# SunScreen EFS Release 3.0
# Installation Guide

901 San Antonio Road
Palo Alto, , CA  94303-4900

Part No:  805-7744
August 1999, Revision B

USA 650 960-1300 Fax 650
969-9131

# SunScreen EFS Release 3.0
# Installation Guide

Part No: 805-7744
August 1999, Revision B


**Please Recycle**

# Contents

**Preface xviii**

**1. Introduction to Installing SunScreen EFS 3.0 1**

What Is SunScreen EFS 3.0 2

Local Administration 2

Remote Administration 2

Operating the Firewall in Routing Mode 3

Operating the Firewall in Stealth Mode 4

Before Installing SunScreen EFS 3.0 4

Upgrading From SunScreen 1.1 or 2.0 to SunScreen EFS 3.0 5

Upgrading from SunScreen SPF-200 to SunScreen EFS 3.0 5

Converting From FireWall-1 to SunScreen EFS 3.0 6

Security Issues 6

Software and Hardware Requirements 6

Online Help and Documentation 8

Installation Problems 8

Re-install 9

Overinstall 9

Uninstall 9

**2. Prerequisites for Installation 11**

Determine Your Security Policy 11

Determine Your Network Configuration 12

Determining Your Initial Level of Security 12

Preparing for Installation 13

Preparing the Screen and Administration Station 13

▼ To Install the Prerequisite Solaris Packages and Kernel Patches on the Screen 14

▼ To Install the Prerequisite Solaris Packages on the Administration Station 15

**3. Installing in Routing Mode 17**

Installation in Routing Mode With Local Administration 18

▼ To Install SunScreen EFS Using the Installation Wizard 18

▼ To Set the PATH and Install SKIP Upgrades 32

▼ To Launch the Administration GUI 32

**4. Installing In Routing Mode With Remote Administration 37**

Supported Configurations For The Administration Station 38

Installing a Remotely Administered SunScreen 38

▼ To Install the Software on the Administration Station Using the Installation Wizard 39

Installing Certificates on the Administration Station 45

▼ Option 1: To Create a Self-Generated Certificate on the Administration Station 46

▼ Option 2: To Install the Issued Certificate on the Administration Station 48

Installing the Software on the Screen 49

▼ Option 1: To Install the Software on the Screen When Using Self-Generated Certificates 50

▼ Option 2: To Install the Software on the Screen When Using Issued Certificates 68

▼ To Set the PATH, Install SKIP Upgrades, and Display the `AdminSetup.readme` File 73

Using SKIP for Encrypted Communication 75

▼ To Use the `skiptool` GUI 75

▼ To Launch the Administration GUI 84

**5. Installing in Stealth Mode 87**

Installing SunScreen EFS 3.0 in Stealth Mode 88

▼ To Install The Software on the Administration Station 89

▼ Option 2: To Install the Software on the Screen When Using Issued Certificates 95

▼ To Set the PATH, Install SKIP Upgrades, and Display the `AdminSetup.readme` File 100

Installing Certificates on the Administration Station 102

▼ Option 1: To Create a Self-Generated Certificate on the on the Administration Station 102

▼ Option 2: To Install the Issued Certificate on the Administration Station 104

Installing the Software on the Screen 105

▼ Option 1: To Install the Software on the Screen Using Self-Generated Certificates 106

Using SKIP for Encrypted Communication 126

▼ To Use the `skiptool` GUI 126

**6. Upgrading to SunScreen EFS 3.0 139**

Overview of the Upgrade from EFS 1.1 or 2.0 140

Preparing to Upgrade 140

Preparing the Screen and Administration Station 141

▼ To Install the Prerequisite Solaris Packages and Kernel Patches on the Screen 141

▼ To Install the Prerequisite Solaris Packages on the Remote Administration Station 142

Upgrading a Locally Administered SunScreen EFS 143

▼ To Upgrade to SunScreen EFS 3.0 in Routing Mode With Local Administration 143

Upgrading a Remotely Administered SunScreen EFS 148

▼ To Upgrade a Remotely Administered Screen 148

▼ To Upgrade a Remote Administration Station 150

Upgrading an EFS 2.0 High Availability (HA) System 155

▼ To Upgrade an EFS 2.0 HA Secondary Machine 155

▼ To Complete the Upgrade of an HA Primary Screen From SunScreen EFS 2.0 156

To Install the SunScreen EFS 3.0 Software on the HA Secondary 157

To Configure The Upgraded HA Cluster 157

Upgrading From SunScreen SPF-200 to SunScreen EFS 3.0 in Stealth Mode 157

▼ To Upgrade from SPF-200 to SunScreen EFS 3.0 in Stealth Mode 158

**7. Converting FireWall-1 to SunScreen EFS 3.0, in Routing Mode 163**

Preparing Your FireWall-1 Configuration for Conversion 163

SunScreen EFS 3.0 Conversion Utility 167

▼ To Install the Conversion Utility 168

Generating Conversion Files 168

▼ To Run the Conversion Utility 169

Troubleshooting the `fwconvert` Utility 170

Conditions for Failure 170

▼ To Clear Conversion Errors, Except Parse Errors 171

▼ To Clear Parse Errors 172

Verifying the Converted Rules 172

Command and Executable Files 173

Log Files 174

Creating the SunScreen EFS 3.0 Configuration 177

▼ Option 1: To Prepare the FireWall-1 Machine to Run SunScreen EFS 3.0 177

▼ Option 2: To Prepare a New SunScreen EFS Machine to Run the Converted FireWall-1 Configuration 178

▼ To Generate the New SunScreen EFS 3.0 Configuration 179

**8. Removing SunScreen EFS 3.0 Software 181**

**A. Using the Command Line For Installing SunScreen EFS 3.0 183**

▼ To Install the Software on the Administration Station Using the Command Line 183

Installing Certificates on the Administration Station 187

▼ Option 1: To Create a Self-Generated Certificate on the Administration Station 187

▼ Option 2: To Install the Issued Certificate on the Administration Station Using Command Line 188

Installing on the Screen Via The Command Line 189

▼ To Install The Software on the Screen Using the Command Line 190

▼ To Use Command-Line SKIP on the Administration Station 194

**B. Upgrading Crypto Modules 197**

# Tables


TABLE P–1 Typographic Conventions xx

TABLE P–2 Shell Prompts xx

TABLE 1–1 SunScreen EFS 3.0 Installation Requirements 6

TABLE 7–1 Known FireWall-1 Reserved Characters 164

TABLE 7–2 Known FireWall-1 Reserved Words 164

TABLE 7–3 What Does and Does Not Convert From FireWall-1 166

TABLE 7–4 Generated Configuration Files 172

TABLE 7–5 How Conversion to SunScreen EFS Affects FireWall-1 Objects 174

# Figures


Figure 1–1 Example of a Locally Administered SunScreen EFS 2

Figure 1–2 Example of a Remotely Administered SunScreen EFS 3

Figure 3–1 Screen Install Wizard's Welcome Window 20

Figure 3–2 Checking Installed Solaris Packages Window 21

Figure 3–3 Secondary HA Designation Window 22

Figure 3–4 The Select Screen Type Window With Routing Selected 23

Figure 3–5 Select Administration Type(s) Window with Local Administration Selected 24

Figure 3–6 Select Type Of Install Window With Default Install Selected 25

Figure 3–7 Ready To Install Window 26

Figure 3–8 Installing Window Showing Installation Status Bar 27

Figure 3–9 Select Initial Security Level Window With Permissive Selected 28

Figure 3–10 Select Name Service(s) Window With Both NIS And DNS Selected 29

Figure 3–11 Screen Configuration Window 30

Figure 3–12 The Screen Configuration Window Once Screen Is Successfully Configured 31

Figure 3–13 Administration GUI Login Page 34

Figure 4–1 Admin Install Wizard's Welcome Window 40

Figure 4–2 Ready To Install Window 42

Figure 4–3 Installing Window Showing Installation Status Bar 43

Figure 4–4 Installation Summary Window 44

Figure 4–5 Administration Station's Self-Generated Certificate 47

Figure 4–6 Screen Install Wizard's Welcome Window 51

Figure 4–7 Checking Installed Solaris Packages Window 52

Figure 4–8 Secondary HA Designation Window 53

Figure 4–9 Select Screen Type Window With Routing Mode Selected 54

Figure 4–10 Select Administration Type(s) Window With Remote Administration Selected 55

Figure 4–11 Select Type Of Install Window With Default Install Selected 56

Figure 4–12 Ready To Install Window 57

Figure 4–13 Installing Window Showing Installation Status Bar 58

Figure 4–14 Installation Summary Window 59

Figure 4–15 Select Certificate Type Window With Self-Generated Certificate Selected 60

Figure 4–16 Self Generated Certificate ID Window 61

Figure 4–17 Generate Screen Certificate Window With Screen's Certificate ID 62

Figure 4–18 Select Initial Security Level Window With Permissive Selected 63

Figure 4–19 Select Name Service(s) Window With Both NIS And DNS Selected 64

Figure 4–20 Screen Configuration Window 65

Figure 4–21 Screen Configuration Window Once Screen Is Successfully Configured 66

Figure 4–22 Screen Reboot Window 67

Figure 4–23 Select Certificate Type Window With Issued Certificate Selected 69

Figure 4–24 Issued Certificate Key Diskettes Window 70

Figure 4–25 Issued Certificate Key Diskettes Window With Issued Certificate ID At Bottom 71

Figure 4–26 Issued Certificate Key Diskettes Window 72

Figure 4–27 `AdminSetup.readme` file 74

Figure 4–28 `skiptool` Main Window 77

Figure 4–29 Skiptool With Add Host Properties Window Completed 79

Figure 4–30 Add SKIP Host Properties Window 81

Figure 4–31 Add SKIP Host Properties Completed 83

Figure 4–32 Administration GUI Login Page 85

Figure 5–1 SunScreen EFS Admin Install's Welcome Window 90

Figure 5–2 The Ready to Install Window 92

Figure 5–3 The Installing Window Showing The Status Bar 93

Figure 5–4 Installation Summary Window 94

Figure 5–5 Select Certificate Type Window With Issued Certificate Selected 96

Figure 5–6 Issued Certificate Key Diskettes Window 97

Figure 5–7 Issued Certificate Key Diskettes Window With Issued Certificate ID At Bottom 98

Figure 5–8 Issued Certificate Key Diskettes Window 99

Figure 5–9 `AdminSetup.readme` file 101

Figure 5–10 Administration Station's Self-Generated Certificate 103

Figure 5–11 Screen Install Wizard's Welcome Window 107

Figure 5–12 Checking Installed Solaris Packages Window 108

Figure 5–13 Secondary HA Designation Window 109

Figure 5–14 Select Screen Type Window With Stealth Selected 110

Figure 5–15 Select Administration Type(s) Window With Remote Administration Selected 112

Figure 5–16 Select Type of Install Window With Default Install Selected 113

Figure 5–17 Ready To Install Window 114

Figure 5–18 Installing Window Showing Installation Status Bar 115

Figure 5–19 Installation Summary Window 116

Figure 5–20 Select Certificate Type Window With Self-Generated Certificate Selected 117

Figure 5–21 Self-Generated Certificate ID Window 118

Figure 5–22 Generate Screen Certificate With Screen's Certificate ID Generated 119

Figure 5–23 Select Initial Security Level Window With Permissive Selected 120

Figure 5–24 Select Name Service(s) Window With Both NIS And DNS Selected 121

Figure 5–25 Screen Configuration Window 122

Figure 5–26 Screen Configuration Window Once Screen Is Configured 123

Figure 5–27 Screen Hardening Window 124

Figure 5–28 Screen Reboot Window 125

Figure 5–29 `skiptool` Main Window 128

Figure 5–30 `skiptool` With Add Host Properties Window Completed 130

Figure 5–31 Add SKIP Host Properties Window 132

Figure 5–32 Add SKIP Host Properties Completed 134

Figure 5–33 Administration GUI Login Page 136

Figure 6–1 Administration GUI Login Page 147

Figure 7–1 FireWall-1 Configuration Convertor Dialog Box 169

Figure 7–2 Error Message From `fwconvert` 171

# Code Examples

# Preface

SunScreen EFS™ 3.0 introduces the first SunScreen product release that combines the popular stealth SunScreen SPF-200 dedicated bridge product with the SunScreen EFS layered router product. You now have greater flexibility when setting up your company's security scheme as a solution to security authentication and privacy requirements, as well as a means of securing your department networks connected to a public internetwork.

This *SunScreen EFS Installation Guide* provides all information necessary to install in either routing or stealth mode from the SunScreen EFS 3.0 CD-ROM on to your network. Other manuals in the SunScreen EFS documentation set include the *SunScreen EFS Administration Guide* and the *SunScreen EFS Reference Manual.*

## Who Should Use This Book

The SunScreen EFS documentation set is intended for SunScreen EFS system administrators responsible for the operation, support, and maintenance of network security. It is assumed that you are familiar with UNIX system administration and TCP/IP networking concepts, and with your network topology.

## How This Guide Is Organized

The *SunScreen EFS 3.0 Installation Guide* is organized into the following chapters:

Chapter 1, Chapter 1, introduces SunScreen EFS 3.0 concepts, including product architecture.

Chapter 2, Chapter 2, covers choosing the level of security for SunScreen EFS 3.0, and preparing for installation with either local or remote administration.

Chapter 3, Chapter 3, contains instructions for installing SunScreen EFS 3.0 in routing mode with local administration.

Chapter 4, “Installing a Remotely Administered SunScreen” on page 38, contains instructions for installing a remotely administered SunScreen EFS 3.0 using self-generated or issued certificates.

Chapter 5, Chapter 5, contains instructions for installing SunScreen EFS 3.0 in stealth mode.

Chapter 6, Chapter 6, contains instructions for upgrading from SunScreen 1.1 or 2.0, or from SPF-200, to SunScreen EFS 3.0, including how to preserve your existing configurations.

Chapter 7, Chapter 7, explains how to convert from FireWall-1, Release 2.1 or 3.0, to SunScreen EFS 3.0.

Chapter 8, Chapter 8, explains how to remove the SunScreen EFS 3.0 software.

Appendix A, Appendix A, shows examples of using the command line to install SunScreen EFS 3.0 in routing mode with remote administration or in stealth mode.

Appendix B, Appendix B, explains how to add additional Crypto modules to your SKIP configuration.

## Ordering Sun Documents

The SunDocsSM program provides more than 250 manuals from Sun Microsystems, Inc. If you live in the United States, Canada, Europe, or Japan, you can purchase documentation sets or individual manuals using this program.

For a list of documents and how to order them, see the catalog section of the SunStore(sm) Internet site at `http://sunstore.sun.com`.

## Accessing Sun Documentation Online

The docs.sun.com Web site enables you to access Sun technical documentation online. You can browse the docs.sun.com archive or search for a specific book title or subject. The URL is `http://docs.sun.com/`.

# What Typographic Conventions Mean

The following table describes the type changes and symbols 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. Type su - to become superuser. |
| **`AaBbCc123`** | What you type, contrasted with on-screen computer output | machine_name% su -<br>Password: |
| *AaBbCc123* | Command-line placeholder; replace with a real name or value | To delete a file, type rm *filename*. |
| *AaBbCcl123* | Book titles, new words or terms, or emphasized words | Read Chapter 6 in *User's Guide*.<br>These are called *class* options.<br>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# |

**TABLE P–2** Shell Prompts *(continued)*

| Shell | Prompt |
|---|---|
| Bourne shell and Korn shell prompt | $ |
| Bourne shell and Korn shell superuser prompt | # |

# Related Books and Publications

The following books may be useful or interesting when installing the SunScreen EFS 3.0:

- *Applied Cryptography*Bruce Schneier, John Wiley & Sons, 1996, 2nd edition, ISBN 0-471-12845-7
- *Building Internet Firewalls*D. Brent Chapman and Elizabeth D. Zwicky O'Reilly &Associates, 1995, ISBN 1-56592-124-0
- *Computer Security Policies and SunScreen Firewalls*Kathryn M. Walker and Linda Croswhite Cavanaugh Sun Microsystems Press, 1998, SSBN 0-13-096015-0
- *Firewalls and Internet Security*Bill Cheswick and Steve Bellovin Addison-Wesley, 1994, ISBN 0-201-63357-4
- *Handbook of Computer-Communications Standards Volume 3: The TCP/IP Protocol Suite*William Stallings, Macmillan, 1990
- *Internetworking with TCP/IP, Volume 1*Douglas E. Comer, Prentice Hall, 1995, ISBN 0-13-216987-8
- *Network and Internetwork Security Principles and Practice*William Stallings, Prentice Hall, 1995, ISBN 0-02-415483-0
- *Practical UNIX and Internet Security*Simson Garfinkel and Gene Spafford, O'Reilly & Associates, 1996, 2nd edition, ISBN 1-56592-148-8
- *TCP/IP Illustrated, Volume 1 The Protocols*W. Richard Stevens, Addison-Wesley, 1994, ISBN 0-201-63346-9
- *TCP/IP Network Administration*Craig Hunt, O'Reilly & Associates, 1992
- *Network Security*Charlie Kaufman, Radia Perlman, and Mike Speciner Prentice Hall, 1995
- *SKIP IP-Level Cryptography* [http://skip.incog.com/]
- *Sun Software and Networking Security* [http://www.sun.com/security]

CHAPTER 1

# Introduction to Installing SunScreen EFS 3.0

This chapter introduces SunScreen EFS 3.0 installation concepts.

Topics covered include:

- What is SunScreen EFS 3.0
- Operating the firewall in routing mode
- Operating the firewall in stealth mode
- Before installing SunScreen EFS 3.0
- Upgrading from SunScreen EFS 1.1 or 2.0, to SunScreen EFS 3.0
- Upgrading from SunScreen SPF-200 to SunScreen EFS 3.0
- Converting from FireWall-1 to SunScreen EFS 3.0
- Security issues
- Software and hardware requirements
- Online help and documentation
- Installation problems

SunScreen EFS 3.0, software can be installed on a single machine (local administration) or on different machines (remote administration).

Remote administration includes the *Screen* and its *Administration Station*. Depending upon how you choose to deploy SunScreen EFS 3.0, the number of Screens and Administration Stations varies. You need a Screen at every point in the network where you want to restrict access. In the strictest sense, you need one Screen for each point in the network that has direct public access (usually one per site). One Administration Station can manage multiple Screens, although more Administration Stations can be installed for redundancy and ease of access. Encryption is used to

protect access and to limit management of a Screen to an authorized Administration Station.

# What Is SunScreen EFS 3.0

SunScreen EFS 3.0 is a software security solution, which is installed on a Solaris®™ -based machine. It lets companies connect their departmental networks to public internetworks securely. SunScreen EFS 3.0 functions as a firewall and router for hosts on the network it is protecting.

The Screen is the firewall responsible for screening packets. The Administration Station is used to define rules and to administer the Screen. The number of Screens and Administration Stations depends on your site's network topology and security policies.

## Local Administration

*Local administration* means that administration of the Screen is conducted on the Screen itself, as shown in Figure 1–1. Local administration does not require encryption as the processes are executing on the Screen. No network traffic is generated, and as such, local administration does not require or utilize encryption.

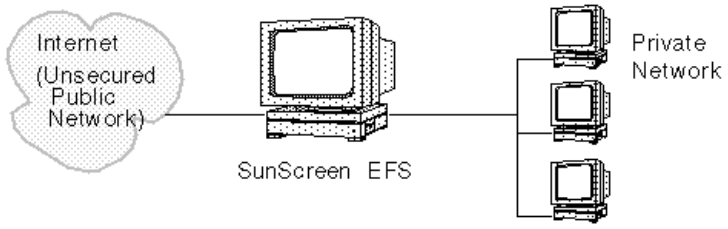



*Figure 1–1* Example of a Locally Administered SunScreen EFS

## Remote Administration

*Remote administration* means that administration of the Screen is conducted on an Administration Station, which is a separate machine from the Screen, as shown in Figure 1–2. Remote administration uses encrypted communication between the Screen and Administration Station to protect access and to limit the management of a Screen to an authorized Administration Station. The data which the administrator

sees is protected, so the information about the security policy in place on the Screen can not be obtained by others.

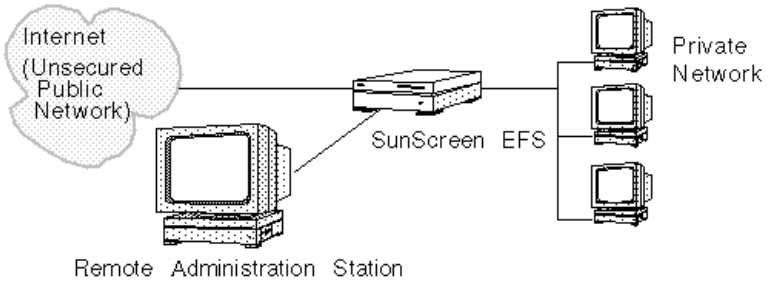



*Figure 1–2* Example of a Remotely Administered SunScreen EFS

The Screen may be both headless and keyboardless, and communicates with the Administration Station through a TCP/IP interface that need not be exposed to the Internet (although it may be exposed to the local network, depending on the topology you use, and your choice of operating in stealth or routing mode).

# Operating the Firewall in Routing Mode

Operate SunScreen EFS 3.0 in routing mode if you need routing functions in addition to firewall capabilities. In this mode, SunScreen EFS 3.0 operates as both a router and a firewall, with at least two exposed IP interfaces, and a hop visible to traceroute and other network utilities. Be aware that your firewall is visible when operating in routing mode, and you have a slightly greater exposure to attack than when operating in stealth mode.

Key differences when operating SunScreen EFS 3.0 in routing, rather than stealth, mode:

- The existing Solaris machine must be acting as a router.
- It makes use of the Solaris IP stack on the filtering interfaces, so it does not possess stealth characteristics.
- It provides IP routing.
- You must divide up different networks, like any router.
- The addition of a SunScreen to your network may require re-numbering IP addresses on your hosts, if you did not already have a router where your SunScreen is being placed.

# Operating the Firewall in Stealth Mode

Operate SunScreen EFS 3.0 in stealth mode if you do not need routing functions, or if you want to decrease possibilities for attacks. In stealth mode, SunScreen EFS 3.0 acts much like a bridge in that no IP interfaces are exposed to the public or private network, and packets are transparently passed through the Screen. While operating in this mode, the SunScreen cannot be attacked through any means other than a denial of service attack, and cannot be seen or detected through traceroute or similar network tools.

Key differences when operating SunScreen EFS in stealth, rather than routing, mode:

- Acts as a bridge, not a router.
- Never requires IP address re-numbering on hosts.
- Configure only the network interface you plan on using for remote administration.

**Caution -** Configuration of additional network interfaces may result in a non-operational Screen.

SunScreen EFS 3.0 allows the use of SPF-style stealth network interfaces. But it does not operate in the exact same fashion as a SunScreen SPF-200 does. Some notable differences between operating SunScreen EFS 3.0 in stealth mode, from the SunScreen SPF-200, are:

- It is a layered product instead of a dedicated installation. It is not able to detect all user installed services which may be vulnerable.
- It does not boot from the CD-ROM.
- An installation diskette is not required.
- Hardening of the OS is not mandatory.

# Before Installing SunScreen EFS 3.0

Before you install SunScreen EFS 3.0, complete the following tasks:

- Be acquainted with these documents:
  - *SunScreen EFS 3.0 Installation Guide*
  - *SunScreen EFS 3.0 Administration Guide*
  - *SunScreen EFS 3.0 Reference Manual*

- *SunScreen EFS 3.0 Release Notes*
- *SunScreen SKIP 1.5 User's Guide*

- Ensure that the system that is to run SunScreen EFS 3.0 is secure—consider reinstalling the Solaris operating environment from CD-ROM to ensure that it has not been altered.
- Install the recommended kernel and security patches.
- Ensure that a set of issued keys and certificates, if you are using them, is available for each host.

After installing SunScreen EFS 3.0, you are ready to set up and implement the security policy for your network. For instructions on administering your SunScreen, refer to the *SunScreen EFS 3.0 Administration Guide*.

# Upgrading From SunScreen 1.1 or 2.0 to SunScreen EFS 3.0

If you are presently running SunScreen EFS 1.1 or 2.0, and you want to use the same configurations when you upgrade to SunScreen EFS 3.0, read the information and instructions in Chapter 6.

**Caution -** To avoid corruption of your existing configurations, do not attempt to manually remove or add packages. Upgrading is *not* an initial installation, and the upgrade script removes packages as needed.

# Upgrading from SunScreen SPF-200 to SunScreen EFS 3.0

You can upgrade the same machine that operates as your SPF-200 Screen to become a SunScreen EFS 3.0 Screen operating in stealth mode. You can also transfer your SPF-200 configurations to a new machine, and perform the conversion on the new machine.

Since SunScreen EFS 3.0 uses ordered packet filtering rules and ordered NAT mappings, you must to review your packet filtering rules after the conversion is complete to verify the filtering order is as you want. NAT mappings have changed

considerably since the release of SPF-200. See the *SunScreen EFS 3.0 Reference Manual* for detail on NAT mappings.

Instructions for upgrading from SunScreen SPF-200 are in Chapter 6.

## Converting From FireWall-1 to SunScreen EFS 3.0

If you are presently using FireWall-1 and plan to use a similar security policy on *SunScreen EFS 3.0,* you have two ways to do this:

- You can convert the machine that is running FireWall-1 to become the SunScreen EFS 3.0 Screen.
- You can convert the security policy configurations on FireWall-1 and use them on a SunScreen EFS 3.0 machine.

Conversion instructions are in Chapter 7.

## Security Issues

The machines that are used as gateways, or that are in vulnerable positions on the network, should have only the minimum Solaris packages installed as designated. This way, fewer potentially exploitable applications are allowed.

If no Solaris applications or services are needed on a SunScreen machine, consider installing the software in stealth mode with the hardened OS feature. This is discussed in Chapter 5.

## Software and Hardware Requirements

Table 1–1 lists the minimum hardware and operating system requirements for installing SunScreen EFS 3.0.

**TABLE 1–1** SunScreen EFS 3.0 Installation Requirements

| Requirement | Description |
|---|---|
| Operating system | Solaris 2.6 or Solaris 7 operating environment for SPARC™ and Solaris x86 platforms.<br>Requires a Java-enabled Web browser compliant with JDK™ 1.1.3 or later. |
| Hardware | All SPARCStation, UltraSPARC, and x86 platforms supported by the Solaris 2.6 and Solaris 7 operating environment. |
| Disk space | Minimum of 1 Gbyte (>300Mbytes unused). |
| Memory | Administration Station: Minimum of 32-Mbytes, 64-Mbytes *strongly* recommended.<br>Screen: Minimum of 32–Mbytes. |
| Network interfaces | For SPARC systems: 10 Mbps or 100 Mbps Ethernet interfaces (`le`, `qe`, `hme`, `be`, `qfe`), or Token Ring, or ATM (155 and 622 Mbps in LAN emulation mode), or FDDI, or PCI-based Ethernet cards.<br>For x86 systems: 10 Mbps or 100 Mbps Ethernet interfaces (`dnet`, `elxl`).<br>Stealth mode supports 10 Mbps or 100 Mbps Ethernet only.<br>See supported devices listed at: http://access1.sun.com/driver/hcl/hcl.html |
| Media | CD-ROM drive and diskette drive. |

The Screen can support up to 15 network interfaces at one time.

A remote Administration Station can connect directly to a Screen only through an Ethernet local area network (LAN) or a Fiber Distributed Data Interface (FDDI). An Administration Station can connect to the Screen by an Asynchronous Transfer Mode (ATM) or Token Ring LAN, but only after it is connected directly to the network by way of an Ethernet or FDDI connection first.

SunScreen EFS 3.0 includes the SunScreen™ SKIP software.

The HotJava™ 1.1.5 browser is packaged on the SunScreen EFS 3.0 CD-ROM and is installed as part of the Default Install when using the installation wizard. If you do not want this version of HotJava installed, select Custom Install instead and deselect package `SUNWdthj`. The following Web browsers are supported:

- HotJava 1.1.5.
- Netscape Navigator™ 4.x with the Java™ plug-in. If you have Internet access, for information on the plug-in, go to http://java.sun.com/products/plugin/1.1.2/index-1.1.2.html.

If you do not have Internet access, we provide the Java plug-in, version 1.1.2, on the SunScreen EFS 3.0 CD-ROM. It is located in the directory `javaplugins`. To install it, see the SunScreen EFS 3.0 on-line help topic "Allow Local File Access".

- Internet Explorer (IE) 4.x with the Java plug-in on Windows 95/98 or NT only.
- Netscape Navigator 4.5 with its own Java, but this has the limitation that you can not read or write files.
- IE 4.01 with its own Java, but this has the limitation that you can not read or write files.
- For an Administration Station which remotely administers a Screen, SunScreen EFS 3.0 allows any machine with a Java-enabled web browser compliant with JDK 1.1.3 or later as an Administration Station, as long as it can connect securely to the Screen using SKIP. See Chapter 4 for more information.

# Online Help and Documentation

Context-sensitive help is available for each page of the Administration graphic user interface (GUI) for SunScreen EFS 3.0. To access the context-sensitive help, click the Help button on a GUI page.

SunScreen EFS 3.0 documentation is automatically installed from the CD-ROM. Once installed, click the Documentation button on the Administration GUI toolbar.

The man pages for SunScreen EFS administration commands are located in `/opt/SUNWicg/SunScreen/man`.

# Installation Problems

On certain workstations that have Solaris 7 pre-installed, problems using the SunScreen EFS 3.0 installation wizard can occur. These are described below.

## Re-install

If the installation wizard is used to install SunScreen EFS 3.0 and `pkgrm` is used to remove it, subsequent attempts to install using the installation wizard results in a message which says that the product is already installed. This can happen even after the software packages have been removed.

If this happens, exit the installation wizard and remove the SunScreen EFS 3.0 packages using `/usr/bin/prodreg` before attempting to re-install SunScreen EFS 3.0 using the installation wizard.

## Overinstall

If you attempt to install SunScreen EFS 3.0 on a machine that already has a complete installation, the installation wizard completes most of the installation but fails during the `pkgadd` of the `SUNWicgSS` package. It then proceeds to remove all packages added to that point.

Subsequent installations through the installation wizard `screenInstaller` or `pkgadd` and `ss_install` are successful.

## Uninstall

The panel displayed after the installation of SunScreen EFS 3.0 packages refers to a log file. This log file mentions the creation of an `uninstall` class during the installation process. Do not attempt the uninstall SunScreen EFS 3.0 with this `uninstall` class. It does not properly remove the SunScreen EFS 3.0 packages.

The correct method is to use `pkgrm` to remove the packages installed from the CD and to remove the `/etc/opt/SUNWicg`, `/var/opt/SUNWicg`, and `/etc/skip` directories. See Chapter 8 for instructions on removing the software.

CHAPTER 2

# Prerequisites for Installation

This chapter details the prerequisites recommended prior to installing SunScreen EFS 3.0.

Topics included are:

- Determine your security policy
- Determine your network configuration
- Determine your initial level of security
- Preparing for installation

Before installing, review the *SunScreen EFS 3.0 Release Notes* for the latest information about this product.

## Determine Your Security Policy

Before actually installing the SunScreen EFS 3.0 software, you should first determine your network security policy. For a more thorough discussion of this topic, we suggest you read *Computer Security Policies and SunScreen Firewalls* by Kathryn M. Walker and Linda Croswhite Cavanaugh. Additional resources are listed in the Preface.

In brief, considerations when creating a security policy are:

- what services do employees need to access?
- what services do customers need to access?
- will you allow Internet access, and if so, what services do users need to access?
- what type of threat are you trying to protect your company from?
- do you need to use Network Address Translation (NAT)?

# Determine Your Network Configuration

Prior to installing SunScreen EFS 3.0, you should make a map of your network. This will help identify any potential security problems inherent in the way the network is currently connected. A diagram of your network will aid installation and should include:

- Routers to the Internet
- FTP, WWW or TELNET servers
- Application relay servers
- Remote networks
- Internal subnetworks
- Your HA configuration
- Proxy services you plan to run

# Determining Your Initial Level of Security

You must determine your initial level of security. You have three possible security levels to choose from when installing SunScreen EFS 3.0 in routing mode. Each security level corresponds to a different set of network services permitted to, from, and through the Screen. If you are in doubt about which security level to select for the `Initial` configuration, use a more permissive security mode. You can always reconfigure it to be more secure by changing the rules using the Administration GUI.

The security levels are as follows:

- *Restrictive* – This level of security denies all traffic to, from, and through the Screen, except encrypted administration traffic. This level is best for deploying the Screen in a hostile network environment. It requires that static routing and the naming service have been configured on the host (that is, names must be resolved by means of a local `hosts` file).
- *Secure* – This level of security denies all traffic to and through the Screen, except encrypted administration traffic. It allows common services (like NFS) *from* the Screen, naming service selection (such as, DNS and NIS), and routing (RIP). This level is a good starting point to get a Screen up and running on a friendly network, where the Screen may not be a stand-alone machine and may depend on NIS, DNS, or NFS to function properly.

- *Permissive* – This level allows the same traffic as the Secure level with the addition of allowing inbound connections to the Screen itself and allowing all traffic through the Screen. This security level is for installing the Screen onto a machine that has multiple network interfaces and is acting as a router, or on a machine that is acting as a server (for example, for NFS, NIS, or HTTP).

You must also determine which naming service to use. You may choose one (NIS or DNS), both (NIS and DNS), or none. For none, deselect both.

In routing mode, SunScreen EFS 3.0 automatically installs all Ethernet interfaces that have been configured on the machine. In stealth mode, *only* the interface used for remote administration should be configured, and the other interfaces must not be configured.

If you are converting FireWall-1 configurations for use on SunScreen EFS 3.0, or when planning to convert a FireWall-1 machine to a SunScreen EFS 3.0 machine, read the information and instructions in Chapter 7 first.

Once the following preparation criteria are met, continue to the appropriate chapter for your particular installation.

# Preparing for Installation

The following sections describe how to prepare for initial installations on both locally and remotely administered SunScreen EFS 3.0 machines.

## Preparing the Screen and Administration Station

SunScreen EFS 3.0 runs on Solaris 2.6 and Solaris 7 operating environments for SPARC and x86 platforms. If you are running Solaris 2.5.1, or earlier, you must upgrade your operating environment to at least Solaris 2.6.

Minimally, the Screen must have installed the Core System Support software group, and the Administration Station must have installed the End User Distribution software group. Prior to installing SunScreen EFS 3.0, additional Solaris packages are required and must be installed.

**Caution -** Do not reinstall the Core System Support software group if you are upgrading from either SunScreen EFS 1.1 or 2.0 to SunScreen EFS 3.0, as described in Chapter 6.

## ▼ To Install the Prerequisite Solaris Packages and Kernel Patches on the Screen

1. **Add the following packages to the Screen from your Solaris CD, if not already on your system:**

   system SUNWdoc Documentation Tools
   system SUNWeuluf UTF-8 L10N For Language Environment User Files
   system SUNWjvjit Java JIT compiler
   system SUNWjvrt JavaVM run time environment
   system SUNWlibC SPARCompilers Bundled libC
   system SUNWlibms SPARCompilers Bundled shared libm
   system SUNWsprot SPARCompilers Bundled tools
   system SUNWtoo Programming Tools
   system SUNWvolr Volume Management (Root)
   system SUNWvolu Volume Management (Usr)
   system SUNWxwice ICE components
   system SUNWxwplt X Window System platform software
   system SUNWxwrtl X Window System & Graphics Runtime Library Links
   system SUNWmfrun Motif RunTime Kit

2. **If you are using Solaris 2.6 as your operating environment, add the following patches, if not already on your system, by typing:**

```
For SPARC systems:
# cd /cdrom/cdrom0/sparc/Patches
# patchadd 106125-06
# patchadd 105181-11
# patchadd 105284-15
# patchadd 105490-04
# patchadd 106040-10
# patchadd 106409-01

For x86 systems:
# cd /cdrom/cdrom0/i386/Patches
# patchadd 106126-06
# patchadd 105182-13
# patchadd 105285-15
# patchadd 105491-04
# patchadd 106041-10
# patchadd 106410-01
```

**Note -** These patches must be added in the order given.

3. **Reboot by typing:**

```
# sync; init 6
```

4. **If you will be operating the SunScreen in routing mode, configure all network interfaces that will be used.**

   See the documentation accompanying the Solaris operating environment, if needed.

5. **If you will be operating the SunScreen in stealth mode, configure only the network interface that will be used for remote administration.**

   See the documentation accompanying the Solaris operating environment, if needed.

## ▼ To Install the Prerequisite Solaris Packages on the Administration Station

1. **If you will be using a remote administration station, add the following packages to the Administration Station from your Solaris CD, if not already on your system:**

   system SUNWjvrt JavaVM run time environment

   system SUNWmfrun Motif RunTime Kit

   system SUNWxwplt X Window System Platform software

2. **If you are using Solaris 2.6 as your operating environment, add the following patches, if not already on your system, by typing:**

```
For SPARC systems:
# cd /cdrom/cdrom0/sparc/Patches
# patchadd 106125-06
# patchadd 105284-15
# patchadd 105490-04
# patchadd 106040-10
# patchadd 106409-01

For x86 systems:
# cd /cdrom/cdrom0/i386/Patches
```

**(continued)**

**(Continuation)**

```
# patchadd 106126-06
# patchadd 105285-15
# patchadd 105491-04
# patchadd 106041-10
# patchadd 106410-01
```

CHAPTER 3

# Installing in Routing Mode

This chapter explains how to install a SunScreen EFS 3.0 in routing mode with local administration. In this configuration, SunScreen EFS 3.0 is installed on a single machine and does not have to use SKIP. Use this installation method if you need routing functions in addition to firewall capabilities, as the SunScreen will function both as a router and a firewall.

Topics covered include:

- Installation of the software on a single machine
- Setting of the PATH and installing SKIP upgrades
- Launching the Administration GUI

SunScreen EFS 3.0 runs on the Solaris 2.6 and Solaris 7 operating environment for SPARC or x86 systems. If you are presently running Solaris 2.5.1 or lower, you must ugrade your operating environment before proceeding.

If you want to install SunScreen EFS 3.0 in routing mode with remote administration, read the information and instructions in Chapter 4.

If you want to install SunScreen EFS 3.0 in stealth mode, read the information and instructions in Chapter 5.

If you are presently running SunScreen EFS 1.1 or 2.0, and want to upgrade to SunScreen EFS 3.0, read the information and instructions in Chapter 6.

If you are presently running SunScreen SPF-200 and want to upgrade to SunScreen EFS 3.0, read the information and instructions in Chapter 6.

If you are converting a running FireWall-1 machine, Release 2.1 or 3.0 to a SunScreen EFS 3.0 machine, read the information and instructions in Chapter 7.

Before installing, review the *SunScreen EFS 3.0 Release Notes* for the latest information about this product.

# Installation in Routing Mode With Local Administration

The following procedures explain how to install SunScreen EFS 3.0 with local administration. Installation is performed on a single machine. Prior to installation, make sure the machine is performing properly as a router.

Do not begin this procedure until you have read the information in Chapter 2.

**Caution -** The installation procedure requires that the machine be rebooted when indicated. Do not perform any other tasks on the machine while installing the software, as a delay in rebooting the machine may affect installation and cause your system to hang.

## ▼ To Install SunScreen EFS Using the Installation Wizard

The installation wizard will guide you through this procedure. You must be on the machine you are installing on in order to use the wizard and must not telnet to the machine.

**Note -** While following this procedure, accept all defaults as given. If you want to choose another option when presented, you should quit the installation wizard and use the appropriate installation procedure. If this happens, see the Table of Contents to locate the correct chapter.

1. **Configure all network interfaces you plan on using.**

   Before continuing with installation, configure all network interfaces you plan on using, if not already done. In routing mode, SunScreen EFS 3.0 will only see the network interfaces that Solaris sees. For details on Solaris network configuration, see the documentation accompanying the Solaris operating environment.

2. **Open a terminal window and become root.**

**Caution -** Ensure that the OpenWindows™ File Manager is not running because it interferes with the operation of the `volcheck` command used for installation.

3. **Insert the SunScreen EFS 3.0 CD-ROM into the CD-ROM drive.**

4. **Mount the CD-ROM by typing:**

```
# volcheck
```

5. **Add the software by typing**

```
# /cdrom/cdrom0/screenInstaller
```

:

---

**Note -** Due to late software changes, the appearance of the installation wizards may differ slightly from that shown. Functionality and performance is not affected. The panels of the installation wizards can be resized, if needed.

