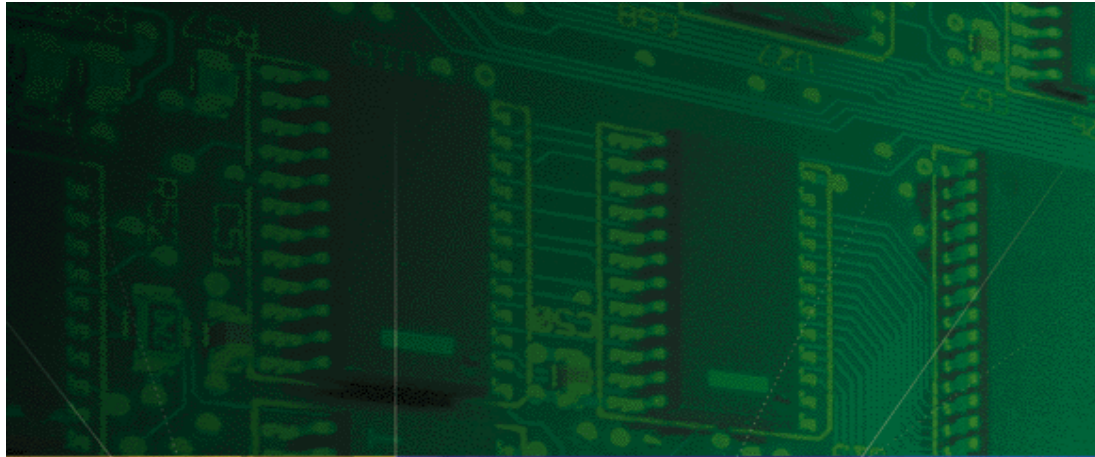




Security and Accounting Server for UNIX

Getting Started Guide



Part No. 1.024.1079-04
Version Number 6.0



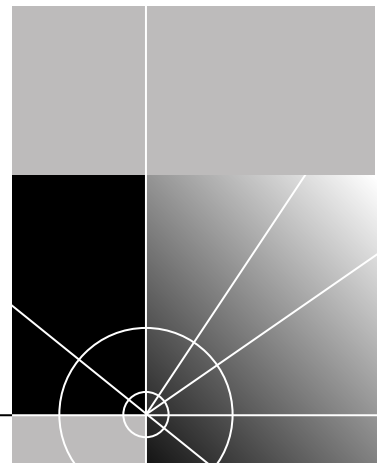
Security and Accounting Server for UNIX

Getting Started Guide

Version 6.0

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

Part No. 1.024.1079-04



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	1
Conventions.....	2
Related Documentation	3
Contact information	3

1 OVERVIEW

Network Interaction	1-1
Security Functions	1-2
Security Features	1-3
Password Management.....	1-3
Proxy Authentication.....	1-3
Local System Password Authentication	1-4
Roaming dialback in NETServer	1-4
Dialback Security.....	1-4
Blacklisting.....	1-4
User Templates.....	1-4
Flexible Database Integration	1-4
Call Restriction	1-4
Accounting Functions.....	1-4
Accounting Features.....	1-5
Flexible Accounting	1-5
Database Table Maintenance.....	1-6
Radius extensions.....	1-6
Accounting secret	1-6
New Features in This Release	1-6
VPN Support	1-6
EAP Support	1-6
Additional Network Access Server Support.....	1-6
Support for Multi-Link with Third-Party Tokens	1-6

Ability to Proxy RADIUS Accounting Records.....	1-6
Crypt format password field	1-6

2 INSTALLATION

System Requirements.....	2-2
For HP-UX	2-2
For Sun Solaris.....	2-2
System Dependencies	2-2
For HP-UX	2-2
For Sun Solaris.....	2-3
Installing Security and Accounting Server	2-3
Accessing the Distribution Files	2-3
For HP-UX 10.20 (from CD-ROM)	2-3
For Sun Solaris with the volume manager (vold) running (from CD-ROM):	2-4
For Sun Solaris without the volume manager (vold) running (from CD-ROM):	2-4
For either HP-UX or Sun Solaris (from a compressed TAR file):	2-4
Running the Install Script	2-5
Setting Up \$SAHOME	2-6
For the Bourne shell:	2-6
For the C shell:	2-6
Uninstalling Security and Accounting Server.....	2-6

