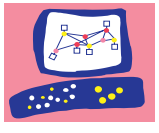
Check Point Account Management Client

Version 4.1

Part No.: 700059
January 2000



CHECK POINT™
Software Technologies Ltd.

We Secure the Internet.

Check Point Software Technologies Ltd.

International Headquarters:
3A Jabotinsky Street
Ramat Gan 52520, Israel
Tel: 972-3-753 4555
Fax: 972-3-575 9256

e-mail: info@CheckPoint.com

U.S. Headquarters:
Three Lagoon Drive, Suite 400
Redwood City, CA 94065
Tel: 800-429-4391 ; (650) 628-2000
Fax: (650) 654-4233

http://www.checkpoint.com

February 3, 2000

Please direct all comments regarding this publication to **techwriters@checkpoint.com.**

Contents

Figures

Tables

Preface

Scope

This book describes how to install and use the Check Point Account Management Client.

Who Should Use this User Guide

This User Guide is written for system administrators who are responsible for maintaining account (user) information.

It assumes you have a basic understanding and a working knowledge of:

- system administration
- the Unix or Windows operating system
- the Windows GUI

Summary of Contents

Chapter 1, “Introduction,” introduces Check Point Account Management and describes its basic concepts.

Chapter 2, “Installing the Account Management Client,” decribes how to install the Account Management Client.

Chapter 3, “Account Management Graphical User Interface (GUI),” describes how to use the Account Management Client’s Graphical User Interface (GUI).

Chapter 4, “Queries,” describes how to formulate and execute queries.

Chapter 5, “User Management,” describes how to manage user, templates and groups with the Account Management Client.

Chapter 6, “Certificate Management,” describes how to use the Account Management Client to create certificates.

Chapter 7, “Troubleshooting,” describes how to solve common problems with the Account Management Client.

What Typographic Changes Mean

The following table describes the typographic changes used in this book.

TABLE P-1 Typographic Conventions

Typeface or Symbol	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories; on-screen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% You have mail.`
`AaBbCc123`	What you type, contrasted with on-screen computer output	`machine_name% su` `Password:`
AaBbCc123	Command-line placeholder: replace with a real name or value	To delete a file, type `rm` *filename*.
AaBbCc123	Book titles, new words or terms, or words to be emphasized	Read Chapter 6 in *User’s Guide*. These are called *class* options. You *must* be root to do this.

Shell Prompts in Command Examples

The following table shows the default system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

TABLE P-2 Shell Prompts

Shell	Prompt
C shell prompt	`machine_name%`
C shell superuser prompt	`machine_name#`
Bourne shell and Korn shell prompt	`$`
Bourne shell and Korn shell superuser prompt	`#`

CHAPTER 1

Introduction

In This Chapter

Overview

Check Point Account Management consists of three components:

1. an LDAP Server containing user, group and template information (third-party software)
2. the Check Point Account Management Client, a GUI used to manage users in the LDAP Server
3. a Check Point module that uses the data on the LDAP Server

   This can be any of the following Check Point products:

   - VPN-1/FireWall-1 Management Module
   - VPN-1/FireWall-1 FireWall Module

This guide describes the Account Management Client.

The LDAP Model

LDAP (Lightweight Directory Access Protocol) is a lightweight version of the X.500 directory access protocol. LDAP is based on a Client/Server model in which an LDAP Client makes a TCP connection to an LDAP server[1], over which it sends requests and receives responses.

1. The default port numbers are 389 for a standard connection and 636 for an SSL connection.

The LDAP information model is based on the entry, which contains information about some object (for example, a person). Entries are composed of attributes, which have a type and one or more values. The schema lists the attributes, their data types (for example, ASCII text, a JPEG photograph, etc.) and how those values behave during directory operations (for example, whether case is significant in comparisons).

Entries are organized in a tree structure, usually based on political, geographical, and organizational boundaries. Each entry is uniquely named relative to its sibling entries by its RDN (relative distinguished name) consisting of one or more distinguished attribute values from the entry. For example, the entry for the person Babs Jensen might be named with the “Barbara Jensen” value from the commonName attribute.

A globally unique name for an entry, called a DN (distinguished name), is constructed by concatenating the sequence of RDNs from the root of the tree down to the entry. For example, if Babs worked for the University of Michigan, the DN of her University of Michigan entry might contain:

```
“cn=Barbara Jensen, o=University of Michigan, c=US”
```

A DN is expressed in the “bottom up” sequence, that is, starting at the lowest level and moving up to the root of the tree.

A different Barbara Jensen who works at The Brown Jug Pub in London, England might have a DN of:

```
“cn=Barbara Jensen, o=The Brown Jug Pub, c=UK”
```

This is illustrated in FIGURE 1-1.

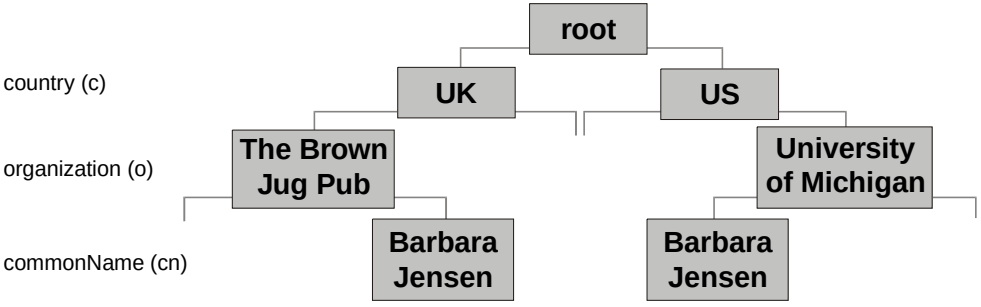


FIGURE 1-1 LDAP Tree Example

LDAP provides operations to authenticate, search for and retrieve information, modify information, and add and delete entries from the tree. The LDAP information model is most appropriate for directories, that is, information which is read much more frequently than it is modified.

In addition to maintaining LDAP users with the Check Point Account Management Client and LDAP Server, it is possible to maintain LDAP users using any LDAP Version 2 and higher compatible server.

Account Management Configuration

This section describes typical Account Management configurations for Check Point products.

VPN-1/FireWall-1

A typical VPN-1/FireWall-1 configuration is depicted in FIGURE 1-2.

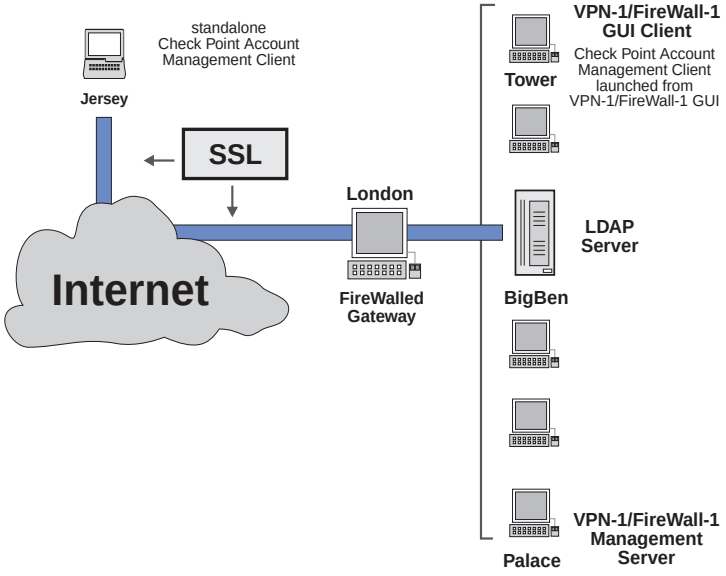


FIGURE 1-2 A typical Account Management configuration (VPN-1/FireWall-1)

Palace, the VPN-1/FireWall-1 Management Server, is the repository of the VPN-1/FireWall-1 database, which includes users defined with the proprietary VPN-1/FireWall-1 User Manager.

Palace's VPN-1/FireWall-1 GUI Clients, for example Tower, can define two kinds of users:

- VPN-1/FireWall-1 users — users defined in the VPN-1/FireWall-1 User Manager, using the VPN-1/FireWall-1 GUI
- LDAP users — users defined on BigBen, the LDAP server, using the AM Client

Jersey, on which VPN-1/FireWall-1 is not installed, can update only LDAP users, using the AM Client. In the configuration depicted in FIGURE 1-2, this communication channel is secured with SSL (Secure Socket Layer).

A system administrator can define a Security Policy on Palace, using the VPN-1/FireWall-1 GUI Client on Tower, and define rules that specify VPN-1/FireWall-1 groups and LDAP groups. When the Security Policy is installed on the FireWalled gateway (London), the User Database (proprietary information about VPN-1/FireWall-1 users) is downloaded to London.

When a VPN-1/FireWall-1 user logs on to London, London has immediate access to the required authentication information in the VPN-1/FireWall-1 User Database. In contrast, when an LDAP user logs on and must be authenticated, London communicates with the LDAP server to obtain the required information.

Account Units

An LDAP Server can contain multiple branches (for example, "o=University of Michigan,c=UK" is a branch). An LDAP Server and a subset of its branches constitute a Check Point Account Unit.

It is possible to maintain the LDAP user database using more than one Account Unit. The advantages of using more than one Account Unit are:

- **compartmentalization** — A large number of users can be distributed across several servers which may be partitioned into several Account Units, each of which is managed by a different administrator. In this way, both efficiency and security can be enhanced.
- **high availability** — Information can be duplicated on several servers. Some LDAP servers provide automatic tools for synchronizing servers.
- **remote sites** — It may be efficient to provide each geographically remote Check Point LDAP Client (for example, VPN-1/FireWall-1) with a close at hand LDAP server.

For more information about Account Units, see "Account Units" on page 177 of *FireWall-1 Administration Guide*.

CHAPTER 2

Installing the Account Management Client

In This Chapter

Minimum Requirements

TABLE 2-1 lists the minimum hardware and operating system required for installing the VPN-1/FireWall-1 Account Management Client.

TABLE 2-1 Minimum Requirements (Account Management Client)

Platforms	Sun SPARC-based systems Intel Pentium 100 MHz and higher HP PA 9000 RS 6000 166 MHz and higher

TABLE 2-1 Minimum Requirements (Account Management Client) (continued)

Operating System	Solaris 2.5 and higher Windows 9x, Windows NT (Intel only) HP-UX 10.x IBM AIX 4.2 and higher
Disk space	Solaris — 12 MB Windows — 7 MB (15 MB for the installation) HP-UX — 30 MB (including JRE) IBM AIX — 6 MB (not including JRE)
Memory	Solaris — 32 MB (64 MB recommended) Windows — 32 MB (64 MB recommended) HP-UX — 64 MB IBM AIX — 64 MB

Installing the Account Management Client

All Platforms

The Account Management Client can be installed on Windows 95, Windows NT (Intel only) and Unix.

The Account Management Client is located on the CD-ROM in the `CPAccountmgmtclnt-11` directory under the platform directory (`windows, AIX` and `HP-UX`) and in the `CPamc-11` directory under the `solaris2` directory.

You can install the Account Management Client either directly from the CD-ROM, or you can recursively copy the installation files from the CD-ROM to a directory on your disk and install from there.

The directory includes an End User License Agreement for the Account Management Client in the file `license.txt` or `license.rtf`. Please read the license agreement before installing the software.

Note – If you are updating an older version of the Account Management Client, a message will appear asking whether you would like to update all the objects on the current Account Unit. For more information on updating your Account Units, see *Check Point Account Management Client Build 140 Release Notes* at `http://www.checkpoint.com/support`.

In This Section

Windows

1 Open the **Start** Menu and choose **Settings**.

2 Choose **Control Panel** from the **Settings** menu.

3 Double click on **Add/Remove Programs** and follow the instructions.

Alternatively, you can open the **Start** Menu and choose **Run**, and then type `windows\cpaccountmgmtclnt-11` (or whatever the location of the SETUP application is) and follow the instructions.