---

The SunScreen EFS 3.0 Screen Install's Welcome window appears, as shown in Figure 3–1.


*Figure 3–1* Screen Install Wizard's Welcome Window

**6. Click Next to continue the installation process.**

The Checking Installed Solaris Packages window appears, as shown in Figure 3–2. Prior to installation of the SunScreen EFS 3.0 software, a check is performed to verify that the prerequisite Solaris packages are installed on your machine.

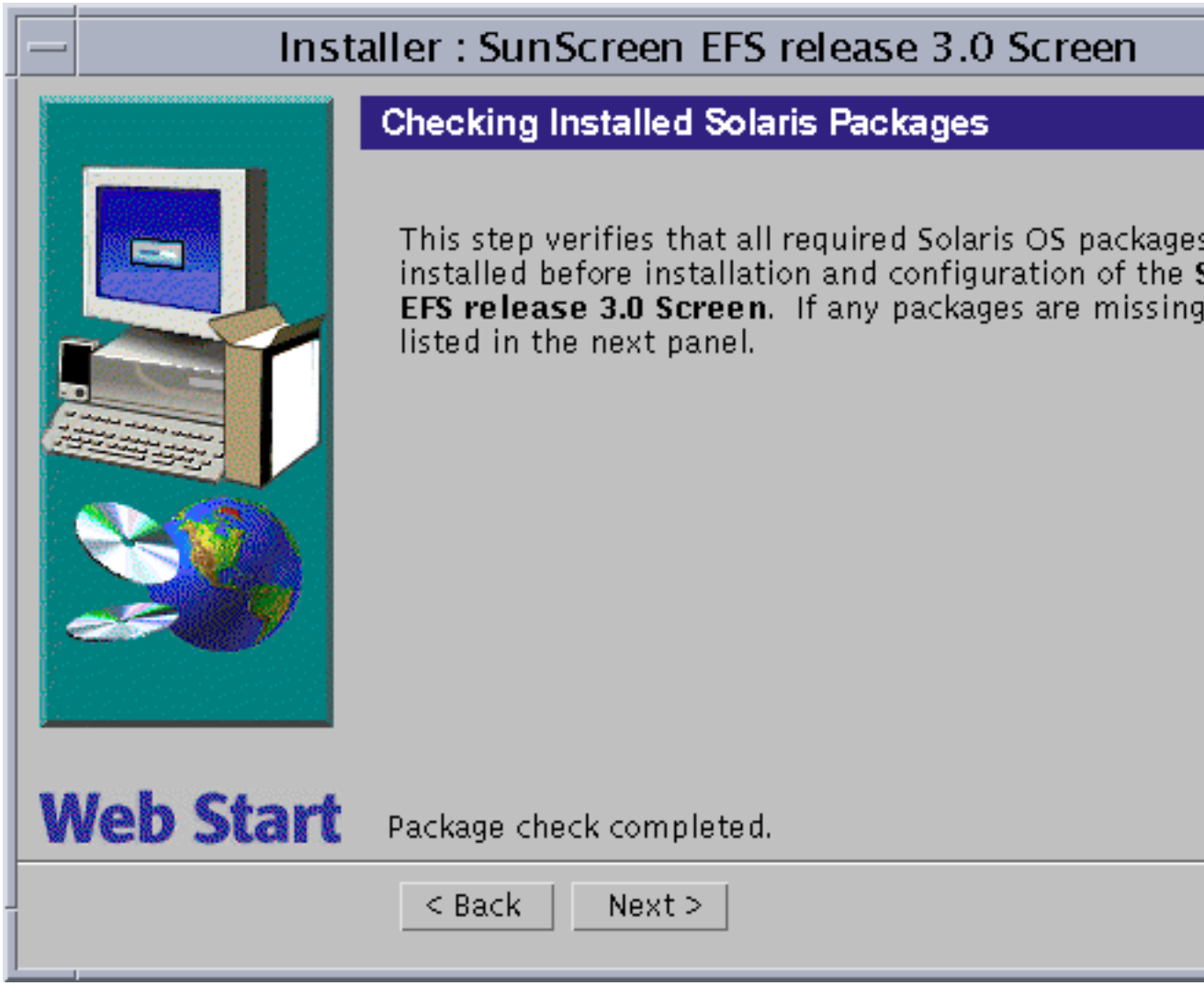



*Figure 3–2* Checking Installed Solaris Packages Window

---

**Note -** If there are missing required packages, a list will be displayed. You must exit the installation wizard at this point and install the required Solaris packages from your Solaris CD.

---

**7. Click Next to continue the installation process.**

The Secondary HA Designation window appears, as shown in Figure 3–3. No is the default.

Choose Yes if you are configuring an HA cluster and are installing the Secondary SunScreen of that cluster. If this is what you want to do, exit the installation wizard and see the *SunScreen EFS 3.0 Administration Guide* for instructions on how to set-up an HA cluster.


*Figure 3–3* Secondary HA Designation Window

8. **Click Next to continue the installation process.**

   The Select Screen Type window appears, as shown in Figure 3–4. You are given two types of installations to choose from: Stealth or Routing. Routing mode is the default.

   If you want to install in stealth mode, exit the installation wizard and see Chapter 5 of this book.


*Figure 3–4* The Select Screen Type Window With Routing Selected

**9. Accept the default, Routing, and Click Next.**

The Select Administration Type(s) window appears, as shown in Figure 3–5. You are given the choice of Local Administration, or Remote Administration, or both. Both are selected when there is a monitor on the Screen and you want an additional Administration Station. Local Administration is the default.

If you want to install a remotely administered SunScreen, exit the installation wizard and see Chapter 4.


*Figure 3–5* Select Administration Type(s) Window with Local Administration Selected

**10. Accept the default, Local Administration, and Click Next.**

The Select Type of Install window appears, as shown in Figure 3–6. You are given two choices: Default Install and Custom Install.

---

**Note -** The HotJava browser, version 1.1.5, is packaged on the SunScreen EFS 3.0 CD-ROM and is installed as part of the Default Install. If you do not want this installed, select Custom Install and deselect package `SUNWdthj`.

---


*Figure 3–6* Select Type Of Install Window With Default Install Selected

**11. Select the type of install desired, and Click Next.**

The disk space on your machine is checked. An error message appears if you do not have enough disk space.

The Ready to Install window appears, as shown in Figure 3–7. The size of the packages to be installed is confirmed.


*Figure 3–7* Ready To Install Window

**12. Click Install Now to continue the installation process.**

The Installing window appears, as shown in Figure 3–8. The status bar shows the progress of the installation.

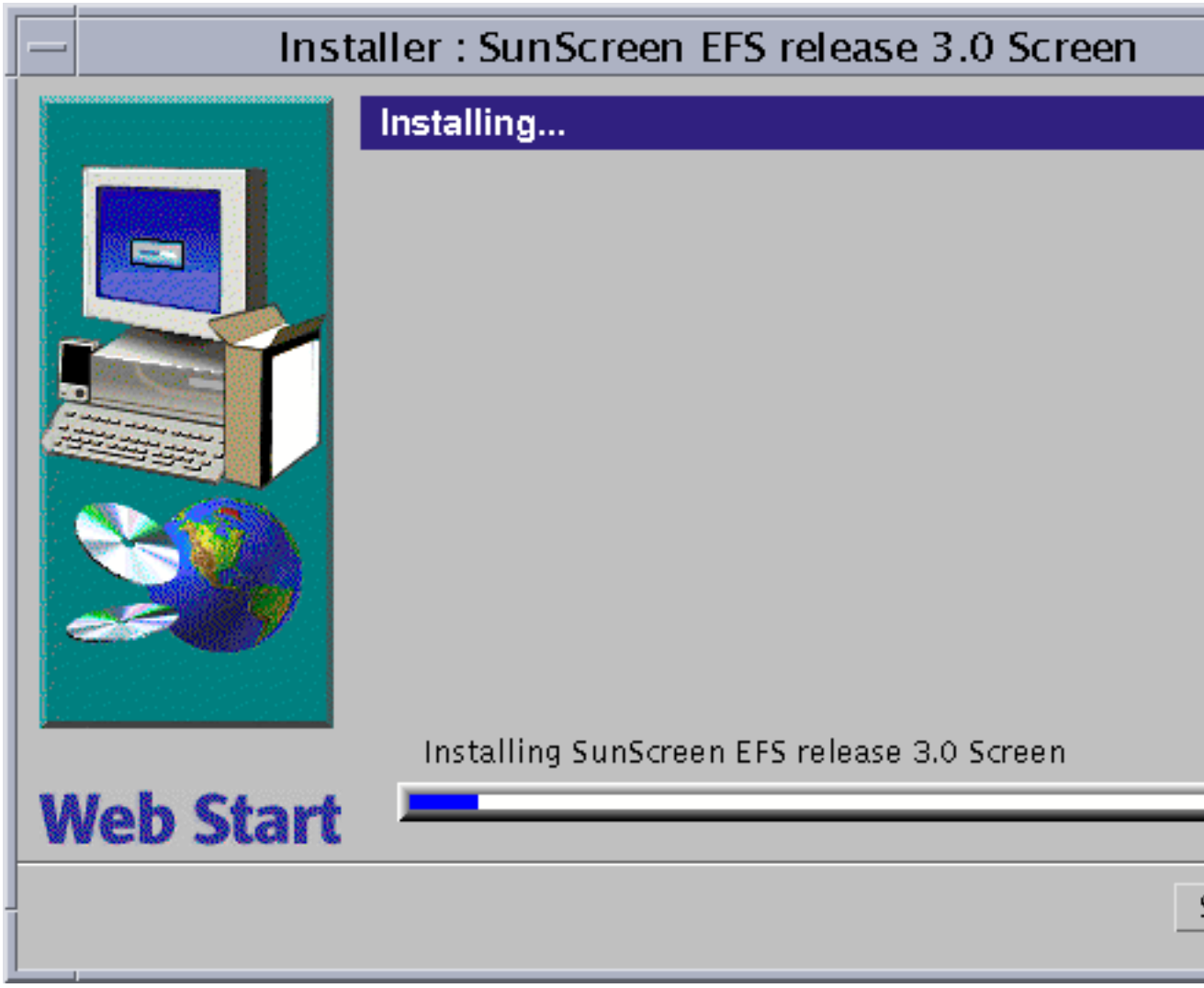



*Figure 3–8* Installing Window Showing Installation Status Bar

Once completed, the Select Initial Security Level window appears.

**13. Select the level of security you want: Restrictive, Secure, or Permissive. Permissive is the default.**

When in doubt, select Permissive as your initial security level, as shown in Figure 3–9. You can change this later if you need to.


*Figure 3–9* Select Initial Security Level Window With Permissive Selected

**14. Click Next to continue the installation process.**

The Select Name Service(s) window appears, as shown in Figure 3–10. You must select the name service that will be used on the Screen. Your choices are both NIS and DNS, either NIS or DNS, or None. For None, deselect both.

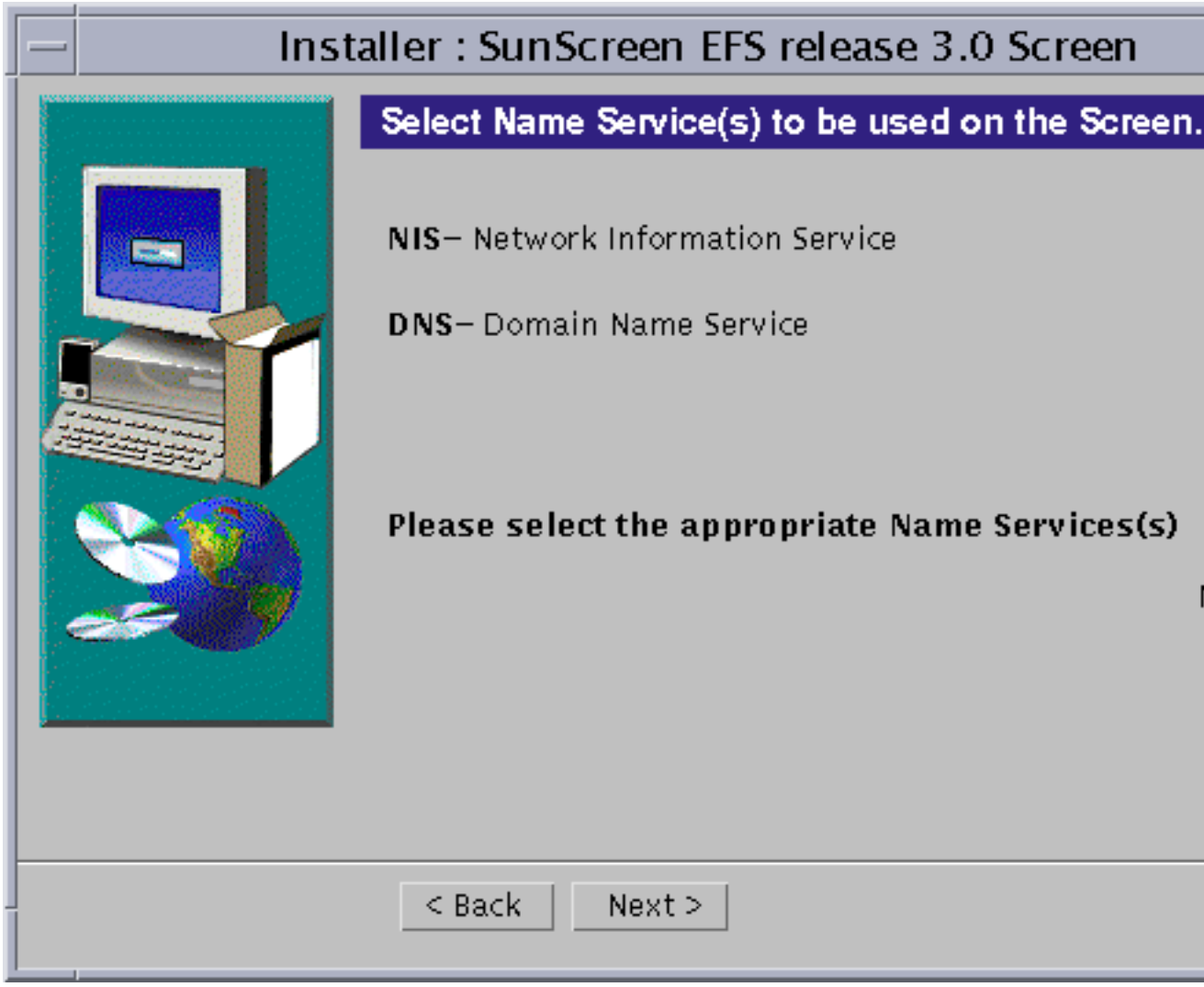



*Figure 3–10* Select Name Service(s) Window With Both NIS And DNS Selected

**15. Click Next to continue the installation process.**

The Screen Configuration window appears with the message: `Configuring Screen`, as shown in Figure 3–11. Figure 3–12 shows the message which appears once the Screen is successfully configured.

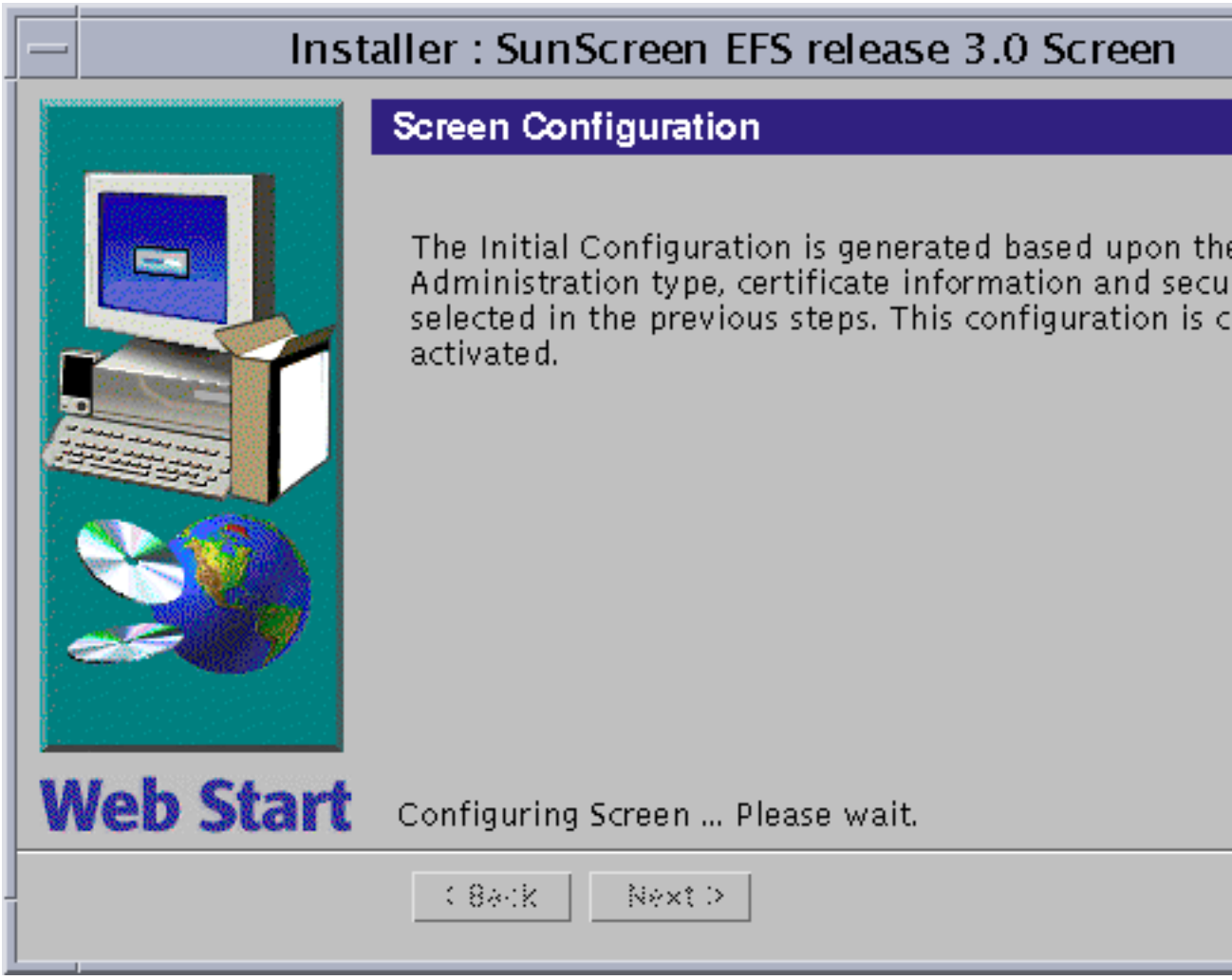



*Figure 3–11* Screen Configuration Window

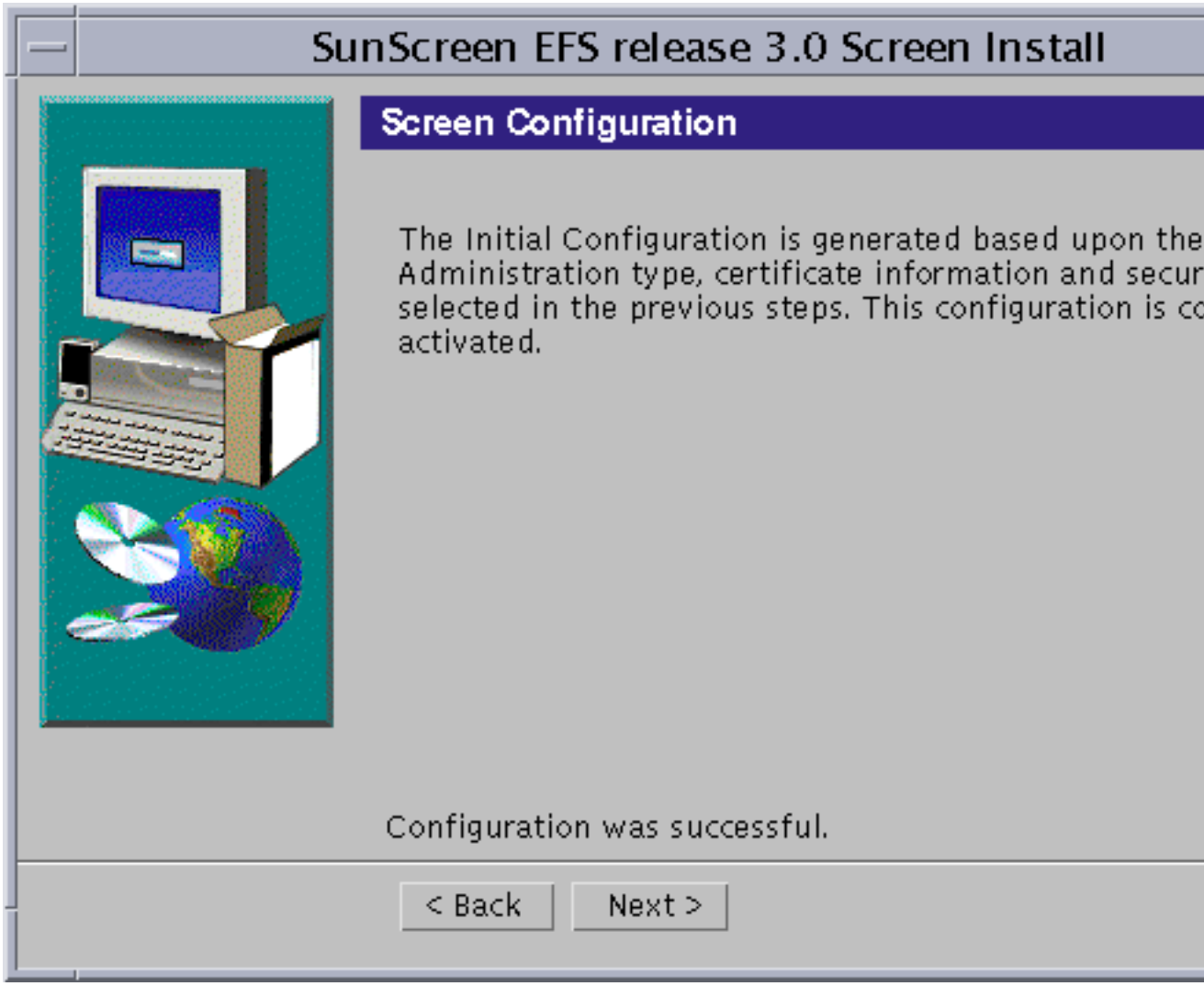



*Figure 3–12* The Screen Configuration Window Once Screen Is Successfully Configured

**16. Click Next to continue the installation process.**

The Screen Reboot window appears.

**17. To reboot the machine, Click the Screen Reboot button.**

The installation wizard disappears.

**Note -** You must reboot the machine at this time in order to complete the installation process.

## ▼ To Set the PATH and Install SKIP Upgrades

1. **Open a terminal window and become root, if not already.**

2. **Set the** `PATH` **and** `MANPATH` **by editing your shell initialization file (such as** `.profile` **or** `.login` **file).**

   a. **Set the** `PATH` **for the Bourne shell by typing:**

   ```
   PATH=/opt/SUNWicg/SunScreen/bin:$PATH
   PATH=/usr/dt/bin:$PATH
   export PATH
   ```

   **Set the** `MANPATH` **for the Bourne shell by typing:**

   ```
   MANPATH=$MANPATH:/opt/SUNWicg/SunScreen/man
   export MANPATH
   ```

3. **Install any SKIP upgrades (Export Controlled [1024–bit] or U.S. and Canada Use Only [2048–bit] keys) as instructed in the documentation that is included with the SKIP upgrade CD-ROM.**

   While the use of encryption is not required in a locally administered Screen, you may want to use encryption for communication over public and private networks.

4. **If SKIP upgrades were installed, reboot by typing:**

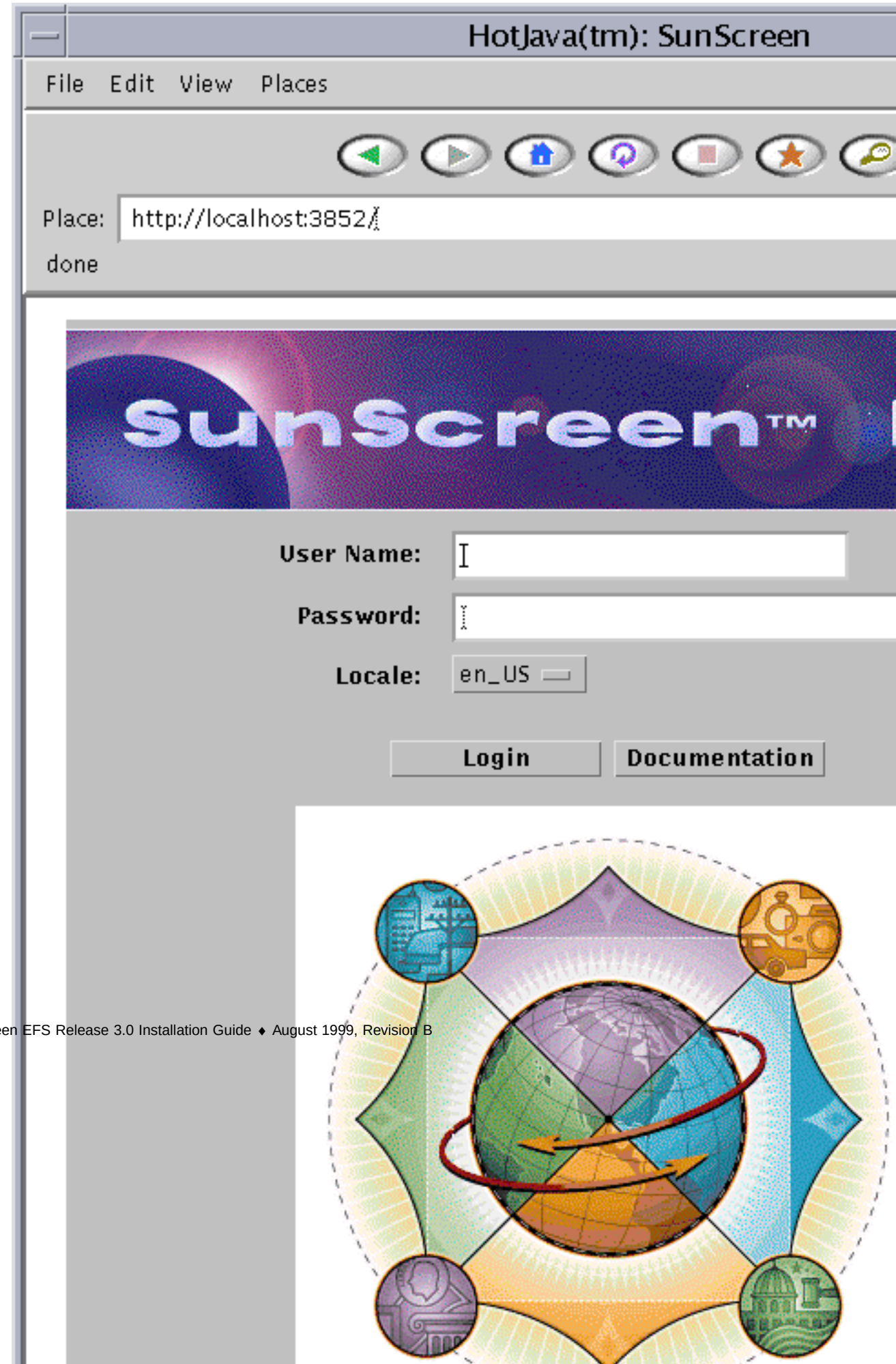
```
# sync; init 6
```

## ▼ To Launch the Administration GUI

1. **To configure and manage your SunScreen from your Administration Station, open a Java-enabled web browser compliant with JDK 1.1.3 or later, and launch the Administration GUI by typing the following URL:**

```
http://localhost:3852
```

The SunScreen EFS Administration GUI appears, as shown in Figure 3–13.


HotJava(tm): SunScreen
File Edit View Places
Place: http://localhost:3852/
done
SunScreen™
User Name:
Password:
Locale:
en_US
Login
Documentation

2. **To login, type the following and Click Login**:

```
User Name: admin
Password: admin
```

You next configure and manage your SunScreen with the Administration GUI. See the *SunScreen EFS 3.0 Administration Guide* for further instructions.

CHAPTER 4

# Installing In Routing Mode With Remote Administration

This chapter explains how to install SunScreen EFS 3.0 on remotely administered SunScreen machines. The software is first installed on the machine that will be the Administration Station, and then on the machine that will be the Screen. Encrypted communication between the Administration Station and the Screen is achieved by use of SunScreen™ SKIP (Simple Key-Management for Internet Protocols).

Topics covered include:

- Supported configurations for the Administration Station
- Installing a remotely administered SunScreen
- Installing the software on the Administration Station
- Installing certificates on the Administration Station
- Installing the software on the Screen
- Using SKIP for encrypted communication

If you are installing on a system without a monitor, using the command line for installation is discussed in Appendix A.

If you want to install SunScreen EFS 3.0 in stealth mode, read the information and instructions in Chapter 5.

If you are presently running SunScreen EFS 1.1 or 2.0, and want to upgrade to SunScreen EFS 3.0, read the information and instructions in Chapter 6.

If you are converting FireWall-1 configurations for use on a SunScreen EFS 3.0, or are planning to convert a FireWall-1 machine to a SunScreen EFS 3.0 machine, read the information and instructions in Chapter 7.

SunScreen SKIP is bundled with and installed as part of SunScreen EFS 3.0. For more information regarding SKIP, refer to the *SunScreen SKIP 1.5 User's Guide.*

Before installing, review the *SunScreen EFS 3.0 Release Notes* for the latest information about this product.

# Supported Configurations For The Administration Station

SunScreen EFS 3.0 allows any machine with a Java-enabled web browser compliant with JDK 1.1.3 or later as an Administration Station, as long as it can connect securely to the Screen using SKIP. The SunScreen EFS 3.0 CD-ROM includes SunScreen SKIP for both SPARC and x86 platforms. This allows any hardware running the Solaris 2.6 or Solaris 7 operating environment to be an Administration Station.

PCs operating Windows 95 or NT 4.x are a supported platform as an Administration Station, using the Administration GUI. This chapter, however, covers Solaris-based Administration Stations only.

# Installing a Remotely Administered SunScreen

This chapter explains how to install SunScreen EFS 3.0 in routing mode with remote administration, using either self-generated or issued certificate technology.

This type of installation requires several steps to complete. You proceed in the following order:

1. Install the SunScreen Administration software on the Administration Station.

This step installs the required SKIP packages on the Administration Station. This is the first prerequisite to creating a secure method of communication between the Administration Station and the Screen. The use of SKIP technology enables encrypted communication between the two.

1. Install the Administration certificate on the Administration Station.
2. Install the SunScreen software on the Screen.

This procedure requires the Administration Station's certificate ID and installs the Screen's certificate.

1. Install the Screen's certificate ID on the Administration Station.
2. Start encrypted communication between the Administration Station and the Screen by enabling SKIP on the Administration Station.

**Note -** The installation procedure requires that the machine be rebooted when indicated. Do not perform any other tasks on the machine while installing the software, as a delay in rebooting the machine may affect installation and cause your system to hang.

Do not begin this procedure until you have read the information in Chapter 2.

## ▼ To Install the Software on the Administration Station Using the Installation Wizard

1. **Open a terminal window on the Administration Station and become root.**

**Caution -** Ensure that the OpenWindows File Manager is not running because it interferes with the operation of the `volcheck` command used for installation.

2. **Insert the SunScreen EFS 3.0 CD-ROM into the Administration Station's CD-ROM drive.**

3. **Mount the CD-ROM by typing:**

```
# volcheck
```

4. **Add the software by typing**

```
# /cdrom/cdrom0/adminInstaller
```

:

**Note -** Due to late software changes, the appearance of the installation wizards may differ slightly from that shown. Functionality and performance is not affected. The panels of the installation wizards can be resized, if needed.

The Admin Install's Welcome window appears, as shown in Figure 4–1.


*Figure 4–1* Admin Install Wizard's Welcome Window

**5. Click Next to continue the installation process.**

The Select Type of Install window appears. You are given two choices: Default Install and Custom Install.

**Note -** The HotJava browser, version 1.1.5, is packaged on the SunScreen EFS 3.0 CD-ROM and is installed as part of the Default Install. If you do not want this installed, select Custom Install and deselect package `SUNWdthj`.

**6. Select the type of install desired, and Click Next.**

The disk space on your machine is checked. An error message appears if you do not have enough disk space.

The Ready to Install window appears, as shown in Figure 4–2. The size of the packages to be installed is confirmed.

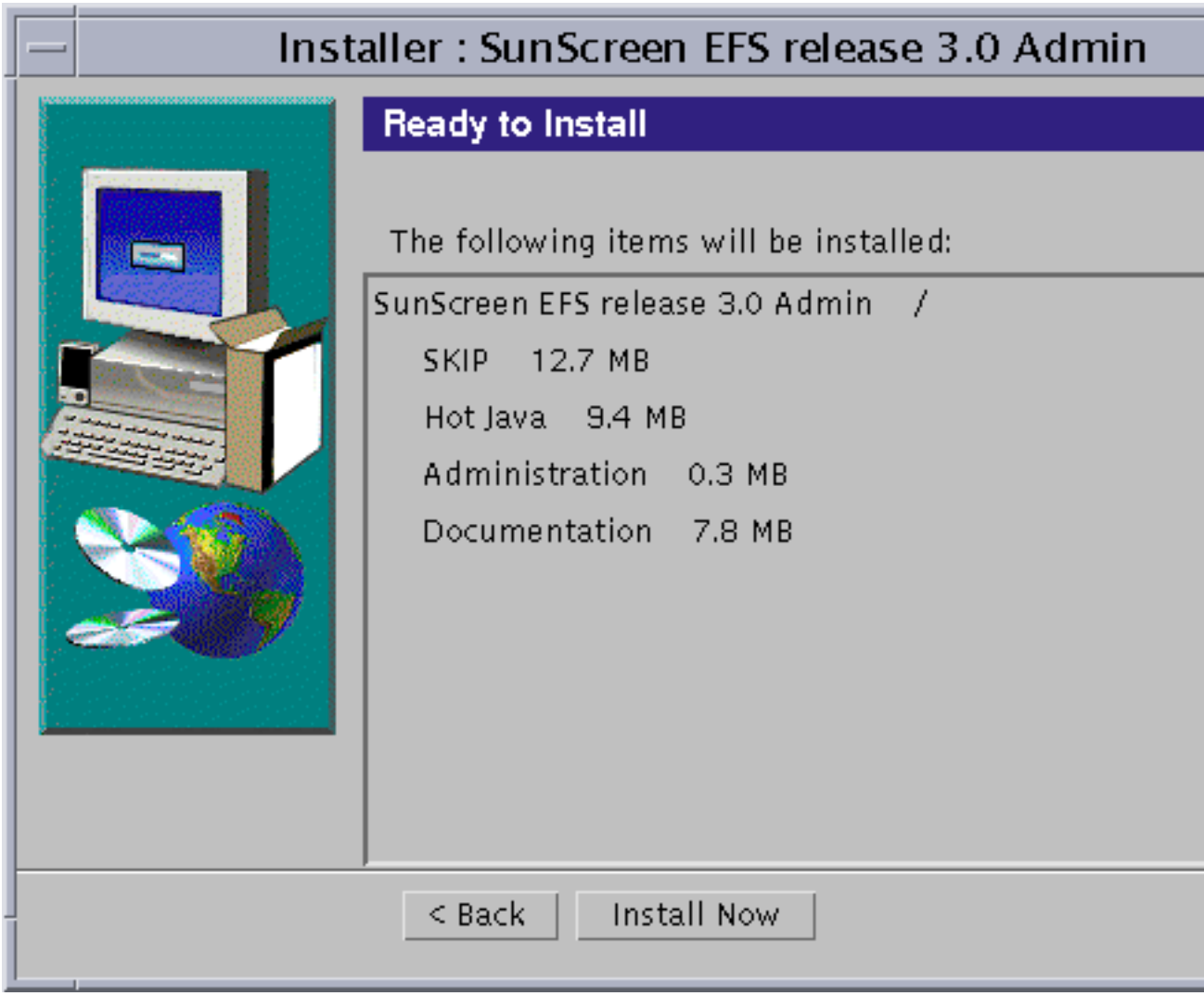



*Figure 4–2* Ready To Install Window

**7. Click Install Now to continue the installation process.**

The Installing window appears, as shown in Figure 4–3. The status bar shows the progress of the installation.

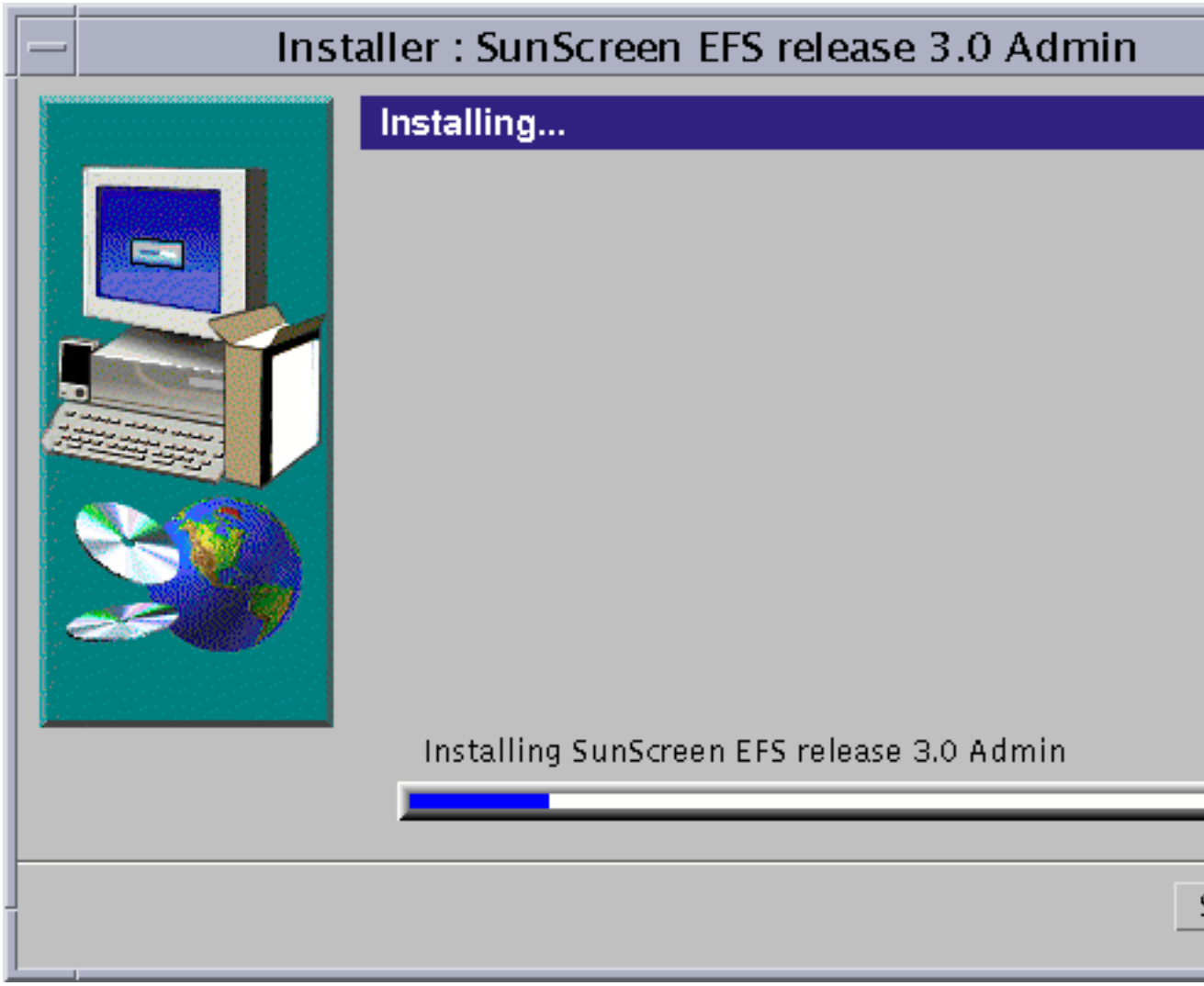



*Figure 4–3* Installing Window Showing Installation Status Bar

**8. Click Next to complete the installation process.**

An Installation Summary appears, as shown in Figure 4–4.

