Security Admin

Version Alpha 8 Graphical User Interface Documentation

Introduction :

When a hacker compromises network security, **80% of the time**, that hacker is a company employee. Because of the devastating consequences of hacking attempts, network administrators need a way to monitor the users connected to the company network.

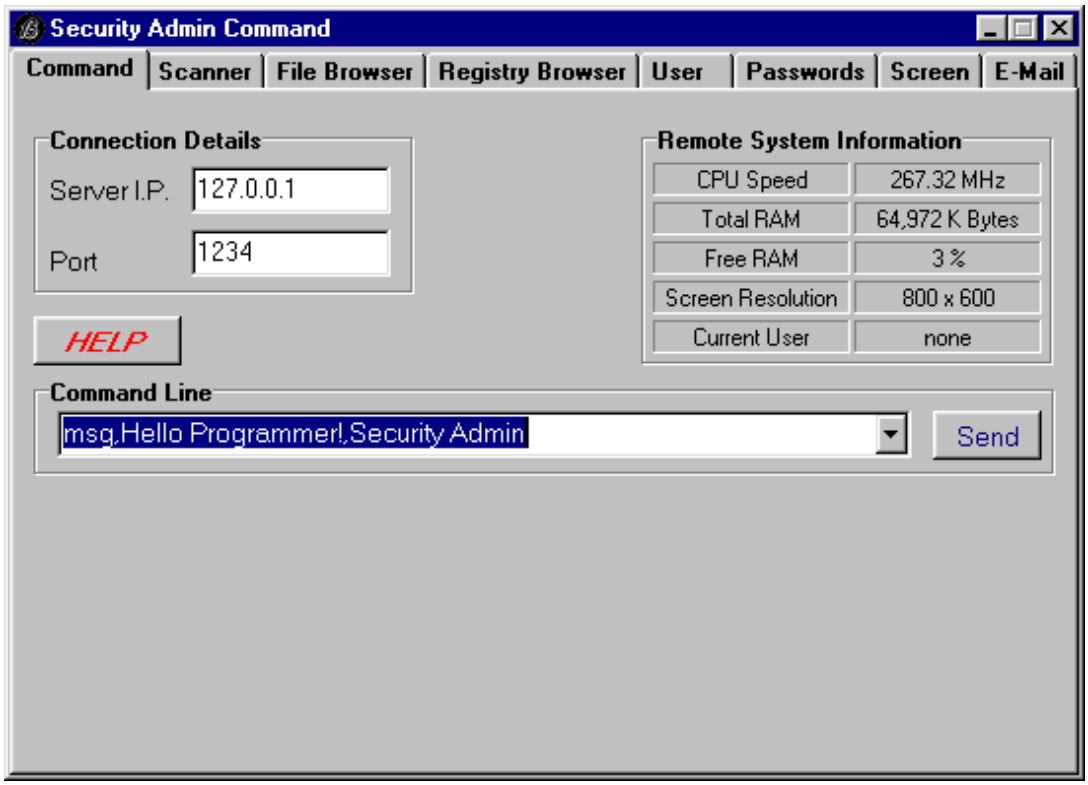
Time and money are wasted when an employee plays solitaire, sells company secrets, or buys pornography over the company's Internet connection. Security Admin assists network administrators by providing a way for them to monitor and control user activity on any computer connected to the company's network.

I saw people wasting time and money at one of my previous places of employment. *If it can go wrong, it probably already has!*

Security Admin is a network administration program written by Golden Stone Software in Inprise Delphi 4 Professional. It operates by sending and receiving commands and files via UDP(User Datagram Protocol) over TCP(Transmission Control Protocol) networks. Security Admin allows administrators to monitor and control user activity over a network. Security Admin server runs invisibly on the remote system while it is controlled by the client.

Security Admin Server is easy to install. Simply execute it on the remote system. The server program automatically installs itself and the original file can be deleted at any time.

