tsd1c/remacc/tokenmgmt.htm>

RDP: If you will be using Remote Desktop Protocol (RDP), please obtain your SWIII IP address, or you SWIII computer name. For more information regarding Remote Desktop Protocol please download RDP Installation and configuration instructions from:

<http://cgweb.tiscom.uscg.mil/documentation/remotedesktopcontrol.htm>

CITRIX: If you will be using CITRIX (ICA Client) after connecting to the Coast Guard Data Network (CGDN), please contact your local servicing IRM/RSM Staff for a CITRIX account and support.

Important Notice: The CGDN+ Extranet Switch allows a user to change their password at first logon; however:

- If you have a **Vasco Data Security** token and have previously logged in and changed your password, you will not be prompted to change your password.
- If you are using a **Vasco Data Security** token for the first time and you do not get prompted to change your password, you must contact the **OSC Customer Support at 304-264-2500 or 1-800-821-7081** to hard code your password.

Firewall Notice:

The following ports must be open on a firewall to allow the extranet client to connect successfully:

Protocol 17 (UDP) source + destination port of 500 must be open
Protocol 50 (ESP) must be open both inbound and outbound, port NA
Protocol 51 (AH) must be open both inbound and outbound, port NA

IPSec protocol is used for our VPN.

Part 1: Copy the File

Nortel Networks Extranet Access Client - Before you begin, you'll need three blank floppy disks: **DOWNLOAD EACH OF THE FOLLOWING** files and save them to their corresponding floppy disk.

If you are using floppy disks:

Disk 1 – [EAC465.zip](#), [EAC465.exe](#)

Disk 2 – [EAC465.zip](#)

Disk 3 – [EAC465.zip](#)

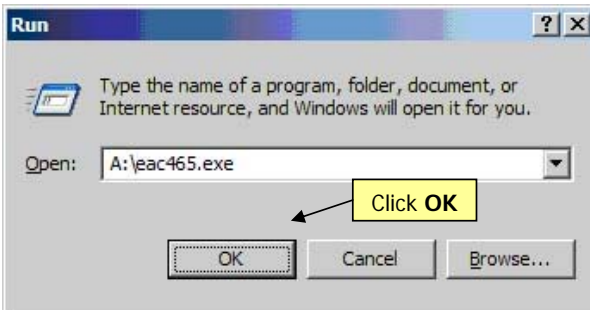
If you plan on coping files to CD:

[EAC465d.exe](#) (3.37MB)

IMPORTANT! Please uninstall any previous version of Nortel's EAC client before continuing with these instructions.

Part 2: EAC Initial Installation

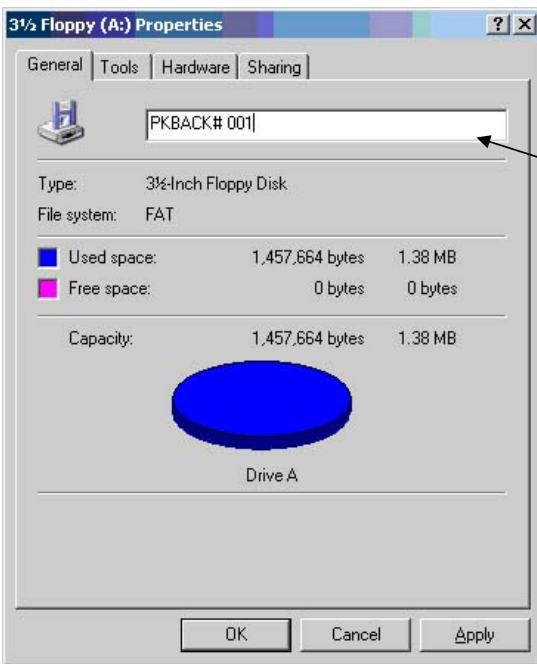
1. When ready to install, insert Disk 1 into your floppy drive, click on the **Start** button, select **Run**. When the Run dialog box appears type: **A:\eac465.exe**



NOTE: If you receive this error when you run eac465.exe from Disk 1, Click **Abort**.

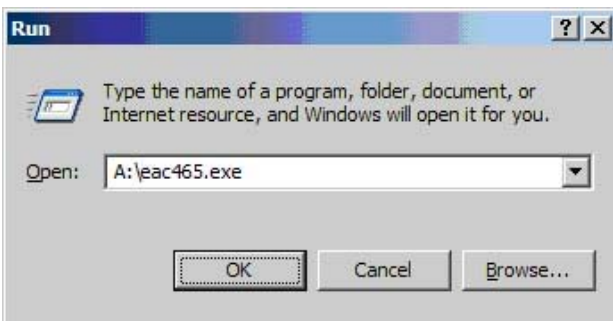


2. Go to **My Computer** or **Windows Explorer**:

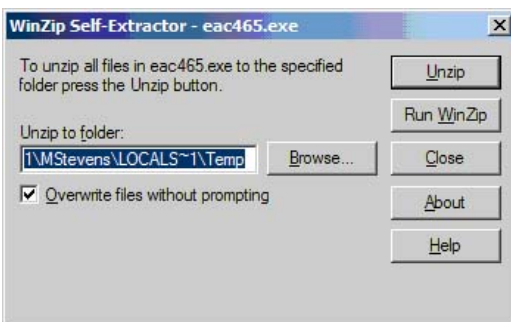


With Disk 1 in the A:\, right click the A:\ and click **Properties**. Type "**PKBACK# 001**" in the Label window and select **OK**. Do the same for Disk 2 and Disk 3. (Type **PKBACK# 002** and **PKBACK# 003**).