4 The **Choose Destination Location** window (FIGURE 2-1) allows you to specify a directory in which the Account Management Client will be installed by clicking on **Browse**.

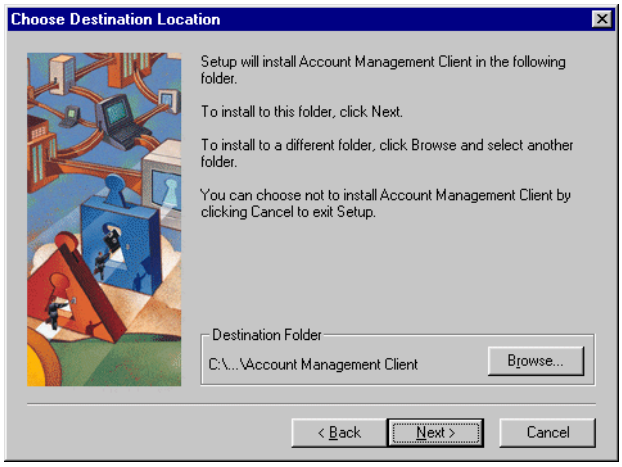


FIGURE 2-1 Choose Destination Location window

If you do not choose a directory, then Account Management will be installed in the default directory, indicated under **Destination Directory**.

Unix Platforms

In This Section

Solaris

On Solaris, the Account Management Client is installed using the command line utility `pkgadd`.

1 Become superuser.

2 Change to the directory `solaris2`.

3 Enter the following command to install the Account Management Client:

```
hostname# pkgadd CPamc-11
```

For information about the `pkgadd` command, refer to the Solaris documentation. `pkgadd` presents a lists of packages, and asks you to choose one to install.

Specify the package you wish to install by entering either its name or its number in the list.

4 To run the Account Management Client,

a Become superuser.

b Enter the following command:

```
hostname# /opt/CPamc-11/account-management/bin/accountMgm
```

HP-UX

Special Notes for HP-UX

If you encounter a problem with the depth of the CD-ROM directories, use the files in hpux/TarFiles.

HP-UX 10.20

The Check Point CD is created in the Rock Ridge format. HP makes available the PFS package (Portable File System) that allows their workstations to recognize this format.

The following URL describes the PFS package.

- http://www.hp.com/wsg/programs/gis.html

The following URLs describe the README files and the drivers.

- ftp://ftp.hp.com/pub/demos/grfxdemos/pfs/README
- ftp://ftp.hp.com/pub/demos/grfxdemos/pfs/pfs.tar.Z

This version of HP-UX already includes the PFS package. However, you'll need to check the man page for the `pfs_mount` command for details on setting up an `/etc/pfs_fstab` file.

You can use the following special `mount` command.

```
pfs_mount -t rrip /dev/device /cdrom
```

Installation

On HP-UX, the Account Management Client is installed using the `swinstall` application.

To install the Account Management Client, proceed as follows:

1. Become superuser.
2. Copy the installation files to the `/tmp` directory.
3. If the `/tmp` directory has not been registered as an installation directory, enter the following command to register it.

```
hostname# swreg -l depot -x select_local=true /tmp
```

   For information about the `swreg` command, refer to the HP-UX documentation.

4. Enter the following command to install the Account Management Client:

```
hostname# swinstall &
```

5. The **SD Install - Software Selection** window is displayed, and then the **Specify Source** window is displayed on top of it.

   For information about the `swinstall` command, refer to the HP-UX documentation.

6. Click on **Source Depot Path**.
7. In the **Depot Path** window, select the directory in which the installation files are located.
8. Click on **OK** to close the **Depot Path** window.
9. Click on **OK** to close the **Specify Source** window.
10. In the **SD Install - Software Selection** window, select **Account Management Client**.
11. From the **Actions** menu, select **Install (analysis)**.
12. When the analysis phase completes, click on **OK**.
13. When the installation phase completes, click on **Done**.
14. From the **File** menu, select **Exit**.
15. To run the Account Management Client,
    a. Become superuser.

b Enter the following command:

```
hostname# /opt/amc/account-management/bin/accountMgm
```

IBM AIX

On IBM-AIX, the Account Management Client is installed using the `smit` application.

To install the Account Management Client, proceed as follows:

1. Become superuser.
2. Change to the `/tmp` directory.
3. Copy the `amc.usr.1.0.0.x` file (from the CD-ROM to the `/tmp` directory.
4. Enter the following command to install the Account Management Client:

```
hostname# smit &
```

   For information about the `smit` command, refer to the AIX documentation.

5. Click on **Software Installation and Maintenance**.
6. Click on **Install and Update Software**.
7. Click on **Install/Update Selectable Software (Custom Install)**.
8. Click on **Install Software Products at Latest Level**.
9. Click on **New Software Products at Latest Level**.
10. In the **New Software Products at Latest Level** window, enter the input device or the name of the directory where the VPN-1/FireWall-1 installation files are located.
11. A dialog box is displayed in which you are asked to review the installation parameters and confirm them.
12. In **SOFTWARE to install**, click on **List**.
13. Select **Account Management Client**.
14. Click on **OK** to start the installation process.
15. When the installation completes, exit `smit`.

16 To run the Account Management Client, type the following command:

```
hostname# /usr/lpp/amc/account-management/bin/accountMgm
```

Special Note for AIX

The Account Management Client installation procedure does not install the Java Runtime Environment (JRE) on AIX. You must install Java version 1.1.x (where x is 6 or higher) before you can use the Account Management Client.

On some versions of AIX, JRE is on the installation CD-ROM. It is also available from IBM on the World Wide Web.

After you install JRE, you must create a symbolic link as follows:

1 Change to the Account Management Client directory:

```
hostname# cd /usr/lpp/amc
```

2 Type the following command:

```
hostname# ln -s /usr/jre1.1.6  java
```

3 Enter the following command to confirm that the symbolic link was successfully created:

```
hostname# ls -l
hostname# java   -> /usr/jre1.1.6
```

Uninstalling the Account Management Client

Windows

To uninstall the Account Management Client, proceed as follows:

1 Open the Windows **Start** menu and choose **Control Panel**.

2 Choose **Add/Remove Programs**.

3 Choose **Account Management Client** (FIGURE 2-2).

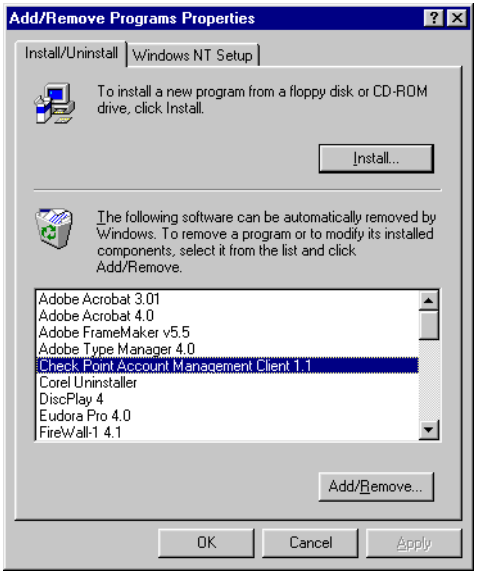


FIGURE 2-2 Uninstalling the Account Management Client

4 Select **Add/Remove**.

5 Select **OK**.

Unix Platforms

To uninstall the Account Management Client, use the same administrative tool that you used to install the Account Management Client, except for Solaris, where you should use `pkgrm`.

After Installing

Removing or Moving the Account Management Client Files

Do not remove or move the Account Management Client files manually.

- To remove the files, uninstall the Account Management Client.
- To move the files, uninstall the Account Management Client and then re-install in another directory.

For information on uninstalling the Account Management Client, see “Uninstalling the Account Management Client” on page 11.

CHAPTER 3

Account Management Graphical User Interface (GUI)

In This Chapter

The Account Management Client

Starting the Account Management Client

To start the Account Management Client, proceed as follows:

TABLE 3-1 Starting the Account Management Client

Windows System	Action
Windows 95 or NT	Double-click on the Account Management Client icon (in `Start/Programs/Check Point Management Clients/ Account Management` Client.
Solaris	Enter **`/opt/CPamc-11AMC/account-management/bin/accountMgm`** at the command line.
HP-UX	Enter **`/opt/amc/account-management/bin/accountMgm`** at the command line.
IBM AIX	Enter **`/usr/lpp/amc/account-management/bin/accountMgm`** at the command line.

You can also start the Account Management Client from within other Check Point applications. In this case, you must define the Account Units in those applications. For more information, see Chapter 4, “Account Management” of *VPN-1/FireWall-1 Administration Guide*.

The **Login** window (FIGURE 3-1) appears.The **Login** (FIGURE 3-1) window appears.

FIGURE 3-1 Login window

To login to an Account Unit, proceed as follows:

1. Select an **Account Unit**.

   If the Account Unit has a Certificate Authority associated with it, its icon includes the seal ( ).

2. Enter the officer profile password in the **Profile Password**.

3. Click on **OK**.

Note – Once you have logged in to an LDAP Server, the only way to log in to another LDAP Server is to run the Account Management Client again.

To define a new **Account Unit**, proceed as follows:

1. Click on **New**.

2 From the menu, choose whether to create an Account Unit with or without a Cetificate Authority.

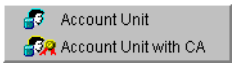


FIGURE 3-2 New Account Unit Menu

The **Account Unit Properties** window (FIGURE 3-3) is displayed.

To change the properties of an existing **Account Unit**, proceed as follows:

1 Select the **Account Unit** you wish to modify.

2 Click on **Edit**.

The **Account Unit Properties** window (FIGURE 3-3 on page 15) is displayed.

Account Unit Properties

The **Account Unit Properties** window defines how to access an Account Unit.

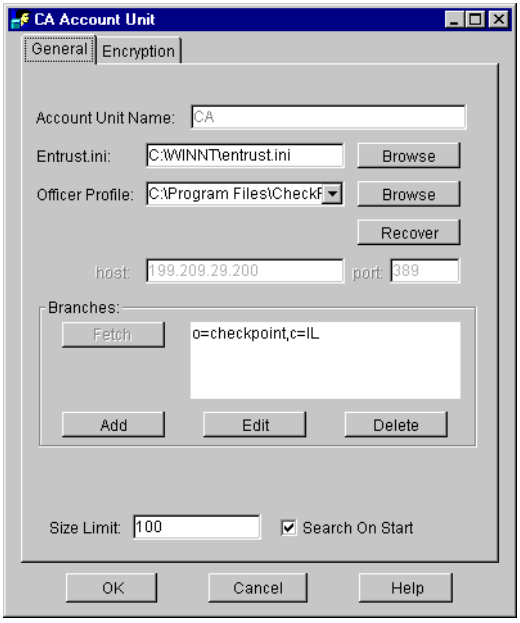


FIGURE 3-3 Account Unit Properties window — General tab (non-CA and CA versions)

Account Unit Properties Window — General Tab

Account Unit — the account unit's name

Host — the IP address or resolvable name of the host on which the LDAP server is running.

Port — the port number

This parameter is ignored if **Use Encryption** is checked in the **Encryption** tab (FIGURE 3-5 on page 18). In this case, the port number specified in the **Encryption** tab is used.

Login DN — the Distinguished Name (DN) that will be used to bind to the LDAP server

Size Limit — the number of entries that will be retrieved in a single query operation

This parameter can also be set from the **Size Limit** window (FIGURE 3-9 on page 25). To display the **Size Limit** window, choose **Size Limit** from the **Edit** menu in the **Account Management Client** window (FIGURE 3-7 on page 22).

Search On Start — whether to search the directory immediately after binding

Because some LDAP Servers have a very large number of entries defined on them, it is best to uncheck this option so as to prevent entries being retrieved unnecessarily. You can then query the Account Unit to display only the entries in which you are interested. See Chapter 4, “Queries” for information about queries.