3 INITIAL CONFIGURATION

Database Installation and Configuration.....	3-1
Installing and Configuring Postgresql	3-2
Creating the Postgres User.....	3-2
Installing Postgres.....	3-2
Configuring the Login Environment	3-2
Initialize the Data Directory	3-3
Test the Installation.....	3-3
Load the Default Data.....	3-4
Uninstalling the Postgresql Database.....	3-4
Configuring an Oracle database.....	3-5
Database Configuration	3-7
Installing the Oracle JDBC driver	3-7

Starting the Database Manager	3-7
Client Configuration.....	3-8
Configuring the Security Server	3-8
Configuring the Accounting Server	3-9
Example configuration	3-10
Setting up a User.....	3-11

4 TESTING THE INSTALLATION

Testing the Installation	4-1
Troubleshooting	4-2

INDEX

ABOUT THIS GUIDE

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

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

This guide is intended for network administrators with some training or experience working with Total Control equipment. It assumes 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

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

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

Conventions

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

Table 1 Notice Icons



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

Table 2 Text Conventions

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

- Total Control™ Security and Accounting Server for UNIX Software Reference

This HTML document, provided on the Security and Accounting Server CD-ROM, includes detailed information about configuring the Server and your database.

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

This Help system describes how to use Security and Accounting Server. It also contains context sensitive help for all the system parameters.

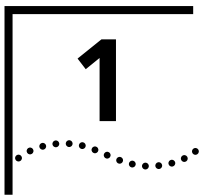
Contact information

Call the appropriate number listed below for technical support.

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

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





OVERVIEW

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

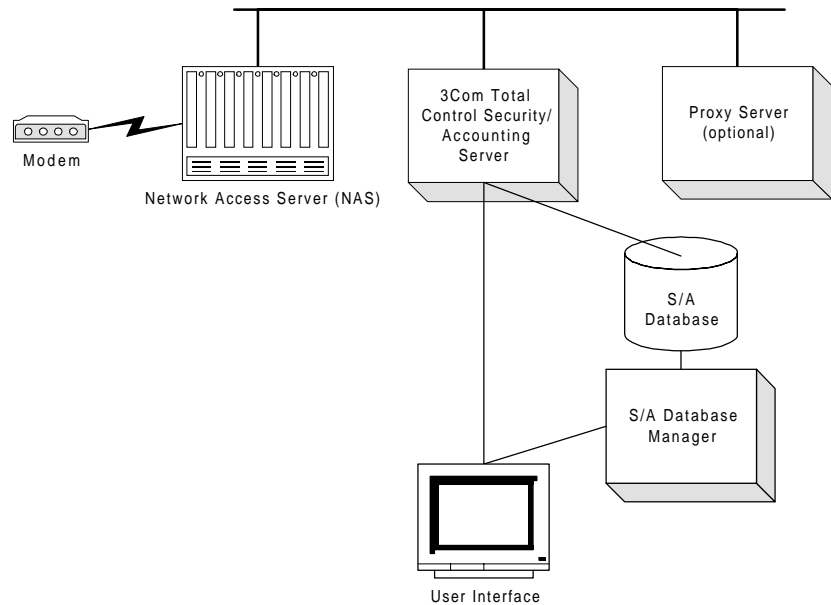
- describes Security and Accounting Server's operation in a client/server environment.
- describes the Server's security and accounting functions.
- introduces the Security and Accounting Database Manager

Network Interaction

Security and Accounting Server is a script-driven program that runs on a UNIX workstation. It interacts with a Network Access Server (NAS) using the industry standard Remote Authentication Dial-In User Service (RADIUS) protocol. The NAS is the hardware that manages incoming and outgoing calls to the modems in a remote access concentrator. Several 3Com products can serve as a NAS:

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

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



The server accesses information in a database to authorize users, and also uses the database to log information about each call.

When a client receives a call, you can forward authentication, authorization, and accounting information to Security and Accounting Server. You can also configure the Server to proxy authentication requests to a 3rd-party authentication server or a UNIX password file.

Security Functions

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

- 1 A user dials into a client.
- 2 The client prompts the user for a username and password.
- 3 The user enters the username and password.
- 4 The client sends information to Security and Accounting Server as an access-request message.
- 5 Security and Accounting Server decides whether to process the authentication request, or pass it on to a 3rd-party authentication server.