3. Go back to **Start**, and Click **Run**. Type in "**A:\eac465.exe**", and then click **OK**



4. Click **Browse** and select the **Desktop**, click **OK**, and then click **Unzip**.



5. You will be prompted for each disk. After the file completes, you will see the following:
Click **OK**, then click **Close** at the WinZip Self-Extractor

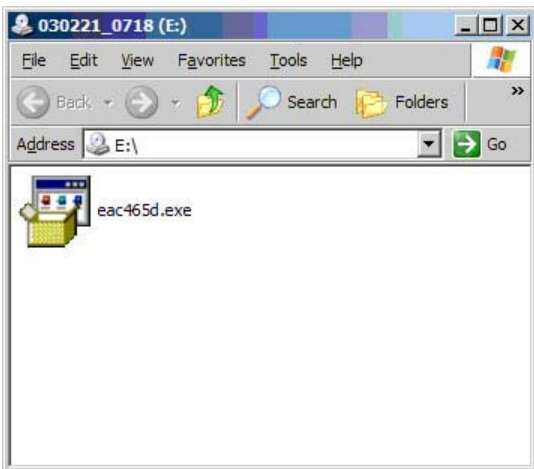


Part 3: Contivity VPN Client Setup

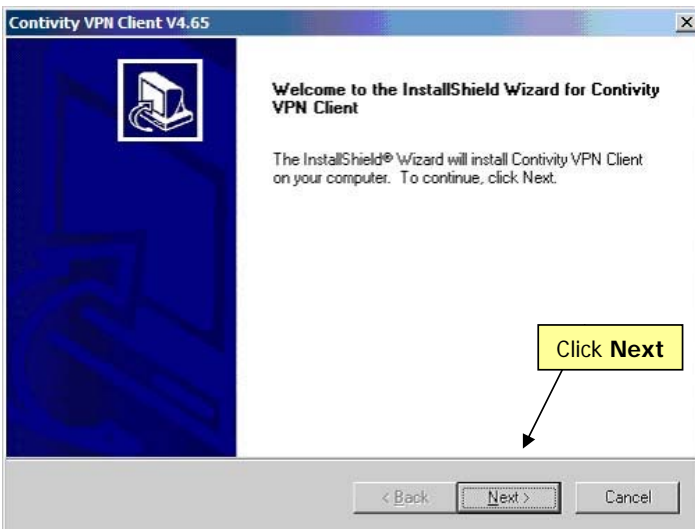
Double-click the **eac465d.exe** on your **Desktop** or from the default location.

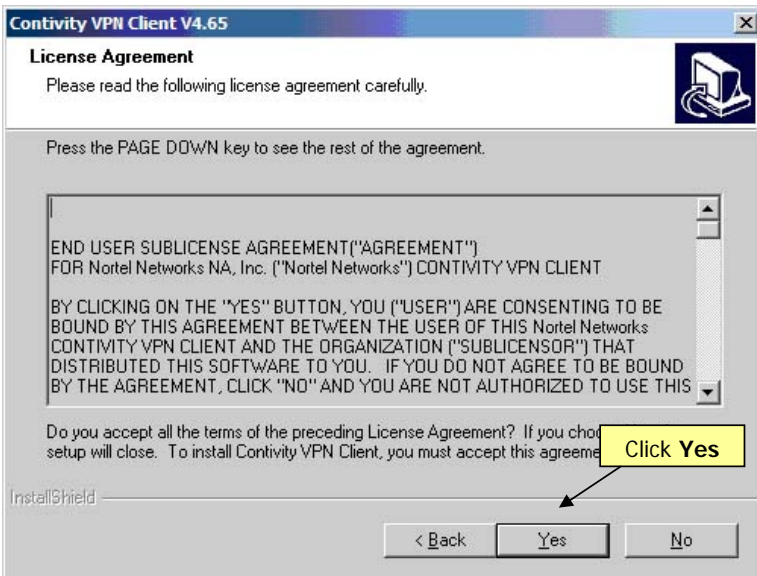
Note: If you are running the EAC 4.65 client from the CD, the following window will pop up:

6. Double-click the **eac465d.exe**

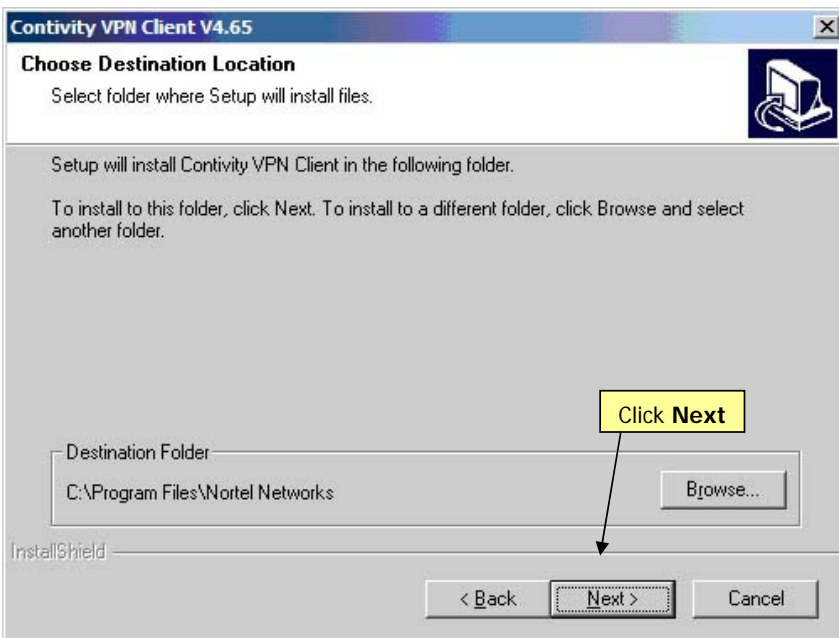


7. The **Contivity VPN Client 4.65** Dialog Box should now appear. Follow the screen shots, and accept the defaults at each step.





