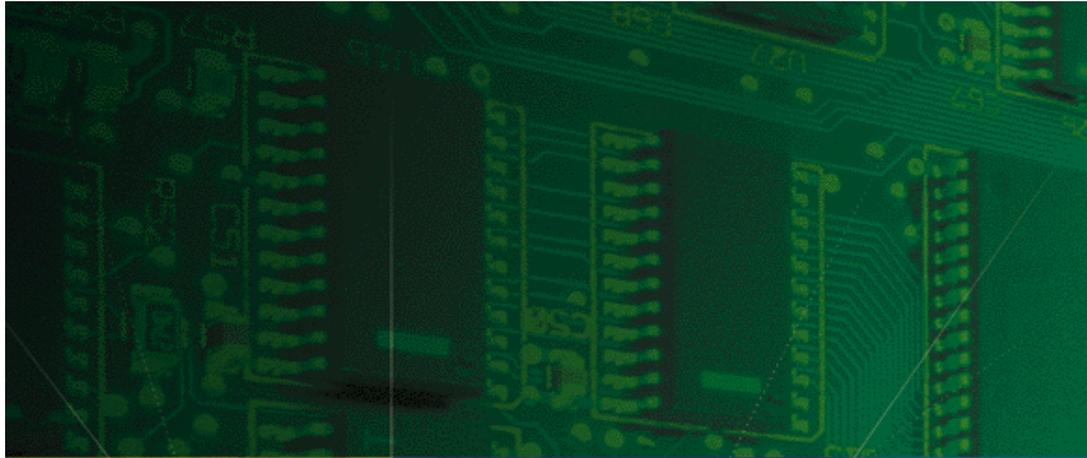




Security and Accounting Server for Windows

Getting Started Guide



Part No. 1.024.1076-03
Version Number 6.0



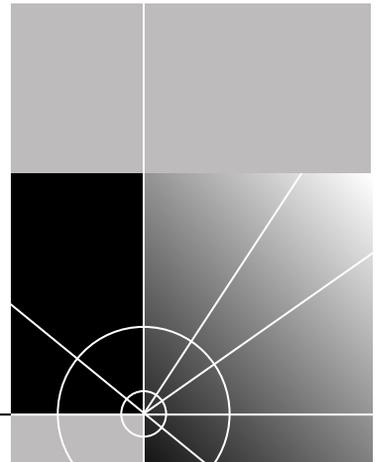
Security and Accounting Server for Windows

Getting Started Guide

Version 6.0

<http://www.3com.com/>

Part No. 1.024.1076-03



3Com Corporation
5400 Bayfront Plaza
Santa Clara, California
95052-8145

Copyright © 1998, 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty of any kind, either implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

UNITED STATES GOVERNMENT LEGENDS:

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

United States Government Legend: All technical data and computer software is commercial in nature and developed solely at private expense. Software is delivered as Commercial Computer Software as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com and the 3Com logo are registered trademarks of 3Com Corporation.

Other brand and product names may be registered trademarks or trademarks of their respective holders.

YEAR 2000 INFORMATION:

For information on Year 2000 compliance and 3Com products, visit the 3Com Year 2000 web page:

<http://www.3Com.com/products/yr2000.html>

CONTENTS

ABOUT THIS GUIDE

Finding Specific Information in This Guide	5
Conventions.....	6
Related Documentation	7
Contact information.....	8

1 OVERVIEW

Network Interaction	1-1
Security Functions	1-2
Security Features	1-3
Accounting Functions.....	1-4
Accounting Features.....	1-5
New Features in this Release.....	1-5
VPN Support	1-5
MS-CHAP, MPPE Support	1-6
EAP Support	1-6
Additional Network Access Server Support.....	1-6
Support for Multi-Link with Third-Party Tokens.....	1-6
Ability to Proxy RADIUS Accounting Records	1-6

2 INSTALLATION

System Requirements	2-1
NMC Dependencies	2-1
Microsoft Access Dependencies.....	2-1
Installing correct ODBC drivers	2-2
Microsoft Graph5 and Graph 8 Error	2-2
Installing Security and Accounting Server.....	2-3

3 INITIAL CONFIGURATION

Database Configuration	3-1
Starting the Database Manager	3-1
Client Configuration	3-2
Configuring the Security Server.....	3-2
Configuring the Accounting Server	3-3
Example Configuration	3-3
Setting Up a New User.....	3-4

4 TESTING THE INSTALLATION AND TROUBLESHOOTING

Testing the installation	4-1
Start Security and Accounting Server	4-1
Testing Your Configuration	4-2
Troubleshooting	4-3
Upgrading to Windows 98	4-3
Edit the services file	4-3
Re-install Security and Accounting Server.....	4-3
Access Quits Unexpectedly.....	4-3
Screen Tab Errors	4-4
Security and Accounting Server Does Not Start	4-4
Microsoft Graph5 and Graph 8 Error	4-4
Winsock32.dll error	4-5
Running S/A on Windows NT.....	4-5
Event Logging.....	4-5
Running Security and Accounting as a Service.....	4-6

INDEX

ABOUT THIS GUIDE

About This Guide provides an overview of this guide, describes guide conventions, tells you where to look for specific information and lists other publications that may be useful.

