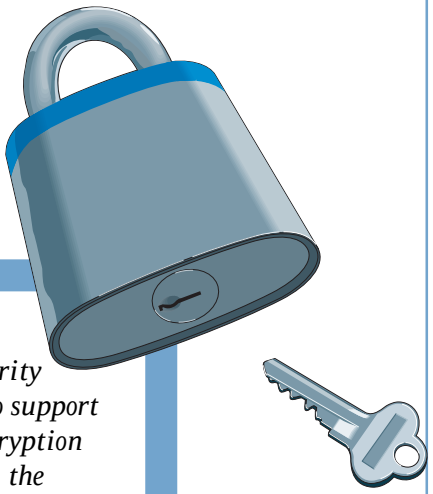
Security Guide



The NetComm Security Guide is provided to support the security and encryption features included in the following products:

- *SmartModem 336*
- *SmartModem 336D*
- *SocketRocket 336*
- *ProRack* 336

CLICK TO CONNECT TO THE 'NET FOR THE LATEST UPDATES
NET CONNECT

Version B
May 1997

NetComm®

Contents

Copyright Information

Security & Encryption

Your modem has many sophisticated security features. Your modem limits caller access by means of user names and passwords. User names and passwords are stored in the modem's non-volatile memory.

With each user name and password a modem command of up to 30 characters may be specified. This allows the implementation of callback to users. Callback is where the modem rings a specified phone number. Even if an unauthorised caller manages to break the modem's security, that caller must be connected to the phone number specified in the remote modem's database.

Also discussed in this section is the topic of DES (Data Encryption Standard) encryption, which allows you to encrypt data being passed to a remote modem.

The Security Menu

All additions and changes to your modem's user and password lists are performed through the Security Menu. This menu is displayed when you use the #S command.

- Type: AT#S <E>

  A prompt will appear: Enter Security Password:

  When you first receive your modem, all passwords will be set as a single Carriage Return (ENTER).

- Press the ENTER key

  The Security Menu will be displayed:

```
SECURITY MENU

Q  = Quit                                1  = List Users
2  = Add or Change Users                 3  = Delete All Users
4  = View Access Record                  5  = Reset Access Record
6  = Security Off                        7  = Security On
8  = Change Security Password            9  = Encryption Controls
A  = Stored Phone Numbers Displayed      B  = Supressed
C  = Set Password Expiry Days            E  = Minimum Password Length
D  = Download Security file to host      U  = Upload Security file from host
L  = Encryption Parameters/Keys LOCK     F  = FREE Encryption and Dial Enable
K  = OutDial Disable                     M  = Dial Stored Phone Numbers Only
N  = Change Database Local/Remote        O  = Clear Statistics
P  = SNMP Database Access En/Disable     Z  = Zero All Accounts
R  = 64bit DES/40bit DES

Access Security: ON      Security Database and Security Mode: FREE
Stored Phone Numbers: DISPLAYED   OutDial: ENABLED
Database: LOCAL
SNMPAccess: ENABLED   DES: 64bit


Enter Security Function :
```

Entering a Security Password

You may choose to have a dedicated security password, thus changing the password assigned for the first security user. To enter a new security password:

- Select Option 8 from the Security Menu <E>

  You will be prompted to enter a new security password. Your modem is case insensitive. Up to 8 characters may be used, including spaces.

When you enter your password, each character will appear on the screen as a # character.

- Type in your new password <E>

  You will be prompted to re-enter the new security password.

- Type in your new password again <E>

  Your new password will be stored in your modem's non-volatile memory.

Adding and Changing Users

Your modem allows you to add new users and change existing users. Selecting option 2 on the Security Menu will result in a prompt:

Enter Name:

To add a new user:

- Type in the name of the new user <E>

User names must not be longer than 30 characters. They are NOT case sensitive.

To change an existing user:

- Type in the name of the user you wish to change <E>

You will be prompted to enter a new name.

- Type in the new name <E>

- If the user is found you will be given the option to change the password, delete the user or zero their access counters.

