



*That guilt shall not escape,  
nor innocence suffer.*



There are two methods currently available for connectivity from LEA (law enforcement agency) to TBI headquarters for the purpose of accessing the Fusion Center systems (for the purpose of this connectivity, there is no difference between accessing CRMS or TNCop.) Each of these methods provides a secure and encrypted path for criminal justice data. LEAs requiring connectivity should first determine the method most suited to their location and then refer to the appropriate section in this document.

### **Method 1: SecuRemote Client VPN Software**

This method is suitable for user stations with public Internet access. This method requires the installation of Checkpoint VPN-1 SecuRemote software (available on a TBI web server) and a user account provided by TBI. The user account is only available after all appropriate training and paperwork have been completed.

### **Method 2: TIES network access (State T1 circuit with Cisco PIX device)**

This method is preferred, but requires that stations/servers reside on a LAN segment that has access to the LEA's TIES network through the PIX device.

# CONNECTIVITY TO THE FUSION CENTER – CRMS AND TNCOP

## SecuRemote Download:

### SecuRemote instructions for outside access to the TNCop and CRMS

Your computer uses a program called SecuRemote to provide a VPN (Virtual Private Network) encryption tunnel from the outside into TNCop and CRMS. This program allows you to access the TNCop, CRMS, and Sex Offender Registry (SOR).

The SecuRemote software link:

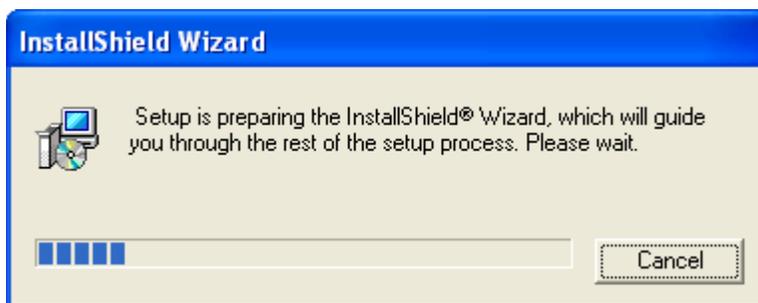
To download click this URL: [SecuRemote.exe](#)

Or copy and paste to your web browser the data below:

[http://www.ticic.state.tn.us/SEX\\_ofndr/SOR/securemote.exe](http://www.ticic.state.tn.us/SEX_ofndr/SOR/securemote.exe)

You may either Save or Open the file. If you select Save be sure to note the location where you are saving it and when the download is complete double click the file to run the installer.

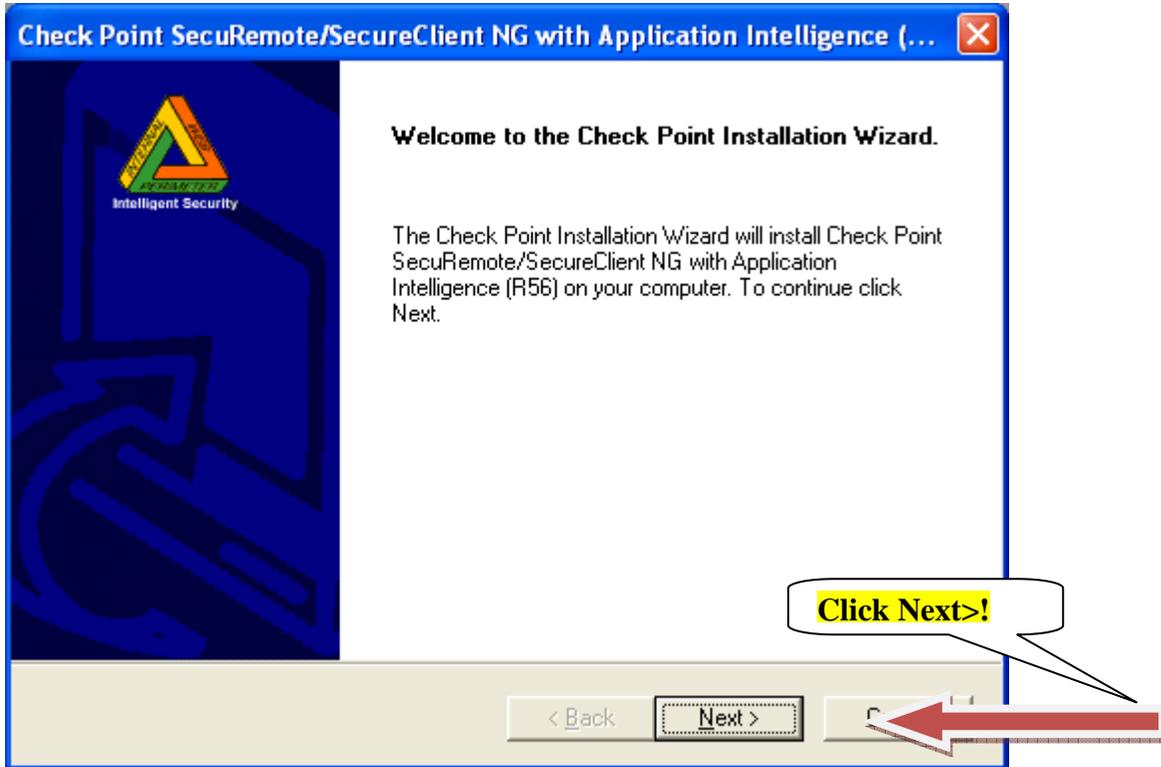
You will see the following screen.