This Getting Started Guide provides you with the information needed to install and start Total Control™ Security and Accounting Server. This guide contains a short description of the application, but does not discuss all of the features of Security and Accounting Server. For more information, refer to the Help system in Security and Accounting Server.

This guide is intended for network administrators with some training or experience working with Total Control equipment. It is assumed that you understand the basics of networking, database management, and Windows 95 or Windows NT operating system.



If the information in the release notes shipped with your product differs from the information in this guide, follow the instructions in the release notes.

Finding Specific Information in This Guide

This table shows the location of specific information in this guide.

If you are looking for	Turn to
Troubleshooting help	Chapter 4
A list of contacts for support	this chapter
How to install Security and Accounting Server	Chapter 2
How to configure Security and Accounting with your database	Chapter 3
How to configure the Server to work with a client	Chapter 3
How to add a user	Chapter 3
A list of new features	Chapter 1

Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

Table 1 Notice Icons

Icon	Notice Type	Description
	Information note	Important features or instructions
	Caution	Information to alert you to potential damage to a program, system, or device

Table 2 Text Conventions

Convention	Description
Syntax	<p>The word "syntax" means you must evaluate the syntax provided and supply the appropriate values. Placeholders for values you must supply appear in angle brackets. Example:</p> <p>Enable RIPIP by using the following syntax:</p> <pre>SETDefault !<port> -RIPIP CONTROL = Listen</pre> <p>In this example, you must supply a port number for <port>.</p>
Commands	<p>The word "command" means you must enter the command exactly as shown in text and press the Return or Enter key. Example:</p> <p>To remove the IP address, enter the following command:</p> <pre>SETDefault !0 -IP NETaddr = 0.0.0.0</pre> <p><i>This guide always gives the full form of a command in uppercase and lowercase letters. However, you can abbreviate commands by entering only the uppercase letters and the appropriate value. Commands are not case-sensitive.</i></p>
Screen displays	This typeface represents information as it appears on the screen.
The words "enter" and "type"	When you see the word "enter" in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says "type."

(continued)

Table 2 Text Conventions (continued)

Convention	Description
[Key] names	<p>Key names appear in text in one of two ways:</p> <ul style="list-style-type: none"> ■ Referred to by their labels, such as “ the Return key” or “ the Escape key” ■ Written with brackets, such as [Return] or [Esc]. <p>If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example:</p> <p style="padding-left: 40px;">Press [Ctrl]+[Alt]+[Del].</p>
<i>Menu commands and buttons</i>	<p>Menu commands or button names appear in italics. Example:</p> <p style="padding-left: 40px;">From the <i>Help</i> menu, select <i>Contents</i>.</p>
Words in <i>italicized</i> type	<p>Italics emphasize a point or denote new terms at the place where they are defined in the text.</p>
Words in bold-face type	<p>Bold text denotes key features.</p>

Related Documentation

The following documents make up rest of the Security and Accounting Server documentation set. Contact your sales representative for ordering information.

- Total Control™ Security and Accounting Server for Windows online Help system

This Help system describes how to use Security and Accounting Server. It also contains context sensitive help for all the system parameters.
- Total Control™ Security and Accounting Server for UNIX Getting Started Guide

This Getting Started Guide contains a brief overview of the Server and instructions to install and start using the software. It also includes the new features included in the release.
- Total Control™ Security and Accounting Server for UNIX Software Reference

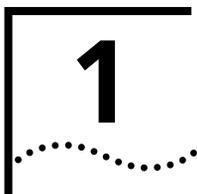
This HTML includes all the information found in the Getting Started Guide and adds detailed information about configuring the Server and your database.

**Contact
information**

Call the appropriate number listed below for technical support.

- If you are calling from the United States or Canada
Dial 1.800.231.8770
- If you are calling from Europe, Middle East, or Africa
Dial 353.1.205.7700
- If you are calling from all other locations
Dial (Your international carrier code) 847.797.6600

For more information about Customer Service, including support, training, service contracts, and ordering printed manuals, visit our website at <http://totalservice.usr.com>.