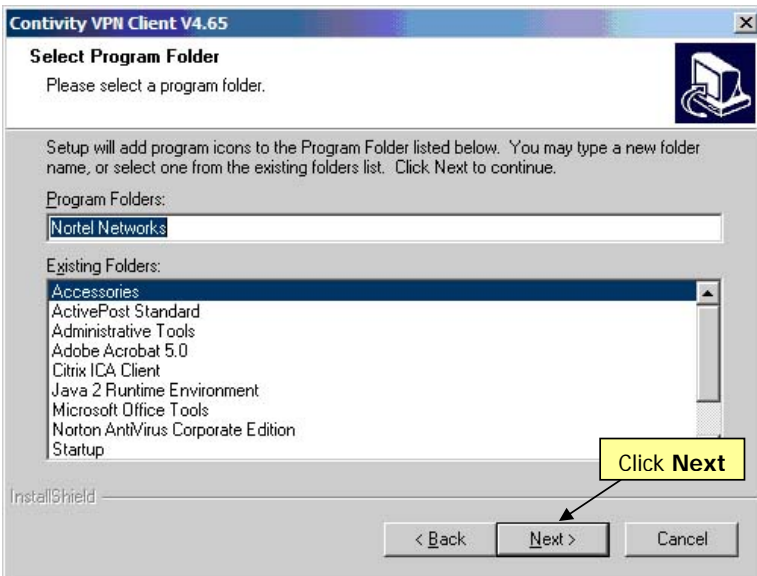
Note: If you receive the following message, Click **OK**.