- 6 If Security and Accounting Server is set to authenticate the user, it runs the authentication script to process the authentication request. The authentication script confirms that:
 - the username and password are listed in the database.
 - the client's IP address and correct shared secret are in the database.
- 7 If authentication is approved, Security and Accounting Server sends an access-accept message, which includes any configuration information stored for that user, to the client.

Security Features Password Management

Security and Accounting Server offers the following password management features:

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

Proxy Authentication

Security and Accounting Server can pass authentication requests to these types of servers or systems:

- TACACS+
- Security Dynamics ACE/Server®
- AXENT Technologies Omniguard/Defender Security Server™
- Secure Computing SafeWord™ (formerly Enigma Logics)
- Bellcore S/KEY™
- EAP RADIUS Servers

Local System Password Authentication

For UNIX®, Security and Accounting Server can authenticate a user that is registered in the `etc/passwd` file.

Roaming dialback in NETServer

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

Dialback Security

Security and Accounting Server can instruct the NAS to dial back a specified phone number to ensure the request was made from that phone number.

Blacklisting

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

User Templates

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

Flexible Database Integration

Security and Accounting Server supports the following type of databases:

- flat text files
- Oracle RDMS
- Postgresql RDMS

Call Restriction

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

Accounting Functions

Security and Accounting Server allows you to capture and log statistics about usage, data transfer, performance, and operation mode. This information is logged in database tables or text files. Security and Accounting Server generates logs as follows:

- 1 A client sends accounting information to the server.
- 2 Security and Accounting server receives the information and stores it in the database or text file.

If the information is sent to the relational database (Postgresql or Oracle):

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

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

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

If the accounting information is sent to text files, it is stored in the following files named according by date:

- Call-related events from the NMC are written to the Call Termination log (YYYYMMDD.CON)
- Non-call-related events from the NMC are written to the Event log (YYYYMMDD.NMC)
- All other RADIUS events are written to the Native RADIUS Call log (YYYYMMDD.RAD)

Each record sent to Security and Accounting Server consists of a set of tabulates. Only those attributes for which there is an entry in OUTDEF.DAT are logged. If an attribute is sent that is not specified in OUTDEF.DAT, it is discarded.

Accounting Features

Security and Accounting supports the following accounting features:

Flexible Accounting

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

Database Table Maintenance

You can import and export database information.

Radius extensions

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

Accounting secret

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

**New Features in
This Release****VPN Support**

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

EAP Support

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

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 3Com NETBuilder II.

Support for Multi-Link with Third-Party Tokens

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

Ability to Proxy RADIUS Accounting Records

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

Crypt Format Password Field

User passwords now can be stored in UNIX crypt format.



2

INSTALLATION

This chapter is designed to help you install Security and Accounting Server for UNIX. The following are the steps you must complete to properly install the software. Each of these steps is discussed in more detail later in this chapter.

- 1** Confirm your system meets the system requirements and all dependencies are in place.
- 2** Install Security and Accounting Server
 - Access the Distribution files.
 - Run the Install Script.
 - Set up the Environment for Security and Accounting.

System 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 - 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

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.

System Dependencies

Install all of the recommended patches for your operating system before attempting to install Security and Accounting Server. System dependencies for each platform follow.

For HP-UX®:

The Security and Accounting Server Console provides a graphical interface for managing the server. This graphical interface requires the X11R5-SHLIBS fileset (a standard part of HP-UX 10.20). This fileset provides the shared libraries for Motif 1.2 and X11R5.

For Sun Solaris™:

The Security and Accounting Server Console provides a graphical interface for managing the server. This graphical interface requires the Motif 1.2.3 Runtime kit, which is a standard part of Solaris 2.4 and above. The Motif 1.2.3 Runtime kit is in the Solaris package *SUNWmfrun* and provides the Motif shared library file: *libXm.so.3*.

If this component was not installed with Solaris, you can load the Solaris 2.x CD-ROM and use the *swmtool* (Software Management Tool) to select the package and install it.

Installing Security and Accounting Server

Installing Security and Accounting Server involves these steps:

- Accessing the files (either from the CD-ROM or a tar file)
- Running the Install script
- Setting up the Environment for Security and Accounting

Accessing the Distribution Files

This section provides instructions to mount the CD-ROM or unpack the tar files. Read the appropriate section depending on your system (HP-UX or Solaris) and the media type (CD-ROM or compressed file).