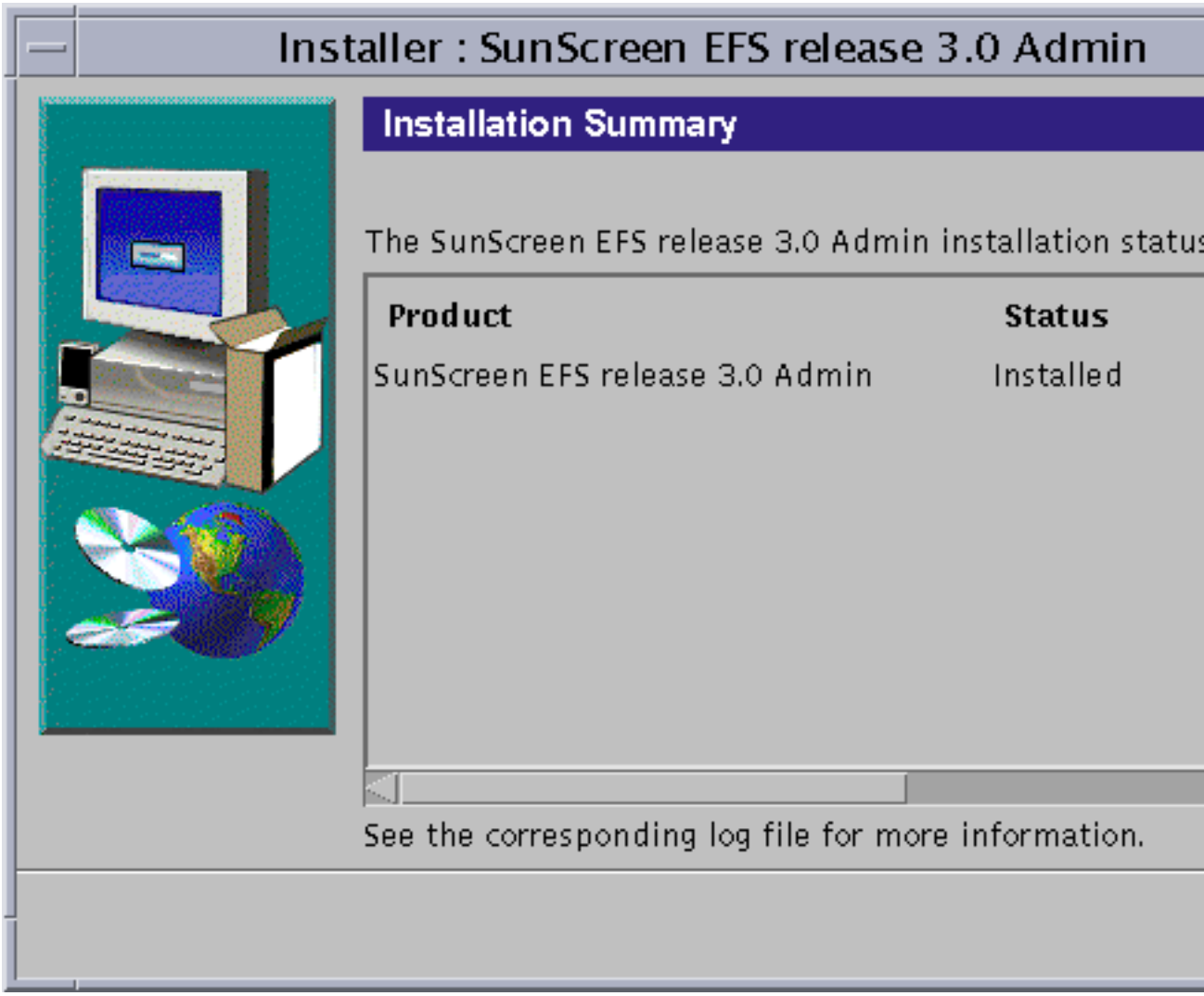



*Figure 4–4* Installation Summary Window

**9. Select Exit to complete the installation process using the installation wizard.**

The installation wizard disappears.

**10. Set the** `PATH` **and** `MANPATH` **by editing your shell initialization file (such as** `.profile` **or** `.login` **file).**

**a. Set the** `PATH` **for the Bourne shell by typing:**

```
PATH=/opt/SUNWicg/SunScreen/bin:$PATH
```

```
PATH=/usr/dt/bin:$PATH
export PATH
```

**b. Set the** `MANPATH` **for the Bourne shell by typing:**

```
MANPATH=$MANPATH:/opt/SUNWicg/SunScreen/man
export MANPATH
```

**11. Eject the CD-ROM from the CD-ROM drive by typing:**

```
# eject cdrom0
```

**12. Install any SKIP upgrades (Export Controlled [1024–bit] or U.S. and Canada Use Only [2048–bit] keys) as instructed in the documentation that is included with the SKIP upgrade CD-ROM.**

**13. Reboot to complete the installation by typing:**

```
# sync; init 6
```

The software packages have been installed. You continue the installation process on the machine that is the Administration Station.

## Installing Certificates on the Administration Station

To obtain encrypted communication between the Administration Station and the Screen, certificates must be installed on both machines. This can be done by either using self-generated certificates or by installing issued certificates. Both methods are done on the Administration Station.

If you are using self-generated certificates, use Option 1. If you are using issued certificates, use Option 2.

## ▼ Option 1: To Create a Self-Generated Certificate on the Administration Station

1. **Open a terminal window and create the required SKIP directories by typing:**

```
# skiplocal -i
```

2. **Create the self-generated certificate on the Administration Station by typing:**

```
# skiplocal -k -f -V
```

The local certificate ID appears, as shown in Figure 4–5. It is the Administration Station's 32-character certificate ID (MKID).

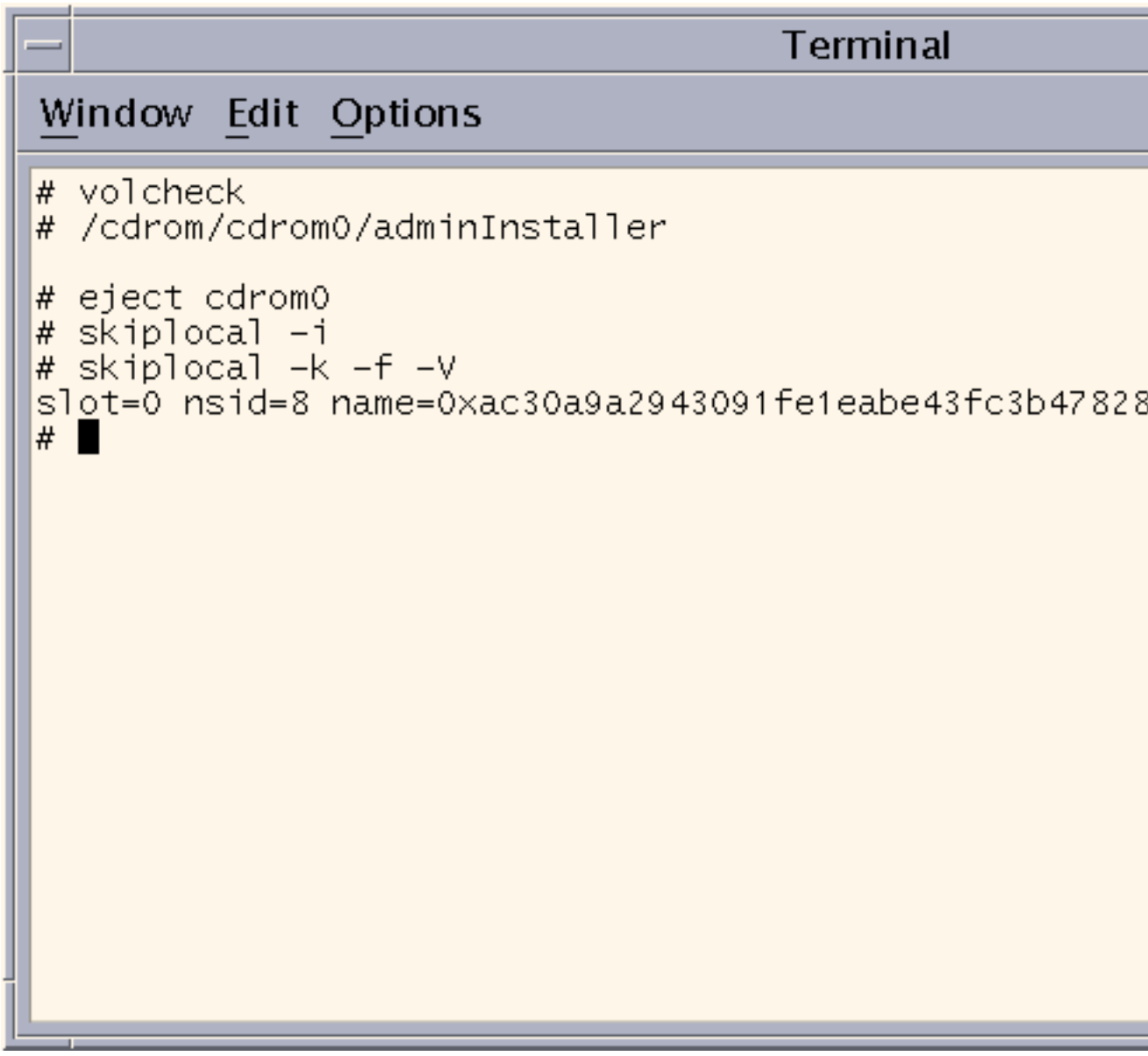



*Figure 4–5* Administration Station's Self-Generated Certificate

**3. Write down the certificate ID, which begins with 'Ox'.**

**4. Add SKIP to all the interfaces by typing:**

```
# skipif -a
```

5. **Reboot to complete the installation by typing:**

```
# sync; init 6
```

The Administration Station's certificate ID has been generated. You next move to the Screen to install the SunScreen software. Continue to the section, "Installing the Software on the Screen" on page 49"Installing the Software on the Screen" on page 49.

## ▼ Option 2: To Install the Issued Certificate on the Administration Station

To do this procedure, you will need the Key and Certificate diskette.

1. **Open a terminal window on the Administration Station and become root.**

**Caution -** Ensure that the OpenWindows File Manager is not running because it interferes with the operation of the `volcheck` command used for installation.

2. **Create the required SKIP directories by typing:**

```
# skiplocal -i
```

3. **Insert the Key and Certificate diskette into the Administration Station's floppy drive.**

4. **Mount the diskette by typing:**

```
# volcheck
```

5. **Install the SKIP keys by typing:**

```
# install_skip_keys -icg /floppy/floppy0
```

6. **Start the SKIP daemon by typing:**

```
# skipd_restart
```

7. **Eject the Key and Certificate diskette by typing:**

```
# eject floppy0
```

8. **Write down the certificate ID, which is eight characters long.**

9. **Add SKIP to all the interfaces by typing:**

```
# skipif -a
```

10. **Reboot to complete the installation by entering:**

```
# sync; init 6
```

The Administration Station's certificate ID has been installed. You next move to the Screen to install the SunScreen software.

## Installing the Software on the Screen

The next step is to install the SunScreen EFS 3.0 software on the machine that serves as the Screen. If you have a monitor and a keyboard attached to your Screen, you can use the installation wizard. If you are operating the Screen without a monitor, you must either temporarily attach a monitor, or install the software via the command line. Command line instructions are located in the Appendix A.

If you are using self-generated certificates, use Option 1. If you are using issued certificates, use Option 2.

---

**Note -** Before starting the procedure below, configure all network interfaces you plan on using, if not already done. SunScreen EFS will only see the network interfaces that Solaris sees. For details on Solaris network configuration, see the documentation accompanying the Solaris operating environment.

---

## ▼ Option 1: To Install the Software on the Screen When Using Self-Generated Certificates

---

**Note -** In this procedure, you need the Administration Station's certificate ID (MKID) from the previous procedure.

---

1. **On the Screen, open a terminal window and become root.**

2. **Insert the SunScreen EFS 3.0 CD-ROM into the Screen's CD-ROM drive.**

3. **Mount the CD-ROM by typing:**

```
# volcheck
```

4. **Add the software by typing:**

```
# /cdrom/cdrom0/screenInstaller
```

The Screen Install wizard's Welcome window appears, as shown in Figure 4–6.


*Figure 4–6* Screen Install Wizard's Welcome Window

**5. Click Next to continue the installation process.**

The Check Installed Solaris Packages window appears, as shown in Figure 4–7. Prior to installation of the SunScreen EFS 3.0 software, a check is performed to verify that the prerequisite Solaris packages are installed on your machine.

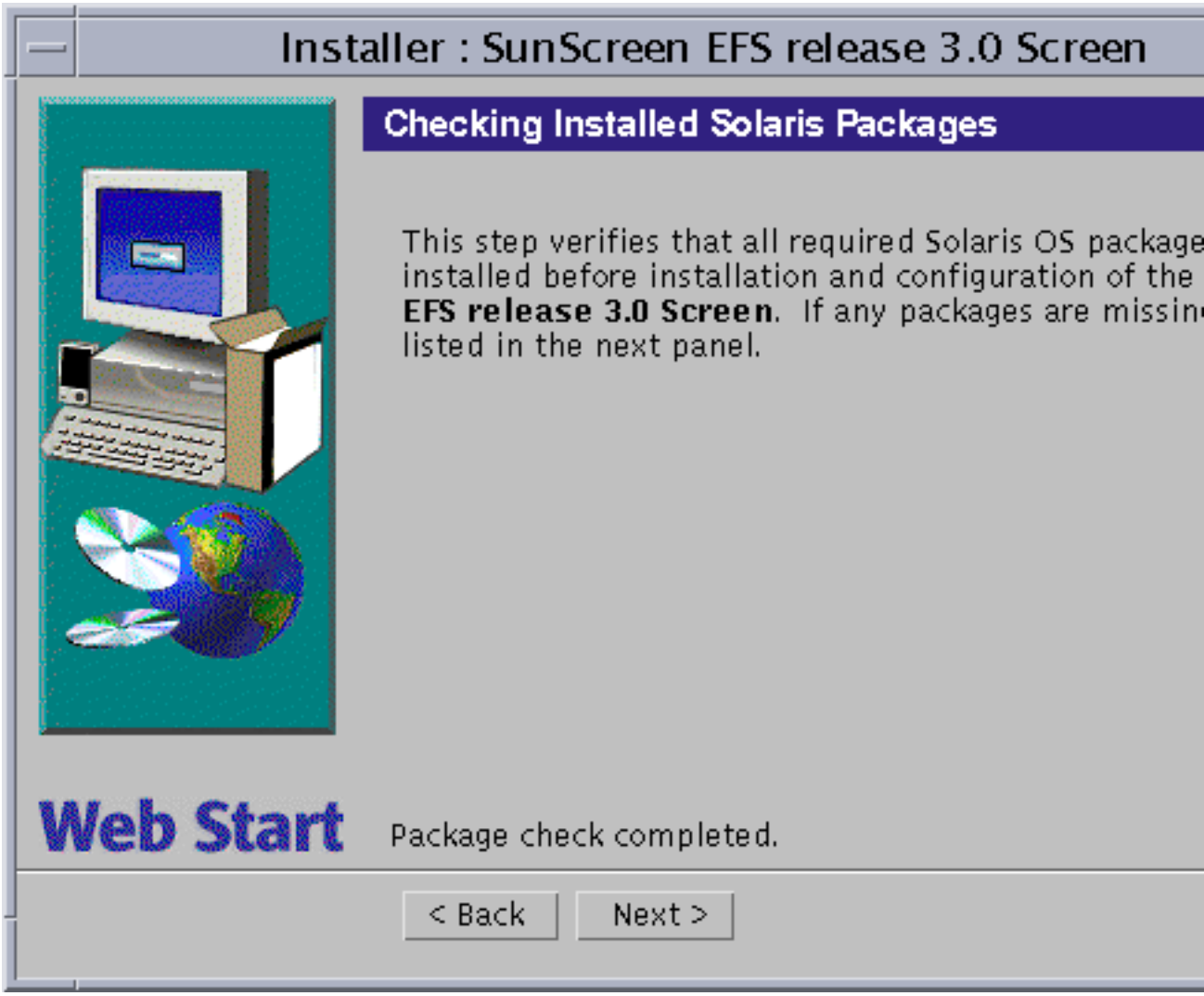



*Figure 4–7* Checking Installed Solaris Packages Window

---

**Note -** If there are missing required packages, a list will be displayed. You must exit the installation wizard at this point and install the required Solaris packages from your Solaris CD.

---

**6. Click Next to continue the installation process.**

The Secondary HA Designation window appears, as shown in Figure 4–8. No is the default.

Choose Yes if you are configuring an HA cluster and are installing the Secondary SunScreen of that cluster. If this is what you want to do, exit the installation wizard and see the *SunScreen EFS 3.0 Administration Guide* for instructions on how to set-up an HA cluster.


*Figure 4–8* Secondary HA Designation Window

7. **Accept the default, No, and Click Next.**

   The Select Screen Type window appears, as shown in Figure 4–9. You are given two types of installations to choose from: Stealth or Routing. Routing mode is the default.


*Figure 4–9* Select Screen Type Window With Routing Mode Selected

8. **Accept the default, Routing mode, and Click Next.**

The Select Administration Type window appears, as shown in Figure 4–10. You are given the choice of Local Administration or Remote Administration. Local Administration is the default.


*Figure 4–10* Select Administration Type(s) Window With Remote Administration Selected

**9. Select Remote Administration and Click Next.**

The Select Type of Install window appears, as shown in Figure 4–11. You are given two choices: Default Install and Custom Install.

---

**Note -** The HotJava browser, version 1.1.5, is packaged on the SunScreen EFS 3.0 CD-ROM and is installed as part of the Default Install. If you do not want this installed, select Custom install and deselect package `SUNWdthj`.

---


*Figure 4–11* Select Type Of Install Window With Default Install Selected

**10. Select the type of install desired, and Click Next.**

The disk space on your machine is checked. An error message appears if you do not have enough disk space.

The Ready to Install window appears, as shown in Figure 4–12. The size of the packages to be installed is confirmed.

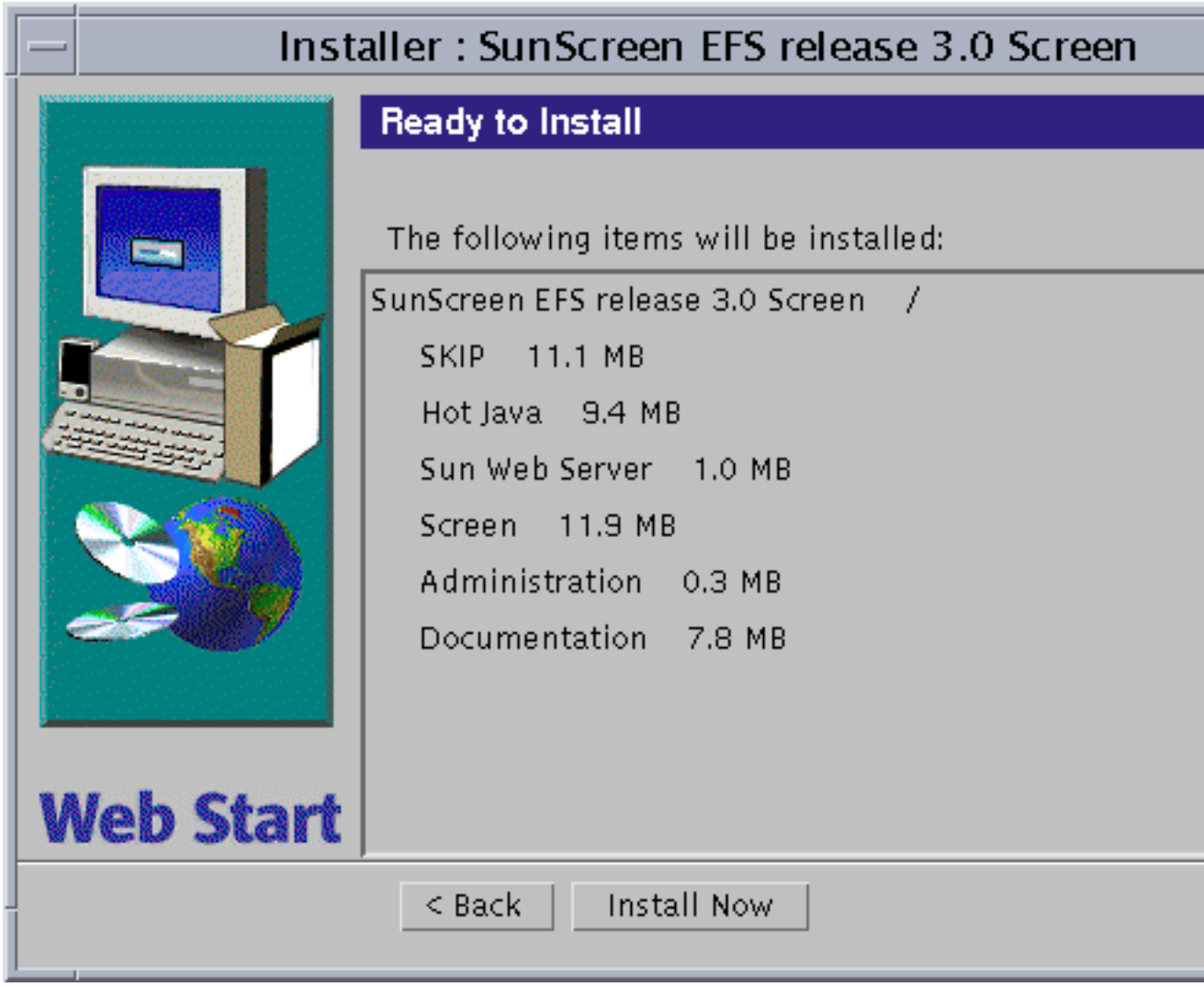



*Figure 4–12* Ready To Install Window

**11. Click Install Now to continue the installation process.**

The Installing Window appears, as is shown in Figure 4–13. The status bar shows the progress of the installation.

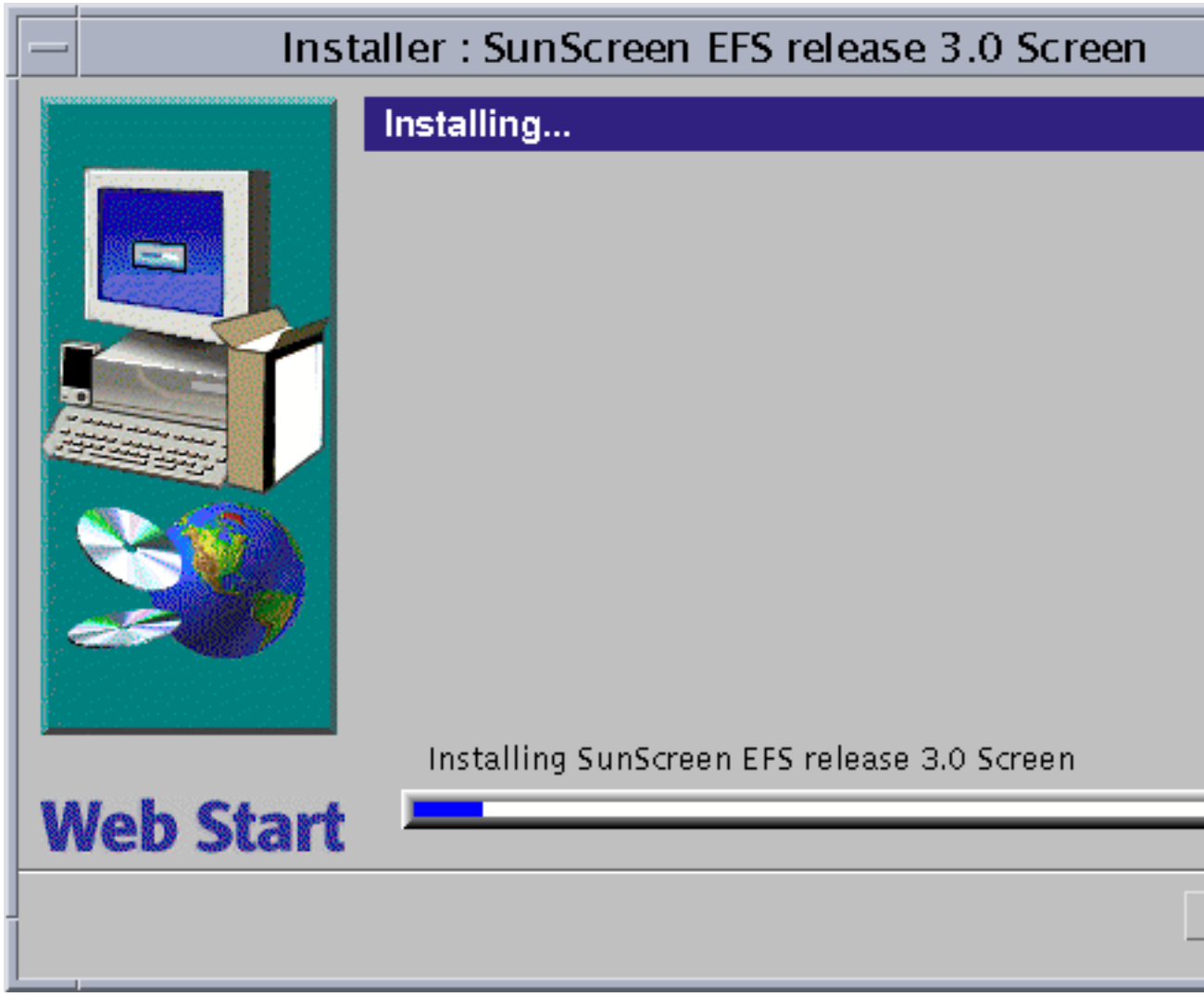



*Figure 4–13* Installing Window Showing Installation Status Bar

Once completed, the Installation Summary window appears, as shown in Figure 4–14. You can resize this window as needed.

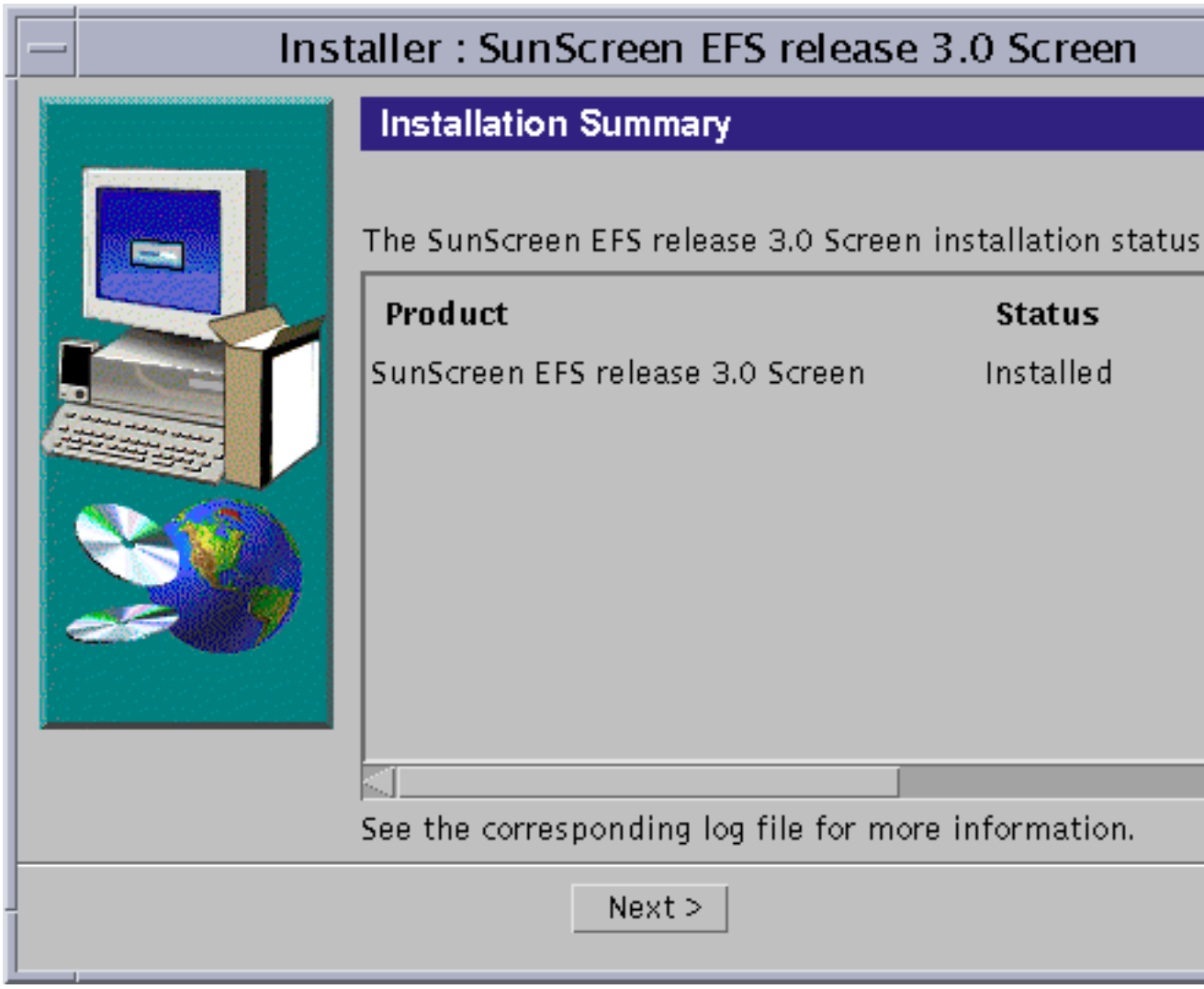



*Figure 4–14* Installation Summary Window

1. **Click Next to continue the installation process.**

   The Select Certificate Type window appears, as shown in Figure 4–15. Self-Generated Certificate is the default.


*Figure 4–15* Select Certificate Type Window With Self-Generated Certificate Selected

---

**Note -** If you are using Issued Certificates, you must now turn to the following procedure, "Option 2: To Install the Software on the Screen When Using Issued Certificates" on page 68. Follow the instructions to install your Issued Certificates. Once completed, return to this procedure and resume with Step 17.

---

2. **Accept the default, Self-Generated Certificate, and Click Next.**

The Self-Generated Certificate ID window appears, as shown in Figure 4–16.


*Figure 4–16* Self Generated Certificate ID Window

**3. Enter the Administration Station's 32-character certificate ID (MKID), obtained in the previous procedure, and Click Next. Do not enter the leading two characters: 0x.**

The Generate Screen Certificate window appears. Wait while the Screen's certificate ID is generated. When completed, the Screen's 32-character certificate ID appears at the bottom of the window, as shown in Figure 4–17.

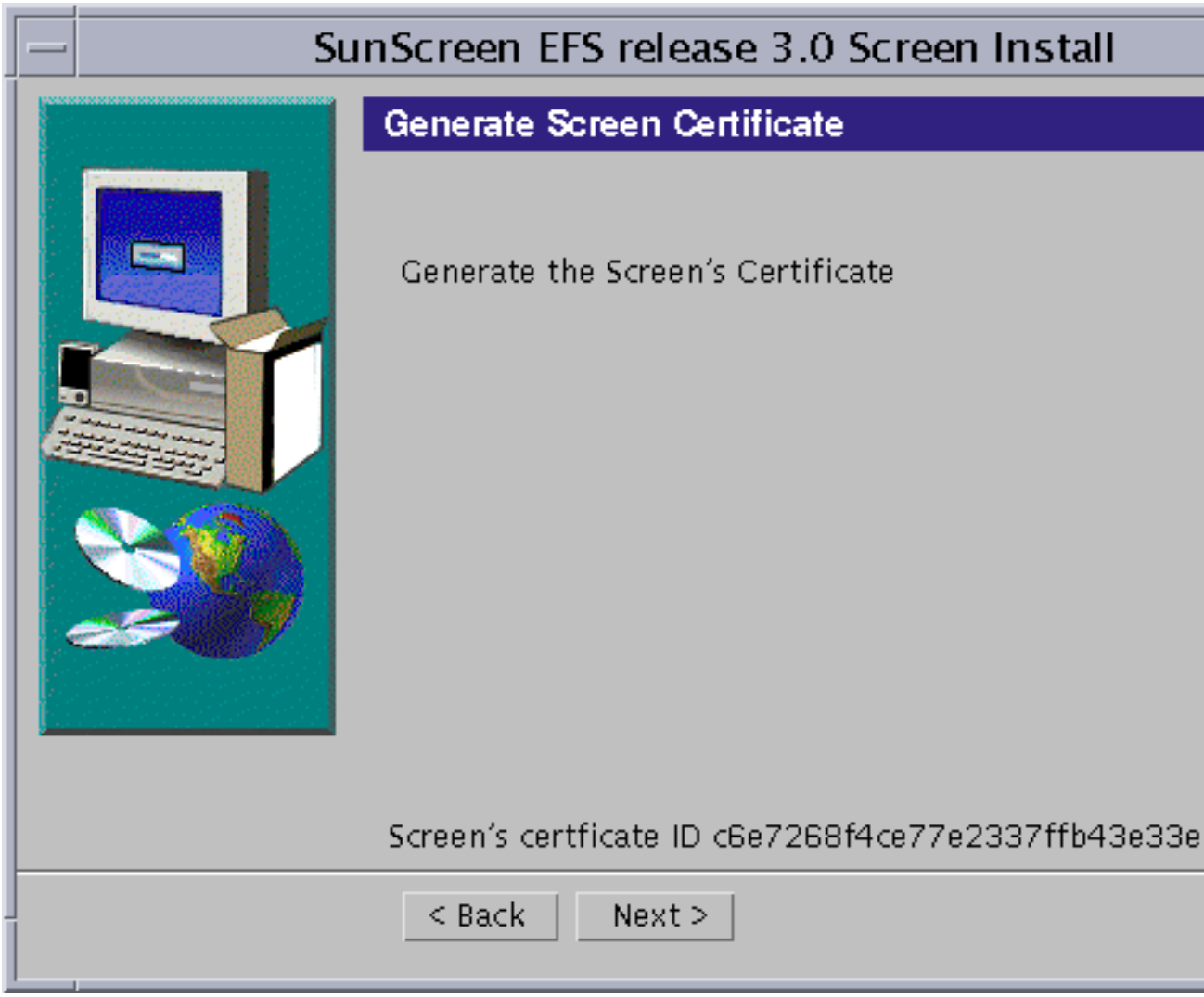



*Figure 4–17* Generate Screen Certificate Window With Screen's Certificate ID

4. **Write down the Screen's 32-character certificate ID (MKID) that appears at the bottom of the window.**

5. **Click Next to continue the installation process.**

   The Select Initial Security Level window appears.

6. **Select the level of security you want: Restrictive, Secure, or Permissive. Permissive is the default.**

   When in doubt, select Permissive as your initial security level, as shown in Figure 4–18. You can change this later if you need to.

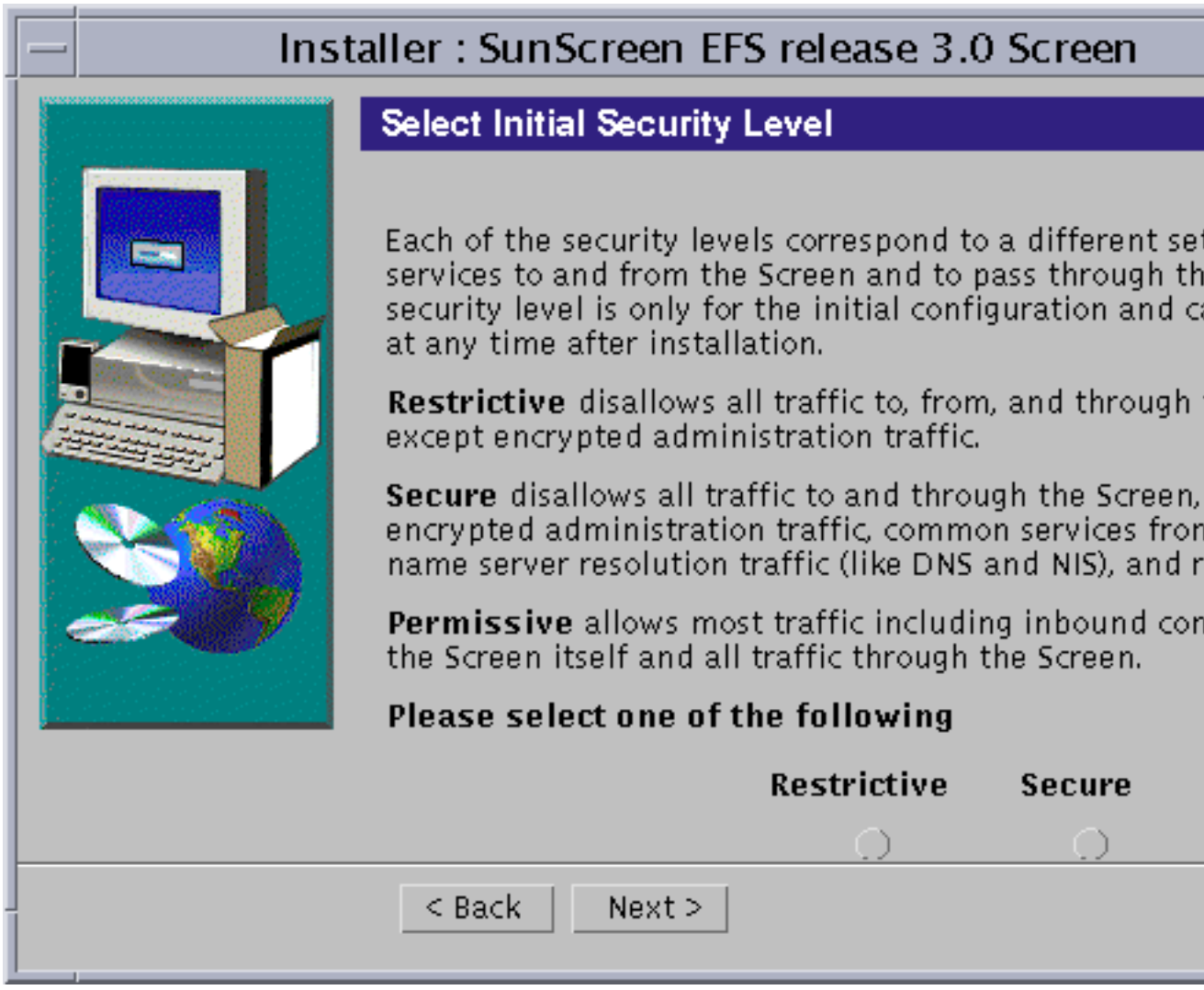



*Figure 4–18* Select Initial Security Level Window With Permissive Selected

7. **Click Next to continue the installation process.**

   The Select Name Service(s) window appears, as shown in Figure 4–19. You must select the name service that will be used on the Screen. Your choices are both NIS and DNS, either NIS or DNS, or None. The default has both NIS and DNS selected. To select just one, deselect the one you do not want. For None, deselect both.