Command :



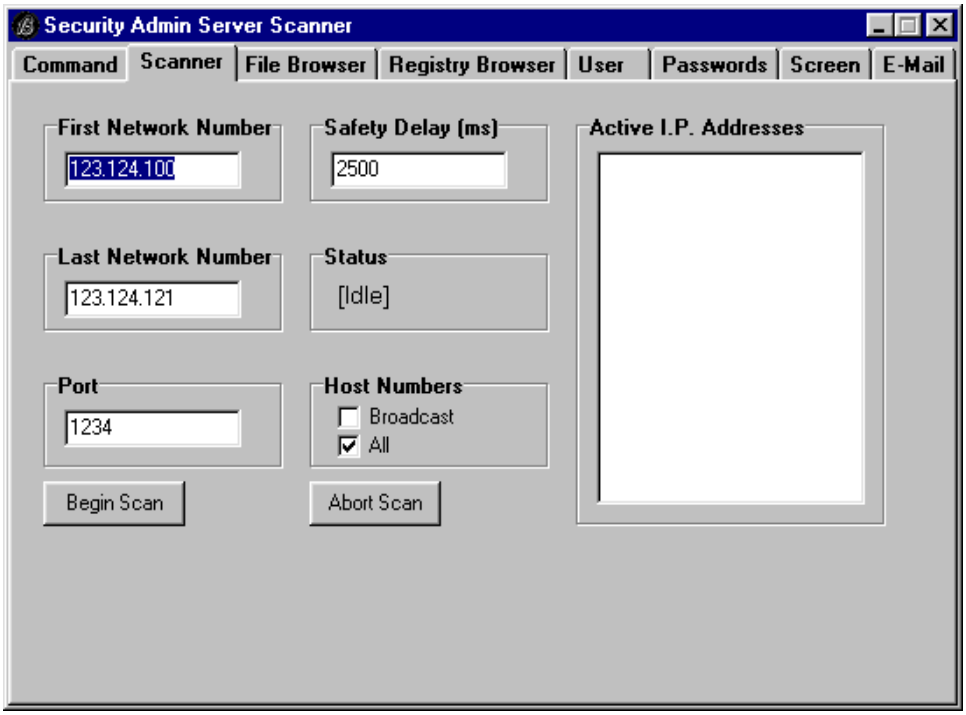
The Command Page contains the connection information as well as information about the remote server computer.

In Connection Details the user can change details regarding the server's I.P. address and port number.

The Remote System Information groupbox displays information about the remote server machine. This information is updated every fifteen seconds. The CPU speed is an approximation. The RAM information refers only to physical memory status. The screen resolution is in pixels (W x H). The Current User refers to the name of the user currently logged on.

The Command Line is intended for advanced users who prefer to implement certain commands manually. See the included file CommandDocumentation.PDF for more details regarding the different commands.

Scanner:



The Security Admin Server Scanner is an extremely powerful tool. It is capable of sending 65,024 queries during each search. This allows you to quickly and easily find all I.P. addresses available for connection.

Security Admin scans by network numbers. If you want to scan 101.102.103.*, you only need to enter the first three octets. The Server Scanner automatically sends queries to all 254 host numbers. You can query network ranges, for instance: 123.124.100.* to 123.124.121.*

If you have enabled access to broadcast addresses on the network, you may scan by sending queries to those addresses. Using broadcast addresses is much faster.

First Network Number:
This is where you enters the beginning network number with which to begin the search.
Example: 123.124.100