For HP-UX 10.20 (from CD-ROM)

- 1 Insert the CD.
- 2 As the user root, create a directory to act as the mount point:

```
mkdir -p /SD_CDROM/sa
```



In this procedure, the /SD_CDROM/sa directory is the mount point. You can use any appropriate directory as the mount point.

- 3 Change the permissions of the mount point directory:

```
chmod 777 /SD_CDROM/sa
```

- 4 Mount the CD-ROM:

```
/sbin/mount /dev/dsk/c0tXd0 /SD_CDROM/sa
```

where **x** is the SCSI address for the CD-ROM drive.

- 5 Change to that directory:

```
cd /SD_CDROM/sa
```

For Sun Solaris with the volume manager (vold) running (from CD-ROM):

- 1 Insert the CD.
- 2 Wait for the CD to be mounted as /cdrom/cdrom0.
- 3 Mount the CD-ROM:

```
cd /cdrom/cdrom0
```

For Sun Solaris without the volume manager (vold) running (from CD-ROM):

- 1 Insert the CD.
- 2 Switch to user root. The # prompt appears.
- 3 Create a directory to act as the mount point:

```
mkdir -p /cdrom/sa
```

- 4 Mount the CD-ROM:

```
mount -F hsfs -r /dev/sr0 /cdrom/sa
cd /cdrom/sa
```

For either HP-UX or Sun Solaris (from a compressed TAR file)

If you received the Security and Accounting Server distribution as an electronic file, follow these steps to extract the compressed file.



*You will need to obtain GNU's **gzip** compression utility to decompress this file. This program is available for free on the Internet.*

- 1 Switch to user root. The # prompt appears.
- 2 Create a temporary directory on a partition with at least 25 MB available:

```
mkdir /temp/sa_inst1
```

- 3 Place the appropriate compressed tar file in the temporary directory.

- HP-UX: **saV060007hp.tgz**
- Solaris: **saV060007sol.tgz**

- 4 Change to the temporary directory:

```
cd /temp/sa_inst1
```

- 5 Extract the files:

- HP-UX: **gzip -dc saV060007hp.tgz | tar xvf -**
- Solaris: **gzip -dc saV060007sol.tgz | tar xvf -**

The following files are extracted:

File	Description
README.txt	
install.txt	installation instructions
Install.sa	installation and removal script
sainstall.cfg	Server installation configuration file
3COMDISK.ID	distribution version and part number
sasol.tar	Sun Solaris 2.x Security and Accounting Server tar file
sahpux10.tar	HP-UX 10.20 Security and Accounting Server tar file
Install.pg	Postgresql installation script
Remove.pg	Postgresql removal script
pgsqlsol.tar	Sun Solaris Postgresql tar file
pgsqlhp.tar	HP-UX Postgresql tar file
pgutils.tar	Postgresql Utilities tar file
jreXXX-solaris2-sparc.bin	Sun Solaris Java Runtime Environment.
jreXXX-os102.tar.z	HP Java Runtime Environment.

Running the Install Script

The installation script will provide you with instructions to guide you through the installation. To run the install script, follow these steps:

- 1 Switch to the super user.



If you do not run the installation script as the super user:

- *the Server is automatically installed as that user.*
- *the services file is not updated with the radius and raddacct entries*
- *the system boot-up files are not installed*
- *the installer is not given the option to make the Server executables setuid*

- 2 Change to the CD-ROM mount point (for CD-ROM) or the temporary directory (for TAR files).
- 3 Run the installation script:

./Install.sa

The default user id is sas. However, any user id can be used.

Setting Up \$SAHOME

After you install Security and Accounting Server, you must set up the SAHOME variable, as follows:

For the Bourne shell:

Edit the user startup file, `.profile`, and define the following variables:

```
SAHOME=/export/home/sas/sa60
export SAHOME
PATH=$PATH:$SAHOME/bin
export PATH
```

For the C shell:

Edit the user startup file, `.cshrc`, and define the following variables:

```
setenv SAHOME /export/home/sas/sa60
set path = ($path $SAHOME/bin)
```

Uninstalling Security and Accounting Server

This procedure guides you through the procedure to remove Security and Accounting Server. During the uninstall, the script prompts you to save configuration and log files for use by a new installation. To uninstall the Server:

- 1 Switch to the super user. If the Server install script was run by another user, log in as that user instead.
- 2 Change to the admin directory:

```
cd $SAHOME/admin
```
- 3 Run the Security and Accounting Server uninstall script:

```
./Install.sa -remove
```

3

INITIAL CONFIGURATION

This chapter provides you with information to:

- install and configure a database to work with Security and Accounting Server.
- configure the Server to perform user authentication and accounting.
- add a new user.