# CONNECTIVITY TO THE FUSION CENTER – CRMS AND TNCOP

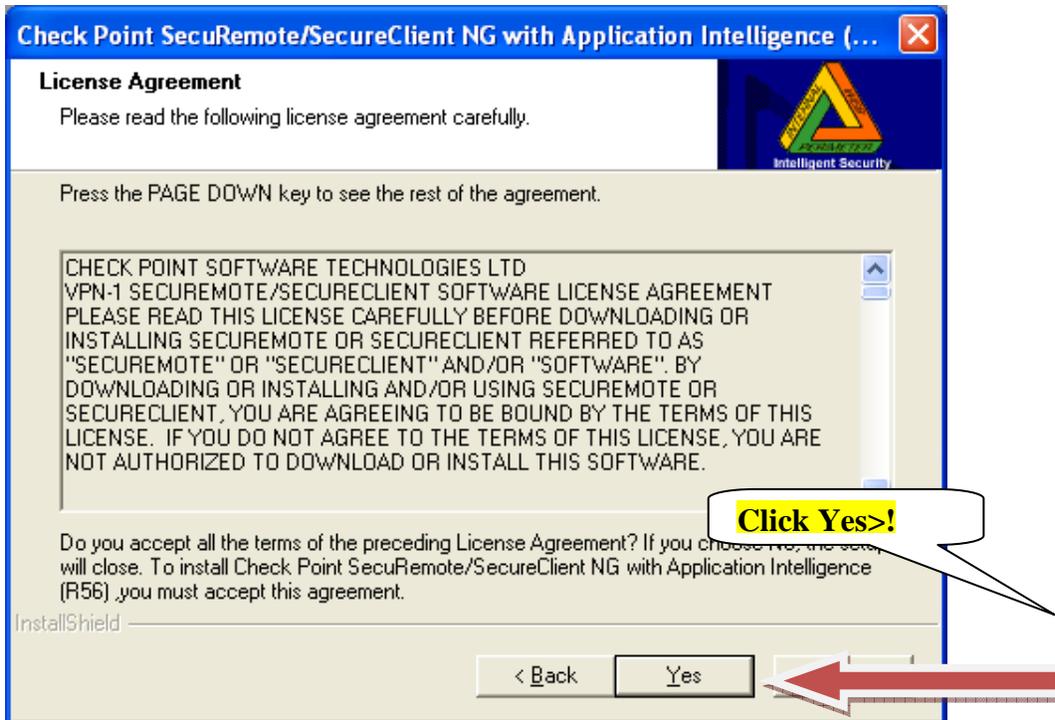
## Welcome to Check Point Installation Wizard

Click the **Next** button.



