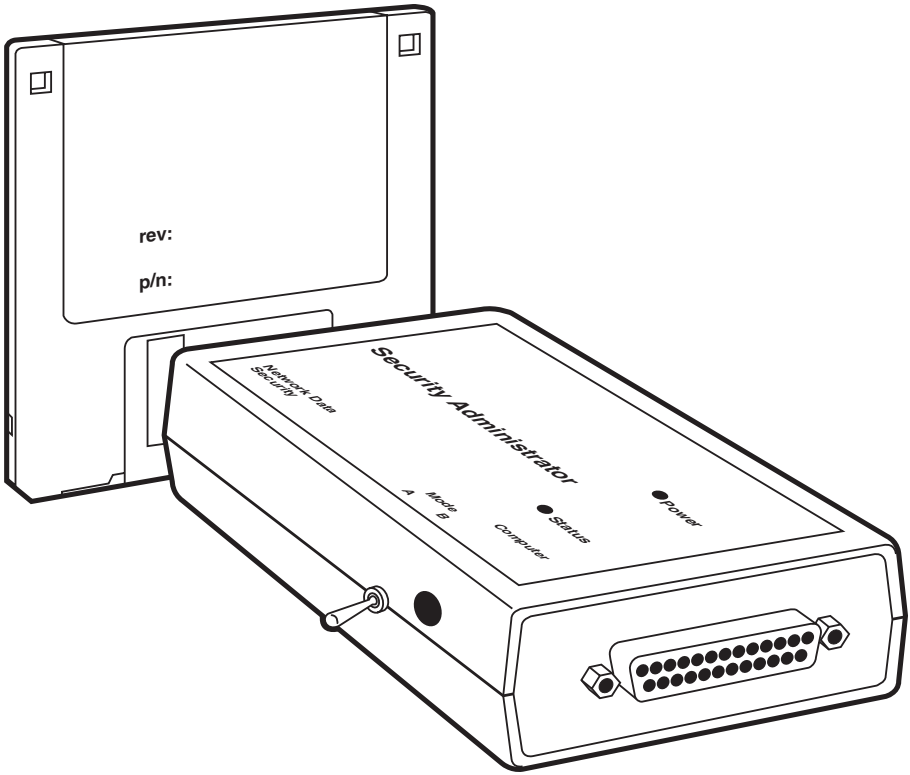
BLACK BOX
NETWORK SERVICES

DECEMBER 1998
AC432A-R2

Security Administrator



CUSTOMER SUPPORT INFORMATION

Order **toll-free** in the U.S. 24 hours, 7 A.M. Monday to midnight Friday: **877-877-BBOX**
FREE technical support, 24 hours a day, 7 days a week: Call **724-746-5500** or fax **724-746-0746**
Mail order: **Black Box Corporation**, 1000 Park Drive, Lawrence, PA 15055-1018
Web site: **www.blackbox.com** • E-mail: **info@blackbox.com**

FEDERAL COMMUNICATIONS COMMISSION AND INDUSTRY CANADA RADIO FREQUENCY INTERFERENCE STATEMENT

Class B Digital Device. This equipment has been tested and found to comply with the limits for a Class B computing device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. If this equipment does cause harmful interference to radio or telephone reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult an experienced radio/TV technician for help.

Caution:

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

To meet FCC requirements, shielded cables and power cords are required to connect this device to a personal computer or other Class B certified device.

This digital apparatus does not exceed the Class B limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de classe B prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.

NORMAS OFICIALES MEXICANAS (NOM)

ELECTRICAL SAFETY STATEMENT

INSTRUCCIONES DE SEGURIDAD

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.
2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.
4. Todas las instrucciones de operación y uso deben ser seguidas.
5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc..
6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.
7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.
8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.
9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.
10. El equipo eléctrico deber ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.

11. El aparato eléctrico deberá ser connectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.

12. Precaución debe ser tomada de tal manera que la tierra fisica y la polarización del equipo no sea eliminada.

13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.

14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.

15. En caso de existir, una antena externa deberá ser localizada lejos de las lineas de energia.

16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.

17. Cuidado debe ser tomado de tal manera que objectos liquidos no sean derramados sobre la cubierta u orificios de ventilación.

18. Servicio por personal calificado deberá ser provisto cuando:

    A: El cable de poder o el contacto ha sido dañado; u

    B: Objectos han caído o líquido ha sido derramado dentro del aparato; o

    C: El aparato ha sido expuesto a la lluvia; o

    D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o

    E: El aparato ha sido tirado o su cubierta ha sido dañada.

Contents

1. Specifications

System Hardware Required — To run software: IBM® PC, PC/XT™, AT®, PS/2®, or compatible

System Software Required — To run software: Microsoft Windows 3.1 or higher

Software Diskette Included — A diskette for compatibility with the Remote Access Server features used with clients and servers running MS Windows NT, Windows 3.1, and Windows 95 included.

System Memory Required — Negligible

Disk Space Required — 315 KB

Cable Required — To DTE: Straight-through-pinned RS-232 (modem) cable (included);
To NDS: Straight-through-pinned RS-232 (modem) cable (included with NDS)

Compliance — Hardware: FCC Part 15 Class A, IC Classclasse B

Standards — Encryption: DES

Interface — EIA RS-232 serial

Protocol — Asynchronous

Data Format — 8 data bits (fixed); 1 or 2 stop bits (user-selectable); even, odd, or no parity (user-selectable)

Flow Control — RTS/CTS (hardware) or X-ON/X-OFF (software), user-selectable; can also can be set to hold DCD until authentication is established or pass it through immediately upon connection

