What is SecureManager?

The SecureManager application is part of Cylink's SecureLAN™ and SecureWAN™ families of products. Used in conjunction with SecureDomain Units (SDUs), SecureManager safeguards LAN and WAN communications using state-of-the-art cryptographic technologies, including DSS digital signatures for authentication, Diffie-Hellman public key management, high speed encryption, challenge numbers, and packet-by-packet initialization vectors.

SecureManager is a tool for implementing security policies between IP or IPX networks, between IP subnets, and between specifically designated IP address ranges, authenticating source and destination addresses and dynamically encrypting network traffic.

Securing Your LAN and WAN Traffic with SecureManager

First, you determine a security policy for each set of addresses (whether network, subnet, or range) to be secured. These policies determine whether network traffic is passed in the clear, encrypted and decrypted, or blocked altogether.

Once you have assigned your subnets and defined your security policies, you draw a map of your network by dragging and dropping graphical objects onto the Network Map in the SecureManager graphical user interface (GUI).

After you place objects on the map, you configure network security by assigning security policies to objects on the Network Map. Once your security polices are configured, whenever traffic passes between Secure Domains, the data must pass through an SDU, which intelligently applies the configured security policy.

As your network evolves, the addresses you secure and their security policies can easily be updated. SecureManager brings integrated and comprehensive security management to the enterprise-wide internetwork, remotely configuring, monitoring and performing software downloads for Cylink SDUs.

Features and Benefits

Networks Supported

- IP Class A, B, and C (TCP, UDP)
- IPX

Industry-standard Platform and Network Management Protocol

SecureManager runs under the Sun Solaris™ operating system and is integrated with the HP OpenView™network management software.

SecureManager uses a secure form of the industry-standard SNMP (Simple Network Management Protocol) v1 protocol when communicating with SDUs—eliminating the possibility of spoofing or eavesdropping. Cylink's enterprise security products use industry-standard as well as proprietary MIBs. Other SNMP-based systems can query, get or set values for non-secured MIB objects (MIB II objects and other standard MIBs) from Cylink secure devices. However, since all security-related operations use Cylink proprietary secured MIB objects, these operations are executed only through SecureManager's secure SNMP protocol.

Complete, Hacker-proof Security and Protection

- Automatic support for digital certificate authentication using DSS
- Diffie-Hellman public key exchange
- DES encryption

Fool-proof authentication procedures prevent unauthorized products from being installed or from masquerading as legitimate devices.

Ease and Flexibility in Assigning Security Policies

The network administrator can create security policy definitions using SecureManager's graphical user interface. With the map-like representation of the network topology, visualizing the network security structure is easy. This simplifies configuring, managing and modifying network security.

Complete Audit Trail

SecureManager can periodically poll each secure device and maintain a complete audit trail of network security management activities, including every administrator operation, user login and/or logout, database incident, and SNMP trap or alarm.

Scalable

- Capable of managing hundreds of SDUs.
- With automatic key generation, as the network grows, security policy changes are easy to manage; major upgrades are unnecessary.

System Requirements

Hardware Requirements

The SecureManager requires the following hardware:

- Sun SPARCstation 5 or 20, or equivalent
- 64 MB RAM
- 250 MB of free disk space recommended
- Color monitor; minimum 17-inch screen recommended
- CD-ROM drive
- Ethernet adapter for network connection
- 3.5-inch floppy disk drive for loading manufacturing certificates and private keys
- Recommended: magnetic tape drive for periodic database backup

NOTE SecureManager does not support the graphics card "cgthree."

Software Requirements

The SecureManager application is published on a CD-ROM disk. On the same disk, a runtime version of Informix 7.10 SE is included. Each SecureManager is shipped with an essential, customer-specific set of four diskettes that contain the SecureManager manufacturing certificate (including the public key) and the SecureManager private key.

The SecureManager application requires the following additional software that is not included on the Cylink CD-ROM disk:

- Sun Solaris UNIX operating system version 2.4 or later
- Hewlett-Packard OpenViewnetwork management software, version 3.3, 4.0, or 4.11 (must include SNMP platform for version 3.3), for Sun/Solaris.

NOTE An internal problem in HP OpenView, Version 4.1, makes it incompatible with SecureManager. The defect was fixed in HP OpenView, Version 4.11. Please upgrade to Version 4.11. Refer to the HP OpenView documentation for the upgrade procedure.

See Appendix A, *Installing SecureManager Software,* for installation instructions.

SecureLAN Products and Concepts

Using SecureDomain Units and the SecureManager application, you can secure your LAN traffic by assigning policies for communications between Entities (networks, subnets, or address ranges). You can also secure IP WAN traffic on public or private networks.

Some terms to become familiar with are *SDU (SecureDomain Unit), Secure Domain, Entity, protected Entity, Secure Group,* and *Secure Group member role.*

SecureDomain Unit (SDU)

Cylink's SecureDomain Unit, or *SDU,* is a standalone hardware device that protects information by securing the data communicated to and from network devices installed behind it. Data communications can use IP or Novell IPX protocols and can be secured via encryption and access control or allowed to pass in the clear.

After an SDU is installed, SecureManager is used to specify which networks or address ranges (Entity definitions) to secure by defining security rules for communications between Entities. This process is referred to as *defining a security policy* for the SDU and the network it protects.

The SDU then functions like a guard at a gate, determining which traffic may pass and under which conditions. The SDU uses its stored security policy to determine what it selectively passes in the clear, encrypts and decrypts, or blocks altogether: it determines which communications packets go through the gate and how, depending on both source and destination of those packets. Therefore, SDUs must be installed at locations that intercept all network communications intended for the protected (secured) network devices.

SecureManager uses secure SNMP messages to configure , reconfigure, and monitor SDUs. SecureManager also generates digital certificates for authenticating each SDU before it becomes operational.

Secure Domain

A *Secure Domain* is a network (or part of a network) that is located entirely behind an SDU. It can include one or more networks, subnetworks, or hosts (all referred to as *Entities*) physically located behind one (and only one) SecureDomain Unit (SDU). A Secure Domain could be an entire site or one server. Data cannot enter or exit a Secure Domain without traversing through a SecureDomain Unit. With all network traffic passing through an SDU, the networked devices behind it reside within a Secure Domain.

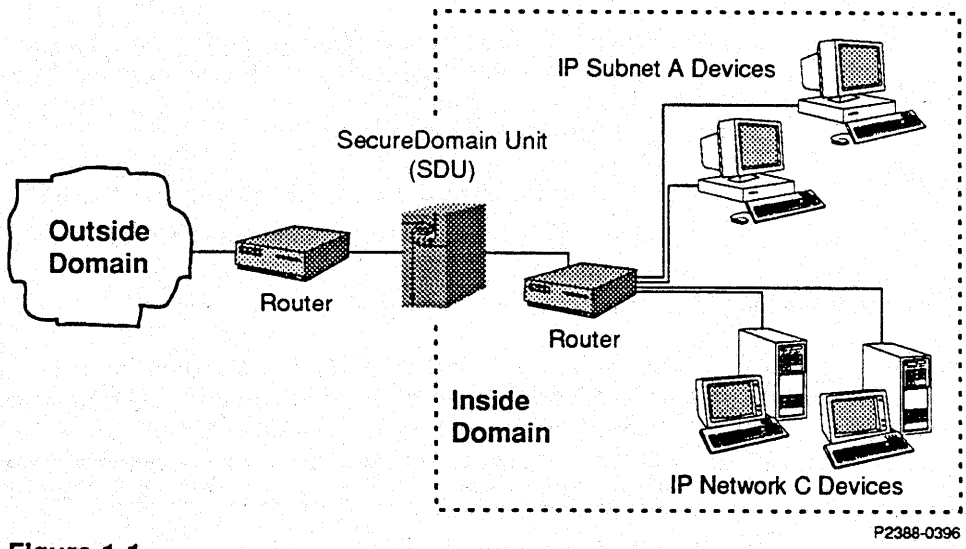


Figure 1-1
SecureDomain Unit and Its Secure Domain

The Secure Domain is a core part of the SecureManager framework that is used in setting security/communications policies via Entities, Secure Groups, and roles within the Secure Groups. In addition, policies are assigned to the SDU itself. These policies govern communications between unprotected devices.

NOTE SecureManager does not secure traffic between Entities in the same Secure Domain.

CAUTION SecureManager and SDU functionality require all network traffic from any node within a Secure Domain to pass through the SDU. Therefore, correct SDU placement is critical. If any traffic can exit its Secure Domain without passing through an SDU, the network cannot be secured as described in this manual.