Branches

The listbox lists the branches of the directory tree that will be retrieved or searched after the Client binds to the LDAP Server.

Note – It is highly recommended that the same branches be defined for an Account Unit both in the Account Management Client and in other Check Point applications.

You can fetch the defined branches by clicking on **Fetch**. Alternatively, you can add branches manually.

Note – Fetch requires a version 3.0 or higher LDAP Server.

To add a branch, click on **Add**. The **Add New Branch** window appears.

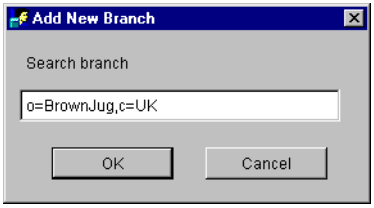


FIGURE 3-4 Add New Branch window

Enter the branch name and click on **OK**. The branch is added to the listbox in the **General** tab of the **Account Unit Properties** window (FIGURE 3-3).

Certificate Authority

If the Account Unit has an associated Certificate Authority, you must specify additional parameters in the **General** tab of the **Account Unit Properties** window.

Entrust.ini — the location of the Entrust initialization file

Click on **Browse** to search for the file.

Officer Profile — the location of the profile file of an Officer

Click on **Browse** to search for the file. The profile can also be a hardware token (see “Hardware Tokens” on page 66 for more information).

Recover — Click **Recover** to recover the specified Officer’s profile.

See “Recovering a Profile” on page 65 for more information.

Account Unit Properties Window — Encryption Tab

The **Encryption** tab of the **Account Unit Properties** window specifies the encryption parameters (if any) of the connection between the Account Management Client and the LDAP Server.

Use this tab only if the LDAP Server is configured to use SSL. The default is that SSL is not selected.

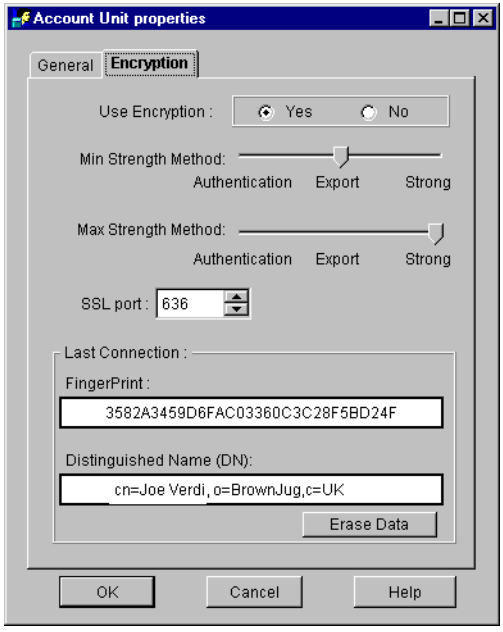


FIGURE 3-5 Account Unit Properties window — Encryption tab

Use Encryption — Select one of the choices:

Yes — Connect to the LDAP Server using SSL.

If you connect using SSL, you must also specify the encryption parameters below. The port number specified in **SSL Port** on this tab is used for the connection.

If the Account Unit has an associated CA, then the Check Point (fw1) and Entrust attributes are maintained in separate connections. The Entrust connection does not use SSL.

No — Connect directly to the LDAP Server.

The port number specified in the **General** tab is used for the connection.

Min Strength Method — This is the weakest encryption method the Account Management Client is prepared to use.

Select one of the methods, where **Authentication** is the weakest and **Strong** is the strongest. For more information, see “Negotiating an Encrypted SSL Session” on page 19.

Max Strength Method — This is the strongest encryption method the Account Management Client is prepared to use.

Select one of the methods, where **Authentication** is the weakest and **Strong** is the strongest. For more information, see "Negotiating an Encrypted SSL Session" below.

Note – The Account Management Client and the LDAP Server will encrypt using the strongest method acceptable to both sides.

SSL Port — The default is 636.

This port, rather than the one specified in the **General** tab, is used for the connection.

Last Connection — This is a description of the last certificate used by the LDAP Server.

The Account Management Client obtains the certificate of the public key used by the LDAP Server, and extracts the Server's name (DN) and computes the public key's fingerprint. The first time you connect to an LDAP Server, you should confirm the fingerprint with the LDAP Server's system administrator by fax or telephone or some other non-network means.

On subsequent connections to the LDAP Server, the Account Management Client requests the Server's fingerprint and compares it to the one it previously obtained and stored. If there is a discrepancy, an error message is issued (see FIGURE 3-6 on page 20).

Erase Data — Erase the fingerprint and DN.

Use this option if you have received a new fingerprint from the LDAP system administrator.

Negotiating an Encrypted SSL Session

Both sides (the LDAP Server and the Account Management Client) negotiate the parameters of the SSL session. For each side, both a minimum strength acceptable method and a maximum strength available method are defined.

TABLE 3-2 lists the methods used for each strength. Note that **Strong** in the Account Management Client corresponds to Very Strong in the table.

TABLE 3-2 Encryption Method Parameters

Strength	Authentication Method	Encryption and Data Integrity Methods
Authentication	RSA (512 bit)	no encryption data integrity: MD5 or SHA-1, depending on the other side
Export	RSA (512 bit)	■ RC4 (40 bit) and MD5, *or* ■ DES (40 bit) and SHA-1
Strong (this cannot be specified in the GUI but can be negotiated)	RSA (1024 bit)	■ RC4 (64 bit) and MD5, *or* ■ DES (40 bit) and MD5 or SHA-1, depending on the other side
Very Strong (this is indicated in the GUI by **Strong**)	RSA (1024 bit)	■ RC4 (128 bit) and MD5 or SHA-1, depending on the other side, *or* ■ 3DES and MD5 or SHA-1, depending on the other side

Note – Additional LDAP communications established by the AMC-integrated Entrust toolkit are not encrypted. However, it does not jeopardize security since the transferred information is not confidential.

When Fingerprints Change

If the fingerprint changes on a later connection, a message window similar to FIGURE 3-6 is displayed.

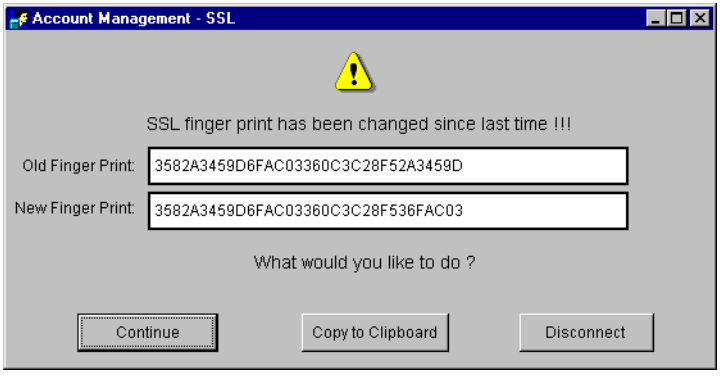


FIGURE 3-6 Fingerprint changed message window

At this point, you have the following choices:

Continue — Make the connection, even though the fingerprint has been changed. The new fingerprint will be stored in place of the previous one.

Warning – This option should be used with extreme caution.

Copy to Clipboard — Copy the old and new fingerprints to the clipboard.

This option makes it easier for you to contact the LDAP Server's system administrator to confirm the new fingerprint. If you choose this option, the message window is not closed, and you will eventually have to choose one of the other options.

Disconnect — Terminate the connection.

User Management

Account Management Window

After you successfully connect to the LDAP Server, the **Account Management Client** window (FIGURE 3-7) is displayed.

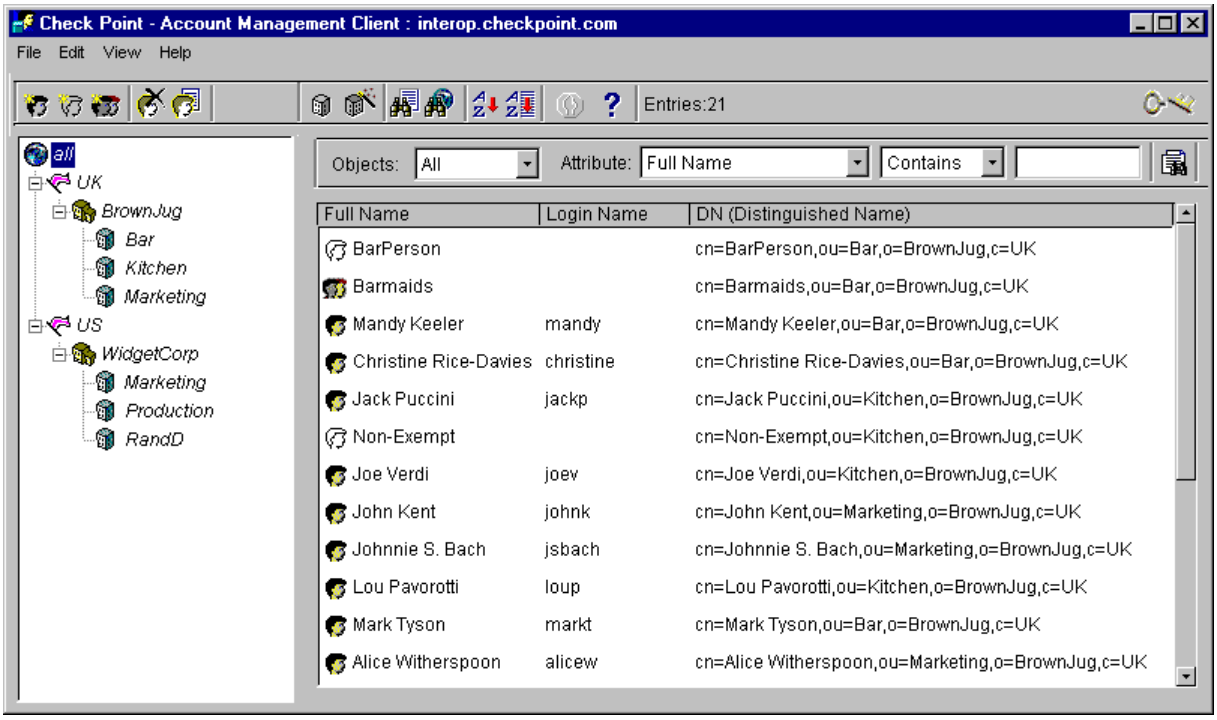


FIGURE 3-7 Account Management window

If **Search on Start** in the **Account Unit Properties** window is checked, the right side of the **Account Management** window displays all the users, groups and templates defined below the highlighted node in the tree displayed in the left side, up to the number specified by the size limit (see “Size Limit” on page 25).

If **Search on Start** in the **Account Unit Properties** window is not checked, the right side of the **Account Management Client** window is empty.

You can query the Account Unit to display the entries in which you are interested. See Chapter 4, “Queries” for information about queries.

Creating an Organizational Unit

New Organizational Unit Window

To create an organizational unit, select the point in the tree under which the organizational unit should be created, and then right-click on it or select **New Organizational Unit** from the **File** menu.

The **New Organizational Unit** window (FIGURE 3-8) is displayed.

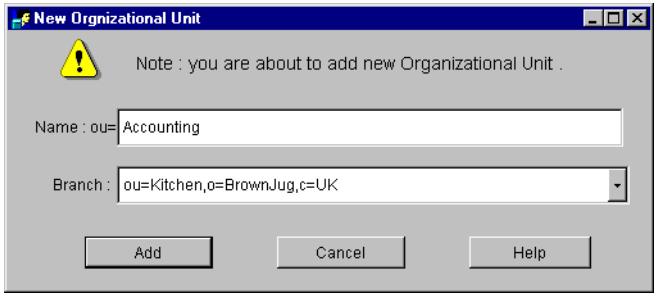


FIGURE 3-8 New Organizational Unit window

1 Enter the name of the new organizational unit.

Warning – "ou=" is implied. Do *not* type it. If you type it (for example, "ou=Accounting"), then the organizational unit's name will include "ou=" (for example, "ou=ou=Accounting").