OVERVIEW

Total Control™ Security and Accounting Server provides call authentication, authorization, and accounting for your network. This chapter:

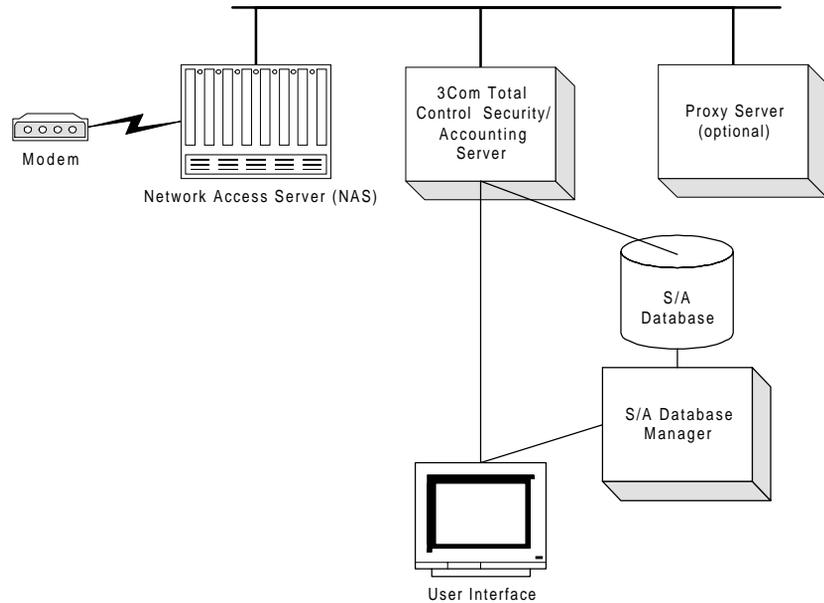
- describes Security and Accounting Server's operation in a client/server environment
- security and accounting functions
- introduces the Security and Accounting Database Manager

Network Interaction

Security and Accounting Server is a client/server security solution. The Security and Accounting Server software resides on personal computer and interacts with Network Access Servers (NAS) using the industry standard Remote Authentication Dial-In User Service (RADIUS) protocol. The NAS is the hardware that manages incoming and outgoing calls to the modems in a remote access concentrator. Several different 3Com products can serve as a NAS:

- Network Management Card (NMC)
- HiPer Access Router Card (HiPer ARC)
- NETServer Card
- NETBuilder II

In addition, Security and Accounting Server integrates with many 3rd-Party NASs. In this document, we use the terms NAS and client interchangeably.



The Server works with a Microsoft Access database to authorize users and to log information about each call.

When a NAS receives a call, you can forward authentication, authorization, and accounting information to Security and Accounting Server. You can also configure the Server to proxy authentication requests to a 3rd-party authentication server, an NT domain, Netware Bindery or NDS.

Security Functions

Security and Accounting Server's security function prevents unauthorized users from making outbound (dial-out) or inbound (dial-in) connections to your network. The Server authenticates users as follows:

- 1 A user dials into a client.
- 2 The client prompts the user for a username and password.
- 3 The user enters the username and password.
- 4 The client sends information to Security and Accounting Server as an access-request message.

- 5 Security and Accounting Server decides whether to process the request, or pass the authentication request on to a 3rd-party authentication server.
- 6 If Security and Accounting Server is set to authenticate the user, it runs the authentication script to process the authentication request:
 - Confirms that the username and password is listed in the database.
 - Confirms that the client's IP address and correct shared secret exist in the database.
- 7 If authentication is valid, Security and Accounting Server sends an access-accept message to the client. This message includes any client configuration information that is stored for the user in the database.

Security Features Password management

Security and Accounting Server offers the following password management features:

- User-initiated password changes
- “No password” option
- Passwords encrypted in database
- Password Flexibility—You are able to configure:
 - minimum password length
 - password expiration date
 - length of time a user can change an expiring password
 - number of failed login attempts before user is blacklisted
 - options available to a user with an expired password

Proxy Authentication

Security and Accounting Server can act as a proxy client and send authentication requests to these types of servers:

- TACACS+
- Novell NetWare Bindery and Novell NDS
- Security Dynamics ACE/Server®
- AXENT Technologies Omniguard/Defender Security Server™
- Secure Computing SafeWord™ (formerly Enigma Logics)
- EAP RADIUS Servers

Local system password authentication

When running on Windows NT, Security and Accounting Server can authenticate a user based on the NT user files.

Enhanced NT proxy support

Security and Accounting Server supports access to multiple NT domains preconfigured by the administrator for each user, or parsed from the user's login.

