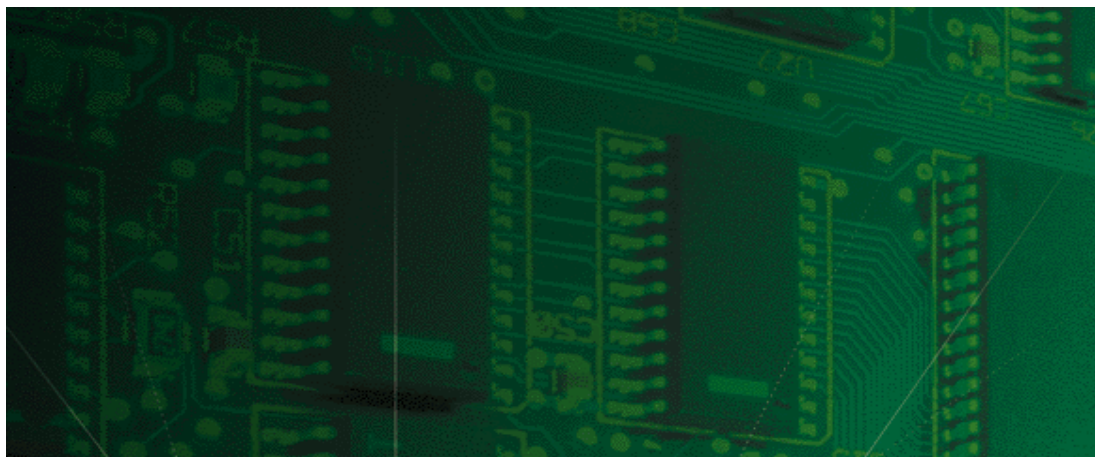




Security and Accounting Server for UNIX

Product Reference



Part No. 1.024.1677-02
Version Number 6.0



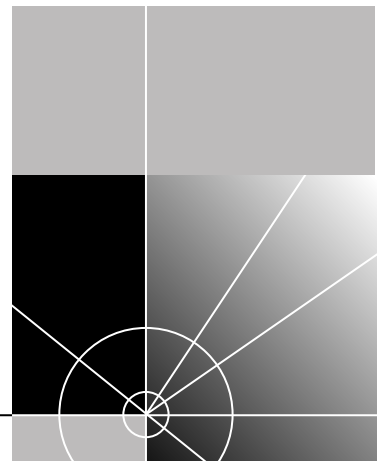
Security and Accounting Server for UNIX

Product Reference

Version 6.0

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

Part No. 1.024.1677-02



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	7
Conventions.....	8
Related Documentation	9

1 SYSTEM OVERVIEW

General Overview	1-1
System Requirements	1-2
Requirements for HP-UX®:	1-2
Requirements for Sun Solaris™:	1-2
New Features in this Release.....	1-3
VPN Support	1-3
EAP Support	1-3
Support for the iPass Corporate Access Service	1-3
Additional Network Access Server Support	1-3
Support for Multi-Link with Third-Party Tokens	1-3
Ability to Proxy RADIUS Accounting Records	1-3
Security and Accounting Components.....	1-3
Database Organization and Components	1-5
Starting the Server.....	1-5
Script Options and Functions.....	1-6

2 CONFIGURING USERS

Configuring Users	2-1
Adding New Users	2-1

Deleting Users	2-2
The Default User	2-2
Authentication Process	2-2
Assigning the Default User.....	2-3
Templates	2-4
Creating a Template.....	2-4
Basing a User On a Template.....	2-4
Passwords.....	2-6
Assigning a Password	2-6
Allowing Users to Change Passwords.....	2-6
Setting a Password Expiration Date	2-6
Dial-in Restrictions	2-7
Turning Dial-In Restrictions On	2-7
Entering the Numbers To Be Validated	2-7
Port Number Checking	2-7
DNIS Checking	2-7
ANI Checking	2-8
Dial Restriction Strings	2-8
Dial Restriction String Example.....	2-8
Concurrent Logins	2-10
Configuring the Server.....	2-10
Configuring the Users.....	2-10
Troubleshooting.....	2-10

3 CONFIGURING SECURITY AND ACCOUNTING SERVER

Configuring Accounting.....	3-1
Logging Call Statistics.....	3-1
Modem Configuration.....	3-1
NMC Configuration.....	3-2
NMC Log Groups.....	3-2
Customizing Call Logging	3-3
Forwarding Accounting Messages.....	3-4
Setting Event Logging.....	3-5
Advanced UNIX Accounting Features	3-6
Database Information	3-7
Flat File Database.....	3-7
Issues with the Flat File Database	3-7

Importing and Exporting Data	3-8
Postgresql or Oracle Databases.....	3-8
Customizing Your Database	3-8
Restricting Database Fields to Eight Characters:.....	3-8
Password Settings	3-9
Proxying	3-10
Before You Begin	3-10
TACACS+.....	3-10
Configuring communication between the Servers	3-10
Proxying User Authentication to TACACS+.....	3-11
Proxying Accounting Information to TACACS+.....	3-11
Configuring the NAS to Perform PAP.....	3-12
RADIUS	3-13
Configuring Communication Between the Servers	3-13
ACE	3-14
Copying the sdconf.rec file.....	3-14
Proxying User Authentication to ACE/Server	3-15
Troubleshooting	3-15
Configuring the NAS to Perform PAP.....	3-15
Omniguard/ Defender™	3-16
SafeWord.....	3-17
Setting the path to sid.cfg.....	3-17
Proxying User Authentication to SafeWord.....	3-17
Troubleshooting	3-18
EAP RADIUS Server.....	3-19
Configuring Communication Between the Servers	3-19
Proxying User Authentication to an EAP Server.....	3-19
S/KEY Integration	3-20
Proxying User Authentication to S/KEY	3-20
iPass Corporate Access	3-21
Restrictions and Limitations.....	3-21
iPass Authentication Process.....	3-21
Installation of iPass at the ISP Site.....	3-22
Installation of iPass at the Corporate Site	3-22
Remote Login Requirements.....	3-22

4 CONFIGURING VPN

Virtual Private Networks.....	4-1
VPN Overview.....	4-1
Tunnel Standards	4-1
Tunneling Using L2TP.....	4-2
Methods of Tunnel Initiation	4-3
Domain Based Authentication.....	4-4
Setting Up Security and Accounting Server #1	4-4
Setting Up Security and Accounting Server #2	4-5
DNIS/ANI Based Authentication.....	4-7
Setting Up Security and Accounting Server #1	4-7
Setting Up Security and Accounting Server #2	4-8
Username Based Authentication	4-9
Setting Up Security and Accounting Server #1	4-9
Setting Up Security and Accounting Server #2	4-10
Tunnel Attributes	4-10

A STANDARD RADIUS ATTRIBUTES

B VENDOR-SPECIFIC ATTRIBUTES

NMC-Specific Extensions (224-240)	B-1
3Com Vendor Specific Extensions (9000_90FF)	B-3
3Com Vendor Specific Extensions (other)	B-8
3Com Vendor Specific Extensions used in non-call termination events	B-10

C SCRIPT LANGUAGE

Script Language Syntax and Rules	C-1
Script Language Syntax.....	C-1
General Syntax Rules	C-1
Script Variables and Lists	C-1
Predefined Variables Lists	C-2
DICTIONARY	C-2
SYSTEM.....	C-2
DICTIONARIES	C-2
SERVER.....	C-2

TABLES	C-3
REQUEST	C-3
Referencing Attributes.....	C-3
Referencing Records.....	C-3
Referencing File Parameters.....	C-4
Script Execution	C-4
Labeled Sections	C-4
Variable References and Assignment Statements	C-5
Control Statements	C-5
Built-in Functions	C-8
ACE/Server Functions	C-11

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 Product Reference offers detailed procedures and information about Security and Accounting Server. The Appendices offer additional technical information useful for customization.

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 UNIX operating systems.



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
**Finding
Specific
Information in
This Guide**

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

If you are looking for	Turn to
An overview of Security and Accounting Server	Chapter 1
How to configure Security and Accounting with your database	Chapter 3
How to configure the Server	Chapter 3
How to configure users, templates, or the default user	Chapter 2
A list of standard RADIUS attributes	Appendix A
A list of vendor-specific attributes	Appendix B
Information about customizing the radserv.scpl	Appendix C

Conventions

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

Table 1 Notice Iconsconventions:notice icons, About This Guide




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

Table 2 Text Conventionsconventions:text, About This Guide

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	<p>This typeface represents information as it appears on the screen.</p>
The words “enter” and “type”	<p>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.”</p>

(continued)



Table 2 Text Conventionsconventions:text, About This Guide (continued)

Convention	Description
[Key] names	Key names appear in text in one of two ways: <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]. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press [Ctrl]+[Alt]+[Del].
Menu commands and buttons	Menu commands or button names appear in italics. Example: From the <i>Help</i> menu, select <i>Contents</i> .
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text.
Words in bold-face type	Bold text denotes key features.

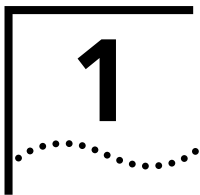
Related Documentation

- The following documents make up rest of the Security and AccountingAccounting Server documentation set. Contact your sales representative for ordering information.
- Total Control™ Security and AccountingAccounting Server for UNIX Getting Started Guide
This guide includes all the information you need to install and start Security and AccountingAccounting Server. It also offers tips on Troubleshootingtroubleshooting the installation.
 - Total Control™ Security and AccountingAccounting Server for Windows 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 a list of new features included in the release.
 - Total Control™ Security and AccountingAccounting Server for Windows online Help system
This Help system describes how to use Security and AccountingAccounting Server. It also contains context sensitive help for all the system parameters.

For information about Customer Service, including technical support, training, service contacts, and ordering printed manuals, call



1-800-231-8770 or visit our website at **<http://totalservice.usr.com>** For sales information call **1-800-877-2677**.



SYSTEM OVERVIEW

This chapter introduces 3Com's Security and Accounting Server. It provides a general overview of the software, including system requirements and new features, and a detailed look at the components that make up Security and Accounting Server.

General Overview

Demand for remote access continues to grow—mobile workers, telecommuters, and home internet users want simple and quick dial-up access. This added demand offers more opportunities for access to your network by unwanted users. Of all the security solutions available in the marketplace, one protocol has risen above the rest: RADIUS (Remote Access Dial-In User Service). RADIUS was developed specifically to provide network security and accounting for a large number of remote users. RADIUS provides comprehensive control over the three stages of network access security - authentication, authorization, and accounting.

Authentication The RADIUS protocol provides a flexible authentication mechanism through which the identity of a user is verified before being granted access to the network. This authentication mechanism also simplifies the administrative burden on the network administrator by allowing all remote access user information to be maintained in a common, centralized database.

Authorization Network administrators can customize RADIUS to restrict access at the modem point of entry, or on access to LAN-based devices. RADIUS provides a means to grant individual users access to specific network privileges or resources.

Accounting The RADIUS protocol also provides accounting information on network inbound and outbound connections, which is fundamental to maintaining tight network security. With this information, the network administrator can spot hacker attacks, identify specific user connection problems or charge users according to their network usage.

Security and Accounting Server is a RADIUS-based program. It builds upon the RADIUS standard to provide additional authentication and authorization control for your Network Access Server (NAS). A NAS is often referred to as a RADIUS client; in this document we will use the terms NAS and client interchangeably.

System Requirements

Requirements for HP-UX®

Resource	Requirement
Hardware Platform:	HP 9000/7xx or higher with CD-ROM drive
Operating System:	HP-UX V10.20 or higher
Prerequisite Software:	X-Windows - X11R5Perl (optional)
System Memory:	at least 32 MB
Application Disk Space:	30 MB for program files plus appropriate space for log files
Network Connection:	Ethernet
Optional Software:	Oracle Database v7.3, 8.0

Requirements for Sun Solaris™

Resource	Requirement
Hardware Platform:	Sun™ SPARCstation™ 5/85 or larger with CD-ROM drive
Operating System:	Sun Solaris V2.5 or above
Prerequisite Software:	X-Windows - X11R5
System Memory:	at least 32 MB
Application Disk Space:	30 MB for program files plus appropriate space for log files
Network Connection:	Ethernet
Optional Software	Oracle Database v7.3 - 8.0



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

New Features in this Release

VPN Support

Security and Accounting Server now supports Virtual Private Networking (VPN) using Layer 2 Tunneling Protocol (L2TP) and Point-to-Point Tunneling Protocol (PPTP) authentication and accounting attributes.

EAP Support

Security and Accounting Server now implements attributes for Extensible Authentication Protocol (EAP). EAP provides extended messaging and token proxy authentication beyond the standard RADIUS protocol.

Support for the iPass Corporate Access Service

iPass allows remote users the ability to roam and dial into any ISP Point of Presence that subscribes to the iPass network. Security and Accounting Server now supports the iPass software needed to safely provide authentication and accounting within the network.

Additional Network Access Server Support

Security and Accounting Server now supports the NETBuilder II for authentication, accounting, and authorization.

Support for Multi-Link with Third-Party Tokens

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

Ability to Proxy RADIUS Accounting Records

Security and Accounting Server can now proxy accounting records to other RADIUS servers and to TACACS+ servers.

Security and Accounting Components

This section contains information about `radserv.scp` and `dictionary.dat`, two basic components of Security and Accounting Server.

Dictionary.dat the dictionary file for all the attributes that the Server can process. It contains translations for parsing requests and generating responses. All transactions are composed of Attribute/Value Pairs.



Do not alter the dictionary.dat file.

Radserv.scp the script that is provided with the Security and Accounting Server. It is a text file containing a BASIC-like language that

can be customized. The script contains the business rules or policy for processing the various types of RADIUS messages that are received and sent by the server. As described in the overview, the script interacts with the server and the database to analyze and process security and accounting requests that are received from the NAS. There are entry points in the script for each of the various types of messages that are processed by the server.

A good starting point for learning about the script is to look at the description of the language located in Appendix C. This describes the various language elements. You can also look at and the `radserv.scp` which is distributed with the Security and Accounting Server software distribution. Key concepts to note in the script include:

- Entry points, such as "Access_Request:" Control is passed to this routine when an Access_Request message is received from the NAS.
- Processing routines, such as Validate-User, which perform various processing functions.
- Information contained in the request packet, such as Request.User_Name.
- References to information contained in the dictionary, such as Dictionary.Request_Type.Access_Challenge, which would have a value of 11, based on the record in `dictionary.dat`.

Database Organization and Components

Security and Accounting Server uses a set of tables to store and access the data used by the server. The following table summarizes the major database tables:

Table Name	Text file equivalent	Description
System	system.txt	Contains the server configuration record for the Server. The parameters in this table are read when the server is started or re-initialized and affect the global operations of the Server
Users	users.txt	Contains records for each user. A user's record contains all of the information about that user.
Clients	clients.txt	Contains records for each of the clients that communicate with Security and Accounting Server. Each record contains the client's IP, port number, address, and secret.
Domains	domains.txt	Contains the mapping relationship (domain name to IP address) used when proxying information to other authentication and accounting servers.
Portgroups	portgroups.txt	Contains the portgroup names and IP addresses used to base authentication on ports and/or ANI/DNIS numbers
Tunnels	tunnels.txt	Contains the attributes associated with each VPN tunnel.
Eaproxies	eaproxies.txt	Contains information specific to EAP proxy servers.

Starting the Server

You can start or stop Security and Accounting Server using the server wrapper script called *saserver*.