Entity

Within SecureManager, the Entity concept represents the set of devices to which a set of security policies applies uniformly—the finest granularity available with SecureDomain Units. Each Secure Domain can contain one or many Entities. Any single address can be part of just one Entity. All network nodes (hosts) in a given Entity must share the same protocol.

In networks running under IP protocols (class A, B, or C only), an Entity consists of a (continuous) range of IP network addresses, an IP subnet, or an entire IP network.

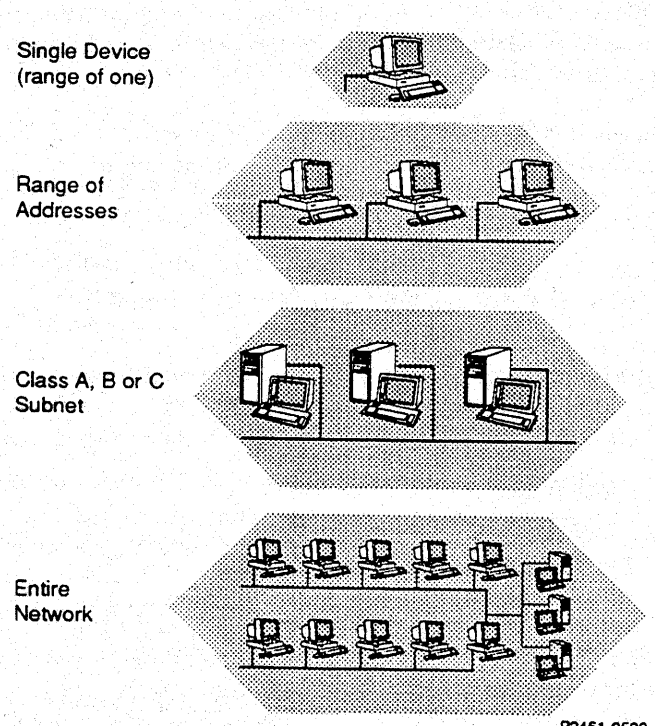


Figure 1-2
Examples of IP Entities

Within an Entity:

- All IP addresses or nodes share the same network address.
- All nodes share the same subnet or network mask.

In networks running under IPX protocols, an Entity consists of all the network devices that share a common network address.

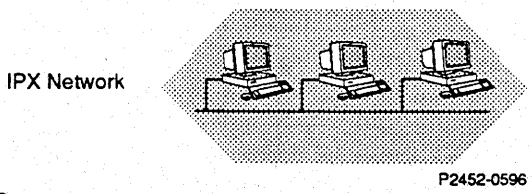


Figure 1-3
IPX Entity

Protected Entity

An Entity is *protected* when all communications to and from it must pass through an SDU (it resides within a Secure Domain) *and* it belongs to at least one Secure Group.

The graphical representation—*icon*—for an Entity shown in the SecureManager user interface and in this manual is a flattened hexagon.

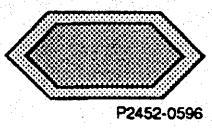


Figure 1-4
Entity Icon

The SDU enforces the Entity and Secure Group security/communications policies when data is sent between SDUs (from one Secure Domain to another).

If an Entity resides outside a Secure Domain, it cannot be protected—it cannot belong to a Secure Group.

The icon for an SDU in the application interface and in this manual looks like a house lying on its side. The pointed side of the SDU icon points towards network addresses that lie outside the Domain. The Secure Domain and its protected (and inside unprotected) Entities reside behind the SDU icon's flat side.

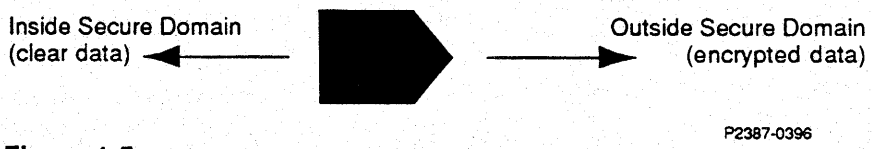


Figure 1-5
SDU Icon

Secure Group

A Secure Group consists of a set of Entities with an assigned internal communications policy that applies to all inter-Domain traffic between members. The membership consists of two or more member Entities (networks, subnets, or address ranges) that reside in at least two different Secure Domains.

When you create a Secure Group in SecureManager, you assign a communications/security (*Internal Packet Handling*) policy (either *Pass* all frames in the clear, *Block* all frames, or *Encrypt* all frames) that applies to all inter-Domain traffic between any two Entities that belong to the Secure Group. This policy assignment effectively determines which (and how) devices in different networks and subnets communicate across the network. Intra-domain communications (between groups or members in the same domain) is not part of the security policy in the SDU.

A Secure Group (with an assigned communications policy of *encrypt*) is the construct within SecureManager that enables encryption. Encryption and decryption occur only between two members of a Secure Group.

Part of the Secure Group definition is the protocol shared by all Entities that belong to the Group—IP and IPX Entities cannot belong to the same Secure Group.

Secure Groups provide the means for certain addresses comprising a local Entity to have their own security policy when communicating with certain addresses (another Entity) that reside in another Secure Domain.

The SDU supports the following types of different network protocols for Secure Groups:

- IP/IP (TCP/IP protocol stack, IP protocol)
- IP/TCP (TCP/IP protocol stack, TCP protocol)
- IP/UDP (TCP/IP protocol stack, UDP protocol)
- IPX (Novell/IPX protocol stack, IPX protocol)
- NCP (Novell/IPX protocol stack, NetWare Core Protocol)
- PEP/NetBIOS (Novell/IPX protocol stack, PEP subprotocol or NetBIOS encapsulated in IPX subprotocol)
- SPX (Novell/IPX protocol stack, Sequenced Packet Exchange protocol)

NOTE The IPX subprotocols are relevant only when defining a new IPX-type Secure Group, and are used to more narrowly define the IPX subprotocol to be used in the Secure Group.

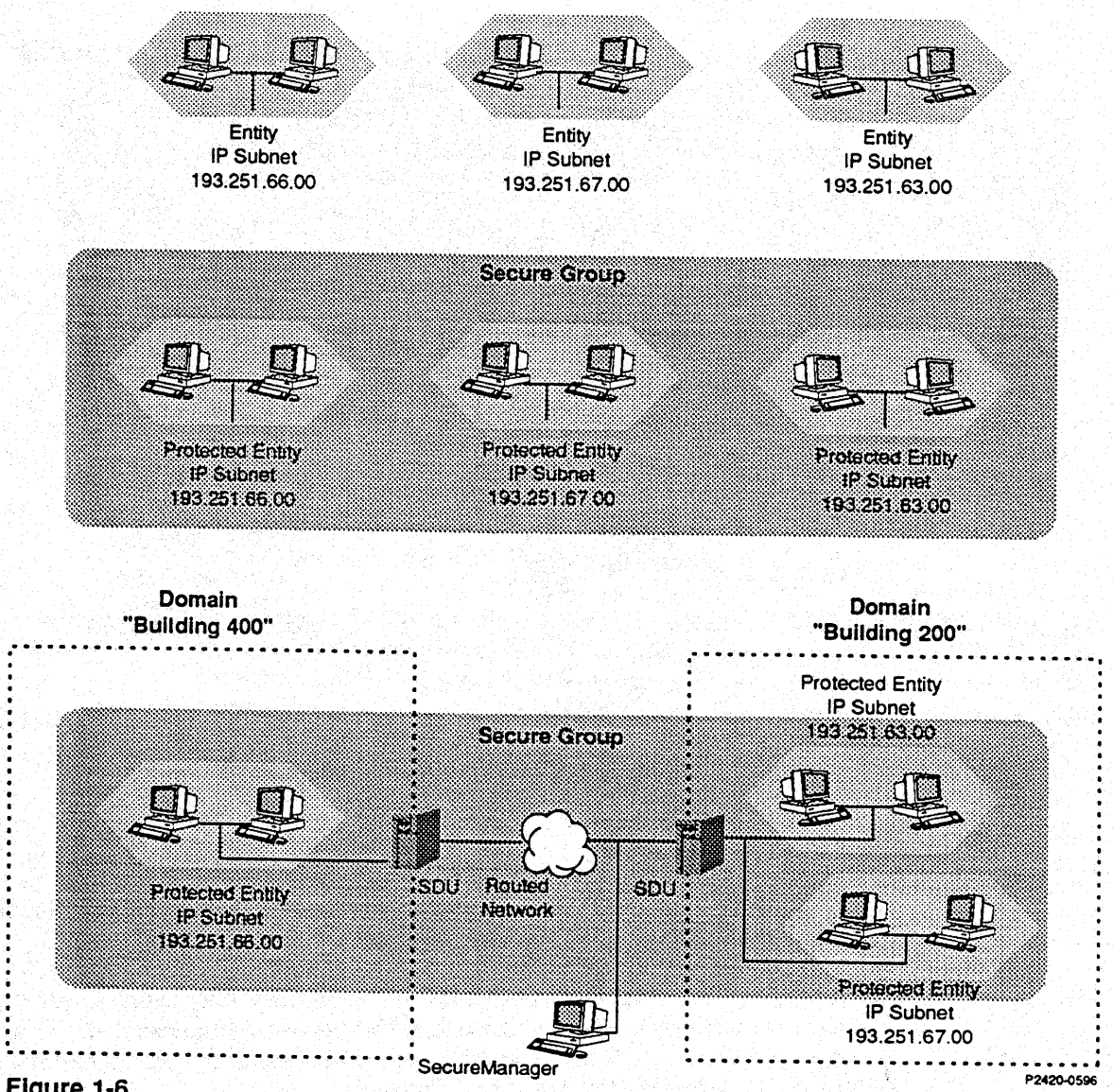


Figure 1-6
Entities, a Secure Group, and Secure Domains

Top: Three Entities
Middle: A Secure Group of Three Entities
Bottom: A Secure Group Consisting of Three Entities in Two Different Secure Domains