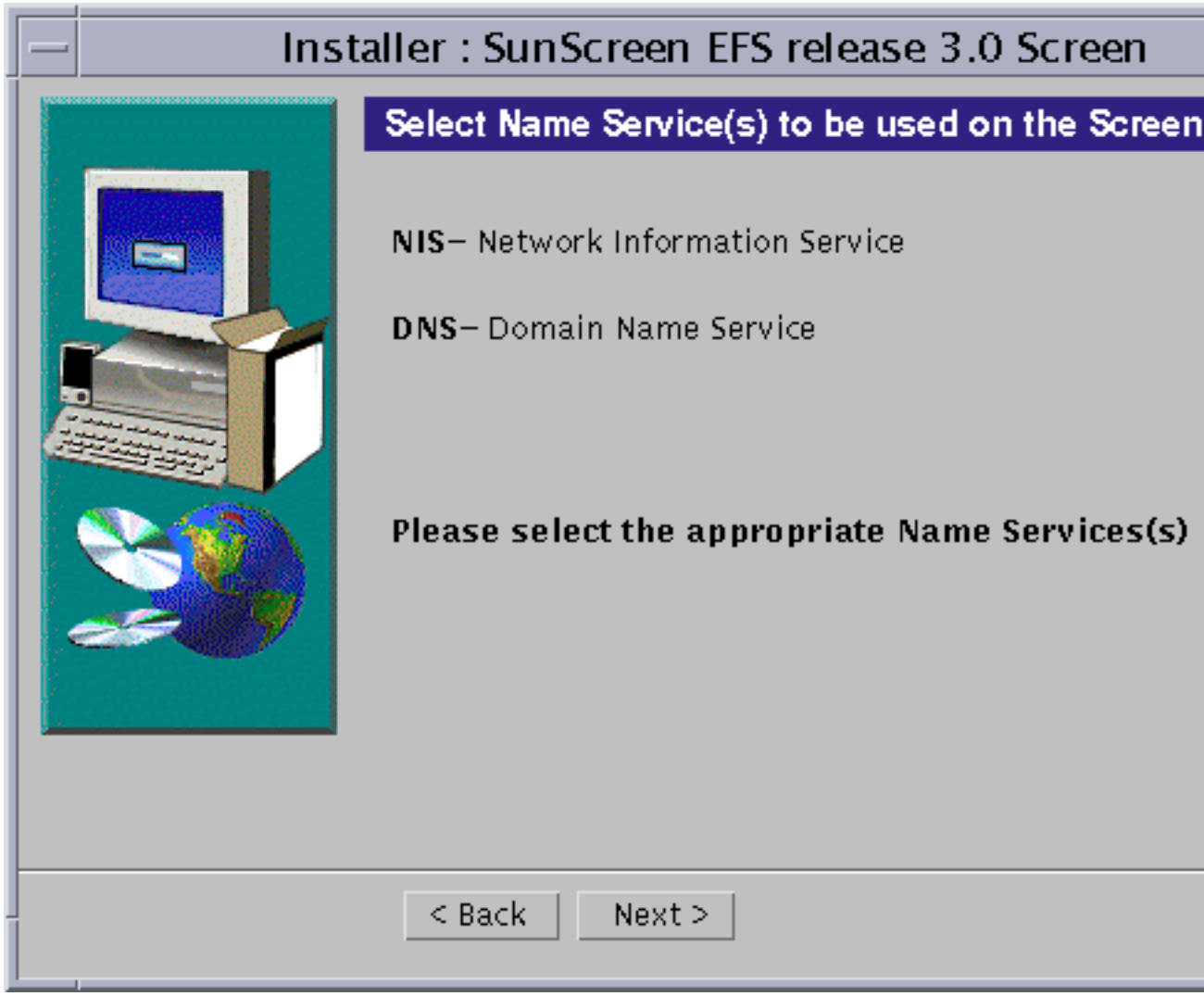



*Figure 4–19* Select Name Service(s) Window With Both NIS And DNS Selected

**8. Select the appropriate Name Service(s), and Click Next.**

The Screen Configuration window appears with the message: `Configuring Screen` as shown in Figure 4–20. Figure 4–21 shows the message that appears once the Screen is successfully configured.

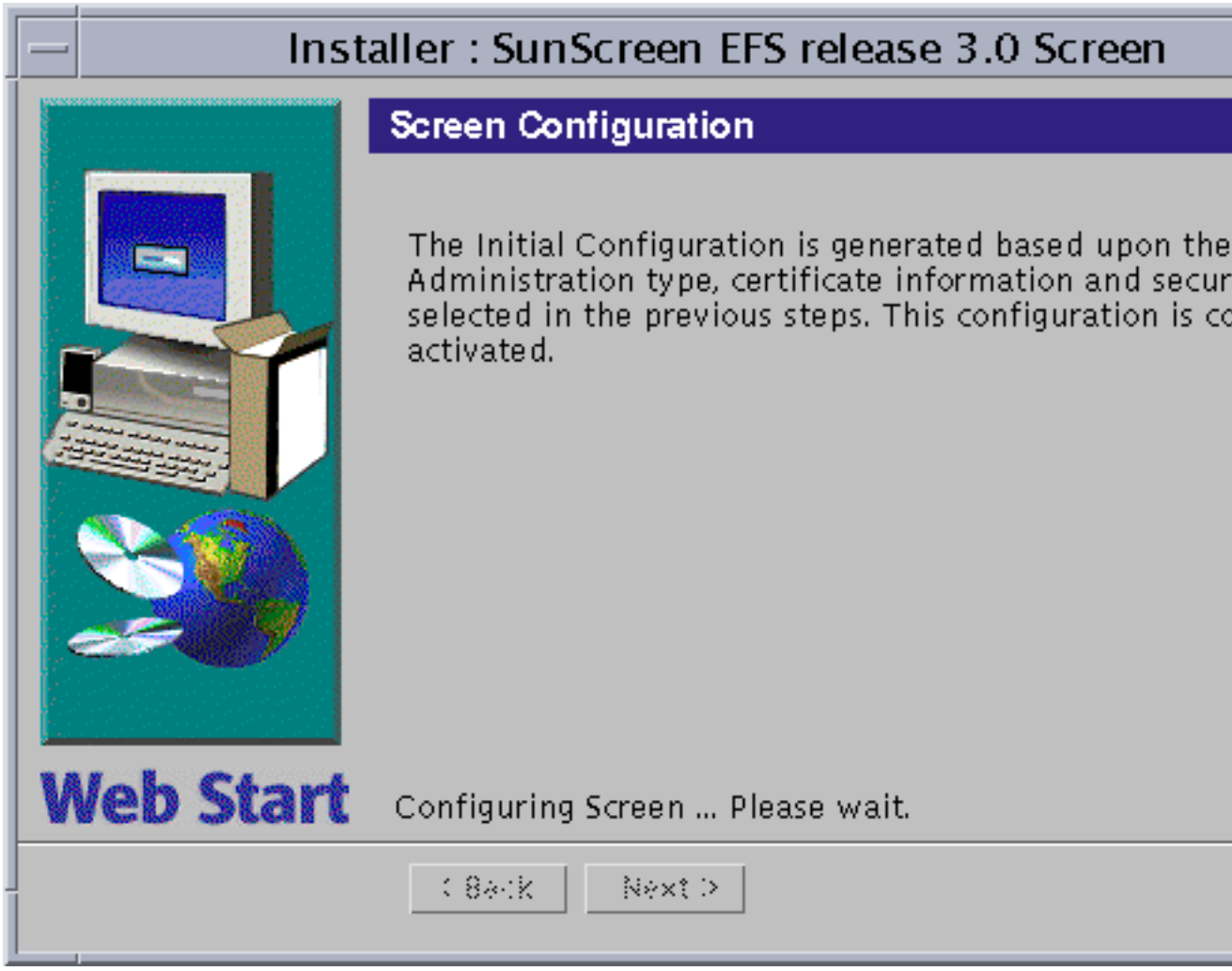



*Figure 4–20* Screen Configuration Window


*Figure 4–21* Screen Configuration Window Once Screen Is Successfully Configured

**9. Click Next to continue the installation process.**

The Screen Reboot window appears, as shown in Figure 4–22.

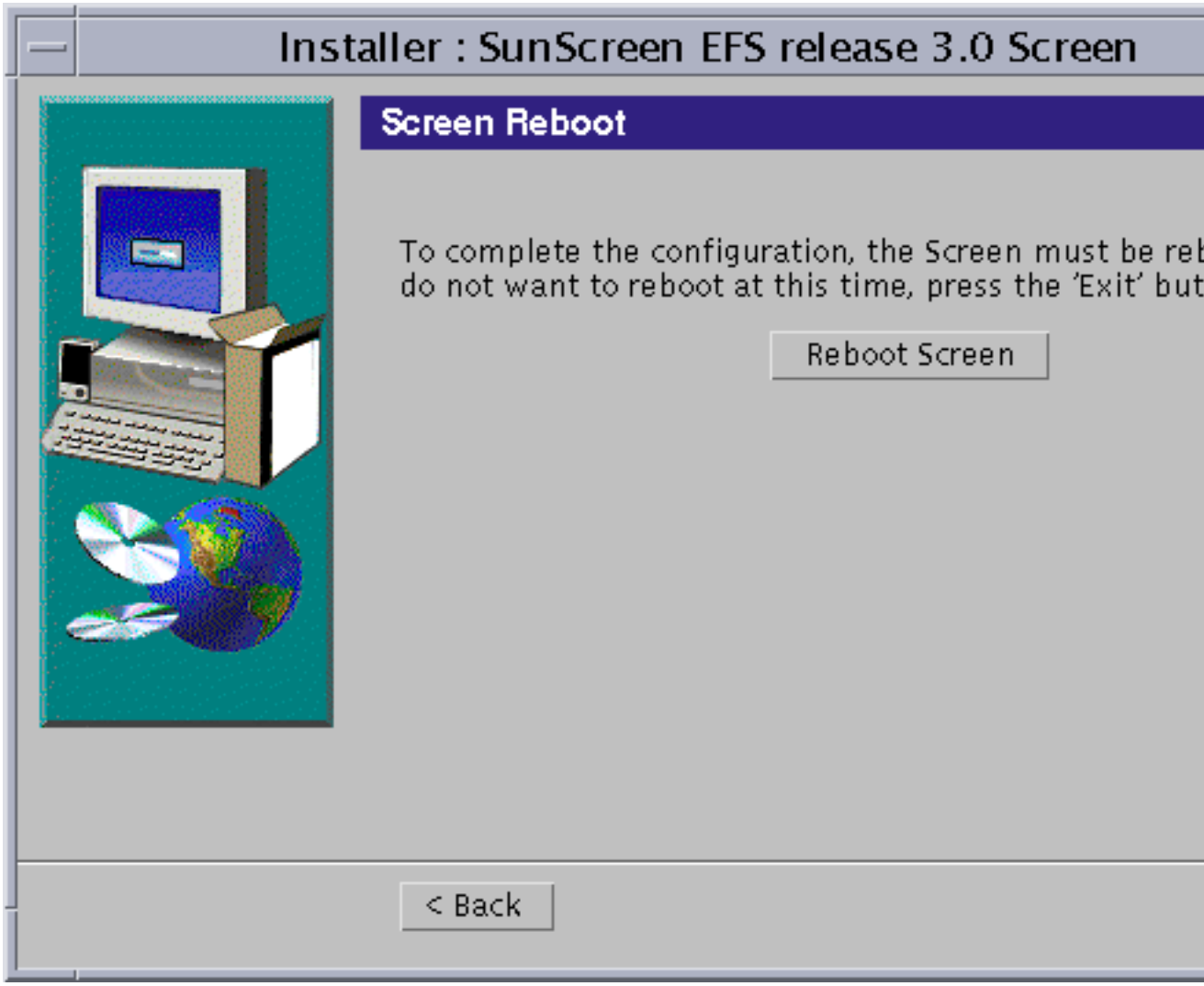



*Figure 4–22* Screen Reboot Window

**10. To reboot the machine, click the Screen Reboot button.**

The installation wizard disappears.

---

**Note -** You must reboot the machine at this time in order to complete the installation process.

---

The software is installed on the Screen. You now proceed to “To Set the PATH, Install SKIP Upgrades, and Display the `AdminSetup.readme` File” on page 73.

## ▼ Option 2: To Install the Software on the Screen When Using Issued Certificates

The procedure to install the software on the Screen when using Issued Certificates is nearly identical to the previous procedure, which used Self-Generated Certificates. The difference is only that your certificates are contained on diskette instead of being self-generated, and they must be installed when the Select Certificate Window appears.

To install the software on the Screen when using Issued Certificates, follow the instructions contained in the procedure, “Option 1: To Install the Software on the Screen When Using Self-Generated Certificates” on page 50. When the Select Certificate Type window appears, select Issued Certificate, and follow the procedure below. Once the certificates are installed, return to the previous procedure and resume with Step 17.

To do this procedure, you will need the Key and Certificate diskette.

1. **From the Select Certificate Type window, select Issued Certificate and Click Next.**

   The Select Certificate Window is shown in Figure 4–23. The Issued Certificate Key Diskettes window next appears, as shown in Figure 4–24.


*Figure 4–23* Select Certificate Type Window With Issued Certificate Selected

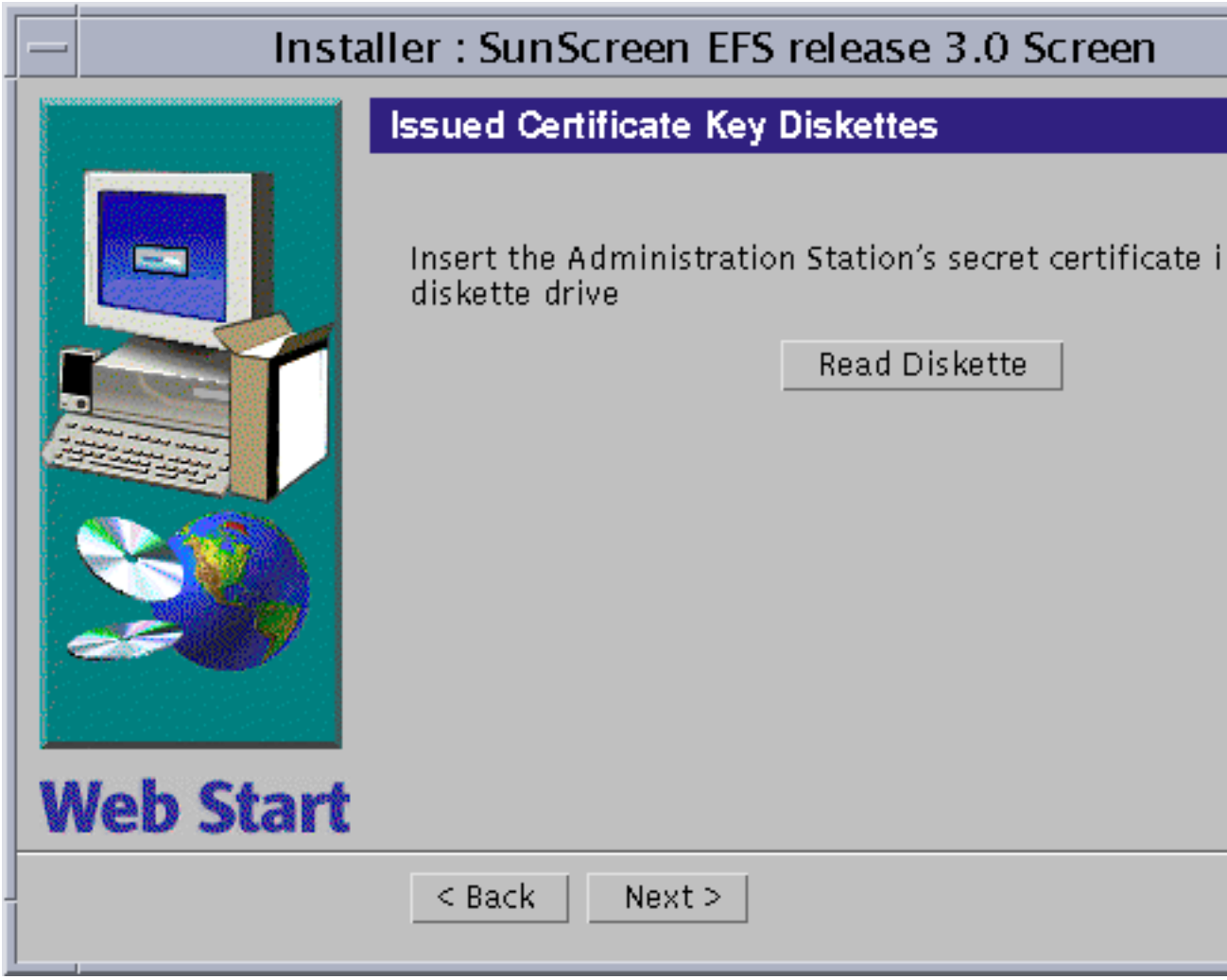



*Figure 4–24* Issued Certificate Key Diskettes Window

2. **Insert the Administration Station's Key and Certificate diskette and Click Read Diskette.**

   Wait until The Issued Certificate ID appears at the bottom of the window, as shown in Figure 4–25.

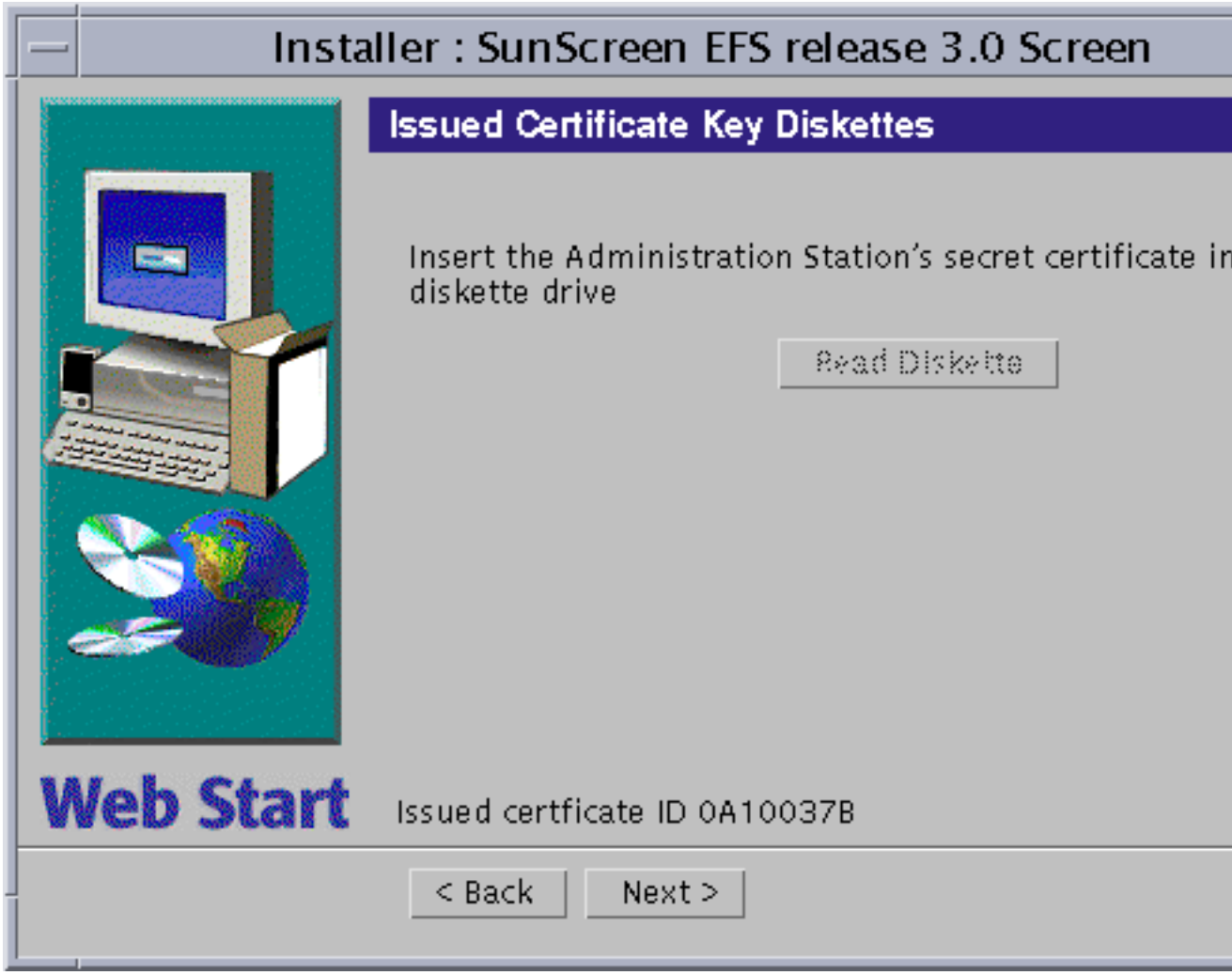



*Figure 4–25* Issued Certificate Key Diskettes Window With Issued Certificate ID At Bottom

3. **Write down the certificate ID, which is eight characters long, and Click Next.**
   The Issued Certificate Key Diskettes window appears, as shown in Figure 4–26.

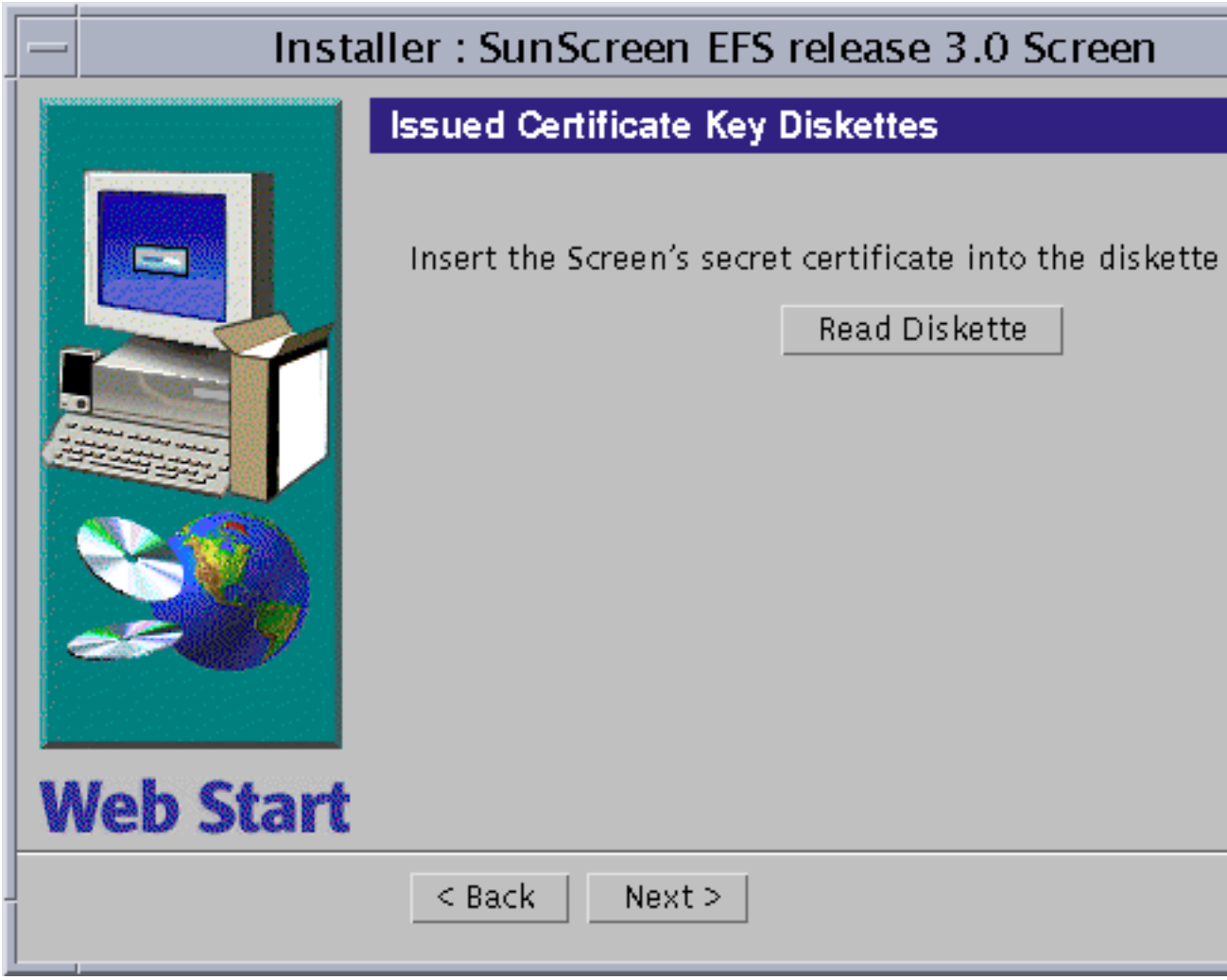



*Figure 4–26* Issued Certificate Key Diskettes Window

4. **Insert the Screen's Certificate ID diskette into the floppy drive and Click Read Diskette button.**

   The Issued Certificate ID appears at the bottom of the window.

5. **Write down the Screen's certificate ID, which is eight characters long, and Click Next.**

   The Select Initial Security Level window appears.

6. **Complete installation on the Screen by following the instructions in the previous procedure, "Option 1: To Install the Software on the Screen When Using Self-Generated Certificates" on page 50. Resume with Step 17.**

## ▼ To Set the PATH, Install SKIP Upgrades, and Display the `AdminSetup.readme` File

1. **On the Screen, open a terminal window and become root, if not already.**

2. **Set the `PATH` and `MANPATH` by editing your shell initialization file (such as `.profile` or `.login` file).**

   a. **Set the `PATH` for the Bourne shell by typing:**

   ```
   PATH=/opt/SUNWicg/SunScreen/bin:$PATH
   PATH=/usr/dt/bin:$PATH
   export PATH
   ```

   b. **Set the `MANPATH` for the Bourne shell by typing:**

   ```
   MANPATH=$MANPATH:/opt/SUNWicg/SunScreen/man
   export MANPATH
   ```

3. **Install any SKIP upgrades (Export Controlled [1024–bit] or U.S. and Canada Use Only [2048–bit] keys) as instructed in the documentation that is included with the SKIP upgrade CD-ROM.**

4. **To display the `AdminSetup.readme` file, in a terminal window type:**

```
# more /etc/opt/SUNWicg/SunScreen/AdminSetup.readme
```

The `AdminSetup.readme` file contains the Screen's certificate ID as well as the command you run in order to give the Administration Station the Screen's certificate ID, as shown in Figure 4–27. Write the command down for later use, which begins with `skiphost -a`.

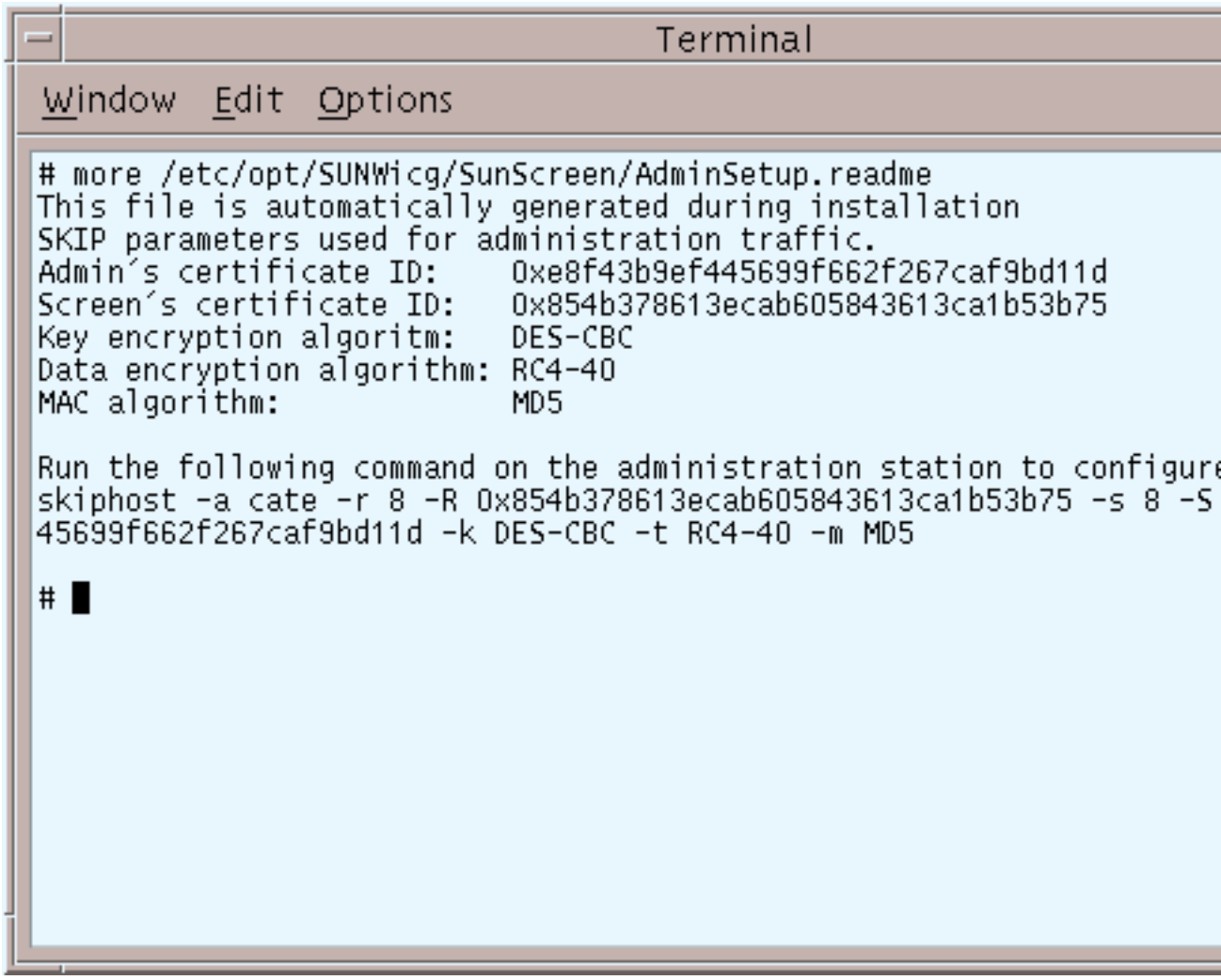



*Figure 4–27* `AdminSetup.readme` file

---

**Tip -** If you trust that the network between the Screen and the Administration Station is secure, you can ftp the `AdminSetup.readme` file from the Screen to the Administration Station. This saves you the task of writing down the information which is required in the next procedure.

---

**5. Eject the CD-ROM by typing:**

```
# eject cdrom0
```

6. **If SKIP upgrades were installed, reboot the Screen by typing:**

```
# sync; init 6
```

You now return to the Administration Station to complete SKIP configuration. Proceed to “Using SKIP for Encrypted Communication” on page 75.

## Using SKIP for Encrypted Communication

To complete the installation of a remotely administered SunScreen in routing mode, encrypted communication between the Administration Station and the Screen must be achieved. This is done by enabling SunScreen SKIP, which was previously installed. In this procedure, you tell the Administration Station what encryption algorithms to use to communicate with the Screen. For more information regarding SunScreen SKIP for Solaris, see the *SunScreen SKIP 1.5 User’s Guide.*

To configure the Administration Station to communicate with the Screen, you must know:

- What access control list (ACL) parameters to set to match the Screen’s encryption settings.
- The Screen’s certificate ID.

The command obtained from the `AdminSetup.readme` file in the previous procedure is now used.

Instructions for using SKIP from the command line are found in Appendix A.

### ▼ To Use the `skiptool` GUI

1. **Open a terminal window and become root, if not already.**

2. **Launch the skiptool GUI by typing:**

```
# skiptool
```

**Note -** You may need to use `skiptool -i` *name_of_interface* (such as qe3) if you wish to set SKIP parameters on a network interface other than the default interface.

The main window of the `skiptool` GUI appears, as shown in Figure 4–28.

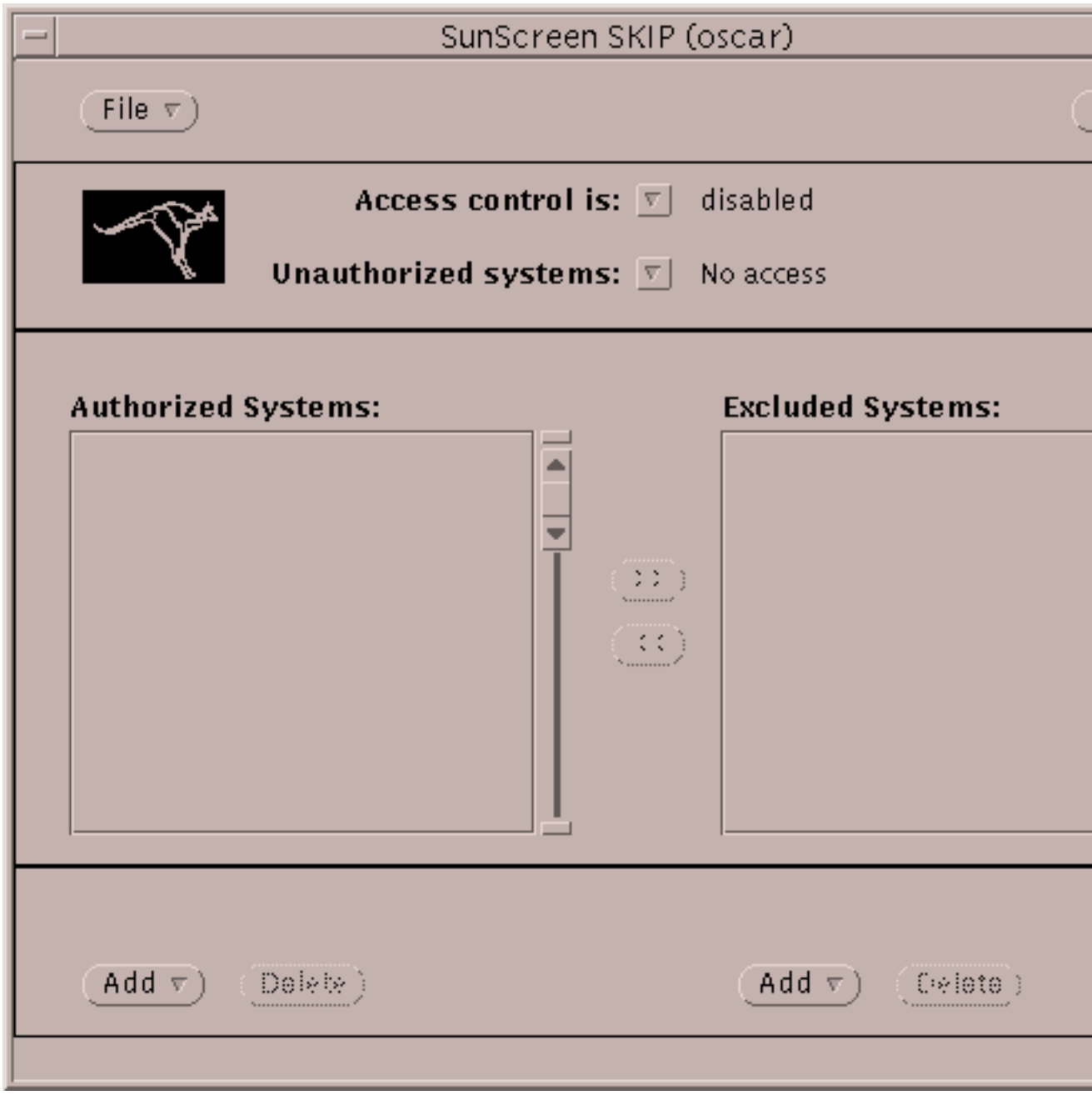



*Figure 4–28* `skiptool` Main Window

You next add a default ACL to talk to unencrypted to all hosts.

1. **Click the Add button, and under Host, choose the Off security option.**
   The Add Host properties window opens.

2. **Type ‘default’ as the Hostname and Click Apply.**
   This is shown in Figure 4–29.

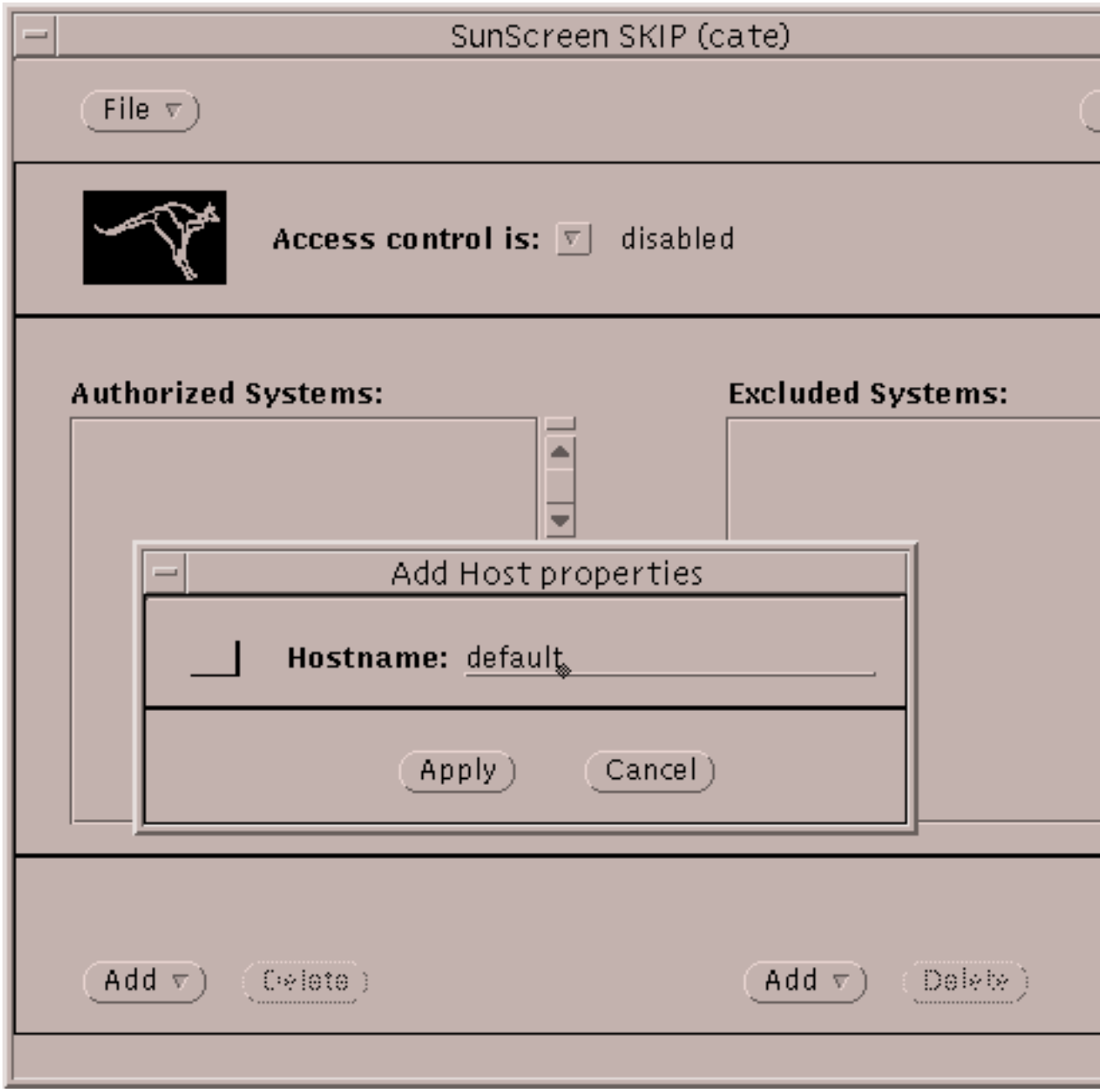



*Figure 4–29* Skiptool With Add Host Properties Window Completed

You next add an ACL so the Administration Station and Screen can use encrypted communication.

3. **Click the Add button, and under Host, choose the SKIP security option.**

   The Add Skip host properties window appears, as shown in Figure 4–30.

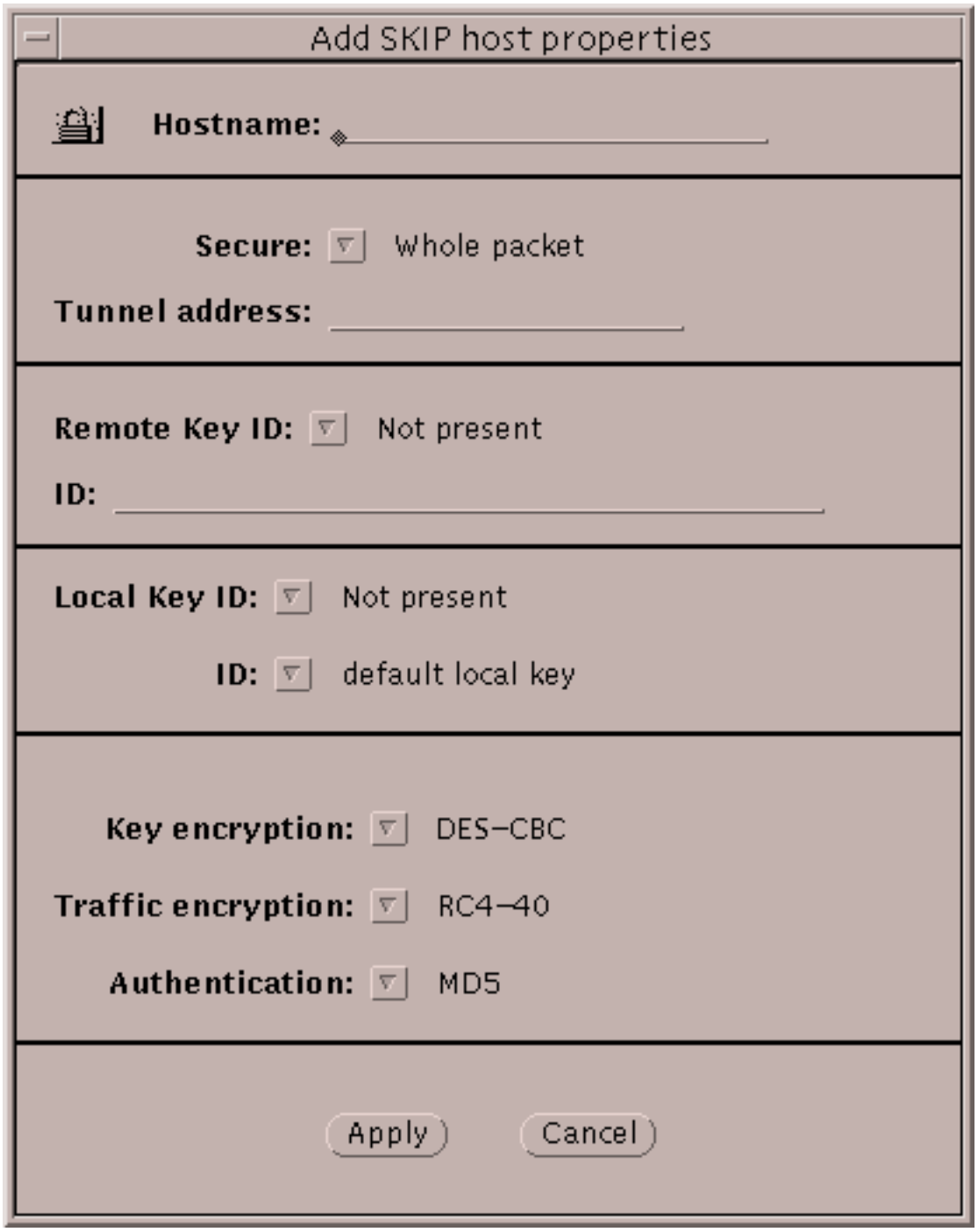



*Figure 4–30* Add SKIP Host Properties Window

Use the information contained in the `AdminSetup.readme` file, obtained in the preceding procedure, and complete the fields.