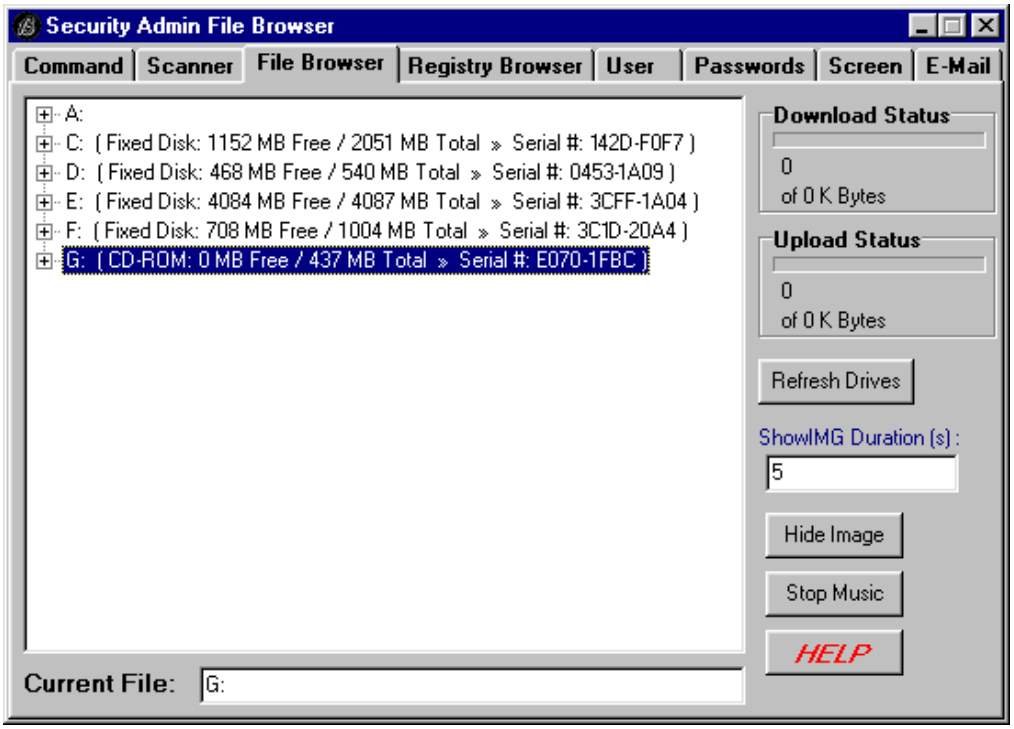
Last Network Number:
This is where ypu enter the network number that will be last in the search. The first two octets must match the First Network Number. The third octet is the only octet that may vary. The third octet in the Last Network Number must be higher than or equal to the third octet in the First Network Number. If the same network numbers are entered for the First and Last Network Number, then only that network number will be scanned.
Example: 123.124.121

Port:
This is the remote port to which the query will be sent. The default port number is 1234. If the server isn't listening on this port, it won't receive the command.
Example: 1234

Safety Delay:
Example: 3000
Security Admin works by sending out bursts of queries(254 at a time). The Safety Delay specifies the delay(in milliseconds) between each burst. The safety delay must be set carefully or the scanner will not function correctly. If the administrator's connection is flooded with scanner queries, there won't be enough bandwidth for the administrator to receive responses to those queries, thus the safety delay is necessary.

How to choose the best Safety Delay:
A safety delay of 2500 should work for 28.8 Kbps modem connections(assuming no other applications are using any bandwidth). For DUN connections, display the connection properties by double-clicking on the DUN connection icon in the system tray. Begin scanning with SSS. Choose a range that covers at least 20 network numbers(Try the second example). Switch back to the connection properties and monitor the number of bytes sent. There should be apparent bursts of data being sent during the search. This should include **pauses** between each burst. If it appears that data is being sent continually, then the Safety Delay has been set too low and the scanner probably won't receive any responses. The Safety Delay only affects Security Admin Server Scanner. This is not a command delay.

File Browser:



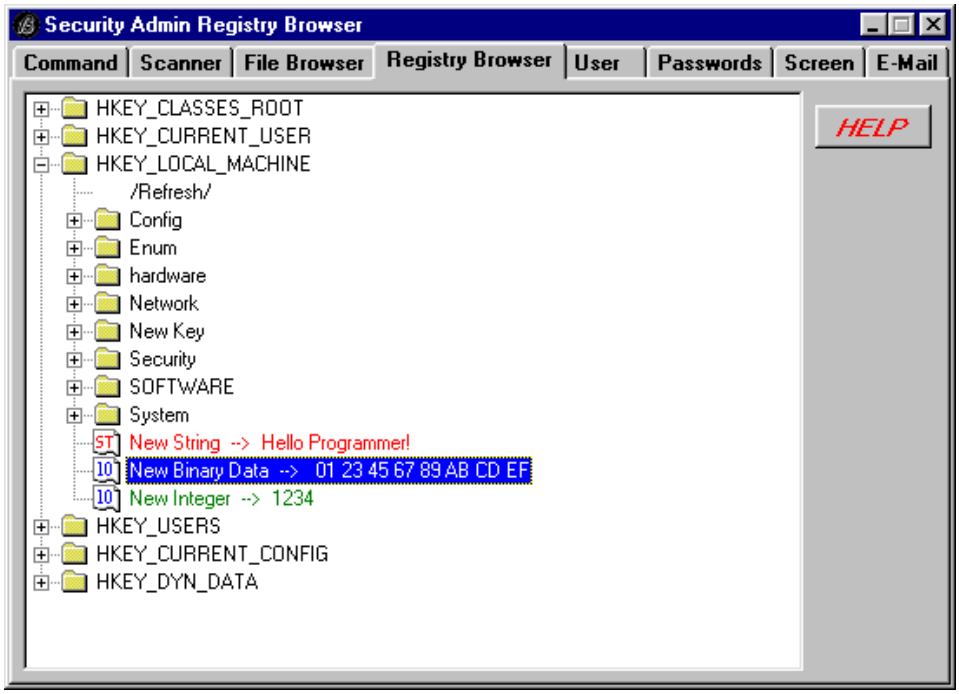
The file browser automatically shows the available remote drive letters when it is activated. You can refresh the file window by clicking on the **Refresh Drives** button.