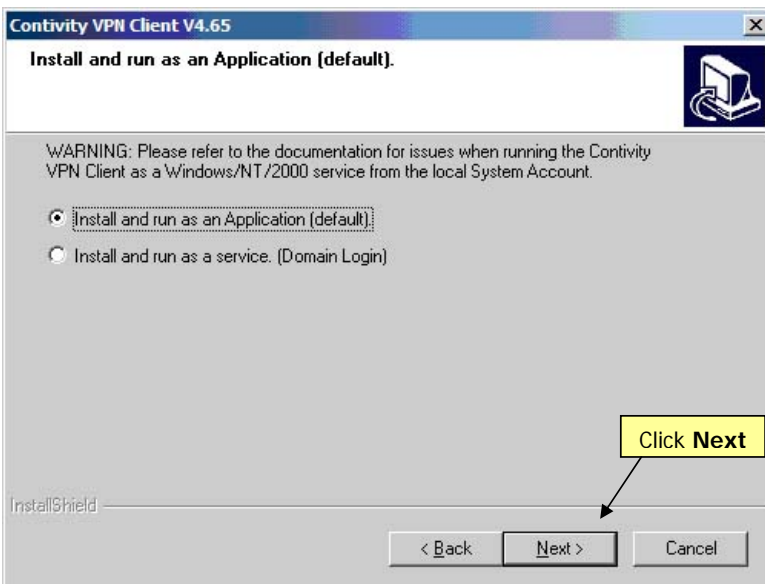
| Extranet Access Client Instructions

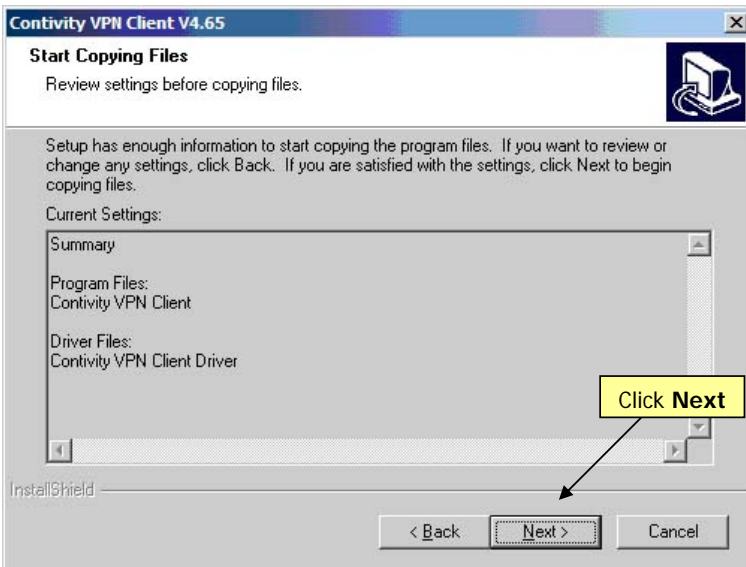
5 of 22

Deleted: 1



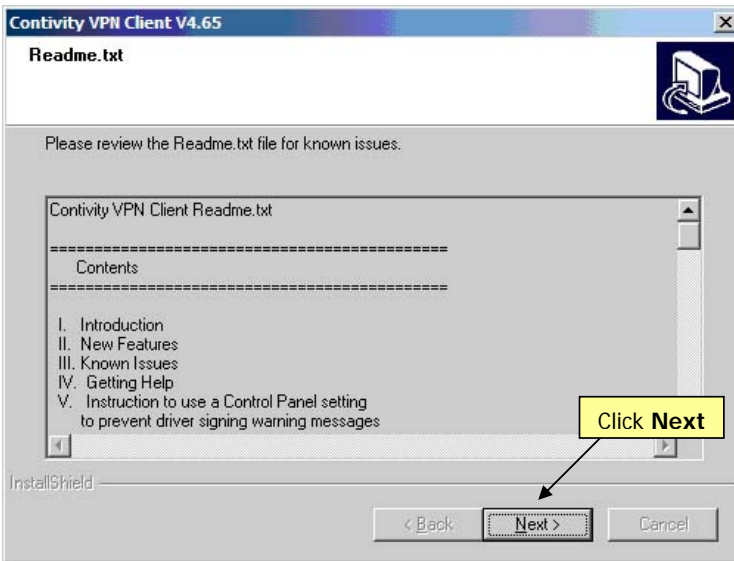
8. Make sure to “Install the client as an Application.”



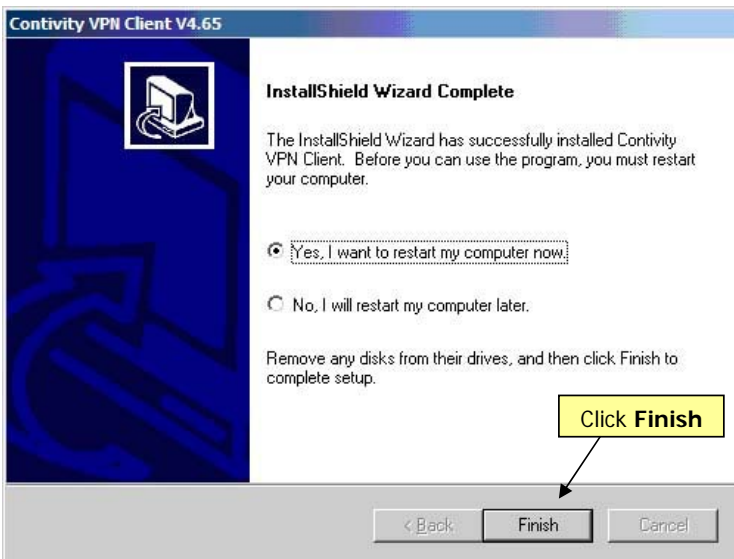


9. If you receive the below message, click **Continue Anyway**.





10. Make sure to select: **"Yes, I want to restart my computer now."**



Part 4: Contivity VPN Client Wizard

This step will run through a one-time setup for your Extranet Access Client. You will need to obtain your Primary and Secondary WINS Server Addresses, as well as your Domain name, from your servicing IRM or RSM staff if you have not already done so.

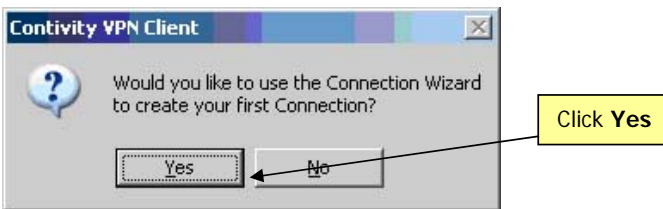
Quick Tip! If you are at work, you may retrieve your Primary and Secondary WINS Server addresses by doing the following from your SWIII:

- Go to a DOS Prompt
- Type ipconfig /all <enter>

11. Click **Start**, **Programs**, **Nortel Networks**, and then **Contivity VPN Client**.



12. When you click **Contivity VPN Client** the following dialog box will appear.



13. At the **New Connection Profile** dialog box type in a profile name, you may call it what you wish. But CGDN+ Extranet is recommended.

New Connection Profile

The Contivity VPN Client creates a secure connection to a remote network. This wizard will guide you through creating a connection profile that stores the information needed to connect you to a particular remote network.

Enter a name for this connection profile:
CGDN+ Extranet

Enter a description (optional):

Click Next

<Back Next> Cancel

14. The **Authentication Type** dialog box will now be displayed. Select the button beside "Username and Password".

Authentication Type

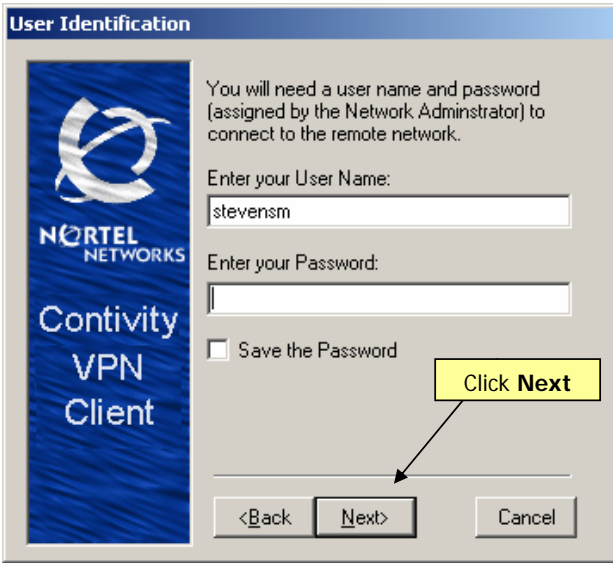
The Contivity VPN Switch can validate your identity based on a Username and Password, a Token Card, or a Digital Certificate (with or without smartcard). Please select the Authentication type for this connection. If you are unsure, select Username and Password.