Roaming dialback in NETServer

Security and Accounting Server allows you to configure login service users for roaming dial-back, which prompts the user for a phone number and then calls the user back.

Dialback security

Security and Accounting Server can confirm a call was made from a specified phone number.

User Templates

When adding new users, you can use any existing user record as a template. Changes to the template affect all users based on that template.

Blacklisting

Blacklisting denies access to a user after a specified number of consecutive unsuccessful login attempts.

Call restriction

Security and Accounting Server can block calls to specified phone numbers.

Accounting Functions

Security and Accounting Server allows you to capture and log statistics about usage, data transfer, performance, and operation mode. The information is logged in Microsoft Access database tables. Security and Accounting Server generates accounting logs as follows:

- 1** A client sends accounting information to the Server.
- 2** Security and Accounting Server receives information from the client and logs the information to two distinct Microsoft Access database tables:

- Call-end messages are written to the CALLS table.
- RADIUS event messages and all other non-call-end messages are written to the EVENTS table.

Each message sent to Security and Accounting Server contains of a set of attributes. Only those attributes for which there is a corresponding column in the CALLS or EVENTS table are logged. If an attribute is sent that does not have a defined column, it is silently discarded.

By default, the CALLS and EVENTS tables contain a column for selected attributes. You can edit these tables to include the columns you need.

Accounting Features **Flexible Accounting**

You can configure your database to log only the information you need.

Reports and charts

You can generate the existing reports and charts, customize the existing reports and charts, or create your own reports and charts.

Database table maintenance

You can import and export database information.

Radius extensions

Security and Accounting Server supports over 200 3Com extensions to the standard RADIUS attributes.

Accounting secret

Security and Accounting Server gives you the option to encrypt accounting messages as specified in the latest RADIUS standard when proxying to a TACACS+ server.

New Features in this Release

VPN Support

Security and Accounting Server now can perform Virtual Private Networking (VPN) with the 3Com HiPer ARC. The Server supports Layer 2 Tunneling Protocol (L2TP) and Point-to-Point Tunneling Protocol (PPTP) authentication and accounting attributes.

MS-CHAP, MPPE Support

Security and Accounting Server now supports Microsoft's Challenge Handshake Authentication Protocol (MS-CHAP) and Microsoft Point-to-Point Encryption (MPPE) session key exchange.

EAP Support

Security and Accounting Server now implements attributes for Extensible Authentication Protocol (EAP) when used with the 3Com HiPer ARC. EAP provides extended messaging and token proxy authentication beyond the standard RADIUS protocol.

Additional Network Access Server Support

Security and Accounting Server now supports the NETBuilder II.

Support for Multi-Link with Third-Party Tokens

Security and Accounting now allows multi-link connections when using token-based authentication.

Ability to Proxy RADIUS Accounting Records

Security and Accounting Server now gives you the option to proxy accounting records to other RADIUS servers.

2

INSTALLATION

This chapter is designed to help you install Security and Accounting Server for Windows. It contains the following two sections:

- System Requirements
- Installation

System Requirements

The following section lists the system and software requirements for Security and Accounting Server.

Resource	Requirement
Hardware Platform	IBM-compatible PC, 486 or better
Operating System	Windows 95, 98, or NT V4.0
Software, Drivers, and Files	MS Graph 5.0, Microsoft Access 95 (V7.0) or Microsoft Access 97 (V8.0), MS Access 32-bit ODBC driver (V3.0)
System Memory	at least 16 MB
Application Disk Space	8 MB for programs plus at least 20MB for log files
Network Connection	Ethernet

NMC Dependencies

If you plan to use the NMC as a client, Total Control Manager version 3.0 or greater must be installed on your management station.

Microsoft Access Dependencies

Before you install Security and Accounting Server, you must install Microsoft Access 7.0 or Microsoft Access 97. In addition, Security and Accounting Server requires 32-bit ODBC drivers to interact with your Access database. To verify you have the correct driver, follow these steps:

- 1 In Windows Control Panel, double-click the **32bit ODBC** icon. If you do not have a 32bit ODBC icon, skip to step 4.
- 2 Click the **ODBC Drivers** tab.

- 3 Find the Microsoft Access Driver and check that the version number is 3.0 or greater.
- 4 If you do not have a 32bit ODBC icon, click the **ODBC** icon instead.
- 5 Click **Drivers...**
- 6 Select the Microsoft Access Driver from the list shown.
- 7 Click **About...** The driver version number displays.

Installing correct ODBC drivers

To install a newer version of the ODBC driver you must install the Data Access section of Microsoft Access.

- 1 Run the Microsoft Access installation program.
- 2 Choose **Custom Setup** during the installation procedure and check **Data Access** from the list of components to install.