To view the contents of a directory, double-click on the **/Refresh/** node. This will delete and refresh the contents of the directory listing.

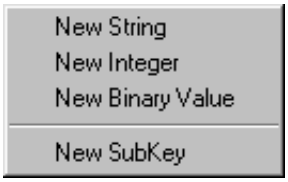
To download any remote file, double-click on the node representing that remote file. Double-clicking on a file automatically initiates the GetFile command. To upload a file, right-click on the destination directory's /Refresh/ node. Download and upload status can be monitored in the File Browser.

By right-clicking on any file, you are prompted to play, show, or execute the file remotely. (This depends on its file extension) You are also given the option to delete a file. The ShowImage duration (seconds) can be set by entering a number in the Show Image Duration edit box.

Registry Browser:

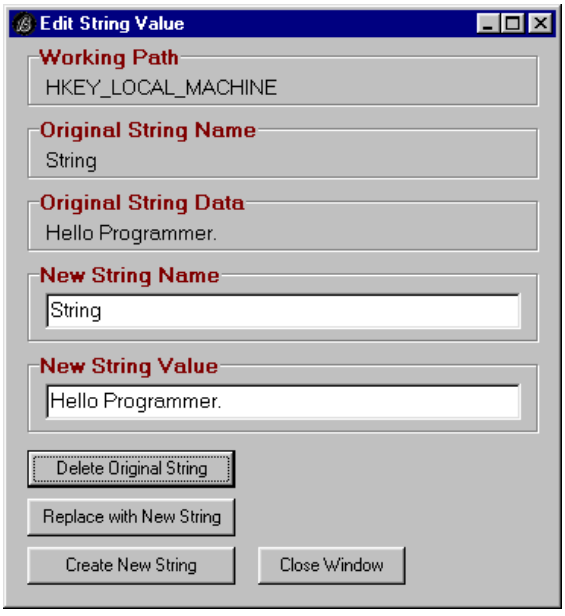


The Registry Browser allows full access to the remote system's registry. You can add, create, and edit registry keys, and values.