☒ Username and Password
☐ Hardware or Software Token Card
☐ Digital Certificate and Smartcard

Click Next

<Back Next> Cancel

15. With the **User Identification** dialog box open, please enter your RAS token username. Be sure **NOT** to enter your password.



The 'User Identification' dialog box from Nortel Networks Contivity VPN Client. It features the Nortel logo and text on the left. The main area contains instructions: 'You will need a user name and password (assigned by the Network Administrator) to connect to the remote network.' Below this are two input fields: 'Enter your User Name:' with the text 'stevensm' entered, and 'Enter your Password:' which is empty. A checkbox labeled 'Save the Password' is unchecked. At the bottom are three buttons: '<Back', 'Next>', and 'Cancel'. A yellow callout box with the text 'Click Next' has an arrow pointing to the 'Next>' button.

16. At the **Group Authentication Information** dialog box select **Yes, I have a Group ID and Group Password**.



The 'Group Authentication Information' dialog box from Nortel Networks Contivity VPN Client. It features the Nortel logo and text on the left. The main area contains instructions: 'Besides a User name and Password, did your Network Administrator give you a Group ID and Group Password? If you are unsure, select No.' Below this are two radio button options: 'Yes, I have a Group ID and Group Password.' (which is selected) and 'No, I do not have a Group ID and Group Password.' Below the radio buttons are two input fields: 'Enter your Group ID:' with the text 'USCG' entered, and 'Enter your Group Password:' which is masked with 'XXXXXXXXXX'. At the bottom are three buttons: '<Back', 'Next>', and 'Cancel'. A yellow callout box with the text 'Click Next' has an arrow pointing to the 'Next>' button.

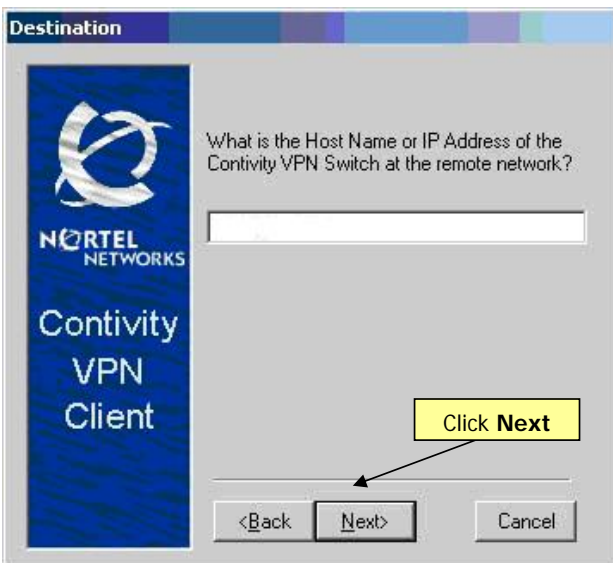
Group ID: **USCG**

Group Password: **extranet1790**

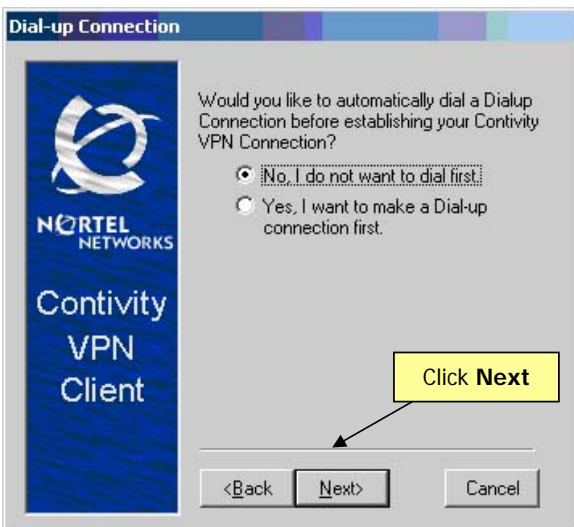
17. At the **Destination** dialog box enter one of the following Host Names based on your location:

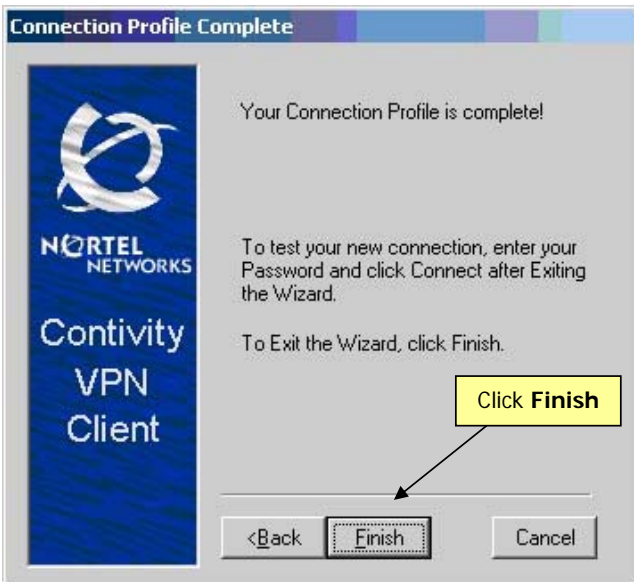
LANT Area: EASOSC1.uscg.mil
OR
EASFIN1.uscg.mil