To start the server enter:

```
$SAHOME/bin/saserver start
```

To stop the server enter:

```
$SAHOME/bin/saserver stop
```

You can also stop the server by sending a SIGTERM signal to the process. The server writes out its PID to the `$SAHOME/data/sa/saserv.pid` file. To stop the server without the script, enter:

```
kill `cat $SAHOME/data/sa/saserv.pid`
```

Security and Accounting Server is a daemon that disassociates from the controlling terminal. It is useful during initial configuration and setup to

run the server in the foreground. This allows you to kill the server with the interrupt key. To run in the foreground, execute:

```
$SAHOME/bin/saserver start -f
```

Script Options and Functions

When you start Security and Accounting Server, you can set options to customize how the Server runs. For example to turn on the Debug & Verbose Modes, enter:

```
$SAHOME/bin/saserver start -v -d
```

A full list of options and their functions follows:

Option	Parameter	Function
-t		Starts Security and Accounting Server in trace packets mode, which logs incoming and outgoing packet information
-v		Starts Security and Accounting Server in verbose mode, which logs all available debugging information
-d		Starts Security and Accounting Server in debug mode, which logs basic debugging information
-s		Activates script debug, which logs script debugging information
-i		Activates input file debug
-f		Runs the Server in the foreground shell. The server does not become a daemon as usual
-l	[file syslog stderr]	Sets the logging type and defaults to file logging
-c		Turns on LOG_CONS, which logs messages to the console if syslogd is not enabled. This option is used only if syslog logging is activated.
-r		Resets the log file (flushes it).
-h		Displays command line help and the server version number.

2

CONFIGURING USERS

Configuring Users

This section will guide you through the steps of adding, modifying, and deleting users.

Before creating a list of users, consider these steps:

- Assemble a list of usernames, passwords, and, if necessary, dial-back phone numbers.
- Gather all relevant client information that you have set up for your clients.
- Create a strategy for assigning passwords.
- Before you decide to use usernames and passwords longer than eight characters, make sure your client will support them.

Adding New Users

To add a new username to the database, follow these steps:


- 1 From Security and Accounting Database Manager, select **User Setup**. The User Configuration screen appears.
- 2 Click **New**. The Add New User window appears.
- 3 Enter a username in the box and click **Add**.



CAUTION: Do not create a user profile and name it "DEFAULT." Security and Accounting Server will register it as the preconfigured template profile, and automatically reject the authentication.

- 4 When you are finished adding new users, click **Cancel**.

Deleting Users To delete a username from the database, follow these steps:

- 1 From Security and Accounting Database Manager, select **User Setup**. The User Configuration screen appears.
- 2 Click **Find**. The Find User window appears.
- 3 Enter the username in the box shown. As you type, Security and Accounting Server searches for matches. When it finds a match, it highlights the username in the Username box on the User Configuration screen.
 *If you want to find user **john**, but the database lists user **johnson** first, enter John followed by a space in the Find User window.*
- 4 To delete this user, click **Delete**.
- 5 To exit the Find User window, click **Cancel**.

The Default User

The default user profile is a unique profile created to handle any users not found in the database. When Security and Accounting Server cannot find a username in the database, it will attempt to authenticate the user using this default user profile. All the characteristics of the set up for the default user will be passed on to this user.

For example, if you have 300 users in your UNIX system, you may not want to recreate all those user records in Security and Accounting Server. If you configure the default user to use the UNIX password file to authenticate users, you won't need to recreate all the users.



Security and Accounting Server supports only one default user.

Authentication Process

The following is an example of the authentication process using the default user configured to use the UNIX password file.

- 1 A user dials in and enters a username and password.
- 2 Security and Accounting Server searches for the user's information in the users table.
- 3 If it cannot find the user's information, it will check for a default user profile.

- 4 Security and Accounting Server finds that the default username is configured and set to authenticate using the UNIX password file.
- 5 Security and Accounting Server forwards the user's information to the UNIX server for authentication.

Assigning the Default User

To set up Security and Accounting Server to use the default user profile, follow these directions.

- 1 Add a new user and assign a username other than "default."

For example, if you wish to set up Security and Accounting Server to proxy requests to a TACACS+ server, you could name this profile *proxy* or *tacacs*.



CAUTION: Do not create a user profile and name it "DEFAULT." Security and Accounting Server will register it as the preconfigured template profile, and automatically reject the authentication.

- 2 From the main screen of Security and Accounting Manager, select **Server Setup**. The SystemTabs screen appears.
- 3 Click the **Security** Tab.
- 4 In the **Default Username** box, enter the username you assigned to the default user profile (ie. tacacs).
- 5 Configure the default user as you would any other user.



*Be sure to check **Deny Access** to prevent someone from logging in directly as this user.*

- 6 Click **Done**.

Templates

To ease the task of adding users, Security and Accounting Server allows you to create user templates. Templates speed the addition of new users by eliminating repetitive data entry.

When you create a template, you can configure it to contain all the basic information of your users. When you base a user on that template, that user profile borrows all the configurations from the template. In addition, when you change the template, all users based on that template reflect the new change.



CAUTION: Do not delete the DEFAULT user profile from the Security and Accounting Server database.

Creating a Template

New templates are created the same way new user records are created. To make a new template, follow the steps to create a new user and configure it appropriately. You can create and use multiple templates, depending on your needs.

Any user record can serve as a template for another user record, though we suggest creating a template that does not also serve as a specific user's login profile.

Basing a User On a Template

To base a new or existing user on a template, follow these steps:

- 1 From Security and Accounting Database Manager, select **User Setup**.
- 2 Create a new user record, or highlight a user record you want to change.
- 3 In the **Template** box on the **General** tab, enter the name of the template profile you want to use.

- 4 Make any special changes to this user's configuration. Each field you leave blank will automatically use the the template's configuration.



When you base a user on a template, the template settings do not appear in that user record. The information displayed in the user record will remain blank, or as the default value.

For example, a template might set the password expiration date to 01/01/99. If the password expiration date field for a user record based on that template is left blank, that user's password will expire on 01/01/99. If the password expiration date in a user record is set to 10/14/99, the default template value is overridden and the expiration date becomes 10/14/99 for that user only.

- 5 When you are finished, click **Done**.

Passwords

Each user can have specific settings assigned to control their passwords. You can configure:

- what the user's password is
- if the user can change the password
- when the password expires

Assigning a Password

To assign a user a new password or to change a current password, follow these steps:



CAUTION: *If you leave the password field blank, the user will be authenticated without entering a password.*

- 1 From the Security and Accounting Database Manager, select **User Setup**.
- 2 Select the user record you want to change.
- 3 On the **General** tab, enter a password string in the **Password** field.

Allowing Users to Change Passwords

To configure a user to be able to change their password at any time, follow these steps:

- 1 From the Security and Accounting Database Manager, select **User Setup**.
- 2 Select the user record you want to change.
- 3 On the **General** tab, check the **Allow Password Changes** box.

Setting a Password Expiration Date

To assign an expiration date to a user's password, follow these steps.

- 1 From the Security and Accounting Database Manager, select **User Setup**.
- 2 Select the user record you want to change.
- 3 On the **General** tab, enter the expiration date of the password in the **Expiration** field.

Enter the expiration date in the format:

Month, Day, Year = MM/DD/YYYY:

June 30, 1998 = 06/30/1998

December 1, 2002 = 12/01/2002



If the field is left blank, the default password age from the global settings is used.

Dial-in Restrictions

Security and Accounting can validate users by checking these three numbers:

- the incoming number using Automatic Number Identification (ANI)
- the dialback or outgoing phone number using Dialed Number Identification Service (DNIS)
- the port numbers the user dialed in to or out from.

To configure Security and Accounting to check one or more of these, complete these tasks:

Turning Dial-In Restrictions On

Follow these steps to turn dial-in restrictions on.

- 1 Start Security and Accounting Database Manager.
- 2 Click **Server Setup**.
- 3 Click the **Security** Tab.
- 4 Check the **Check Dial In Restrictions?** box.
- 5 Click **Done**.

Entering the Numbers To Be Validated

Each user may be assigned specific port numbers, ANI numbers, or DNIS numbers. To configure these numbers, follow these steps:

Port Number Checking

- 1 On the **General** Tab of the User Configuration screen, select the **Check Port Number?** box.
- 2 In the **Port Number Name List** field, enter a port group number. This defines a set of modems you defined as a port group.

DNIS Checking

DNIS is a feature of 800/900 lines that provides you with the number the caller dialed to reach your system. Essentially, DNIS tells you the number the person called.

Security and Accounting Server will compare the number that the remote user dialed with the DNIS Restriction List.

- 1 On the **General** Tab of the User Configuration screen, select the **Check DNIS?** box.
- 2 In the **DNIS Restriction** field, enter the restriction strings to define allowable phone numbers to which remote users can dial. For more info on Dial Restriction Strings, see the following section.

ANI Checking

ANI - Automatic Number Identification: a feature that forwards a calling party's telephone number. Essentially, ANI tells you the number of the phone that is dialing your system..

- 1 On the **General** Tab of the User Configuration screen, select the **Check ANI?** box.
- 2 In the **ANI Restriction List** field, enter a dial restriction string to define the allowable phone number from which remote users can dial. For more info on Dial Restriction Strings, see the following section.

Dial Restriction Strings

Dial restriction strings define allowed and restricted phone numbers for users.

A dial restriction string contains up to 20 entries, separated by colons. Each entry allows or disallows a phone number or group of phone numbers. Each entry must begin with either a plus sign (+) for an allowed number or a minus sign (-) for a disallowed number.

You can use wildcards in the entries. The single-character wildcard (to replace one character) is a question mark (?); the global-character wildcard (to replace any number of characters) is a dollar sign (\$). You should end your dial restriction string with either +\$ or -\$, to indicate how to handle numbers not specified in the list.



You should also add the \$ wildcard after numbers you want to specifically disallow. If you do not, a user could bypass the restriction by dialing extra numbers to break the exact match.

Dial Restriction String Example

+1617\$:+1312\$:-1\$:-5551234\$:+\$

The following table explains the entries in this dial restriction string.

String	Function
+1617\$	Allows all calls within the 617 area code
+1312\$	Allows all calls within the 312 area code
-1\$	Excludes any other long distance calls (outside of 617 and 312)
-5551234\$	Excludes the local number 5551234. The dollar sign at the end ensures that the user does not break the match by adding extra digits.
+\$	Allows all other local calls

Concurrent Logins

Security and Accounting Server allows you to configure the number of login sessions a user can have at one time. As a default, Security and Accounting does not limit the login sessions.

Configuring the Server

For concurrent logins to work, Security and Accounting Server must be set to process both security and accounting messages. Before proceeding, make sure that the Server is receiving and processing both types of messages.

To configure Security and Accounting to process concurrent logins, follow these steps:

- 1 From the Security and Accounting Database Manager, click **Server Setup**.
- 2 Click the **Accounting** Tab
- 3 Check the **Enable Login Tracking** box.

Configuring the Users

To limit how many concurrent sessions a user can have, follow these steps:

- 1 From the Security and Accounting Database Manager, click **User Setup**.
- 2 Click the **General** tab.
- 3 In the field labeled **Maximum Number of concurrent sessions**, enter the number of concurrent sessions for this user. For example:
 - 0 = no limit
 - 1 = 1 authentication at a time
 - 2 = 2 authentications at a time.

Troubleshooting

Follow these steps if concurrent logins will not work:

- 1 Make sure that Enable Login Tracking feature turned on.
- 2 Check that Security and Accounting Server is configured to process security requests.
 - Is the RADIUS Security Service Name configured on Security Tab?
 - Is there a separate entry for security (IP, port number, secret, type) defined on the RADIUS Clients Tab?

- 3 Check that Security and Accounting Server is configured to process accounting messages.
 - Is the RADIUS Accounting Service Name configured on Accounting Tab?
 - Is there a separate entry for accounting (IP, port number, secret, type) on the RADIUS Clients Tab?
- 4 Check that the client is configured to forward security and accounting messages to Security and Accounting Server.

3

CONFIGURING SECURITY AND ACCOUNTING SERVER

Configuring Accounting

Security and Accounting Server can log information sent to it from any NMC, NETServer, or HiPer ARC. Before you attempt to log accounting information from any of these NASs, make sure you have upgraded to the latest code for each card.

Logging Call Statistics

To log calls statistics from an NMC:

- each NMC client (modem) must be configured to generate and forward call termination conditions (traps).
- the NMC must be configured to communicate with Security and Accounting Server.

Modem Configuration

- 1 In Total Control Manager, select the modems you want to configure.
- 2 From the **Fault** Menu, select **Trap Settings**. The Modem Faults window appears.
- 3 In the **Parameter Group** list box, choose **Trap Enables**.
- 4 For each modem, choose **enableLog** for the following traps to capture statistics about incoming calls:

- On Incoming Call
- On Incoming Termination

If you want to gather statistics on outgoing calls, set **enableLog** for:

- On Outgoing Call
- On Outgoing Termination

Chassis NACs regularly send unsolicited messages to the NMC to notify it of regular events:

- If traps are enabled (enableTrap) for these events, the NMC sends a trap message to the management station (Example: Total Control Manager).
- If logging is enabled (enableLog), the NMC sends a log message to an authentication server (Example: Security and Accounting Server).
- If traps and logging are enabled (enableAll), both messages are set.
- If all are disabled (disableAll), the NMC discards the event notification and sends no message.

NMC Configuration

- 1 In Total Control Manager, select the NMC card.
- 2 From the **Configure** menu, select **Programmed Settings**. The NMC Programmed Settings window appears.
- 3 In the **Parameter Group** list box, choose **Logging Group**.
- 4 In the **Primary Log Server IP Address** field, enter the IP address of the workstation running Security and Accounting Server.
- 5 In the **Log Group Selection**, choose which NMC log groups to send to Security and Accounting Server. See the NMC Logging Group section below for information about the various logging groups.

NMC Log Groups The 3Com Network Management Card (NMC) can capture and send accounting attributes specific to 3Com equipment. These attributes are grouped into four categories, based on the information provided:

- **Group 1** — Usage Statistics (always sent)
- **Group 2** — Data Transfer Statistics
- **Group 3** — Performance Statistics
- **Group 4** — Operating Mode Statistics
- **Group 5** — RIMMIE information

See Appendix B for a full listing of attributes in each group.

The NMC automatically sends all attributes from Group 1 to Security and Accounting Server. You can configure which, if any, of the other groups

should also be sent. Use the table below to decide which logging group selection to make:

Selection	Log Groups Included
None	Group 1
2	Groups 1, 2
3	Groups 1, 3
4	Groups 1, 4
5	Groups 1, 5
23	Groups 1, 2, 3
24	Groups 1, 2, 4
25	Groups 1, 2, 5
34	Groups 1, 3, 4
35	Groups 1, 3, 5
45	Groups 1, 4, 5
234	Groups 1, 2, 3, 4
235	Groups 1, 2, 3, 5
245	Groups 1, 2, 4, 5
345	Groups 1, 3, 4, 5
2345	Groups 1, 2, 3, 4, 5

Customizing Call Logging

Security and Accounting Server can be customized to log additional call attributes, beyond the ones already listed in the Calls and Events tables. The Dictionary.dat file contains a list of all of the RADIUS and vendor-specific attributes which can be logged by Security and Accounting Server.

To log additional information, find the attribute that contains the information you want. Next, add a field to the Calls or Events table with the name of the attribute.



The database utilities that are provided with Security and Accounting only import or export the standard set of attributes. If you customize your database, you risk losing the information from those extra attributes when you import the data to a new database.

Forwarding Accounting Messages

Security and Accounting Server has the ability to forward accounting messages based upon the security messages it receives.

- 1 You can forward accounting messages to a generic RADIUS server, an additional Security and Accounting Server, or another dedicated accounting solution.

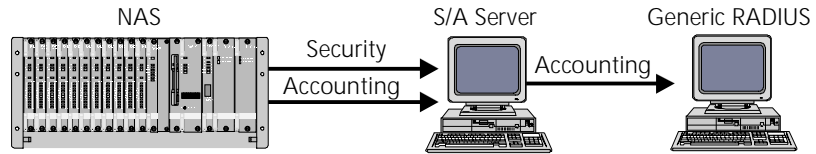


Figure 3-1 Forwarding accounting messages to another server.

To forward accounting messages:

- On the **Accounting** tab, enter the other RADIUS server's IP address in the **Accounting Server IP Address** field. To control which accounting messages will be forwarded, see Setting Event Logging.
- 2 You can also configure Security and Accounting Server to generate accounting information from security requests it receives. Security and Accounting can be set to forward these accounting messages back to itself.

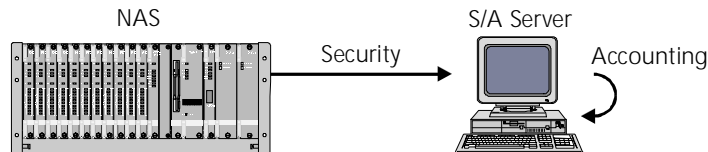


Figure 3-2 Working with a NAS that does not generate accounting messages.