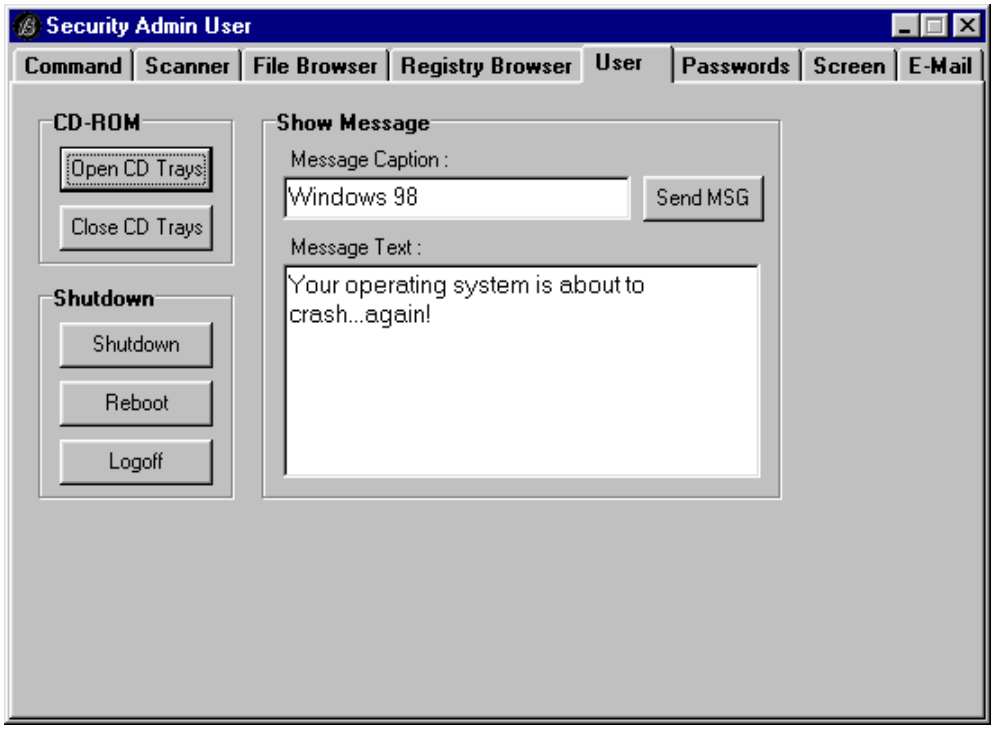
Double-clicking on **/Refresh/** will update the list of keys and values at the current location. Right-clicking on **/Refresh/** gives you a list of options regarding the creation of new keys and values.

Double-clicking on existing keys or values will show a dialog for changing or adding keys or values, depending on the type of item you double-click.



In the Registry Browser, all string values are red, integer values are green, and binary values are blue.

User :



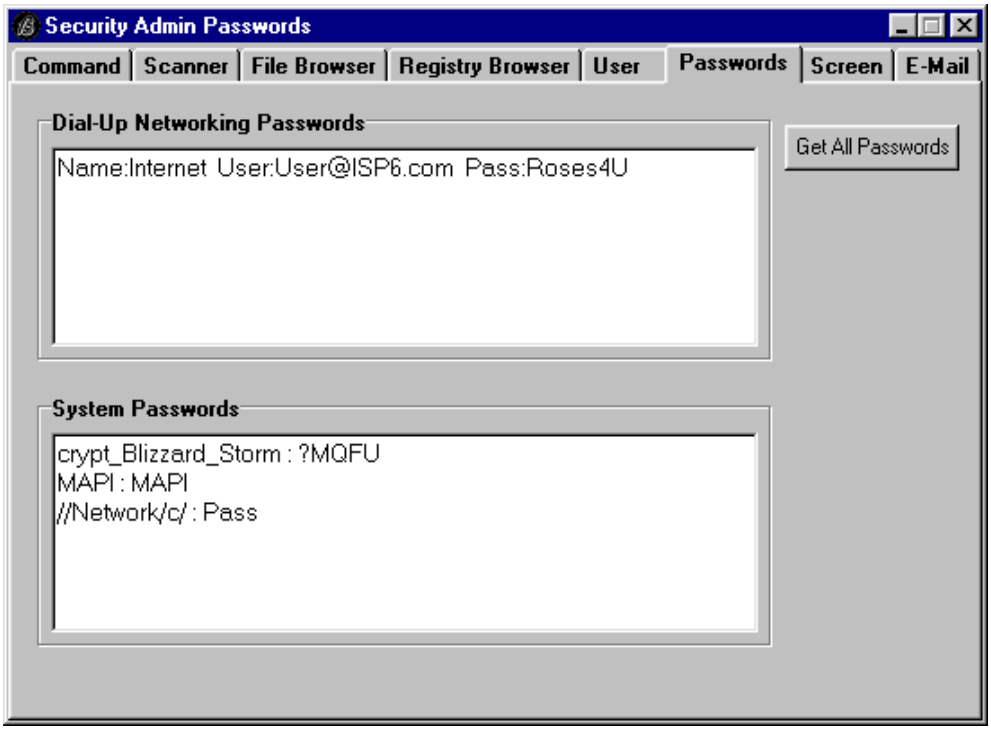
The User Page manipulates the remote computer in a way that directly affects the remote user.