Data Rates —	38,400, 19,200, 9600, 4800, 2400, 1200, or 300 bps or autodetecting (user-selectable)
Maximum Distance —	50 ft. (15.2 m) to DTE or NDS
User Controls —	(1) Side-mounted MODE toggle switch (nonfunctional)
Diagnostics —	Power-up diagnostic
Indicators —	(2) Top-mounted LEDs: POWER and STATUS
Connectors —	(2) Side-mounted DB25: (1) male (to DTE), (1) female (to NDS)
Leads/Signals Supported —	1 through 8, 20, and 22 (the PGND, TD, RD, RTS, CTS, DSR, SGND, RLSD [DCD], DTR, and RI signals respectively)
MTBF —	Greater than 20,000 hours
Maximum Altitude —	20,000 ft. (6096 m)
Temperature Tolerance —	Operating: 32 to 122˚ F (0 to 50˚ C); Storage: –148˚ to 158˚ F (–100 to 70˚ C)
Humidity Tolerance —	Up to 85% noncondensing
Power —	From wallmount power supply: Input: 120 VAC, 60 Hz; Output: 9 VDC, 300 mA; Consumption: Roughly 1.3 VA at power-up, 1 VA thereafter
Size —	1.4"H x 2.8"W x 4.9"D (3.6 x 7.1 x 12.4 cm)
Weight —	Net: 0.7 lb. (0.3 kg); Shipping: 2.1 lb. (1 kg)

2. Introduction

The Security Administrator (SA) provides system administration for our Network Data Security devices: It offers additional programming and management capabilities to an installed base of NDSes.

With the SA, you can perform any of these powerful functions:

1. Search for a specific ID in an NDS's Authorization Table.
2. Delete a specific ID.
3. Suspend a specific ID.
4. Restore a previously suspended ID.
5. Block all or a portion of unused memory locations from authorization programming.
6. Unblock previously blocked memory locations.
7. Set a data rate for serial communication.
8. Disable the NDS's SECURITY switch.
9. Enable automatic "bulletin-board mode" for outbound connections.

You can administer an NDS by just temporarily attaching it to an SA, as shown in Figure 2-1 on the next page. You can set optional passwords for this process to prevent unauthorized users from examining or changing an NDS's programming and configuration.

The complete Security Administrator package consists of a system module (hardware), a serial connector cable, a power supply, a 3.5" software diskette, and this manual. You will be connecting the SA's system module to the serial port (COM*n*:) of the computer that will be used for NDS administration; you will be installing the software on the same computer (the computer must be running the Microsoft® Windows® 3.10 or higher operating system)

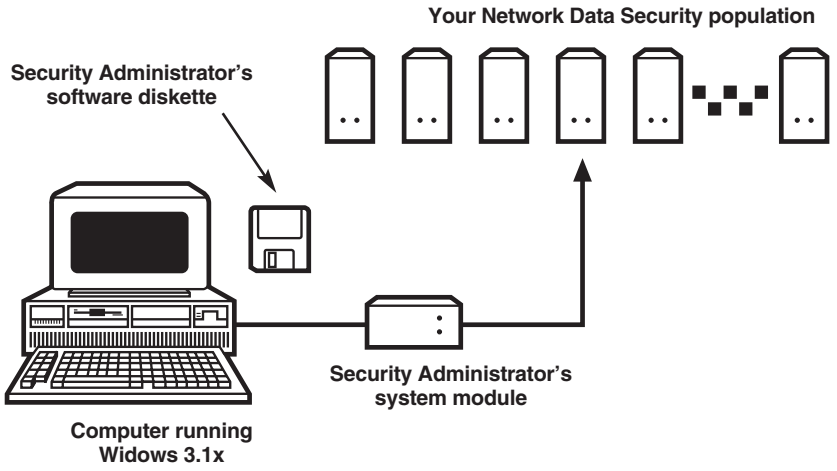


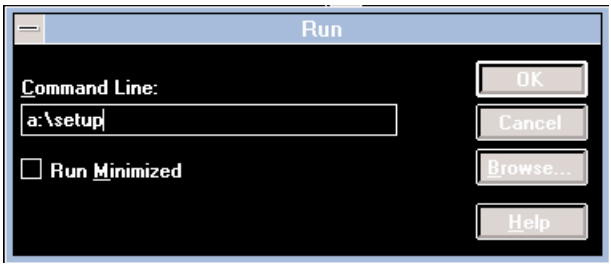
Figure 2-1. A typical Security Administrator setup.

3. Software Installation

The Security Administrator's software must be installed on a PC with Windows 3.1x. The machine must also have an serial port available for use by the SA's software.

3.1 The Installation Procedure

1. Turn on your computer and start Windows.
2. Insert the Security Administrator's diskette into the appropriate drive.
3. In the PROGRAM MANAGER, select RUN from the FILE menu. Enter <drive>:\SETUP, where <drive> is the drive that the SA's software diskette is in. In this example, the diskette drive's drive letter is A:



4. SETUP will ask you which hard-disk directory you want the software to be installed in. As shown below, C:\BLACKBOX is the default directory, but you may specify an alternative directory if you like.

5. A program group called Security Administrator will appear. As shown below, it will contain three items: the Security Administrator main program, the NDS Troubleshooting Guide, and a ReadMe file.

This completes the installation of the Security Administrator software.

3.2 Simulation/Practice Operation

The Security Administrator's software may be run, at this point, without any hardware connections. The software can simulate an environment with several dozen Network Data Security units, so that you can become familiar with how the software works before you actually have to use it during a hardware connection.

1. Double-click on the Security Administrator icon to start the software.
2. The connection screen appears, indicating SA NOT ATTACHED:

3. Enter **sa demo** as the password. The characters will appear as asterisks, as shown in the screen shot above. Click on ATTACH, then OK (or press Enter twice).
4. All SA functions (setting passwords, suspending and restoring IDs, etc.) can now be simulated—see **Chapter 5** for instructions about how to access and use them. When you're finished, select Exit from the software's File menu.

4. Hardware Installation

To install the Security Administrator's hardware, called the "system module," take these steps described below. Please note that to connect the system module to a Network Data Security unit, the NDS must be temporarily disconnected from the equipment it's normally attached to.

1. Apply power to both the NDS and the SA's system module by plugging their power supplies into working electrical outlets. (Both boxes will begin operating automatically, because neither of them has an ON/OFF switch. To power them down, unplug them.) The system module will light its POWER LED and (while it runs its power-on diagnostic) its STATUS LED. After about two seconds, the STATUS LED should go dark (the POWER LED remains lit.) If the STATUS LED stays on for more than two seconds, the SA might be defective or broken; call Black Box for technical support.