# CONNECTIVITY TO THE FUSION CENTER – CRMS AND TNCOP

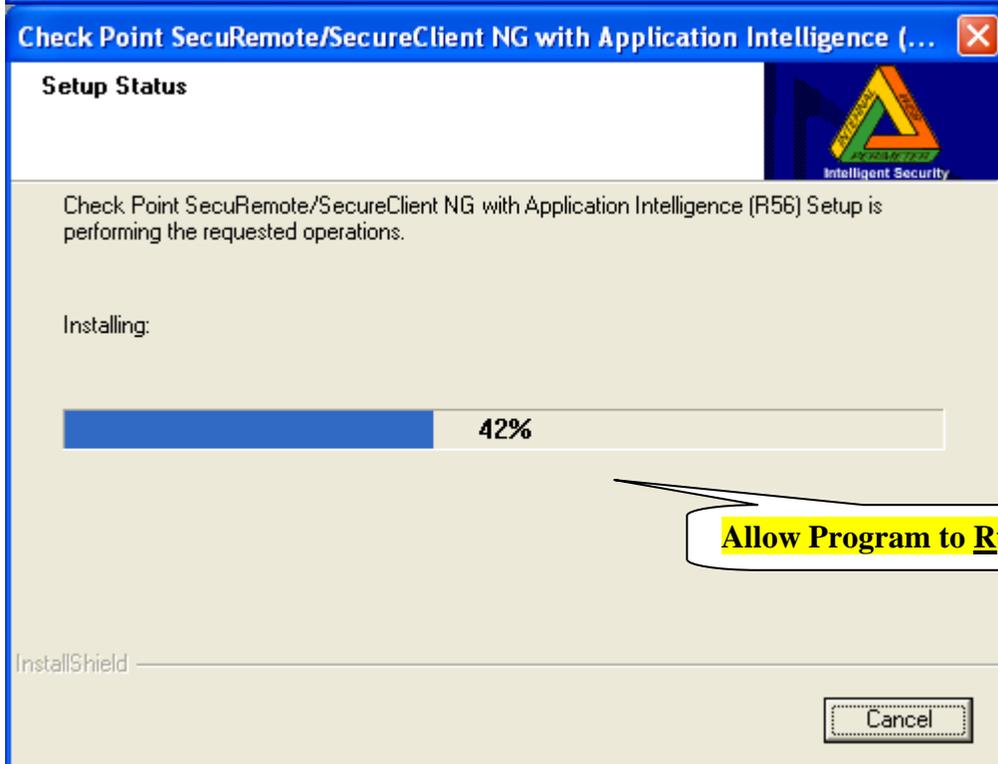
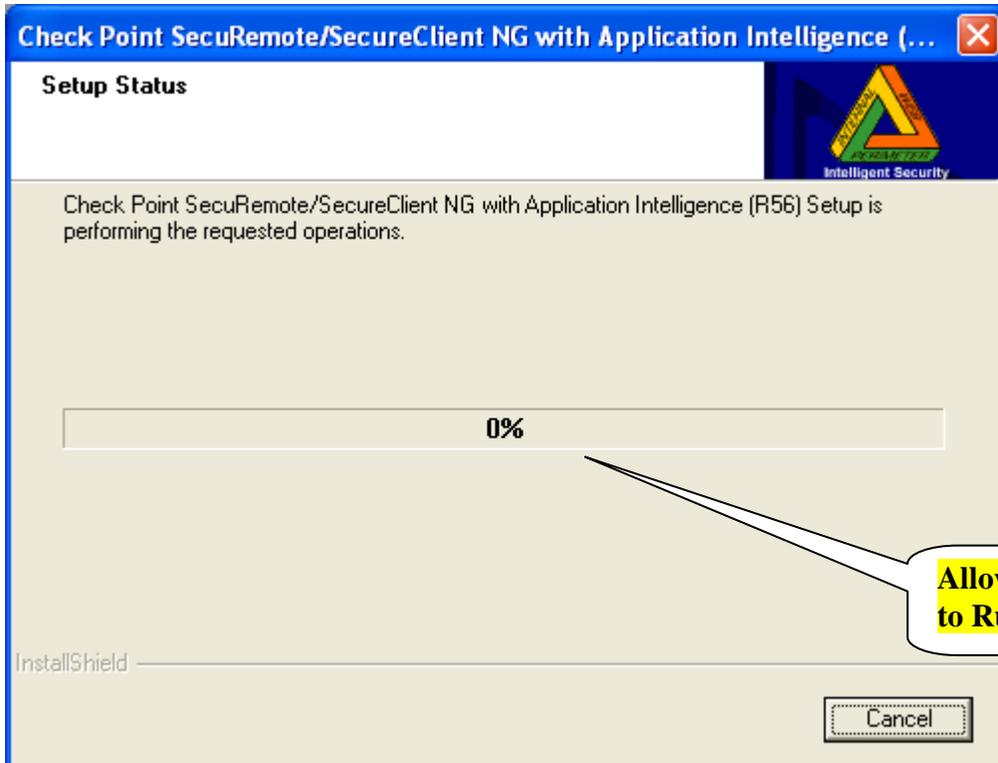
Click the **Yes** button.