The CD-ROM group box allows you to open and close the remote computer's CD trays. If that computer has multiple CD devices, this feature opens or closes them all simultaneously.

The Shutdown group box lets you shut down the remote server. The remote machine shuts down without prompting the user for confirmation.

The Show Message group box allows you to send a message to the user on the remote server. The message can have multiple lines.

Passwords :

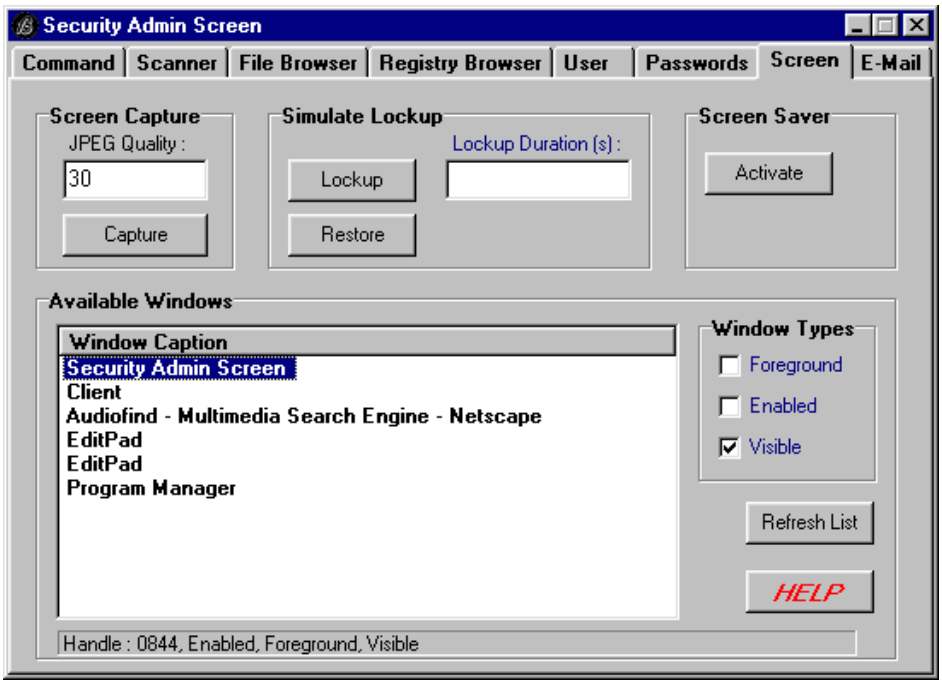


The Passwords Page shows information about remote network resources. Click on Get All Passwords to display the password information.

All Dial-Up Networking account information is displayed. This includes the connection name, the login name, and the password.

The system passwords are cached passwords relating to network resources.

Screen :



The Screen Page provides access to features that affect what the remote user sees and has access to.

The Screen Capture group box is for taking a remote screen capture. The screen image is automatically sent to the client as a JPEG image whose quality is specified in the JPEG Quality edit box. The JPEG quality can be any integer from 1 to 100. Click on the Capture button to take a screen capture.

The Simulate Lockup feature causes the remote user to lose control of the computer. All task-switching (Alt+Tab, Ctrl+Esc, Ctrl+Alt+Del, etc.) is disabled and all keyboard and mouse activity is nullified. The duration (in seconds) can be specified. For unlimited duration, leave this entry blank. Clicking on the Restore button will return all access to the remote user, regardless of the duration setting.

To enable and activate the screen saver on the remote system, click on the Activate Screen Saver button.

The Refresh List button refreshes the list of available windows. The user can choose to view any desired combination of windows by selecting Foreground, Enabled, and/or Visible.

When you click on a window, its handle and properties appear in the status bar.

You can remotely control the windows available to the remote user. Right-clicking over the name of the desired window displays this menu, which lists different ways you can control that window. The caption of the remote windows is irrelevant; all window management features operate by **window handles**.