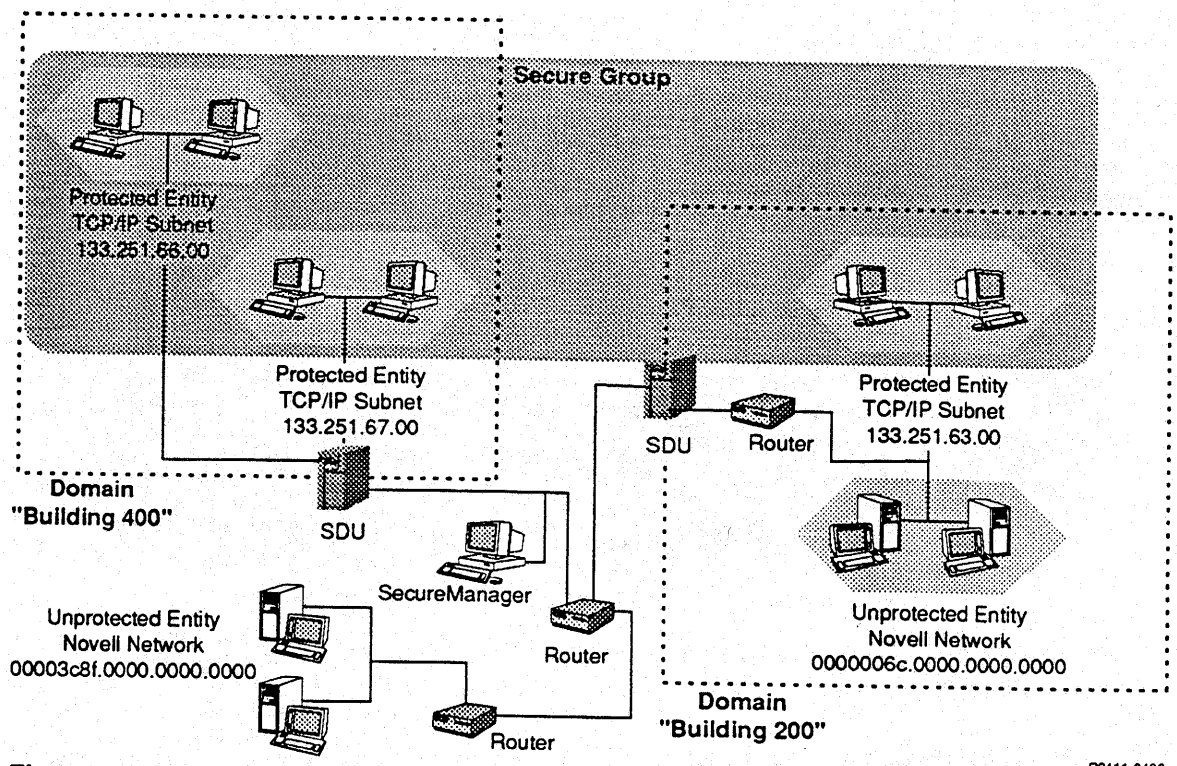


Figure 1-7
A Secure Group Spanning Two Secure Domains

Secure Group Roles

Within a Secure Group, additional policies can be implemented for individual Entities via member roles—Root, Leaf, Meshed Root, or Meshed Leaf. By assigning a role to each member of a Secure Group, you can establish access control within the Group. Roles determine which Secure Group members can communicate with each other by blocking traffic between some members. Secure Group member roles that allow communications between members are referred to as *compatible;* those that do not are *incompatible.*

See "Adding Members to a Secure Group" in Chapter 4, *Implementing Security Policies.*

Enterprise Security Policy Summary

Using these terms just discussed—SDU (SecureDomain Unit), Secure Domain, Entity, protected Entity, Secure Group, and Secure Group member role—the SecureManager security policies can be summarized.

SecureManager provides four different primary building blocks to create your enterprise network security policy:

1. The primary instrument is the *Secure Group* with its internal packet handling assignment.

2. Second to Secure Groups are *Secure Group membership and member roles.*

3. The third security option is the *Entity insecure communications assignment.*

4. Fourth is the *SDU insecure communications assignment.*

The first two building blocks are critical, because they apply to communications between protected Entities. The third building block applies to communications between Entities with incompatible roles, or Entities that do not belong to the same Secure Group (where at least one Entity belongs to a Secure Group that is protected). The fourth building block applies to communications between unprotected Entities (where neither belongs to a Secure Group).

Refer to Appendix B for more information about Security Policy assignments.

Chapter 2
User Interface Conventions

This chapter explains how to use the SecureManager application's interface including its maps, and the graphical objects.

Inside this chapter:

The SecureManager Window

The SecureManager main window contains the Network Map, the main menu, an icon-based tool bar below the main menu, a palette (column) of network object icon prototypes, a color key, and a scrolling message box.

Using SecureManager's four maps (listed below), you build a graphical representation of your network and define the security relationships among the various Entities you are securing.

You can display all four maps at once. To build your network layout, you drag and drop icons onto the Network Map, which is always displayed in the SecureManager window. You also drag objects from the Network Map onto the Uninstalled SDU Map and the Secure Groups Map as summarized below.

Network Map	Drag and drop network object icon prototypes onto the Network Map from the left. Drag and drop uninstalled SDU icons onto the Network Map from the Uninstalled SDU Map.
Location Map	A simplified view of the entire Network Map. Change the section of the Network Map displayed. Change the area included in the Network Map.
Uninstalled SDU Map	Drag and drop uninstalled SDU icons from here onto the Network Map to register them. When you drag and drop SDU icons from the Network Map to the trash to delete them from the Network Map, they reappear here.
Secure Groups Map	Drag and drop Entity icons from the Network Map onto Secure Group (rectangle) icons here to add members to a Secure Group. Drag and drop Entity icons from the Network Map onto the special Secure Group icon here to remove members from a Secure Group.

Understanding the Uninstalled SDU and Secure Groups Maps is essential for building your network security framework.

The Network Map

Open maps or the audit log or start a polling cycle with tool bar icons.

Information bar displays graphical object names and tool bar icon functions.