The default **Branch** is the selected tree object (if it exists on the LDAP Server), but you can select another one.

2 Click on **Add**.

objectclass

When you create an organizational unit in this way, the following objectclass is added to the corresponding LDAP entry:

- objectclass=organizationalUnit

Creating a Tree Object

If a node in the tree is overlaid by a "X", then one of the following conditions is true:

- It is defined in the `slapd.conf` file (on the LDAP Server) with the `suffix` parameter, but it does not exist in the LDAP directory.
- It is defined as a branch in the Account Unit (see "Branches" on page 16), but is not defined in the `slapd.conf` file with the `suffix` parameter.

In the first case, you can create the object in the LDAP directory by:

- right-clicking on it and choosing **Create this Object** from the menu, *or*
- selecting it and choosing **Create Tree Object** from the **File** menu.

In the second case, the object cannot be created with the Account Management Client, because it must already be present in `slapd.conf` (see "Modifying slapd.conf (on the LDAP Server)" below).

objectclass

When you create a tree object in this way, one of the following objectclasses is added to the created object:

- objectclass=organization (if the selected object belongs to the type Organization)
- objectclass=organizationalUnit (if the selected object begins with an organizationalUnit)

Modifying slapd.conf (on the LDAP Server)

The `slapd.conf` file usually contains definitions of the root branches. You can modify the `slapd.conf` file in two ways:

- using any text editor
- using your LDAP Server's configuration utility

SSL

If the  icon appears above the Query bar to the right, then the connection is encrypted by SSL.

If the  icon appears (a broken key), then the connection is not encrypted by SSL.

Querying the LDAP Directory

For information about how to list, update and query users, see Chapter 4, "Queries".

Show All

To show all the entries, without regard to queries, click on  in the toolbar. The number of entries retrieved is subject to the size limit (see "Size Limit" on page 25).

Show All should be used with LDAP Servers containing a small number of entries.

Size Limit

The entries listed in the **Account Management Client** window are those satisfying the last applied query (see Chapter 4, “Queries”). The number of entries is limited by the size limit, which can be specified either in the **General** tab of **Account Unit Properties** window (FIGURE 3-3 on page 15) or in the **Size Limit** window (FIGURE 3-9).

To open the **Size Limit** window, choose **Size Limit** from the **Edit** menu. The **Size Limit** window (FIGURE 3-9) is displayed.

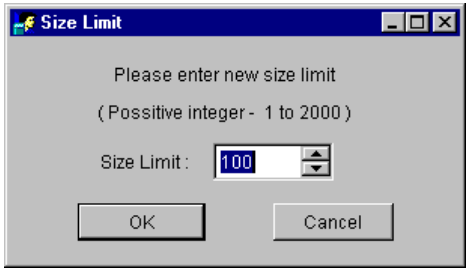


FIGURE 3-9 Size Limit window

Size Limit — the maximum number of entries that will be retrieved by a query

For example, if there are 3,000 entries in a branch and the size limit is 100, only the first 100 entries will be displayed.

Closing the Account Management Client

To close the Account Management Client, select **Exit** from the **File** menu.

Account Management Client Menus

File Menu

TABLE 3-3 File Menu Commands

Menu Entry	Toolbar Button	Description	See
New User		Create a new user.	"Creating a User" on page 42
New Template		Create a new template.	"Creating a Template" on page 56
New Group		Create a new group.	"Creating a Group" on page 58
Delete		Delete the currently selected object.	Chapter 5, "User Management
New Organizational Unit		Create a new Organizational Unit under the currently selected tree object.	"Creating an Organizational Unit" on page 23
Create Tree Object		Create the currently selected tree object (currently X'd over).	"Creating a Tree Object" on page 23
Exit	none	Close the Account Management Client.	"Closing the Account Management Client" on page 25

Edit Menu

TABLE 3-4 Edit Menu Commands

Menu Entry	Toolbar Button	Description	See
Show All		Show all the entries, without regard to queries.	"Show All" on page 24
Query		Open the **Query** window.	"Query Window" on page 30
Properties		Display the properties of the currently selected object.	Chapter 5, "User Management
Manage CA		Open the **Manage CA** window.	"Managing the Certificate Authority" on page 67
Certificate		Manage the selected object's certificate.	"Managing Certificates" on page 64
Size Limit	none	Limit the number of records returned by a query.	"Size Limit" on page 25

View Menu

TABLE 3-5 View Menu Commands

Menu Entry	Toolbar Button	Description	See
Sort by Full Name		Sort the entries by the user's full name.	You can also click on the column title.
Sort by Login Name		Sort the entries by the user's login name.	You can also click on the column title.

Help Menu

TABLE 3-6 Help Menu Commands

Menu Entry	Toolbar Button	Description
Contents		Open the Account Management Client online Help system.
About Account Management	none	Display the **About Account Management** window, which shows the version and build numbers of the Account Management Client.

Account Management Client Toolbar

FIGURE 3-10 Account Management Toolbar

The toolbar buttons are shortcuts for menu commands (see TABLE 3-7).

Toolbar Buttons and their Corresponding Menu Commands

TABLE 3-7 Toolbar buttons and their corresponding menu commands

Toolbar Button	Menu Command	Toolbar Button	Menu Command
	**File➤New User**		**File➤Create Tree Object**
	**File➤New Template**		**Edit➤Query**
	**File➤New Group**		**Edit➤Show All**
	**File➤Delete**		**View➤Sort by Full Name**
	**File➤Properties**		**View➤Sort by Login Name**
	**Edit➤Manage CA**		none
	**Edit➤Cerificate**		**Help➤Contents**
	**File➤New Organizational Unit**		This button is on the Query bar (see Chapter 4, “Queries”).

CHAPTER 4

Queries

In This Chapter

Querying the LDAP Directory

The entries listed in the **Account Management** window are those satisfying the last applied query. The number of entries is limited by the size limit specified in the **General** tab of **Account Unit Properties** window (FIGURE 3-3 on page 15) or in the **Size Limit** window.

There are two ways to query the LDAP directory:

- For simple queries (queries with only one condition), use the Query bar.
- For complex queries (queries with more than one condition), use the **Query** window.

Query Bar

The Query bar (FIGURE 4-1) enables you to define and execute a simple query. To define and execute a complex query, use the **Query** window (see "Query Window" on page 30).

The Query bar is displayed above the list of LDAP entries on the right side of the **Account Management** window.

FIGURE 4-1 Query Bar

To query the LDAP database using the Query bar, proceed as follows:

1. Make a selection (**Users**, **Groups**, *etc*.) from the **Objects** dropdown list.
2. Make a selection (**Full Name**, **Login Name**, *etc*.) from the **Attributes** dropdown list, or enter the name of an attribute.
3. Select an operator (see TABLE 4-1 on page 31 for a list of operators and their meanings).
4. Enter a value in the rightmost box on the Query bar.
5. Click on  or press Enter to execute the query and display the results.

Query Window

The **Query** window (FIGURE 4-2 on page 30) enables you to define and execute a complex query. To define and execute a simple query, use the Query bar (see "Query Bar" on page 29).

To open the **Query** window, click on  in the toolbar or select **Query** from the **Edit** menu.

The **Query** window (FIGURE 4-2) is displayed.

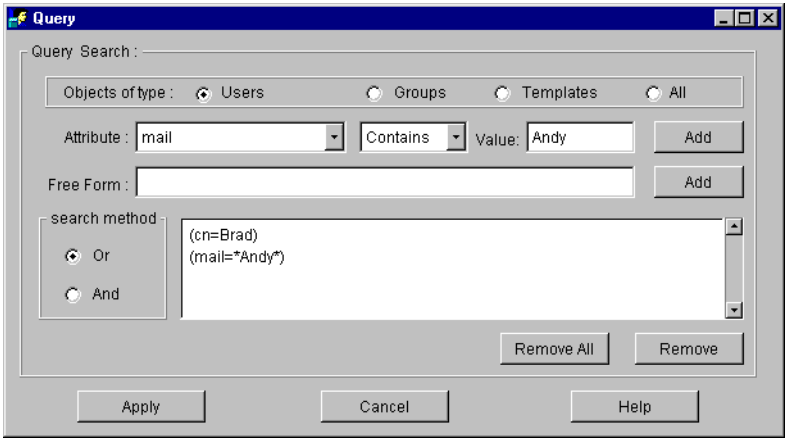


FIGURE 4-2 Query window

Defining the Query

To define a query, select values from the dropdown lists and enter values in the text boxes. Use the **Add** buttons to add criteria to the query.

Objects of Type — Only objects of the selected type will be returned by the query.

Select an object (**Users**, **Templates** or **Groups**) to restrict the types of entries that will be returned, or select **All** if you do not wish to restrict the types of entries.

Attributes — To include an attribute in the query, proceed as follows:

1. From the first dropdown list, select an attribute.

   You can either select an attribute from the list or enter an attribute. The list of available VPN-1/FireWall-1 attributes, including their formats and permitted values, is given in TABLE 4-3 on page 34.

2. From the second dropdown list, select an operator (see TABLE 4-1).

TABLE 4-1 Operators - meaning of values

value	meaning
is	The attribute's value must be equal to **Value**.
is not	The attribute's value is not equal to **Value**.
starts with	The attribute's value starts with **Value**.
ends with	The attribute's value ends with **Value**.
contains	The attribute's value contains **Value**.
less than	The attribute's value is less than or equal to **Value**.
greater than	The attribute's value is greater than or equal to **Value**.
sounds like	The attribute's value sounds like **Value**.

Note – The "less than" and "greater than" operators are supported by LDAP Version 3.0 and higher servers only.

3. Enter the **Value** to which the entry's **Attribute** will be compared.

   You must take care that **Value** corresponds to the attribute's type and format, as described in "Attributes" on page 34. For example, if **Attribute** is fw1expiration-date, then **Value** should be of the form `yyyymmdd` (for example, 20 August 1968 is 19680820).

4. Click on **Add** to add the condition to the query (in the text box to the right of **Search Method**).

You can repeat this procedure as often as necessary. Each time, another condition is added to the query.

Free Form — Enter a free form LDAP condition (query expression) and click on **Add** to add it to the query.

See RFC 1558 for information about the syntax of LDAP query expressions.

Search Method — This specifies whether the conditions are ANDed or ORed together.

To remove a condition from the query, select it and click on **Remove**.

To clear the query (remove all of its conditions), click on **Remove All**.

Executing the Query

To execute the query and display the results, click on **Apply**. The **Query** window remains open, allowing you to view the results and modify the query if needed.

To close the **Query** window, click on **Cancel**.

Template Masking

Query conditions are applied to attributes defined at the user level, and not to attributes defined at the template level. For example, if a query condition specifies users whose expiration date is after 31 July 1999, then users for whom an expiration date has not been specified will *not* be selected, even if their template specifies an expiration date after 31 July 1999.

Query Filter

When you execute a query, the Account Management Client queries the LDAP directory, using a filter constructed from the query. For example, the query shown in FIGURE 4-2 on page 30 becomes the following filter:

```
filter:(&(|(objectclass=fw1person)(objectclass=person)
(objectclass=organizationalPerson)(objectclass=inetOrgPerson))
(|(cn=Brad)(mail=*Andy*)))
```

When the Account Management Client starts and the **Account Management Client** window is first displayed, the entries displayed are those returned by the following query:

```
filter:(|(objectclass=organization)(objectclass=organizationName)
         (objectclass=OrganizationalUnitName)
          (objectclass=organizationalUnit))
```

Also, tree objects specified under **Branches** in the **Account Unit Properties** window (FIGURE 3-3 on page 15) are displayed, even if they do not exist on the LDAP Server.