Database Installation and Configuration

Security and Accounting Server stores authentication and accounting information in a database. Security and Accounting can interact with a flat file format database or a relational database, such as Postgresql or Oracle.

A flat file database provides minimal features and requires no initial configuration. Relational databases allow more flexibility and expendability but require some configuration. When you install Security and Accounting Server, the flat files database the default database. If you plan to use a relational database, you must configure the database for use with Security and Accounting Server.

The following sections describe the installation and configuration procedures required for a Postgresql or Oracle database.

Installing and Configuring Postgresql

This release of Security and Accounting Server includes Version 6.2.1 of the Postgresql SQL engine. Postgresql is a UNIX public domain SQL engine. The Postgresql installation directory includes the Postgresql users guide and FAQ in the doc directory. For more information about Postgresql, see <http://www.postgresql.org>.

To install the Postgresql database you complete the following tasks:

- Create the user *postgres*
- Install the distribution files
- Configure the login environment for user postgres
- Initialize the data directory and create the database
- Test the database creation
- Install Security and Accounting Server default data.

Creating the Postgres User

Add a new user, *postgres*, to your system.

Install the home directory on a local disk in a partition with at least 20 MB of free disk space.

Installing Postgres

Follow these steps to install Postgres:

- 1 As user root, execute the Postgresql install script. The script changes the owner of the Postgresql files to user postgres.

```
cd installation_directory
./Install.pg
```
- 2 Follow the installation procedure to install the database distribution files. You may accept the default directory, */usr/local/pgsql*, or install to another directory.

Configuring the Login Environment

The data directory is the directory where all the database files will be stored. Normally, the database files are located in */postgres/data/*.

To specify which directory is the postgres directory:

- 1 Execute the file *\$HOME/bin/pgrc.sh* within user postgres's login initialization file (*.profile* or *.cshrc*). The proper environmental variables are listed in this file.

```
. $HOME/sa/bin/pgrc.sh
```

OR

- 1 Add the variables in `pgrc.sh` manually to your login initialization file:

If you did not install Postgresql into the default directory, you must change these variables:

- Set `PGINSTALLDIR` to the directory that you specified in step 2 above.
- Set `PGDATA` to the directory you want to use for your database. This is normally `PGDATA=$HOME/data` for user Postgresql.

- 2 Log out. Log back in as user *postgres* to activate the new variables.

Initialize the Data Directory

Follow this procedure to initialize the default Postgresql database and to create the Security and Accounting Server database and schema:

- 1 Log in as user *postgres* and execute the Postgresql Security and Accounting database initialization script.

```
postgres$ cd $HOME/sa/bin
postgres$ pg_sadb_init
```

The name of the database is *secact60*.

The script will create a *root* database user.

- 2 If you installed Security and Accounting Server under user *sas*, you must create a database user for that login. To create that user, enter:

```
postgres$ createuser sas
```

Answer yes to the questions presented.

Test the Installation

Follow these steps to test the database installation:

- 1 Start the interactive SQL monitor to display the database schema. To display the tables and indexes in the database, enter:

```
postgres$ psql secact60
secact60=> \d
```

The names of the database tables display:

Owner	Relation	Type
postgres	calls	table
postgres	callsindex	index

- 2 To quit the sql monitor, enter:

```
secact60=> \q
```

Load the Default Data

Now that the postgres is installed and running properly, load the default data:

- 1 Log in as the user running Security and Accounting Server — typically user *sas*.
- 2 Make sure the Postgresql database is running. As user postgres, enter:

```
postmaster -S
```

If the database was already running, ignore the error shown.

- 3 Edit the `$SAHOME/bin/radserv.cfg` file.

In the *[system]* section set *DefaultDatabase* to *postgresql*:

```
DefaultDatabase = postgresql
```

- 4 Execute the *saUtil* program with the *-I* option to import the default files. Use the *-v* and *-d* options to produce additional output in `$SAHOME/log/saUtil.log`.

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

Uninstalling the Postgresql Database

To remove the Postgresql distribution and utilities, follow these steps:

- 1 Switch to the user *root*. The *#* prompt appears.
- 2 Change to the remove directory:

```
cd postgres_home_dir/sa/admin
```

- 3 Run the Postgresql database uninstall script:

```
./Remove.pg
```



This procedure does not remove the postgresql data directory.