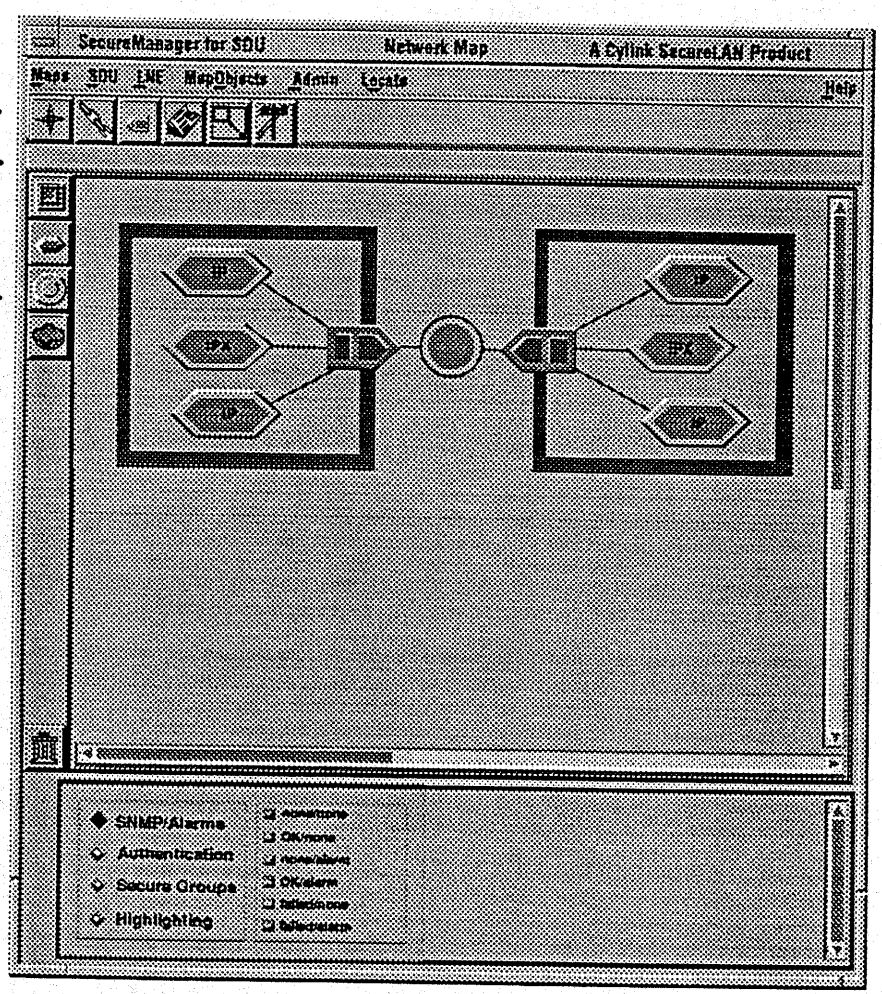
Use network object icons to build your Network Map. Drag from the palette with the middle mouse button to place on the Network Map.

Open the pop-up menu of a network object icon with the right mouse button.

Scroll bars allow easy navigation.

Color zones of network objects signify various types of status. Different color keys interpret four different types of status.

Messages are displayed in the scrolling message area at the bottom of the window.



P2410-1096

Figure 2-1
The SecureManager Main Window with the Network Map

By building an accurate Network Map, you create a sound structure for assigning security policies.

The Location Map

To open the Location Map, choose *Location* from the *Maps* menu or click the Location Map tool bar icon.

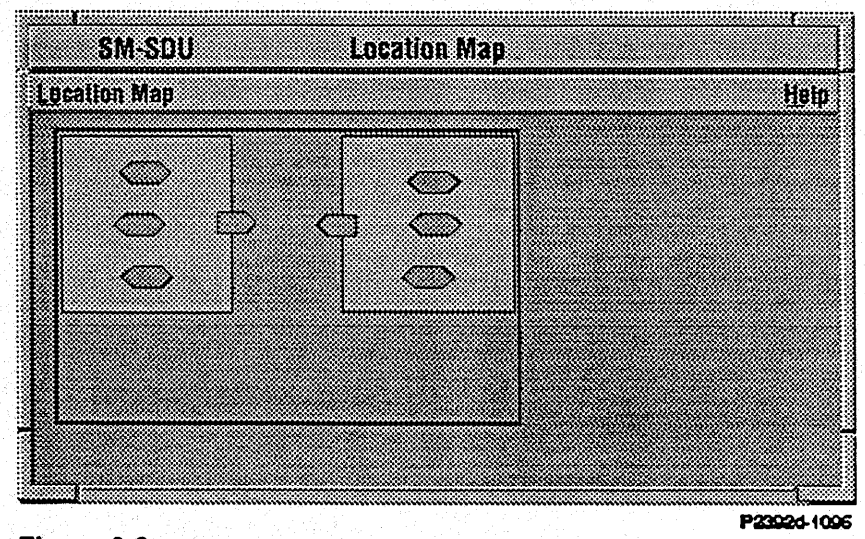


Figure 2-2
Location Map

When open, the Location Map always displays a small version of the entire Network Map. If only part of the entire Network Map is displayed, the Location Map shows clearly which part, relative to the entire Network Map, is displayed; a red rectangle frames the displayed area.

Use the Location Map to change the area of the Network Map displayed. To change the part of your network displayed on the Network Map, move the cursor around inside the Location Map. A black rectangle follows the cursor. Click the left mouse button when the black rectangle frames the area you want displayed. The black rectangle turns red and the previous red rectangle disappears.

Use the Location Map to change the area displayed in the Network Map or to get a comprehensive view of the entire mapped area. In the Location Map, you can see all of the icons that are highlighted, even if some are not visible in the Network Map.

The scale of the Location Map changes to reflect the total mapped area.

Chapter 3
Creating a Security Framework

This chapter describes the steps involved in creating a representation of the secure network to be managed by SecureManager. This includes building a graphical representation of your network and the registration and authentication of SecureDomain Units. The rest of the process (creating Secure Groups and assigning roles) is described in detail in Chapter 4, *Implementing Security Policies*.

Inside this chapter:

Overview

This chapter includes a check list of the entire installation and setup process and a complete description of the first part of the procedure. This includes planning your network layout and adding Secure Domains to your Network Map. With Domains on the Network Map, you can add (register) SDUs and assign IP addresses to them. Then place Entities (representing networks, subnets, and IP address ranges) inside the Secure Domains. This chapter explains how to do these steps.

The second part is fully described in Chapter 4, *Implementing Security Policies*. To complete the procedure, implement your enterprise security policy by creating Secure Groups and defining how members (Entities) in different Domains communicate with one another within each Secure Group. You can add additional restrictions to specific Secure Group members via roles. These steps are fully described in Chapter 4. The interaction between different security policies configured within SecureManager is introduced in Chapter 4 and fully explained in Appendix B.

Use the sequence of seventeen steps below as a checklist as you secure your network traffic with SecureManager and SecureDomain Units. The specific procedures for security assignments are noted ☞. These procedures are critical to the correct operation of the SecureLAN system.

Creating a Network Layout: A Summary

1. **Plan your enterprise network security.**

   a. In addition to the background described in the preface of this document, you need to understand concepts unique to Cylink's SecureManager. Study Chapters 1, 2 and 4 and Appendix B.

   b. Designate IP addresses for all SDUs.

2. **Install the workstation on which you will install the SecureManager application on the network backbone, so it will be outside all Secure Domains (Appendix A).**

3. **Install Solaris and HP OpenView.**

   Refer to the Sun Microsystems and HP documentation included with the products. If your system was shipped with Solaris pre-installed, you generally do not have to re-install it.

4. **Install Informix SE 7.10 and SecureManager (SM) (Appendix A).**

   Both applications are on the SecureManager CD-ROM. You will at this time load the SecureManager manufacturing certificate (which contains the public key) and the SecureManager private key. These files are on the four custom diskettes that are bundled with the SecureManager CD-ROM.

5. **Launch SecureManager from within OpenView (Appendix A).**

6. **In the SM GUI (graphical user interface), start populating your Network Map by placing Secure Domains on it (Chapter 3).**

7. **In the SM GUI, load the SDU manufacturing certificates (Figure 3-2).**

   You will need the unique SDU manufacturing certificate diskette for each SDU.

8. **In the SM GUI, assign IP addresses to SDUs (Figure 3-3).**

9. **In the SM GUI, verify that the SM BOOTP server is running.(Figure 3-4).**

   The SM BOOTP server is responsible for downloading IP addresses to the SDUs.

10. **Physically connect the SDUs to the same IP network as SM and plug in the power cords. IP addresses are downloaded to the SDUs during this temporary connection (refer to the *SecureDomain Installation Guide).***

NOTE The user has no access to the internal hardware of the SecureDomain Unit.

11. **Power cycle the SDUs and confirm on the SDU front panel that the IP addresses have been downloaded correctly (step 6 on page 3-10).**

NOTE See "Assign and Download (Initialize) the IP Address" for an alternative method of assigning IP addresses to SDUs.

12. **Power down and disconnect the SDUs, re-connect them to the network at their permanent locations, and plug in the power cords.**

13. **In the SM GUI, register the SDUs (place them on the Network Map) (Chapter 3 and Figure 3-5).**

14. **In the SM GUI, authenticate the SDUs (Figure 3-6).**

15. **In the SM GUI, configure the SDUs, if necessary ("Global Policies" in Chapter 4, "Configuring an SDU" in Chapter 5, and Appendix B).**

    Assign the SDU insecure communications policies in the Global Policies view (Figure 4-17) of the Configuration of SDU dialog box (Figure 5-4) and other SDU policies in the Global Policies view as necessary.

16. **Define Entities.**

    Assign the Entity insecure communications policies (Figure 3-8).

17. **Optional: In the SM GUI, add network links, routers and clouds to your Network Map (Chapter 3).**

18. **After all of your SecureDomain Units have been authenticated, create Secure Groups ("Defining a Secure Group" in Chapter 4).**

    a. Assign the Secure Group internal packet handling policy ("Defining a Secure Group" in Chapter 4).

    b. Add members (Entities) to Secure Groups ("Adding Members to a Secure Group" in Chapter 4).

    c. Assign roles to individual member Entities within Secure Groups ("Assigning Roles within a Secure Group" in Chapter 4).