If you are adding a new user or changing a user, you will be prompted for a new Password (maximum characters = 15).

You then will be prompted for 'Options' after the password has been entered. You may key S or E or both, if you do not want either option key ENTER.

❑ S Specifies that the user is a supervisor and has full remote access rights to the remote modem.

- If you key **** you will be able to issue almost all AT commands on the remote modem and access the full security database if you have the global security password. (See remote access)

❑ E Your user password does not expire.

- This would be for automated systems that cannot respond to prompts to enter a new password when it expires

The modem will now prompt you to enter a modem command. Modem commands consist of up to 30 characters and may include spaces. When you enter a new command, the previous command will be overwritten.

☞ Do not include an Attention Code (AT) with your command. Your modem automatically places an AT at the start of this command when it is executed.

If you do not want to specify a modem command or want to leave the current command as it is:

- Press ENTER

If you want to remove the existing command but do not wish to replace it with another command:

- Press the Spacebar <E>

See details on Callback Security later in this section for more information about using commands with your user names.

If you do not enter a command you will be given the option of entering a SuperSecure DES Key for the user. To use this feature refer to the 'SuperSecure Advanced Security Mode' or else press ENTER to go on to the next user.

Removing Users

Your modem allows you to remove individual users or all the users currently stored in your modem. To remove an individual user:

- Select option 2 from the Security Menu

  You will be prompted to enter a new user name.

- Type in the name of the user you wish to delete <E>

  If the user is found, select the 'D' option to delete.

To delete all the users stored in your modem:

- Select option 3 from the Security Menu

  You will be prompted to confirm that you wish to remove all user names, passwords and commands

- Press Y <E>

Listing Existing Users

To list all user names, and commands.

- Select option 1 from the Security Menu <E>

  Your modem will list the user names.

  Passwords are never displayed.

☞ Your computer must be capable of displaying at least 80 characters per line for the user list to be displayed in its correct format.

The Access Record

Selecting option 4 and option 5 from the Security Menu allows you to view and change the access records. Your modem keeps a tally of the number of successful (granted) and unsuccessful (denied) attempts to connect to your modem using each user name.

Your modem allows every caller three attempts to enter the correct user name and password. If the caller cannot correctly enter the password, a record is made by your modem that an unsuccessful attempt has been made to use that particular user name.

If the number of unsuccessful calls for any user name reaches 255, that user name will be locked and callers will no longer be able to use it, even if the correct password is used. You will not be able to use that particular user name until the access record for all users has been reset.

If, however, the caller does correctly enter the password, your modem records that a successful attempt was made to connect with that user name.

You should regularly check the number of successful and unsuccessful attempts to connect to your modem.

- Select option 4 to view the access record <E>

An unusually high number of unsuccessful attempts to connect with a particular user name may indicate someone is trying to violate your modem's security.

Over a period of many months one of the security users may legitimately accumulate 255 errors, in which case, your modem will automatically lock that user. If this occurs, select option 2, enter the user's name and select the Z option to clear his access record.

Each attempted access with an unknown name increments the 'Invalid Usernames Received' count at the top of the list.

Enabling Modem Security

Selecting option 6 or option 7 allows you to disable or enable your modem's security mode. With security mode enabled, whenever your modem answers an incoming call it will demand the caller enter a user name and password — the following message will appear on the caller's computer screen:

Enter Name:

If only one of the modems is configured to use error correction, there will be a slight delay between the time the modems connect and when the caller is asked to enter his user name.

When the caller enters his name all characters will be displayed as # characters. The caller is allowed three attempts to correctly enter his name. Your modem is not case sensitive to user names.

If the caller enters a valid user name, your modem will ask the caller to enter the password associated with that user name.

Enter Password:

If the caller enters his password correctly, your modem will send the message ACCESS GRANTED and the caller will have access to the computer connected to your modem.

If the caller cannot, within three attempts, enter the correct user name and password, your modem will send the message ACCESS DENIED and will hang up.

Quitting the Menu

The Quit Security Menu option allows you to return to local command state from the security menu.