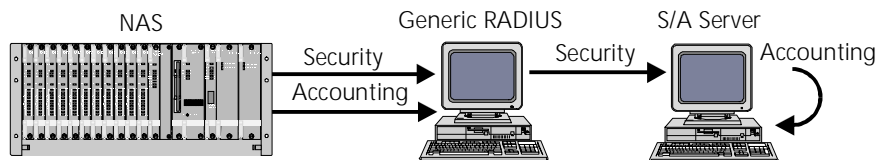


Figure 3-3 Working with a proxy agent that does not forward accounting messages.

To create accounting messages and forward them to the same Security and Accounting Server:

- On the **Accounting** tab, enter the IP address of Security and Accounting Server in the **Accounting Server IP Address** field.

Setting Event Logging

When you set Security and Accounting Server to generate accounting messages, you have the option to choose which events you want to log.

Only the event options you select will be forwarded to accounting

The screenshot shows a window titled "SystemTabs" with a red banner at the top that reads "RESTART THE SERVER TO ACTIVATE ANY CHANGES MADE HERE". Below the banner are several tabs: "Security", "Accounting" (which is selected), "RADIUS Clients", "Passwords", and "Advanced Options".

Under the "Accounting" tab, there are two main input fields:

- RADIUS Accounting Service Name:** A text box containing "radaacct". To the right of this field is a note: "Typically 'radaacct', the name of the accounting service as found in the SERVICES file. Leave blank if RADIUS accounting is not being used."
- Accounting Server IP Address:** A text box containing "1". To the right of this field is a note: "The IP address of the accounting server. This is used by the security server to log messages to the accounting server. If blank, the security server will not send messages to the accounting server."

Below these fields is a section titled "Event Logging" with a list of checkboxes and their corresponding descriptions:

- ☐ **Failed Logins** (Description: If the Accounting Server IP Address has been set, then the events checked here will be sent to the Accounting Server IP Address, using the port number found in the SERVICES file under the RADIUS Accounting Service Name.)
- ☐ **Successful Logins**
- ☐ **User Blacklisted**
- ☐ **Password Changes**
- ☐ **Security Breaches**

To the right of the "Event Logging" section is a button labeled "Advanced" with "UNIX only" written in red text below it.

At the bottom of the window, there is a note: "To avoid encrypting accounting messages, do not give a secret for the accounting server." and a "Done" button.

Advanced UNIX Accounting Features

There are several advanced accounting features offered only for UNIX systems. To access these options, from the **Accounting** tab, click **Advanced**.

The image shows a dialog box titled "Advanced Accounting Options" with a red "UNIX Only" label at the top. The dialog contains several configuration fields for UNIX accounting features. Each field has a text input box and a description to its right. The fields are: "Server time type" (with a dropdown menu), "Disk low script" (with a text input box), "Disk low threshold" (with a numeric input box set to 10 and a "megabytes" label), "Disk full script" (with a text input box), "Disk full threshold" (with a numeric input box set to 10 and a "megabytes" label), "Nightly rollover script" (with a text input box), "Disk space check interval" (with a numeric input box set to 10 and a "minutes" label), "Use flat files for accounting" (with an unchecked checkbox), "Accounting data path" (with a text input box), and "Accounting log file interval" (with a numeric input box set to 10 and a "minutes" label). A "Done" button is located at the bottom right of the dialog.

Field	Description
Server time type:	Type GMT or LOCAL to set the server time.
Disk low script:	Script to execute when disk low threshold reached.
Disk low threshold: 10 megabytes	Threshold for executing disk low script.
Disk full script:	Script to execute when disk full threshold executed.
Disk full threshold: 10 megabytes	Threshold for executing disk full script.
Nightly rollover script:	Name of script to be executed at midnight.
Disk space check interval: 10 minutes	Time interval for checking disk space limits.
Use flat files for accounting: <input type="checkbox"/>	Check this box to log accounting data to text files.
Accounting data path:	Directory path for accounting data files.
Accounting log file interval: 10 minutes	Default value = 0 results in daily log files. Any other number represents the number of minutes for which each log file records data.

Done

Database Information

Flat File Database

These files can be edited with any UNIX file editor, such as *vi*. Make sure that only one person edits your database files at a time. UNIX file editors cannot lock a file during an editing session. The last editing session closed overwrites all others open at the same time, so data will be lost.

When editing the files with an editor, follow these rules:

- Put quotes around all string fields to the right of the equal sign, even if empty.
- A comma must end each record
- Make sure that you have the correct number of commas in the record. The number of commas for each record = Number of STRUCTURE fields - 1
- DO NOT delete the DEFAULT record, it is used by the security database editor.
- If any of these files are updated, the Server must restarted.
- Do not enter quotes in a field unless it is two quotes signifying an empty field (" ").

Issues with the Flat File Database

The flat file version of the server by default does not provide the following features:

- encrypting a user's password
- password changing
- updating password expiration
- real-time login tracking
- blacklisting
- encrypting the clients shared secret.

These features were disabled because of significant server performance degradation and concurrent file access problems brought on by the nature of a text based database.

Importing and Exporting Data

Postgresql or Oracle Databases

To import the default data into the database, run:

```
$SAHOME/bin/saUtil -I -v -d
```

This imports the default data files stored in \$SAHOME/lib/sa/db to the database. Look at the log file for errors.

The Import/Export Data options in the saUtil program are as follows:

Option	Description
Import All Security Tables	Imports the system.txt, users.txt, clients.txt, domains.txt, and portgrps.txt into the appropriate tables
Export All Security Tables	Does the reverse of the Import All Security Tables option and puts the files into \$SAMHOME/data/sa/export with a filename of the form: YYYYMMDD
Import Specific Table	Interactively prompts user to enter a file name and table name into which the database is inserted.
Export Specific Table	Interactively prompts the user to enter a file name and table name to export. YYYYMMDD is appended to the filename.
Export Accounting CALLS Table	Exports the CALLS table in the filename format: YYYYMMDD
Export Accounting EVENTS Table	Exports EVENTS table in the filename format: YYYYMMDD

These routines expect the imported data to be in the \$SAHOME/data/sa/import directory. The routines export data to the \$SAHOME/data/sa/export directory. To import data with these routines, you must move the proper files into the \$SAHOME/data/sa/import directory.

Customizing Your Database

Some clients may restrict a username or password to eight characters. The RADIUS protocol supports usernames and passwords up to 64 characters. A user authentication will be rejected if one of these clients encounters login information longer than eight characters.

Restricting Database Fields to Eight Characters

- 1 Go into design mode on the database.
- 2 Delete all relationships involving the USER_NAME field, using menu option Tools-Relationships.

- 3 Select the User Table, select View-Table Design, and change the length of the USER_NAME and PASSWORD fields to 8 characters long. Some usernames and passwords may be truncated by this action.

Password Settings

Security and Accounting Server allows you to configure the global characteristics of user passwords. Refer to the table below for further information on configuring password settings.

To change any of the following settings:

- 1 From Security and Accounting Database Manager, click **Server Setup**.
- 2 Click the **Passwords** tab.
- 3 When you have finished, click **Done**.

Field	Description	Default
Minimum Length	The minimum number of characters a user password must contain. Note: When this parameter is changed, only new passwords or user-initiated password changes are affected. The database is not scanned to determine if current passwords conform.	4
Default Age	The number of days a password is valid	45
Expiration Warning	The number of days of warning a user will receive, upon successful login, that their password will expire.	5
Allow Blacklisting	When checked, Security and Accounting Server will track successive login failures. When the Blacklist Threshold (below) is reached, the user account is blacklisted, and the user is denied access with or without the correct password.	off
Blacklist Threshold	The number of successive failed login attempts allowed before a user is blacklisted.	25
Prompt on Expiration	When checked, Security and Accounting will prompt the user to change their password when it expires.	off
Change Keyword	The keyword to substitute for a password change. When the user enters this keyword, Security and Accounting Server prompts the user to input a new password. Note: If this field is left blank, this feature is disabled.	NEWPASS

Proxying

Security and Accounting Server is able to pass authentication requests to a variety of other authentication solutions. This process is called proxying. This chapter explains how to set up Security and Accounting Server to proxy security requests.

Before You Begin

Before attempting to use another system of authentication, verify that the NAS and Security and Accounting Server are installed and configured properly. Refer to the Getting Started Guide for installation instructions.

Once local authentication works properly, configure a user to use the proxy of choice. Turn on debugging information on Security and Accounting Server, and, if available, in the proxy server. If the user does will not authenticate, check the Server log file for information to determine the cause of the problem.



You cannot perform CHAP when you proxy authentication to another server. For more information about PAP, CHAP, and how they effect proxying authentication, see [Configuring the NAS to Perform PAP](#).

TACACS+

To proxy user authentication requests and accounting information to a TACACS+ server, you must configure Security and Accounting Server to:

- communicate with the TACACS+ Server
- proxy user authentication to TACACS+
- proxy accounting information to TACACS+

Configuring communication between the Servers

- 1 From the Security and Accounting Database Manager, select **Server Setup**. The SystemTabs screen appears.
- 2 Click the **Advanced Options** tab
- 3 Click **Proxy Servers**. The Proxy Server Parameters window appears.
- 4 Click the **TACACS+** tab.
- 5 In the **TACACS+ Server IP address** box, enter the IP address assigned to your TACACS+ Server.
- 6 In the **TACACS Plus service name** box, enter the service name for processing TACACS+ messages. The default name is `tacacs+`. If you do not know the name of the TACACS+ Server, search the services file found at `/etc/services`.

- 7 In the **TACACS+ Server secret** box, enter the secret key that you defined on the TACACS+ server.

Proxying User Authentication to TACACS+

- 1 From the Security and Accounting Database Manager, select **User Setup**.
- 2 In the **Username** box, type the name of a user you would like to configure.
- 3 On the **General** tab, set the **Authentication** listbox to *TACACS PLUS*.

Edit the *radserv.scp* By default, a TACACS+ user's service type is set to Menu Prompt. The *radserv.scp* file must be edited to use the default user's configuration.

- 1 Locate the following entry in the *radserv.scp* file:

```
; For Tacacs+, once we authenticate, should we prompt for
; a valid config, or use the default user's config?
TacacsPrompt = 1
```

- 2 Edit the file as shown:

```
TacacsPrompt = 0
```

Proxying Accounting Information to TACACS+

Security and Accounting Server provides you with a program to convert 3Com accounting output files to a TACACS+ formatted file. The included *tacacsConversion* program requires a Security and Accounting Server configured with the correct *outdef.dat* file. This is necessary to log the proper RADIUS attributes.

TacacsConversion Command Usage The *tacacsConversion* program resides in the \$SAHOME/bin directory along with the other Security and Accounting Server programs.

```
tacacsConversion [-d] [-i input_accting_file] [-o output_tac_file] - [def
accting_def_file]
```

- **-v** — Prints out version number
- **-d** — Dynamic Mode, Real time TACACS+ conversion using *accting* file, *YYMMDD.rad*, based on current day
- **-def acct_def_file** — use an alternate accounting server output definition file.

- **-i input_accting_file** — use as input accounting file instead of the default of `$SAHOME/data/sa/YMMDD.rad`, where YMMDD is based on the previous day.
- **-o output_tac_file** — used as the TACACS+ output file instead of `$SAHOME/data/sa/YMMDD.tac`, where YMMDD is based on the previous day.

The `-d` option will print the Security and Accounting Server generic RADIUS messages in the TACACS+ format dynamically as the records are written to the `$SAHOME/data/sa/YMMDD.rad` file.

The TACACS+ records will be printed to the screen and to the `$SAHOME/data/sa/YMMDD.tac` file. The file will be flushed so the user could immediately process the data if so desired.

The `-i` and `-o` options will use alternate file names instead of the default files in the `$SAHOME` directory structure. This will allow you to run the conversion program on any file.

Configuring the NAS to Perform PAP

By default the HiPer ARC is set to *PPP receive_authentication any*. The HiPer ARC auto-detects the dial-up clients settings. Since most dial-up clients will try to negotiate CHAP first, the password is encrypted.

Security and Accounting Server supports CHAP, but only when using the local database. When proxy authentication is used, the password is encrypted, but cannot be decrypted by the NT server — therefore the authentication fails.

To configure the HiPer ARC to default to PAP authentication, enter the following command on the HiPer ARC:

```
set ppp receive_authentication pap
```

For more information about `PPP receive_authentication` or `PPP authentication_preference`, refer to the *HiPer ARC Product Reference*.

RADIUS Security and Accounting Server can pass the authentication and accounting responsibility to another RADIUS server.

To indicate that a user's authentication should be performed on another RADIUS server, the server's domain name must be included with the username on login. The format is *username@domainname*. When a user includes a domain after their username, Security and Accounting Server automatically checks for a domain name match in the RADIUS Proxy Domains table. If it finds a match, it will forward the authentication information to the RADIUS server at that domain.

Configuring Communication Between the Servers

To configure the domain information of another RADIUS Server, follow these steps:

- 1 From the Security and Accounting Database Manager, select **Server Setup**. The SystemTabs screen appears.
- 2 Click the **Advanced Options** tab.
- 3 Click **Proxy Servers**. The Proxy Server Parameters screen appears.
- 4 Select the **RADIUS** tab.
- 5 Click **RADIUS Proxies/Tunnel Domains**. The RADIUS Proxy and Tunnel Domains screen appears.
- 6 Enter the following data in the appropriate fields:

Field Name	Description	Example
DOMAINNAME	The domain name a user would include after their username	isp.com <i>See note below.</i>
AUTH_IP	The IP address of the RADIUS server that will perform the authentication for this domain	123.45.6.78
AUTH_PORT_NO	The port number that the RADIUS server will receive authentication messages on. This must be set to the same port on both servers.	1645 (default)
ACCT_IP	The IP address of the RADIUS server that will provide accounting services for this domain	123.45.6.78
ACCT_PORT_NO	The port number that the RADIUS server will receive accounting information on. This must be set to the same port on both RADIUS servers	1646 (default)



The domain listed in this field does not need to be the registered domain name of that IP address. This field is used to link the user with the IP address of the forwarding RADIUS server. Whatever name is used in this field must be entered by the user during their login: username@domainname.

7 Click **Done**.

ACE ACE/Server provides the SecureID token-based authentication for dial-in users. To use ACE/Server to authenticate users, follow these steps:

- Copy the client library file, `sdconf.rec`.
- Proxy user authentication to ACE/Server

Copying the `sdconf.rec` file

Security and Accounting must have access to a copy of the ACE/Server's client library file, `sdconf.rec`. This file is typically located in the `/ace/data` directory on the system running the ACE/Server software.

Place a copy of the `sdconf.rec` file in the `var/ace/` directory of the system running Security and Accounting Server. You may need to create this directory structure.

You can install the `sdconf.rec` file in a different directory, but you must set the correct path. To change the path to the client library file, follow these steps:

- 1** From Security and Accounting Database Manager, click **Server Setup**. The SystemsTabs window appears
- 2** Click the **Advanced Options** tab
- 3** Click **Proxy Servers**. The Proxy Server Parameters window appears.
- 4** Click the **ACE** tab.
- 5** In the **VAR_ACE** box, enter the path to the shared client library file, `sdconf.rec`, on your system. The default directory is `/ace/data`, but `sdconf.rec` can be stored in any directory.

Proxying User Authentication to ACE/Server

To configure Security and Accounting Server to proxy an authentication request to an ACE/Server, follow these steps:

- 1 From Security and Accounting Database Manager, click **User Setup**. The User Configuration window appears.
- 2 Click **Find**.
- 3 In the **Username** box, type the name of a user you would like to configure.
- 4 Click **Load Data**. Information about that user is displayed.
- 5 On the **General** tab, set the Authentication list box to **SecureID**.
- 6 Click **Done**.

Troubleshooting

To troubleshoot your system, try to authenticate a user using just the ACE/Server. If this fails:

- 1 Check that the `sdconf.rec` file is present on the system running Security and Accounting Server and that the path to the file is correct.
- 2 Make sure the ACE/Server client software is running.
- 3 Check that the **Timeout in seconds** box in the ACE tab is not set too small. Security and Accounting Server may be cancelling the connections before the ACE/Server can reply. The default value is 120.
- 4 Check the Security and Accounting Server file `security.log` for errors in the connection.
- 5 Check for errors in the configuration of the users or default user.