NOTE For each SecureManager installation you can define up to 100 IP Range LNEs and create up to 96 Secure Groups.

Place Secure Domains

A Secure Domain identifies a collection of Entities (usually networks) that are secured by a SecureDomain Unit (SDU) and are eligible to become protected (become a Secure Group member) because they are inside the Secure Domain. A Secure Domain must be a secure network perimeter protected by one (and only one) SDU.

Network traffic cannot enter or exit a Secure Domain without traversing through a SecureDomain Unit. The SecureManager application uses the Secure Domain as a logical boundary that defines which Entities can be protected by a particular SDU.

A Secure Domain may include the networks, subnets, or network devices operated by a department, such as accounting, or the networks or subnets located in a specific area of the enterprise network, such as a campus, building or floor.

NOTE Network subnets must be designated before you proceed.

To define a Secure Domain and establish it on the Network Map:

1. **Select (with the middle mouse button) the Secure Domain map object icon and drag and drop it onto the Network Map.**

   The View/Modify Domain attributes dialog box opens.

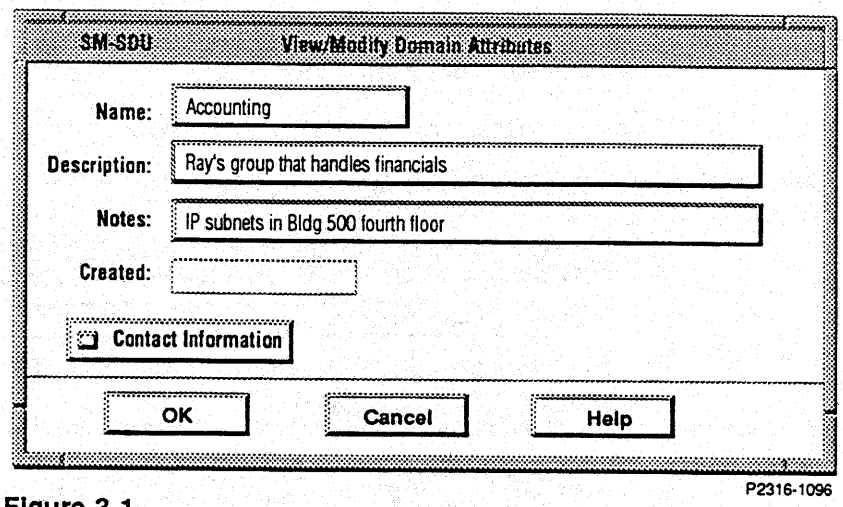


Figure 3-1
Domain Attributes

2. **Optional: Enter descriptive information that identifies the Secure Domain.**

   Use either the default Domain Name or enter a new Domain Name. Valid names are made up of 16 or fewer printable alphanumeric characters, including spaces.

3. **Click <OK>.**

   You can add or edit Secure Domain information at any time. Choose *Attributes* from the Secure Domain's pop-up menu. The View/Modify Domain Attributes dialog box opens. Edit fields you need to change.

CAUTION Do not nest Secure Domains or try to stack SDUs on the Network Map! Do not place more than one SDU on a single Ethernet segment. Do not have more than one network path leading from each Domain to be secured. (If more than one path exists, the SDU displays the message "CASCADED CONFIG.")

Verify that any network firewalls in the path of secure connections can transmit IP addresses to the SDU, SecureManager, and all Entities.

Load the SDU's Manufacturing Certificate

To place SDUs on the Network Map, start with the Uninstalled SDUs Map.

1. **To open the Uninstalled SDU Map, choose *Uninstalled SDUs* from the *Maps* menu or click the SDU tool bar icon.**

2. **Choose *Load* from the Uninstalled SDU menu.**

   The Load SDU Certificates dialog box opens.

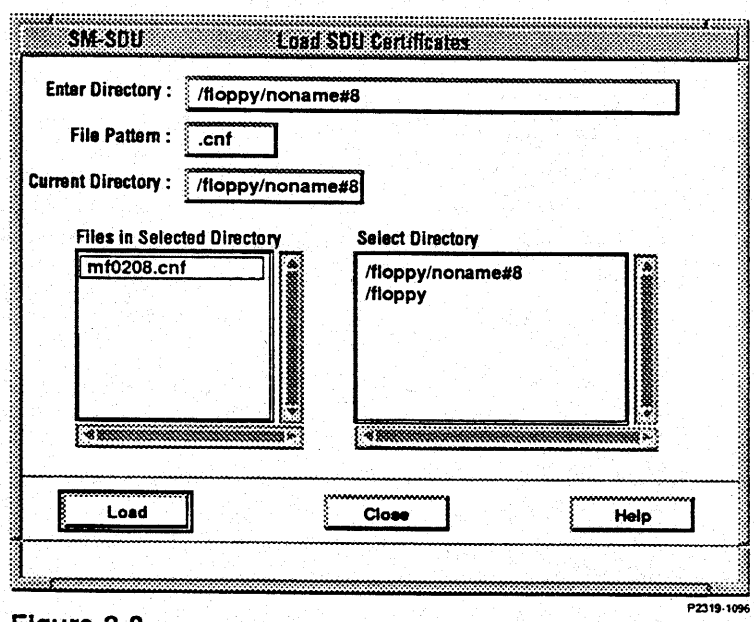


Figure 3-2
Load SDU Certificate

3. **Insert the certificate diskette specific to that SDU.**

To mount the diskette volume and open a File Manager window displaying the diskette directories, you may need to type `volcheck` in a shell window.

In this File Manager window, locate the *full* path name of the SDU manufacturing certificate. Use this path name in step 4 below.

4. **In the *Enter Directory* field of the Load SDU Certificates dialog box, type the full path name to the SDU manufacturing certificate on the floppy, and press <Return>.**

   The file name of the manufacturing certificate on the floppy appears in the *Files in Selected Directory* box. Each SDU manufacturing certificate floppy contains one directory with one file.

5. **Select (highlight) the manufacturing certificate file.**

6. **Click <Load>.**

   A rectangular icon representing the Uninstalled SDU appears in the Uninstalled SDUs map. The icon displays the SDU's Unit ID number and its (factory assigned) MAC address.

7. **Click <Close>.**

8. **Click <Eject> in the File Manager window.**

   The certificate information, which includes the public key, is stored in the SecureManager database.

NOTE

The Unit ID and MAC address are read from the SDU's certificate. You must use the correct (matching) manufacturing certificate floppy for each SDU.

Close the window displaying the contents of the manufacturing certificate diskette by clicking <Eject>. This will also eject the diskette allowing you (if necessary) to insert the diskette for the next SDU.

If you are loading certificates for several SDUs, you can copy the certificate files into a directory, enter the path to that directory in the *Enter Directory* field, and select and load all of the certificate files in one operation.

Assign and Download (Initialize) the IP Address

The method for assigning IP addresses described below is one of several different methods available for assigning IP addresses to SDUs. In most situations, this is the most expedient option. Alternatives are described in Appendix A.

1. **Assign an IP address to the SDU:**
   Open the pop-up menu of the Uninstalled SDU rectangular icon; then choose *BOOTP* (Bootstrap Protocol) *Table Entry*.

   The Create/Modify BOOTP Table Entries box opens.

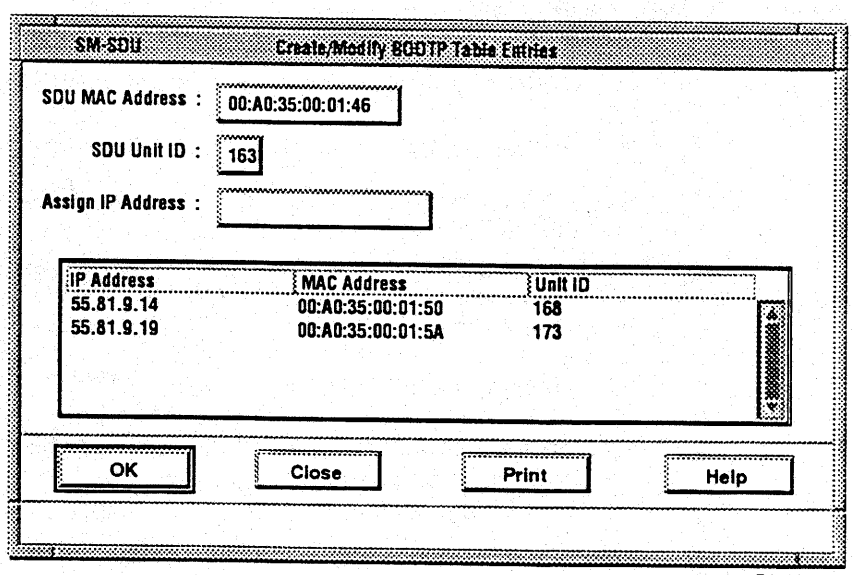


Figure 3-3
Create/Modify BOOTP Table Entries

   The SDU Unit ID and MAC address values from the uninstalled SDU icon are automatically displayed in the appropriate fields in this dialog box.