The correct ODBC driver will automatically be installed.

Microsoft Graph5 and Graph 8 Error

If you install the Access 97 upgrade to Access 95 you will encounter the following message:



Ignore this message.

The graphing functionality will work in Access; the message is presented by design by Microsoft. If you would like more information, search for article ID Q163701 and Q169071 on the Microsoft support online web page.

Installing Security and Accounting Server

Follow these steps to install Security and Accounting Server for Windows 95, 98, or Windows NT.



*If you are installing for NT, you will be prompted to install Security and Accounting Server as a service. If you choose the automatic service option, you will not be able to use the Security and Accounting Console to monitor and manage the operations of the Server. See *Running S/A as a Service* for more information.*

- 1 Insert the product CD into your CD-ROM drive.
- 2 From the Windows desktop, click **Start -> Run...**
- 3 In the **Open** text box, type **x:\setup** where **x** is the drive letter of your CD-ROM.
- 4 Click **OK**. The Installation Program window appears.
- 5 Follow the setup program instructions to complete the installation.



CAUTION: *Security and Accounting Server will not run if you install NetWare support but do not have the NetWare client from Novell.*

- 6 Review the README file.



3

INITIAL CONFIGURATION

This chapter will show you how to configure Security and Accounting Server to communicate with your NAS and to perform user authentication and accounting. After you configure the Server, you will also learn how to add a new user.

Database Configuration

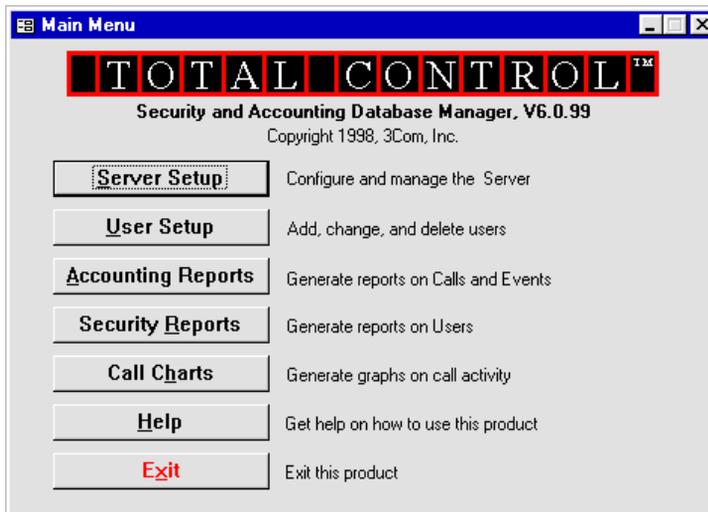
Security and Accounting Server stores authentication and accounting information in the Microsoft Access database. The Database Manager is used to manage the database tables.

Starting the Database Manager

To start Security and Accounting Database Manager, follow these steps:

- 1 Click **Start** -> **Programs** -> **USR Management Applications** -> **TC Security and Accounting Database Manager**.

Security and Accounting Database Manager appears.



Client Configuration

To properly configure the server, you must perform these steps:

- Configure the Security portion of the server.
- *Optional:* Configure the Accounting portion of the server. Skip this step if you do not plan to use Security and Accounting Server to capture accounting information or if you plan to proxy accounting information to another server.
- Set up a user.

Configuring the Security Server

To configure Security and Accounting Server to process security requests from your NAS, follow this procedure

- 1 Start Security and Accounting Database Manager.
- 2 Click **Server Setup**. The System Settings screen appears.
- 3 Click the **RADIUS Clients** tab.

System Settings
RESTART THE S/A SERVER TO ACTIVATE ANY CHANGES MADE HERE

Security | Accounting | **RADIUS Clients** | Passwords | Advanced Options

	IP	Port	Secret	Type
▶	127.0.0.1	1645	*****	3Com HiPer, NETS...
	127.0.0.1	1646	*****	3Com SA Server
*		1645		Generic RADIUS

Enter the IP address, UDP port, secret, and type of every machine and server that is allowed to communicate with this server. Failing to enter approved RADIUS clients will result in security breach notifications on every message from the unlisted clients
 To prevent encryption of accounting server messages, specify no secret for the accounting server.

Done

- 4 In the open field, enter the IP address, Port, Secret, and NAS Type for the client that will communicate with Security and Accounting Server.
 - **IP:** IP address of the NAS that controls the incoming calls (NMC, HiPer, etc.).
 - **Port:** UDP Port number - Use 1645 for security requests.