After clicking on the **Yes** option you will see a new screen. This is the install screen for SecuRemote.

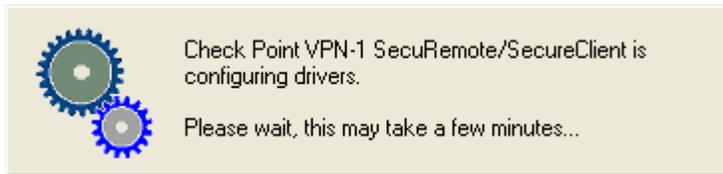
# CONNECTIVITY TO THE FUSION CENTER – CRMS AND TNCOP

Allow this program to run.



## CONNECTIVITY TO THE FUSION CENTER – CRMS AND TNCOP

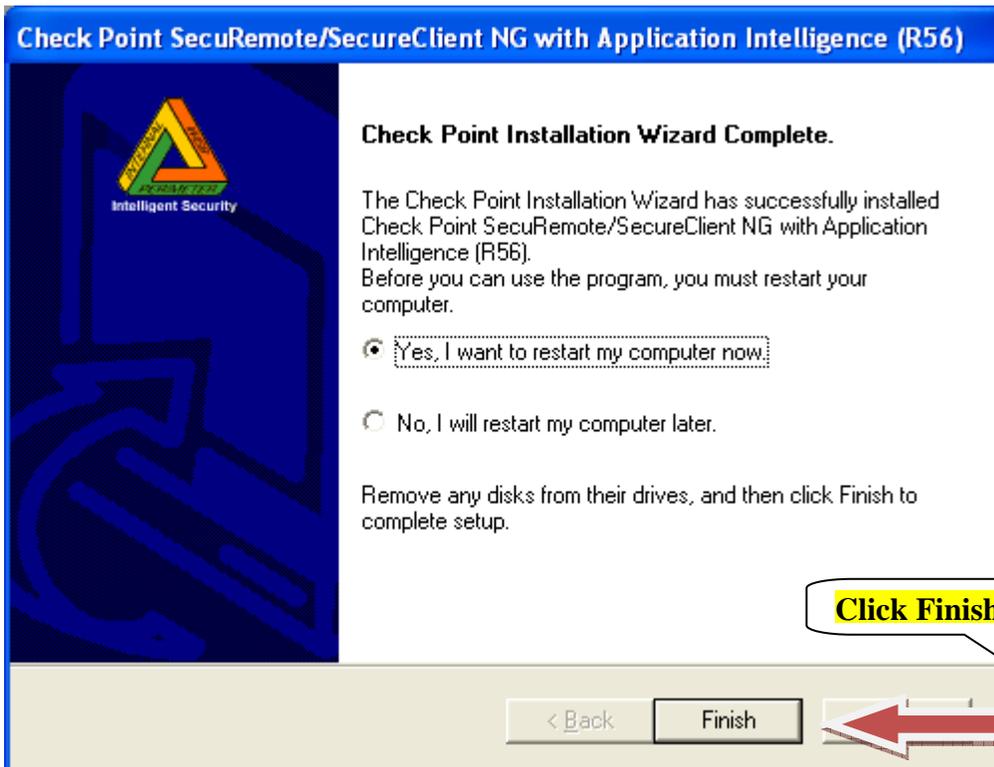
Upon completion of the program to run you will see the below screen, **allow the process to run.**



You may see this screen; if not then proceed with the **Finish** Option below.

Insure the Radio button is clicked on the **“Yes, I want to restart my computer now”** as shown below.

**Click Finish.**



Upon completion of the SecuRemote install and the computer restarted a Gold key in the bottom right corner of your screen's taskbar will appear.