Configuring the NAS to Perform PAP

By default the HiPer ARC is set to *PPP receive_authentication any*. The HiPer ARC auto-detects the dial-up clients settings. Since most dial-up clients will try to negotiate CHAP first, the password is encrypted.

Security and Accounting Server supports CHAP, but only when using the local database. When proxy authentication is used, the password is encrypted, but cannot be decrypted by the NT server — therefore the authentication fails.

To configure the HiPer ARC to default to PAP authentication, enter the following command on the HiPer ARC:

```
set ppp receive_authentication pap
```

For more information about PPP receive_authentication or PPP authentication_preference, refer to the HiPer ARC Product Reference.

Omniguard/ Defender™

To configure Security and Accounting Server to proxy authentication to AXENT Technologies Omniguard/Defender Security Server™, follow these steps:

- 1** From the Security and Accounting Database Manager, select **Server Setup**. The SystemTabs screen appears.
- 2** Click the **Advanced Options** tab.
- 3** Click **Proxy Servers**. The Proxy Server Parameters screen appears.
- 4** Click the **Defender** tab.
- 5** In the **Timeout** field, enter the number of seconds Security and Accounting should wait before canceling a proxy to the Defender Server.
- 6** In the **Agent** field, enter the name of the Defender Agent that Security and Accounting Server will communicate with.
- 7** In the **Server** field, enter the IP address of the Defender Security Server.
- 8** In the **Secondary Server** field, enter the IP address of the optional backup Defender Security Server.
- 9** In the **Key** fields, enter the SecureNet™ Key (SNK). This is the SNK DES Key Hex Value listed in the AssureNet server setup screen.

First split the 8 digit key in half. Convert the first 4 digits into hexadecimal and enter it into the first field. Do the same to the last 4 digits of the key and enter that hexadecimal number in the second field. This key number should support both the primary and secondary servers.

Refer to the *Defender Security Server Operational Manual* for more information.

SafeWord To configure Security and Accounting Server to proxy its information to Secure Computing SafeWord™, follow these steps:

- Set the path to the sid.cfg file
- Proxy user authentication to SafeWord

Setting the path to sid.cfg

Security and Accounting Server needs to access the information in contained in the SafeWord sid.cfg file. To set the path, follow these steps:

- 1** From the Security and Accounting Database Manager, select **Server Setup**. The SystemTabs screen appears.
- 2** Click the **Advanced Options** tab.
- 3** Click **Proxy Servers**. The Proxy Server Parameters screen appears.
- 4** Click the **SafeWord** tab.
- 5** In the SafeWord Configuration File box, enter the path to the Safeword sid.cfg file. The default location is /usr/safeword/sid.cfg.
- 6** Click **Done**.

Proxying User Authentication to SafeWord

To configure Security and Accounting Server to proxy an authentication request to SafeWord, follow these steps:

- 1** From Security and Accounting Database Manager, click **User Setup**. The User Configuration window appears.
- 2** Click **Find**.
- 3** In the **Username** box, type the name of a user you would like to configure.
- 4** Click **Load Data**. Information about that user is displayed.
- 5** On the **General** tab, set the Authentication list box to **SafeWord**.
- 6** Click **Done**.

Troubleshooting

To troubleshoot your system, follow these steps:

- 1** Try to authenticate a request from the SafeWord client to the SafeWord Server. If this fails, read the SafeWord documentation for troubleshooting help.
- 2** Check that the SafeWord sid.cfg file resides in the location you entered in the Security and Accounting Server.
- 3** Make sure that SafeWord client software is running.
- 4** Check the SafeWord Server Timeout box in the **SafeWord** tab to see if the timeout is set too short. Security and Accounting Server may be cancelling the connections before SafeWord can reply. The default value is 120 seconds.
- 5** Check the Security and Accounting Server file security.log for errors in the connection.
- 6** Check for errors in the configuration of the users or default user.

EAP RADIUS Server The Extensible Authentication Protocol (EAP) is a PPP extension that provides flexible support for a wide range of authentication methods.

Configuring Communication Between the Servers

To configure Security and Accounting to proxy its information to an EAP capable server:

- 1 From the Security and Accounting Database Manager, select **Server Setup**. The SystemTabs screen appears.
- 2 Click the **Advanced Options** tab.
- 3 Click **Proxy Servers**. The Proxy Server Parameters screen appears.
- 4 Select the **EAP** tab and click **EAP Proxy**. The Extensible Authentication Protocol Data screen appears.
- 5 In the **Name** box, enter a name to identify this server.
- 6 In the **Port** box, enter the port number that this server will communicate on, typically 1645.
- 7 In the **IP** box, enter the IP address of the EAP RADIUS server.
- 8 In the **Secret** box, enter the secret of the EAP RADIUS server.

Proxying User Authentication to an EAP Server

To configure Security and Accounting Server to proxy an authentication request to an EAP server, follow these steps:

- 1 From Security and Accounting Database Manager, click **User Setup**. The User Configuration window appears.
- 2 Click **Find**.
- 3 In the **Username** box, type the name of a user you would like to configure.
- 4 Click **Load Data**. Information about that user is displayed.
- 5 On the **General** tab, set the Authentication list box to **EAP RADIUS Proxy**.
- 6 Choose an EAP server from the EAP Server Name list box.
- 7 Click **Done**.

S/KEY Integration To setup the Security and Accounting Server to work with the S/KEY system follow these steps:

- 1 Install the S/KEY system on the UNIX host. This normally involves putting an S/KEY policy file in `/etc/skeypolicy`.
- 2 In the policy file, define the location of the databases.

```
keyfile /tmp/skeyDB
keyaudit /tmp/skeyAudit
```

- 3 If you do not want users to have local accounts on the UNIX system, set the `local_account_required` field to *no* in the policy file.

```
local_account_required      no
```
- 4 Add all the S/KEY users to the S/KEY database. This is normally done with the `skey_adduser` utility. Every user that wants to authenticate using S/KEY must have a valid login in the S/KEY database.
- 5 Test the S/KEY system by compiling `example2.c`. Read the S/KEY documentation for more information. Do not continue until you can properly authenticate an S/KEY user outside of the S/KEY system.

Proxying User Authentication to S/KEY

To configure Security and Accounting Server to proxy authentication to the S/KEY system, follow these steps:

- 1 From Security and Accounting Database Manager, click **User Setup**. The User Configuration window appears.
- 2 Click **Find**.
- 3 In the **Username** box, type the name of the user you would like to configure.
- 4 Click **Load Data**. Information about that user is displayed.
- 5 On the **General** tab, set the Authentication list box to **SKEY**.
- 6 Click **Done**.

iPass Corporate Access

iPass Corporate Access is a service that allows remote access users to connect to the internet or intranets with a local phone call. The iPass network partners with hundreds of ISPs to provide encrypted authentication and accounting at points of presence (POPs) all over the world.

Restrictions and Limitations

iPass is currently only supported in Sun Solaris 2.5.1 with Security and Accounting Server.

The iPass server currently supports only PPP/SLIP users. Even though a user may be configured as a LOGIN user, iPass will disregard it and pass on a request for a PPP connection.

iPass Authentication Process

The following steps provide an overview of how iPass authenticates users. In this example, a user dials into a "remote" ISP that uses Security and Accounting Server.

- 1 A remote user dials in to the NAS and is prompted for authentication by Security and Accounting Server.
- 2 The user enters a username followed by their corporate domain. The format is: *username@domain*.
- 3 Security and Accounting Server searches through the local database for a match to this user. If it is unsuccessful in finding a match, it then forwards the authentication to the iPass NetServer.

iPass is the last authentication method attempted by Security and Accounting Server after all other authentication methods.

- 4 The iPass NetServer encrypts the user information and forwards it to the nearest iPass Transaction Center. From the Transaction Center, the information is routed to the user's corporate network, based on the domain information given.
- 5 The corporate site's RoamServer receives the information, decrypts it, and strips the domain suffix from the login information before forwarding it to the corporate authentication server.
- 6 The corporate authentication server accepts or rejects the user information. It then sends this information back to Security and Accounting Server using the same iPass network in reverse.
- 7 Finally, Security and Accounting Server sends the NAS a message to either allow or deny access to the user.

Installation of iPass at the ISP Site

- 1 Install Security and Accounting Server version 6.0.99.
- 2 Install the iPass NetServer software on the same management station as Security and Accounting Server. The NetServer software consists of a set of APIs that Security and Accounting Server call.

Follow the directions found in the *iPass RoamServer Installation and Administration Guide*. Even though this guide refers to the RoamServer, the installation of the NetServer is the same.

Installation of iPass at the Corporate Site

- 1 Install Security and Accounting Server version 6.0.99.
- 2 Install the iPass RoamServer software on a management station at the corporate site. Again, follow the directions found in the *iPass RoamServer Installation and Administration Guide*.
- 3 Configure the RoamServer to communicate with Security and Accounting Server.
- 4 Start the RoamServer. The *vnas* daemon must be running for the RoamServer to work.

Remote Login Requirements

Users who plan to use a remote ISP must login with their normal username followed by the @ symbol and the domain name of their corporate network. The format is *username@domain*.



Security and Accounting Server uses the format username@domain to proxy authentication to other domains, such as other RADIUS servers. Be aware that if an iPass user logs in using a domain configured in Security and Accounting Server's DOMAINS table, the authentication will be forwarded to the IP address that matches that domain, not to iPass.

For more information, see Proxying to another [RADIUS](#) Server.

4

CONFIGURING VPN

Virtual Private Networks

This section gives a brief overview of Virtual Private Networks (VPN) and explains how Security and Accounting Server implements VPN support.

VPN Overview

A VPN is a Wide Area Network (WAN) link over a shared public network. This shared public network is typically the internet or an IP backbone from a network service provider. VPNs use a technique called 'tunneling' to transmit data packets safely across this public network.

VPNs are useful to businesses because they can:

- outsource the management of remote access to a network service provider. By using a VPN, a company can eliminate remote access concentrators, servers, and the personnel needed to operate that equipment.
- reduce the number of access lines into a corporate site. Many companies have separate high speed lines for their data and internet connections. A VPN could eliminate the need for a separate line to carry the data.
- use the internet or carry data (rather than paying long distance phone charges). By dialing in to a local ISP, a telecommuter can eliminate the long distance call directly to the company remote access concentrator.

Tunnel Standards

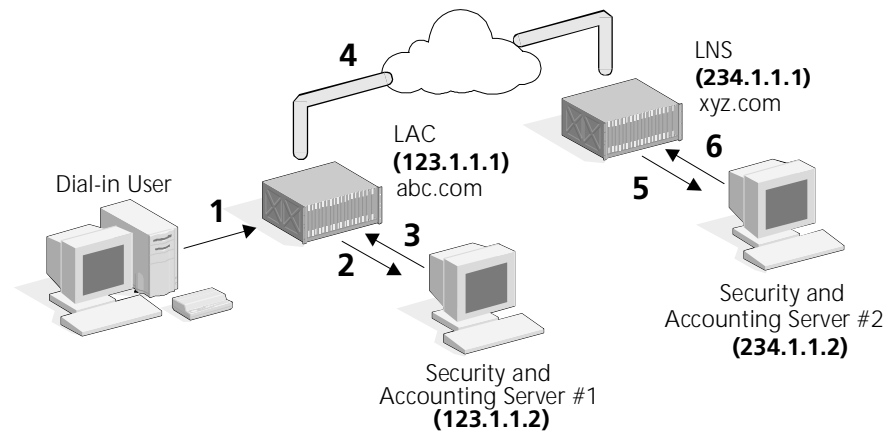
Security and Accounting Server supports the leading standards for dial-up VPNs: Layer 2 Tunneling Protocol (L2TP) and Point-to-Point Tunneling Protocol (PPTP). PPTP, for use with Microsoft Windows NT, was one of the first protocols for use for dial-up VPNs. L2TP, an open tunneling protocol, builds upon the features implemented in PPTP and supports tunneling over frame relay and ATM networks.

Refer to the following table for the major differences between L2TP and PPTP:

Feature	L2TP	PPTP
Support for Windows NT Server acting as a Network Server?	No	Yes
Built-in Security?	Yes — designed for non-IP networks dial-in applications	No — but can be used with Microsoft Point-to-Point Encryption (MPPE) and Microsoft Challenge Handshake Access Protocol (MS-CHAP)
Protocols Used?	Control Channel = User Datagram Protocol Data Channel = User Datagram Protocol	Control Channel = Transmission Control Protocol Data Channel = Generic Routing Encapsulation
Ability to terminate tunnel at either end of the tunnel?	Yes	No

Tunneling Using L2TP

The following section describes the initiation of an L2TP tunnel using Security and Accounting Server:



- 1 A user dials into a local point of presence. The NAS that accepts this call is referred to as the Tunnel Initiator or L2TP Access Concentrator (LAC).
- 2 The LAC sends an Access Request message to Security and Accounting Server #1.

- 3 Security and Accounting Server recognizes that the tunneling request came from a LAC. It returns an Access Accept message to the LAC containing the necessary tunnel information to start the tunnel. The user is not authenticated at this point, the access accept allows the LAC to initiate the tunnel.
- 4 The LAC opens a tunnel to the remote NAS, referred to as the Tunnel Terminator or the L2TP Network Server (LNS), and passes its domain name information to the LNS.
- 5 The LNS sends an Access Request message to Security and Accounting Server #2 and forwards the domain name of the LAC.
- 6 Security and Accounting Server #2 sends an Access Accept back to the LNS after authenticating the tunnel user. It returns only the Tunnel Password and Tunnel Security attributes. This message is used to authenticate the tunnel.
- 7 Now the user completes a normal PPP authentication at the LNS within the tunnel.

Methods of Tunnel Initiation

There are three ways to initiate an L2TP tunnel with Security and Accounting Servers:

- [Domain Based Authentication](#) — configure each domain in the DOMAINS table to link to a specific tunnel configuration. Each user that dials in with that specific domain will have access to the VPN.
 - [Setting Up Security and Accounting Server #1](#)
 - [Setting Up Security and Accounting Server #2](#)
- [DNIS/ANI Based Authentication](#) — configure a new tunnel using the Called_Station_ID attribute (DNIS), or Calling_Station_ID attribute (ANI) and link that user directly to a specific tunnel configuration.
 - [Setting Up Security and Accounting Server #1](#)
 - [Setting Up Security and Accounting Server #2](#)
- [Username Based Authentication](#) — configure a new tunnel user and link that user directly to a specific tunnel setting.
 - [Setting Up Security and Accounting Server #1](#)
 - [Setting Up Security and Accounting Server #2](#)

For each configuration, you must set up both Servers, one at each end of the tunnel.

Domain Based Authentication

Setting Up Security and Accounting Server #1

To configure Security and Accounting Server at the LAC, follow these steps:

Setting Up the Tunnel Domain This procedure links the domain that the user logs in with, *joe@abc.com*, with a specific tunnel configuration.

- 1 In Security and Accounting Database Manager, click **Server Setup**. The SystemTabs screen appears.
- 2 Select the **Advanced Options** tab.
- 3 Click **Proxy Servers/Domains**. The RADIUS Proxy and Tunnel Domains screen appears.
- 4 Select the **RADIUS** tab and click **RADIUS Proxies/Tunnel Domains**.
- 5 Click **New** and fill out the following information, based on the example configuration shown above:
 - **Domain Name** — **xyz.com**
 - **Tunnel Name** — **xyztunnel**



Do not enter information in the Authentication or Accounting fields. If you do, Security and Accounting Server will proxy the request messages to the IP address indicated as a standard RADIUS proxy.

- 6 Click **Done**.
- 7 Click **Done** once more to return the **Advanced Options** tab.

Configuring the Tunnel Attributes Follow this procedure to set up the LAC end of the tunnel.

- 1 From the **Advanced Options** tab, click **Tunnel Attributes**. The Tunnel Configuration Data screen appears.
- 2 Click **New** and fill out the following information, based on the example configuration shown above:
 - **Tunnel Name** — **xyztunnel**
 - **Tunnel Type** — **L2TP**
 - **Tunnel Server Endpoint** — **234.1.1.1**
- 3 Click **Done**.