NOTE

Do not run cable from the NDS to the system module before you power them up. This is because if they are interconnected before you power them up, and there is too long of a delay after plugging one unit in before you plug in the other unit, the units will be unable to authenticate each other.

2. Run the included serial cable from the system module's **Computer** connector to a free serial (COM*n*:) port on the administration computer (the computer that the SA's software is installed on).

NOTES

If you would rather, you can run a standard straight-through-pinned RS-232 (modem) cable from the SA to the computer instead of using the SA's cable.

It doesn't matter which of the administration computer's serial ports you connect the system module's cable to, even if the computer has more than one free serial port. The SA's hardware will automatically scan all of the serial ports and find the system module's connection.

3. Disconnect the NDS and the cable that came with it from their existing attachments. Temporarily run the NDS's cable from the NDS's **Computer** connector to the system module's **Network Data Security** connector. Your hardware setup should look like the one shown in Figure 4-1 on the next page.

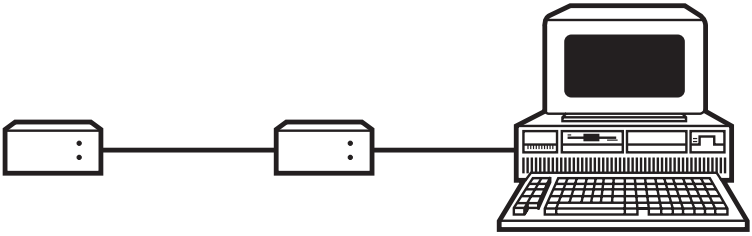


Figure 4-1. Hardware links.

NOTE

If you would rather, you can run a standard straight-through-pinned RS-232 (modem) cable from the NDS to the system module instead of using the NDS's cable.

This completes your hardware installation. You are now ready to begin using the SA's software to administer the connected NDS. A brief summary of how to do this is given in **Section 5.1**, but we recommend you read all of **Chapter 5**.

NOTE

There is a two-position MODE switch on the bottom of the SA's system module. This switch is intended to support potential enhancements which may be implemented through future releases of the SA's software. At present, however, the switch has no function.

5. Operation

This chapter describes how to operate the Security Administrator hardware and software. **Section 5.1** presents a short synopsis of the operating procedures; **Sections 5.2** through **5.17** present the procedures in detail; and **Section 5.18** describes special procedures you must use to administer one NDS with several SAs.

5.1 Summary

The sequence in which you would administer a Network Data Security unit with the Security Administrator goes roughly like this:

In Windows, run the SA's software. It will detect the physical presence of the NDS and will present a connection screen through which you can "attach to" (establish communication with) it.

At this point, an optional Administration Password can be assigned to this NDS (you can assign one to each NDS). If you assign one, this password is required for any future SA attachment to this NDS.

You can now use the software to perform various NDS-management functions such as suspending and restoring IDs and blocking and unblocking memory locations.

An optional Maintenance Password can also be assigned to this NDS (you can assign one to each NDS). If you assign one, this password is required for changing the NDS's ID setup or the status of any of its memory locations. (With two levels of passwords, certain users can be granted enough access to see current settings, while the right to make changes is reserved for those with authority to do so. Each Administration or Maintenance Password is stored in the NDS to which it is assigned and is therefore associated with *that* NDS only.)

To activate changes in authorization status (suspension, restoration, or deletion of IDs or blocking or unblocking of memory locations), you must now use the **Update** function to download the changes into the NDS's authorization table. (Only the **Set Empty Count** function occurs in real time; see **Sections 5.12** and **5.14**.) The **Update** key on the software's Toolbar becomes active ("darkened in" as opposed to "grayed out") when an update is required (see **Section 5.16**).

When you are finished updating the NDS's authorization table, unplug the NDS, disconnect it and its cable from the SA, and return them to service in their previous location.

An SA can provide administrative services to an unlimited number of Network Data Security units.

5.2 Getting Started

NOTE

If you have been running the SA's software in sa demo **mode, you must Exit and restart the program before you can administer a real NDS.**

1. In Windows, open the Security Administrator program group and double-click on the Security Administrator icon to start the software.
2. The connection screen appears, indicating SA NOT ATTACHED.
3. If an Administration Password exists for the connected Network Data Security unit, it must be entered now. If this is a new NDS for which a new password will be entered, use the **Change Password** function in the **Security Control** screen of the **Network Data Security** menu (see **Section 5.5**).
4. After the Security Administrator's STATUS light has stopped blinking, click on ATTACH.
5. Notice the indicated version and serial number (ID) of the attached NDS.
6. Click on **OK**. Uploading all records from the NDS's ID table to the SA's software takes a few moments.

A **Network Data Security SAWIN - Audits** screen then appears, as shown on the next page.

5.3 The Audits Screen

The contents of the connected Network Data Security unit's ID table are displayed at the **SAWIN - Audits** screen, shown below. This is the main screen from which you will adminster and configure the NDS.

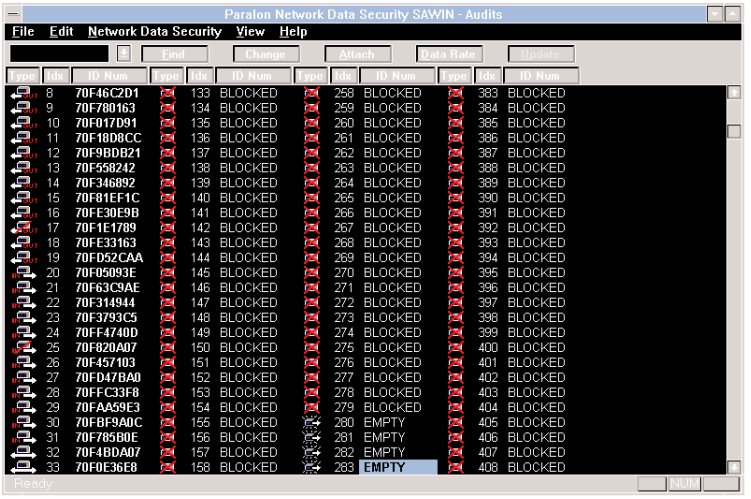


Figure 5-1. The Audits Screen.