- **Secret:** A common password, four characters or longer, between the Security Server and the NAS. The secret must also be stored on the NAS.
 - **Type:** The type of this NAS
- 5 Click **Done**.

Configuring the Accounting Server

This procedure will configure Security and Accounting Server to process accounting information from your NAS.

- 1 From Security and Accounting Database Manager, click **Server Setup**. The SystemTabs screen appears.
- 2 Click the **RADIUS Clients** tab.
- 3 Enter the IP address, Port, Secret, and NAS Type for the client that will communicate with Security and Accounting Server.
 - **IP:** IP address of the NAS that controls the incoming calls (NMC, HiPer, etc.) This IP address is usually the same as the security client.
 - **Port:** UDP Port number - Use 1646 for accounting information.
 - **Secret:** A common password, four characters or longer, between the Accounting Server and the NAS. The secret must also be stored in the NAS.
 - **Type:** The type of the NAS
- 4 Click **Done**.

Example Configuration

If you are using a single chassis with one HiPer ARC, and are capturing Accounting messages, your client configuration would look like this:

IP	Port	Secret	Type
1.2.3.4	1645	*****	3Com HiPer, NETServer 8/16 V4.0, NETBuilder
1.2.3.4	1646	*****	3Com HiPer, NETServer 8/16 V4.0, NETBuilder



If you do not want to encrypt the accounting messages, simply leave the secret field blank on the second line. Remember, 1645 is the security port, 1646 is the accounting port.

Setting Up a New User

Once you have configured Security and Accounting Server to perform authentication, you are ready to begin entering users. When a user dials in to your NAS, the NAS will try to authenticate the user using its local table first. If it cannot find that user, it will pass the access request to Security and Accounting.

To set up a new user, follow these steps:

- 1 Start Security and Accounting Database Manager.
- 2 Click **User Setup**. The User Setup screen appears.

The screenshot shows the 'User Configuration' dialog box with the following fields and options:

- Username:** BLACK-LISTED
- General Tab:**
 - Template: [Dropdown]
 - Authentication: 3COM [Dropdown]
 - Password: [Masked Field]
 - Expr: 1/1/00 [Text] [Reset]
 - Failed Logins: 100 [Text] [Reset]
 - Allow Password Changes:
 - Deny Access:
 - Dial In Restrictions:
 - Check Port Number?: Port Number Name List: [Dropdown]
 - Check DNIS?: DNIS Restriction List: [Text]
 - Check ANI?: ANI Restriction List: [Text]
 - Maximum number of concurrent Sessions: 0 [Text]
 - Tunnel Name: [Dropdown] Tunnel Setup Request:
 - Hosts via DNS: [Text] Interim Accounting Interval: [Text]

- 3 Click **New** to enter a new user record.
- 4 In the **Username** field, enter a login name for this user.
- 5 On the **General** tab, choose **3Com** from the **Authentication** list box.



If you plan to proxy authentication requests to another server, choose the appropriate option from the Authentication list box. Refer to the Help system for information about proxying to other servers.

- 6 In the **Password** field, enter a password for this user.
- 7 In the appropriate NAS tab (NMC, NETServer 3.x, HiPer and NETServer 8/16 V4, NETBuilder), fill out any special information unique to this user.

For detailed information about these settings, refer to manuals that shipped with the NAS.

- 8 When finished configuring this user with your NAS, click **Done**.



When you install Security and Accounting, there are a set of sample user records preconfigured in the system (i.e. Framed-PPP, Menu-Default, etc.). These records are intended to demonstrate configurations for different service types. To eliminate a potential security breach, you should delete these samples.



4

TESTING THE INSTALLATION AND TROUBLESHOOTING

This chapter introduces the Security and Accounting Server Console and the client.exe testing program. You will also find troubleshooting information for Security and Accounting Server, and issues specific to Windows NT installations.

Testing the installation

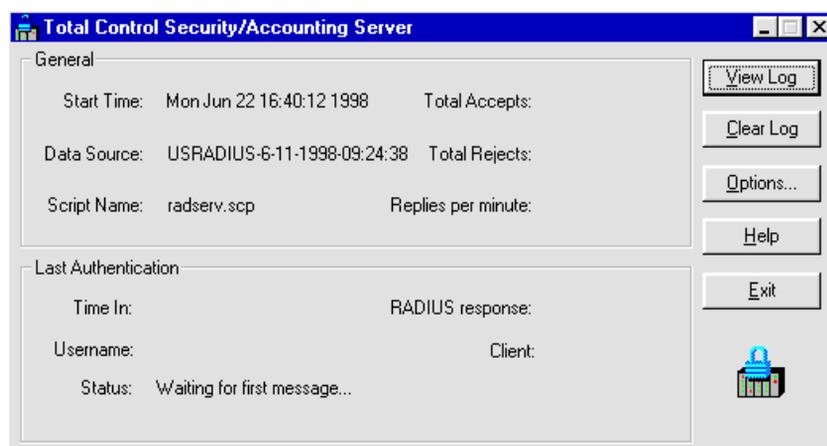
Now that you have configured the basics of Security and Accounting Server and added a user, you should test the installation and initial configuration.