Configuring the Tunnel Initiator Table Security and Accounting Server must be able to recognize that the request is coming from the Tunnel Initiator, or LAC.

- 1 From the **Advanced Options** tab, click **Tunnel Initiators**. The Tunnel Initiator Data screen appears.
- 2 Click **New** and fill out the following information, based on the example configuration shown above:
 - **NAS IP Address** — 123.1.1.1
 - **Tunnel Name** — xyztunnel
- 3 Click **Done**.

Setting Up Security and Accounting Server #2

To configure the Security and Accounting Server at the LNS, follow these steps:

Configuring the Tunnel Attributes Follow this procedure to set up the LNS end of the tunnel.

- 1 From Security and Accounting Database Manager, click **Server Setup**. The SystemTabs screen appears.
- 2 Select the **Advanced Options** tab.
- 3 Click **Tunnel Attributes**. The Tunnel Configuration Data screen appears.
- 4 Click **New** and fill out the following information, based on the example configuration shown above:
 - **Tunnel Name** — abctunnel
 - **Tunnel Password** — anypassword
 - **Tunnel Security** — Data Only, Control Only, Both, or None
- 5 Click **Done**.

Adding the New Tunnel User This "tunnel user" will be used to authenticate the tunnel session. Once the tunnel is authenticated, another access request is sent over the secured tunnel to Security and Accounting Server #2 to authenticate the dial-in user.

- 1 From Security and Accounting Database Manager, click **User Setup**. The User Configuration screen appears.
- 2 Add a user *abc.com* and assign this user a unique password.

- 3 At the bottom of the **General** tab, select **Tunnel Setup Request?**
- 4 In the **Tunnel Name** field, enter *abctunnel*, the name you assigned to this tunnel configuration.

The screenshot shows the 'User Configuration' dialog box with the 'General' tab selected. The 'Tunnel Name' field contains 'abctunnel' and the 'Tunnel Setup Request?' checkbox is checked. The 'Username' field contains 'DEFAULT' and the 'Password' field contains 'default'. The 'Expiration' field is set to 'MM/DD/YYYY'. The 'Failed Logins' field contains '0' and the 'Deny Access' checkbox is unchecked. The 'Dial In Restrictions' section includes checkboxes for 'Check Port Number?', 'Check DNIS?', and 'Check ANI?', all of which are unchecked. The 'Port Number Name List', 'DNIS Restriction List', and 'ANI Restriction List' fields are empty. The 'Maximum Number of concurrent sessions' field contains '0'. The 'Hosts Via DNS' field is empty, and the 'Host Domain name' field is empty. The 'Acct. Interim Interval' field is empty, and the 'Interval in seconds between subsequent Acctg. Interim Msgs. (Min 60, Max 600)' field is empty.

Adding a User Now that the tunnel configuration is set up, the users still need to be authenticated at the LNS. Add these users as you would any other.



The access request message will arrive at Security and Accounting Server #2 in the format: joe@abc.com. You can enter the username as joe@abc.com only if you do not have a domain proxy set up. For more information about Domains, see [RADIUS Proxy Domains](#).

DNIS/ANI Based Authentication

Setting Up Security and Accounting Server #1

Configuring the Tunnel Attributes Follow this procedure to set up the LAC end of the tunnel.

- 1 In Security and Accounting Database Manager, click **Server Setup**. The SystemTabs screen appears.
- 2 Select the **Advanced Options** tab.
- 3 Click **Tunnel Attributes**. The Tunnel Configuration Data screen appears.
- 4 Click **New** and fill out the following information, based on the example configuration shown above:
 - **Tunnel Name** — `dnistunnel`
 - **Tunnel Type** — `L2TP`
 - **Tunnel Server Endpoint** — `234.1.1.1`
- 5 Click **Done**.

Configuring the Tunnel Initiator Table This table indicates to Security and Accounting Server that the request is coming from the Tunnel Initiator, or LAC.

- 1 From the **Advanced Options** tab, click **Tunnel Initiators**. The Tunnel Initiator Data screen appears.
- 2 Click **New** and fill out the following information, based on the example configuration shown above:
 - **NAS IP Address** — `123.1.1.1`
 - **Tunnel Name** — `dnistunnel`
- 3 Click **Done**.

Adding the New Tunnel User This "tunnel user" will be used to authenticate the tunnel session. Once the tunnel is authenticated, another access request is sent over the secured tunnel to Security and Accounting Server #2 to authenticate the dial-in user.

- 1 From Security and Accounting Database Manager, click **User Setup**. The User Configuration screen appears.
- 2 Add a new user `3125551212`. Use the DNIS or ANI number as the username. Assign the user a unique password.
- 3 In the **Tunnel Name** field, enter `dnistunnel`, the name you assigned to this tunnel configuration.

Setting Up Security and Accounting Server #2

Configuring the Tunnel Attributes Follow this procedure to configure the LNS end of the tunnel.

- 1 From Security and Accounting Database Manager, click **Server Setup**. The SystemTabs screen appears.
- 2 Select the **Advanced Options** tab.
- 3 Click **Tunnel Attributes**. The Tunnel Configuration Data screen appears.
- 4 Click **New** and fill out the following information, based on the example configuration shown above:
 - **Tunnel Name** — `dnistunnel`
 - **Tunnel Password** — `anypassword`
 - **Tunnel Security** — `Data Only, Control Only, Both, or None`
- 5 Click **Done**.

Adding the New Tunnel User This “tunnel user” will be used to authenticate the tunnel session. Once the tunnel is authenticated, another access request is sent over the secured tunnel to Security and Accounting Server #2 to authenticate the dial-in user.

- 1 From Security and Accounting Database Manager, click **User Setup**. The User Configuration screen appears.
- 2 Add a user `abc.com` and assign this user a unique password.
- 3 At the bottom of the **General** tab, select **Tunnel Setup Request?**
- 4 In the **Tunnel Name** field, enter `dnistunnel`, the name you assigned to this tunnel configuration.

Adding a User Now that the tunnel configuration is set up, the users still need to be authenticated at the LNS. Add these users as you would any other.

In this case, add a user named 8475551212.

Username Based Authentication

Setting Up Security and Accounting Server #1

Configuring the Tunnel Attributes Follow this procedure to set up the LAC end of the tunnel.

- 1 In Security and Accounting Database Manager, click **Server Setup**. The SystemTabs screen appears.
- 2 Select the **Advanced Options** tab.
- 3 Click **Tunnel Attributes**. The Tunnel Configuration Data screen appears.
- 4 Click **New** and fill out the following information, based on the example configuration shown above:
 - **Tunnel Name** — `xyztunnel`
 - **Tunnel Type** — `L2TP`
 - **Tunnel Server Endpoint** — `234.1.1.1`
- 5 Click **Done**.

Configuring the Tunnel Initiator Table This step configures Security and Accounting Server to recognize that the access request is coming from the Tunnel Initiator, or LAC.

- 1 From the **Advanced Options** tab, click **Tunnel Initiators**. The Tunnel Initiator Data screen appears.
- 2 Click **New** and fill out the following information, based on the example configuration shown above:
 - **NAS IP Address** — `123.1.1.1`
 - **Tunnel Name** — `xyztunnel`
- 3 Click **Done**.

Adding a New User Follow this procedure to add a user that will use the VPN connection.

- 1 From Security and Accounting Database Manager, click **User Setup**. The User Configuration screen appears.
- 2 Add a new user and assign this user a unique password.
- 3 In the **Tunnel Name** field, enter `xyztunnel`, the name you assigned to the tunnel configuration above.
- 4 When you are finished configuring this user, click **Done**.

Setting Up Security and Accounting Server #2

Configuring the Tunnel Attributes Follow this procedure to configure the LNS end of the tunnel.

- 1 From Security and Accounting Database Manager, click **Server Setup**. The SystemTabs screen appears.
- 2 Select the **Advanced Options** tab.
- 3 Click **Tunnel Attributes**. The Tunnel Configuration Data screen appears.
- 4 Click **New** and fill out the following information, based on the example configuration shown above:
 - **Tunnel Name** — `abctunnel`
 - **Tunnel Password** — `anypassword`
 - **Tunnel Security** — `Data Only, Control Only, Both, or None`
- 5 Click **Done**.

Adding the New Tunnel User This “tunnel user” will be used to authenticate the tunnel session. Once the tunnel is authenticated, another access request is sent over the secured tunnel to Security and Accounting Server #2 to authenticate the dial-in user.

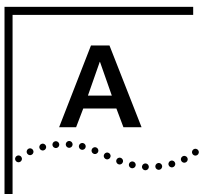
- 1 From Security and Accounting Database Manager, click **User Setup**. The User Configuration screen appears.
- 2 Add a new user *joe*. Assign the user a unique password.
- 3 At the bottom of the **General** tab, select **Tunnel Setup Request?**
- 4 In the **Tunnel Name** field, enter *abctunnel*, the name you assigned to this tunnel configuration.

Adding a User Now that the tunnel configuration is set up, the users still need to be authenticated at the LNS. Add these users as you would any other.

Tunnel Attributes The following attributes are located in the Tunnels table:

Table Field (Attribute Number)	Description	Example
Tunnel_Name (VSA 0x9007)	Name you assign to a common set of tunnel attributes.	XYZ

Table Field (Attribute Number)	Description	Example
Tunnel_Type (64)	Tunneling protocol to be used.	PPTP L2TP
Tunnel_Medium_Type (65)	Medium supported by the tunnel initiator.	IP (version 4) E.164 (Frame Relay, ATM, SMDS)
Tunnel_Client_Endpoint (66)	IP address of the initiator (access concentrator) of the tunnel.	123.123.123.123 or server.abc.com
Tunnel_Server_Endpoint (67)	IP address of the terminator (network server) of the tunnel.	234.234.234.234 or server.xyz.com
Acct_Tunnel_Conn_ID (68)	Uniquely identifies a tunnel session for accounting purposes.	Assigned by Security and Accounting
Tunnel_Password (69)	Password used to encrypt information passed to HiPer ARC.	crater6 (Must be 3 characters or longer)
Tunnel_Preference (83)	Relative priority of this set of tunnel attributes Forwarded, but not used by the HiPer ARC	
Tunnel_Security (VSA 0x9844)	Vendor-specific attribute that defines which part of the tunnel will have security enabled.	None Control Only Data Only Both Data and Control
Tunnel_Assignment_ID	Forwarded, but not used by the HiPer ARC	
Tunnel_Private_Group_ID	Forwarded, but not used by the HiPer ARC	



STANDARD RADIUS ATTRIBUTES

These are the standard RADIUS attributes used by Security and Accounting Server

Attribute	Type	Value	Description
User_Name	1	Text£32	Indicates the name of the user to be authenticated. It is only used in Access-Request packets.
User_Password	2	Text£16	Indicates the password of the user to be authenticated, or the user's input following an Access-Challenge. It is only used in Access-Request packets.
CHAP_Password	3		Indicates the response value provided by a PPP Challenge-Handshake Authentication Protocol (CHAP) user in response to the challenge. It is only used in Access-Request packets. The CHAP challenge value is found in the CHAP_Challenge Attribute (60) if present in the packet, otherwise in the Request Authenticator field.
NAS_IP_Address	4		Indicates the identifying IP Address of the NAS which is requesting authentication of the user. It is only used in Access-Request packets. Either NAS-IP-Address or NAS-Identifier should be present in an Access-Request packet.
NAS_IP_Port	5		Indicates the physical port number of the NAS which is authenticating the user. It is only used in Access-Request packets. Note that this is using "port" in its sense of a physical connection on the NAS, not in the sense of a TCP or UDP port number. Either NAS-Port or NAS-Port-Type (61) or both should be present in an Access-Request packet, if the NAS differentiates among its ports.
Service_Type	6	1= Login 2= Framed 4= Callback 8= DialOut 10= Admin	Indicates the type of service the user has requested, the type of service to be provided, or a change in the type of link to be configured. It may be used in both Access-Request and Access-Accept packets. A NAS is not required to implement all of these service types, and must treat unknown or unsupported Service-Types as if an Access-Reject had been received instead.

Attribute	Type	Value	Description
Framed_Protocol	7	1= PPP 2= SLIP 3= PPTP 4= RFC1490	Indicates the framing to be used for framed access. It may be used in both Access-Request and Access-Accept packets. The default is value is PPP.
Framed_IP_Address	8	Uint32 ip address	Indicates the address to be configured for the user. It may be used in Access-Accept packets. It may be used in an Access-Request packet as a hint by the NAS to the server that it would prefer that address, but the server is not required to honor the hint. Th default is 0.0.0.0 to speicfy an address from the local pool.
Framed_IP_Netmask	9	Uint32 ip address	Indicates the IP netmask to be configured for the user when the user is a router to a network. It may be used in Access-Accept packets. It may be used in an Access-Request packet as a hint by the NAS to the server that it would prefer that netmask, but the server is not required to honor the hint. The default ip address is 255.255.255.255.
Framed_Routing	10	0= None 1= Broadcast 2= Listen 3= Broadcast-Listen	Indicates the routing method for the user, when the user is a router to a network. It is only used in Access-Accept packets. This attribute only applies to IP ripv1.
Filter_Id	11	Text£254	Indicates the name of the filter list for this user. Zero or more Filter-Id attributes may be sent in an Access-Accept packet. Identifying a filter list by name allows the filter to be used on different NASs without regard to filter-list implementation details.
Framed_MTU	12	Uint32	Indicates the Maximum Transmission Unit to be configured for the user, when it is not negotiated by some other means (such as PPP). It is only used in Access-Accept packets. PPP connections are set between 100 and 1514; SLIP connections between 100 and 1006. The default is 1514.
Framed_Compression	13	1=VJ TCP/IP	Indicates a compression protocol to be used for the link. It may be used in Access-Accept packets. It may be used in an Access-Request packet as a hint to the server that the NAS would prefer to use that compression, but the server is not required to honor the hint. The default is VJ TCP/IP header compression. More than one compression protocol Attribute may be sent. It is the responsibility of the NAS to apply the proper compression protocol to appropriate link traffic. This attribute has only one setting because PPP does not support IPX header compression.

Attribute	Type	Value	Description
Login_IP_Host	14	UInt32 ip address	Indicates the system with which to connect the user, when the Login-Service Attribute is included. It may be used in Access-Accept packets. It may be used in an Access-Request packet as a hint to the server that the NAS would prefer to use that host, but the server is not required to honor the hint. The default is 0.0.0.0. The address 255.255.255.255 initiates a user prompt; 0.0.0.0 causes the server to pick a connection host from the default host table.
Login_Service	15	0= Telnet 1= Rlogin 2= Clear-TCP	Indicates the service which should be used to connect the user to the login host. It is only used in Access-Accept packets. The default is Telnet.
Login_Port	16	UInt32	Indicates the TCP (or LAT) port with which the user is to be connected, when the Login_Service Attribute is also present. It is only used in Access-Accept packets. The default is 23, the default telnet port.
Old_Password (NMC Only)	17	Text£16	Prompts for the existing password before allowing the user to change to a new password. This attribute is used only in Password-Request packets.
Reply_Message	18	Text<254	Indicates text which may be displayed to the user. When used in an Access-Accept packet, it is the success message. When used in an Access-Reject packet, it is the failure message. It may indicate a dialog message to prompt the user before another Access-Request attempt. When used in an Access-Challenge packet, it may indicate a dialog message to prompt the user for a response. Multiple Reply-Message's may be included and if any are displayed, they must be displayed in the same order as they appear in the packet. The default is NULL.
Callback_Number	19	String<254	Indicates a dialing string to be used for callback. It may be used in Access-Accept packets. It may be used in an Access-Request packet as a hint to the server that a Callback service is desired, but the server is not required to honor the hint.
Callback_ID	20		Indicates the name of a place to be called, to be interpreted by the NAS. It may be used in Access-Accept packets.
Expiration (deprecated)	21	String<254	Specifies the date the password expires.
Framed_Route	22	String<254	Provides routing information to be configured for the user on the NAS, specifying the static route or set of routers the connection must take. It is used in the Access-Accept packet and can appear multiple times. The default is NULL. The format is Framed Route = "destination gateway metric," where destination is the IP address of the host, gateway is the router to the host or network, and metric, or hop-count, is the number of routers between the destination and gateway. The framed route can appear multiple times.