PAC Area: EASALA1.uscg.mil

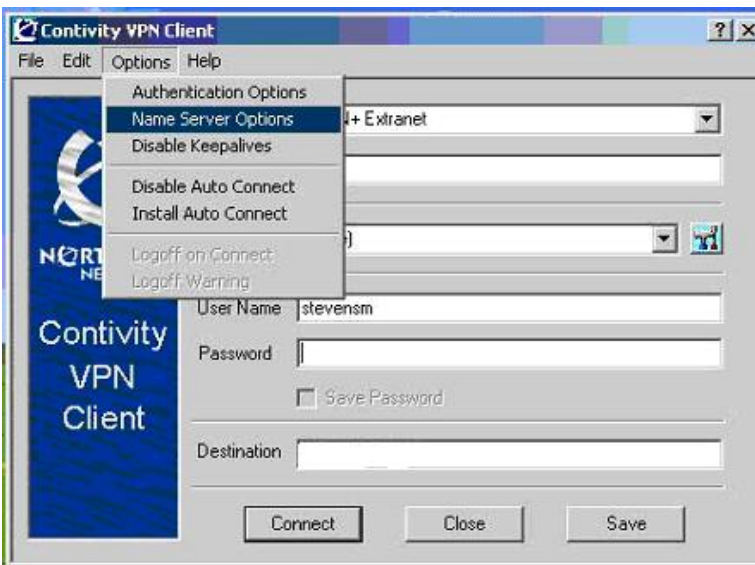


18. Select **No, I do not want to dial first.**

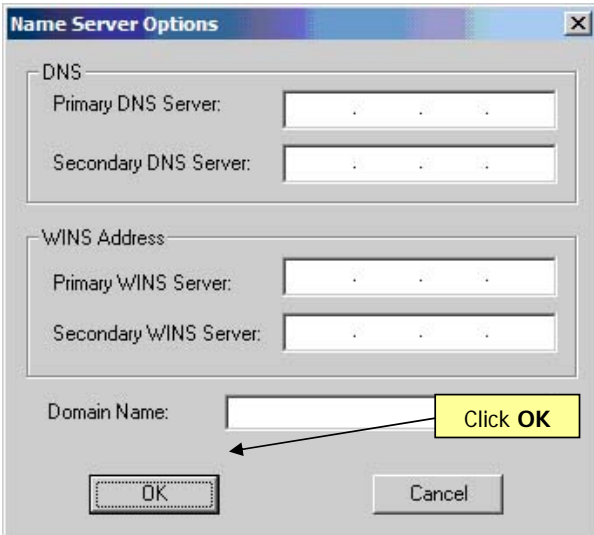




19. You should now see the following screen. Click **Options**, then **Name Server Options**.



20. With the **Name Server Options** dialog box open type your **Primary and Secondary WINS Server** addresses and your **Domain Name**.

The image shows a 'Name Server Options' dialog box. It has three sections: 'DNS' with 'Primary DNS Server' and 'Secondary DNS Server' text boxes; 'WINS Address' with 'Primary WINS Server' and 'Secondary WINS Server' text boxes; and 'Domain Name' with a text box. At the bottom are 'OK' and 'Cancel' buttons. A yellow callout box with the text 'Click OK' has an arrow pointing to the 'OK' button.

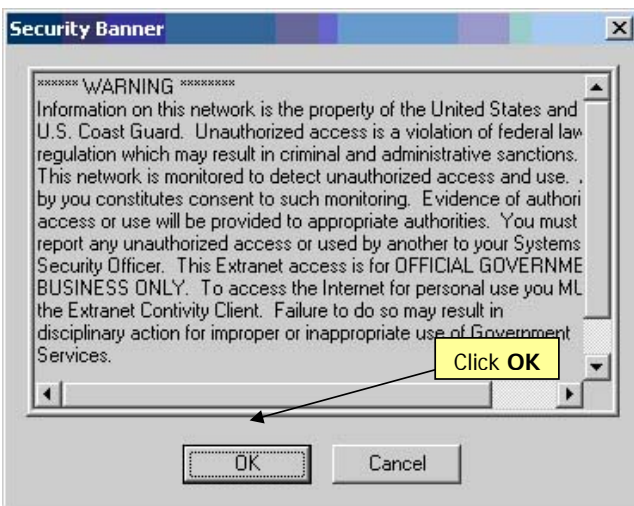
Note: You will need to connect to your ISP before connecting through Extranet. If you have a cable modem or ISDN, you should already have an established connection.

21. At the main **Contivity VPN Client** dialog box Click **Save**

22. Next, type in your RAS password. Then push the arrow on the token and append your password with the six digits that displays. Then click **Connect**

The image shows the 'Contivity VPN Client' dialog box. It has a menu bar with 'File', 'Edit', 'Options', and 'Help'. On the left is a blue sidebar with the Nortel Networks logo and the text 'Contivity VPN Client'. The main area contains fields for 'Connection' (a dropdown menu showing 'CGDN+ Extranet'), 'Description', 'Dialup' (a dropdown menu showing '(None)'), 'User Name' (containing 'stevensm'), 'Password', a 'Save Password' checkbox, and 'Destination'. At the bottom are 'Connect', 'Close', and 'Save' buttons.