Start Security and Accounting Server

The Security and Accounting Console lets you monitor and manage the operations of the Server. To start Security and Accounting Server follow these steps:

- 1 Click **Start -> Programs -> USR Management Applications -> TC Security and Accounting Server.**

The Security and Accounting Console appears.



- 2 Click **Options**. The Logging Options screen appears.
- 3 Check **Debug Mode**, **Verbose Mode**, and **Trace Packets**. Security and Accounting Server will provide detailed information about the security requests coming into the Server — useful if you need to troubleshoot your system.
- 4 Click **OK**.

Testing Your Configuration

We bundle a program you can use to test your Security and Accounting and become familiar with it before you connect it to your chassis. `Client.exe` is located in the `Ursuite` folder.

- 1 Open the `Ursuite` folder on your hard drive. Double-click `client.exe` to start the testing program. The Server Address window appears.

The screenshot shows a dialog box titled "Server Address" with the following fields and options:

- IP:** 127.0.0.1
- Secret:** testing123
- UDP Port, with common values:**
 - 1645 - Traditional Security
 - 1646 - Traditional Accounting
 - 1812 - IANA Security
 - 1813 - IANA Accounting
- Challenge:**
 - If checked, the client responds to RADIUS challenges with a fixed response.
 - Automatic challenge response
 - The automatic challenge response, i.e

Buttons for **OK** and **Cancel** are at the bottom.



You can use the default IP and Secret settings (127.0.0.1 and testing123) only if they still appear on the RADIUS Clients tab in the Database Manager.

- 2 Click **OK**. The Security Testing Client window appears.
- 3 From the File menu, select **Send Interactive...**
- 4 Enter the username and password of a user you entered into the Security and Accounting database.

- 5 Click **OK**
- 6 Check in the Security and Accounting Console that the user was authenticated:
 - The **Client** field should contain the IP address of the NAS through which the call was routed.
 - The **RADIUS Message** field should contain *Access-Accept*.
 - Click **View Log** and look for evidence of Access-Accept packets sent to the defined client in the log.

Troubleshooting

This section covers the major troubleshooting issues involved with the installation of Security and Accounting Server.

Upgrading to Windows 98

Security and Accounting Server supports Windows 98. However, if you install the Windows 98 upgrade to Windows 95, the *services* file is overwritten. Before you install the upgrade, understand that you will need to perform one of the following steps:

Edit the services file

- 1 Make a physical copy of the services file.
- 2 Install the Windows 98 upgrade.
- 3 Manually edit the new services file to include the radius, radacct, and tacacs records found in the old services file.

Re-install Security and Accounting Server

After installing the Windows 98 upgrade, re-install Security and Accounting Server. The installation will automatically place the correct entries in the services file.

Access Quits Unexpectedly

Some versions of Microsoft's VBA232.DLL file have bugs and can cause Microsoft Access to quit unexpectedly. If you encounter this problem, download a newer version of the file from Microsoft's web site. The corrected version should be 1,025KB and be dated on or after 3/8/96, 2:11 PM.

Screen Tab Errors

Some versions of Microsoft Access 7.0 do not accept the COMCTL32.OCX file installed by Security and Accounting Server. If you encounter errors when Access attempts to display tabbed screens:

- 1 Remove the COMCTL32.OCX file from the \windows\system directory.
- 2 Copy the COMCTL32.OCX file from the \usrsuite\security\97 directory to the \windows\system directory.
- 3 Initialize the new file in Access:
 - a From the **View** menu, select **Form Design**.
 - b From the **View** menu, select **Code**.
 - c From the **Run** menu, select **Compile All Modules**.
 - d From the **File** menu, select **Save All Modules**

Security and Accounting Server Does Not Start

If the server will not start and gives one of the following messages:

- Missing DLL file CLXWIN32.DLL
- The procedure or entry point SUnMapLS_IP_EBP_8 could not be located in the dynamic link library KERNEL32.DLL.

Follow these steps:

- 1 Find the file: \usrsuite\security\usrstub.dll.
- 2 Rename it to usr.dll.

Microsoft Graph5 and Graph 8 Error

If you install Access 97 over Access 95 you will encounter the following message:



Ignore this message.