Attribute	Type	Value	Description
Framed_IPX_Network	23	Unit32	Indicates the IPX Network number to be configured for the user. It is used in Access-Accept packets. The default is 00000000.
State	24		This Attribute is available to be sent by the server to the client in an Access-Challenge and must be sent unmodified from the client to the server in the new Access-Request reply to that challenge, if any. This Attribute is available to be sent by the server to the client in an Access-Accept that also includes a Termination-Action Attribute with the value of RADIUS-Request. If the NAS performs the Termination-Action by sending a new Access-Request upon termination of the current session, it must include the State attribute unchanged in that Access-Request. In either usage, no interpretation by the client should be made. A packet may have only one State Attribute. Usage of the State Attribute is implementation dependent.
Class	25		This Attribute is available to be sent by the server to the client in an Access-Accept and should be sent unmodified by the client to the accounting server as part of the Accounting-Request packet if accounting is supported. No interpretation by the client should be made.
Vendor_Specific	26		This Attribute allows vendors to support their own extended Attributes not suitable for general usage. It must not affect the operation of the RADIUS protocol. Servers not equipped to interpret the vendor-specific information sent by a client must ignore it (although it may be reported). Clients which do not receive desired vendor-specific information should make an attempt to operate without it, although they may do so (and report they are doing so) in a degraded mode.
Session_Timeout	27	Unit32	Sets the maximum number of seconds of service to be provided to the user before termination of the session or prompt. This Attribute is available to be sent by the server to the client in an Access-Accept or Access-Challenge packet. The default is 0.
Idle_Timeout	28	Unit32	Sets the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt. This Attribute is available to be sent by the server to the client in an Access-Accept or Access-Challenge. The default is 300.
Termination_Action	29		Indicates what action the NAS should take when the specified service is completed. It is only used in Access-Accept packets.
Called_Station_Id	30		Allows the NAS to send in the Access-Request packet the phone number that the user called, using Dialed Number Identification (DNIS) or similar technology. Note that this may be different from the phone number the call comes in on. It is only used in Access-Request packets.

Attribute	Type	Value	Description
Calling_Station_Id	31		Allows the NAS to send in the Access-Request packet the phone number that the call came from, using Automatic Number Identification (ANI) or similar technology. It is only used in Access-Request packets.
NAS_Identifier	32		Contains a string identifying the NAS originating the Access-Request. It is only used in Access-Request packets. Either NAS-IP-Address or NAS-Identifier should be present in an Access-Request packet.
Proxy_State	33		This Attribute is available to be sent by a proxy server to another server when forwarding an Access-Request and must be returned unmodified in the Access-Accept, Access-Reject or Access-Challenge. This attribute should be removed by the proxy server before the response is forwarded to the NAS. Usage of the Proxy-State Attribute is implementation dependent. A description of its function is outside the scope of this specification.
Login_LAT_Service	34		Indicates the system with which the user is to be connected by LAT. It may be used in Access-Accept packets, but only when LAT is specified as the Login-Service. It may be used in an Access-Request packet as a hint to the server, but the server is not required to honor the hint. Administrators use the service attribute when dealing with clustered systems, such as a VAX or Alpha cluster. In such an environment several different time sharing hosts share the same resources (disks, printers, etc.), and administrators often configure each to offer access (service) to each of the shared resources. In this case, each host in the cluster advertises its services through LAT broadcasts. Sophisticated users often know which service providers (machines) are faster and tend to use a node name when initiating a LAT connection. Alternately, some administrators want particular users to use certain machines as a primitive form of load balancing (although LAT knows how to do load balancing itself).
Login_LAT_Node	35		Indicates the Node with which the user is to be automatically connected by LAT. It may be used in Access-Accept packets, but only when LAT is specified as the Login-Service. It may be used in an Access-Request packet as a hint to the server, but the server is not required to honor the hint.

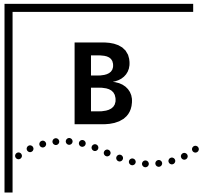
Attribute	Type	Value	Description
Login_LAT_Group	36		Contains a string identifying the LAT group codes which this user is authorized to use. It may be used in Access-Accept packets, but only when LAT is specified as the Login-Service. It may be used in an Access-Request packet as a hint to the server, but the server is not required to honor the hint. LAT supports 256 different group codes, which LAT uses as a form of access rights. LAT encodes the group codes as a 256-bit bitmap. Administrators can assign one or more of the group code bits at the LAT service provider; it will only accept LAT connections that have these group codes set in the bit map. The administrators assign a bitmap of authorized group codes to each user; LAT gets these from the operating system, and uses these in its requests to the service providers.
Framed_AppleTalk_Link	37		Indicates the AppleTalk network number which should be used for the serial link to the user, which is another AppleTalk router. It is only used in Access-Accept packets. It is never used when the user is not another router.
Framed_AppleTalk_Network	38		Indicates the AppleTalk Network number which the NAS should probe to allocate an AppleTalk node for the user. It is only used in Access-Accept packets. It is never used when the user is another router. Multiple instances of this Attribute indicate that the NAS may probe using any of the network numbers specified.
Framed_AppleTalk_Zone	39		Indicates the AppleTalk Default Zone to be used for this user. It is only used in Access-Accept packets. Multiple instances of this attribute in the same packet are not allowed.
Acct_Status_Type	40		Indicates whether this Accounting-Request marks the beginning of the user service (Start) or the end (Stop). It may be used by the client to mark the start of accounting (for example, upon booting) by specifying Accounting-On and to mark the end of accounting (for example, just before a scheduled reboot) by specifying Accounting-Off.
Acct_Delay_Time	41		Indicates how many seconds the client has been trying to send this record for, and can be subtracted from the time of arrival on the server to find the approximate time of the event generating this Accounting-Request. (Network transit time is ignored.) Note that changing the Acct-Delay-Time causes the Identifier to change; see the discussion under Identifier above.
Acct_Input_Octets	42		Indicates how many octets have been received from the port over the course of this service being provided, and can only be present in Accounting-Request records where the Acct_Status_Type is set to Stop.
Acct_Output_Octets	43		Indicates how many octets have been sent to the port in the course of delivering this service, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.

Attribute	Type	Value	Description
Acct_Session_Id	44		This attribute is a unique Accounting ID to make it easy to match start and stop records in a log file. The start and stop records for a given session must have the same Acct_Session_Id. It is strongly recommended that the Acct_Session_Id be a printable ASCII string. For example, one implementation uses a string with an 8-digit upper case hexadecimal number, the first two digits increment on each reboot (wrapping every 256 reboots) and the next 6 digits counting from 0 for the first person logging in after a reboot up to $2^{24}-1$, about 16 million. Other encodings are possible.
Acct_Authentic	45		This attribute may be included in an Accounting-Request to indicate how the user was authenticated, whether by RADIUS, the NAS itself, or another remote authentication protocol. Users who are delivered service without being authenticated should not generate Accounting records.
Acct_Session_Time	46		Indicates how many seconds the user has received service for, and can only be present in Accounting-Request records where the Acct_Status_Type is set to Stop.
Acct_Input_Packets	47		Indicates how many packets have been received from the port over the course of this service being provided to a Framed User, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
Acct_Output_Packets	48		Indicates how many packets have been sent to the port in the course of delivering this service to a Framed User, and can only be present in Accounting-Request records where the Acct_Status_Type is set to Stop.
Acct_Terminate_Cause	49		Indicates how the session was terminated, and can only be present in Accounting-Request records where the Acct_Status_Type is set to Stop.
Acct_Multi_Session_Id	50		
Acct_Link_Count	51		
CHAP_Challenge	60		Contains the CHAP Challenge sent by the NAS to a PPP Challenge-Handshake Authentication Protocol (CHAP) user. It is only used in Access-Request packets. If the CHAP challenge value is 16 octets long it may be placed in the Request Authenticator field instead of using this attribute.
NAS_Port_Type	61		Indicates the type of the physical port of the NAS which is authenticating the user. It can be used instead of or in addition to the NAS-Port (5) attribute. It is only used in Access-Request packets. Either NAS-Port (5) or NAS-Port-Type or both should be present in an Access-Request packet, if the NAS differentiates among its ports.

Attribute	Type	Value	Description
Port_Limit	62		Sets the maximum number of ports to be provided to the user by the NAS. This Attribute may be sent by the server to the client in an Access-Accept packet. It is intended for use in conjunction with Multilink PPP [7] or similar uses. It may also be sent by the NAS to the server as a hint that that many ports are desired for use, but the server is not required to honor the hint.
Login_LAT_Port	63		Indicates the Port with which the user is to be connected by LAT. It may be used in Access-Accept packets, but only when LAT is specified as the Login-Service. It may be used in an Access-Request packet as a hint to the server, but the server is not required to honor the hint.
Tunnel_Type	64		Indicates the tunneling protocol(s) to be used. It may be included in Access-Request, Access-Accept and Accounting-Request packets. If the Tunnel-Type Attribute is present in an Access-Request packet, it should be taken as a hint to the RADIUS server as to the tunnelling protocols supported by the tunnel initiator; the RADIUS server may ignore the hint, however. A tunnel initiator is not required to implement any of these tunnel types; if a tunnel initiator receives an Access-Accept packet which contains only unknown or unsupported Tunnel-Types, the tunnel initiator must behave as though an Access-Reject had been received instead.
Tunnel_Medium_Type	65	1= IP (version 4) 2= IP6 (version 6) 3= NSAP 4= HDLC (8-bit multidrop) 5= BBN 1822 6= 802 7= E.163 (POTS) 8= E.164 (SMDS, Frame Relay, ATM) 9= F.69 (Telex) 10= X.121 (X.25, Frame Relay) 11= IPX 12= Appletalk 13= Decnet IV 14= Banyan Vines 15= E.164 with NSAP format subaddress	Indicates which transport medium to use when creating a tunnel for those protocols (such as L2TP) that can operate over multiple transports. It may be included in both Access-Request and Access-Accept packets; if it is present in an Access-Request packet, it should be taken as a hint to the RADIUS server as to the tunnel mediums supported by the tunnel initiator. The RADIUS server may ignore the hint.

Attribute	Type	Value	Description
Tunnel_Client_Endpoint	66		Contains the address of the initiator end of the tunnel. It may be included in both Access-Request and Access-Accept packets to indicate the address from which a new tunnel is to be initiated. If the Tunnel-Client-Endpoint Attribute is included in an Access-Request packet, the RADIUS server should take the value as a hint; the server is not obligated to honor the hint, however. It should be included in Accounting-Request packets which contain Acct-Status-Type attributes with values of either Start or Stop, in which case it indicates the address from which the tunnel was initiated. This Attribute, along with the Tunnel-Server-Endpoint and Acct-Tunnel-Connection-ID attributes, may be used to provide a globally unique means to identify a tunnel for accounting and auditing purposes.
Tunnel_Server_Endpoint	67		Indicates the address of the server end of the tunnel. The Tunnel-Server-Endpoint Attribute MAY be included (as a hint to the RADIUS server) in the Access-Request packet and MUST be included in the Access-Accept packet if the initiation of a tunnel is desired. It SHOULD be included in Accounting-Request packets which contain Acct-Status-Type attributes with values of either Start or Stop and which pertain to a tunneled session. This Attribute, along with the Tunnel-Client-Endpoint and Acct-Tunnel-Connection-ID Attributes, may be used to provide a globally unique means to identify a tunnel for accounting and auditing purposes.
Acct_Tunnel_Connection_ID	68		
Tunnel_Password	69		May contain a password to be used to authenticate to a remote server. It may only be included in an Access-Accept packet.
ARAP-Password	70		
ARAP-Feature	71		
ARAP-Sone-Access	72		
ARAP-Security	73		
ARAP-Security-Data	74		
Password-Retry	75		
Prompt	76		
Connect-Info	77		
Configuration-Token	78		
EAP-Message	79		Encapsulates Extensible Authentication Protocol (EAP) packets to allow the NAS to authenticate dial-in users via EAP without having to understand the protocol.
Signature	80		

Attribute	Type	Value	Description
Tunnel_Private_Group_ID	81		Indicates the group ID for a particular tunneled session. The Tunnel-Private-Group-ID Attribute may be included in the Access-Request packet if the tunnel initiator can pre-determine the group resulting from a particular connection and should be included in the Access-Reply packet if this tunnel session is to be treated as belonging to a particular private group. Private groups may be used to associate a tunneled session with a particular group of users. For example, it may be used to facilitate routing of unregistered IP addresses through a particular interface. It should be included in Accounting-Request packets which contain Acct-Status-Type attributes with values of either Start or Stop and which pertain to a tunneled session.
Framed_IP_Address_Pool_Name	217		
Char_Noecho	250		This is an alternative attribute that directs the NETServer to not echo the password entered.



VENDOR-SPECIFIC ATTRIBUTES

These are the 3Com specific or vendor-specific attributes supported in Security and Accounting Server.

NMC-Specific Extensions (224-240)

This table describes each attribute supported by Security and Accounting Server.

Attribute	Type	Values	Description
User_Group_Name	223		
Dial_In_Sec_Mode	224	0 = Pass Through (Default) 1 = Dialback Stored Number 2 = Dialback Entered Number	Identifies the type of dial-in security mode used for this user once the initial login sequence is passed. It specifies one of three possible values: <ul style="list-style-type: none">■ Pass-Thru, where the user is connected directly to the DTE.■ Dial-Back Stored Number, where the NMC disconnects the modem and dials back a stored number for this user.■ Dial-Back Entered Number, where the user is prompted to supply a number at which to be called back.
Req_Db_Mdm_Sel	225		If this field is enabled, the NMC prompts dial-back users at login for a dial-back modem. The system displays all valid choices from the list of Allowed Dial-Back Modems in a menu. Users must enter the number that appears on the menu next to their choice. If this field is disabled, the NMC checks the Allowed Dial-Back modem field, polls the modems, and reserves the first available modem to dial back. The default for this field is disabled.
Req_Db_Login_Valid	226		If enabled, the security system issues a login validation sequence during dial back. The default is not to perform dialback login validation.
Dialback_Group_Names	227		This field represents a list of dialback groups that this user, or user group, is a member of. A user or user group may be a member of zero, one, or more dialback groups.
Dial_In_Call_Rest	228		This field represents a list of restricted or allowed dial back phone numbers issued during dial-in security sessions.

Attribute	Type	Values	Description
Dial_Out_Call_Rest	229		This field represents a list of restricted or allowed dial-out phone numbers.
Logins_Before_Blacklist	230		
Failed_Logins	231		
Allowed_DB_Modems	233		Applies only for dialback groups and to both Dial-Back Stored and Dial-Back Entered Number modes. This is a string field that defines what modems may dial back a user. Modems are specified in slot/channel or dial back modem group format in a comma separated list. The default is empty. You may specify a range of modems. If you use SAME_MODEM, then the modem used for dial-in will be the dialback modem. All modems must be in the same chassis. When alternate modems are selected for dialback, the system checks the specified dialback modem for availability and reserves it. If the modem is in use, the system advises the user and terminates the call.