1. **Type *Name_of_Screen* in the Hostname field.**

2. **In the Secure field, select Whole Packet from the drop-down list.**

3. **In the Remote Key ID, make the appropriate selection from the drop-down list.**
   Refer to the `AdminSetup.readme` file to select the correct Remote Key ID. For self-generated certificates on the Administration Station, select MD5 (DH Public Value). For issued certificates, select IPv4. See Figure 4–31 for a sample of the Add SKIP Host Properties window completed.

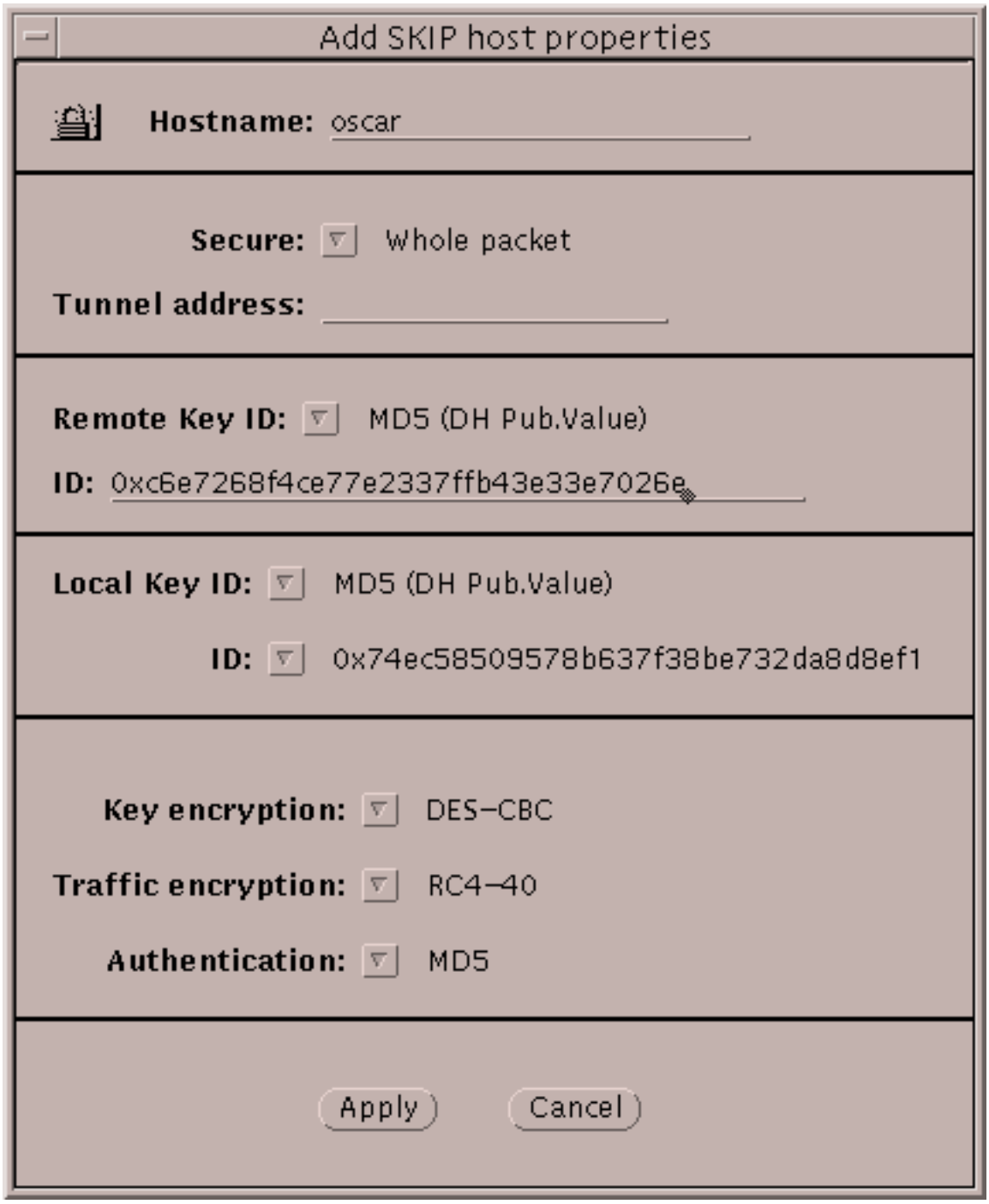



*Figure 4–31* Add SKIP Host Properties Completed

4. **In the Local Key ID, make the appropriate selection from the drop-down list.**

   Refer to the `AdminSetup.readme` file to select the correct Local Key ID. For self-generated certificates on the Administration Station, select MD5 (DH Public Value). For issued certificates, select IPv4. The ID value is filled in automatically.

5. **Turn SKIP on. From the pulldown menu for "Access control is:", located at the top of the `skiptool` window, select 'enabled'.**

---

**Note -** When you select enabled from the pulldown menu, a window appears when you save the configuration. Click Cancel to prevent these required systems, which are part of the default configuration, from showing up in the Authorized Systems window.

---

6. **Select Save from the File pulldown menu.**

---

**Note -** After configuring SKIP, check that the encryption parameters and the certificate ID (MKID) values match on both the Administration Station and the Screen.

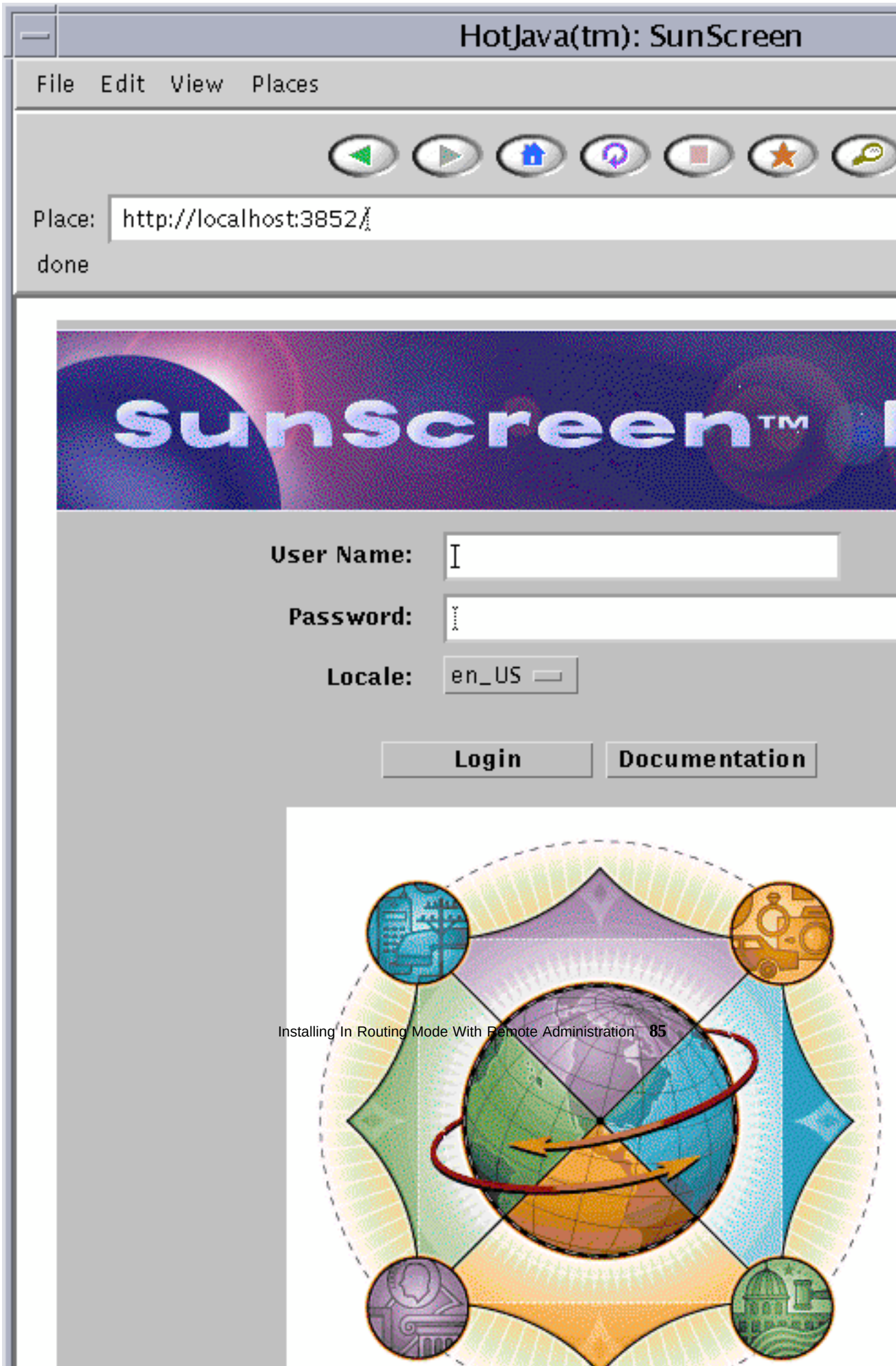
---

## ▼ To Launch the Administration GUI

1. **To configure and manage your SunScreen from your Administration Station, run a Java-enabled Web browser compliant with JDK 1.1.3 or later, and launch the Administration GUI by typing the following URL:**

```
http://Name_of_Screen:3852/
```

The Administration GUI appears, as shown in Figure 4–32.


HotJava(tm): SunScreen
File Edit View Places
Place: http://localhost:3852/
done
SunScreen™
User Name:
Password:
Locale: en_US
Login
Documentation

2. **To login, type the following and Click Login**:

```
User Name: admin
Password: admin
```

You next configure and manage your SunScreen with the Administration GUI. See the *SunScreen EFS 3.0 Administration Guide* for further instructions.

CHAPTER 5

# Installing in Stealth Mode

This chapter explains how to install a remotely administered SunScreen EFS 3.0 in stealth mode. You can use local administration on a SunScreen running in stealth mode, but that configuration is not recommended and is not covered in this chapter. The software is first installed on the machine that will be the Administration Station, and then on the machine that will be the Screen. Encrypted communication between the Administration Station and the Screen is achieved by use of SunScreen SKIP (Simple Key-Management for Internet Protocols).

If you are installing on a system without a monitor, the procedures for installation using the command line are described in Appendix A.

Topics covered include:

- Installing SunScreen EFS 3.0 in stealth mode
- Installing the software on the Administration Station
- Installing certificates on the Administration Station
- Installing the software on the Screen
- Using SKIP for encrypted communication

**Note -** If you have used the SunScreen SPF-200 product, the installation method is changed considerably. Please read this entire chapter before proceeding with installation in stealth mode.

Before installing, review the *SunScreen EFS 3.0 Release Notes* for the latest information about this product.

# Installing SunScreen EFS 3.0 in Stealth Mode

Operating SunScreen EFS 3.0 in stealth mode acts much like a bridge in that no IP interfaces are exposed to the public or private network, and packets are transparently passed through the Screen. When operating in stealth mode, the firewall cannot be directly attacked through any means other than a denial of service attack, and cannot be seen or detected through traceroute or similar network tools.

Prior to beginning the procedure that follows, configure only the network interface that will be used for remote administration. See the documentation accompanying the Solaris operating environment, if needed.

**Caution -** In this procedure, you will be asked if you want to harden the Screen. Hardening is optional and if chosen, is an automated removal of Solaris files and packages which might otherwise make the Screen vulnerable to an attack. Once you have hardened your Screen, it becomes a dedicated firewall and the machine can not be used for another purpose without first reinstalling the Solaris operating environment.

The following procedures explain how to install SunScreen EFS 3.0 in stealth mode using either self-generated or issued certificate technology.

This type of installation requires several steps to complete. You proceed in the following order:

1. Install the SunScreen Administration software on the Administration Station.

This step installs the required SKIP packages on the Administration Station. This is the first prerequisite to creating a secure method of communication between the Administration Station and the Screen. The use of SKIP technology enables encrypted communication between the two.

1. Install the Administration certificate on the Administration Station.
2. Install the SunScreen software on the Screen.

This procedure requires the Administration Station's certificate ID and installs the Screen's certificate.

1. Install the Screen's certificate ID on the Administration Station.
2. Start encrypted communication between the Administration Station and the Screen by enabling SKIP on the Administration Station.

**Note -** The installation procedure requires that the machine be rebooted when indicated. Do not perform any other tasks on the machine while installing the software, as a delay in rebooting the machine may affect installation and cause your system to hang.

Do not begin this procedure until you have read the information in Chapter 2.

## ▼ To Install The Software on the Administration Station

1. **Open a terminal window and become root.**

**Caution -** Ensure that the OpenWindows™ File Manager is not running because it interferes with the operation of the `volcheck` command used for installation.

2. **Insert the SunScreen EFS 3.0 CD-ROM into the CD-ROM drive.**

3. **Mount the CD-ROM by typing:**

```
# volcheck
```

4. **Add the software by typing**

```
# /cdrom/cdrom0/adminInstaller
```

:

**Note -** Due to late software changes, the appearance of the installation wizards may differ slightly from that shown. Functionality and performance is not affected. The panels of the installation wizards can be resized, if needed.

The SunScreen EFS Admin Install's Welcome window appears, as shown in Figure 5–1.


*Figure 5–1* SunScreen EFS Admin Install's Welcome Window

**5. Click Next to continue the installation process.**

The Select Type of Install window appears. You are given two choices: Default Install and Custom Install. Default Install is the default.

**Note -** The HotJava browser, version 1.1.5, is packaged on the SunScreen EFS 3.0 CD-ROM and is installed as part of the Default Install. If you do not want this installed, select Custom Install and deselect package `SUNWdthj`.

6. **Select the type of install desired, and Click Next.**

   The disk space on your machine is checked. An error message appears if you do not have enough disk space.

   The Ready to Install window appears, as shown in Figure 5–2. The size of the packages to be installed is confirmed.

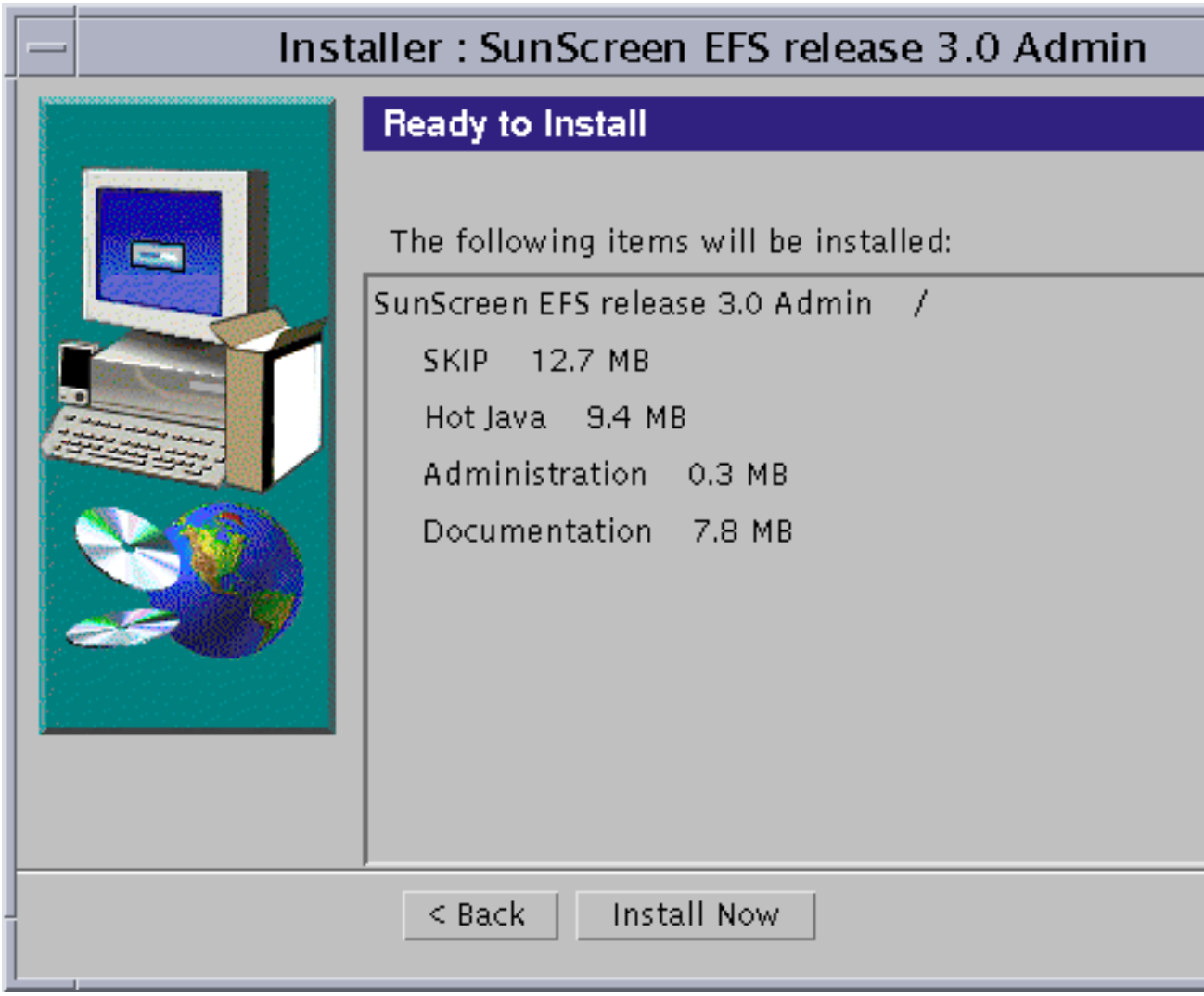



*Figure 5–2* The Ready to Install Window

**7. Click Install Now to continue the installation process.**

The Installing window appears, as shown in Figure 5–3. The status bar shows the progress of the installation.

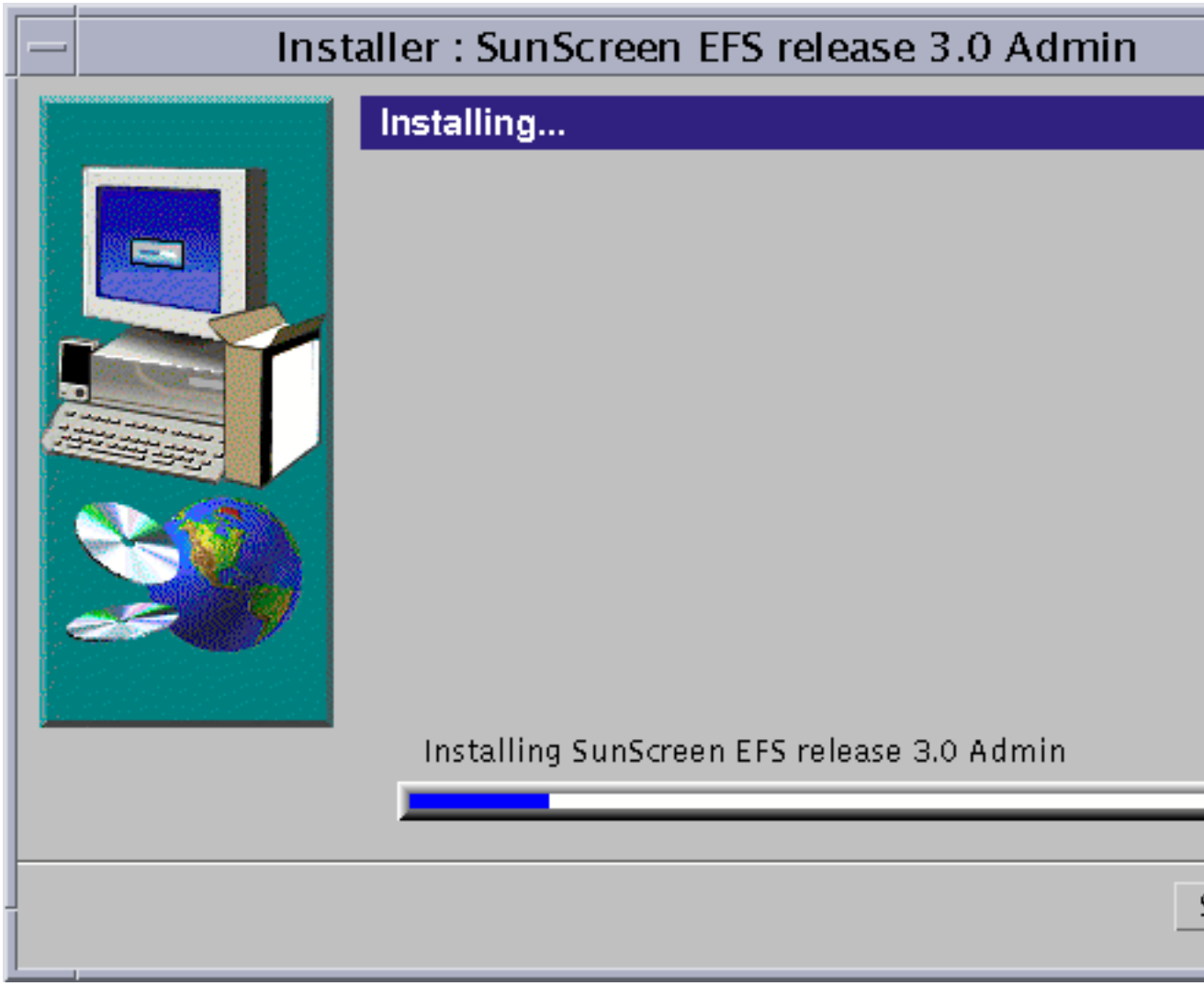



*Figure 5–3* The Installing Window Showing The Status Bar

**8. Click Next to complete the installation process.**

An Installation Summary window appears, as shown in Figure 5–4.

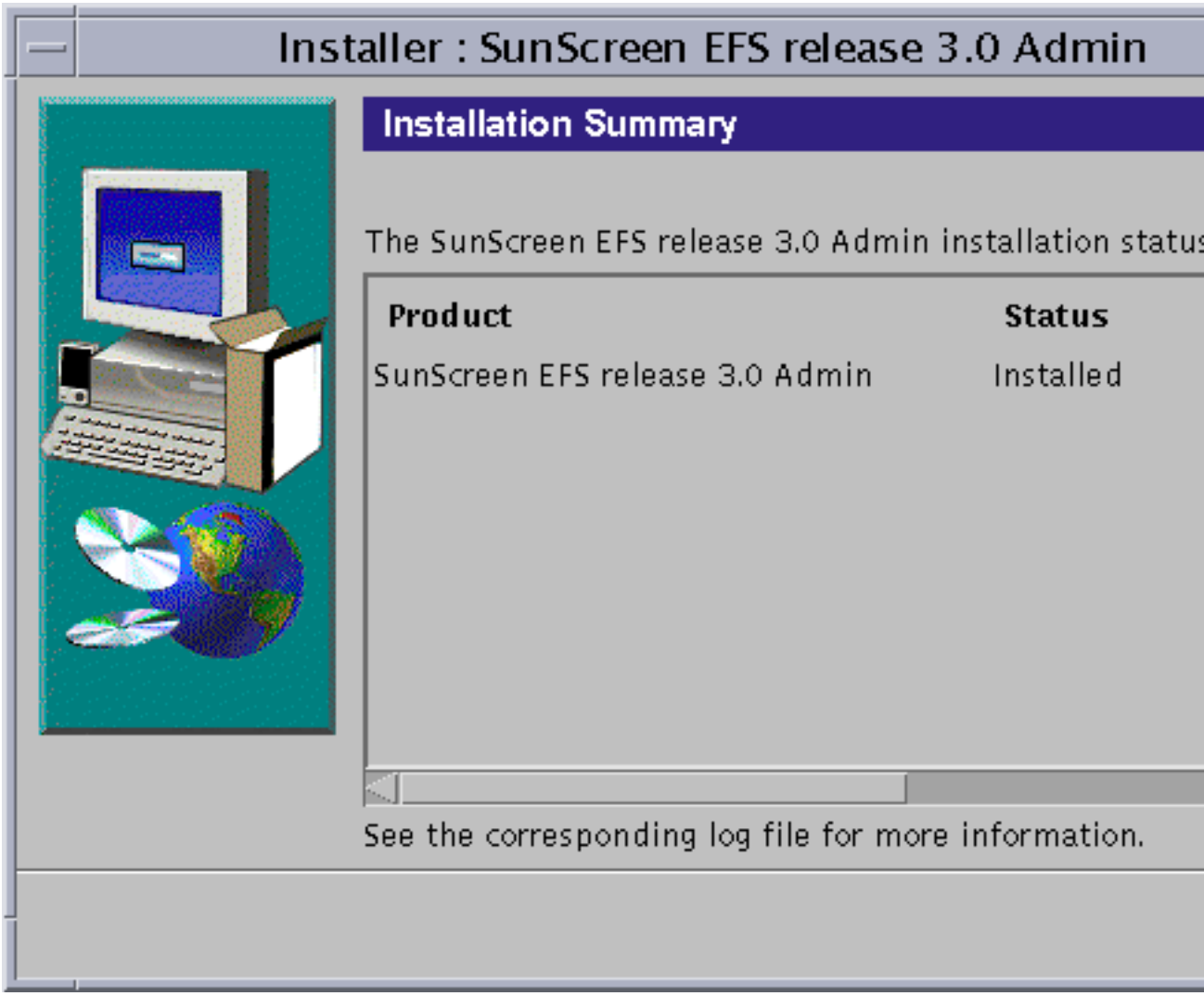



*Figure 5–4* Installation Summary Window

**9. Select Exit to complete the installation process using the installation wizard.**

The installation wizard disappears.

**10. Set the** `PATH` **and** `MANPATH` **by editing your shell initialization file (such as** `.profile` **or** `.login` **file).**

**a. Set the** `PATH` **for the Bourne shell by typing:**

```
PATH=/opt/SUNWicg/SunScreen/bin:$PATH
```

```
PATH=/usr/dt/bin:$PATH
 export PATH
```

**b. Set the** `MANPATH` **for the Bourne shell by typing:**

```
 MANPATH=$MANPATH:/opt/SUNWicg/SunScreen/man
export MANPATH
```

**11. Eject the CD-ROM from the CD-ROM drive by typing**

```
# eject cdrom0
```

:

**12. Install any SKIP upgrades (Export Controlled [1024–bit] or U.S. and Canada Use Only [2048–bit] keys) as instructed in the documentation that is included with the SKIP upgrade CD-ROM.**

**13. Reboot to complete installation by typing**:

```
# sync; init 6
```

The software packages have been installed. You continue the installation process on the machine that is the Administration Station.

You now return to the Administration Station and proceed with “To Set the PATH, Install SKIP Upgrades, and Display the `AdminSetup.readme` File” on page 100.

## ▼ Option 2: To Install the Software on the Screen When Using Issued Certificates

The procedure to install the software on the Screen when using Issued Certificates is nearly identical to the previous procedure, which used Self-Generated Certificates. The difference is only that your certificates are contained on diskette instead of being self-generated, and they must be installed when the Select Certificate Window appears.

To install the software on the Screen when using Issued Certificates, follow the instructions contained in the procedure, “To Install The Software on the Administration Station” on page 89. When the Select Certificate Type window

appears, select Issued Certificate and follow the procedure below. Once the certificates are installed, return to the previous procedure and resume with Step 17.

To do this procedure, you need the Key and Certificate diskette.

1. **From the Select Certificate Type window, select Issued Certificates and Click Next.**

   The Select Certificate Window is show in Figure 5–5. The Issued Certificate Key Diskettes window next appears, as show in Figure 5–6.


*Figure 5–5* Select Certificate Type Window With Issued Certificate Selected

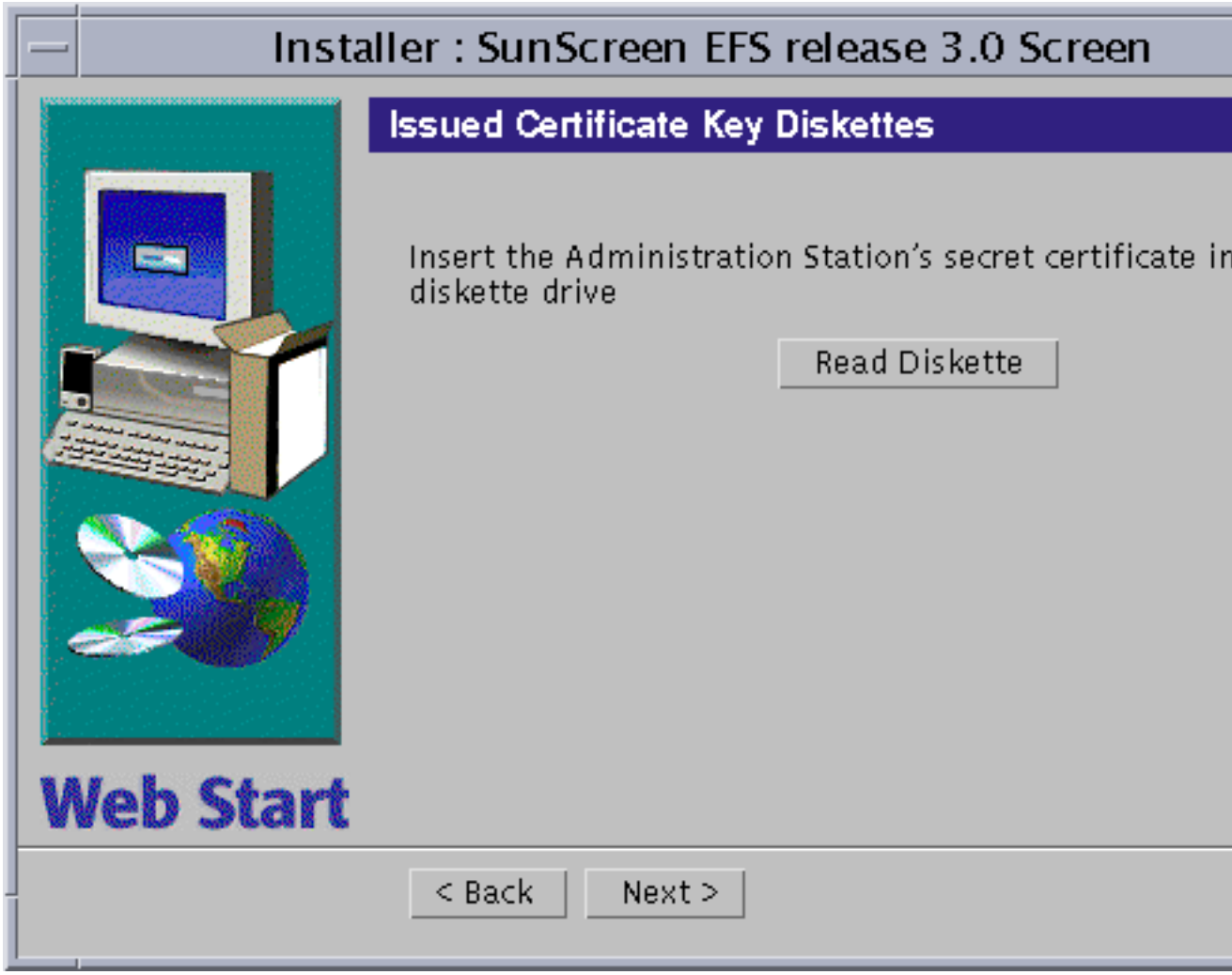



*Figure 5–6* Issued Certificate Key Diskettes Window

**2. Insert the Key and Certificate diskette and Click Read Diskette.**

Wait until the Issued Certificate ID appears at the bottom of the window, as show in Figure 5–7.

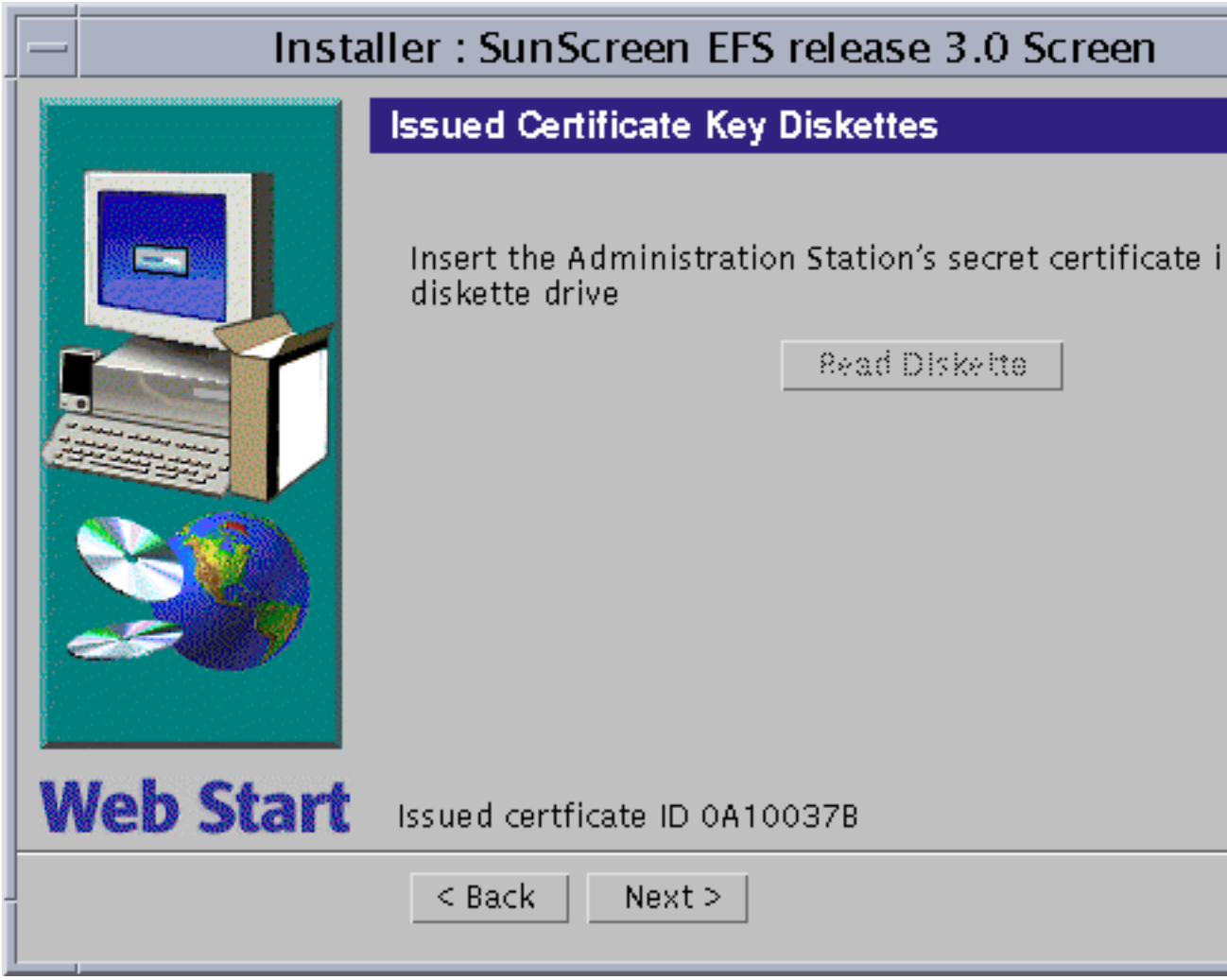



*Figure 5–7* Issued Certificate Key Diskettes Window With Issued Certificate ID At Bottom

3. **Write down the certificate ID, which is eight characters long, and Click Next.**
   The Issued Certificate Key Diskettes window appears, as shown in Figure 5–8.

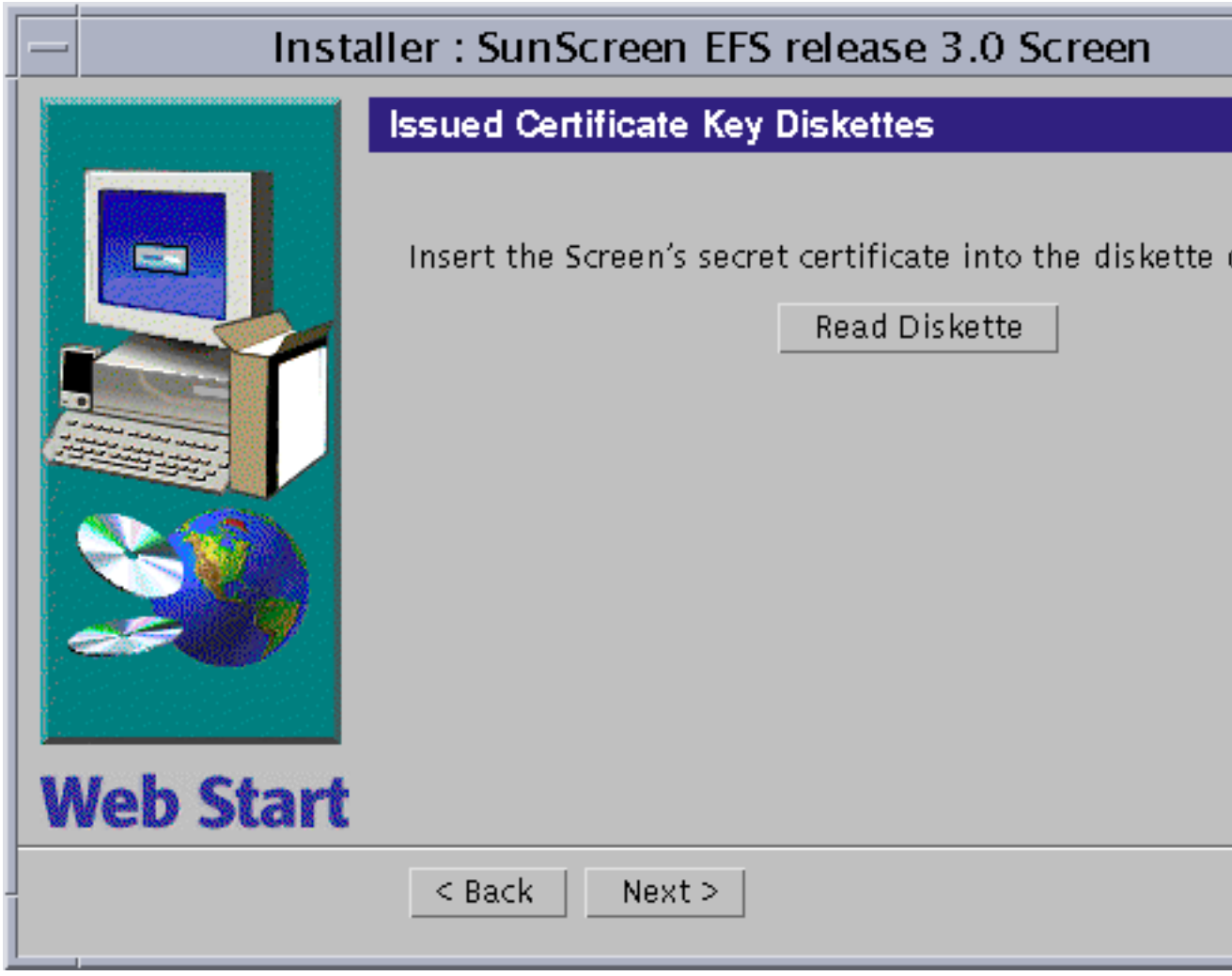



*Figure 5–8* Issued Certificate Key Diskettes Window

4. **Insert the Screen's Certificate ID diskette into the floppy drive and Click Read Diskette button.**

   The Issued Certificate ID appears at the bottom of the window.