Configuring an Oracle database

Security and Accounting Server uses the Oracle Call Interface (OCI) to connect to an Oracle database. This section describes how to configure Security and Accounting Server using Oracle OCI.

In order for Security and Accounting Server to use an Oracle database, Oracle SQL-Net should be installed on the workstation running Security and Accounting Server.



These procedures assume you are familiar with the Oracle Products. If you are not, ask your Oracle Database Administrator to assist you.

1 Install Security and Accounting Server.

If you have not already installed Security and Accounting Server, follow the steps listed in Chapter 2.

2 Edit the radserv.cfg file:

- a In the *[oracle]* section, set the *OracleHome* field to point to the install directory:

```
OracleHome = /opt/oracle7
```

- b In the *[oracle]* section, set the *Uid* and *Password* fields. Ask your Oracle Database Administrator for your Uid information. The Uid consists of a username, an optional password, and an optional service name. The service name can take different forms:

- name
- name/password
- name@service_name
- name/password@service_name

```
Uid = scott
```

```
Password = tiger
```

- c In the *[system]* section, set the *DefaultDatabase* field to *oracle*.

```
DefaultDatabase = oracle
```

3 Create the Oracle database schema:

As the Oracle user, execute the `create_sadbora.sql` script in `$$AHOME/lib/sa/db` from within `sqlplus`:

```
oracle7$ sqlplus scott/tiger (use your username/password)  
sqlplus> @ path_to_file/create_sadbora.sql
```

```
sqlplus> commit;
```

- 4 Load the Default Data. Use the -l option to import the default files. Use the -v and -d options to produce additional output in \$SAHOME/log/saUtil.log.

```
cd $SAHOME/bin  
./saUtil -l -v -d
```

- 5 Start the Server.

```
saserver start -v -d
```

- 6 Check that the server started properly. The log file \$SAHOME/log/saserv.log shows the Oracle schema being printed out.

Database Configuration

Security and Accounting Server provides a graphical interface for server configuration. The Security and Accounting Database Manager uses JDBC drivers to connect and manage your database. If you use an Oracle database, you must download Oracle's JDBC driver, as follows:

Installing the Oracle JDBC driver

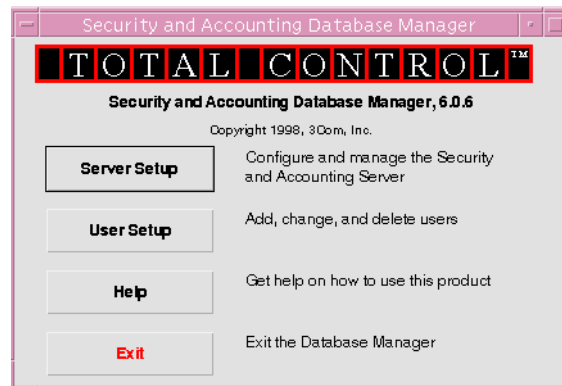
- 1 Download the thin JDBC driver for your platform from http://www.oracle.com/products/free_software/
- 2 Put the classes111.zip file from the JDBC driver package into the \$SAHOME/lib directory.

Starting the Database Manager

To start Security and Accounting Database Manager, enter:

```
cd $SAHOME/bin  
sadbm
```

The Security and Accounting Database Manager window appears.



Client Configuration

To properly configure the server, complete these tasks:

- configure the Security portion of the server.
- *Optional:* configure the Accounting portion of the server. Skip this task if you do not plan to capture accounting information.
- set up users.

Configuring the Security Server

Follow this procedure to configure Security and Accounting Server to process authentication requests from your client.

- 1 Start Security and Accounting Database Manager
- 2 Click **Server Setup**. The SystemTabs screen appears.
- 3 Click the **RADIUS Clients** tab.
- 4 Click **RADIUS CLIENTS**. The RADIUS Clients and Server Data screen appears.

IP	PORT_NO	SECRET	NAS_TYPE
DEFAULT	1645	shared_secret	
127.0.0.1	1646	secret	
127.0.0.1	1645	secret	

To prevent encryption of Accting Server msgs, leave the secret field blank for the accounting server.