3Com Vendor Specific Extensions (9000_90FF)

Attribute	Type	Value	Description
IP_Input_Filter	x9000		The various filter attributes (0x9000 to 0x9005) are all 'string' types. They provide a means to specify filters on the RADIUS server in the standard NETServer format (as described in the NETServer user's manual), on a per user basis.
IPX_Input_Filter	x9001		
IP_Output_Filter	x9003		
IPX_Output_Filter	x9004		
SAP_Output_Filter	x9005		
Tunnel_Name	x9007		Identifies a common set of attributes. Used primarily for the user interface.
Tunnel_Authenticator	x900B		This attribute is used for CCA Phase 2 users. It is of string type and contains the Session Key encrypted with the secret shared between the Frame Relay Gateway and the RADIUS server.
Packet_Index	x900C		This attribute is an Integer type. It is used as an index in the Resource Query messages. A non-zero value indicates that more data is available.
Cutoff	x900D		OBSOLETE
Access_Accept_Packet	x900E		OBSOLETE
Secondary_DNS_Server	x9010		
Primary_NBNS_Server	x9011		
Secondary_NBNS_Server	x9012		
Syslog_Tap	x9013	0 = Off (default) 1 = Raw (log raw data) 2 = Framed (log data as SLIP/PPP frames)	<p>This attribute is sent by the NETServer.</p> <p>The difference between 1 and 2 is that with 1, there is no guarantee of how the bytes will be grouped together. As the NETServer receives them, they are logged. With 2, the bytes are logged as a single SLIP/PPP frame that is passed to the higher layer IP stack. It is possible to get garbage characters that are tossed by the PPP framer code, and those will not get logged for case 2.</p> <p>In authentication-accept: When this attribute is sent to the NAS with the value "1" (On), all data sent and received on that user's port will be syslogged to the loghost configured in the NAS. When the user exits the service (for example, by hanging up), the data stream for that port will no longer be syslogged. If the value is "0" (Off), or the attribute is not in the accept packet, the NAS will not log the data stream. Other packet types do not use this attribute. NETServer version 3.3 supports this feature.</p>

Attribute	Type	Value	Description
Message_Integrity_Check	x9014		Sent by the NETServer, this attribute ensures that the filter change request came from an authorized source and was not changed during transit.
Call_Tracking_ID	x9015		OBSOLETE
Log_Filter_Packet	x9017		Sent by the NETServer, this attribute indicates if the filter packets should be logged to syslog for this user.
Chassis_Call_Slot	x9019	1-15	Identifies which slot the T1 or PRI card resides.
Chassis_Call_Span	x901A	0 or 1	Identifies the T1 or ISDN-PRI span line the call is carried on.
Chassis_Call_Channel	x901B	T1 = 0-23 PRI = 0-29	Identifies the DS0 or B-channel that the value is carried on.
Keypress_Timeout	x901C		Indicates the number of seconds to wait for a response from the user when a request is displayed.
Unauthenticated_Time	x901D		Indicates the number of seconds between the time of connection and the time of successful authentication.
VPN_Encrypter	x901E		Attribute used by the RADIUS server to encrypt the session key and by the NAS to decrypt the key.
Acct_VPN_Gateway	x901F		Identifies the location ID and the Gateway IP address to the accounting server. The information is gathered from the VPN Gateway attribute.
Re_CHAP_Timeout	x9020		Indicates the number of seconds between periodic CHAP challenges.
Local_Framed_IP_Address	x9026		Identifies the IP address of the local end of the dial-up PPP link.
Speed_of_Connection	x9801	0 = Auto (Default) 1 = 56 2 = 64 3 = Voice	Indicates the speed of the connection for framed users. The default is Auto.
Max_Channels	x9802	1 2 (Default)	Indicates the maximum number of channels that can be used for a LAN-to-LAN connection. Specifying one (1) disables multilink PPP.
Channel_Expansion	x9803	1-100 75 (Default)	Specifies the percentage for a channel expansion for a LAN-to-LAN connection. When usage of the first channel exceeds this percentage, PPP will add a second channel.
Channel_Decrement	x9804	1-100 25 (Default)	Specifies the percentage for a channel reduction for a LAN-to-LAN connection. When usage of the second channel drops below this percentage, PPP will drop the second channel.
Expansion_Algorithm	x9805	1 = Constant (Default) 2 = Linear	Specifies the expansion algorithm used to decompress incoming PPP data.

Attribute	Type	Value	Description
Compression_Algorithm	x9806	0=Stac 1=Ascend 2=MS (default) 3=Auto	Specifies the packet compression used to compress PPP data.
Receive_Acc_Map	x9807	UINT32	Specifies whether the NAS uses the asynchronous control character map to filter incoming data. 0xFFFFFFFF is default.
Transmit_Acc_Map	x9808	UINT32	Specifies whether the NAS uses the asynchronous control character map to filter outgoing data. 0xFFFFFFFF is default.
Where_Compression	x9809	1=Bundle 2=Links	Sent by the NETServer, this attribute indicates where the compression should be handled. The default is Bundle.
Compression_Reset_mode	x980a	0=Auto (Default) 1=Reset every packet 2=Reset on error	Indicates when to reset the dictionary.
Min_Compression_Size	x980b	128 - 1514 256 (Default)	Indicates the minimum packet compression size in Kb allowed.
IP	x980c	1 = enabled (Default) 2 = disabled	Indicates whether IP is enabled for the user.
IPX	x980d	1 = enabled (Default) 2 = disabled	Indicates whether IPX is enabled for the user.
Filter_Zones	x980e	1 = enabled (Default) 2 = disabled	Indicates whether ARAP filter zones are enabled for the user.
Appletalk	x980f	1 = enabled (Default) 2 = disabled	Indicates whether Appletalk is enabled for the user.
Bridging	x9810	1 = enabled (Default) 2 = disabled	Indicates whether Bridging is enabled for the user.
Spoofing	x9811	1 = enabled (Default) 2 = disabled	Indicates whether protocol Spoofing is enabled for the user.
Send_Password	x9814		Indicates the password to be sent when logging into a remote location. Required for two-way LAN-to-LAN connection.
Start_Time	x9815		Indicates the time a timed location user should start each day.

Attribute	Type	Value	Description
End_Time	x9816		Indicates the time a timed location user should stop each day.
Send_Script1	x9817		This attribute is a send-reply dial out script.
Reply_Script1	x9818		This attribute is a send-reply dial out script.
Send_Script2	x9819		This attribute is a send-reply dial out script.
Reply_Script2	x981a		This attribute is a send-reply dial out script.
Send_Script3	x981b		This attribute is a send-reply dial out script.
Reply_Script3	x981c		This attribute is a send-reply dial out script.
Send_Script4	x981d		This attribute is a send-reply dial out script.
Reply_Script4	x981e		This attribute is a send-reply dial out script.
Send_Script5	x981f		This attribute is a send-reply dial out script.
Reply_Script5	x9820		This attribute is a send-reply dial out script.
Send_Script6	x9821		This attribute is a send-reply dial out script.
Reply_Script6	x9822		This attribute is a send-reply dial out script.
Terminal_Type	x9823	vt100 (Default)	Indicates the terminal type the user is using.
Apple_Network_range	x9824		Indicates the appletalk network range defined for the outbound user.
Local_IP_Address	x9825	0.0.0.0 (Default)	This attribute is used for dedicated circuits and indicates the local IP address for the user.
Routing_Protocol	x9826	1 = Rip1 (Default) 2 = Rip2	This attribute indicates which routing protocol is being used.
Modem_Group	x9827	all slot:1 slot:2 etc.	Indicates the modem group configured for the user.
IPX_Routing	x9828	0 = none (Default) 1 = send 2 = listen 3 = respond 4 = all	Indicates the routing procedure for IPX to take.
IPX_Wan	x9829	1 = enabled (Default) 2 = disabled	This attribute indicates whether IPX WAN is enabled.

Attribute	Type	Value	Description
IP_RIP_Policies	x982a	1 = SendDefault 2 = SendRoutes 4 = SendSubnets 8 = AcceptDefault 0x10 = SplitHorizon 0x21 = PoisonReverse 0x40 = FlashUpdate 0x80 = SimpleAuth 0x100 = V1Send 0x200 = V1Receive 0x400 = V2Receive 0x800000 = Silent	Indicates the rip policy flags for a connection. This attribute need only be specified if the user needs to deviate from the defaults set by the FRAMED_ROUTING attribute.
IP_RIP_Simple_Auth_Password	x982b		This attribute contains the string value of the simple authentication password used when the simple authentication bit is set in the IP RIP policy flags.
IP_Input_Filter	x9000		The various filter attributes (0x9000 to 0x9005) are all 'string' types. They provide a means to specify filters on the RADIUS server in the standard NETServer format (as described in the NETServer user's manual), on a per user basis.
IPX_Input_Filter	x9001		
IP_Output_Filter	x9003		

3Com Vendor Specific Extensions (other)

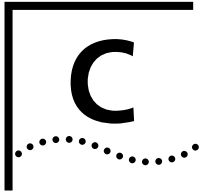
The following accounting attributes are sent by the NMC:

Attribute	Type	Value	Description
Event_Id	xBFBE		This attribute indicates a unique value for each type of event (based on the number of the event as defined in chs_traps.mib plus 5)
Event_Date_Time	xBF2F		This attribute indicates the value of nmcGmtime at the point when the NMC processed the event
Chassis_Slot	xBF39		This attribute indicates the slot number associated with this event
Channel	xBF38		This attribute indicates The channel number associated with this event
Call_Start_Date_Time	xBFF7		This attribute indicates the value of nmcGmtime at the point when the call start event occurred
Call_End_Date_Time	xBFF6		This attribute indicates the value of nmcGmtime at the point when the call end event occurred
Connect_Term_Reason	x009B		
Failure_to_Connect_Reason	x0069		
Last_Number_Dialed_Out	x0066		
Last_Number_Dialed_In_DNIS	x00E8		
Last_Callers_Number_ANI	x00E9		
Characters_Sent	x0071		
Characters_Received	x0072		
Blocks_Sent	x0075		
Blocks_Received	x0076		
Blocks_Resent	x0077		
Line_Reversals	x007A		
Number_Of_Characters_Lost	x007B		
Initial_Rx_Link_Data_Rate	xBF2D		
Final_Rx_Link_Data_Rate	xBF2C		
Initial_Tx_Link_Data_Rate	x006A		

Final_Tx_Link_Data_Rate	x006B
Retrains_Requested	x0078
Retrains_Granted	x0079
Number_of_Blers	x007D
Number_of_Link_Timeouts	x007E
Number_of_Fallbacks	x007F
Number_of_Upshifts	x0080
Number_of_Link_NAKs	x0081
Default_DTE_Data_Rate	x005E
Sync_Async_Mode	x0067
Originate_Answer_Mode	x0068
Modulation_Type	x006C
Equalization_Type	x006F
Fallback_Enabled	x0070
Back_Channel_Data_Rate	x007C
Simplified_MNP_Levels	x0099
Simplified_V42bis_Usage	x00C7

3Com Vendor Specific Extensions used in non-call termination events

Attribute	Type	Value	Description
Chassis_Temperature	xBF31		
Chassis_Temp_Threshold	xBE84		
Actual_Voltage	xBF32		
Expected_Voltage	xBF33		
Power_Supply_Number	xBF34		
Card_Type	xBE85		
Connect_Time_Limit	xBFE7		
Number_of_Rings_Limit	xBFE6		
DTE_Data_Idle_Timeout	x0048		
DTR_False_Timeout	x00BE		
Fallback_Limit	x00BF		
Block_Error_Count_Limit	x00C0		
DTR_True_Timeout	x00DA		
Security_Login_Limit	xBEDE		
Security_Resp_Limit	xBEFA		
DTE_Ring_No_Answer_Limit	xBF17		



SCRIPT LANGUAGE

Script Language Syntax and Rules

This section

Script Language Syntax

- Bracketed items [] are considered optional.
- An ellipse (...) indicates that more than one occurrence may be used.
- Items in boldface are required syntax or keywords
- Language elements that are obvious are not defined; for example, <alphanumeric string>.

General Syntax Rules

- A script file can contain comment lines starting with the pound sign (#) or a semicolon (;). All characters following the pound sign or semicolon are ignored.
- Maximum length of each line in the script file is 255 characters.
- Statements can continue onto another line by placing a backslash (\) at the end of the line. Make sure the backslash is not part of a commented line or the backslash will be ignored.
- Only one statement or label is permitted on a single line.
- The script language is not case-sensitive.

Script Variables and Lists

The script language permits named variables. Variable names may be any alphanumeric character including dashes (-) and underscores (_). Maximum length is 32. Variables contain a string or numeric values. The values of string variables must be enclosed in quotes. For example:

```
ThisVariable = 20  
OtherVariable = "Twenty"
```

Variable lists are set of variables, or other lists, collected together. List name and variable member are separated by a period (.) using the following format:

```
list-name.variable-name
```

For example:

```
MyList.Access.Denied.Disconnect.Reply = "Disconnecting Now"
MyList.Message = "Hello"
```

There is no limit on the depth of a list. Variables within a list are ordered alphabetically.

Predefined Variables Lists

DICTIONARY

This predefined list is loaded during the Security Server's initialization. It contains all attributes and associated values that are read from the dictionary(ies). For example:

```
DICTIONARY.Framed-Protocol.PPP=1
DICTIONARY.Framed-Protocol.SLIP=2
```

The exact nature of this dictionary will vary depending upon the contents of the dictionary(ies).

SYSTEM

This predefined list is created from the SYSTEM section of the Security Server Configuration File during initialization. It contains all the parameters and associated values contained in that file. For example:

```
SYSTEM.ACE$Challenge-Support=1
SYSTEM.ACE$Server-Timeout=45
```

DICTIONARIES

This predefined list contains the variables associated with each parameter specified in the DICTIONARIES section of the Security Server Configuration file.

SERVER

This predefined list contains the variables associated with each parameter specified in the SERVER section of the Security Server Configuration file. For example:

```
SERVER.Accounting.ip = "192.77.123.156"
```

```
SERVER.Accounting.port = 1646
```

TABLES

This predefined list contains the variables associated with each parameter specified in the TABLES section of the Security Server Configuration file. For example:

```
TABLES.USERS = "users.txt"
TABLES.CLIENTS = "clients.txt"
```

REQUEST

This predefined list contains the variables associated with each field in the current RADIUS request packet. For example:

Variable	Description
Request.Request-Type	Numeric value of the request type.
Request.Identifier	Numeric value of the identifier.
Request.Authenticator	String of 16 characters.
Request.IP	String IP address of the requesting client.
Request.Port	Numeric port of the requesting client.

Additional variables are added to the REQUEST list based on the attributes found in the request packet. The variable names are constructed from the associated attribute contained in the dictionary file.

Referencing Attributes

When the dictionaries are first read during the start up, a DICTIONARY variable list is created for each entry using the following format:

```
DICTIONARY.attribute-name[.textual-value=numeric-value]
```

textual-value and numeric-value are based on the VALUE entries in the dictionary, and may not be present for all attributes. For example, Framed-Protocol might look something like this:

```
DICTIONARY.Framed-Protocol.PPP=1
DICTIONARY.Framed-Protocol.SLIP=2
```

Referencing Records

The authorization script can read or update an field associated with a particular record match in a data file. Use the following syntax:

```
table-name[key-value].field-name
```


table-name refers to the file (Clients, Users, and so on) containing the key-value. The key-value is the record that the script searches for in the table-name. The script then reads or updates the field-name.

Referencing File Parameters

Configuration parameters (RADSERV.CFG) can also be referenced from the authorization script:

```
section-name.parameter
```

section-name would be, for example, SYSTEM. parameter could be any one of the SYSTEM parameters; for example, BlackList.

Script Execution

The authorization script is executed at startup and for each new RADIUS packet received by the server. Note, however, that script execution begins at the label associated with the event.

For example:

Event	Execution Label
At server startup time	StartUp:
At server shutdown time	ShutDown:
Receive Access-Request (1) packet	Access-Request:
Receive Access-Accept (s) packet	Access-Accept:
Receive unknown packet	UnknownPacket:

If the execution label is not found in the script, an error is reported in the log file.

Labeled Sections

Option	Description
<label>: <statement>	<label> names a section of code. It can appear on anywhere in the script, but must appear on a line by itself. An implied RETURN statement is at the end of the labeled section.

Variable References and Assignment Statements

References	Assignments
<variable> = <expression>	Normal assignment statements.
<list-name>.<variable>=<expression> <table-name>[<key-expression>]. <field-name> = <expression>	Variables and variable lists are declared when first assigned a value.
<expression> :=	Expressions that evaluate to a string or numeric value.
<numeric-literal>	Numeric literals are whole numbers.
" <string-literal> "	Strings must be surrounded by double quotation marks.
<variable>	Returns the current value of the <variable> specified.
@<variable>	Indirection operator. Returns the current value of the variable whose name is <variable>.
<list-name>.<variable>	Return the current value of the <variable> in the <list-name>.
<table-name>[<key-expression>]. <field-name>	Returns the value of the specified <field-name> associated with the record matching the <key-expression> in the specified <table-name>. The <table-name> must be defined in the [TABLES] section of the Server Configuration file. The <field-name> must be from the set of fields specified in the <table-name>.
<function-call>	Return the value of the built in function.
<expression> < + - * / > <expression>	Simple integer computations. Complex multi-operator expressions are not supported. The operators must be surrounded by spaces. String variables can be concatenated using the + operator.