2. **Type the IP address that you want to assign to the SDU in the *Assign IP Address* field and then click <Close>.**

   Once you have assigned the IP address here, the rectangular icon in the Uninstalled SDU Map will show this IP address.

CAUTION SecureManager does not support Class D and E IP addresses!

CAUTION

Do not use place-holder zeros in IP addresses!
Incorrect: 208.188.115.007
Correct: 208.188.115.7

NOTE

You can use another BOOTP server; you do not have to use SecureManager's. For further information, "Assigning IP Addresses" in Appendix A.

3. **If you are using SecureManager's integrated BOOTP server to assign IP addresses to SDUs, verify that the BOOTP server is running. Choose *BOOTP Server* from the *Admin* menu.**

   The BOOTP Server dialog box opens.

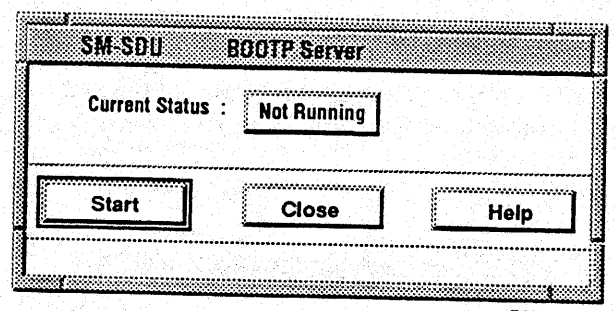


Figure 3-4
BOOTP Server

Normally the BOOTP server starts automatically when SecureManager is launched. The *Current Status* field is either *Running* or *Not Running*.

If the BOOTP server is not running, click <Start> in the BOOTP Server dialog box and then <Close>.

You need to start the BOOTP server before power cycling an SDU for the first time; this step is not necessary before subsequent power cycles.

4. **Physically connect the SDU.**

   Be sure to install the SDUs "facing" in the right direction (clear/cipher).

NOTE

Although you can use three different types of Ethernet cable (thick, thin, or twisted pair/10baseT), you must use the same type of cable for both SDU Ethernet interfaces (clear and encrypted). If you use 10baseT, you must use the correct type of 10baseT cable. Use the straight-through type to connect to a hub and the cross-over type to connect to a PC. For further information, refer to the SecureDomain Installation Guide.

CHAPTER 6
System Administrative Tasks

This chapter explains system administrative and maintenance tasks. Some tasks are routine, while others may never be necessary.

Inside this chapter:

To set the duration of inactivity time:

1. Select *Inactivity Timeout* from the *Admin* menu.

   The Inactivity Timeout dialog box opens.

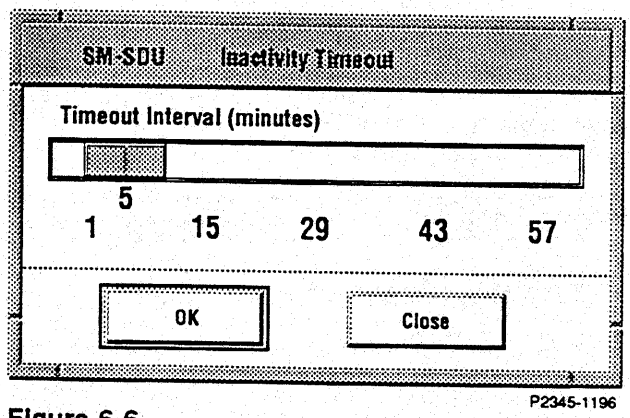


Figure 6-6
Inactivity Timeout

2. Using the slider, set the desired interval.
3. Click <OK> to confirm the value.

   Click <Close> to return to the main window without changing the value.

Changing the Encryption Password

To change the Encryption Password, choose *Encryption Password* in the *Admin* menu. Type the old and new passwords in the appropriate fields.

Using the Locate Function in HP OpenView

This option allows the addition of SecureManager to the HP OpenView main menu. Icons corresponding to those selected on the SecureManager Network Map will be highlighted in HP OpenView. This function can also be used from HP OpenView to locate icons on the SecureManager network map corresponding to those in HP OpenView.

To use this feature:

1. Highlight the SecureDomain Unit on the SecureManager network map.

2. Choose *Locate in OpenView* from the *SDU* menu.

   The corresponding SDU icon will be highlighted in HP OpenView.

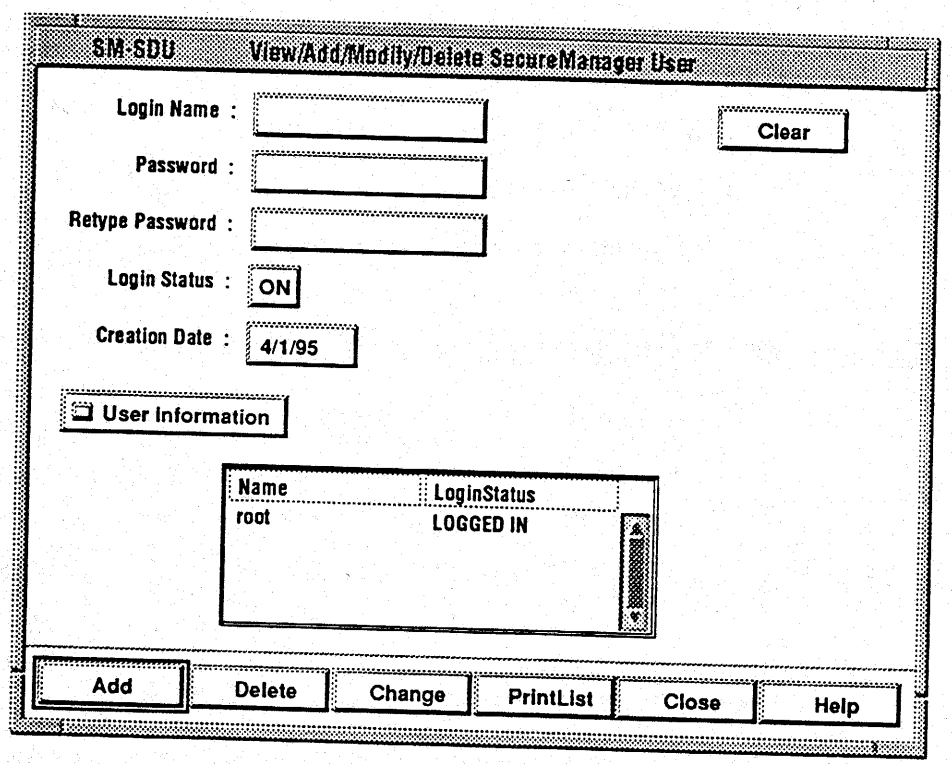
Managing SecureManager Users

Use this function to add, modify, delete, or view the status of authorized SecureManager users.

NOTE No more than one user can be logged in to SecureManager at one time.

1. Choose *User* from the *Admin* menu.

   The View/Add/Modify/Delete SecureManager User dialog box opens.



P2342-1196

Figure 6-7
View/Add/Modify/Delete SecureManager User

Loading the SecureManager Manufacturing Certificate

This option is primarily for setting up a second (backup) SecureManager server.

To reinstall the SecureManager manufacturing certificate:

1. **Choose *Load Manufacturing Certificate* from the *Admin* menu.**

   The Load SM from Media dialog box opens.

2. **Select the directory where the file is located in the list on the right side.**

   The files contained in that directory are then listed on the left side.

3. **Select the file from the list on the left side.**
4. **Click <Load>.**
5. **Restore the corresponding secret keys.**

   See "Restoring the SecureManager Private Key" in the section immediately following.

Backing Up and Restoring the SecureManager Private Key

Backing Up the SecureManager Private Key

Using this method, the Secure Manager private key is backed up in three separate parts, each with its own path. The key cannot be restored unless two of the three parts are used.

To back up the private key:

1. **Choose *Private Key... Backup* from the *Admin* menu.**

   The Backup SecureManager Private Key dialog box opens.