Note – The query shown in FIGURE 4-2 on page 30 is the default query for the Account Management Client. To modify the default parameters, make changes in the `AMC.properties` file (see "AMC.properties File" on page 72).

objectclass

Users

When a new user is added by the VPN-1/FireWall-1 Account Management Client, or when an existing user is modified, the following objectclasses are added by default:

- objectclass=person
- objectclass=fw1person
- objectclass=organizationalPerson
- objectclass=inetOrgPerson

To modify the default parameters, make changes in the `AMC.properties` file (see "AMC.properties File" on page 72).

Templates

Templates are of the objectclass fw1template.

Groups

Groups are of the objectclass groupOfNames..

Note – The Account Management Client allows you to query and edit groups of the objectclass groupOfUniqueNames created in the Netscape LDAP Server.

LDAP Schema

Proprietary Attributes

OID

Each of the proprietary object classes and attributes (all of which begin with "fw1") has a proprietary Object Identifier (OID), listed below.

TABLE 4-2 Object Class OIDs

object class	OID
fw1template	1.3.114.7.3.2.0.1
fw1person	1.3.114.7.3.2.0.2

The OIDs for the proprietary attributes begin with the same prefix ("1.3.114.7.4.2.0.X"). Only the value of "X" is different for each attribute. The value for "X" is given in the table below.

Attributes

TABLE 4-3 Attributes

attribute	"X" in OID	fw1person	fw1template	default	remarks
cn					The entry's name. In the Account Management Client, this is referred to as "Common Name". For users this can be different from the uid attribute — the name used to login to the VPN/FireWall Module. This attribute is also used to build the LDAP entry's distinguished name, that is, it is the RDN of the DN.
uid					The user's login name, that is, the name used to login to the VPN/FireWall Module. This attribute is passed to the external authentication system in all authentication methods except for "Internal Password", and must be defined for all these authentication schemes. The login name is used by VPN-1/FireWall-1 to search the LDAP server(s). For this reason, each user entry should have its own unique uid value. It is also possible to login to the VPN/FireWall Module using the full DN. The DN can be used when there is an ambiguity with this attribute or in "Internal Password" when this attribute may be missing. The DN can also be used when the same user (with the same uid) is defined in more than one Account Unit on different LDAP Servers.
description				"no value"	Descriptive text about the user.
mail				"no value"	User's email address.
member					An entry can have zero or more values for this attribute. **In a template:** The DN of user entries using this template. DNs that are not users (object classes that are not one of: "person", "organizationalPerson", "inetOrgPerson" or "fw1person") are ignored. **In a group:** The DN of user, group or live template entries that are members of this group.

TABLE 4-3 Attributes (continued)

attribute	"X" in OID	fw1person	fw1template	default	remarks
userPassword					Must be given if the authentication method (fw1auth-method) is "Internal Password". The value can be hashed using "crypt". In this case the syntax of this attribute is: "{crypt}xxyyyyyyyyyy" where "xx" is the "salt" and "yyyyyyyyyy" is the hashed password. It is possible (but not recommended) to store the password without hashing. However, if hashing is specified in the LDAP Server, you should not specify hashing here, in order to prevent the password from being hashed twice. You should also use SSL in this case, to prevent sending an unencrypted password. The VPN/FireWall Module never reads this attribute, though it does write it. Instead, the LDAP bind operation is used to verify a password.

TABLE 4-3 Attributes (continued)

<table>
<tr><th>attribute</th><th>"X" in OID</th><th>fw1person</th><th>fw1template</th><th>default</th><th>remarks</th></tr>
<tr><td>fw1auth-method</td><td>1</td><td>✔</td><td>✔</td><td>"undefined"</td><td>One of the following:
■"S/Key" ■"RADIUS"
■"SecurID" ■"TACACS"
■"OS Password" ■"Defender"
■"Internal Password" ■"undefined"

This default value for this attribute is overridden by Default Scheme in the Authentication tab of the Account Unit window in the VPN-1/FireWall-1 GUI (see "LDAP Account Unit Properties Window — User Preferences Tab" on page 337 of VPN-1/FireWall-1 Administration Guide). For example: an LDAP server can contain LDAP entries that are all of the object-class "person" even though the proprietary object-class "fw1person" was not added to the server's schema. If Default Scheme in the VPN-1/FireWall-1 GUI is "Internal Password", all the users will be authenticated using the password stored in the "userPassword" attribute.</td></tr>
<tr><td>fw1auth-server</td><td>2</td><td>✔</td><td>✔</td><td></td><td>The name of the server that will perform the authentication This field must be given if fw1auth-method is "S/Key" or "RADIUS" or "TACACS". For all other values of fw1auth-method, it is ignored. Its meaning is given below:
<table><tr><th>method</th><th>meaning</th></tr><tr><td>S/Key</td><td>name of the workstation on which the VPN/FireWall Module is installed</td></tr><tr><td>RADIUS</td><td>name of a RADIUS server, a group of RADIUS servers, or "Any"</td></tr><tr><td>TACACS</td><td>name of a TACACS server</td></tr></table></td></tr>
</table>

TABLE 4-3 Attributes (continued)

attribute	"X" in OID	fw1person	fw1template	default	remarks
fw1pwdLastMod	3	✔	✔	If no value is given, then the password has never been modified.	The date on which the password was last modified. The format is `yyyymmdd` (for example, 20 August 1998 is 19980820). A password can be modified using the Account Management Client (see "New User Window - Authentication Tab" on page 45 of *Account Management Client),* or through the VPN/FireWall Module as a part of the authentication process.
fw1Skey-number	4	✔	✔		Length of initial S-Key chain. This attribute is required if the authentication method is S/Key.
fw1Skey-seed	5	✔	✔		The seed from which the S-Key chain was generated (with the addition of a secret). This attribute is required if the authentication method is S/Key.
fw1Skey-passwd	6	✔	✔		The last value of the initial S-Key chain This attribute is required if the authentication method is S/Key.
fw1Skey-mdm	7	✔	✔	MD4	The hash function used by S/Key Valid values are "MD4" and "MD5". This attribute is required if the authentication method is S/Key.
fw1expiration-date	8	✔	✔	"no value"	The last date on which the user can login to a VPN/FireWall Module, or "no value" if there is no expiration date. The format is `yyyymmdd` (for example, 20 August 1998 is 19980820). The default is "no value".
fw1hour-range-from	9	✔	✔	"00:00"	The time from which the user can login to a VPN/FireWall Module. The format is `hh:mm` (for example, 8:15 AM is 08:15).
fw1hour-range-to	10	✔	✔	"23:59"	The time until which the user can login to a VPN/FireWall Module. The format is `hh:mm` (for example, 8:15 AM is 08:15).
fw1day	11	✔	✔	all days of the week	The days on which the user can login to a VPN/FireWall Module. Can have the values "SUN","MON",...*etc*.

TABLE 4-3 Attributes (continued)

attribute	"X" in OID	fw1person	fw1template	default	remarks
fw1allowed-src	12	✔	✔	"no value"	The names of one or more network objects from which the user can run a client, or "Any" to remove this limitation, or "no value" if there is no such client. The names should match the name of network objects defined in VPN-1/ FireWall-1 management station.
fw1allowed-dst	13	✔	✔	"no value"	The names of one or more network objects which the user can access, or "Any" to remove this limitation, or "no value" if there is no such network object. The names should match the name of network objects defined on the VPN-1/ FireWall-1 Management Station.
fw1allowed-vlan	14	✔	✔	"no value"	currently not used
fw1SR-keym	15	✔	✔	"Any"	The algorithm used to encrypt the session key in SecuRemote. Can be "CLEAR", "FWZ1", "DES" or "Any".
fw1SR-datam	16	✔	✔	"Any"	The algorithm used to encrypt the data in SecuRemote. Can be "CLEAR", "FWZ1", "DES" or "Any".
fw1SR-mdm	17	✔	✔	"none"	The algorithm used to sign the data in SecuRemote. Can be "none" or "MD5".
fw1enc-fwz-expiration	18	✔	✔		The number of minutes after which a SecuRemote user must re-authenticate himself or herself to the VPN/FireWall Module.
fw1sr-auth-track	19	✔	✔	"none"	The exception to generate on successful authentication via SecuRemote. Can be "none", "cryptlog" or "cryptalert".
fw1groupTemplate	20	✔	✔	"FALSE"	This flag is used to resolve a problem related to group membership. The group membership of a user is stored in the group entries to which it belongs and not in the user entry itself. Therefore there is no clear indication in the user entry if information from the template about group relationship should be used. If this flag is "TRUE", then the user is taken to be a member of all the groups to which the template is a member. This is in addition to all the groups in which the user is directly a member.

TABLE 4-3 Attributes (continued)

attribute	"X" in OID	fw1person	fw1template	default	remarks
fw1ISAKMP-EncMethod	21	✔	✔	"DES", "3DES"	The key encryption methods for SecuRemote users using IKE[1]. This can be one or more of: "DES", "3DES". A user using IKE may have both methods defined.
fw1ISAKMP-AuthMethods	22	✔	✔	"signatures"	The allowed authentication methods for SecuRemote users using IKE[1]. This can be one or more of: "preshared", "signatures".
fw1ISAKMP-HashMethods	23	✔	✔	"MD5", "SHA1"	The data integrity method for SecuRemote users using IKE[1]. This can be one or more of: "MD5", "SHA1". A user using IKE must have both methods defined.
fw1ISAKMP-Transform	24	✔	✔	"ESP"	The IPSec Transform method for SecuRemote users using IKE[1]. This can be one of: "AH", "ESP".
fw1ISAKMP-DataIntegrityMethod	25	✔	✔	"SHA1"	The data integrity method for SecuRemote users using IKE[1]. This can be one of: "MD5", "SHA1".
fw1ISAKMP-SharedSecret	26	✔	✔		The pre-shared secret for SecuRemote users using IKE[1]. The value can be calculated using the `fw ikecrypt` command line (see "VPN-1 Accelerator Card" on page 57 of *Check Point Account Management Client*).
fw1ISAKMP-DataEncMethod	27	✔	✔	"DES"	The data encryption method for SecuRemote users using IKE[1].
fw1enc-Methods	28	✔	✔	"FWZ"	The encryption method allowed for SecuRemote users. This can be one or more of: "FWZ", "ISAKMP" (meaning IKE).

1. IKE was formerly known as ISAKMP or ISAKMP/OAKLEY.

CHAPTER 5

User Management

In This Chapter

Managing Users

You can manage users from the **Account Management** window (FIGURE 5-1 on page 42). In addition, you can query the Account Unit to display the entries in which you are interested (see Chapter 4, "Queries" for information about queries).

In This Section

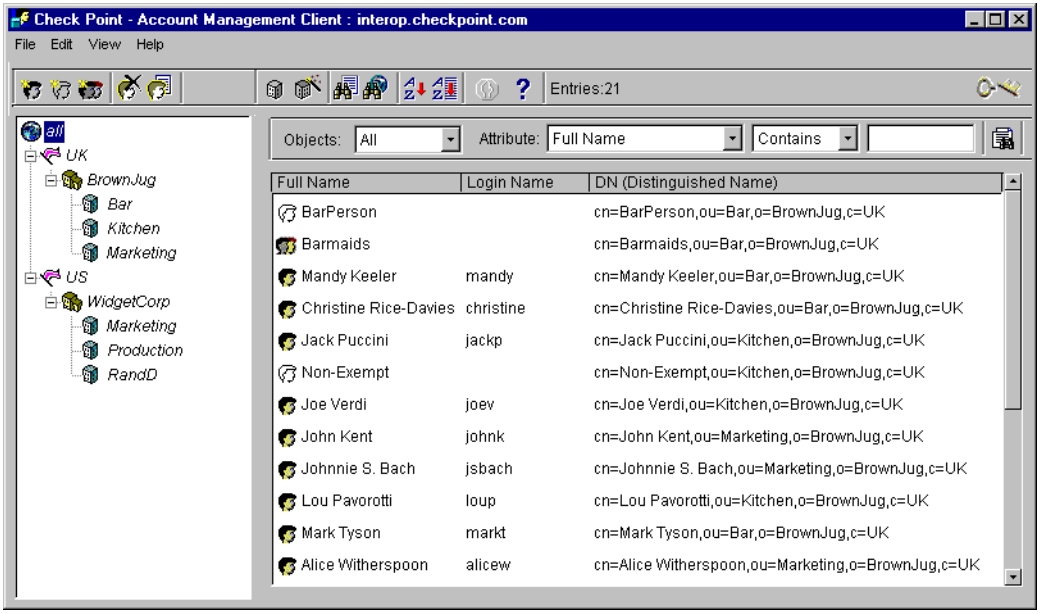


FIGURE 5-1 Account Management window

Creating a User

To create a new user, click on  in the toolbar, or select **New User** from the **File** menu. The **New User** window (FIGURE 5-3 on page 44) is displayed. Enter the relevant information on the different tabs.