## CONNECTIVITY TO THE FUSION CENTER – CRMS AND TNCOP

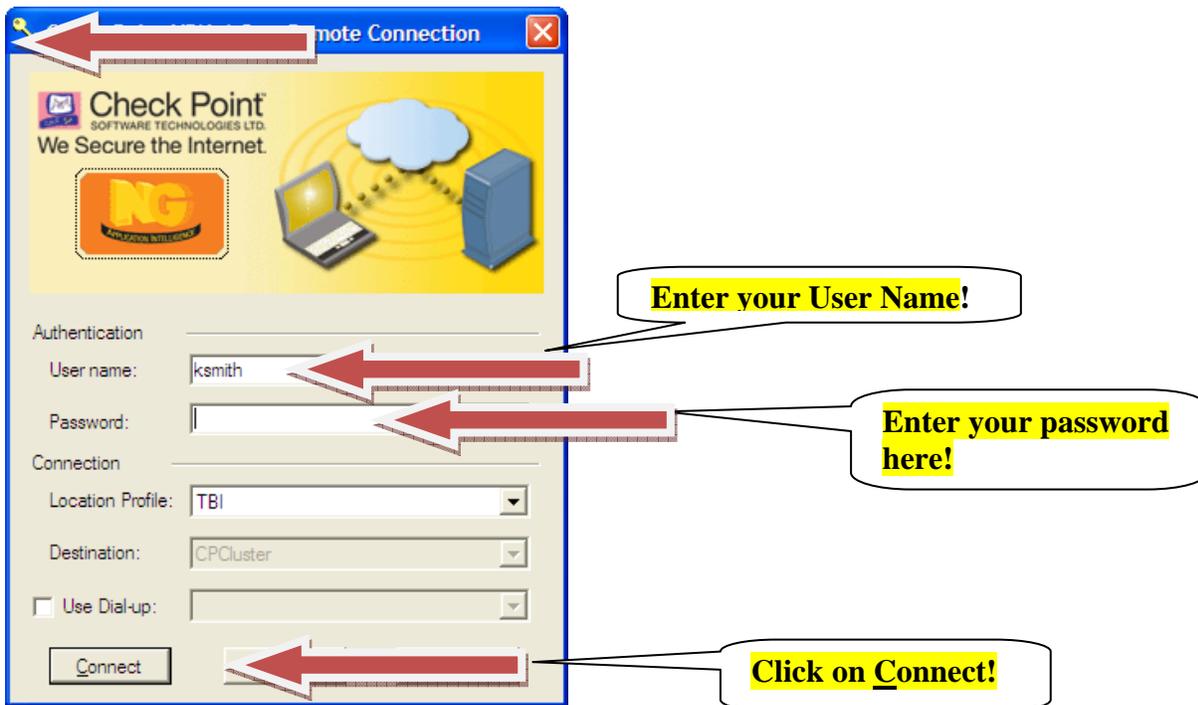
Once your computer has restarted you may receive a message; **SecuRemote is going to update the following...** TBI, select Cancel on this screen.

### Method 1: SecuRemote Client VPN Software

#### NOTE:

**SecuRemote may be installed on any computers that need access.**

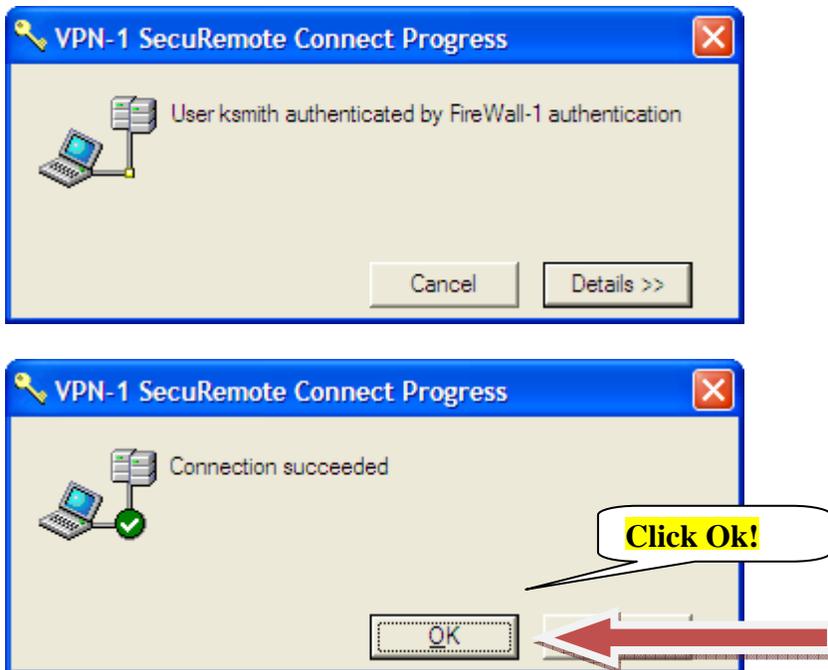
To activate your SecuRemote client, double click on the SecuRemote icon located in the lower right hand corner of your desktop, in the system tray. This will bring up the VPN-1 SecuRemote© Connection screen.