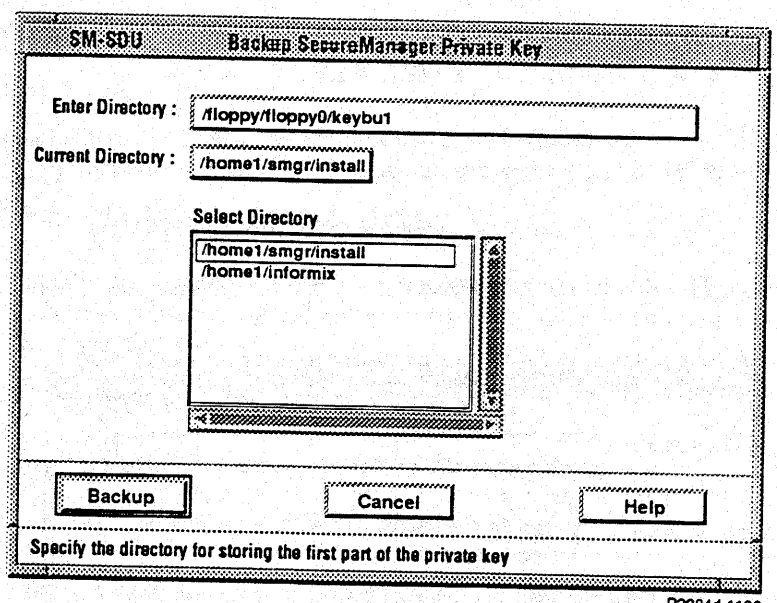


Figure 6-9
Backup SecureManager Private Key

2. Enter or select the path name to the directory (on a floppy) where the first part of the key will be stored.

3. Click <Backup>.

   The first component of the private key will be backed up.

4. Repeat steps 2 and 3 on different floppies to back up the second and third parts of the key.

CAUTION For security reasons, never store the different parts of the key on the same media. Store each of the three parts of the key separately.

NOTE Backup files will automatically be given a filename suffix of .sk.

5. Click<Cancel> to exit the dialog box without backing up the key.

Restoring the SecureManager Private Key

This operation allows restoration of previously backed-up keys. Any two of the three key components can be used. To restore the private key:

1. Choose *Private Key... Restore* from the *Admin* menu.

   The Restore SecureManager Private Key dialog box opens.

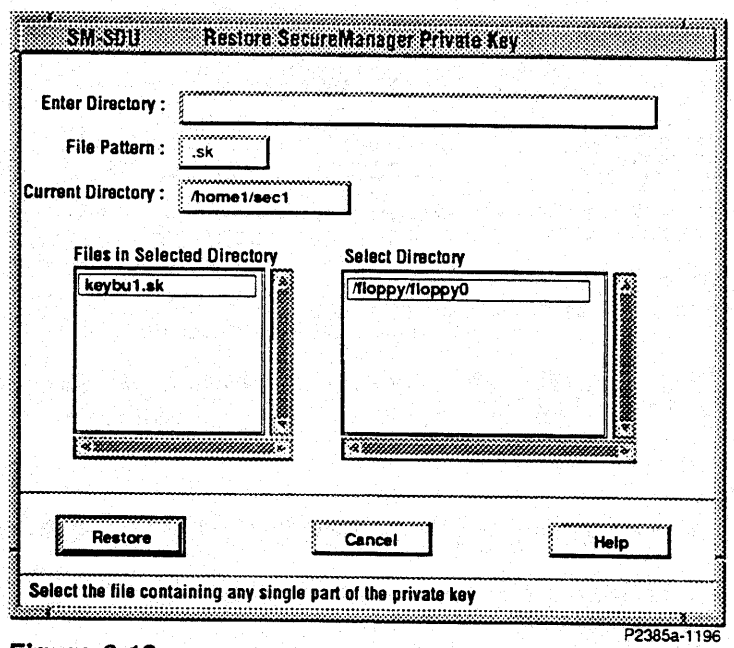


Figure 6-10
Restore SecureManager Private Key

2. Enter or select the path name to the directory (on a floppy) that contains one of the backup files.

   All files in that directory with the extension .sk are listed. There should be only one such file in any given directory.

3. Highlight the .sk file and click <Restore>.

   The first component is restored.

4. Repeat steps 2 and 3 with a second part of the key to complete the key restoration.

5. Click <Cancel> to close the dialog box without restoring the key.

Archiving and Restoring the SecureManager Database

Archiving the SecureManager Database

The SecureManager database should be archived on a regular basis. Between scheduled archiving, all changes to the database are recorded in an incremental log.

To archive the SecureManager database:

1. Choose *Database... Archive* from the *Admin* menu.

   The Database Archive dialog box opens.

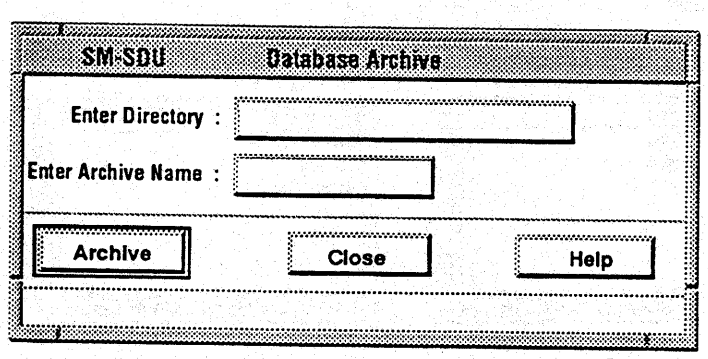


Figure 6-11
Database Archive

2. Enter the name of the directory to be used for the archive, then the name of the archive file.
3. Click <OK> to archive the database.

   Click <Close> to close the dialog box without archiving.

NOTE To access this database in the future, you will need the encryption password current at the time of archiving. See Appendix A, *Installing SecureManager Software.*

Restoring the SecureManager Database

The SecureManager database can be restored with or without the incremental log.

To recover the SecureManager database:

1. Choose *Database... Recover* from the *Admin* menu.

   The Database Recover dialog box opens.

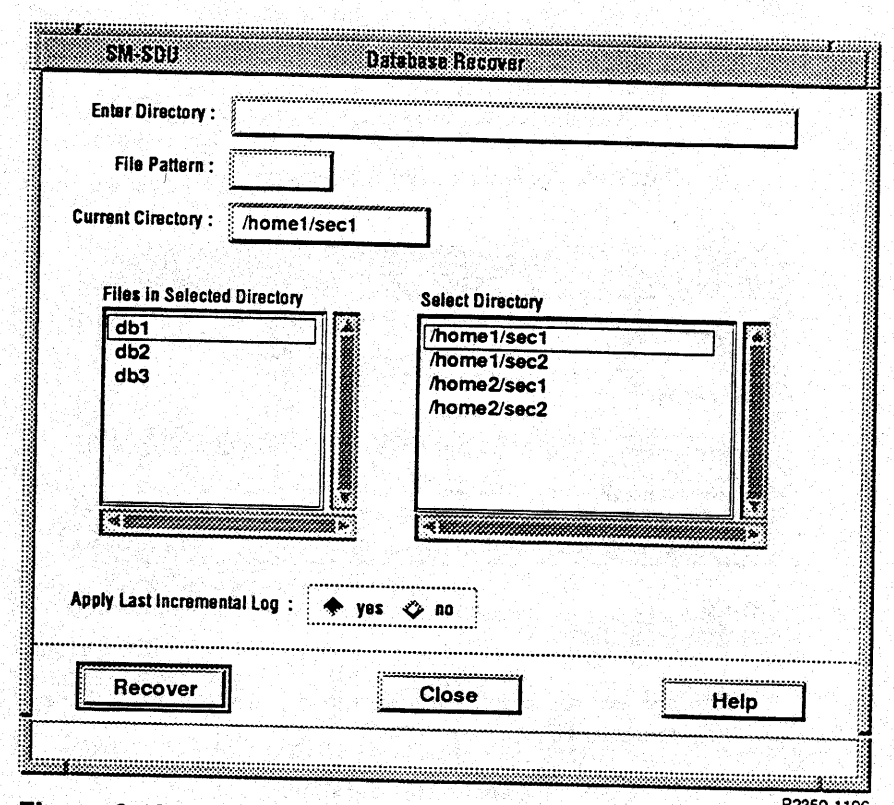


Figure 6-12
Database Recover

2. Enter or select the name of the directory used for the archive.
3. Enter the *File Pattern* (extension), if any, used for archive files.

   All files in the directory matching the file pattern will be displayed in the list box.

4. Highlight the desired archive file under *Select Directory*.

5. Indicate whether or not to apply the last incremental log by selecting *yes* or *no*.

   If you select *No*, the database is **restored**. It is reinstated as it was at the last backup.