5. **Write down the Screen's certificate ID, which is eight characters long, and Click Next.**

   The Select Initial Security Level Window appears.

6. **Complete installation on the Screen by the following the instructions in the previous procedure, "To Install The Software on the Administration Station" on page 89. Resume with Step 17.**

## ▼ To Set the PATH, Install SKIP Upgrades, and Display the `AdminSetup.readme` File

1. **On the Screen, open a terminal window and become root, if not already.**

2. **Set the `PATH` and `MANPATH` by editing your shell initialization file (such as `.profile` or `.login` file).**

   a. **Set the `PATH` for the Bourne shell by typing:**

   ```
   PATH=/opt/SUNWicg/SunScreen/bin:$PATH
   PATH=/usr/dt/bin:$PATH
   export PATH
   ```

   b. **Set the `MANPATH` for the Bourne shell by typing:**

   ```
   MANPATH=$MANPATH:/opt/SUNWicg/SunScreen/man
   export MANPATH
   ```

3. **Install any SKIP upgrades (Export Controlled [1024–bit] or U.S. and Canada Use Only [2048–bit] keys) as instructed in the documentation that is included with the SKIP upgrade CD-ROM.**

4. **To display the `AdminSetup.readme` file, in a terminal window type:**

```
# more /etc/opt/SUNWicg/SunScreen/AdminSetup.readme
```

The `AdminSetup.readme` file contains the Screen's certificate ID as well as the command you run in order to give the Administration Station the Screen's certificate ID, as shown in Figure 5–9. Write the command down for later use, which begins with `skiphost -a`.

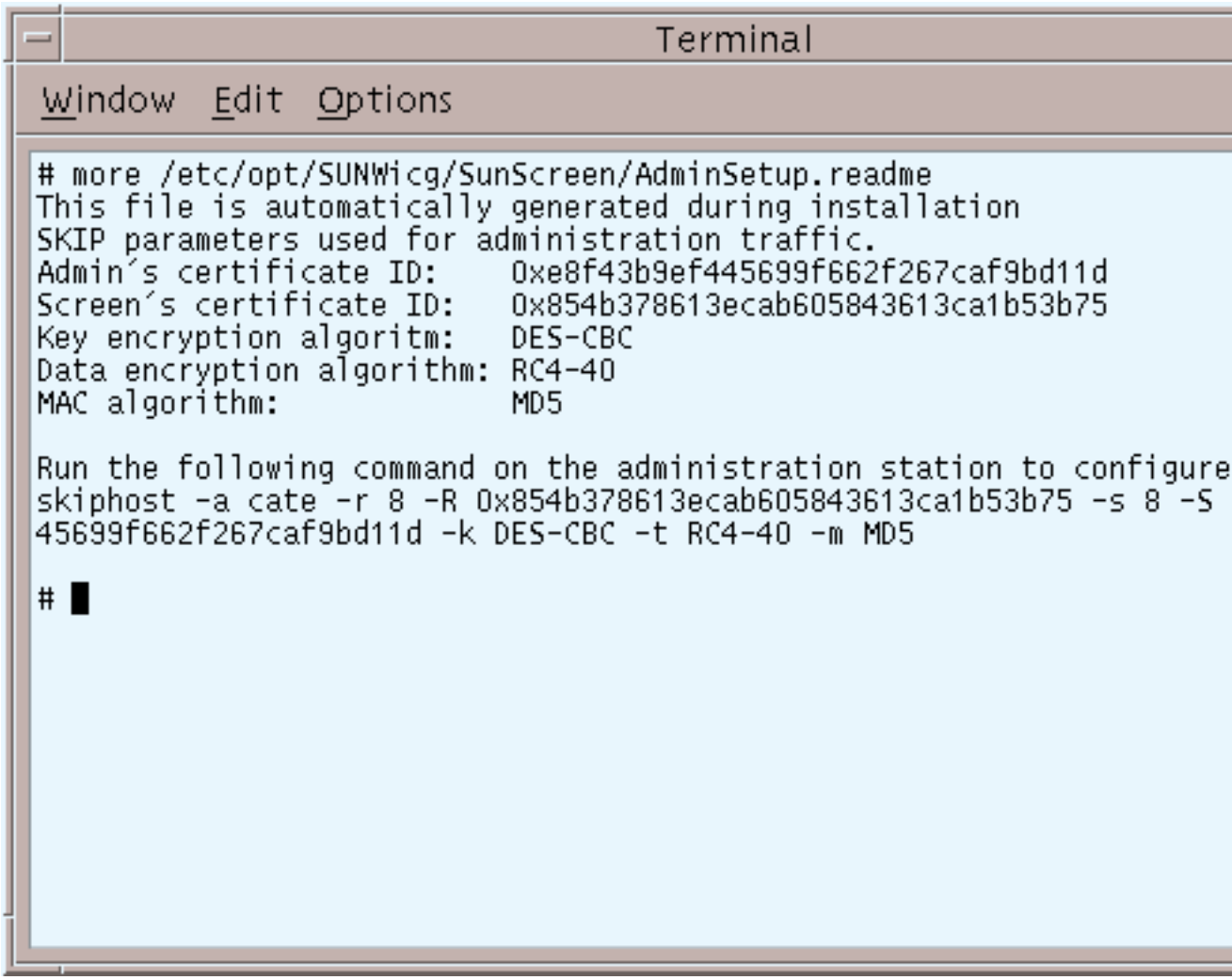



*Figure 5–9* `AdminSetup.readme` file

**5. Eject the CD-ROM by typing:**

```
# eject cdrom0
```

**6. If SKIP upgrades were installed, reboot the Screen by typing:**

```
# sync; init 6
```

You now return to the Administration Station to complete SKIP configuration. Proceed to “Using SKIP for Encrypted Communication” on page 126.

## Installing Certificates on the Administration Station

To obtain encrypted communication between the Administration Station and the Screen, certificates must be installed on both machines. This can be done by either using self-generated certificates or by installing issued certificates. Both methods are done on the Administration Station.

If you are using self-generated certificates, use Option 1. If you are using issued certificates, use Option 2.

### ▼ Option 1: To Create a Self-Generated Certificate on the on the Administration Station

1. **Open a terminal window and create the required SKIP directories by typing:**

```
# skiplocal -i
```

2. **Create the self-generated certificate on the Administration Station by typing:**

```
# skiplocal -k -f -V
```

The local certificate ID appears, as shown in Figure 5–10. It is the Administration Station’s 32-character certificate ID (MKID).

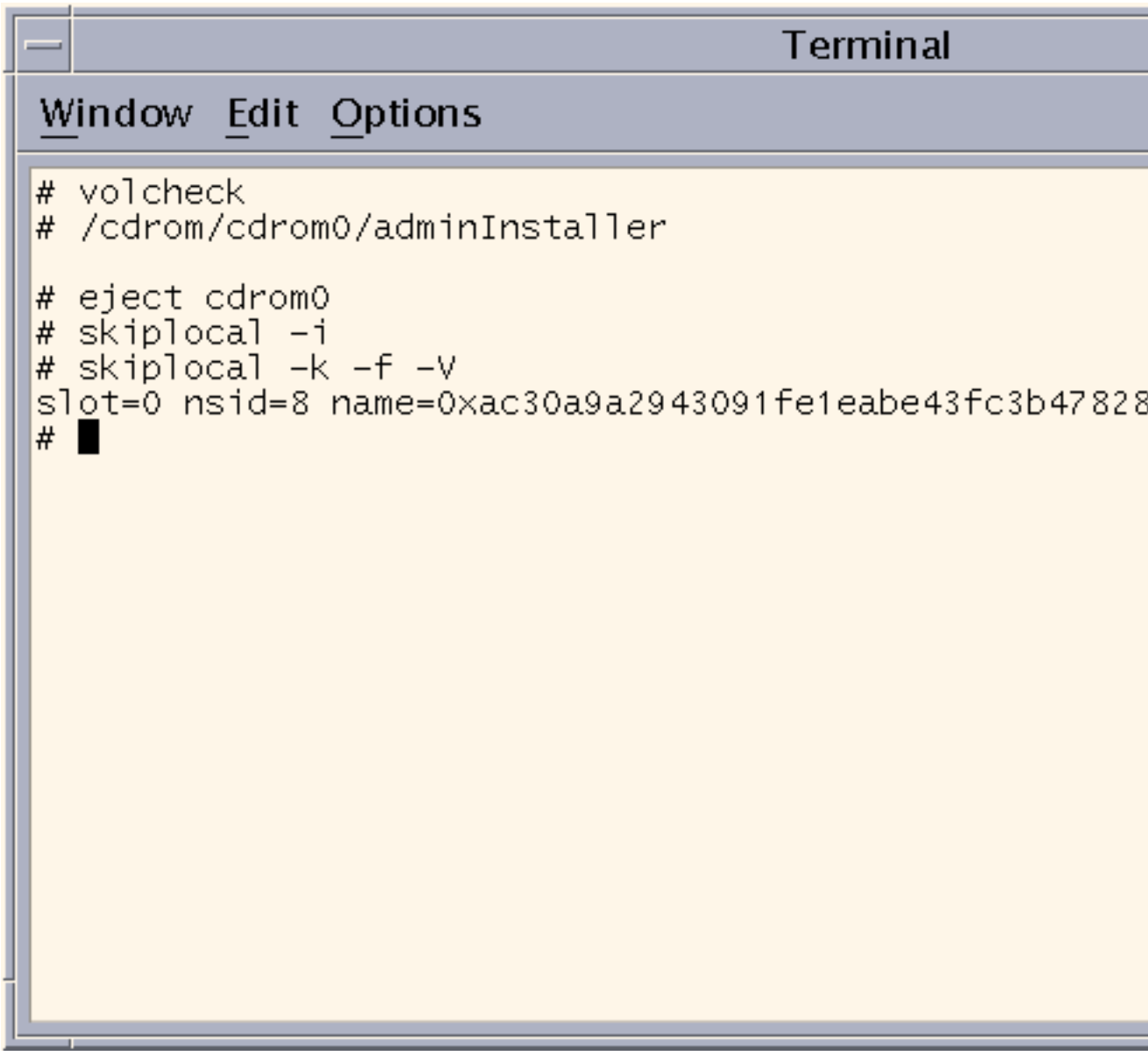



*Figure 5–10* Administration Station's Self-Generated Certificate

**3. Write down the certificate ID, beginning with Ox.**

**4. Add SKIP to all the interfaces by typing:**

```
# skipif -a
```

5. **Reboot to complete the installation by typing:**

```
# sync; init 6
```

The Administration Station's certificate ID has been generated. You next move to the Screen to install the SunScreen software. Continue to the section, "Installing the Software on the Screen" on page 105.

## ▼ Option 2: To Install the Issued Certificate on the Administration Station

To do this procedure, you will need the Key and Certificate diskette.

1. **Open a terminal window on the Administration Station and become root.**

**Caution -** Ensure that the OpenWindows File Manager is not running because it interferes with the operation of the `volcheck` command used for installation.

2. **Create the required SKIP directories by typing:**

```
# skiplocal -i
```

3. **Insert the Key and Certificate diskette into the Administration Station's floppy drive.**

4. **Mount the floppy by typing:**

```
# volcheck
```

5. **Install the SKIP keys by typing:**

```
# install_skip_keys -icg /floppy/floppy0
```

6. **Start the SKIP daemon by typing:**

```
# skipd_restart
```

7. **Eject the Key and Certificate diskette by typing:**

```
# eject floppy0
```

8. **Write down the certificate ID, which is eight characters long.**

9. **Add SKIP to all the interfaces by typing:**

```
# skipif -a
```

10. **Reboot to complete the installation by typing:**

```
# sync; init 6
```

The Administration Station's certificate ID has been installed. You next move to the Screen to install the SunScreen software.

# Installing the Software on the Screen

The next step is to install the SunScreen EFS 3.0 software on the machine that serves as the Screen. If you have a monitor and a keyboard attached to your Screen, you can use the installation wizard. If you are operating the Screen without a monitor, you must either temporarily attach a monitor and keyboard, or install the software via the command line. Command line instructions are located in Appendix A.

**Note -** Before starting the procedure below, configure *only* the network interface you plan on using for remote administration, if not already done. Configuration of additional network interfaces may result in a non-operational Screen. For details on Solaris network configuration, see the documentation accompanying the Solaris operating environment.

**Caution -** If you configure a network interface and later set it to stealth mode, the Screen will hang upon activation. If this happens, you must first reboot the Screen in single user mode; second, remove the file `/etc/hostname.`*interface_name*, which will unconfigure that interface; and third, reboot again.

## ▼ Option 1: To Install the Software on the Screen Using Self-Generated Certificates

**Note -** In this procedure, you need the Administration Station's certificate ID (MKID) from the previous procedure.

1. **On the Screen, open a terminal window and become root.**

2. **Insert the SunScreen EFS 3.0 CD-ROM into the Screen's CD-ROM drive.**

3. **Mount the CD-ROM by typing:**

```
# volcheck
```

4. **Add the software by typing:**

```
# /cdrom/cdrom0/screenInstaller
```

The SunScreen EFS Screen Install Welcome window appears, as shown in Figure 5–11.


*Figure 5–11* Screen Install Wizard's Welcome Window

**5. Click Next to continue the installation process.**

The Check Installed Solaris Packages window appears, as shown in Figure 5–12. Prior to installation of the SunScreen EFS 3.0 software, a check is performed to verify that the prerequisite Solaris packages are installed on your machine.

**Note -** If there are missing required packages, a list will be displayed. You must exit the installation wizard at this point and install the required Solaris packages from your Solaris CD.


*Figure 5–12* Checking Installed Solaris Packages Window

**6. Click Next to continue the installation process.**

The Secondary HA Designation window appears, as shown in Figure 5–13. No is the default.

Choose Yes if you are configuring an HA cluster and are installing the Secondary SunScreen of that cluster. If this is what you want to do, exit the installation wizard and see the *SunScreen EFS 3.0 Administration Guide* for instructions on how to set-up an HA cluster.


*Figure 5–13* Secondary HA Designation Window

**7. Accept the default, No, and Click Next.**

The Select Screen Type window appears, as shown in Figure 5–14. You are given two types of installations to choose from: Stealth or Routing. Routing mode is the default.


*Figure 5–14* Select Screen Type Window With Stealth Selected

**8. Select Stealth mode and Click Next.**

The Select Administration Type window appears, as shown in Figure 5–15. You are given the choice of Local Administration or Remote Administration. Local Administration is the default.

**Caution -** When operating in stealth mode, only Local Administration of the Screen is not a supported configuration. Even if the plan is to use Local Administration primarily for the Screen, the administrator should verify that Remote Administration is configured properly .


*Figure 5–15* Select Administration Type(s) Window With Remote Administration Selected

**9. Select Remote Administration, and Click Next.**

The Select Type of Install window appears, as shown in Figure 5–16. You are given two choices: Default Install and Custom Install.


*Figure 5–16* Select Type of Install Window With Default Install Selected

---

**Note -** The HotJava browser, version 1.1.5, is packaged on the SunScreen EFS 3.0 CD-ROM and is installed as part of the Default Install. If you do not want this installed, select Custom Install and deselect package `SUNWdthj`.

---

**10. Select the type of install desired, and Click Next.**

The disk space on your machine is checked. An error message appears if you do not have enough disk space.

The Ready to Install window appears, as shown in Figure 5–17. The size of the packages to be installed is confirmed.


*Figure 5–17* Ready To Install Window

**11. Click Install Now to continue the installation process.**

The Installing Window appears, as shown in Figure 5–18. The status bar shows the progress of the installation.

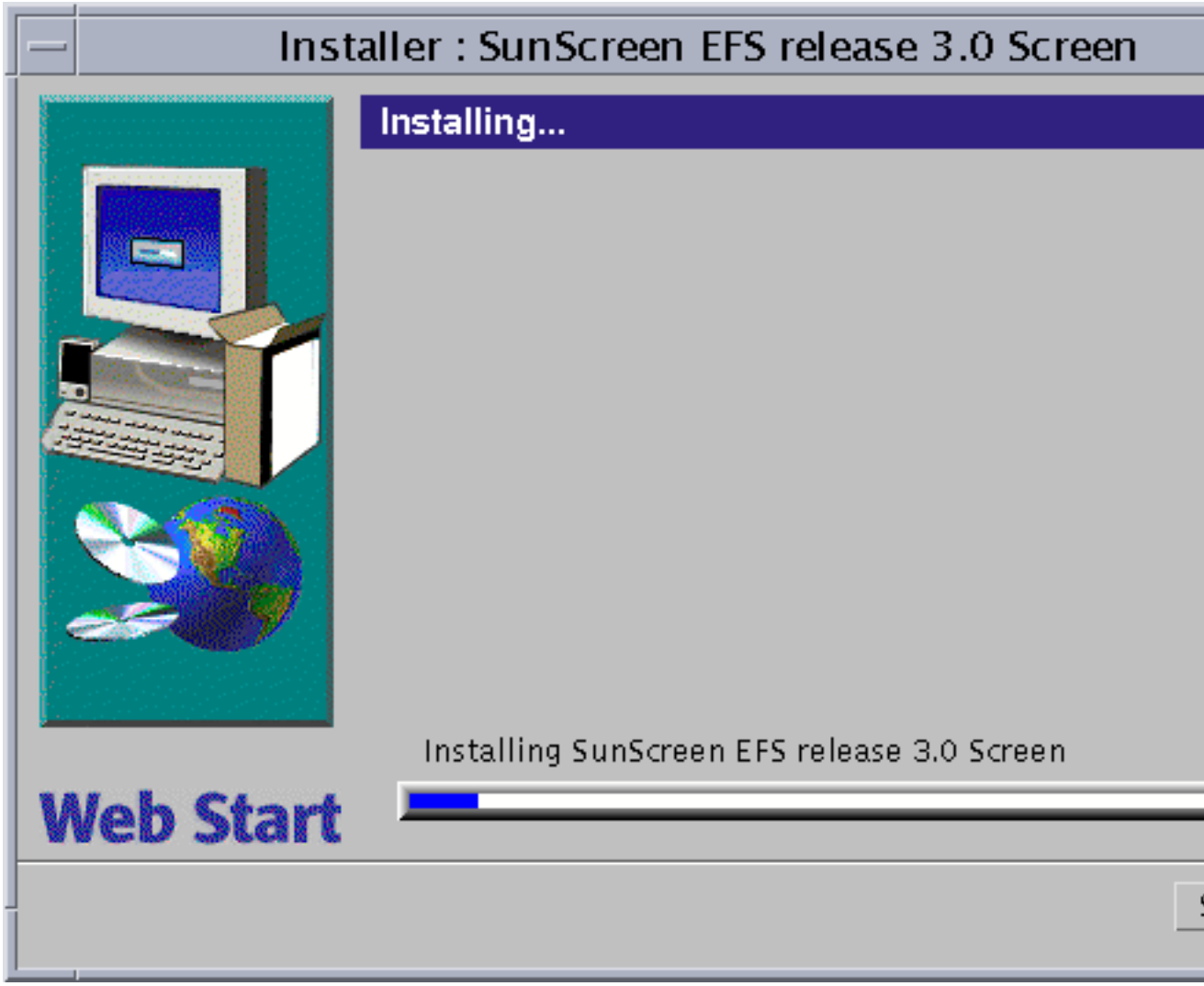



*Figure 5–18* Installing Window Showing Installation Status Bar

Once completed, the Installation Summary window appears, as shown in Figure 5–19. This window can be resized if needed.


*Figure 5–19* Installation Summary Window

**12. Click Next to continue the installation process.**

The Select Certificate Type window appears. Self-Generated Certificate is the default, as shown in Figure 5–20.


*Figure 5–20* Select Certificate Type Window With Self-Generated Certificate Selected

---

**Note -** If you are using Issued Certificates, you must now turn to the following procedure, “To Install The Software on the Administration Station” on page 89. Follow the instructions to install your Issued Certificates. Once completed, return to this procedure and resume with Step 17.

---

**13. Accept the default, Self-Generated Certificate, and Click Next.**

The Self-Generated Certificate ID window appears, as shown in Figure 5–21.


*Figure 5–21* Self-Generated Certificate ID Window

**14. Enter the Administration Station's 32-character certificate ID (MKID), obtained in the previous procedure, and Click Next. Do not enter the leading two characters: 0x.**

The Generate Screen Certificate window appears. Wait while the Screen's certificate ID is generated. When completed, the Screen's 32-character certificate ID appears at the bottom of the window, as shown in Figure 5–22.

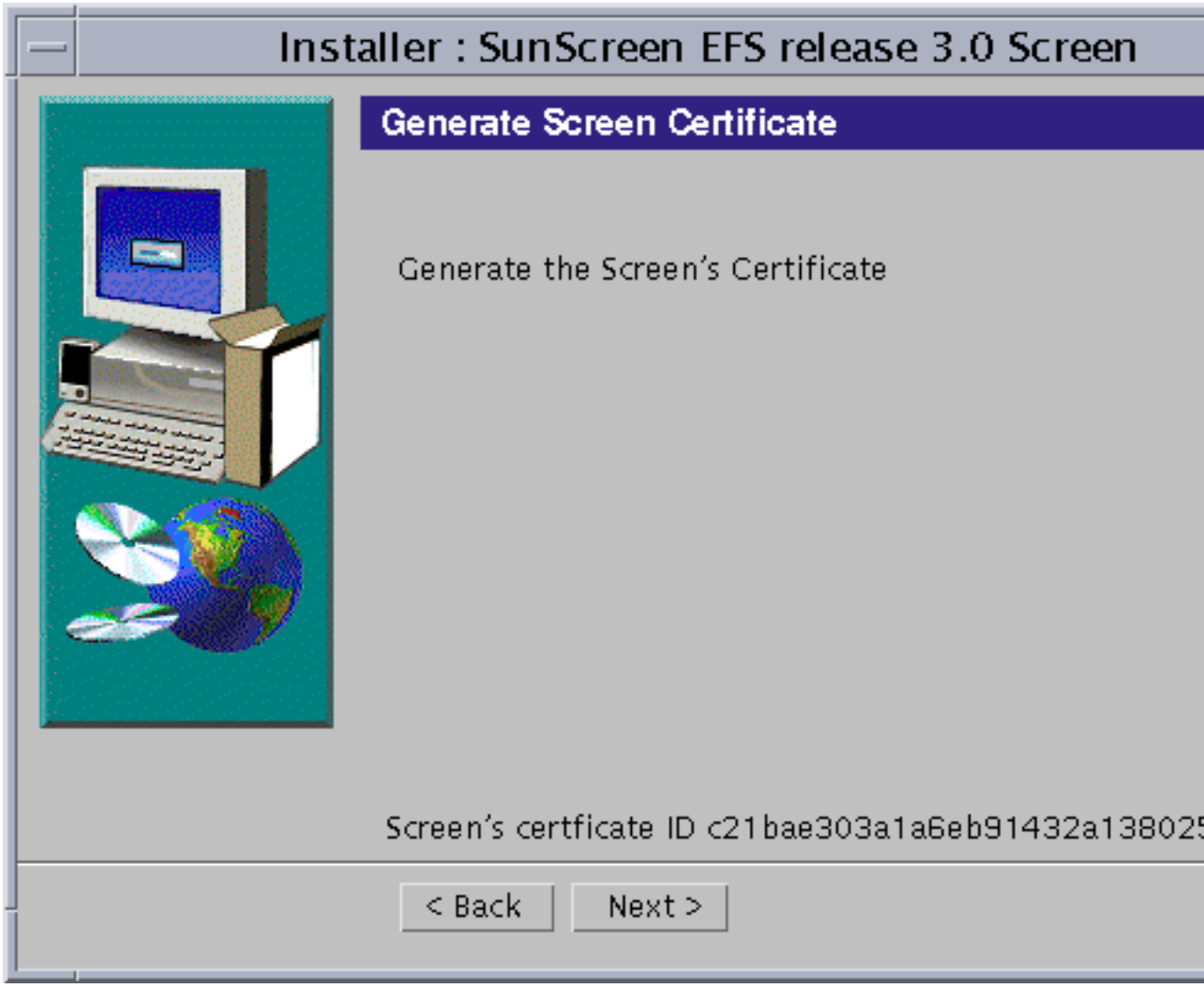



*Figure 5–22* Generate Screen Certificate With Screen's Certificate ID Generated

**15. Write down the Screen's 32-character certificate ID (MKID) that appears at the bottom of the window.**

**16. Click Next to continue the installation process.**

The Select Initial Security Level window appears.

**17. Select the level of security you want: Restrictive, Secure, or Permissive. Permissive is the default.**

When in doubt, select Permissive as your initial security level, as shown in Figure 5–23. You can change this later if you need to.


*Figure 5–23* Select Initial Security Level Window With Permissive Selected

**18. Click Next to continue the installation process.**

The Select Name Service(s) window appears, as shown in Figure 5–24. You must select the name service that will be used on the Screen. Your choices are both NIS and DNS, either NIS or DNS, or None. The default has both NIS and DNS selected. To select just one, deselect the one you do not want. For None, deselect both.

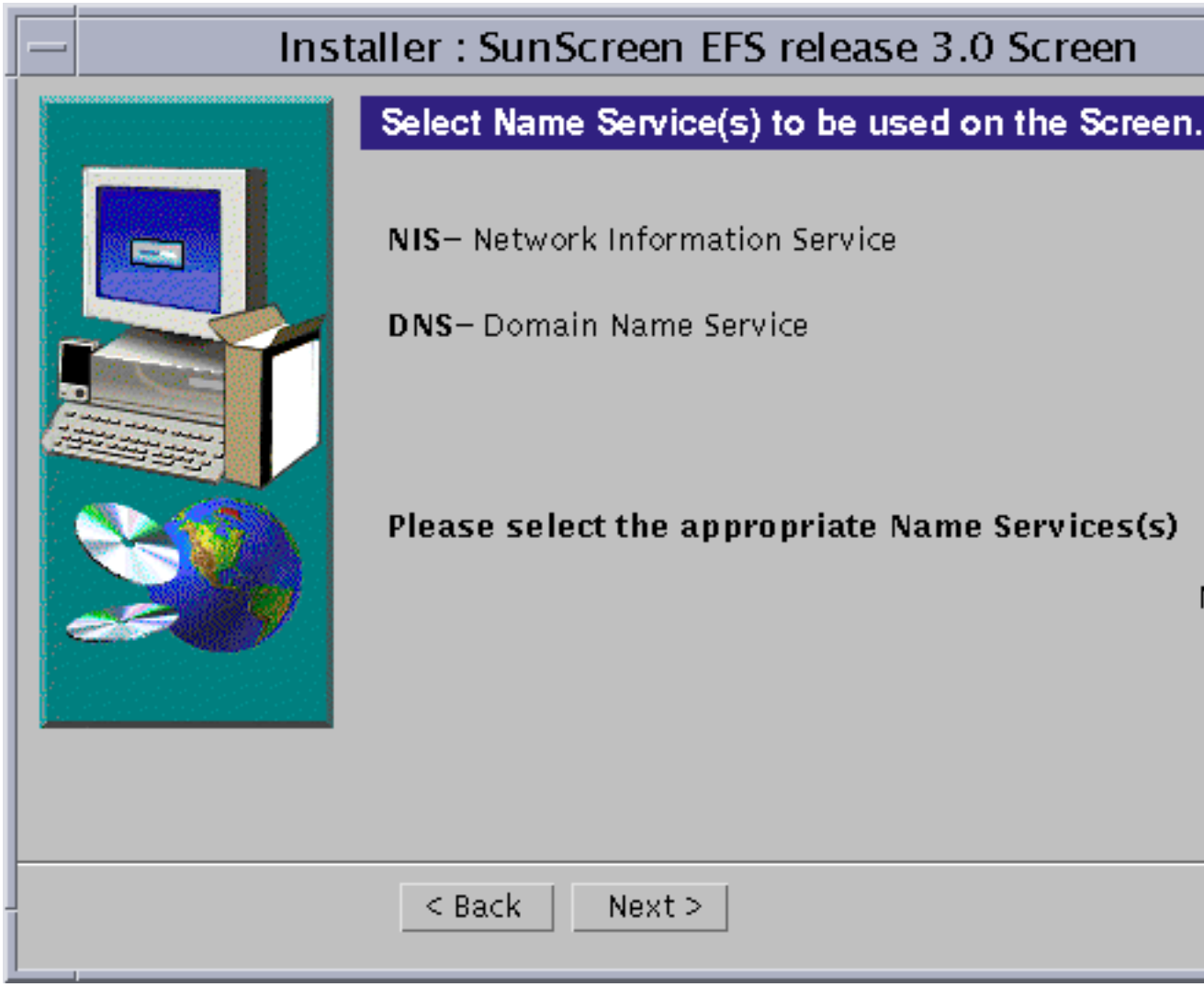



*Figure 5–24* Select Name Service(s) Window With Both NIS And DNS Selected

**19. Select the appropriate Name Service(s), and Click Next.**

The Screen Configuration window appears with the message: `Configuring Screen`, as shown in Figure 5–25. Figure 5–26 shows the message which appears when the Screen is successfully configured.

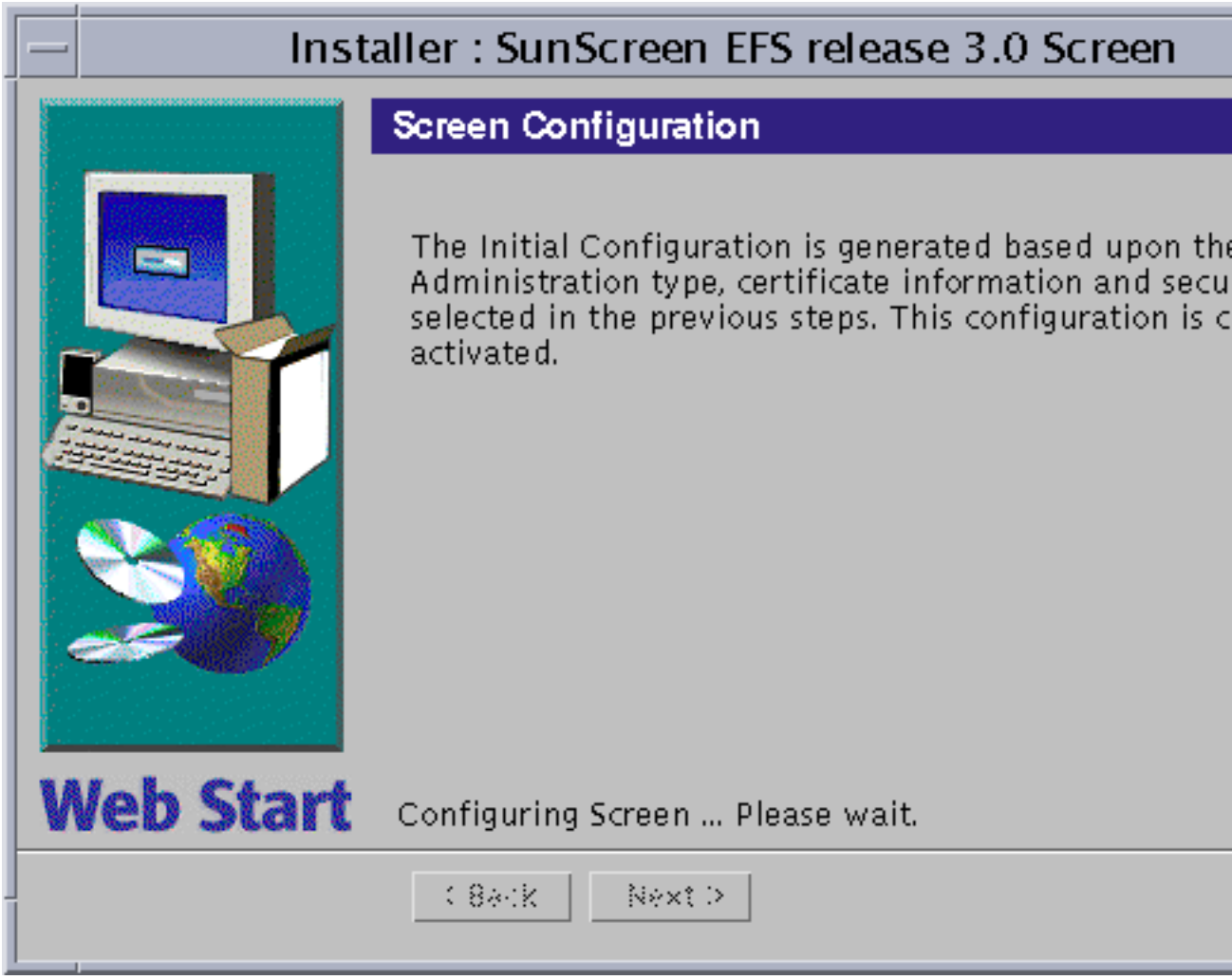



*Figure 5–25* Screen Configuration Window

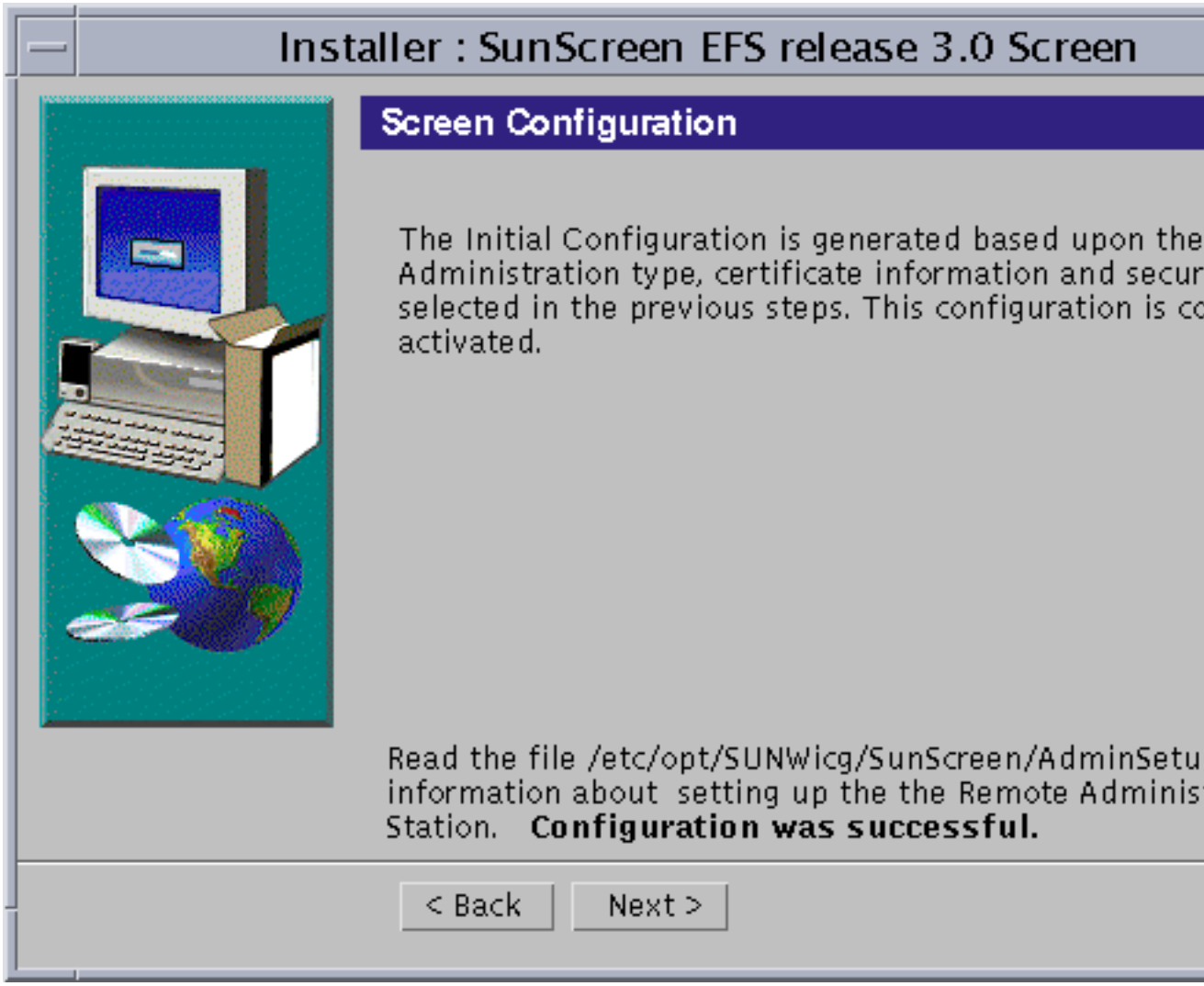



*Figure 5–26* Screen Configuration Window Once Screen Is Configured

**20. Click Next to continue the installation process.**

The Screen Hardening window appears, as shown in Figure 5–27.

**Caution -** Hardening is optional and if chosen, is an automated removal of Solaris files and packages which might otherwise make the Screen vulnerable to an attack. Once you have hardened your Screen, it becomes a dedicated firewall and the machine can not be used for another purpose without first reinstalling the Solaris operating environment.


*Figure 5–27* Screen Hardening Window

**21. (Optional) To Harden your Screen, Click the Harden Screen button and Click Next.**

The Screen Reboot window appears, as shown in Figure 5–28.

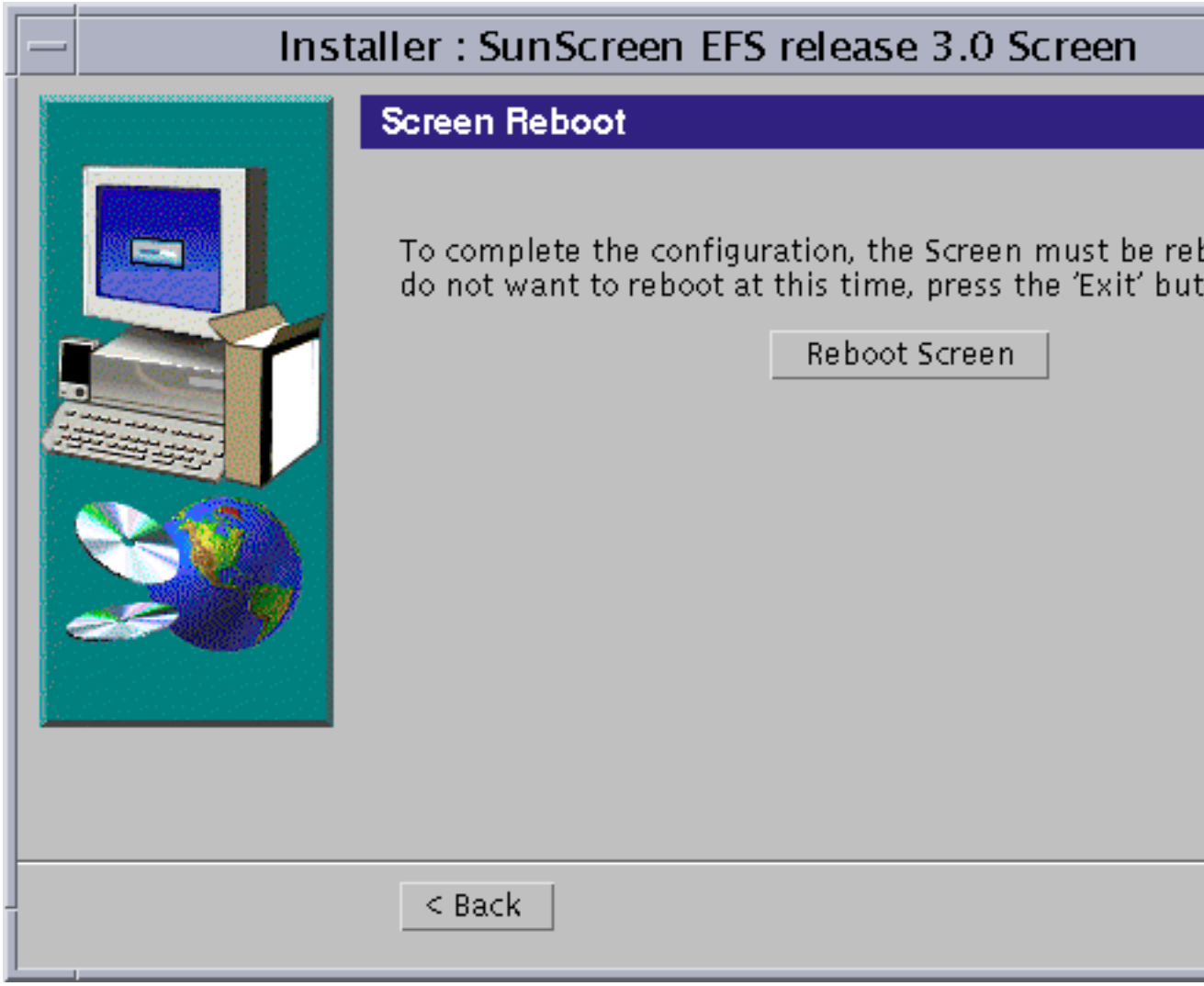



*Figure 5–28* Screen Reboot Window

**22. To reboot the machine, Click the Screen Reboot button.**

The installation wizard disappears.