New **Delete** To delete a record, select a cell in the record and then press the Delete button. **Done**

- 5 Enter the IP address, Port, Secret, NAS Type, and Chassis ID for the NAS that will communicate with Security and Accounting Server.
 - **IP:** IP address of the NAS that controls the incoming calls (NMC, HiPer ARC, etc.).
 - **PORT_NO:** UDP Port number - typically 1645 for security requests.
 - **SECRET:** A common password, four characters or longer, between the Security Server and the NAS. The identical secret must also be stored on the NAS.

- **NAS_TYPE:** The type of NAS client at this IP address.
- **Chassis ID:** If you have multiple chassis, an ID you can assign to this chassis. This field is optional.

6 Click **Done**.

Configuring the Accounting Server

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



Skip these procedures if you do not plan to use the accounting features of Security and Accounting Server.

- 1 Start Security and Accounting Database Manager.
- 2 Click **Server Setup**. The SystemTabs screen appears.
- 3 Click the **RADIUS Clients** tab.
- 4 Click **RADIUS Clients**.
- 5 Enter the IP address, Port, Secret, NAS Type, and Chassis ID for the NAS that will communicate with Security and Accounting Server.
 - **IP:** IP address of the NAS that controls the incoming calls (NMC, HiPer, etc.) This IP address is usually the same as the security client.
 - **PORT_NO:** UDP Port number - Typically 1646 for accounting information.
 - **SECRET:** An optional password, four characters or longer, used to encrypt information passed between the Accounting Server and the NAS. The identical secret must also be stored in the NAS. This field is optional.
 - **NAS_TYPE:** The type of NAS client at this IP address
 - **CHASSIS_ID:** If you have multiple chassis, the ID number you assigned to this chassis.
- 6 Click **Done**.

**Example
configuration**

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

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



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

Setting up a User

When a user dials in to the NAS, the NAS will check for the user's login ID in its local database first. If it cannot find the ID, it passes the access request to Security and Accounting Server. To configure a user in Security and Accounting Server:

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

The screenshot shows the 'User Configuration' window with the 'General' tab selected. The sidebar on the left contains buttons for 'New', 'Find', 'Delete', and 'Done', along with a 'Username:' field showing 'DEFAULT'. The main configuration area includes a 'Template' field, an 'Authentication' dropdown set to '3COM', a 'Password' field set to 'default', an 'Expiration' field set to 'MM/DD/YYYY', and a 'Failed Logins' field set to '0'. There are checkboxes for 'Allow Password Changes' and 'Deny Access'. The 'Dial In Restrictions' section contains checkboxes for 'Check Port Number?', 'Check DNS?', and 'Check ANI?', along with 'Port Number Name List', 'DNS Restriction List', and 'ANI Restriction List' fields. A 'Maximum Number of concurrent sessions' field is set to '0'. The 'Tunnel' section has a 'Tunnel Name' field, a 'Tunnel Setup Request' checkbox, and a note: 'Flag to indicate if this record will be used for Tunnel Setup Authentication.' The 'Hosts Via DNS' section has a 'Hosts Via DNS' field, a 'Host/Domain name to use in a DNS lookup' field, an 'Acct. Interim Interval' field set to '0', and an 'Interval in seconds between subsequent Acctg. Interim Msgs. (Min 60, Max 600)' field.

- 3 Click **New** to start a new user record.
- 4 Enter a user name and click **Add**.
- 5 On the **General** tab, choose 3Com from the **Authentication** list box.



If you plan to proxy authentication requests to another server, choose one of the other options from the Authentication list box. Refer to the Security and Accounting Product Reference for information about proxying to other servers.

- 6 In the **Password** field, enter a password for this user.
- 7 In the appropriate NAS tab (NMC, NETServer 3.x, HiPer ARC/SuperStack II/NETServer 8/16 V4, NetBuilder II) fill out any special information for this user's configuration. For detailed information about these settings, refer to the manuals that came with the NAS.
- 8 When finished configuring this user with your NAS, click **Done**.