- Press 0 <E>

  Your modem will issue an OK message. You will be returned to local command state.

Callback Security

As mentioned earlier, your modem allows you to specify a modem command with every user name and password. This feature allows you to implement modem *callback*. Callback means that after a caller has successfully connected, your modem will hang up and then dial the caller.

Even if an unauthorised caller successfully connects to your modem, that caller will have to be using the phone line which your modem is going to call back.

Three commands are required to implement callback. First, you must hang up your modem with a H command.

Before your modem can call the caller back, it must wait for the caller's modem to hang up and return to local command state. S Register 27 contains a value representing the number of seconds your modem will wait before commencing dialling. The default value for this register is 0 — your modem will begin to dial as soon as it receives a dial command.

It is necessary, therefore, to place another value in S Register 27 to allow the caller's modem sufficient time to hang up before your modem begins to dial. A 30-second delay should be sufficient time to allow most modems to hang up, so place an S27=30 in the command.

Using a 30-second delay means the telephone exchange, in most cases, will disconnect the call. This ensures unauthorised callers cannot 'fool' callback security by not hanging up after your modem hangs up.

Alternatively, contact your telephone company — some telephone companies offer an automatic disconnect facility, which assumes a caller cannot remain off-hook after the modem has hung up.

Place a D command and the caller's phone number in the command. Assuming the caller's phone number is 1234567, you will now have a command which looks like this:

H S27=95 D1234567

After the user has been called back and has completed the call, your modem will hang up, automatically issue an ATZ command to restore all the stored settings and return to local command state. The ATZ command will effect some settings - to save your configuration, issue a &W after you initialize the modem.

☞ UK Modems. Telephone exchanges in the UK may not hangup after 30 seconds. Consult the supplier of your telephone line for a possible solution.

☞ If security is enabled, the answering modem will not assert DCD or DSR until a valid user name and password are received. If \Q5 is selected, CTS will not be asserted until a valid user name and password are received.

Downloading the Security File

Selecting option 'D' from the security menu will enable a dump of the security database to your computer for storage or editing. You will be asked to type 'Y' to start the download.

The file format is:

"<user name>", "<password>", "<command>", nnn, mmm CR LF where nnn and mmm are the 3 digit Granted and Denied Access Counts and CR and LF are Carriage Return and Line Feed.

The last entry has only a CR LF

☞ The download will take place at the current terminal speed. No flow control is acknowledged. If your computer cannot accept the file at the current data rate exit security and autobaud to a lower speed.

Example: "FRED", "NURK", "HS27=30DT3277502", 000, 000 is a valid entry.

☞ The Socket Rocket only supports a security user database of 100 users, so if this limit is exceeded you may have to:

- Download the Security Database to diskette

- Using a text editor, delete all users except the desired users (up to 100)
- The last entry has only a CR LF
- Upload as per the following

Uploading the Security File

Selecting option 'U' from the security menu will enable a security file in the format described under the Download command to be uploaded into the modem. You will first be warned that your existing database will be overwritten and then told to start uploading the file.

When the upload is finished the modem will return to the security menu. The upload will take place at the current terminal speed. The modem can accept data at 115Kbps.

☞ If the data is not in the correct format, the file can be corrupted, so edit with care and always keep a copy of the unmodified download file.

Encryption

Your modem supports Data Encryption Standard (DES) encryption. DES encryption allows you to encrypt data being passed to a remote modem. The remote modem must support Cipher Feedback (or CFB) DES encryption in order to decrypt the data sent from your modem.

The #E1 command is used to enable DES encryption.

The modem requires you to enter an encryption *Key* and an *Initial Value*. These are two 16-character hexadecimal numbers. Both the Key and Initial Value are specified by the user, making the encrypted data virtually impossible to decrypt without access to the Key and Initial Value.

Both modems must have DES encryption and error correction selected and must use the same encryption Key and the same Initial Value.

☞ Only use a reliable error correction mode when using DES encryption. This will ensure you will only establish encrypted connections.

