

Chapter 3

How to Logon

3-1. General.

a. To ensure you have accurate information in the Leads-Reports application and/or the TOS, you must logon properly and create a secure connection with your ISP. The following steps will demonstrate the process for connecting to your ISP and creating a secure tunnel through PERMIT/Client. Once connected you may replicate with Leads-Reports, review different actions and reports on the TOS, and check your e-mail.

b. There are three steps to establishing the connectivity and replicating. They are:

- (1) Connect to the network.
- (2) Establish a secure connection.
- (3) Extended authentication.

c. You will need:

- (1) Your NT user ID and password.
- (2) Your PKI disk.
- (3) Your PKI password.
- (4) Your ISP user ID and password.

✓ If you do not have any of these, contact your Rctg Bn IMS.

3-2. Connect to the network.

a. After successfully logging on your laptop with your NT logon ID and password you are now ready to get connected. You first need to connect to your ISP. You must have your computer connected to a telephone line to dial-in and then click the **Dial-Up Networking** icon on your desktop.



b. You will need to select the local area from the **Phonebook entry to dial** drop-down arrow. It starts by country, then state, and then city. Make sure that the entry you select is not a long distance call. If there is no listing under the drop-down arrow for your area, contact your Rctg Bn IMS to determine what number you should use. You will need to delete the prefix and area code to make it a local number. Click the **Dial** button.

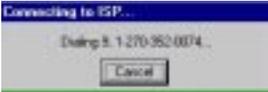


c. Your ISP user ID and password will be provided by your Rctg Bn IMS. You will need to enter your ISP **User name** and **Password**. Your user name will always start with **internet.gv111._____**. Now you need to enter your **Password**. Your password is case sensitive and is assigned to you and is only used for connecting to your ISP. Notice that the password is entered as asterisks.

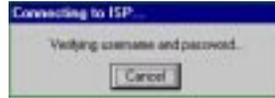
d. You do not need to fill in the **Domain** window, so click **OK**.

USAREC Pam 601-32

✓ Notice that you cannot save your password for later use.

e. You  are now connecting to your ISP.

f. The system will verify your user name and password.



g. The system then registers your computer on the network and you will get a message stating that you are connected.

h. If you get an error message try to resolve by doing the following:

(1) ☒ Error 5. Make sure the user name and password are entered correctly and remember that it is case sensitive. Make sure you have nothing entered in the Domain field. If you continue to get the error your account may be locked. Contact your Rctg Bn IMS or the SOC for further assistance.

(2) ☒ Error 633. This usually means that you didn't hang up from the previous connection. Right mouse click on the ISP icon and select hang up.

(3) ☒ Error 678 or 692. Make sure the user has the correct telephone number to dial the ISP.

(4) ☒ Error 718. Make sure the Domain field is blank. If there is anything in the Domain field the connection will not be made.

(5) ☒ Error 734. Right mouse click on the ISP icon and select Edit Entry and Modem Settings. Next select the Security Tab and on the tab, select **Accept Any Authentication Including Clear Text**, and hit **OK** to save changes.

3-3. Establish a secure connection.

a. To get a secure connection, an application called PERMIT/Client was installed. This application creates a secure connection through your local ISP to ensure the information you are transmitting or receiving cannot be seen by unauthorized users. You must have a secure connection to replicate, send projections, and view reports through the TOS. This secure connection is also required to access your USAREC e-mail account and the USAREC Intranet.