   If you select *Yes*, the database is **recovered**. It is reinstated as it was at the last backup with the addition of the log since the last backup.

NOTE Do not apply the incremental log to any but the latest database archive.

6. Click <Recover> to recover the database.

   Click <Close> to close the dialog box without archiving.

Software Installation

- If this is your first SecureManager installation, proceed with the procedure outlined below.
- If you have already installed other SecureManager products on your system, or if you are upgrading an earlier installation of SecureManager for SecureDomain units, use the procedure outlined in the section "Installing an Upgrade," later in this appendix.

CAUTION

If you have already installed SecureManager for SecureDomain—or other SecureManager products, you should back up your existing SecureManager Informix database on separate media (diskettes, tape, etc.) before continuing with this installation procedure. The installation procedure deletes any existing database as part of the installation.

Also, the database schema changed in Version 3.01 of SecureManager. If you are using a version of Securemanager older than 2.01, you must update SecureManager to at least Version 2.01 before continuing with this installation; otherwise, your database will be lost because SecureManager 3.01 cannot be used to recover database information archived in SecureManager versions earlier than 2.01.

The SecureManager installation process consists of the following tasks:

- Logging into the system.
- Installing Informix.
- Preparing for HP OpenView integration.
- Installing SecureManager.

The tasks are performed in the order presented by the installation program.

Login to the System

1. **Log in as root.**
2. **Launch OpenWindows by typing:**

   ```
   openwin
   ```

3. **If you are not in the C shell, type in a window:**

   ```
   csh
   ```

Install Informix

The process of installing Informix consists of the following tasks:

- Creating the Informix user and group.
- Setting up the Informix file system and copying the Informix files.
- Installing Informix.
- Creating an Informix server.

Create the Informix User and Group

1. **If your system already has an Informix User and Group, skip ahead to the section "Set Up the Informix File System and Copy the Informix Files."**
2. **If your system does not have an Informix User and Group, go to the `/bin` directory and type:**

   ```
   admintool
   ```

   You can also open Administration Tool in File Manager.

   If you are using an earlier version of Solaris Administration Tool, Version 2.5, go to Step 3.

   If you are using Version 2.5 of Solaris Administration Tool, go to Step 4.

3. **For users of earlier versions of Solaris Administration Tool than Version 2.5:**

   a. **Click <DataBase Manager>.**

      The Load Database dialog appears.

   b. **Select *Group*.**
      Select *None* for *Naming Service*.
      Click <Load>.

      The Database Manager - Group Database dialog appears.

   c. **Choose *Add Entry* from the pull-down *Edit* menu.**

      The Database Manager - Add Entry dialog appears.

d. **Type `informix` for the *Group Name*.**
Type a number 100 or larger for the *Group ID*.
Click <Add>.

Leave other items as they are.

e. **In the Administration Tool main window, Click <User Account Manager>.**

The User Account Manager: Select Naming Service dialog appears.

f. **Select *None* for *Naming Service*.**
Click <Apply).

The User Account Manager dialog appears.

g. **From the *Edit* menu, choose *Add User*.**

The User Account Manager: Add User dialog appears.

h. **Type `informix` for the *User Name*.**
Type a number 100 or larger for the *User ID*.
Type `informix` for the *Primary Group*.
Select *Normal password...*

The User Account Manager: Set Password dialog appears.

i. **Type and retype your Informix database password.**

j. **In the User Account Manager: Add User dialog:**

Click the Create Home Directory checkbox so that a home directory is created automatically.

Note that if the box is checked and the directory already exists, the operation will fail. When you have already manually created the home directory, leave this box unchecked.

Type `/opt/informix` in the *Path:* field.
Type the machine name of the Informix server.

Leave other items as they are. Permissions are set automatically during Informix and SecureManager installation.

k. **Click <Add> and then click <Exit> to exit the Administration Tool.**

4. For users of Solaris Administration Tool, Version 2.5:

   a. In the Admintool: Users dialog, select *Groups* on the *Browse* menu.

      The Admintool: Groups dialog appears.

   b. In the Admintool: Groups dialog, select *Add* on the *Edit* menu.

      The Admintool: Add Group dialog appears.

   c. Type the group name in the Group Name field.
      Type the group ID in the Group ID field.
      Click <OK>.

      The new group is added to the list shown in the Admintool: Groups dialog.

   d. In the Admintool: Groups dialog, select *Users* on the *Browse* menu.

      The Admintool: Users dialog appears.

   e. In the Admintool: Users dialog, select *Add* on the *Edit* menu.

      The Admintool: Add User dialog appears.

   f. Type `informix` for the *User Name*.
      Type a number 100 or larger for the *User ID*.
      Type the group ID from the earlier group configuration for the *Primary Group*.
      Select *Normal password...* under Account Security.

      The Set Password dialog appears.

   g. Type and retype your Informix database password.

   h. Type `/opt/informix` in the *Path:* field.

      Leave other items as they are.

   i. Click <Apply> and then exit the Administration Tool.

Log in to SecureManager

1. **Launch SecureManager from within OpenView. Choose *Start Secure Manager* from the *SecureMgr* menu.**

   You can also launch SecureManager by typing `smgr` from a window, but you will not be able to use the Open View network management tools. (You will not be able to register SDU icons or objects in OpenView.)

2. **In the SecureManager Login dialog box, enter your passwords.**

User Name:	`root`
User Password:	`lansecure`
Database Password:	(assigned when creating the user named *informix* in the section, "Create the Informix User and Group," earlier in this appendix)
Encryption Password:	(assigned during step 4 of the section, "Load the SecureManager Manufacturing Certificate and Assign the (Database) Encryption Password, SecureManager," earlier in this appendix.

3. **Change the SecureManager user password for root the first time you log in to SecureManager.**

NOTE The first time only the root account, using the password *lansecure*, can log in. Change this password.

Add additional users and assign passwords in the SecureManager User Management dialog box accessible via the *Admin* menu (see Chapter 6, "System Administrative Tasks"). To use SecureManager (that is, to be set up as a SecureManager user), you must be an existing UNIX user.

SecureManager users can change their own passwords only. Only root users can add or delete users or change passwords other than their own.

All other SecureManager functions and commands are accessible to anyone logged in to SecureManager. However, no more than one user can be logged in to SecureManager at any one time.

IMPORTANT The Inactivity Timeout function requires the user to re-enter a password after the SecureManager application has been left unattended for the set timeout period. After the timeout has elapsed, you cannot perform operations in SecureManager until you enter the password in the SecureManager Inactivity Timeout dialog box.

Although the SecureManager Inactivity Timeout dialog box always opens automatically after the inactivity period has elapsed, it is not always visible on the desktop. If mouse clicks produce no effect for no apparent reason, the SecureManager Inactivity Timeout dialog is probably hidden on the desktop. To enter the password, you may need to move the SecureManager main window temporarily so that it is out of the way and the SecureManager Inactivity Timeout dialog box is visible.

To set the Inactivity Timeout period, see "Setting the Inactivity Timeout" in Chapter 6, *System Administrative Tasks*.

Installing an Upgrade

If you have already installed other SecureManager products on your system, or you are upgrading an earlier installation of SecureManager for SecureDomain units, use the procedure outlined in this section.

CAUTION If you have already installed SecureManager for SecureDomain—or other SecureManager products, you should back up your existing SecureManager Informix database on separate media (diskettes, tape, etc.) before continuing with this installation procedure. The installation procedure deletes any existing database as part of the installation.

To install an upgrade:

1. **Log in as root.**
2. **Launch OpenWindows by typing:**

   ```
   openwin
   ```

3. **If you are not in the C shell, type in a window:**

   ```
   csh
   ```

4. **Verify that the following environment settings are present.**

   For SecureManager:

   ```
   setenv SM_HOME your_SecureManager_home_directory
   ```

For Informix:

```
setenv INFORMIXDIR Informix_home_directory
setenv INFORMIXSERVER securedb
set path=($INFORMIXDIR/bin /opt/OV/bin)
```

5. **Insert the SecureManager CD-ROM disk into the drive.**

6. **Invoke the SecureManager installation script. Type a command similar to the following:**

   ```
   /cdrom/directory_name/smgr/install/installsm
   ```

   where *directory_name* is replaced by one of the directory names found in the `/cdrom` directory. The names take the form *name#n*. For example, cylink#0 or cdrom#0.

   The SecureManager installation script begins, and displays the main installation menu, which lists the following choices:

   1. SecureDomain Unit
   2. SecureFrame Unit
   3. SecureNode
   4. Quit Installation

7. **Select option 1 (SecureDomain Unit).**

   If there has been a previous installation, the installation program checks the presence and integrity of the SecureManager database, displays installation status information, and prompts you to specify what kind of installation should be performed.