Enter your SecuRemote username and password and click on the Connect button to connect.

It will authenticate and you will receive the following progress screens.

## CONNECTIVITY TO THE FUSION CENTER – CRMS AND TNCOP



Once successful, SecuRemote will minimize itself back to the task bar, and it will give you a key icon , notice this is without the red x , to let you know that it is connected and that the session is encrypted.

### **NOTE: For RMS agencies only!**

Currently SecuRemote has a default disconnect of Seven (7) days. In order to prevent loss of transmission of data a person MUST physically disconnect and reconnect to SecuRemote twice a week.

**TBI** is reviewing hardware options to eliminate the problems associated with this disconnect timeout. Until another option is identified a manual disconnect/reconnect is recommended on Monday and Friday to avoid disconnection from TBI and subsequent delays in uploads.

To disconnect from SecuRemote just double click/or right click on the key icon  and select disconnect. You will get a pop up window asking if you are sure and just click YES.

## **SecuRemote instructions for: Disconnecting and Connecting!**

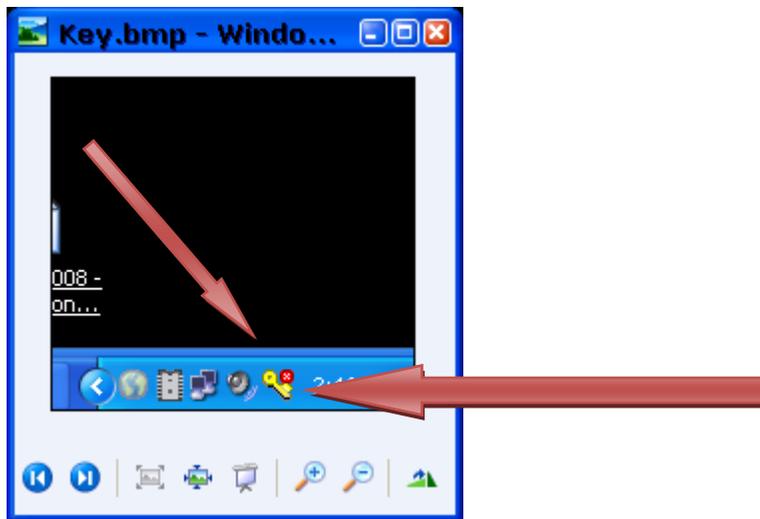
To prevent the time out issue with connection to SecuRemote you must disconnect and reconnect weekly. The process to perform this action is to manually input the commands on the server.

Below is the procedure to connect and disconnect from SecuRemote.



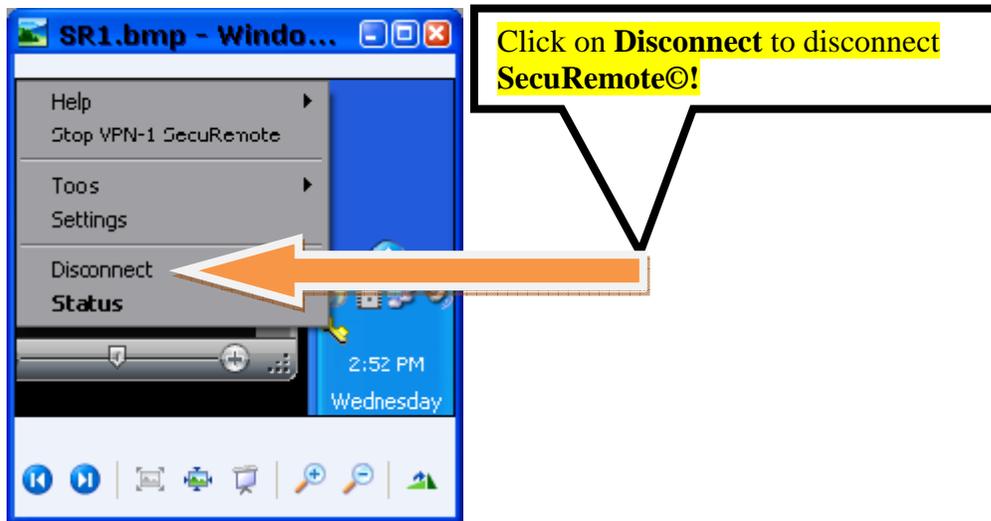
Located in the lower right hand corner of your desktop, in the system tray is the key.