Control Statements

Option	Description
CALL <label>	A subroutine call to a label. Control is returned when a RETURN statement is executed.
RETURN	Return from a subroutine call. If RETURN is not in the subroutine, the script stops executing, and the server awaits another request to process.

Option	Description
BREAK	Breaks out of a FOR loop, CASE section, or WHILE loop.
EXIT	Immediately stops execution of a script. This is normally executed after a RESPOND statement. Note that this does not force the server to exit.
IF (<boolean>) <statement>... ENDIF	
WHILE (<boolean>) <statement>... ENDWHILE	Executes the block of statements as long as <boolean> is TRUE. The <boolean> is evaluated at the start of the block.
<boolean> =	All boolean expressions evaluate to TRUE or FALSE.
<expression> [!]InTable <table-name>	Tests if the value of the expression can be found as a key in the specified table. Use ! for not in the table.
<variable> [!]InList <list-name>	Tests to see if the <variable> is contained in the variable list. Use ! for not in the table.
<expression><rel-op> <expression>	Simple relational test.
<relational-operator>{ ==, !=, >, >=, <, <= }	Used to compare either numeric or string expressions. <ul style="list-style-type: none"> ■ == equal to ■ != not equal to ■ > greater than ■ >= greater than or equal to ■ < less than ■ <= less than or equal to
SWITCH (<expression>) CASE <literal-value>: [CASE DEFAULT: <statement>...] ENDSWITCH	Switch blocks. The <expression> is evaluated at run time, and then execution is transferred to the CASE section of which the <literal-value> is equal to the <expression>. If no match is found, the CASE DEFAULT section is executed, if present. A BREAK is implied at the end of each CASE section, so you cannot "fall through" to the next CASE section.

Option	Description
FOREACH (<variable> IN <list-name> ENDFOR	Iterates across a list of variable, assigning the specific variable-name to <variable>. To reference the actual value, use the @<variable> indirection operator.
RESPOND (<request-type>, <string-secret-expression>, [,<list-name>])	<p>RESPOND sends a response packet to the client that originally sent the current request. <request-type> is typically passed using a reference to the <code>DICTIONARY.Request-Type.<name></code></p> <p><string-secret-expression> must be appropriate for the client receiving the response.</p> <p>All variables in the <list-name> with a matching entry in the RADIUS dictionary will be sent with the packet.</p> <p>NOTE: The RADIUS " Authenticator" is adjusted to reflect a response packet using the secret and MD5 encryption.</p>
SEND (<server-ip-string>, <server-port-num>, <request-type-num> <request-id-num> <authentication-string>, <list-name>)	<p>Sends a RADIUS packet to the specified server using parameters and attributes listed in the argument. It is also used if further authentication is required by another RADIUS server.</p> <p>All variables in the <list-name> with a matching entry in the RADIUS dictionary will be sent with the packet. Any "Password" attribute must be encrypted with the <code>MD5\$()</code> function before issuing a SEND command.</p> <p>NOTE: This function causes an <code>Access-{type}</code> packet to be returned to the server asynchronously. This will execute the <code>Access-{type}: labled</code> section.</p>
EXEC (<string-expression>)	Pass the <string-expression> to the native operation system so that it is executed. For example, <code>EXEC(" USBEEP !!!Security Breach!!!")</code>
EMPTY (<list-name>)	Empties the variable list.
REMOVE (<variable> [,<list-name>])	Removes the specified <variable> from the variable from the variable list. If the variable list is not specified, the variable will be removed from the global list.
DISPLAY (<string-expression>)	Displays a <string-expression> in a display window on a screen or logs it to a file.

Option	Description
StartTimer (<id> <milliseconds>)	This does not interrupt any currently processing command. It starts a timer of <milliseconds> duration with <id>. When the timer fires, the section of code labeled TIMER-<id> is executed. Timers continue to fire until they are explicitly stopped. The Id must be a numeric value.
StopTimer (<id>)	Stops the timer with <id>.
DEBUG (SET, [No]Trace)	Turns execution track On (SET,Trace) or Off (SET,NoTrace).
DEBUG (SHOW, {Variables Compiled Script})	Dumps the indicated internal structure to the log file or displays it on a screen.

Built-in Functions

Option	Description
SD\$CHALRESPONSE	Handle the response to a challenge for an ACE user. Returns an ACE specific value. The code value is the ACE code returned from the initial SD\$CHECK call.
ISASCII	Returns 1 if the string is all ASCII characters
REPLACES	Returns the <string> with each "search" character replaced with the "replace" character. The search and replace character must be surrounded with double quote marks and cannot be the same.
SW\$AUTH	Authenticate a SafeWord AS user. Returns a string with the first ASCII character being 1 (Accept), 2 (Reject), or 3 (Challenge). The text that follows is text, if any, is a tab followed by the challenge text to present to the client as the next prompt.
SW\$CHALRESPONSE	Handle the response to a challenge for an SafeWord user. Returns exactly as SW\$AUTH returns.
SELECT	Returns '1' if the key was found in the indicated table, otherwise it returns '0'. If found, the list-name will contain a list of variables, each associated with a field-name in the table.
INSERT	Returns '1' if the row was successfully inserted into the indicated table. Field values are stored based on matching the variable names in the list with the actual field names in the table.

Option	Description
LCL\$AUTH	Authenticates the user against the local system. On NT, a domain name may be passed, or NULL. Returns -1 on error, 0 on failure to authenticate, or 1 on successful authentication.
DP\$AUTH	Authenticate a Digital Pathways Defender user. Returns a string with the first ASCII character being 1 (Accept), 2 (Reject), or 3 (Challenge). The text that follows is text, if any, is a tab followed by the challenge text to present to the client as the next prompt.
DP\$CHALRESPONSE	Handle the response to a challenge for an Defender user. Returns exactly as DP\$AUTH returns.
GETHOSTBYNAME	Call to resolve a host name to an IP address. Uses the local system resolver. Subsequent calls to GETNEXTHOST will return the next name found. No more entries than <max_num> will be returned.
TOUPPER	Converts the passed string to upper case
VALIDATEPHONENO	Validates a phone number against the passed in call restriction list. The call restriction list is a semicolon separated list of numbers, with wildcards allowed. Returns 1 if the phone number is allowed.
GETSERVBYNAME	Looks up a service name, using the service type (e.g., TCP or UDP), and returns the value found in a SERVICES file.
ENCRYPT\$ (<string-expression>)	Returns a string. This encrypts a string expression using an internal algorithm (not MD5).
DECRYPT\$ (<string-expression>)	Returns a string. This decrypts a string expression using an internal algorithm (not MD5).
MD5\$ (<string-authenticator-expression>, <string-secret-expression>, <string-password-expression>)	Returns a string associated with applying the MD5 encryption algorithm to the password string. If the string is already encrypted, this variable returns clear-text; otherwise it encrypts the password.

Option	Description
MD5CHAP (<string-challenge>, <string-Chap-Password-expression>, <string-password-expression>)	Returns a numeric. This returns a 1 if the CHAP response matches the CHAP challenge, and returns a 0 otherwise. The Chap-Password typically contains the 1-character Chap-Id followed by the 16-octet response. The 16 octet response is typically the Request.Authenticator attribute. The password must be clear text.
LENGTH (<string-expression>)	Returns the number of characters in a string-expression.
FORMAT\$ (<format-string-expression> [, <variable> . . .])	Returns a string based on the <format-string-expression> and the values of all variables listed. The <format-string-expression> is identical to that used in the C sprintf function. String substitution must use %s, while all numeric values must use %ld (long signed integers).
NUM (<string-expression>)	Returns a numeric value of the string expression.
STR\$ (<numeric-expression>)	Returns a string value of the numeric expression.
INSTR (<string>, <search-string>)	Searches <string> for <search-string> and returns a 0 if the <search-string> is not found. Otherwise it returns the position of the first letter of the <string> in the <search-string>.
MID\$ (<string>, <start> [, <size>])	Returns a substring of <string> starting in the position specified by <start>. The size of the substring is determined by <size>.
DATE (<date-string>)	Returns the number of seconds since midnight January 1, 1970. The <date-string> must be in format mm/dd/yyyy [hh[:mm[:ss]]].
DATE\$ (<date-number>)	Returns the date in the form of mm/dd/yyyy hh:mm:ss based on seconds since midnight January 1, 1970.
NOW ()	Returns the number of seconds since midnight January 1, 1970.
ASK\$ (<prompt-string>)	This function interactively prompts with the <prompt-string>, and returns the value entered as a string expression. In Windows, a dialog box is used. In UNIX, stdin is used.

ACE/Server Functions

Option	Description
SD\$CHECK (<user-name-string>, <passcode-string>)	<p>Request that the <user-name-string> and <passcode-string> be checked for authorization.</p> <p>After a call to SD\$CHECK, the following new variables are available to the script:</p> <ul style="list-style-type: none"> ■ ACE\$SD.MIN_PIN_LEN: The minimum number of characters in a PIN. ■ ACE\$SD.MAX_PIN_LEN: The maximum number of characters in a PIN. ■ ACE\$SD.USER_SELECTABLE: If set to 0, the ACE Server generates the PIN. If set to 1, the user may set the PIN. ■ ACE\$SD.ALPHANUMERIC: If set to 0, the PIN must be numeric. If set to 1, an alphanumeric PIN is acceptable. ■ ACE\$SD.SYSTEM_PIN: The ACE Server generated PIN if ACE\$SD.SELECTABLE is set to 0. <p>When the authorization check is finished, SD\$CHECK returns one of the following numeric values:</p> <ul style="list-style-type: none"> ■ ACM-OK ■ ACM_ACCESS_DENIED ■ ACME_NEXT_CODE_REQUIRED ■ ACM_NEW_PIN_REQUIRED <p>If the messages ACM_NO_CONFIG_FILE or ACM_NO_UDP_PORT are returned, the system does not have access to an ACE Server.</p>
SD\$NEXT (<user-name-string>, <passcode-string>)	<p>This function is issued in response to a ACM_NEXT_CODE_REQUIRED message. It is used to check the next passcode/password entered by the user.</p> <p>Returns either ACM_NEXT_CODE_OK (user is authorized) or ACM_NEXT_CODE_BAD (no authorization).</p> <p>The messages ACM_NO_SESSION is returned if there was no previous call to SD\$CHECK with the same user name.</p>
SD\$PIN (<user-name-string>, <pin-string>)	<p>This function is issued in response to a ACM_NEW_PIN_REQUIRED message to reset the PIN.</p> <p>Returns either ACM_NEW_PIN_ACCEPTED or ACM_NEW_PIN_REJECTED.</p> <p>The messages ACM_NO_SESSION is returned if there was no previous call to SD\$CHECK with the same user name.</p>



INDEX

A

Accounting Features	
Advanced UNIX	3-6
ACE/Server	
Proxying to	3-14
Troubleshooting	3-15
adding new users	2-1
Advanced UNIX Accounting Features	3-6
Allowing Users to Change Passwords	2-6
ANI Checking	2-8
Assigning a Password	2-6
Assigning the Default User	2-3
Authentication Process	2-2

B

Basing a User On a Template	2-4
Blacklist Threshold	3-9
Blacklisting	3-9

C

Call Statistics	
Logging	3-1
Calls table	3-3
CHAP	3-10
Clients table	1-5
clients.txt	3-8
Concurrent Logins	2-10
Configuring the Server	2-10
Configuring the Users	2-10
Troubleshooting	2-10
Configuring Accounting	3-1
Configuring Users	2-1
Creating a template	2-4
Customizing Call Logging	3-3
Customizing Your Database	3-8

D

Database Information	3-7
Database Organization and Components	1-5
Default User	2-2
Assigning the	2-3
Defender Security Server, Proxying to	3-16

Deleting Users	2-2
Deny Access	2-3
Dial Restriction Strings	2-8
Dial-in Restrictions	2-7
ANI Checking	2-8
DNIS Checking	2-7
Entering the Numbers To Be Validated	2-7
Port Number Checking	2-7
Turning On	2-7
Dictnary.dat	1-3, 3-3
DNIS Checking	2-7
Domains table	1-5
domains.txt	1-5, 3-8

E

EAP RADIUS Server, Proxying to	3-19
Eaproxies table	1-5
eaproxies.txt	1-5
Entering the Numbers To Be Validated	2-7
Events table	3-3
Exporting Data	3-8

F

flat file database	
issues	3-7
flat file fatabase	3-7
Forwarding Accounting Messages	3-4

G

General Overview	1-1
------------------------	-----

H

HP-UX® requirements	1-2
---------------------------	-----

I

Importing and exporting data	3-8
iPass Corporate Access	3-21
Authentication Process	3-21
Installation at the Corporate Site	3-22
Installation at the ISP Site	3-22
Remote Login Requirements	3-22

Restrictions and Limitations 3-21

L

L2TP 4-1, 4-2
 Logging Call Statistics 3-1

M

Modem Configuration 3-1

N

new features
 ability to proxy RADIUS accounting 1-3
 additional NAS support 1-3
 EAP support 1-3
 iPass support 1-3
 multi-link support with 3rd-party tokens 1-3
 VPN support 1-3
 New Features in this Release 1-3
 NEWPASS 3-9
 NMC Configuration 3-2
 NMC Log Groups 3-2

O

Omniguard/Defender, Proxying to 3-16
 Oracle 1-2, 3-8

P

Passwords 2-6
 Allowing Users to Change 2-6
 Assigning 2-6
 Change Keyword 3-9
 Default Age 3-9
 Expiration Warning 3-9
 Minimum Length 3-9
 prompting for change on expiration 3-9
 Setting an Expiration Date 2-6
 settings 3-9
 Port Number Checking 2-7
 Portgroups table 1-5
 portgroups.txt 1-5, 3-8
 Postgresql or Oracle Databases 3-8
 PPTP 4-1
 Proxying 3-10, 3-11
 Accounting Information to TACACS+ 3-11
 User Authentication to ACE/Server 3-15
 User Authentication to an EAP Server 3-19
 User Authentication to S/KEY 3-20
 User Authentication to SafeWord 3-17
 User Authentication to TACACS+ 3-11

R

RADIUS 1-1
 RADIUS, Proxying to 3-13
 Radserv.scp 1-3
 restricting database field length 3-8
 Restrictions, Dial-in 2-7

S

S/KEY, Proxying to 3-20
 SafeWord
 setting the path to sid.cfg 3-17
 Troubleshooting 3-18
 troubleshooting 3-18
 SafeWord, Proxying to 3-17
 saserver 1-5
 saUtil 3-8
 Script options and functions 1-6
 sdconf.rec 3-14
 copying 3-14
 SecureID 3-14
 SecureNet Key 3-16
 Security and Accounting Components 1-3
 Security and Accounting Server
 options when starting 1-6
 starting the server 1-5
 stopping the server 1-5
 Setting Event Logging 3-5
 sid.cfg 3-17
 SNK 3-16
 Solaris requirements 1-2
 starting the server 1-5
 options 1-6
 stopping the server 1-5
 System Requirements 1-2
 System table 1-5
 system.txt 1-5

T

TACACS+ 3-10
 Command Usage 3-11
 TACACS+, Proxying to 3-10
 Templates 2-4
 Basing a User on a 2-4
 Creating 2-4
 tunnel
 attributes 4-10
 initiation 4-3
 standards 4-1
 Tunneling Using L2TP 4-2
 Tunnels table 1-5
 tunnels.txt 1-5

U

User Authentication Process	2-2
User Templates	2-4
Users	1-5
Adding	2-1
Configuring	2-1
Deleting	2-2
Users table	1-5

V

Virtual Private Networks	4-1
VPN	1-3, 4-1
Benefits	4-1
DNIS/ANI Based	4-7
Domain Based	4-4
Overview	4-1
Tunnel Attributes	4-10
Tunnel Standards	4-1
Username Based	4-9
Using L2TP	4-2



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. 1.024.1677-02