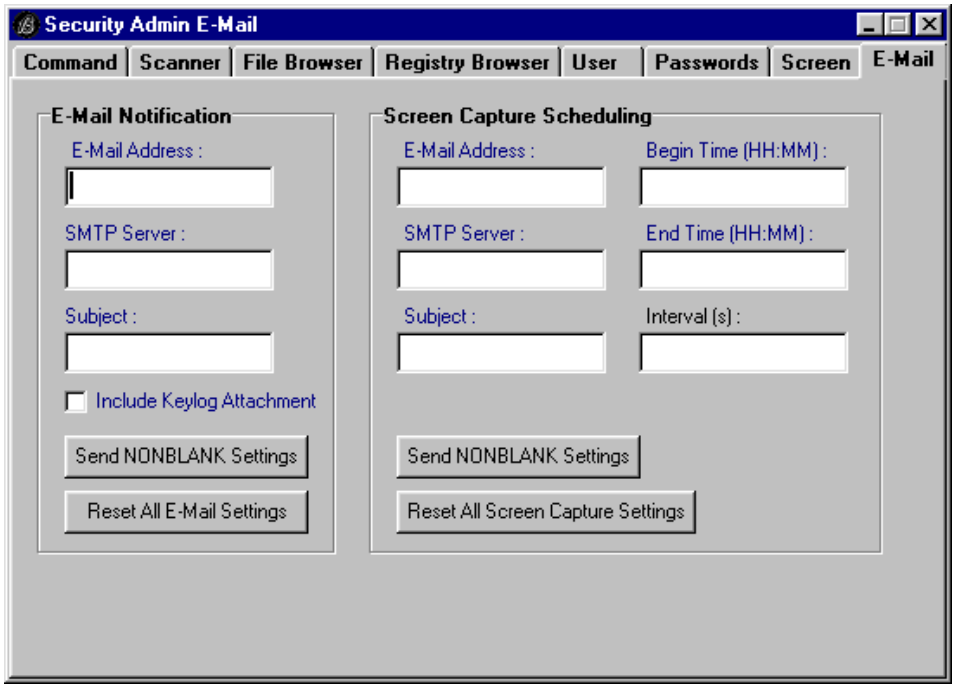
Minimize, Maximize, and Resize are self-explanatory.

Bring to Front will make the selected window to the foreground window. Kill Focus will remove focus from the current window.

Hide will make a window invisible. Its icon is also removed from the task bar. Although the window isn't visible, its program **IS** still running. To make the window visible again, click on Show.

To close a window, click on Request Close. The window may prompt the user for confirmation. (For instance, the user may be asked to save the current document or cancel the close request.) The Force Close option **forces** a window to close immediately, bypassing any confirmation.

E-Mail:



When a server connects to a TCP network, Security Admin can notify the you of this event via E-mail. The E-mail, containing the new I.P. address and the current time, is sent automatically whenever the machine gains a new I.P. address. To change any of the E-mail settings, type the new information in the appropriate edit box and click on Send Non-blank Settings. This will update the information stored on the server. If any entry is blank, it will be ignored. For security reasons, you cannot view the existing settings if there are any.

To delete all E-mail notification settings, click on Reset All E-mail Settings.

If E-mail notification is insufficient, Screen Capture Scheduling may prove useful. Screen Capture Scheduling is a way to monitor activity on the server even if it is not connected to a network. The server can take screen captures during a certain time of the day. They are strored as numbered JPEG images with quality 25. When the server connects to the network, the images are automatically E-mailed in groups of five.

The Begin and End time settings must be in the form hh:mm using 24-hour time. For instance, 9:00 is nine O'clock in the morning and 21:00 is nine O'clock at night. The interval setting specifies how often screen images are captured. This setting must be in seconds. For instance, a setting of 30 causes the screen captures to be taken every 30 seconds. A setting of 600 causes screen captures every ten minutes. If any entry is blank, it will be ignored. For security reasons, you cannot view the existing settings if there are any.

If you decide to use this feature, always calculate how many images it will create. You may not want 20 MB of E-mail attachments!

To delete all Screen Capture Scheduling settings, click on Reset All Screen Capture Settings.

To disable Screen Captures, set one of the three values on the right to 'none' (without the quotation marks). If the three values on the left have valid settings, any remaining JPEG images will be sent.

To continue screen capturing, but prevent the mailing of the JPEGs, set any of the values on the left to 'none' (without the quatation marks). If the three values on the right have valid settings, screen captures will continue according to those settings. Leaving this feature partially operational is not recommended.