**Note -** You must reboot the machine at this time in order to complete the installation process.

# Using SKIP for Encrypted Communication

To complete the installation in stealth mode, encrypted communication between the Administration Station and the Screen must be achieved. This is done by enabling SunScreen SKIP, which was previously installed. In this procedure, you will need to tell the Administration Station what encryption algorithms to use to communicate with the Screen. For more information regarding SunScreen SKIP, see the *SunScreen SKIP 1.5 User's Guide*.

To configure the Administration Station to communicate with the Screen, you need to know:

- What access control list (ACL) parameters to set to match the Screen's encryption settings.
- The Screen's certificate ID.

The command obtained from the `AdminSetup.readme` file in the previous procedure is now used.

Instructions for using SKIP from the command line are found in Appendix A.

## ▼ To Use the `skiptool` GUI

1. **Open a terminal window and become root, if not already.**

2. **Launch the skiptool GUI by entering:**

```
# skiptool
```

**Note -** You may need to use the `skiptool -i` *name_of_interface* (such as qe3) if you wish to set SKIP parameters on an interface other than the default interface.

The skiptool GUI appears, as shown in Figure 5–29.

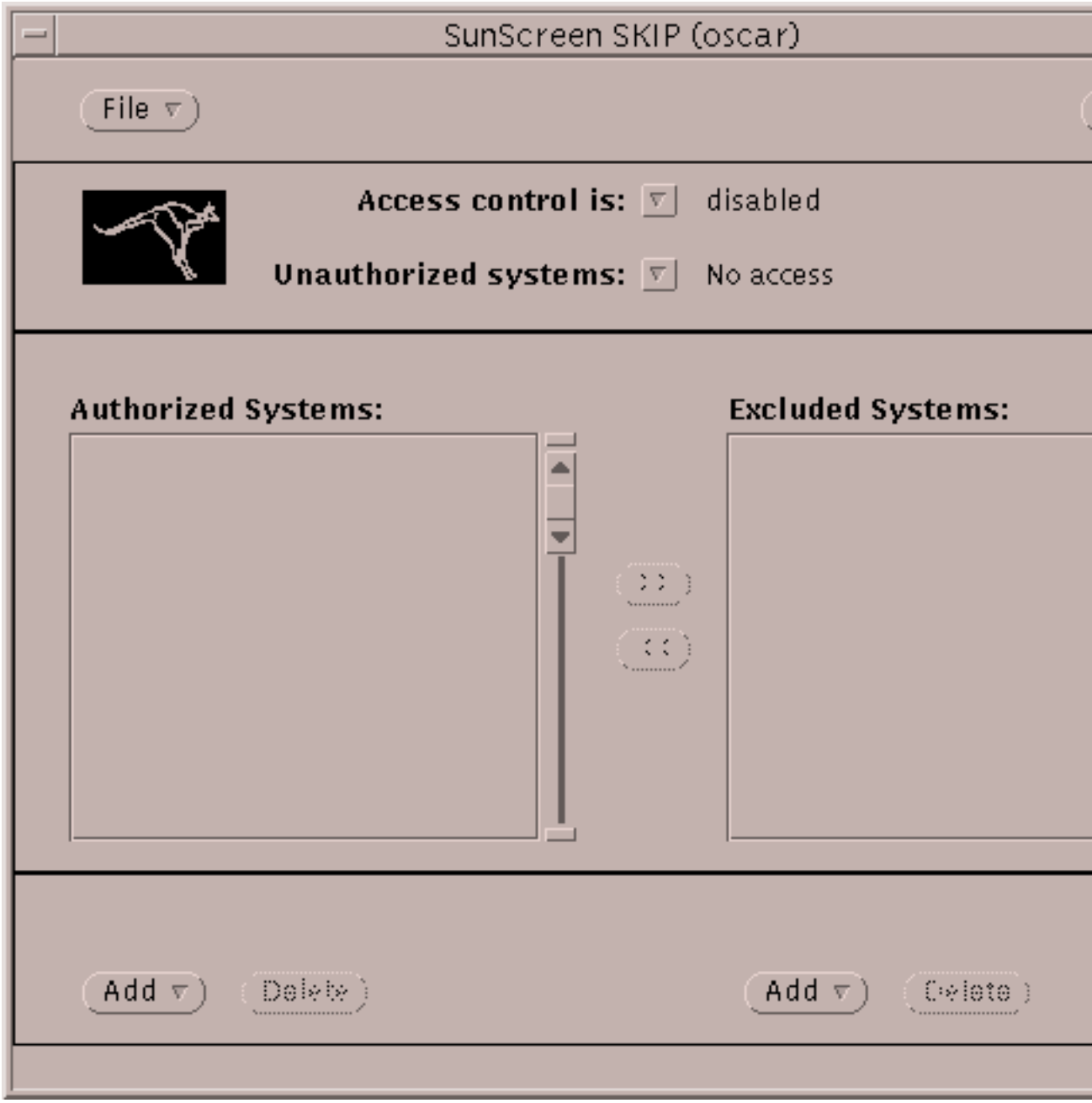



*Figure 5–29* `skiptool` Main Window

You next add a default ACL to talk to unencrypted to all hosts.

3. **Click the Add button, and under Host, choose the Off security option.**
   The Add Host properties window opens.

4. **Type ‘default’ as the Hostname and Click Apply.**
   This is shown in Figure 5–30.

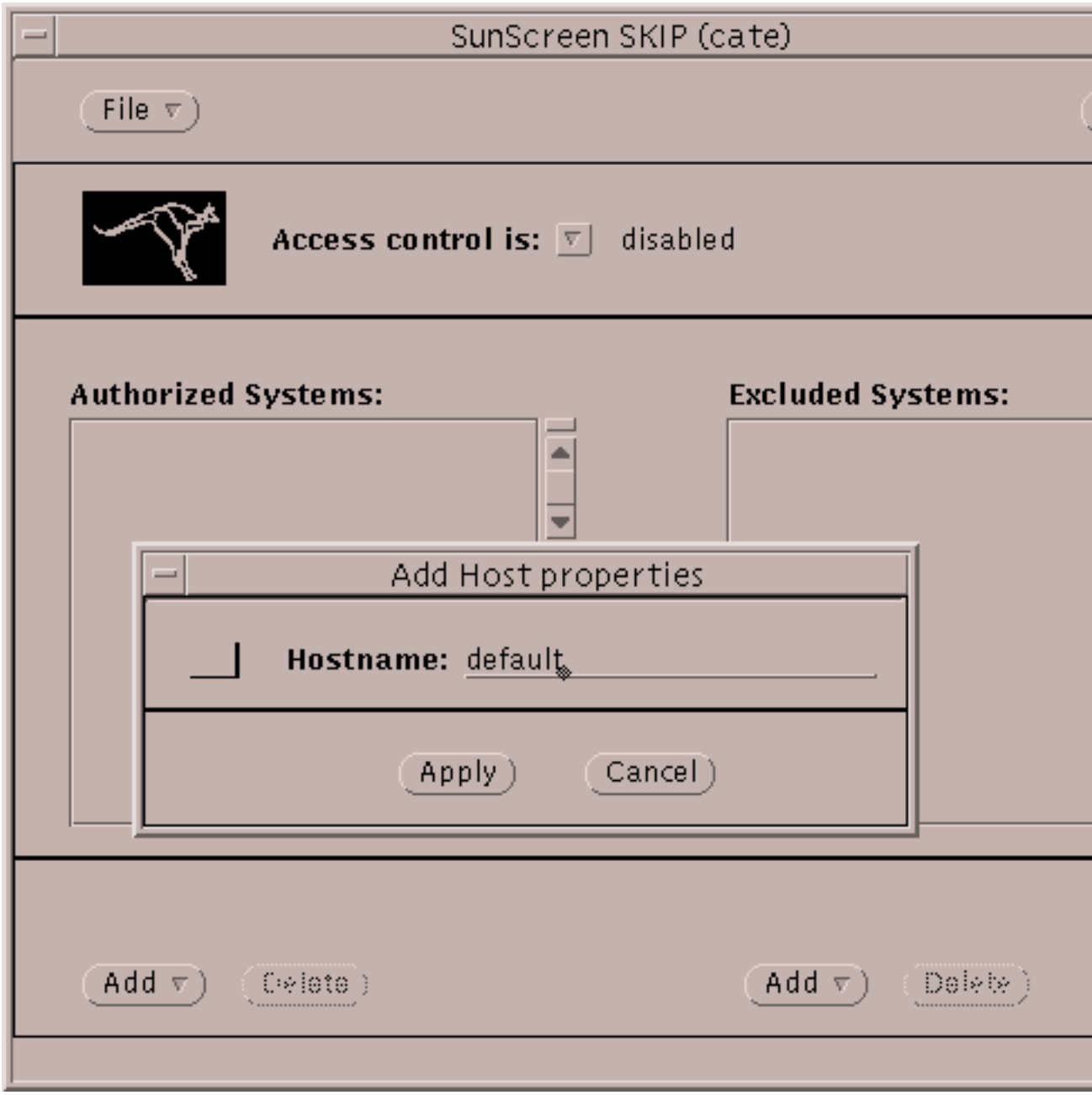



*Figure 5–30* `skiptool` With Add Host Properties Window Completed

You next add an ACL so the Administration Station and Screen can use encrypted communication.

Click the Add button, and under Host, choose the SKIP security option.

The Add Skip host properties window appears, as shown in Figure 5–31.

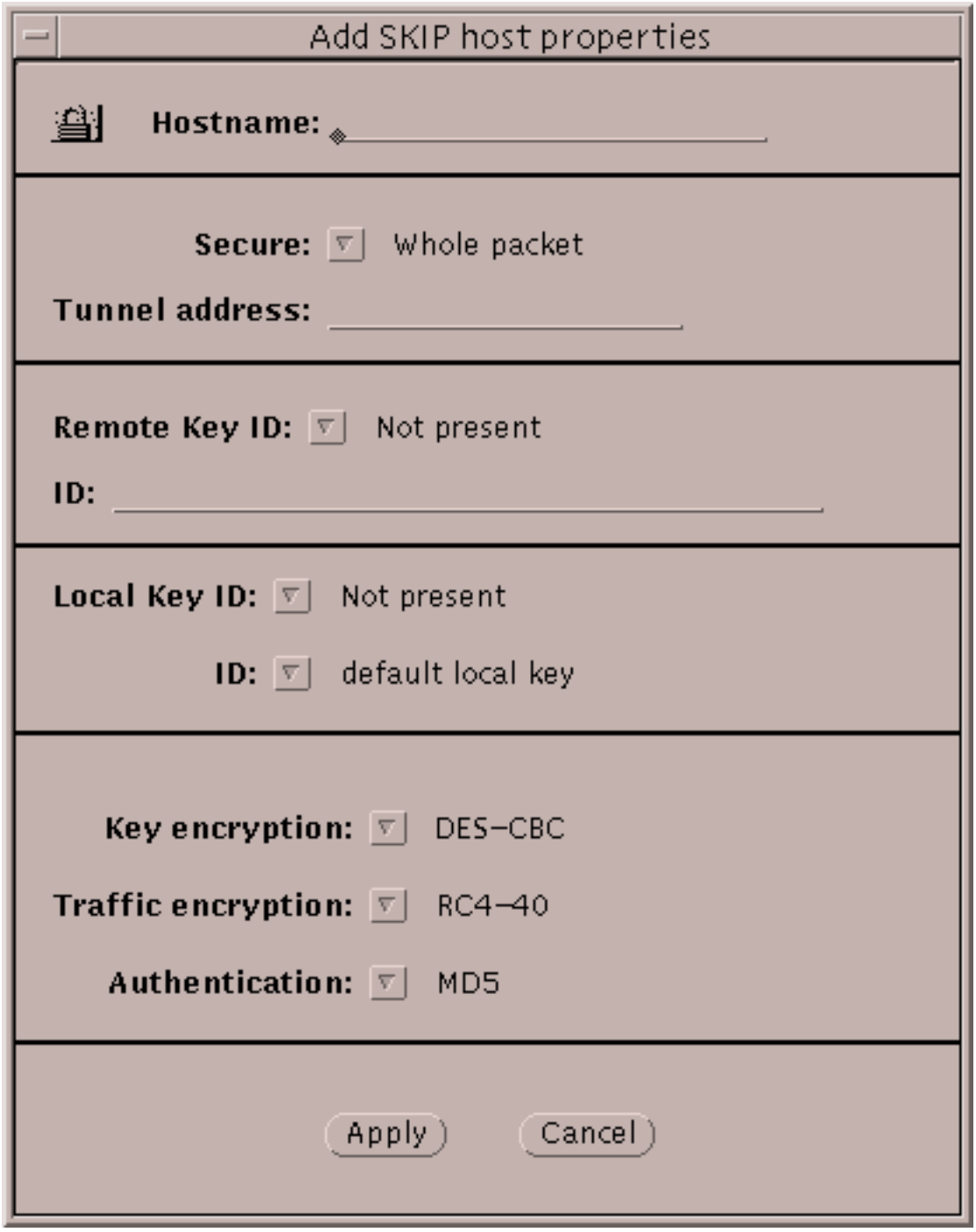



*Figure 5–31* Add SKIP Host Properties Window

Use the information contained in the AdminSetup.readme file, obtained in the preceding procedure, and complete the fields.

5. **Type *Name_of_Screen* in the Hostname field.**

6. **In the Secure field, select Whole Packet from the drop-down list.**

7. **In the Remote Key ID, make the appropriate selection from the drop-down list.**
   Refer to the `AdminSetup.readme` file to select the correct Remote Key ID. For self-generated certificates on the Administration Station, select MD5 (DH Public Value). For issued certificates, select IPv4. See Figure 5–32 for a sample of the Add SKIP Host Properties window completed.

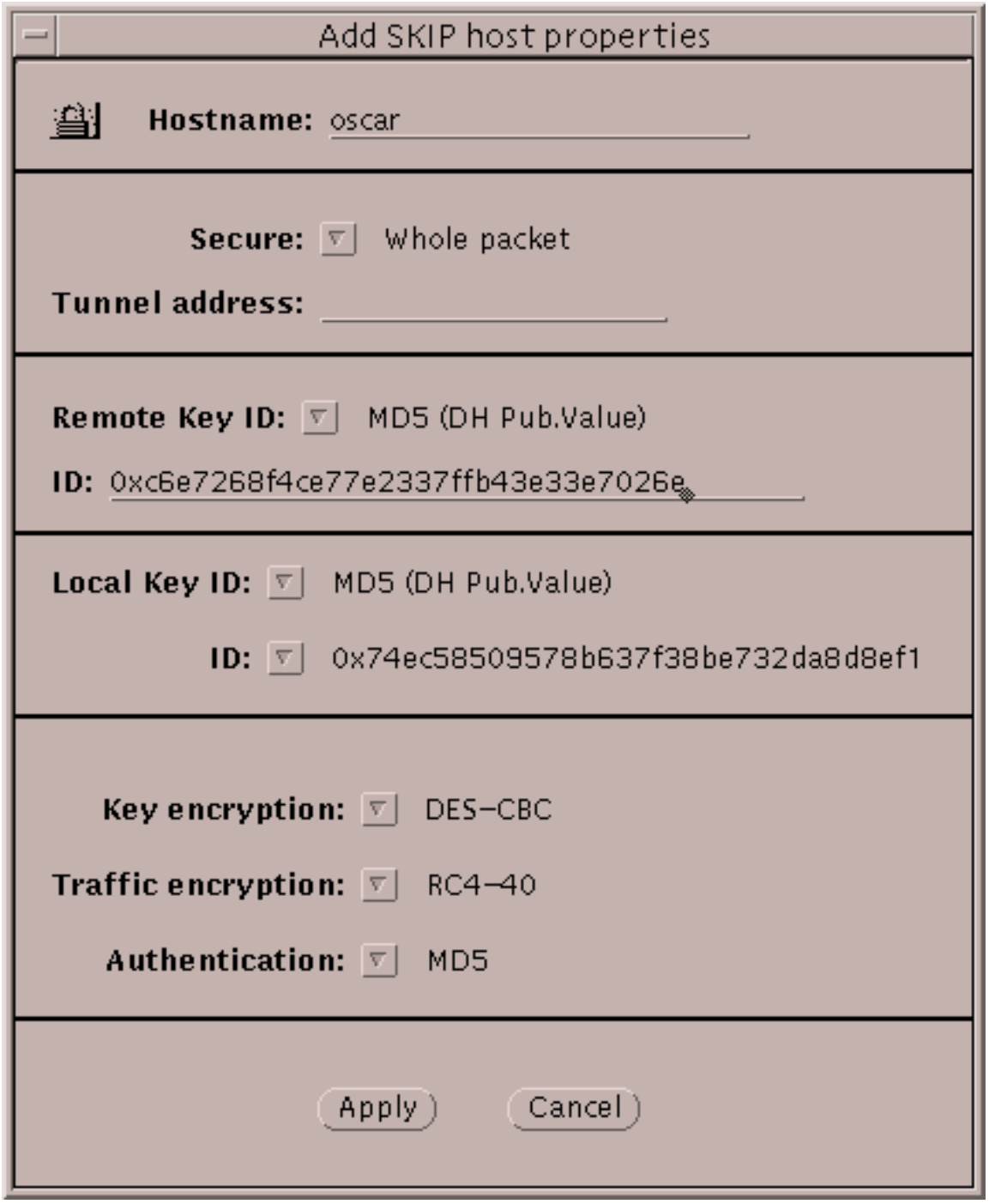



*Figure 5–32* Add SKIP Host Properties Completed

8. **In the Local Key ID, make the appropriate selection from the drop-down list.**

   Refer to the `AdminSetup.readme` file to select the correct Local Key ID. For self-generated certificates on the Administration Station, select MD5 (DH Public Value). For issued certificates, select IPv4.The ID value is filled in automatically.

9. **Turn SKIP on. From the pulldown menu for "Access control is:", located at the top of the `skiptool` window, select 'enabled'.**

---

**Note -** When you select enabled from the pulldown menu, a window appears when you save the configuration. Click Cancel to prevent these required systems, which are part of the default configuration, from showing up in the Authorized Systems window.

---

10. **Select Save from the File pulldown menu.**

---

**Note -** After configuring SKIP, check that the encryption parameters and certificate ID (MKID) values match on both the Administration Station and the Screen.

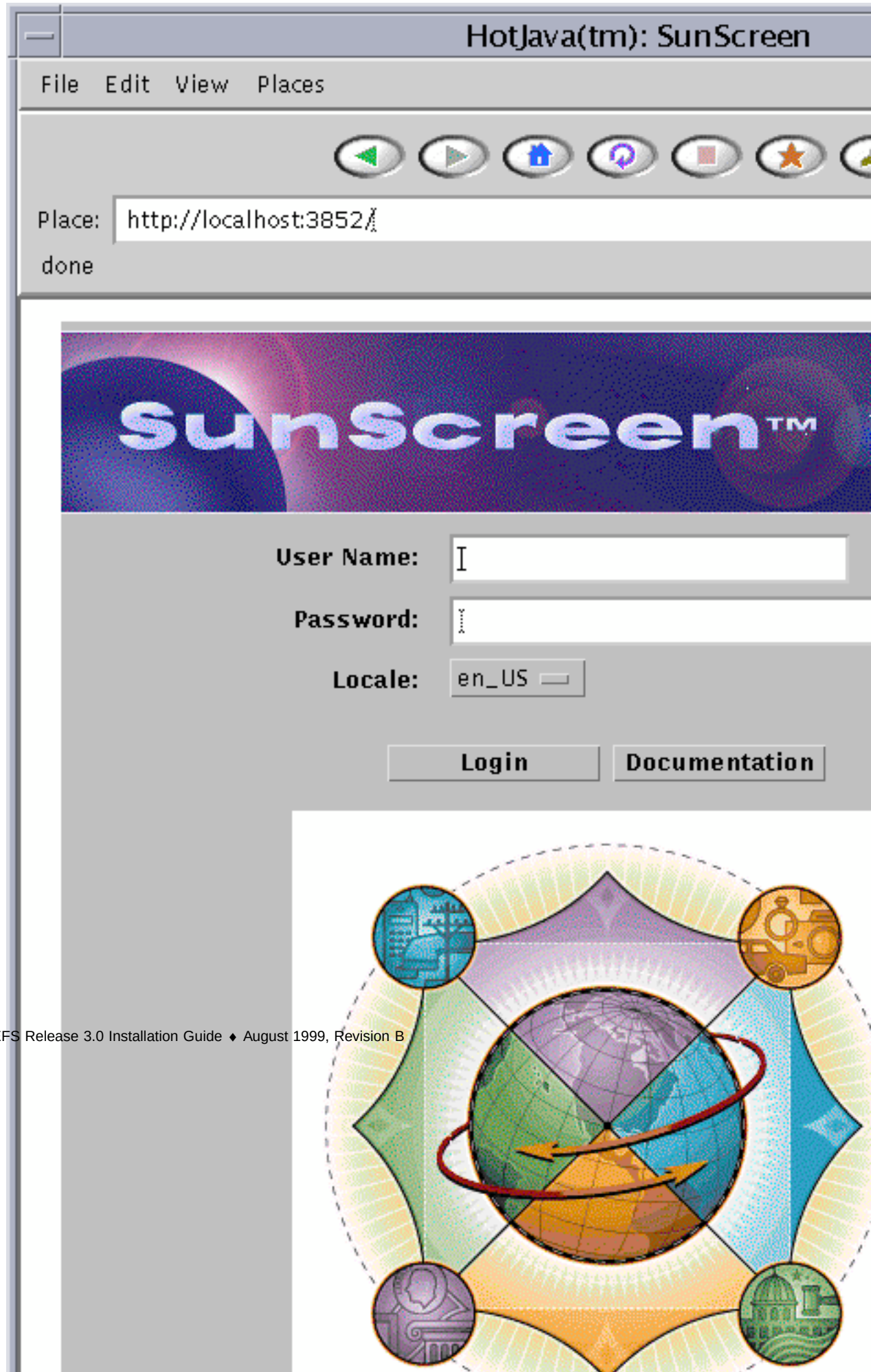
---

## ▼ To Launch the Administration GUI

a. **To configure and manage your SunScreen from your Administration Station, run a Java-enabled Web browser compliant with JDK 1.1.3 or later, and launch the Administration GUI by typing the following URL:**

```
http://Name_of_Screen:3852/
```

The Administration GUI appears, as shown in Figure 5–33.


HotJava(tm): SunScreen
File Edit View Places
Place: http://localhost:3852/
done
SunScreen™
User Name:
Password:
Locale: en_US
Login
Documentation

**b. To login, type the following and Click Login:**

```
User Name: admin
Password: admin
```

You next configure and manage your SunScreen with the Administration GUI. See the *SunScreen EFS 3.0 Administration Guide* for further instructions.

CHAPTER 6

# Upgrading to SunScreen EFS 3.0

This chapter explains how to upgrade to SunScreen EFS 3.0 from either SunScreen EFS 1.1 or 2.0, or SunScreen SPF-200.

Topics covered include:

- Overview of the upgrade from SunScreen EFS 1.1 or 2.0
- Preparing to upgrade
- Upgrading a locally administered SunScreen EFS
- Upgrading a remotely administered SunScreen EFS
- Upgrading an EFS 2.0 High Availability (HA) System
- Upgrading from SPF-200 to SunScreen EFS

**Caution -** This is not an initial installation. To retain your existing SunScreen EFS 1.1 or 2.0 configurations, you must take special care when upgrading to SunScreen EFS 3.0. Do not remove your existing software packages; this will be done as part of the procedure and must only be done in this manner.

For a remotely administered SunScreen EFS, the order in which the upgrade software is installed is different from the order given for an initial installation. Upgrade software is installed on the Screen first and then on the Administration Station. This order prevents damaging the configurations and makes communication between the Administration Station and the Screen easier.

**Note -** Since SunScreen EFS 3.0 uses ordered packet filtering rules and ordered NAT mappings, you must review your packet filtering rules after the conversion is complete to verify the filtering order is as you want. NAT mappings have changed considerably between earlier releases and SunScreen EFS 3.0. Please see the *SunScreen EFS Reference Manual* for detail on NAT mappings.

Before installing, review the *SunScreen EFS 3.0 Release Notes* for the latest information about this product.

Do not begin any of these procedures until you have read the information in Chapter 2.

# Overview of the Upgrade from EFS 1.1 or 2.0

The SunScreen EFS 3.0 CD-ROM includes a program that automatically backs up your SunScreen EFS 1.1 or 2.0 configurations, certificates, and packages to elsewhere in the filesystem in case the upgrade fails. Then the program automatically removes your SunScreen EFS 1.1 or 2.0 software packages and then installs the SunScreen EFS 3.0 software packages. The following procedures describe how to upgrade both locally and remotely administered SunScreen EFS machines.

---

**Note -** Before starting the upgrade procedure to SunScreen EFS 3.0, first make a backup of your existing logfiles. The upgrade procedure will remove your existing logfiles and they will be lost if a backup is not performed. Refer to your SunScreen EFS 1.1 or 2.0 documentation for backup procedures, if needed.

---

---

**Caution -** To retain configurations and SKIP keys and certificates (including your system's SKIP local identities) between software upgrades, do not remove `/etc/opt/SUNWicg`.

---

# Preparing to Upgrade

The following sections describe how to prepare both locally administered and remotely administered machines for upgrading.

---

**Note -** If you want to use the command line, be aware that some commands and some arguments have been removed or added since SunScreen EFS 1.1 and 2.0. Check the `man` pages and the *SunScreen EFS 3.0 Reference Manual* before using.

---

Before proceeding, verify that all the software packages required for your operating environment are installed.

## Preparing the Screen and Administration Station

SunScreen EFS, Release 3.0, runs on Solaris 2.6 and Solaris 7 operating environments for SPARC and x86 platforms. If you are running Solaris 2.5.1, or earlier, you must upgrade your operating environment to at least Solaris 2.6. In addition to the Solaris Core System Support packages, there are additional Solaris packages required prior to installing SunScreen EFS.

**Caution -** Do not reinstall the Core System Support software group if you are upgrading from SunScreen EFS 1.1 or 2.0 to SunScreen EFS 3.0.

### ▼ To Install the Prerequisite Solaris Packages and Kernel Patches on the Screen

1. **Add the following packages to the Screen from your Solaris CD, if not already on your system:**

   system SUNWdoc Documentation Tools
   system SUNWeuluf UTF-8 L10N For Language Environment User Files
   system SUNWjvjit Java JIT compiler
   system SUNWjvrt JavaVM run time environment
   system SUNWlibC SPARCompilers Bundled libC
   system SUNWlibms SPARCompilers Bundled shared libm
   system SUNWsprot SPARCompilers Bundled tools
   system SUNWtoo Programming Tools
   system SUNWvolr Volume Management (Root)
   system SUNWvolu Volume Management (Usr)
   system SUNWxwice ICE components
   system SUNWxwplt X Window System platform software
   system SUNWxwrtl X Window System & Graphics Runtime Library Links
   system SUNWmfrun Motif RunTime Kit

2. **If you are using Solaris 2.6 as your operating environment, add the following patches, if not already on your system, by typing:**

```
For SPARC systems:
# cd /cdrom/cdrom0/sparc/Patches
# patchadd 106125-06
# patchadd 105181-11
# patchadd 105284-15
```

**(continued)**

(Continuation)

```
# patchadd 105490-04
# patchadd 106040-10
# patchadd 106409-01

For x86 systems:
# cd /cdrom/cdrom0/i386/Patches
# patchadd 106126-06
# patchadd 105182-13
# patchadd 105285-15
# patchadd 105491-04
# patchadd 106041-10
# patchadd 106410-01
```

**Note -** These patches must be added in the order given.

3. **Reboot by typing**:

```
# sync; init 6
```

## ▼ To Install the Prerequisite Solaris Packages on the Remote Administration Station

1. **If you will be using a remote administration station, add the following packages to the Administration Station from your Solaris CD, if not already on your system**:

   system SUNWjvrt JavaVM run time environment

   system SUNWmfrun Motif RunTime Kit

   system SUNWxwplt X Window System Platform software

2. **If you are using Solaris 2.6 as your operating environment, add the following patches, if not already on your system, by typing**:

```
For SPARC systems:
# cd /cdrom/cdrom0/sparc/Patches
# patchadd 106125-06
# patchadd 105284-15
# patchadd 105490-04
# patchadd 106040-10
# patchadd 106409-01

For x86 systems:
# cd /cdrom/cdrom0/i386/Patches
# patchadd 106126-06
# patchadd 105285-15
# patchadd 105491-04
# patchadd 106041-10
# patchadd 106410-01
```

# Upgrading a Locally Administered SunScreen EFS

The following procedures explain how to upgrade to SunScreen EFS 3.0 from either SunScreen EFS 1.1 or 2.0.

**Note -** The upgrade software automatically backs up your system in case the upgrade fails. If there are any other system backups you want to make, do so now before performing the upgrade.

## ▼ To Upgrade to SunScreen EFS 3.0 in Routing Mode With Local Administration

**1. Open a terminal window and become root.**

**Caution -** Ensure that the OpenWindows File Manager is not running because it interferes with the operation of the `volcheck` command used for installation.

2. **Insert the SunScreen EFS 3.0 CD-ROM into the CD-ROM drive.**

3. **Mount the CD-ROM by typing:**

```
# volcheck
```

4. **Start the upgrade software by typing:**

```
# /cdrom/cdrom0/upgrade
```

   The software backs up existing SunScreen EFS packages for you. The file and package names will appear as output on your monitor. Wait until this completes.

5. **Next, the software automatically removes the existing SunScreen SKIP and SunScreen EFS 1.1 or 2.0 software packages. Wait until this completes.**

   The packages are removed automatically one-by-one. No confirmations are needed or accepted. The file and package names will appear as output on your monitor.

6. **Next, the SunScreen EFS 3.0 software is automatically installed for you. Wait until this completes.**

   The file and package names will appear as output on your monitor.

7. **Next your existing SunScreen EFS 1.1 or 2.0 configurations are automatically converted to SunScreen EFS 3.0 policies. Wait until this completes.**

   If there are any conversion errors, they are itemized as output on your monitor.

8. **Remove the SunScreen EFS, Release 1.1 or 2.0 PATH and MANPATH from your shell initialization file.**

9. **Set the SunScreen EFS 3.0 `PATH` and `MANPATH` by editing your shell initialization file (such as `.profile` or `.login` file).**

   a. **Set the `PATH` for the Bourne shell by typing:**

   ```
   PATH=/opt/SUNWicg/SunScreen/bin:$PATH
   PATH=/usr/dt/bin:$PATH
   export PATH
   ```

   b. **Set the `MANPATH` for the Bourne shell by typing:**

   ```
   MANPATH=$MANPATH:/opt/SUNWicg/SunScreen/man
   export MANPATH
   ```

10. **Eject the CD from the CD-ROM drive by typing:**

```
# eject cdrom0
```

**11. Install any SKIP upgrades (Export Controlled [1024–bit] or U.S. and Canada Use Only [2048–bit] keys) as instructed in the documentation that is included with the upgrade SKIP CD-ROM.**

While you do not need to use encryption in a locally administered SunScreen EFS, you may want to use encrypted communication over public and private networks.

**Caution -** Do not run the installation wizard as it is for an initial installation only and can corrupt your existing configurations.

**12. Reboot by typing:**

```
# sync; init 6
```

**13. Open a terminal window and become root, if not already.**

**14. List the policies that have been converted by typing:**

```
# ssadm policy -l
```

**Note -** NAT mappings have changed considerably in SunScreen EFS 3.0. If you are using NAT, you must modify it before activating the configuration. If you are converting from SunScreen EFS 1.1, be aware that ordered rules is a new feature. See the *SunScreen EFS 3.0 Reference Manual* for more detail.

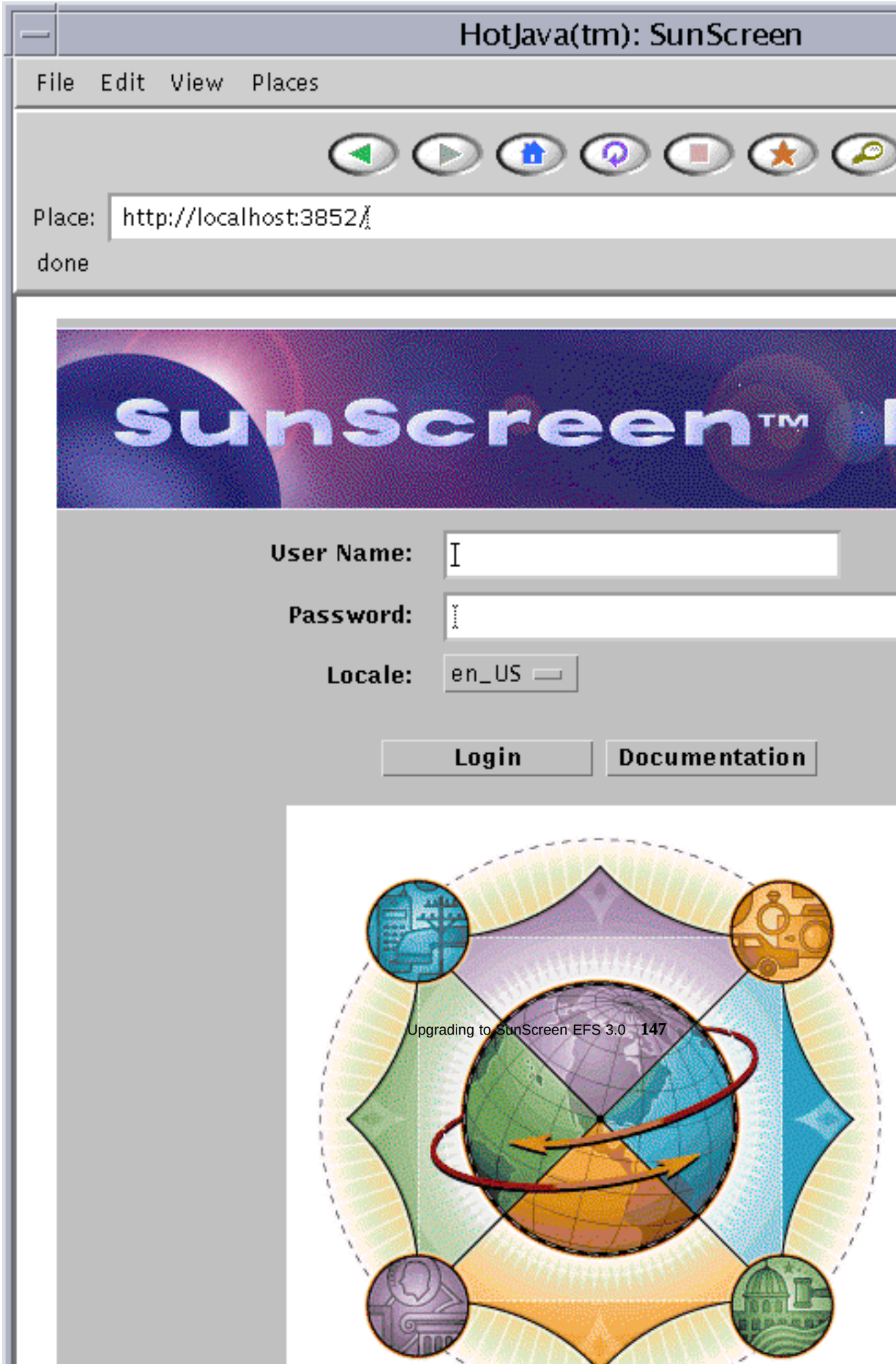
**15. Choose the one policy that you want to activate by typing:**

```
# ssadm activate configuration_name
```

**16. To configure and manage your SunScreen from your Administration Station, run a Java-enabled Web browser compliant with JDK 1.1.3 or later, and launch the Administration GUI by typing the following URL:**

```
http://localhost:3852
```

The Administration GUI login page appears, as shown in Figure 6–1


HotJava(tm): SunScreen
File Edit View Places
Place: http://localhost:3852/
done
SunScreen™
User Name:
Password:
Locale: en_US
Login
Documentation

To configure and manage SunScreen EFS, see the *SunScreen EFS 3.0 Administration Guide.*

# Upgrading a Remotely Administered SunScreen EFS

The following procedures explain how to upgrade to a remotely administered SunScreen EFS 3.0 from either SunScreen EFS 1.1 or 2.0. The upgrade software automatically backs up your system in case the upgrade fails. If there are any other system backups you want to make, do so now before performing the upgrade.

---

**Note -** The upgrade procedure for remote administration requires that you install the upgrade software on the Screen first and then on the Administration Station.

---

## ▼ To Upgrade a Remotely Administered Screen

1. **Open a terminal window on the Screen and become root.**

---

**Caution -** Ensure that the OpenWindows File Manager is not running because it interferes with the operation of the `volcheck` command used for installation.

---

2. **Insert the SunScreen EFS 3.0 CD-ROM into the CD-ROM drive.**

3. **Mount the CD-ROM by typing:**

```
# volcheck
```

4. **Start the upgrade software by typing:**

```
# /cdrom/cdrom0/upgrade
```

5. **Next, the program automatically does a back up of your existing SunScreen EFS configurations, software packages, and certificates.**

The file system names appear as output on your monitor. Wait until this completes.

6. **Next, the software automatically removes the existing SunScreen SKIP and SunScreen EFS 1.1 or 2.0 software packages. Wait until this completes.**

   The packages are removed automatically one-by-one. No confirmations are needed or accepted. The file and package names will appear as output on your monitor.

7. **Next, the SunScreen EFS 3.0 software is automatically installed for you. Wait until this completes.**

   The file and package names will appear as output on your monitor.

8. **Next your existing SunScreen EFS 1.1 or 2.0 configurations are automatically converted to SunScreen EFS 3.0 policies. Wait until this completes.**

   If there are any conversion errors, they are itemized as output on your monitor.

9. **Remove the SunScreen EFS, Release 1.1 or 2.0 PATH and MANPATH from your shell initialization file.**

10. **Set the SunScreen EFS 3.0** `PATH` **and** `MANPATH` **by editing your shell initialization file (such as** `.profile` **or** `.login` **file).**

    a. **Set the** `PATH` **for the Bourne shell by typing**:

    ```
    PATH=/opt/SUNWicg/SunScreen/bin:$PATH
    PATH=/usr/dt/bin:$PATH
    export PATH
    ```

    b. **Set the** `MANPATH` **for the Bourne shell by typing**:

    ```
    MANPATH=$MANPATH:/opt/SUNWicg/SunScreen/man
    export MANPATH
    ```

11. **Eject the CD from the CD-ROM drive by typing**:

```
# eject cdrom0
```

12. **Install any SKIP upgrades (Export Controlled [1024–bit] or U.S. and Canada Use Only [2048–bit] keys) as instructed in the documentation that is included with the upgrade SKIP CD-ROM.**

**Caution -** Do not run the installation wizard as it is for an initial installation only and can corrupt your existing configurations.

**13. Reboot by typing:**

```
# sync; init 6
```

**14. Open a terminal window and become root, if not already.**

**15. List the policies that have been converted by typing:**

```
# ssadm policy -l
```

**Note -** NAT mappings have changed considerably in SunScreen EFS 3.0. If you are using NAT, you must modify it before activating the configuration. If you are converting from SunScreen EFS 1.1, be aware that ordered rules is a new feature. See the *SunScreen EFS 3.0 Reference Manual* for more detail.

**16. Choose the one policy that you want to activate by typing:**

```
# ssadm activate configuration_name
```

You next move to the remote Administration Station.

## ▼ To Upgrade a Remote Administration Station

**1. Open a terminal window on the Administration Station and become root.**

**Caution -** Ensure that the OpenWindows File Manager is not running because it interferes with the operation of the `volcheck` command used for installation.