4

TESTING THE INSTALLATION

This chapter introduces the Security and Accounting Server Console. It also contains troubleshooting information for Security and Accounting Server

Testing the Installation

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

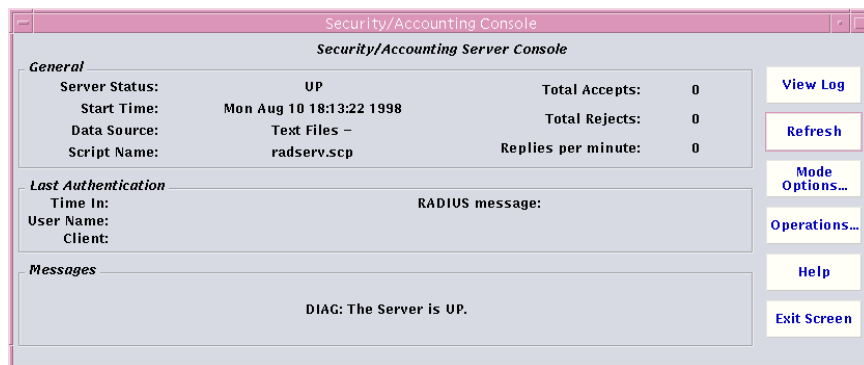
- 1 Start Security and Accounting Server.

```
cd $SAHOME/bin  
./saserver start
```

- 2 Start the Security and Accounting Console by entering:

```
saConsole
```

The Security and Accounting Console appears.



- 3 Click **Mode Options**. The Logging Options window appears.
- 4 Select **Verbose Mode**, **Trace Packets**, and **Debug Mode** to send information to the log file.
- 5 Route a call through a defined client.

- 6 Confirm that the user is authenticated:
 - In the Security and Accounting Console, look for the username in the **Last Authentication** section.
 - The **Client** field should contain the IP address of the NAS through which the call was routed.
 - The **RADIUS Message** field should contain *Access-Accept*.
- 7 In the Security and Accounting Console, click **View Log**.
Look for evidence of Access-Accept packets sent to the defined client.
- 8 Confirm accounting information has been sent:
Inspect the CALLS and EVENTS tables. Or, if you are logging to text files, inspect *.CON, *.NMC, and *.RAD) for accounting events.

Troubleshooting

Follow these steps if you are having trouble authenticating a user.

- 1 Check that the client's IP address and RADIUS secret have been entered into the RADIUS Clients tab. Also, check that the UDP port is set to 1645 for security requests.
- 2 Make sure that the Server has been restarted to accept any new changes. Any time the Server's configuration is changed, Security and Accounting Server must be restarted for those changes to take effect.
- 3 Make sure the Security and Accounting Server workstation can communicate with the client. Try to ping the client from the workstation to be sure.

INDEX

A

Accounting	1-5
Accounting Features	1-6

B

Blacklisting	1-4
--------------------	-----

C

Call Restriction	1-4
CALLS table	1-5
Client Configuration	3-8
Configuring	
Accounting	3-9
Oracle	3-5
Postgresql	3-2
Security	3-8
Users	3-11
conventions	
notice icons, About This Guide	2
text, About This Guide	2
crypt	1-7

D

Database Integration	1-4
Database Manager	
Starting	3-7
Debug Mode	4-1
Dialback Security	1-4
Distribution Files	2-3

E

EAP	1-6
EAP Support	1-6
EVENTS table	1-5

F

Features	
Accounting	1-6
New	1-6
Security	1-3

I

Installing	
Postgresql	3-2
Security and Accounting Server	2-3
iPass	1-6

L

L2TP	1-6
------------	-----

M

Mode Options	4-1
multi-link	1-7

N

NAS	1-1
New Features	1-6

O

Oracle	
Configuring	3-5
OUTDEF.DAT	1-5

P

Password Management	1-3
Postgresql	
Installing	3-2
overview	3-2
PPTP	1-6
Proxy Authentication	1-3

R

RADIUS	1-1
radserv.cfg	3-4, 3-5
Roaming dialback in NETServer	1-4

S

saConsole	4-1
sadbm	3-7

SAHOME	
For the bourne shell	2-6
For the C shell.....	2-6
saUtil.....	3-4, 3-6
Security.....	1-2
Security and Accounting Console	4-1
Security and Accounting Server	
Accounting Features	1-6
Installing	2-3
Security Features.....	1-3
Uninstalling	2-6
Security Features	1-3
System Requirements, Sun Solaris.....	2-2
System Requirments, HP-UX.....	2-2

T

Total Control Manager.....	2-2
Trace Packets	4-1

U

UDP Port.....	3-8, 3-9
Uninstalling	
Postgresql	3-4
Security and Accounting Server	2-6
User Templates	1-4

V

Verbose Mode.....	4-1
VPN.....	1-6



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. 1.024.1079-04