You can choose to let the new user inherit data from a template by specifying the name of the template on the **Identification** tab (FIGURE 5-3 on page 44) and checking **From Template** in each of the other tabs.

Modifying a User

To modify a user, proceed as follows:

1 Select the user in the list on the right side of the screen.

2 Do one of the following:

- click on  in the toolbar, *or*
- select **Properties** from the **File** menu, *or*
- right-click on the entry and select **Edit Properties** from the menu.

FIGURE 5-2 Object Menu

3 Open the relevant tab and make the changes.

If you change the template to which a user is attached, and the new template requires more information, the user information will be incomplete, and you must review all the tabs to enter the correct information for the user.

For example, if a user was attached to a template whose authentication method is OS Password, and you attach the user to a template whose authentication method is S/Key, the required information for the user will not be defined. In this case, you must add the required information to the tab.

Deleting a User

To delete a user, proceed as follows:

1 Select the user in the list on the right side of the screen.

2 Click on  in the toolbar or select **Delete** from the **File** menu or right-click on the entry and select **Delete Entry** from the menu.

New User Window — Identification Tab

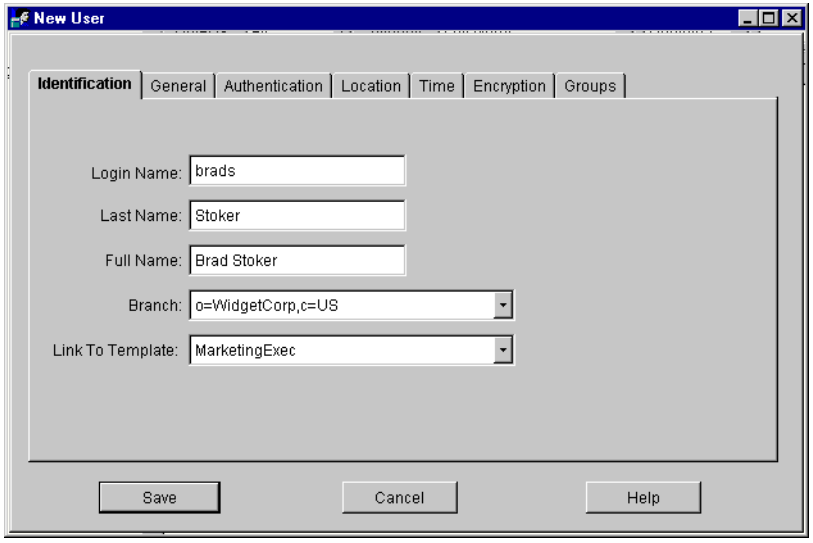


FIGURE 5-3 New User window — Identification tab

Login Name — the user's login name

Warning – You must not define more than one user with the same uid (login name) in the same branch.

Last Name — the user's last name (surname or family name)

This field is required only if schema checking is on in the LDAP Server. For more information about schema checking, see "Schema Checking" on page 189 of *VPN-1/FireWall-1 Administration Guide*.

Full Name — the user's full name, including the last name (surname)

Branch — the branch in the tree in which the user is situated

The default is the branch currently selected in the tree on the left part of the window. You can select another branch from the drop-down menu.

Link to Template — the template (if any) to which the user's definition is linked.

The linkage is "live," that is, changes to the template are reflected in all the users linked to the template.

New User Window — General Tab

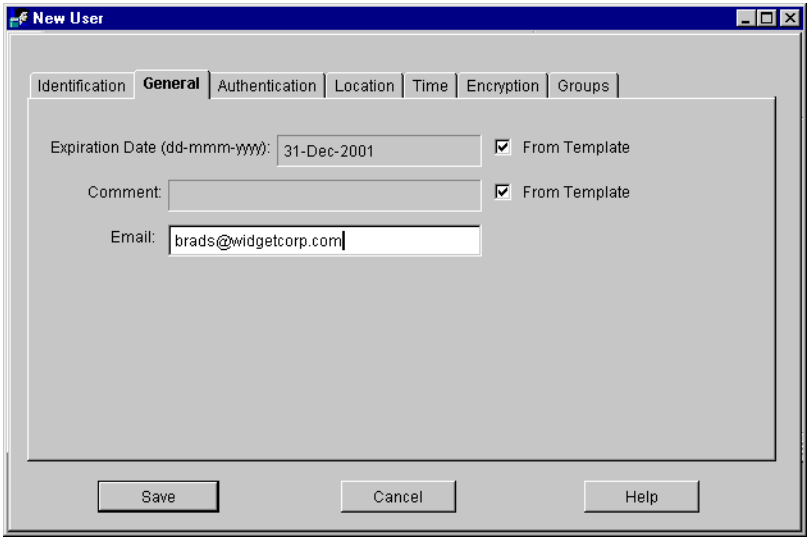


FIGURE 5-4 New User window — General tab

Expiration Date — the date after which this user definition is no longer valid.

If **From Template** is checked, this field is taken from the template given in the **Link to Template** field in the **Identification** tab of the **New User** window (FIGURE 5-3 on page 44).

Comment — descriptive text

If **From Template** is checked, this field is taken from the template given in the **Link to Template** field in the **Identification** tab of the **New User** window (FIGURE 5-3 on page 44).

Email — the user's email address

To enter more than one email address, separate them with the ";" character. For example, if the user has two email addresses: "joe@bigcorp.com" and "joe@coldmail.com", enter "joe@bigcorp.com;joe@coldmail.com". Each email address will be saved as a separate value.

New User Window — Authentication Tab

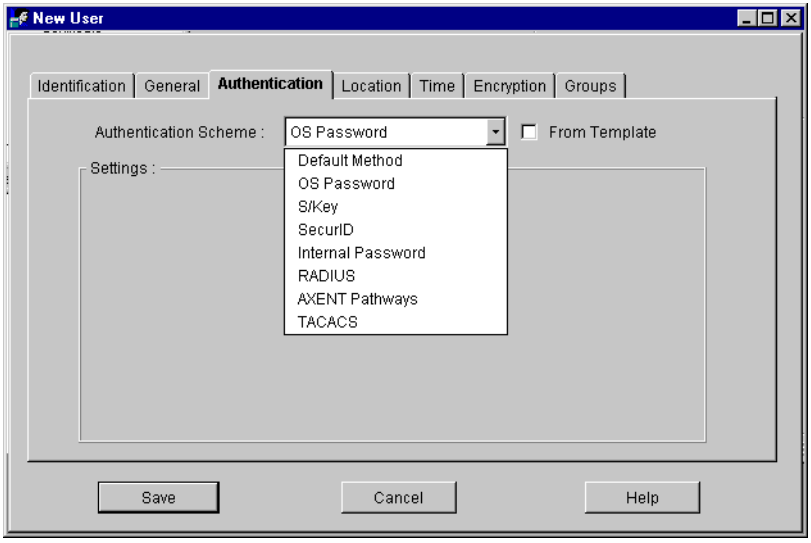


FIGURE 5-5 New User window — Authentication tab

Authentication Scheme — the scheme that will be used to authenticate this user

If **From Template** is checked, this field is taken from the template given in the **Link to Template** field in the **Identification** tab of the **New User** window (FIGURE 5-3 on page 44).

Select a scheme from the drop down list. For some of the schemes, additional data is required. After you select one of these schemes, the contents of the window change and the required fields are displayed.

- **Default Method** — The authentication method used for this user is the one specified in **Default Scheme** in the **Authentication** tab of the **Account Unit** window in the VPN-1/FireWall-1 GUI.
- **OS Password** — The user is challenged to enter his or her OS password.
- **S/Key** — The user is challenged to enter the value of requested S/Key iteration.

  A user whose authentication scheme is S/Key can be authenticated only on one gateway. See “S/Key” below for an explanation of how to define S/Key authentication.
- **SecurID** — The user is challenged to enter the number displayed on the Security Dynamics SecurID card.

- **Internal Password** — The user is challenged to enter his or her VPN-1/FireWall-1 password on the gateway.

  The advantage of an internal password over a OS password is that a user does not require an OS account on the gateway to use an internal password.
- **RADIUS** — The user is challenged for the response, as defined by the RADIUS server.
- **AXENT Pathways** — The user is challenged for the response, as defined by the AXENT Pathways server.
- **TACACS** — The user is challenged for the response, as defined by the TACACS server.

S/Key

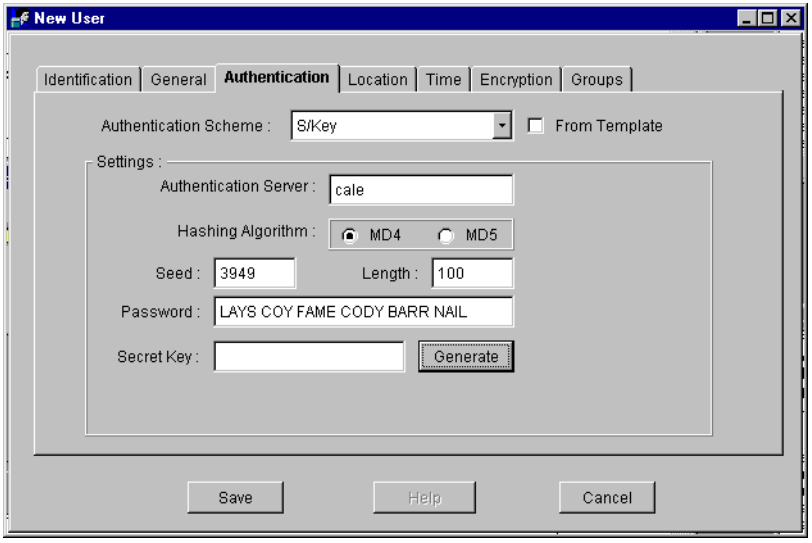


FIGURE 5-6 New User window — S/Key Authentication

The meaning of the fields in this window is as follows:

Authentication Server — the server that will authenticate the user

Seed — a random number

The Account Management Client suggests a 4-digit random seed, but you can change it.

Password — This is computed by the Account Management Client after you enter **Secret Key** and click on **Generate**.

Alternatively, you can enter **Password** manually.

Length — number of iterations

Secret Key — chosen by the user

Secret Key should be at least 10 characters long.

There are several options for using the S/Key Authentication window, as follows:

To Generate and Save a Sequence of Passwords

1. Enter **Seed**, **Secret Key**, and **Length**.

   Secret Key should be at least 10 characters long.

2. Click on **Generate**.

If the User Already Has Prepared a Sequence of Passwords

1. Enter **Seed**, **Length** (the number of the last password used), and last-used **Password**.

2. *Do not* click on **Generate**.

   The S/Key password is saved. If **Seed** and **Length** are not entered, the user is prompted for them.