At this screen, you can select from these menus:

- **File — Update**, print-control, and **Exit** functions (see **Sections 5.16** and **5.17**)
- **Edit — Find**, **Change**, and **Set Empty Count** (see **Sections 5.7** through **5.14**) functions
- **Network Data Security — Attach**, **Set Data Rate**, and **Security Control** (see **Sections 5.5**, **5.6**, **5.15**, and **5.18**) functions
- **View — Sort by...**, **View Filter** (see **Section 5.4**), **Refresh**, and **Status-Bar Control** functions
- **Help —** Help functions for the SA

You may also use these Toolbar keys:

- **Type —** Displays ID table in order of authorization types
- **Idx —** Displays ID table in order of memory locations
- **ID Num —** Displays ID table in numeric order of actual NDS IDs
- **Find —** Invokes a search for a specific ID, as entered in the Find box (see **Section 5.7**)
- **Change —** Starts the change process for modifying the status of the NDS's memory locations (see **Sections 5.8** through **5.14**)
- **Attach —** Initiates the attachment process for connection to a new NDS

- **Data Rate —** Allows you to program of serial data-communication speed (see **Section 5.15**)
- **Update —** Downloads all changes back to the connected NDS (see **Section 5.16**); this function is available only when changes have been made but haven't yet been downloaded

5.4 View Filters

You can use view filters to organize the Network Data Security unit's ID-table display. With view filters, users can customize the audit screen so that it displays only those memory locations characterized by types of authorization status that interest them.

Access the Security Administrator's view filters by selecting View Filter from the View menu. The six filters appear in a View Selection window. Clicking on a filter's checkbox to select a type of authorization status causes that type to be included in the table display and in any printed output of authorizations (see **Section 5.17**). Deselecting a type of status causes that type to be omitted from the display and any printed output.

To see the state of, or to select or deselect any of, the SA's view filters, take these steps:

1. Click on the **View** menu to open it.
2. Select **View Filter**. The View Selection window (shown at the top of the next page) will appear.
3. Select or deselect any type of authorization status by clicking on the corresponding checkbox. An "X" in the box indicates that that type of status will appear in the audit screen's ID-table display and in authorization printouts, and an empty box indicates that that type of status will not appear.

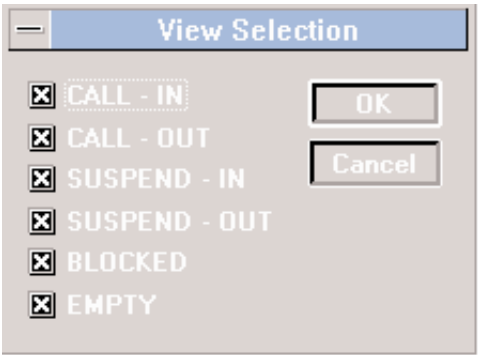


Figure 5-2. View Selection Screen.

- **CALL - IN** controls the display of all authorizations which can call in to the Network Data Security unit. This includes two-way authorizations.
- **CALL - OUT** controls the display of all authorizations to which the NDS can call out. This includes two-way authorizations.
- **SUSPEND - IN** controls display of all suspended inbound authorizations, including suspended two-way authorizations.
- **SUSPEND - OUT** controls display of all suspended outbound authorizations, including suspended two-way authorizations.
- **BLOCKED** controls display of all blocked (empty but unavailable for programming) memory locations in the table.
- **EMPTY** controls display of all empty [and available for programming] memory locations in the table.

NOTE

The display and printout of two-way authorizations is inclusive, not exclusive. This means that if *either* CALL - IN *or* CALL - OUT is selected, active two-way authorizations appear. Likewise, if either SUSPEND - IN or SUSPEND - OUT is selected, suspended two-way authorizations appear.

5.5 Passwords

Using passwords with the Security Administrator is optional. Different NDSes in your population can have the same passwords or unique individual passwords. *If you use them, exercise extreme caution. Passwords are associated with, and stored in, the specific Network Data Security unit being accessed or programmed, not the SA. If you lose a password, there is* ***absolutely*** *no way to recover it!*

There are two password levels available (either type of password can be used independently of the other):

- When you define an **Administrative Password** for an NDS, this password must be entered before an SA can "attach to" (access) the unit.
- When you define a **Maintenance Password** for an NDS, users must enter this password before they can make changes to the unit's ID authorizations and memory locations.

To add or change a password:

1. Select **Security Control** from the **Network Data Security** menu.
2. Select **Admin** or **Maintenance** as the password you wish to add or change.
3. Enter the old password if (and only if) you are changing an existing password.
4. Enter the new password (it must be between 5 and 8 characters long).
5. Verify it by reentering it.
6. Click on **OK**. The new password is now in effect.

5.6 Additional Security Controls

5.6.1 Disabling the SECURITY Switch

You can use the Security Administrator to disable the connected Network Data Security unit's SECURITY switch. In this mode, the NDS's logical SECURITY setting is always ACTIVE regardless of the physical position of the switch.

When the SECURITY switch is disabled, inbound connections are allowed only when an authorized NDS is at the calling node. Outbound connections in the clear are permitted only when **BBS detect - Outbound** is enabled (see **Section 5.6.2**).

To disable the connected NDS's SECURITY switch, take these steps:

1. Select **Security Control** from the **Network Data Security** menu.

2. Select **Switch always ACTIVE** so that the checkbox has an "X" in it.

3. Click on **OK**.

To re-enable the SECURITY switch, reselect **Switch always ACTIVE** so that the checkbox is empty.

The **Switch always ACTIVE** setting has no effect on the SECURITY switch during NDS-authorization programming.

5.6.2 BBS Detect - Outbound

You can also program Network Data Security units to allow outbound connections to non-secure modems for use with public bulletin boards and on-line services. While **BBS detect - Outbound** is enabled, if the NDS's computer dials out, connects with a modem without an NDS, and receives any incoming data within 2 seconds, the NDS can allow connection and

full-duplex data communication in-the-clear, regardless of the SECURITY switch's position or enabled/disabled status.

BBS detect - Outbound will not allow two unauthorized NDSes to connect.