25. You should now see the **Security Banner**. When it is displayed, you are connected to the CGDN.



26. You may check **Do not show this message in the future**.



Part 5: Changing your PIN (password):

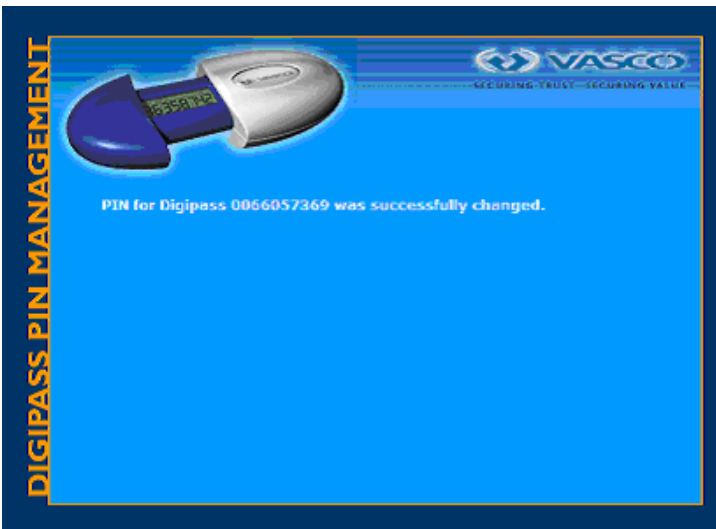
27. Each user is assigned an initial PIN. This is a strong password that can be changed by going to the following website: <http://radius01.osc.cgdn.uscg.mil/scripts/changepin.html>

Note: Users are no longer forced to change their password upon initial login.

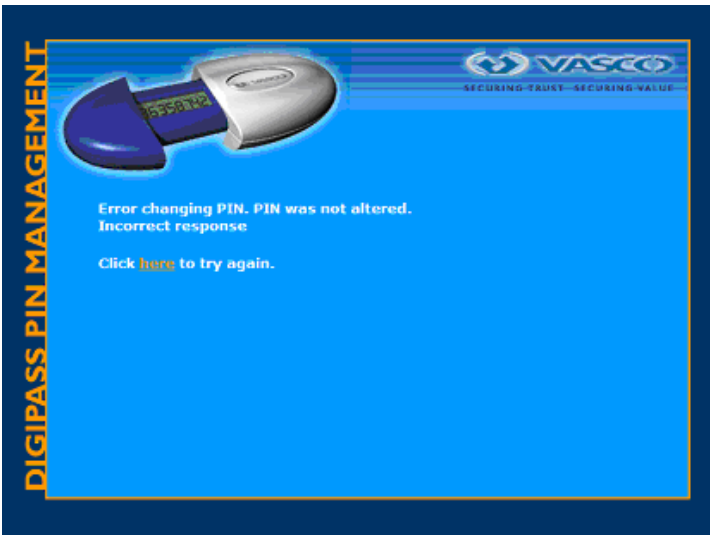
28. Type in your token **User Name**, and then your **Old PIN** (initial password). Type in a **New PIN**. This will be your new token password. It must be exactly eight characters and should be alphanumeric. Type in the PIN again to **Confirm New PIN**. Hit the arrow on the token and type in the six digits in the **Digipass Response** field, and then click **Go!**



You should receive the following message when the PIN has been changed successfully.



If you receive the following message, please try again. If you continue to experience problems changing your PIN, please contact OSC-Customer Support at 1-800-821-7081 for assistance.



29. Now that you are connected to the CGDN and have changed your password you may access your SWIII desktop. You will need to load your ICA CITRIX client or Remote Desktop Connection.

NOTE: Citrix is supported by your local ESU.

Part 6: Configuring the Remote Desktop Protocol

NOTE: If your user account is CAC logon enforced then complete the attached addendum for Activ Client 6.1 home use install. **NOTE:** The Remote Desktop Protocol is supported by TISCOM. Please contact the TISCOM Helpdesk at: 1-800-847-2479 Option 3 (0630-1700)

Deleted: 1
1

30. Click **(Start, Programs, Accessories, Communication)** and click the Remote Desktop Connection icon. The following window will be displayed. Click **Options**.

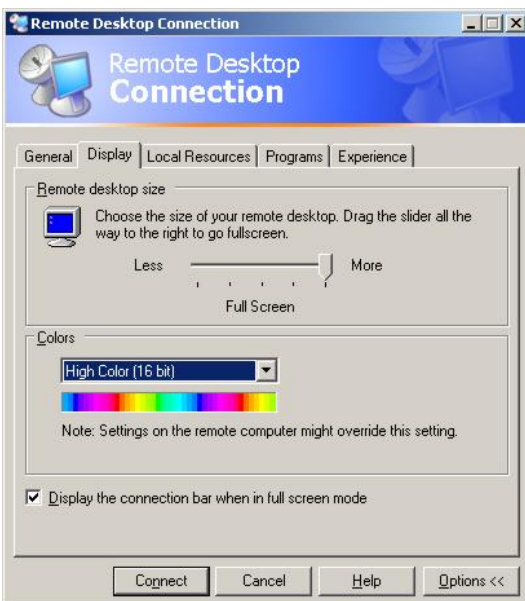


31. Ensure you have the **General** tab selected and enter the **IP address** or **Computer Name** of your SWIII. You can enter your SWIII username, password and Domain name but if your account is CAC login enforced then do not enter username, password,

Deleted: .



32. In the **Display** tab you will choose the size and color depth of the RDP session. The settings shown above are the preferred settings. Keep in mind the higher color (number of bits) will slow your session down. Once complete click on the **Local Resources** tab.