The modem can store up to 10 DES Key/IV pairs. Use AT*K to select the Key you wish to use. For example AT*K5 tells the modem to use the key and IV from register 5.

To enter the DES Key and Initial Value:

- Type: AT#S <E>
- Type: 9 <E>

  You will be prompted with the following message:

  Select DES Key register (0-9) (Key ENTER/or main menu):
  You should select one of the 10 available registers to store the new Key.
  The modem will respond:

  Enter New DES Key:.....

  Re-enter DES Key:.....

Enter new DES IV:.....

Re-enter DES IV:.....

- Enter the Key and Initial Value as a 16-character hexadecimal number <E>

  You will be prompted to re-enter the Key and Initial Value, to verify the correct Key and Initial Value has been entered.

  You may then enter a new DES Key into another register or press ENTER to return to the main menu.

To enable DES encryption, issue the AT#E1 command. The next time your modem establishes a connection with another modem, it will encrypt outgoing data and attempt to decrypt incoming data.

☞ For countries other than Australia, DES encryption is only available to end users who meet the security requirements of the Australian Department of Defence. Contact your modem supplier for details of making application for a DES equipped modem to be supplied to you.

SuperSecure Advanced Security Mode

SuperSecure mode allows you to :

- ❑ Have an individual password and an individual DES KEY.
- ❑ Automatically change the DES key in a random manner after each connection without the keys ever being knowable.
- ❑ Have a different password on the answering modem to the originating modem.
- ❑ Timed expiry of passwords.

With these new features, a link between two modems will be very secure. No other modem can dial either modem and connect because the third party will not know the keys of the other users, even if both passwords are known.

Entering a Key for Each User

- Enter AT#E2 to enable SuperSecure mode
- Select the security menu using AT#S
- Enter the security password to gain access to the security menu
- Set up the modem's primary DES KEY and Initial Value (IV) as per standard DES setup
- Select Option 2 to add new users
- Enter the username
- Enter the password to be used by your modem (not necessarily the same as the password on the modem you are going to dial)

☞ Do not use a / character in any password, because this character is reserved.

- When the modem prompts you for a command, do not enter a command because you will not be prompted for the DES KEYS
- Enter the 16 hex digit DES secondary KEY for the user, all 16 digits must be keyed
- Enter the 16 hex digit DES secondary Initial Value (IV) for the user, all 16 digits must be keyed
- Enter the 2 hex digit Key Encryptor (KE) for the user, both digits must be keyed

☞ The Key, IV and KE can have any value but must be exactly the same on both answering and orignating modems.

☞ For maximum security do not use keys or initial values that have easy to remember values.

☞ A KE of 00 turns off random key rotation.

- Enter as many users as you wish whilst in this mode
- Press ENTER at the username prompt to return to the menu

☞ You do not have to turn security on to use SuperSecure. The #E2 option forces it on always.

- Enter 0 to exit the security menu

☞ The remote modem must not only support SuperSecure but must also have a matching username/password and KEYS before access can be gained.

Accessing a System Using SuperSecure

If both your modem and the remote modem have been correctly setup you can:

❑ Dial the remote system.

❑ The modems will connect and enter security dialog mode using the modem's primary key.

❑ This key must be the same for both modems.

- Enter your username
- Press ENTER
- Enter your user password stored in the remote modem then '/'
- Enter your password stored in your modem
- Press ENTER

☞ You may backspace to correct errors but you will not be able to see what is typed since all characters are echoed as #

- Do not use the / character in any password
- If the password is the same on both modems then only one password needs to be entered

Connection

- ❑ You will then CONNECT if the username, both passwords, all of the KEYS, IVs and KEs match.
- ❑ The data will be correct and error free, but encrypted on the line using a KEY unknown to anyone.