Even if **BBS detect - Outbound** is enabled, the NDS still does not permit inbound calls to connect unless there is an authorized NDS at the calling node. Inbound security is always maintained.

To enable **BBS detect - Outbound**, take these steps:

1. Select **Security Control** from the **Network Data Security** menu.

2. Select **BBS detect - Outbound** so that the checkbox has an "X" in it.

3. Click on **OK**.

Switch always ACTIVE and **BBS detect - Outbound** mode can be used independently or together. When you enable both of them, the NDS's computer maintains automatic full-time inbound security, outbound secure-connection capability to authorized NDSes, and transparent connections to public on-line services like CompuServe® or the Internet.

5.7 Searching for an NDS ID

With the Security Administrator software, you can do a table-wide search for a specific user-supplied NDS ID. The result of the search will either place the highlighted cursor on that ID, in its memory location, or return an AUTHORIZATION NOT FOUND message.

To do such a search, take these steps:

1. Click on **Find**. The Find Serial Number window will appear.

2. Enter a specific ID for the search (this is not case-sensitive—letters can be either upper- or lowercase).
3. Click on **OK**.
4. The software either moves the cursor to highlight the ID location, or displays the message AUTHORIZATION NOT FOUND.
5. The software maintains a list of all IDs entered for searches. To recall any ID, first click on the Find box's down-arrow.
6. Select the ID from the list. It appears in the Find box and can now be edited.
7. If there are more than five stored entries, scroll with the up- and down-arrows.

5.8 Deleting an NDS ID

A Network Data Security unit's ID table contains authorized IDs of other NDSes. You can use the Security Administrator to delete these IDs, but this function should be used carefully. The only way to *add* an authorization to an NDS's table is to physically mate that NDS with another one. This means that once you delete an ID with the SA, that ID cannot be restored without mating both NDSes concerned.

We strongly recommend that users familiarize themselves with, and consider as an alternative, the **Suspend** and **Restore** functions in the SA's software (see **Sections 5.9** and **5.10**) before they use the **Delete** function.

To delete an ID, take these steps:

1. Select the ID you want to delete.

2. Click on **Change** or press Enter to activate the **Network Data Security properties** window for the highlighted ID.
3. If a Maintenance Password has been assigned for this NDS, you must enter it now.
4. Click on **Delete**.
5. When the message "Are you sure you want to delete this authorization?" appears, click on **OK**.
6. After you delete an ID, that memory location in the table must be assigned Empty or Blocked status.
7. Click on **OK**.

5.9 Suspending an NDS ID

You can use the Security Administrator software's **Suspend** function to "deauthorize" a previously authorized Network Data Security ID. Suspended authorizations are unable to communicate but remain in the table, available for future restoration. This can be particularly useful if NDSes are lost or stolen or are being moved or shipped for repair, because the authorization can be restored easily if the units are recovered or redeployed.

To suspend an ID, take these steps:

1. Select the ID you want to suspend.
2. Click on **Change** or press Enter to activate the **Network Data Security properties** window for the highlighted ID.
3. If a Maintenance Password

has been assigned for this NDS, you must enter it now.

4. Select **Suspend**.
5. Click on **OK**.

A slash appears across the audit-screen icon of this ID to show that the ID's authorization is now suspended.

A suspended ID continues to occupy the same memory location in the NDS's ID table as it did before.

5.10 Restoring a Suspended NDS ID

To restore a suspended Network Data Security unit's ID, so that that NDS can communicate with the connected NDS as normal, take these steps:

1. Select the suspended ID you want to restore.
2. Click on **Change** or press Enter to activate the **Network Data Security properties** window for the highlighted ID.
3. If a Maintenance Password has been assigned for this NDS, you must enter it now.
4. Select **Active**.
5. Click on **OK**.

The slash across the audit-screen icon of this ID disappears to show that the ID's authorization is now active.

When a previously suspended authorization ID is restored, it resumes the status it had prior to suspension: one-way inbound, one-way outbound, or two-way).

5.11 Blocking a Single Unused Memory Location

You might find it desirable to block some or all of the unused memory locations in a Network Data Security unit's ID table, in order to prevent additional authorizations from being programmed into that NDS. If you want to block all of the unused locations in an NDS's table, see **Section 5.12**. If you want to block only one location (or one location at a time), take these steps:

1. Select the memory location you want to block.
2. Click on **Change** or press Enter to activate the **Network Data Security properties** window for the highlighted ID.
3. If a Maintenance Password has been assigned for this NDS, you must enter it now.
4. Select **Blocked**.
5. Click on **OK**.

The audit-screen display for this memory location is "Xed out" to show that the location is now blocked.

Blocked memory locations remain blocked until you unblock them.

5.12 Blocking All Unused Memory Locations

If you want to block only one (or only one at a time) of the unused memory locations in the ID table of the connected Network Data Security unit, see **Section 5.11**. If you want to block all of the unused locations in an NDS's table, take these steps:

1. Click on **Edit**.
2. Select **Set Empty Count**.
3. If a Maintenance Password has been assigned for this NDS, you must enter it now.
4. Enter 0 for **Number of empty records**, then click on **OK**.
5. Any memory locations which were Empty are now Blocked.

5.13 Unblocking a Single Memory Location

Memory locations which have been blocked must be unblocked before new authorizations can be programmed into them. To unblock a group of memory locations at the same time, see **Section 5.14**. To unblock only one location (or one location at a time), take these steps:

1. Select the Blocked memory location that you want to unblock.
2. Click on **Change** or press Enter to activate the **Network Data Security properties** window for the highlighted ID.
3. If a Maintenance Password has been assigned for this NDS, you must enter it now.
4. Select **Empty**.
5. Click on **OK**.

The audit-screen display for this memory location changes to show that the location is now empty and can accept a new authorization ID.

5.14 Unblocking a Group of Memory Locations

Memory locations which have been Blocked must be unblocked before new authorizations can be programmed into them. To unblock only one location (or one location at a time), see **Section 5.13**. To unblock a group of memory locations at the same time, take these steps:

1. Click on **Edit.**
2. Select **Set Empty Count**.
3. If a Maintenance Password has been assigned for this NDS, you must enter it now.
4. Enter the total required number of empty records.
5. Click on **OK**.