☒ **“WARNING”** WHEN YOU RECEIVED YOUR PKI DISK YOU SIGNED A DOCUMENT THAT STATED THAT YOU **WOULD** PROTECT YOUR PKI DISK AND NOT SHARE IT. DO **NOT** SHARE YOUR PKI DISK. DO NOT LOAN YOUR PKI DISK TO ANYONE. TREAT YOUR PKI DISK AS IF IT WERE **YOUR PERSONAL CREDIT CARD!** THE PKI IS **YOUR** “SIGNATURE.” IT IS YOUR IDENTITY. IF AN INAPPROPRIATE ACTION IS DONE ON THE SYSTEM OR ON THE INTERNET, IT WILL BE ATTRIBUTED BACK TO **YOU!**

b. Once this connection message box has disappeared, you need to position your mouse pointer over the task bar at the bottom of your screen. If your task bar is hidden, position your mouse at the bottom of your screen and the bar should appear.



c. Notice the two icons highlighted in the system tray of the task bar. Once you are connected to the ISP, you will see the icon on the right that looks like a small telephone. Sometimes this icon may be flashing blue in the background. The icon flashes blue to indicate that a connection has been made and that you are receiving data. The icon on the left is the PERMIT/Client icon.

d. Normally the PERMIT/Client icon will be showing a red T with a strikeout symbol. This is showing that the application is currently disabled. To create a secure connection you will be required to enable the application and login. In order to accomplish this you will need to get to the **PERMIT/Client** main menu. Right click on the **PERMIT/Client** icon to show the main menu.



e. This is the **PERMIT/Client** menu. Notice the green highlighted area. This identifies the location for your connection. The Tier your computer will go through depends on where you are located. As a user, you should not change this setting. If you do change it, you will not receive a valid connection.



f. If there is a checkmark by **Disable**, click on **Disable** one time to enable this program. If there is no checkmark the application is already enabled and you should go to the next step.



g. Now you need to login. Note that the strikeout symbol is gone and the **PERMIT/Client** icon is now enabled.



h. Right click on the **PERMIT/Client** icon. Click **Login User**.

i. Before selecting the **Browse** button, you must insert your PKI disk. A PKI disk should have been issued to you by your Rctg Bn IMS. You can use your PKI disk to access only your information. Your PKI disk and password should be treated like a credit card. No one should know your password. Click **Browse**.

✓ Do not share your PKI disk.



j. Click on your ID certificate. The certificate should now show in the file name field. Click **OK**. Do not use your e-mail certificate. You cannot replicate successfully using this certificate. You may need to change the drive from C: to A: before you can find the certificate.

k. Enter your PKI password. Again, notice that the password is encoded as asterisks. Click **OK**. The system will now create a secure tunnel for you.

✓ If you lose your PKI disk or forget your logon ID or password contact your Rctg Bn IMS immediately.



3-4. Extended authentication.



a. The Extended Authentication window opens when you have to verify the computer's login information. It will open with the **UserID** filled in based on the NT logon. Enter your **Password**. This password is the same password as your NT logon password. Click **OK**.



b. The system will then ask you to wait while it authenticates and creates a Subnet. You do not need to click **OK** because the system will automatically forward.



c. Once you are authenticated and a secure connection has been made, the green T will show a lock symbol around it.

d. If there is a problem getting this secure connection, you may need to try Reload Policy under the **PERMIT/Client** menu. This is only necessary if after a few minutes you do not get a secure connection. This will search another path for you to get a secure connection. To do this task, right click on the **PERMIT/Client** icon and then click on **Reload Policy**. In most cases this will establish a secure connection. If you still cannot get a secure connection, check to ensure you are still connected to your ISP. You may need to start the process over again before you can get a secure connection.



✓ Remember that you cannot complete replication without a secure connection.

e. The Asset Management Agent program will run the first time you dial-in. It does this each time you restart your computer. It will check your hard drive to ensure all required programs and files are installed. It will also check for and report any unauthorized programs that you have installed to your System Administrator. There is no problem with using your laptop while Asset Management Option (AMO) is running; however, using applications that require the network (i.e., Replication, e-mail, or Internet) may cause these applications to run slower due to the amount of resources being used by AMO. Normally, AMO will take around 1 to 3 minutes to run and should be allowed to complete its operation prior to using other applications that would use the network.



✓ Remember, once you have completed all your actions that require a connection to your ISP, you need to disconnect and disable your **PERMIT/Client** application and ISP connection. You only have so many hours per month, do not waste them being connected needlessly.