Disconnection

- ❑ If the primary DES KEY mis matches you will not be able to read the "username" prompt.
- ❑ The modems will disconnect if:

- The secondary key, IV or KE mismatches (you will also receive a message)
- An error corrected link cannot be established
- Wrong username and/or password is used. You will be given another two chances to enter them before the modem disconnects

Example:

ATDT 456 4321
RINGING
RINGING
Enter name: MarkStein
Enter password: Fudge/Vanilla
Access granted

- 'Fudge' is Mark Stein's password on the remote system
- 'Vanilla' is the password on the local modem
- 'Access granted' confirms that the passwords are correct
- Secondary keys mismatch if the secondary KEY, IV or KE are different

Enabling Rotating Secondary Keys

- ❑ If you enter a KE of 00 for the user, then the secondary key will remain the same for each connection.
- ❑ If the KE is not 00 then this value is used as a seed to create a random new secondary key for the user on each connection.
- ❑ After the initial connection is made with the KEY, IV and KE you have entered, these values will change on both modems to new values which are not accessible by any means.
- ❑ If an event occurs that corrupts the KEY, IV or KE on either modem, then both modems will have to be manually set back toa known starting point.
- ☞ To ensure random unknown keys, make two connections between the secure modems after they have been initialised.

Symmetrical Operation

- ❑ Either modem can originate the call.
- ❑ Remote modem's password is first.
- ❑ Local modem's password is second.

Automatic Synchronisation

- ❑ The keys only change after a successful connection is achieved at both ends.
- ❑ If either modem drops out during the security handshake before the CONNECT message, the modems will automatically resynchronise on the next connection.

Password Expiry Option

You may specify the number of days you have before the password must be changed. By default this option is OFF, to enable it select the C option from the security menu. You will then be prompted for the number of days before a password expires (1-255 days). The access record (Option 4) displays the password age limit and the age of each user's password.

❑ When a password is within 5 days of expiry a message will be given before the connect message.

❑ After the password has expired, you will be informed and will not be allowed another connection until a new password is entered. The access record also notes if you have been informed of the expiry.

❑ Either the remote or the local password or both may expire.

☞ There is no real time clock inside the modem. When the modem is turned off the clock stops. Therefore the expiry timers actually time the number of days that the modem is turned on and not elapsed days.

Entering a Password in the Remote Modem's Database

When connected in SuperSecure, you may change your password.

- Enter **** with a 1 second guard time on either side of the stars
- Enter your current password
- Enter your new password
- Verify your new password
- You will then be returned online

Entering a New Password in the Local Modem's Database

When connected in SuperSecure, to change your password:

- Enter in the escape sequence +++
- Enter in the *S command
- Enter your new password
- Verify your password
- ATO to return online

☞ If you are not online or in the current session of SuperSecure, you must identify yourself by entering your current username and password before being able to enter your new password.

Minimum Password Length

You can specify the minimum password length accepted by the modem by the E option from the Security Menu. Its power-on default is 3 characters.

Uploading and Downloading the SuperSecure Database

- To ensure the integrity of your modem's security database the sensitive fields are encrypted with the modem's primary key. Your password and DES KEYS are scrambled but will be restored when uploaded into a modem with the same primary key.

- You may delete unwanted records and modify the unencrypted fields, but the encrypted fields must not be touched.

- If you wish to enter a new user, you may do so using the same format as the other records.

  The three digit control field at the start of each record should be set to the following values for a new user:

  000 Not SuperSecure User, no DES keys specified (use for dialback)
  001DES keys specified
  003 DES keys specified, Supervisor Status
  005 DES keys specified, No password expiry
  007 DES keys specified, No password expiry and Supervisor Status

- The record format is:

  aaa, "<username>", "<encrypted password>", "<command>", "bbb,ccc,ddd,eee,fff,ggg", "<encrypted key>", "<encrypted> IV", "<encrypted KE>"CR,LF

  - aaa is 3 digit control number
  - bbb is 3 digit access granted count
  - ccc is 3 digit access denied count
  - ddd is 3 digit days since password change
  - eee is 3 digit reserved
  - fff is 3 digit reserved
  - ggg is 3 digit reserved

☞ The control number should not be touched on existing users.