Ten memory locations immediately become Empty (capable of receiving new authorization IDs). Empty memory locations can be anywhere in the ID table and are not necessarily numerically sequential.

The **Set Empty Count** function sets the total number of Empty (open and available) memory locations. For example, if there had already been four Empty locations when you took the steps described above, only six more Blocked locations would have been made Empty. If there had been more than ten Empty locations, the steps described above would have Blocked all but ten of the Empty locations.

5.15 Setting Serial Communication Parameters

When you connect them to external modems, Network Data Security units can use their "Autobaud" feature to automatically detect and synchronize with the current data rate. Autobaud works from 300 bps to 38,400 bps. NDSes use it not just to initially synchronize with the data rate, but also to maintain synchronization as the data rate changes throughout the communication session. Autobaud is factory-preset to "enabled" in all NDSes.

If you want to "hard code" an NDS's data rate, the Security Administrator gives you "override capability." You can use the software's **Set Data Rate** function to set a permanent data rate for the connected NDS. Afterward, whenever the NDS is involved in data communication, it will immediately begin synchronization at that data rate and maintain that rate throughout the session. This may be necessary in order to use the NDS with a small percentage of modems and routers.

The SA's software can also customize various other serial-communication parameters, as described in the following subsections.

5.15.1 Changing the Preset Data Rate, Data Format, and Flow Control

To change the data rate, parity, stop bits, or type of flow control that the connected Network Data Security unit will use, select **Set Data Rate** from the **Network Data Security** menu. The **Communications Setup** window then appears, as shown at right. Select your desired **Data Speed**, **Parity**, **Stop Bits**, and **Flow Control**. These parameters and their possible settings are explained in more detail on the next page.

You may set these parameters at the **Communications Setup** window:

- **Data Speed:** The data rate in bps. You can either force the NDS to use a single set speed for all data communication (38,400, 19,200, 9600, 4800, 2400, 1200, or 300 bps), or you can turn on the Autobaud feature by selecting "Auto Detect" or the default setting, "Auto Detect - Set if 38400." The difference between the two types of Auto Detect is that the former cannot reach 38,400 bps, but is slightly more efficient because it does not have to reset the computer's UART.
- **Parity:** The parity type (even, odd, or none). (The NDS doesn't support mark or space parity.) No parity is the default setting of this parameter.
- **Stop Bits:** The number of stop bits (either 1 or 2). (The NDS does not support 1.5 stop bits, and always uses 8 data bits.) The default setting of this parameter is 1 stop bit.
- **Flow Control:** The type of flow control to be used between the NDS and the DTE. (This option is only active if the connected NDS is version 1.9 or higher.) You can select RTS/CTS (hardware—the default), X-ON/ X-OFF (software), or neither (none). (You can select both, but as long as X-ON/X-OFF is selected, the NDS will use only software flow control on the DTE side. It always uses hardware flow control on the modem side.)

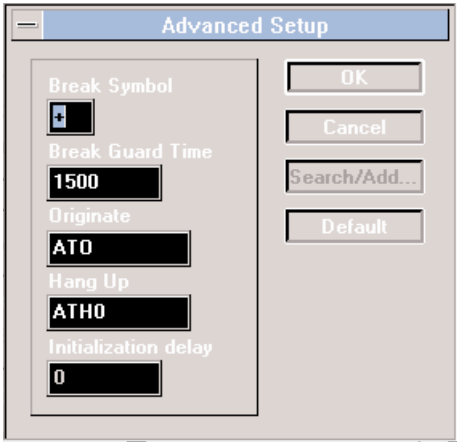
  You can also independently turn "Hold DCD" on or off. If Hold DCD is on, the NDS will not pass anything through from the modem to the DTE until authentication with the NDS at the remote site is complete. This is the default setting, but it causes problems with certain applications, particularly those involving Windows NT™. For these applications, turn Hold DCD off, which will cause the NDS to pass everything through.

You may also press any of these buttons:

- Click on **OK** to approve your changes (including any you might have made in the **Advanced Setup** window), have the software download them back to the NDS, and close the **Communications Setup** window.
- Click on **Cancel** to discard your changes and close the **Communications Setup** window.
- Click on **Advanced** to access the more complex options in the **Advanced Setup** window (see **Section 5.15.2**).
- Click on **Default** to have the window display the default values for all parameters. (The parameters are not actually restored to their default settings unless you proceed to click on **OK**.)

5.15.2 Changing the Advanced-Setup Options

While you are in the **Communications Setup** window, you can click on the **Advanced** button to bring up the **Advanced Setup** window, as shown below:



You may set these parameters, which govern NDS↔modem interaction, at this window:

- **Break Symbol:** The character that will be repeated three times to represent the Break signal. The default value of this parameter is "+" (the plus sign).
- **Break Guard Time:** The time in milliseconds before and after the transmission of a Break signal (three break characters) during which data transmission must stop in order for the Break to be recognized.
- **Originate:** After receiving a Break, the Network Data Security unit goes into Command mode, transferring data in the clear. Receiving the Originate command from the attached computer causes the NDS to switch back to Data mode (encryption active). The default value for this parameter is the standard modem Originate command, ATO.
- **Hang Up:** The NDS will send this command to the attached modem if it cannot establish a session. The default value for this parameter is the standard modem Hang Up command, ATH0.
- **Initialization Delay:** How long, in milliseconds, the NDS will transfer all data in the clear (unencrypted) after detecting the DCD (Data Carrier Detect) signal. During initialization, some modems cause DCD to go high relatively early, after which certain transmissions must continue in

order to complete initialization. The maximum value for this parameter is 2000 (2 seconds); the default setting is 0 (no delay).

You may also press any of these buttons:

- Click on **OK** to approve your changes and close the **Advanced Setup** window. (Your changes aren't downloaded back to the NDS until you click on **OK** in the **Communications Setup** window.)
- Click on **Cancel** to discard your changes and close the **Advanced Setup** window.
- The **Search/Add...** button will be active only if the connected NDS is version 1.9 or higher. Certain applications for the Apple® environment use programs such as ARA (Apple Remote Access) and Timbuktu that cannot edit modems' initialization strings. Click on this button to have the NDS search the connected modem's initialization string for the &F command and, if it is there, add &C1 after it. This ensures that the modem allows DCD to follow carrier rather than holding it high.
- Click on **Default** to have the window display the default values for all parameters. (The parameters are not actually restored to their default settings unless you proceed to click on **OK**.)