Click the Gold Key to bring a menu up as shown below.

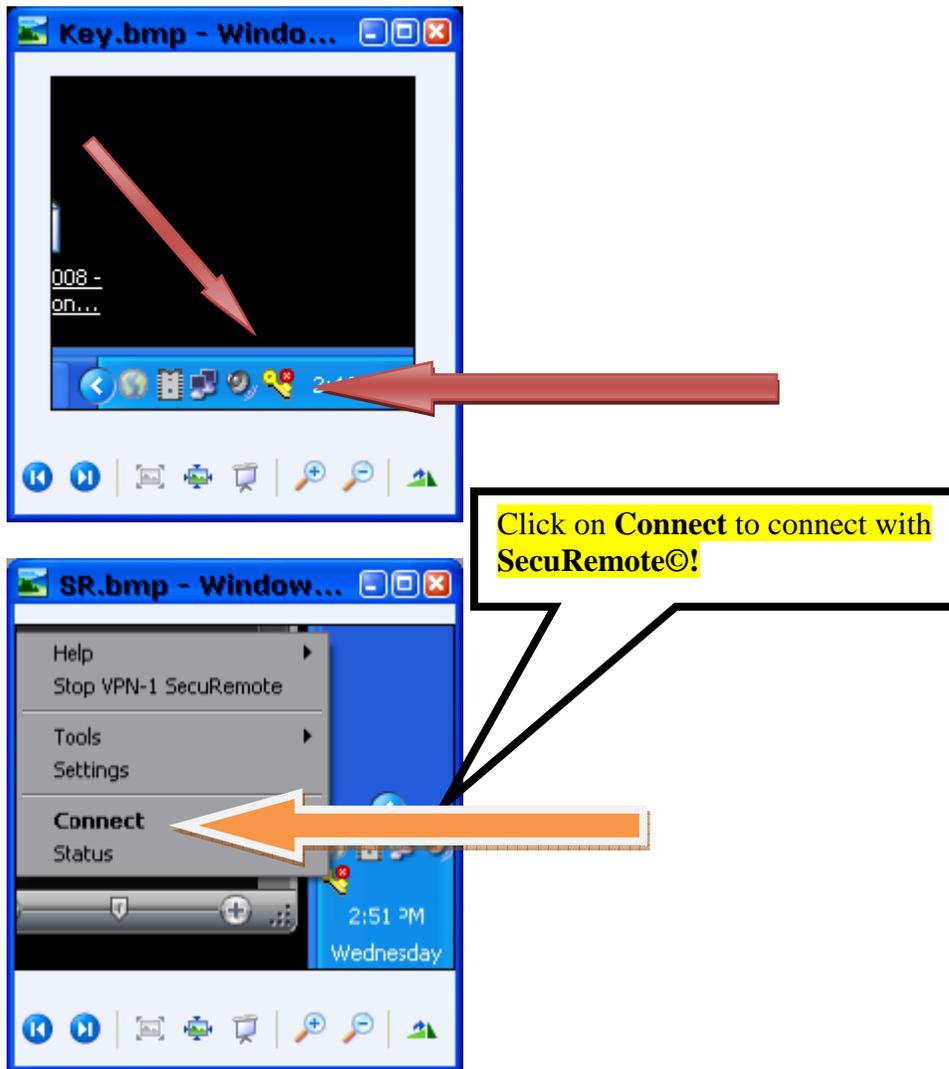


Clicking on this key will bring a menu up as shown below.

# CONNECTIVITY TO THE FUSION CENTER – CRMS AND TNCOP



To reconnect, click on the key again.



## **Method 2: TIES network access (State T1 circuit with Cisco PIX device)**

- **This method is preferred, but requires that stations/servers reside on a LAN segment that has access to the LEA's TIES network through the PIX device.**
- **Accessibility to the TIES network will vary among LEA locations and thus must be determined by appropriate personnel within the LEA's support staff possessing networking expertise.**
- **Briefly, the accessibility to the TIES network is determined in large part by the IP address scheme associated with the stations/servers requiring access to the Fusion System versus the IP address scheme associated with the LEA's TIES network.**
- **If they are different then the feasibility of achieving connectivity using this method must be determined locally and is dependent upon the specific network configuration at that agency.**
- **Assistance with this determination may be provided by TBI IS staff, but the responsibility of implementation of the networking changes rests with the LEA.**