The graphing capabilities of Access will function despite the error. For more information, search for article ID Q163701 and Q169071 on the Microsoft support online web page.

Winsock32.dll error

If you are running Security and Accounting Server as a service on Windows NT you will encounter an error when starting the Security and Accounting Console.

Since the Server is already running as a service, NT will not let you run the Server as an application. To avoid this error, stop the Security and Accounting Server service and start it as an application via the Start button. See other NT issues in Running S/A on Windows NT.

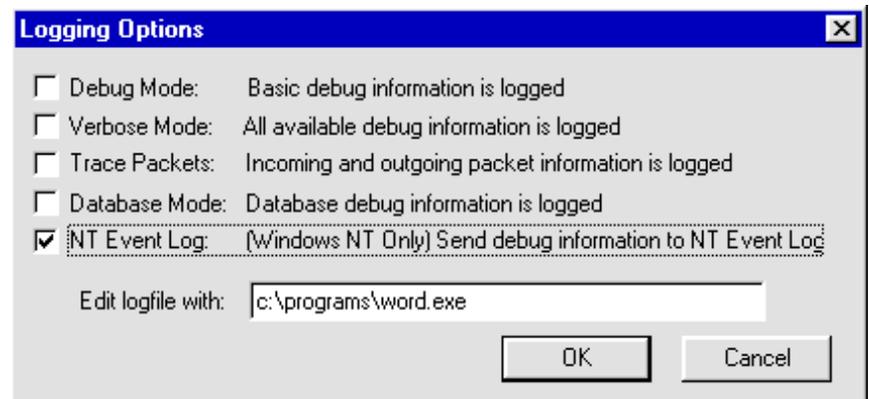
Running S/A on Windows NT

There are some differences with Security and Accounting Server when run on Windows NT. The following subsections cover these differences.

Event Logging

Security and Accounting Server allows you to log information to the NT Event Log. To turn on NT Event Logging:

- 1 Select **Options** in the Security and Accounting Console. The Logging Options window appears.



- 2 Select **NT Event Log**.



If you enable this service, the NT event log will fill up quickly with information. Periodically clean out this event file, or set the file to automatically purge itself on a regular basis.

- 3 Click **OK**.

Running S/A as a Service

If you decide to run Security and Accounting Server as a service of NT, you will not be able to view the Security and Accounting Console. As with many other programs, if you want to view the graphical interface, you must start the program as an application.



If you choose to run Security and Accounting as an NT service, the security.log file moves to the \winnt\system32\ directory.

INDEX

A

Accounting Features 1-5
Accounting Functions 1-4

B

Blacklisting 1-4

C

Call restriction 1-4
CALLS table 1-5
Configuring
 Accounting 3-3
 New User 3-4
 RADIUS Clients 3-2
 Security 3-2
conventions
 notice icons, About This Guide 6
 text, About This Guide 6

D

Dialback security 1-4

E

EAP 1-6
EAP Support 1-6
Enhanced NT proxy support 1-4
EVENTS table 1-5
Example Configuration 3-3

F

Features
 Accounting 1-5
 New 1-5

I

Installing Security and Accounting Server 2-3

L

L2TP 1-5
Local system password authentication 1-4

M

Microsoft Access Dependencies 2-1
Microsoft Graph5 and Graph 8 Error 2-2
MPPE Support 1-6
MS-CHAP Support 1-6
multi-link 1-6

N

NAS 1-1
Network Interaction 1-1
New Features in this Release 1-5
NMC Dependencies 2-1

P

Password management 1-3
PPTP 1-5
proxy 3-4
Proxy Authentication 1-3

R

RADIUS 1-1
Roaming dialback in NETServer 1-4

S

Secret 3-3
Security and Accounting Server
 Installing 2-3
 Starting 4-1
Security Features 1-3
Security Functions 1-2
Setting Up a New User 3-4
Starting Security and Accounting Server 4-1
Starting the Database Manager 3-1
System Requirements 2-1

T

- Testing Your Configuration 4-2
- Troubleshooting 4-3
 - Access quits unexpectedly 4-3
 - Microsoft Graph5 and Graph 8 Error 4-4
 - Screen Tab Errors 4-4
 - Security and Accounting Server Does Not Start 4-4
 - Winsock32.dll error 4-5

U

- UDP Port 3-2, 3-3
- User Templates 1-4

V

- VPN Support 1-5

W

- Windows 98 4-3



3Com Corporation
5400 Bayfront Plaza
P.O. Box 58145
Santa Clara, CA
95052-8145

©1999
3Com Corporation
All rights reserved
Printed in the U.S.A.

Part No. 1.024.1076-03