5.16 Saving Changes

When you begin running the Security Administrator's software, the **Update** button at the far right of the **Audits** screen is "grayed out" and inactive. But when you make any changes to the authorization IDs, passwords, or any other options except communication parameters that you've uploaded from a connected Network Data Security unit, the **Update** button becomes active ("darkens in"). Once it does, click on it to download your changes to the connected NDS, which will save the new settings permanently in its NVRAM (nonvolatile memory).

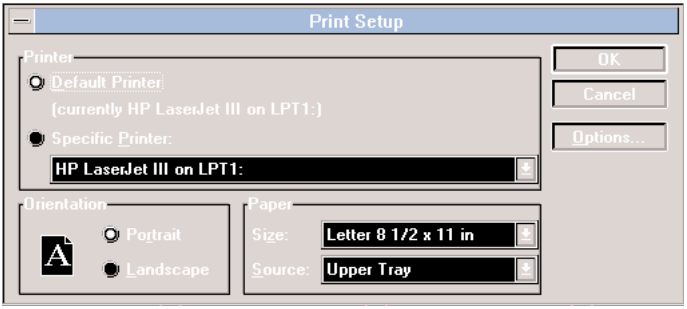
5.17 Printing

With the Security Administrator's software, you can not only print out the authorization table of the connected Network Data Security unit, you can even verify what the printout will look like before you do so. The print functions are in the **File** menu.

5.17.1 Print Setup...

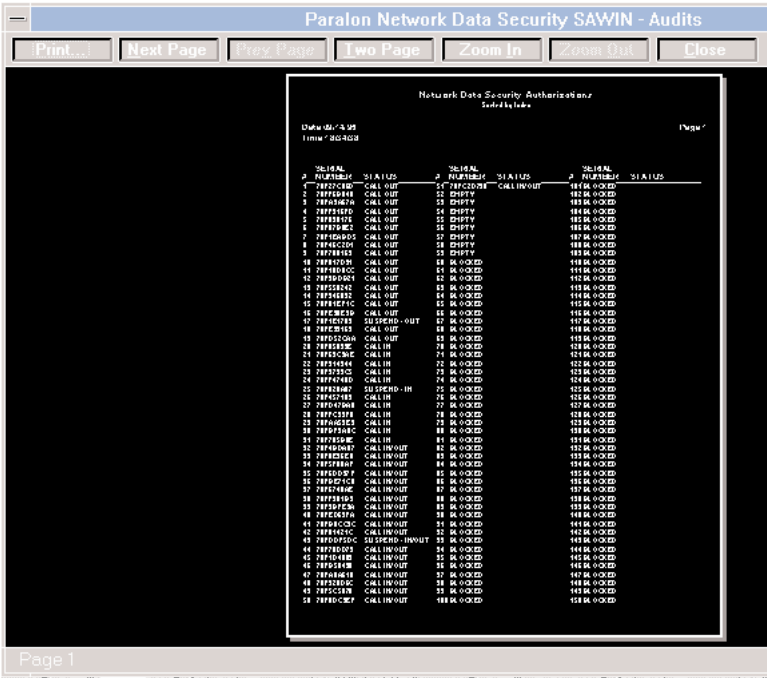
When you select **Print Setup...** from the **File** menu, the **Print Setup** window appears, as shown below. At this window, you can choose and configure your desired printer in the same way you would for most Windows applications.

For more information about printing and printer configuration, refer to your Windows documentation.



5.17.2 PRINT PREVIEW

When you select **Print Preview** from the **File** menu, the background **Audits** screen changes (as shown below) to display how the authorization-ID table should appear on paper if you use the Security Administrator's software to print it out.



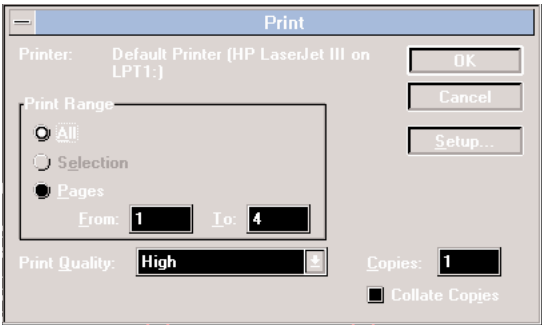
5.17.3 PRINT

When you select **Print** from the **File** menu, the **Print** window appears (it will be similar to the one shown below). At this window, you can trigger the actual printing of the connected NDS's authorization table. All information that was displayed in the print preview will be printed, unless you limit the print range (see below).

Consider using view filters (see **Section 5.4**) to avoid printing unnecessary information.

Depending on your printer and the view filters you have chosen, the number of pages printed will vary.

For more information about printing and printer configuration, refer to the documentation for Windows and/or your printer.



5.18 Using Multiple Security Administrators

This section pertains only to those applications in which individual Network Data Security units are to be maintained by more than one Security Administrator.

Each NDS can be attached to and administered by up to five different SAs. When NDSes ship from the factory, they have one "open" SA-ID slot (memory location) available, plus four more "locked" slots:

When an SA makes the initial attachment to an NDS, the open slot is used. From now on, no other SAs can be attached to that NDS until you enable such an attachment with the **Attach another SA** function:

To allow another SA to attach, select **Security Control** from the **Network Data Security** menu. If necessary, enter the Maintenance Password. Select **Attach another SA to this Network**. Click on **OK**. The connected NDS can now accept another SA attachment, as shown below.

When two or more of an NDS's SA slots are filled, any of the authorized SAs can execute the **Attach another SA** function, enabling another to be added.

When all five of an NDS's slots are occupied with valid authorized SA IDs, no more SAs can be authorized to attach to that NDS. Any of the five SAs can remove *themselves*, leaving space for a new authorization.