New User Window — Location Tab

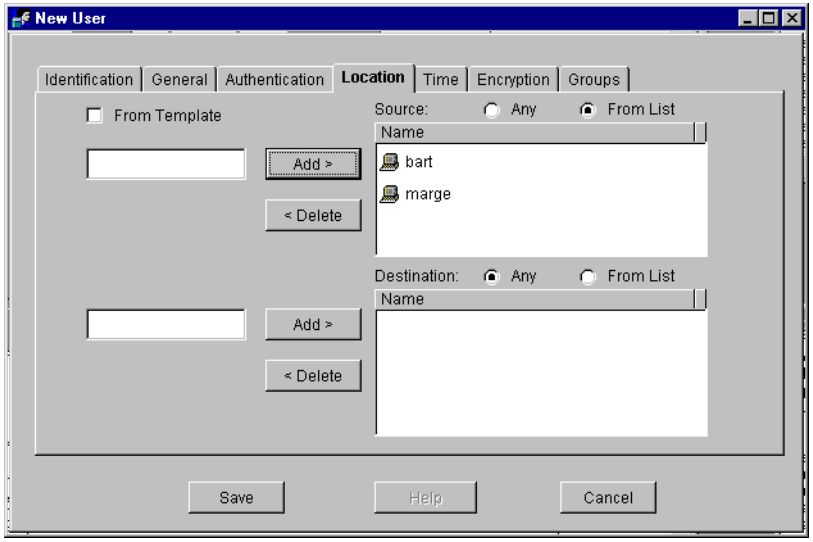


FIGURE 5-7 New User window — Location tab

The **Location** tab specifies the allowed sources and destinations for the user.

If **From Template** is checked, this information is taken from the template given in the **Link to Template** field in the **Identification** tab of the **New User** window (FIGURE 5-3 on page 44).

Source

The upper part of the tab specifies the allowed sources. If **Any** is checked, then there is no restriction on the user's source. If **From List** is checked, then the user is allowed to connect only from the listed hosts.

To add a host to the list of allowed hosts, enter its name (not its IP address) in the text box to the left of the list and click on **Add**. The object must be defined in the VPN-1/FireWall-1 database as a network object. To delete a host from the list, select it in the list and click on **Delete**.

Note – The VPN-1/FireWall-1 Policy Editor will ignore the defined sources if **Intersect with user database** is disabled in the **General** tab of the **Client Authentication Action Properties** window (see Chapter 15, "Authentication" in *Check Point VPN-1/FireWall-1 Administration Guide*).

Destination

The upper part of the tab specifies the allowed destinations. If **Any** is checked, then there is no restriction on the user's destination. If **From List** is checked, then the user is allowed to connect only to the listed hosts.

To add a host to the list of allowed hosts, enter its name (not its IP address) in the text box to the left of the list and click on **Add**. The object must be defined in the VPN-1/FireWall-1 database as a network object. To delete a host from the list, select it in the list and click on **Delete**.

Note – The VPN-1/FireWall-1 Policy Editor will ignore the defined destinations if **Intersect with user database** is disabled in the **General** tab of the **Client Authentication Action Properties** window (see Chapter 15, "Authentication" in *Check Point VPN-1/FireWall-1 Administration Guide*).

New User Window — Time Tab

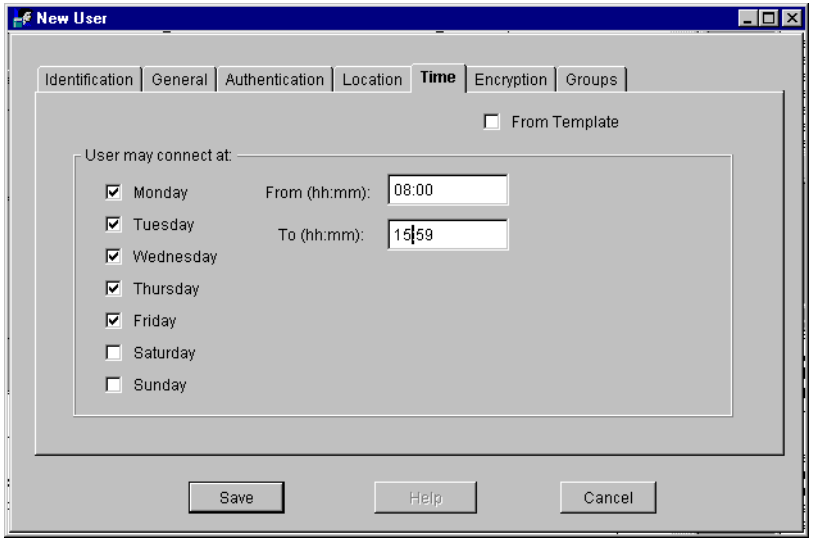


FIGURE 5-8 New User window — Time tab

The **Time** tab specifies the days of the week and the times of day that the user is allowed to connect.

If **From Template** is checked, this information is taken from the template given in the **Link to Template** field in the **Identification** tab of the **New User** window (FIGURE 5-3 on page 44).

Check the days of the week on which the user is allowed to connect.

Specify a time period, between **From** and **To**, during which the user is allowed to connect.

New User Window — Encryption Tab

The **Encryption** tab specifies the encryption and data integrity methods for Client Encryption (SecuRemote) for the user. If **From Template** is checked, this information is taken from the template given in the **Link to Template** field in the **Identification** tab of the **New User** window (FIGURE 5-3 on page 44).

There are two tabs within the **Encryption** tab: one for FWZ and one for IKE.

Note – From Template applies to both **Encryption** tabs.

FWZ Encryption (for SecuRemote Users)

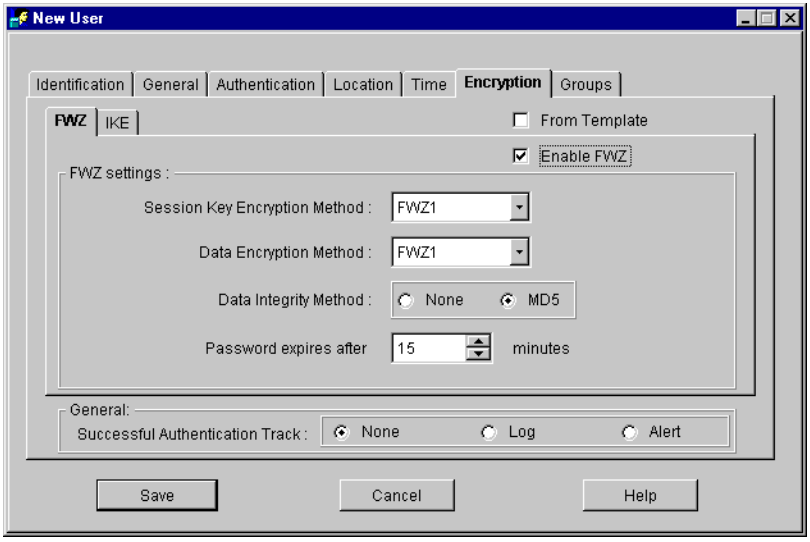


FIGURE 5-9 New User window — FWZ Encryption tab

Session Key Encryption Method — the encryption algorithm for session keys

The available choices depend on the encryption algorithms installed.

Note – You cannot choose an encryption method if your VPN/FireWall module does not support it.

You can also choose **Clear** (meaning no encryption) or **Any** (meaning the session key encryption method is chosen by the other party).

Data Encryption Method — the encryption algorithm for communications packets

The available choices depend on the encryption algorithms installed.

You can also choose **Clear** (meaning no encryption) or **Any** (meaning the data encryption method is chosen by the other party).

Data Integrity Method —the cryptographic checksum method to be used for ensuring data integrity

General — In **Successful Authentication Track**, choose one of the following:

- **None** — no logging or alerting
- **Log** — log the event
- **Alert** — issue an alert

IKE Encryption (for SecuRemote Users)

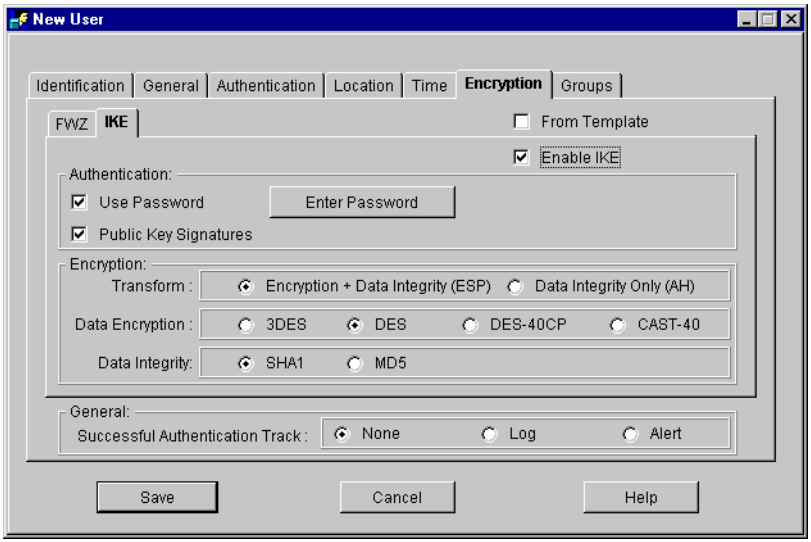


FIGURE 5-10 New User window — IKE Encryption tab

Authentication — Choose one or both of the following:

- **Use Password** — The user authenticates himself or herself using a password.

  If you select this authentication method, then click on **Enter Password** to display the **IKE Password** window (FIGURE 5-11 on page 54) so that you can enter the password, which is stored on the LDAP server in encrypted form.

  For more information, see “IKE Password Window” on page 54.

- **Public Key Signatures** — The user authenticates himself or herself using a certificate.

Encryption — Select **Transform**, **Data Encryption Method** and **Data Integrity Method**.

Transform — Choose one of the following:

- **Encryption + Data Integrity (ESP)** — The Security Association will include both encryption and data integrity (authentication).
- **Data Integrity Only (AH)** — The Security Association will include only data integrity (authentication).

Data Encryption Method — the encryption algorithm for communications packets (available only if **Encryption + Data Integrity (ESP)** is chosen)

The available choices depend on the encryption algorithms installed.

Choose one of the available algorithms. You should choose one of the algorithms available to the SecuRemote Client. If you choose an algorithm stronger than any of those available to the SecuRemote Client, the connection will fail.

The algorithms available on the SecuRemote Server depend on the VPN-1/ FireWall-1 software version and license.

The algorithms available on the SecuRemote Client depend on the SecuRemote Client software version. To see which versions are available on the SecuRemote Client, select **About** from the SecuRemote Client's **Help** menu.

TABLE 5-1 lists the available methods on the Client.

TABLE 5-1 Client About SecuRemote window text and encryption methods

text in About box	available encryption algorithms
Export	40 bit algorithms (CAST-40 and DES-40CP)
DES	DES (in addition to those listed under Export)
Strong	3DES (in addition to those listed under DES and Export)

Data Integrity Method —the cryptographic checksum method to be used for ensuring data integrity

General — In **Successful Authentication Track**, choose one of the following:

- **None** — no logging or alerting
- **Log** — log the event
- **Alert** — issue an alert

IKE Password Window

FIGURE 5-11 IKE Password window

New Password — Enter the password.

Re-enter Password — Confirm the password by entering it again.

Key for Encrypting Password — Enter the key to be used to encrypt users' IKE pre-shared secrets on the LDAP server.

This field corresponds to the **IKE Key** field in the **Encryption** tab of the **LDAP Account Unit Properties** window in the VPN-1/FireWall-1 GUI.

Key for Encrypting Password is the same for all users on an Account Unit (even though it is defined in a **User Properties** window). You define this only once. Once it is defined, it appears as the default value for all other users when you open their **IKE Password** windows.