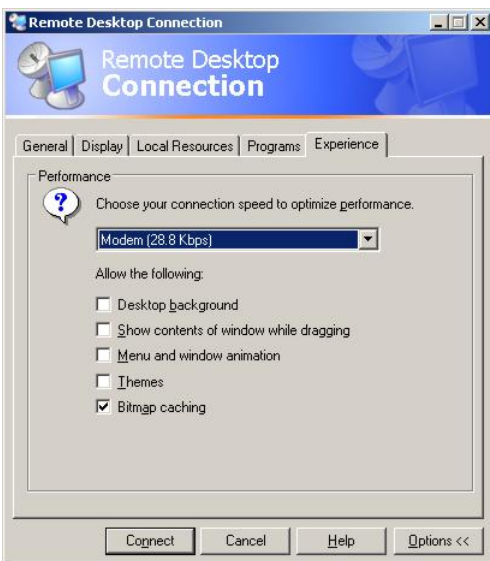


Deleted: 1

1. In the Local Resources tab choose the following settings. Using sounds will slow your remote session. For **Remote computer sound select:** Do not play. For Local devices you can select **Disk drives** and / or **Printers** to make these devices accessible with you remote desktop session. This will allow you to see the local devices of you SWIII form any of the applications being used during the remote desktop session. Click the **Experience** tab.



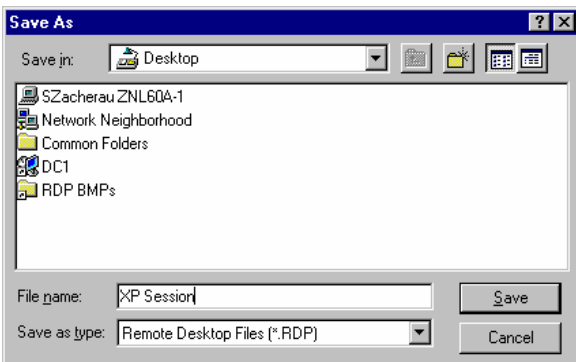
2. Ensure the **Bitmap caching** selection is checked; selecting other settings will slow your session down. Click the **General** tab.



35. Click **Save As...** underneath **Connection Settings**.

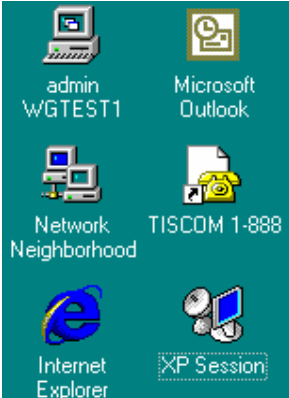


36. The **Save As** window will be displayed. In the File name field fill in a descriptive name for the RDP client configuration (i.e. Remote Desktop or XP Session) and in the **Save in** field click the drop down arrow and scroll to the top and click the **Desktop**. Click the **Save** button. This will create a shortcut on your desktop that you will be able to double click after you have connected to the CGDN.

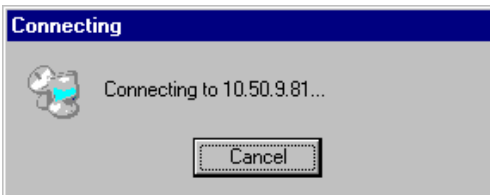


Part 7: Establishing a Remote Desktop Connection

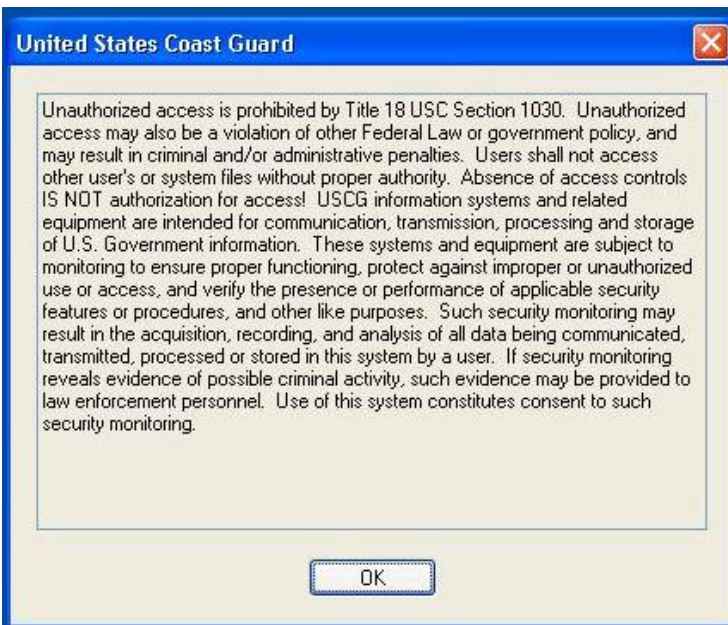
37. Connect to the CGDN+ using your Remote Access solutions.
Start the RDP Client by double clicking on the shortcut you created on your desktop (i.e. Remote Desktop or XP Session).



38. The RDP client will begin making a connection to your workstation.



39. Click OK to acknowledge the Unauthorized Access Warning.



40. Once the workstation is found you will be need to logon with your Domain credentials just as if you were at work. If you are logging on with your CAC then once you click OK to acknowledge the unauthorized access banner you will then need to remove and re-insert your CAC to bring up the unauthorized banner again and click "ok" but this time you will be prompted with a pin box where you can enter your pin number.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 40 + Alignment: Left + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25"

Deleted: 40.

Deleted: Once the workstation is found you will be need to logon with your Domain credentials just as if you were at work.



Deleted: 1