To remove the current SA's authorization from the connected NDS, select **Security Control** from the **Network Data Security** menu. If necessary, enter a Maintenance Password. Select **Remove this SA from this Network**. Click on **OK**. The SA immediately loses its attachment to the connected NDS. If any other SAs are still authorized to attach to this NDS, the current SA cannot be reattached to it until you OK the attachment through one of the authorized SAs.

If all SA authorizations are removed, the NDS retums to its original "one-plus-four-empty" status, as shown at the top of the previous page.

6. Troubleshooting

If you have difficulty operating a Network Data Security unit, refer to your NDS manual. You can also refer to the NDS Troubleshooting Guide included with the Security Administrator's software. To bring up the Guide on-screen, click on its icon in the Security Administrator program group. (The Guide is actually a Microsoft Word for Windows document, so you must have Word for Windows or a compatible Windows word-processing or desktop-publishing package to view or print it.)

If you have difficulty with a Security Administrator, call Black Box as directed below.

6.1 Calling Black Box

If you determine that your Security Administrator's hardware or software is malfunctioning, *do not attempt to alter or repair it.* The hardware is particularly likely to be irreparably damaged during any such attempt, because as a security device it is designed to be tamper-resistant and to break rather than be compromised. Contact Black Box instead; the problem might be solvable over the phone.

Before you do, make a record of the history of the problem. Black Box will be able to provide more efficient and accurate assistance if you have a complete description, including:

- The nature and duration of the problem.
- When the problem occurs.
- The components involved in the problem.
- Any particular application that, when used, appears to create the problem or make it worse.

6.2 Shipping and Packaging

If you need to transport or ship your Security Adminstrator:

- Package it carefully. We recommend that you use the original container.
- Before you ship a unit for repair or return, contact Black Box to get a Return Materials Authorization (RMA) number, and make sure you include everything you received with the unit when you ship it.

Glossary

Administration Password

An optional password you can assign to a particular Network Data Security unit. When an NDS is assigned an Administration Password, users must enter the password in order to attach a Security Administrator to the NDS. Administration Passwords must be 5 to 8 characters long.

BBS detect - Outbound
An option that, if enabled, allows an NDS to establish outbound connections with public on-line services while maintaining inbound security.

Blocked
An empty memory location that is unavailable for authorization programming. Blocked memory locations cannot be programmed until they are changed to Empty.

Delete ID
Removes an authorization ID from the connected NDS's ID table. Once an ID is deleted, it cannot be recovered without mating the hardware.

Empty
A memory location available for authorization programming. When two NDSes are mated for programming, the first Empty memory location found in each NDS's ID table is used for storing the new authorization ID.

Maintenance Password
An optional additional password you can assign to a particular Network Data Security unit. When an NDS is assigned a Maintenance Password, users must enter the password in order to change the status of memory locations. Maintenance Passwords must be 5 to 8 characters long.

Memory locations
500 RAM locations in each NDS that are used for storing authorization IDs.

Restore ID
Reinstates the original authorization status for a suspended ID. The restored ID occupies the same table location and has the same authorization status (one-way inbound, one-way outbound, or two-way) that it did before and during suspension.

Search for/Find ID
Scans the authorization table for a specific ID.

Suspend ID
Removes authorization status from a programmed ID without removing the ID from the table. A suspended ID still occupies one table location.

Switch always ACTIVE
An option that, if enabled, logically locks the SECURITY switch of the connected NDS in the ACTIVE position, regardless of the switch's physical position. This option has no effect on the switch during authorization programming.

Unblocking
Changes the status of a Blocked location to Empty.

TRADEMARKS USED IN THIS MANUAL

Apple is a registered trademark of Apple Computer, Inc.
AT, IBM, and PS/2 are registered trademarks, and PC/XT is a trademark, of IBM Corporation.
CompuServe is a registered trademark of CompuServe Incorporated.
Microsoft and Windows are registered trademarks, and Windows NT is a trademark, of Microsoft Corporation.

All other trademarks are the property of their respective owners.

DISCLAIMERS

The manufacturer will not be liable to you or anyone else for any damages that result from the the use, misuse, or failure of this product, or from the breach of any express or implied warranties. Such damages might include damage to other equipment; lost data; lost profits; compromise of private, confidential, or classified material or information; or any indirect, special, consequential, incidental, or punitive damages however caused. In no event will the manufacturer be liable for any amount greater than the suggested retail price of the Security Administrator.

(Some states do not allow the limitation or exclusion of incidental or consequential damages, so the above limitation and exclusions might not apply to you.)

In no event will the manufacturer be liable for any loss of programmed authorizations or for reprogramming specific authorizations which might have been programmed into any Security Administrator ("SA"). The manufacturer does not warrant uninterrupted or error-free operation of the SA, or that data encrypted by the SA cannot be decoded by an unauthorized third party.

The software of the Security Administrator ("SA") that is described in this document is furnished under the the license agreement described below. The software may be used or copied only in accordance with the terms of this agreement. This agreement will be construed according to the laws of the State of Washington.

LICENSE AGREEMENT

By using the Security Administrator's software, you accept the following terms of this License Agreement. If you do not agree with these terms, you should not use the SA; return it promptly for a refund.

The manufacturer retains ownership of the SA's software. All of the SA's software is provided with a limited license that governs your use of the software with Network Data Security and SA hardware. These are the terms of your limited license:

1. You may load this software on up to four (4) computers, provided that when it is run during actual connection with SA hardware it is run on only one computer at a time. You may not load this software on any computer that is not under the direct and continuous control of the licensee.
2. You may not transfer this software to another party without express written permission from the manufacturer.
3. You may not distribute, rent, sublicense, or lease this software or its documentation.
4. You may not translate, decompile, or disassemble this software. You may not reverse-engineer any part of the SA hardware or software, nor may you create any derivative works.
5. You may not transmit this software across any telecommunications link.

This license and your right to use this software will be automatically terminated if you fail to comply with any provision of this license agreement.

The manufacturer retains all rights not specifically granted. Nothing in this license agreement constitutes a waiver of the manufacturer's rights under U.S. copyright laws or any other federal or state law.

1000 Park Drive • Lawrence, PA 15055-1018 • 724-746-5500 • Fax 724-746-0746