An exception to this is the following scenario: Suppose you have defined two Account Units in VPN-1/FireWall-1. Then, you start the Account Management Client directly (that is, not from within VPN-1/FireWall-1) and define an Account Unit that includes the two Account Units you defined in VPN-1/FireWall-1. Each of the VPN-1/FireWall-1 Account Units will have a different **IKE Key** field, so in the Account Management Client, you must then specify different **Key for Encrypting Password** fields for different users, depending on the VPN-1/FireWall-1 Account Unit on which each user is defined. To avoid this complication, you should define the same Account Units both in VPN-1/FireWall-1 and in the Account Management Client.

Re-enter Key for Encrypting Password — Confirm the key by entering it again.

Key Last Used for Branch — The last used branch is shown here.

This field is useful when you are defining users in different branches, where each branch is a separate VPN-1/FireWall-1 Account Unit and may have different keys for encrypting IKE passwords. See “Key for Encrypting Password” on page 54 for more information.

New User Window — Groups Tab

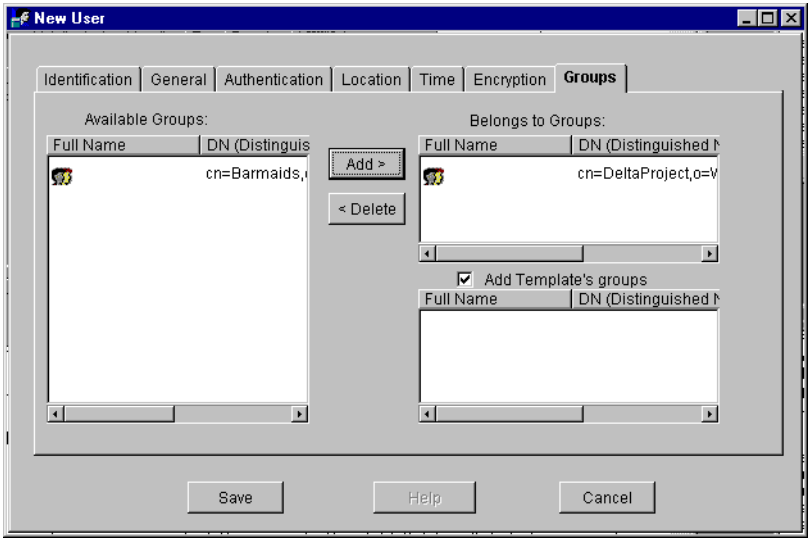


FIGURE 5-12 New User window — Groups tab

The **Groups** tab lists the groups to which the user belongs.

To add the user to a group, select the group in the left list box (labeled **Available Groups**) and click on **Add**.

Alternatively, you can do this using the Group window (see “Changing a Group” on page 59).

To delete the user from a group, select the group in the right list box (labeled **Belongs to Group**) and click on **Delete**.

Alternatively, you can do this using the Group window (see “Changing a Group” on page 59.

If you check **Add Template’s Groups**, then the user is *also* added to all the groups defined in the template given in the **Link to Template** field in the **Identification** tab of the **New User** window (FIGURE 5-3 on page 44).

Templates

A definition of a user can be based on a template from which the user will inherit properties. In VPN-1/FireWall-1 Account Management, a template is “live,” that is, changes made to a template are applied to all users who continue to inherit at least some of their properties from the template.

In This Section

Creating a Template

To create a new template, click on  in the toolbar, or select **New Template** in the **File** menu. The **New Template** window is displayed.

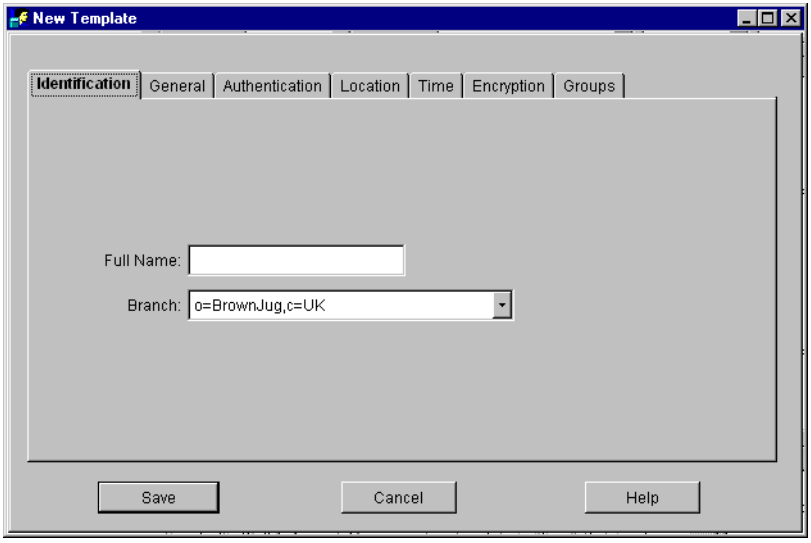


FIGURE 5-13 New Template window — Identification tab

The tabs and fields of the **New Template** window correspond to those of the **New User** windows, except for the following:

- There is no **Link to Template** field in the **Identification** tab.
- There are no **From Template** fields in the other tabs.
- There are no user-specific fields, such as **Email** (FIGURE 5-4 on page 45).

The link between a template and the users whose definitions are linked to the template is a live link, that is, any changes made to the template are made to the users as well, to the fields on those tabs for which the **From Template** field is checked in the user's definition.

Changing a Template

To change a template, proceed as follows:

1. Select the template in the list on the right side of the screen.
2. Click on  in the toolbar or select **Properties** from the **File** menu.
3. Open the relevant tab and make the changes.

   When you modify a template, all the users attached to the template are modified accordingly. If the modified template requires more information, the user's data will be incomplete. For example, if a user was attached to a template whose authentication method is OS Password, and you changed the authentication method to S/Key, the necessary information will not be defined for the user. In this case, you must add the required information for all the users affected by the change in the template.

Deleting a Template

To delete a template, proceed as follows:

1. Select the template in the list on the right side of the screen.
2. Click on  in the toolbar or select **Delete** from the **File** menu.

   When you delete a template, all the users attached to the template are detached and are no longer attached to any template.

Groups

In This Section

Creating a Group

To create a new group, click on  in the toolbar, or select **New Group** from the **File** menu. The **New Group** window is displayed.

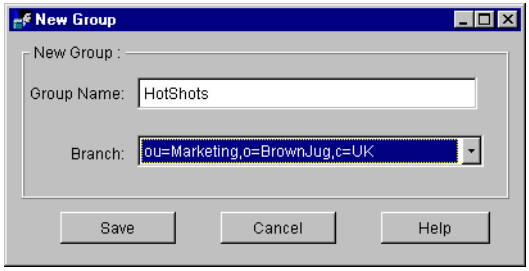


FIGURE 5-14 New Group window

1. Enter a **Full Name** for the group.
2. Enter a **Branch** for the group.
3. Click on **Save**.
4. Add members to the group by selecting them from the list on the left (FIGURE 5-15) and clicking on >>.
5. You can delete a member from the group by selecting the member in the list on the right and clicking on <<.

A group's DN is of the form "cn=*Full Name*, ou=*Branch*. For example, the group defined in FIGURE 5-14 has a DN of "cn=HotShots,ou=Marketing,o=BrownJug,c=UK".

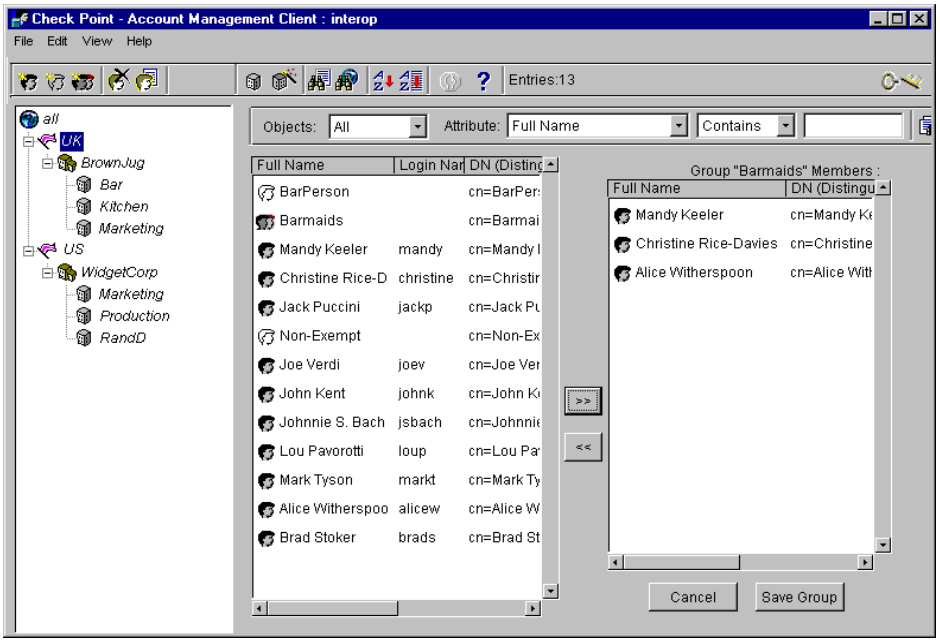


FIGURE 5-15 Adding Members to a Group

Changing a Group

To change a group, proceed as follows:

1. Select the group in the list on the right side of the screen.
2. Click on  in the toolbar or select **Properties** from the **File** menu.
3. Add members to the group by selecting them from the list on the left (FIGURE 5-15) and clicking on  .

   To select all the entries in a column, use Ctrl-A.

Deleting a Group

To delete a group, proceed as follows:

1. Select the group in the list on the right side of the screen.
2. Click on  in the toolbar or select **Delete** from the **File** menu.

   To select all the entries in a column, use Ctrl-A.

CHAPTER 7

Troubleshooting

In This Chapter

Error Messages

TABLE 7-1 lists the Account Management Client error messages.

TABLE 7-1 Account Management Client Error Messages

Error Number	Meaning	Course of Action
1	LDAP Server internal error.	
2		
3	Time limit (default 3600 milliseconds) exceeded.	
4	Size limit exceeded.	Use a more restrictive query or increase size limit (**Size Limit** on the **Edit** menu).
5		
6		
7	Strong authentication not supported.	
8	Strong authentication required.	Try again using SSL.
9	Partial results returned.	

TABLE 7-1 Account Management Client Error Messages (continued)

Error Number	Meaning	Course of Action
16	No such attribute — attempt to read or write an attribute not supported by the LDAP Server.	Add the VPN-1/FireWall-1 (fw1 prefix) attributes to the schema supported by the LDAP Server or turn schema checking off.
20	Client synchronization problem — two Clients are attempting to update the same entry at the same time.	Requery, refresh and update again.
21	Invalid syntax in free form query.	Correct the syntax.
32	Client synchronization problem — a Client is attempting to access an entry deleted by another Client.	Requery.
33	Alias problem — the VPN-1/FireWall-1 Client does not search for aliased objects.	
34	Invalid Full Name, for example: "Full Name: Norma+Baker"	Change to the form: Baker+lastName=Norma
70	Too many entries returned by query.	Use a more restrictive query.
87	Invalid syntax in free form query.	Correct the syntax.
90	Out of memory.	Make more memory or more disk space available on the LDAP Server.

Configuration

AMC.properties File

This file is created when the Account Management Client is installed and should be modified only when needed. TABLE 7-2 lists the more important parameters in the file.

TABLE 7-2 AMC.properties file parameters

parameter	meaning
`AddUserDefaultOC`	If `TRUE`, add the object classes defined under `UserDefaultOC` to users edited with the Account Management Client, when those object classes are missing from the user's definition (this can happen if the user was created by another LDAP Client).
`UserDefaultOC`	See "AddUserDefaultOC" above.
`GroupRequiresMember`	If `TRUE`, a dummy member is added to a newly-defined group which would otherwise be empty.
`OrganizationUnitOC`	A list of the non-leaf elements to be displayed in the tree at the left hand side of the Account Management Client window (FIGURE 3-7 on page 22).

Index