Security Database Lock Option

From the Security Menu you may elect to LOCK the security database with the 'L' option. When locked, the user cannot change the #E setting or clear the security database even with the &F. command or power-on reset with the Mode Switch depressed.

The only way to alter the database or #E selection is to enter the Security Menu with the security password and unlock the database with the 'F' (Free) command.

The current state: LOCKED or FREE is displayed below the Security Menu.

☞ Shorting out the NOVRAM battery will erase the database but will result in the modem being only partially functional. Such modems need to be returned to the factory for re-configuration.

Outdial Disable Option

If modems are to be used only for receiving calls option 'K' can be selected. This does not allow the modem to dial out. If an attempt to do so, users will be informed that a SECURITY LOCKOUT is in place and the call will not be successful.

The outdial feature will be useful for system administrators who wish to control the use of modems within remote offices or restrict modems to being used for receiving calls only.

Dial Stored Phone Numbers Only Option

Option 'M' is similar to Option 'K' but restricts the modem to dialling only those numbers listed in the stored phone number fields as set with the &Z command.

The stored numbers must then be dialled using the ATDS=X command where X is the position of the stored number as set with the AT&Z command.

New stored numbers cannot be added by the user once the dial restriction has been enabled.

General Notes on Data Security

- ❑ By using SuperSecure you now have
  - Ensured that the phone link between two modems is secure
  - Ensured that no other user can access either modem when #E2 is enabled
- ❑ The weak link in the system is now the cable between your modem and your computer.
  - It should be kept visible at all times to prevent wire tapping
  - The modem, computer and interconnecting cable should be physically secure to prevent access
- ❑ With specialised equipment, the data on the lines and the image on an screen can be read, due to wires and video screens radiating radio frequency signals which can be picked up over a distance. You may need advice on radio frequency screening if this concerns you.

Distinctive Ring

The modem is able to discriminate between three different types of rings. This is useful if you purchase the Telstra Duet service. With Telstra Duet, two phone numbers are shared for one telephone line. One is for voice and the second is for your modem.

To enable the modem to answer only when your modem number is dialled, issue the command AT-SDR=4S0=2 (this can be saved with AT&W). For most users, AT-SDR=4S0=2 will be suitable. Do not set Auto Answer for less than two rings when Distinctive Ring is enabled.

Distinctive Ring Commands

AT-SDR=n,	where n=0 to 7, default=0
AT-SDR=0	Any ring detected and reported as "RING"
AT-SDR=1	Single ring detected and reported as "RING1"
AT-SDR=2	Double ring detected and reported as "RING2"
AT-SDR=3	Single and Double ring detected and reported as "RING1" or "RING2"
AT-SDR=4	Triple ring detected and reported as "RING3"
AT-SDR=5	Single and Triple ring detected and reported as "RING1" or "RING3"
AT-SDR=6	Double and Triple ring detected and reported as "RING2" or "RING3"
AT-SDR=7	Any ring detected and reported as "RING1" or "RING2" or "RING3"

Contact Information

Please contact NetComm for help, information, sales enquiries or to join the NetComm Info Mailing List:

Customer Care Centre

Updates:	Click on the NetConnect icon, located on the front page, to connect to the internet and receive NetComm's latest product information and updates. *Your computer will need to be configured with an internet connection to use this feature.*
Email:	support@netcomm.com.au
Web Page:	http://www.netcomm.com.au
FTP site:	ftp.netcomm.com.au
Fax:	(02) 9887 4274
Phone:	1 800 642 067or 9878 7473 in the Sydney metropolitan area
BBS:	(02) 9878 3755

TeleMarketing

Fax:	(02) 9805 0254
Phone:	1 800 269 950 or 9878 7333 in the Sydney metropolitan area

Mailing List

For the latest sales and technical information, subscribe to the NetComm Info Mailing List by sending an e-mail to:

mailing-list@netcomm.com.au

In the body of the message enter the word:

subscribe

This will add your e-mail address to the NetComm Information Mailing List and you will be e-mailed news and updates regularly.