**2. Remove each SunScreen EFS, Release 1.1 or 2.0, package individually by typing:**

```
For SunScreen EFS 1.1:
#  pkgrm SUNWicgSA

For SunScreen EFS 2.0:
# pkgrm SUNWicgSA SUNWicgSD SUNWicgSM SUNWHJicg
```

3. **Follow the program prompts and answer all the questions with `y`.**

   The `pkgrm` program ends with the statement:
   `Removal of` *name_of_package* `was successful.`

   ---

   **Note -** If you did not originally install any of these packages, omit them from the string or else remove the packages one at a time.

   ---

4. **Remove the SKIP software packages by typing:**

```
# pkgrm SICGcrc2 SICGcrc4 SICGes SICGkeymg SICGkisup SICGbdcdr
```

5. **If needed, remove any SKIP crypto upgrades by typing:**

```
# pkgrm SICGcdes SICGc3des SICGcsafe SICGkdsup SICGkusup
```

6. **Insert the SunScreen EFS 3.0 CD-ROM into the Administration Station's CD-ROM drive.**

7. **Mount the CD-ROM by typing:**

```
# volcheck
```

8.

```
For SPARC systems:
#  pkgadd  -d /cdrom/cdrom0/sparc

For x86 systems:
#  pkgadd  -d /cdrom/cdrom0/i386
```

**Add the SunScreen EFS 3.0 packages by typing:**

For SPARC systems, you are prompted with a menu of packages to install:

```
The following packages are available:
1  SUNWbdc       SKIP Bulk Data Crypt  1.5 Software
                   (sparc) 1.5
  2  SUNWbdcx      SKIP Bulk Data Crypt (64-bit) 1.5 Software
                   (sparc) 1.5
  3  SUNWdthj      HotJava Browser for Solaris
                   (sparc) 1.1.5,REV=1998.12.03
  4  SUNWes        SKIP End System  1.5 Software
                   (sparc) 1.5
  5  SUNWesx       SKIP End System (64-bit) 1.5 Software
                   (sparc) 1.5
  6  SUNWfwcnv     SunScreen Firewall conversion
                   (sparc) 3.0
  7  SUNWhttp      Sun WebServer daemon and supporting binaries
                   (sparc) 2.0
  8  SUNWicgSA     SunScreen Administration Software
                   (sparc) 3.0
  9  SUNWicgSD     SunScreen online documentation
                   (sparc) 3.0
 10  SUNWicgSM     SunScreen man pages
                   (sparc) 3.0

... 7 more menu choices to follow;
<RETURN> for more choices, <CTRL-D> to stop display:


 11  SUNWicgSS     SunScreen Firewall
                   (sparc) 3.0
 12  SUNWkeymg     SKIP Key Manager Tools 1.5 Software
                   (sparc) 1.5
 13  SUNWkisup     SKIP I-Support module 1.5 Software
                   (sparc) 1.5
 14  SUNWrc2       SKIP RC2 Crypto Module
                   (sparc) 1.5
 15  SUNWrc4       SKIP RC4 Crypto Module  1.5 Software
                   (sparc) 1.5
 16  SUNWrc4x      SKIP RC4 Crypto Module (64-bit) 1.5 Software
                   (sparc) 1.5
 17  SUNWsman      SKIP Man Pages 1.5 Software
                   (sparc) 1.5
```

**(continued)**

**(Continuation)**

```
Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:
```

For x86 systems, you are prompted with a menu of packages to install:

```
The following packages are available:
1  SUNWbdc       SKIP Bulk Data Crypt  1.5 Software
                   (i386) 1.5
  2  SUNWdthj      HotJava Browser for Solaris
                   (i386) 1.1.5,REV=1998.12.03
  3  SUNWes        SKIP End System  1.5 Software
                   (i386) 1.5
  4  SUNWfwcnv     SunScreen Firewall conversion
                   (i386) 3.0
  5  SUNWhttp      Sun WebServer daemon and supporting binaries
                   (i386) 2.0
  6  SUNWicgSA     SunScreen Administration Software
                   (i386) 3.0
  7  SUNWicgSD     SunScreen online documentation
                   (i386) 3.0
  8  SUNWicgSM     SunScreen man pages
                   (i386) 3.0
  9  SUNWicgSS     SunScreen Firewall
                   (i386) 3.0
 10  SUNWkeymg     SKIP Key Manager Tools 1.5 Software
                   (i386) 1.5

... 4 more menu choices to follow;
<RETURN> for more choices, <CTRL-D> to stop display:


 11  SUNWkisup     SKIP I-Support module 1.5 Software
                   (i386) 1.5
 12  SUNWrc2       SKIP RC2 Crypto Module
                   (i386) 1.5
 13  SUNWrc4       SKIP RC4 Crypto Module  1.5 Software
                   (i386) 1.5
 14  SUNWsman      SKIP Man Pages 1.5 Software
                   (i386) 1.5

Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:
```

1. **For SPARC systems, enter: 1-5, 8, 10, 12-17 For x86 systems, enter: 1-3, 6, 8, 10-14**

2. **Follow the program prompts, answering all the questions with `y`.**
   When completed, you return to the same menu of packages.

3. **Type `q` to quit `pkgadd`.**

4. **Move the SKIP keys by typing:**

```
# cp -rp /etc/opt/SUNWicg/skip/* /etc/skip/.
```

5. **Eject the CD-ROM from the CD-ROM drive by typing:**

```
# eject cdrom0
```

6. **Install any SKIP upgrades (Export Controlled [1024–bit] or U.S. and Canada Use Only [2048–bit] keys) as instructed in the documentation that is included with the upgrade CD-ROM.**

7. **Reboot to complete the upgrade by typing:**

```
# sync; init 6
```

8. **Open a terminal window and become root, if necessary.**

9. **To configure and manage your SunScreen from your Administration Station, run a Java-enabled Web browser compliant with JDK 1.1.3 or later, and launch the Administration GUI by typing the following URL:**

```
http://localhost:3852
```

To configure and manage SunScreen EFS, see the *SunScreen EFS 3.0 Administration Guide.*

# Upgrading an EFS 2.0 High Availability (HA) System

**Note -** Do not run the upgrade procedure on a HA Secondary machine. It is to be run only on the EFS 2.0 HA Primary machine.

To upgrade an EFS 2.0 HA System, you must:

1. Upgrade the EFS 2.0 HA Primary machine.

To upgrade the EFS 2.0 Primary machine, follow the procedure "To Upgrade to SunScreen EFS 3.0 in Routing Mode With Local Administration" on page 143.

1. Upgrade the EFS 2.0 HA Secondary machine.

To upgrade an HA Secondary machine, you must:

1. Remove the EFS 2.0 software packages
2. Install the EFS 3.0 software packages on the machine that will be an HA Secondary
3. Configure your HA cluster

For more information on configuring and managing HA clusters, see the *SunScreen EFS 3.0 Administration Guide.*

## ▼ To Upgrade an EFS 2.0 HA Secondary Machine

1. **On the machine that is the EFS 2.0 Secondary, become root, if necessary.**

2. **Remove the EFS 2.0 software packages by typing:**

```
# pkgrm SUNWicgSS SUNWicgEF SUNWicgSA SUNWicgSD SUNWicgSM SUNWHJicg
```

**Note -** If you did not originally install any of these packages, omit them from the string or else remove the packages one at a time.

3. **Remove the SKIP software packages by typing:**

```
# pkgrm SICGcrc2 SICGcrc4 SICGes SICGkeymg SICGkisup SICGbdcdr
```

4. **If needed, remove any SKIP crypto upgrades by typing:**

```
# pkgrm SICGcdes SICGc3des SICGcsafe SICGkdsup SICGkusup
```

5. **Remove all old EFS 2.0 certificates, configurations, and logfiles by typing:**

```
# rm -rf /var/opt/SUNWicg /etc/opt/SUNWicg
```

6. **Reboot your machine to complete the removal of the EFS 2.0 installation by typing:**

```
# sync; init 6
```

## ▼ To Complete the Upgrade of an HA Primary Screen From SunScreen EFS 2.0

After you have upgraded the SunScreen EFS 2.0 HA primary Screen to SunScreen EFS 3.0, you must perform this procedure to define your HA primary Screen's HA interface. This is done only on the HA primary Screen and not on any of the HA secondary Screens. Before proceeding, you must know the following information:

- the machine name of the HA primary Screen
- the IP addresses on your dedicated HA network
- the network interface that connects to that network
- the name of the SunScreen EFS 2.0 active configuration

In this example:

- the name of the HA primary Screen is "haprimary"
- the addresses of the dedicated HA network are 129.129.129.0 to 129.129.129.255
- the network interface that connects them is `qfe0`
- the name of the SunScreen EFS 2.0 active configuration is "Initial"

After you have completed the upgrade program on the HA primary Screen and have rebooted:

1. **On the HA primary Screen, open a terminal window and become root.**

2. **Type the following:**

```
# ssadm edit Initial
edit> add address qfe0 RANGE 129.129.129.0 129.129.129.255
edit> delete interface qfe0
edit> add interface SCREEN haprimary qfe0 HA qfe0
edit> save
edit> quit
```

3. **Activate the configuration by typing:**

```
# ssadm activate Initial
```

### To Install the SunScreen EFS 3.0 Software on the HA Secondary

See the *SunScreen EFS 3.0 Administration Guide* for instructions.

### To Configure The Upgraded HA Cluster

See the *SunScreen EFS 3.0 Administration Guide* for instructions on setting up an EFS 3.0 HA cluster.

## Upgrading From SunScreen SPF-200 to SunScreen EFS 3.0 in Stealth Mode

The upgrade from SunScreen SPF-200 to SunScreen EFS 3.0 requires a unique set of steps. You can use the same machine that operates as the SPF-200 Screen and upgrade it to become a SunScreen EFS 3.0 Screen in stealth mode. If choosing this option, be aware that this will require significant downtime and you should plan a time that is convenient for this.

**Note -** It is recommended you have your original installation diskette for your SPF-200 Screen in the event that the upgrade procedure fails and you must then return to your original SPF-200 configuration.

## ▼ To Upgrade from SPF-200 to SunScreen EFS 3.0 in Stealth Mode

1. **Perform a backup of the SPF-200 Screen. Refer to your SPF-200 documentation, if needed.**

   This should be stored in a secure location as it contains sensitive information that must be protected.

2. **Perform a backup the SPF-200 Administration Station, following regular Solaris procedures.**

   This should be stored in a secure location as it contains sensitive information that must be protected.

3. **Install Patch 105047-21 on the Administration Station and Screen, if not already installed.**

   This patch is available through Sun Service.

4. **Insert the SunScreen EFS 3.0 CD-ROM into the Administration Station's CD-ROM drive.**

5. **Mount the CD-ROM by typing:**

```
# volcheck
```

6. **You must install a special patch onto the Screen. From the Administration Station, install the SPF-200 patch on the Screen by typing:**

```
# ss_client Name_of_Screen ss_patch install noreboot < \
/cdrom/cdrom0/sparc/Patches/spfUpgradePatch.tar.Z
```

**Note -** Do not install this patch on the Administration Station itself or any other system. Do not reboot your system.

7. **You must gather the SPF-200 configurations and send them back to the Administration Station. Run the special script to do this by typing:**

```
# ss_client Name_of_Screen config2 > 200config.tar
```

This file contains sensitive information. The SKIP connection creates secure, encrypted communication between the Administration Station and the Screen. Do not send this file over insecure lines. To move this file, use a diskette or a secured connection only.

**Note -** Do not change the name of the file from `200config.tar`.

8. **From the Administration Station, obtain your Administration Station's certificate ID by typing:**

```
# skiplocal list
```

A list of encryption certificate IDs is displayed.

9. **Write down the correct certificate ID for your Administration Station.**

10. **On the Screen, install either Solaris 2.6 or Solaris 7, following the instructions accompanying your Solaris CD.**

**Note -** You must do a fresh installation since the SPF-200 OS can not be upgraded.

11. **On the Administration Station, verify that your operating environment is at least Solaris 2.6. If not, upgrade your operating environment as necessary.**

12. **On the Screen, using the same interface id that the SPF-200 used as its administrative interface (e.g. `le0`), configure that interface only.**

    See the Solaris documentation, if necessary.

13. **Remove the old SunScreen SPF-200 Administration Station software by typing:**

```
# pkgrm SUNWicgSA
```

**14. Remove the old SKIP packages from the Administration Station by typing:**

```
# pkgrm SICGcrc2 SICGcrc4 SICGes SICGkeymg SICGkisup SICGbdcdr

To remove any SKIP crypto upgrades:
# pkgrm SICGcdes SICGc3des SICGcsafe SICGkdsup SICGkusup
```

**15. On the Administration Station, install the SunScreen EFS 3.0 software by following the instructions in Chapter 5.**

**16. On the Administration Station, move the SKIP keys by typing:**

```
# cp -rp /etc/opt/SUNWicg/skip/* /etc/skip/.
```

**17. Reboot the Administration Station by typing:**

```
# sync; init 6
```

**18. On the Screen, install the SunScreen EFS 3.0 software by following the instructions in Chapter 5.**

Enter the Administration Station's certificate ID from Step 9 when prompted.

**19. On the Administration Station, create a session on the Screen by entering:**

```
# SSADM_TICKET_FILE=$HOME/.ssadmticket
# export SSADM_TICKET_FILE
# touch $SSADM_TICKET_FILE
# chmod go= $SSADM_TICKET_FILE
# ssadm -r Name_of_Screen login admin admin
```

**20. On the Administration Station, verify that you are able to remotely administer the upgraded Screen by typing:**

```
# ssadm -r Name_of_Screen active
```

**21. On the Administration Station, begin the conversion of the SPF-200 configurations to SunScreen EFS 3.0 policies on the Screen by typing:**

```
# ssadm -r Name_of_Screen spf2efs < 200config.tar
```

**22. Verify your migrated configuration before activating it. To view/update the migrated configurations, open a Java-enabled web browser compliant with JDK 1.1.3 or later and launch the Administration GUI by typing:**

```
http://Name_of_Screen:3852
```

---

**Note -** NAT mappings have changed considerably in SunScreen EFS 3.0. If you are using NAT, you must modify it before activating the configuration. Be aware that ordered rules is a new feature. See the *SunScreen EFS 3.0 Reference Manual* for more detail.

---

See the *SunScreen EFS 3.0 Administration Guide* for instructions on using the Administration GUI.

**1. On the Administration Station, activate your migrated configuration by entering:**

```
# ssadm -r Name_of_Screen activate Name_of_Configuration
```

CHAPTER 7

# Converting FireWall-1 to SunScreen EFS 3.0, in Routing Mode

This chapter explains how to convert a machine running FireWall-1, Release 2.1 or 3.0, to a machine running SunScreen EFS 3.0, in routing mode.

Topics covered include:

- Preparing your FireWall-1 configuration for conversion
- Converting FireWall-1 to SunScreen EFS 3.0
- SunScreen EFS conversion utility
- Generating conversion files
- Troubleshooting the `fwconvert` utility
- Creating the configuration
- After conversion

Before installing, review the *SunScreen EFS 3.0 Release Notes* for the latest information about this product.

## Preparing Your FireWall-1 Configuration for Conversion

Before starting the conversion of your FireWall-1 configuration to a SunScreen EFS 3.0 performing in routing mode, please read this section carefully. There are certain limitations which must be addressed before running the conversion utility. You will experience unrecoverable errors if you do not first review your existing FireWall-1

configurations and modify those that will not convert directly to SunScreen EFS 3.0 rules. The following tables list those limitations that are known.

Prior to converting your FireWall-1 to SunScreen EFS 3.0, you should check your FireWall-1 configuration files and hand edit any that may contain reserved characters in comments and object names, or reserved words used for object names. If any of the following characters or reserved words are mis-used, you will need to first hand-edit these to remove or replace them. See TABLE 7-1 for a list of known reserved characters.

**TABLE 7–1** Known FireWall-1 Reserved Characters

| | **Illegal Characters** | **Illegal Characters** |
|---|---|---|
| String contains | ‘ ‘ (space) | ‘+’ |
| | ‘*’ | ‘?’ |
| | ‘)‘ | ‘)’ |
| | ‘{‘ | ‘}’ |
| | ‘[‘ | ‘]’ |
| | ‘!’ | ‘#’ |
| | ‘<‘ | ‘>’ |
| | ‘=’ | ‘,’ (comma) |
| | ‘:’ (colon) | ‘:’ (semicolon) |
| | ‘’’ (quote) | ‘‘’ (back quote) |
| | ‘””’ (double quote) | ‘/’ (slash) |
| | ‘\’ (back slash) | ‘\t’ (tab) |

Table 7–2 contains a list of known reserved words which must not appear in the FireWall-1 object names, and must be edited prior to conversion:

**TABLE 7–2** Known FireWall-1 Reserved Words

| | | |
|---|---|---|
| “accept” | “expcall” | “hosts” |
| “modify” | “pass” | “set” |
| “and” | “expires” | “if” |
| “navy blue” | “r_arg” | “skippeer” |
| “black” | “firebrick” | “ifaddr” |
| “netof” | “r_cdir” | “src” |
| “blue” | “foreground” | “ifid” |
| “nets” | “r_cflags” | “static” |
| “broadcasts” | “forest” | “in” |
| “nexpires” | “r_ckey” | “sync” |
| “green” | “call” | “format” |
| “inbound” | “not” | “r_connarg” |
| “targets” | “date” | “from” |
| “interface” | “or” | “r_ctype” |
| “day” | “fwline” | “interfaces” |
| “orange” | “r_entry” | “tod” |
| “define” | “fwrule” | “ipsecmethods” |
| “origsport” | “r_proxy_action” | “ufp” |
| “delete” | “gateways” | “ipsecdata” |
| “origdst” | “r_xlate” | “wasskipped” |
| “do” | “gold” | “keep” |
| “origsrc” | “record” | “xlatedport” |
| “domains” | “gray 101” | “limit” |
| “other” | “red” | “xlatedst” |

**TABLE 7–2** Known FireWall-1 Reserved Words *(continued)*

| | | |
|---|---|---|
| “drop” | “green” | “log” |
| “outbound” | “refresh” | “xlatesport” |
| “dst” | “hold” | “magenta” |
| “packet” | “reject” | “xlatesrc” |
| “dynamic” | “host” | “medium slate” |
| “packetid” | “routers” | “xor” |
| “r_tab_status” | “vanish” | “direction” |
| “get” | “kbuf” | “gateways” |
| “netobj” | “resourceobj” | “servobj” |
| “servers” | “tracks” | “cyan” |
| “dark green” | “dark orchid” | “forest green” |
| “medium slate blue” | “red” | “sienna” |
| “yellow” | “to” | |

There are known limitations when converting from a machine running FireWall-1 configurations to a machine running SunScreen EFS 3.0. Certain object-types and rules will migrate with no difficulty, while others will not. Those rules which are known not to migrate contain an operation which is performed on the Source, Destination, or Service in the original FireWall-1 rule, as SunScreen EFS 3.0 does not support any of these operations. Table 7–3 lists what is known to migrate and what is known not to migrate when converting from FireWall-1 to SunScreen EFS 3.0.

**TABLE 7–3** What Does and Does Not Convert From FireWall-1

| **Does Migrate** | **Does Not Migrate** |
|---|---|
| Host Objects | Resources |
| Group Objects | NAT Mappings |
| Network Objects | Gateway Objects |

**TABLE 7–3** What Does and Does Not Convert From FireWall-1 *(continued)*

| Does Migrate | Does Not Migrate |
|---|---|
| Most Rules | Encryption and Authentication Information / Rules |
| | Domain Objects |
| | Router Objects |
| | Switch Objects |
| | Logical Objects |
| | FW-1 Services or User Defined Services |
| | Install Objects |
| | Rules which contain any Object or Service that can not migrate |
| | Using an Object Type as an Object Name |

**Note -** NETWORK is not a supported type in SunScreen EFS 3.0. You must modify objects of this type first, before trying to access the configuration (called a “Policy” in SunScreen EFS 3.0) using the Administration GUI.

# SunScreen EFS 3.0 Conversion Utility

The following procedures explain how to install, generate, and run the conversion utility.

## ▼ To Install the Conversion Utility

1. **Open a terminal window and become root on the FireWall-1 machine, if you are not already.**

2. **Insert the SunScreen EFS 3.0 CD-ROM into the CD-ROM drive.**

3. **Mount the CD-ROM by typing:**

```
# volcheck
```

4. **Add the software by typing:**

```
For SPARC systems:
# pkgadd -d /cdrom/cdrom0/sparc SUNWfwcnv

For x86 systems:
# pkgadd -d /cdrom/cdrom0/i386 SUNWfwcnv
```

5. **Continue the installation when prompted by pressing Return.**

   The various files in `SUNWfwcnv` are displayed as they are installed. The installation ends with the following message:
   `Installation of` SUNWfwcnv `was successful.`

The SunScreen EFS conversion utility is now installed in `/opt/SUNWfwcnv/bin`.

# Generating Conversion Files

The following procedures explain how to generate conversion files.

The `fwconvert` utility, located in the `/opt/SUNWfwcnv/bin` directory, is used to generate files that create the SunScreen EFS 3.0 configuration from the original FireWall-1 configuration. The `fwconvert` utility examines the rules and objects in your FireWall-1 security policy and generates new configuration files with commands for configuring SunScreen EFS 3.0.

`fwconvert` uses the following FireWall-1 configuration files:

- *policy.name*`.W`, for FireWall-1, Release 2.1, files
- *policy.name*`.pf`, for FireWall-1, Release 3.0, files
- `objects.C`, for FireWall-1, Release 2.1 and 3.0 files

where *policy.name* is either `default` or the name you have given your policy. These files are located in the `/opt/SUNWfw/conf` directory.

Verify the location of these files and the name of the policy file (indicated by the `.pf` or `.W` extension) before you run `fwconvert`.

---

**Note -** You must run the conversion utility on the FireWall-1 machine, even if you are configuring SunScreen EFS 3.0 on another machine.

---

## ▼ To Run the Conversion Utility

1. **Open a terminal window and become root on the FireWall-1 machine, if you are not already.**

2. **Run the conversion program by typing:**

```
# /opt/SUNWfwcnv/bin/fwconvert &
```

`fwconvert` displays the FW-1 Configuration Convertor dialog box with the default values already inserted, as shown in Figure 7–1.

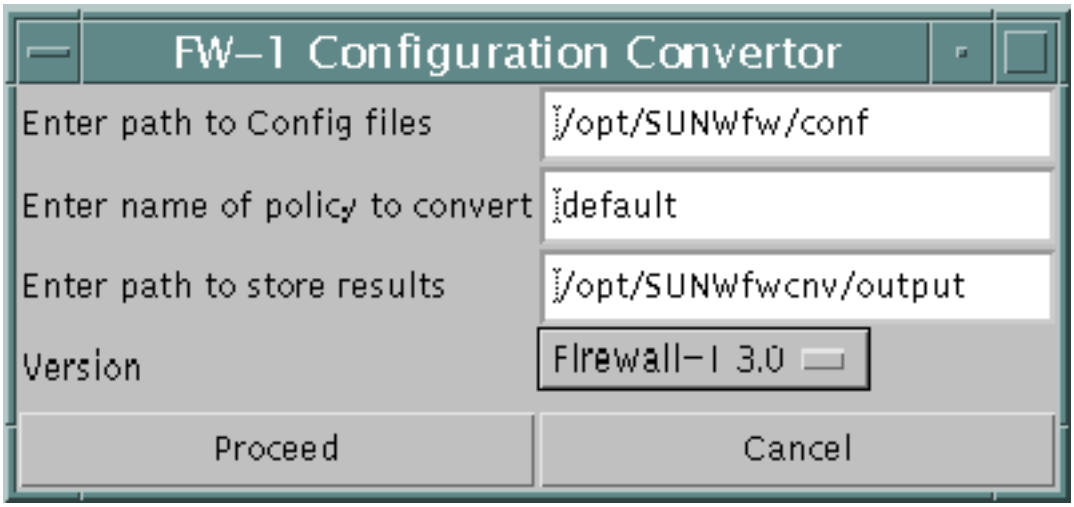



*Figure 7–1* FireWall-1 Configuration Convertor Dialog Box

3. **Type the path name where the FireWall-1 conversion files are located, or accept the default, if appropriate.**

4. **Type the name of the policy file you want to convert, if different from the default.**

   **Note -** Do not type the `.pf` or `.W` extension.

5. **Type the name of the directory where you want to store the new configuration files, or accept the `/opt/SUNWfwcnv/output` default.**

6. **Pull down the Version menu and choose the release number of your FireWall-1 software, or accept the default, if appropriate.**

7. **Click Proceed to start the conversion.**

   `fwconvert` reads the file *policy.name*`.pf` (or *policy.name*`.W`) and the `objects.C` files and generates the files used to generate the SunScreen EFS configuration.

   When `fwconvert` completes successfully, the FireWall-1 Configuration Convertor dialog box displays a DONE button.

8. **Click DONE to exit `fwconvert`.**

# Troubleshooting the `fwconvert` Utility

The following section describes how to troubleshoot the `fwconvert` utility.

## Conditions for Failure

The following conditions can cause the conversion to fail:

- You do not have permission to read files in `/opt/SUNWfw/conf` or the directory you specified as the location of the FireWall-1 configuration files.
- You do not have permission to write files into the directory that you specified for storing the results of `fwconvert`.
- The path names that you specified to the Convertor are incorrect.
- The policy name that you specified is incorrect.

- One of the FireWall-1 configuration files you need to convert is missing.

When `fwconvert` encounters these conditions, it displays an error message in the FW-1 Convertor dialog box, as shown in Figure 7–2.

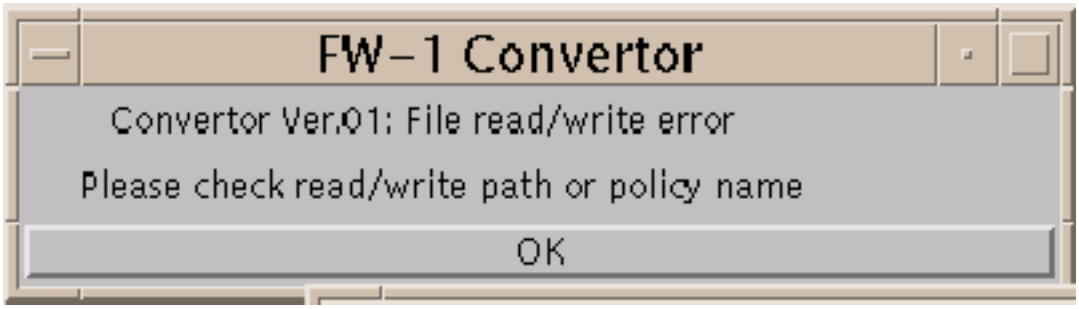



*Figure 7–2* Error Message From `fwconvert`

---

**Note -** When data can not be parsed, this error is displayed on the terminal window and not in the FW-1 Converter dialog box.

---

## ▼ To Clear Conversion Errors, Except Parse Errors

1. **Click the OK bar to clear the error message in the FW-1 Convertor dialog box.**

2. **Change permissions on the affected directories, if applicable.**

3. **Fill in the corrected information in the `fwconvert` FW-1 Convertor dialog box, making sure you have the accurate path names and file names that you need to specify.**

4. **Click the Retry button.**

   When it completes successfully, the FireWall-1 Configuration Converter displays the DONE button.

5. **Click DONE to exit `fwconvert`.**

   `fwconvert` creates a set of files that are used to generate the SunScreen EFS configuration.

6. **Verify the converted Rules.**

   For more information, see the following section, Verifying the Converted Rules.

After the conversion is complete, the generated configuration files are located in the directory you specified in the FireWall-1 Configuration Converter dialog box, `/opt/SUNWfwcnv/output` by default. The *policy.name*_`Objects` and *policy.name*_`Rules` files must reside in the same directory as *policy.name*_`efscfg` before you can run the *policy.name*_`efscfg` generation program. It is suggested you first examine these files to confirm that the information was correctly converted.

### ▼ To Clear Parse Errors

1. **Hand edit the line containing the error.**

2. **Restart `fwconvert`.**
   See the procedure “To Run the Conversion Utility”, if needed.

## Verifying the Converted Rules

`fwconvert` creates three types of files from the FireWall-1 configuration files: command, executable, and log files. See Table 7–4 for a complete list. These files are described below.

**TABLE 7–4** Generated Configuration Files

| File Type | File Name | Description |
|---|---|---|
| Data File | *policy.name*_`Objects` | Contains the commands for configuring the SunScreen EFS addresses. |
| Data File | *policy.name*_`Rules` | Contains the commands for adding SunScreen EFS rules that use the generated objects. |
| Executable Script | *policy.name*_`efscfg` | Generates a SunScreen EFS configuration from the commands *policy.name*_`Objects` and *policy.name*_`Rules`. |

**TABLE 7–4** Generated Configuration Files *(continued)*

| File Type | File Name | Description |
|---|---|---|
| Log File | *policy.name*_Obj.log | Contains the objects from FireWall-1 that are not supported by SunScreen EFS. |
| Log File | *policy.name*_Rule.log | Contains the rules from FireWall-1 that could not be added. The rule is shown as a SunScreen EFS rule command with an explanation of the reason why the rule is not supported. |
| Log File | *policy.name*_Unused.log | List of the FireWall-1 objects that cannot be used in SunScreen EFS. |

# Command and Executable Files

When you create the new SunScreen EFS 3.0 configuration, you run the configuration program, which then executes the command files. You do not need to take further action on the command and executable files.

Examples of the `policy.name_Objects` file, `policy.name_Rules` file, and the `policy.name _efscfg` file, respectively, follows.

```
# The address commands may contain other addresses which need to be created.
# These objects are logged in the policyname_Obj.log file

 add_nocheck Address  "mailhost-INT" HOST 205.167.60.6 COMMENT "Object from FW-
1"
 add_nocheck Address  "mailhost-EXT" HOST 207.82.121.5 COMMENT "Object from FW-
1"
 add_nocheck Address  "localnet" NETWORK 205.167.60.00 255.255.255.00  COMMENT
"Object from FW-1, will need to be modified before using the GUI"
 add_nocheck Address  "talon" HOST 205.167.60.200 COMMENT "Object from FW-
1"
 add_nocheck Address  "exosecure-alc" HOST 207.82.121.254 COMMENT "Object from FW-
1"
 save
```

```
add_nocheck Rule  "ip all" "*" "*"  ALLOW  LOG SUMMARY
 save
```

```
#!/bin/csh


setenv PATH .:/usr/bin:/usr/sbin:/bin:/opt/SUNWicg/SunScreen/bin


echo Creating Policy: 4complex

ssadm policy -a 4complex

echo Adding Policy Addresses

/opt/SUNWicg/SunScreen/bin/
ssadm edit -P 4complex < 4complex_Objects

echo Adding Policy Rules

/opt/SUNWicg/SunScreen/bin/ssadm edit -P 4complex < 4complex_Rules

echo Finished!
```

# Log Files

The log files describe instances where `fwconvert` could not directly convert your FireWall-1 policy to an equivalent SunScreen EFS 3.0 policy. After conversion, you should review the contents of the log files to determine further actions that might be necessary for the new SunScreen EFS 3.0 configuration.

## *policy.name*_`Obj.log`

The *policy.name*_`Obj.log` file lists objects found in your FireWall-1 security policy that were not directly supported in SunScreen EFS 3.0. Table 7–5 lists the FireWall-1 objects and shows whether they were converted to SunScreen EFS.

**TABLE 7–5** How Conversion to SunScreen EFS Affects FireWall-1 Objects

| FireWall-1 Object | EFS Equivalent | Conversion Status |
|---|---|---|
| Host | Host | Yes. |
| Network | None | Yes. Does not appear in the GUI but will show up on the command line. To make them visible in the GUI, manually change the NETWORK objects to RANGE objects via the command line. |
| Router | None | No. See the *policy.name*_`Obj.log` file for details. |
| Switch | None | No. See the *policy.name*_`OBJ log` file for details. |
| Domain | None | No. See the *policy.name*_`OBJ log` file for details. |
| Group | Group | Yes. |
| Gateways | None | No. However, they are logged in the *policy.name*_`OBJ.log` file. Gateways require more configuration within SunScreen EFS to assure that the IP addresses of the gateway are correct. See the `ss_interfaces` man pages for more information. |

Following is a sample which shows the *policy.name*_`Obj.log` file, similar to the file that you can generate from your FireWall-1 policy.

```
/***** SunScreen EFS 3.0: Firewall-1 conversion log *****/
/***** @(#)ObjStore.java        3.6 99/03/
03 Sun Microsystems, Inc. *****/

Objects of type: gateway, need some user decisions
You had a gateway with name "skil" ipaddr 205.167.60.13
If this is the gateway on which SunScreen is being installed please refer to the
'ssadm edit' command to enable the interfaces
```

## *policy.name*_`Rule.log`

This file shows rules generated from FireWall-1 rules that cannot be used in the SunScreen EFS environment without modification. The *policy.name*_`Rule.log` file explains why these rules were not added to the SunScreen EFS firewall, for example:

- Source, Destination, or Installed on objects are of a type not supported by SunScreen EFS 3.0
- FireWall-1 Service is of a type not supported by SunScreen EFS 3.0

- FireWall-1 Action is not supported by SunScreen EFS 3.0

SunScreen EFS 3.0 does not support FireWall-1 encryption, user authentication, or client authentication. Encryption in SunScreen EFS 3.0 is accomplished through SKIP, as explained in the *SunScreen EFS 3.0 Reference Manual*. For more information regarding SKIP, see the *SunScreen SKIP 1.5 User"s Guide*.

**Caution -** All FireWall-1 rules are generated during the conversion. You must manually remove any rules that you do not need.

The following shows a sample of a *policy.name*_`Rule.log` file such as you might find after FireWall-1 to SunScreen EFS conversion.

```
/***** SunScreen EFS 3.0: Firewall-1 conversion log *****/
/***** @(#)RuleStore.java       3.5 99/03/
03 Sun Microsystems, Inc. *****/


Rule below not added as the action Encrypt is configured differently in SunScreen
EFS.
 add_nocheck Rule  "smtp" "aiims" "*" Encrypt



Rule below not added as the action Encrypt is configured differently in SunScreen
EFS.
 add_nocheck Rule  "echo" "aiims" "*" Encrypt



Rule below not added as the action User Authentication is not valid in SunScreen EFS.
 add_nocheck Rule  "ftp" "*" "aiims" User



Rule below not added as the action Client Encryption/
Authentication is not valid in
SunScreen EFS.
 add_nocheck Rule  "dns" """ "*" Client
```

## *policy.name*_`Unused.log`

The following lists FireWall-1 objects encountered in your policy that are not supported by SunScreen EFS.

```
#Invalid Objects from FW-1
#Wed Mar 31 17:40:23 PST 1999
invalidobj1=gateway skil
```

# Creating the SunScreen EFS 3.0 Configuration

The following procedures explain how you prepare for and generate the new SunScreen EFS 3.0 configuration.

Choosing which of the next two procedures to follow depends on whether you plan to run SunScreen EFS 3.0 on the former FireWall-1 machine or on a new machine. Option 1 discusses preparing the FireWall-1 machine to become a SunScreen EFS 3.0 machine. Option 2 discusses preparing a new machine to run the converted FireWall-1 configurations.

---

**Note -** Only one of the following two procedures must be done.

---

## ▼ Option 1: To Prepare the FireWall-1 Machine to Run SunScreen EFS 3.0

1. **Open a terminal window and become root.**

2. **Save the existing FireWall-1 configuration files located in the /opt/SUNWfw/conf directory as a backup.**

3. **Use the** `pkgrm` **command to remove the** `SUNWfw` **package by typing:**

```
# pkgrm SUNWfw
```

4. **Upgrade your operating environment to at least Solaris 2.6, if not already done.**
   See your Solaris documentation for instructions, if necessary.

5. **Install the additional Solaris packages and kernel packages required as listed in Chapter 2, if not already done.**

   ---

   **Note -** Prior to installing the SunScreen EFS software, make sure that the machine is performing properly as a router.

   ---

6. **Insert the SunScreen EFS 3.0 CD-ROM into the CD-ROM drive.**

7. **Mount the CD-ROM by typing:**

```
# volcheck
```

8. **Add the SunScreen EFS software by typing:**

```
# /cdrom/cdrom0/screenInstaller
```

This command sets up the `Initial` configuration. It is not equivalent to the FireWall-1 policy. The installation wizard performs the initialization required by SunScreen EFS 3.0.

The SunScreen EFS installation wizard's Welcome window appears. The installation wizard will guide you through the installation process. For more detailed instructions, see Chapter 3.

9. **Reboot the system by typing:**

```
# sync; init 6
```

Continue to the section, "To Generate the New SunScreen EFS Configuration."

## ▼ Option 2: To Prepare a New SunScreen EFS Machine to Run the Converted FireWall-1 Configuration

---

**Note -** Prior to installing the SunScreen EFS software, make sure that the machine is performing properly as a router.

---

1. **Open a terminal window and become root, if not already.**

2. **Upgrade your operating environment to at least Solaris 2.6, if not already done.**
   See your Solaris documentation for instructions, if necessary.

3. **Install the additional Solaris packages and kernel packages required as listed in Chapter 2, if not already done.**

4. **Insert the SunScreen EFS 3.0 CD-ROM into the CD-ROM drive.**

5. **Mount the CD-ROM by typing:**

```
# volcheck
```

6. **Copy the generated configuration files to a directory on the new SunScreen EFS 3.0 machine.**

7. **Add the SunScreen EFS 3.0 software on the new SunScreen EFS machine by typing:**

```
# /cdrom/cdrom0/screenInstaller
```

The SunScreen EFS Screen Install's Welcome window appears. The installation wizard will guide you through the installation process. For more detailed instructions, see Chapter 3.

8. **Reboot the new SunScreen EFS machine by typing:**

```
# sync; init 6
```

Continue to the section, "To Generate the New SunScreen EFS Configuration."

## ▼ To Generate the New SunScreen EFS 3.0 Configuration

1. **Open a terminal window and become root, if not already.**

2. **Change to the directory where the conversion files were saved and make the *policy.name*_efscfg file executable by typing:**

```
# chmod 544 policy.name_efscfg
```

Verify that the commands in the generated file are accurate.

3. **Run the script by typing:**

```
# ./policy.name_efscfg
```

*policy.name*_`efscfg` creates the new SunScreen EFS 3.0 configuration from the FireWall-1 configuration, which is similar to the FireWall-1 policy.

See the *SunScreen EFS 3.0 Administration Guide* for instructions on activating the configuration.

CHAPTER 8

# Removing SunScreen EFS 3.0 Software

This chapter explains how to remove the SunScreen EFS 3.0 software from your machine.

## *To Remove SunScreen EFS*

1. **If you have used Proxies in your configuration:**

   Remove all rules that use proxies (or else instantiate a policy that uses no proxies) to restore the `sendmail` and `inetd` daemons to their original Solaris functionality. On configurations with a number of centrally managed Screens, it may be simpler to restore these daemons manually:

   a. **If the FTP or telnet proxies are in use, the `ftp` or `telnet` services will have been commented out in `/etc/inet/inetd.conf` (preceded with `#efs#`); for example:**

```
#efs#ftp  stream tcp nowait root /usr/sbin/in.ftpd in.ftpd  #efs#telnet stream tcp nowait root /usr/sbin/in.telnetd in.t
```

   Remove the commenting prefix (`#efs#`).

   b. **If the SMTP proxy is in use, in `/etc/init.d/sendmail`, the command that invokes `sendmail` as a listening daemon will have been altered to look like:**

```
/usr/lib/sendmail -q15m & #efs{-bd}
```

   Move the commented `{-bd}` option back into its original location:

```
/usr/lib/sendmail -bd -q15m &
```

2. **Use `pkgrm` to remove the software packages originally installed on the machine.**

3. **To remove the configurations and log files, you must remove these files**:
   - `/var/opt/SUNWicg` and its descendants, which contains the SunScreen packet logfiles.
   - `/etc/opt/SUNWicg` and its descendants, which contains the SunScreen configurations and policies.
   - `/etc/skip` and its descendants, which contains the SKIP keys and certificates.

   ---

   **Note -** These three sets of files are not removed as part of the `pkgrm` command. Therefore, you must remove these files manually, if you are done with them.

   ---

   If you do not remove these files and reinstall the software, the old configurations and rules are retained, in addition to the `Initial` policy. You may end up with unwanted duplicates. You can delete these using the Administration GUI.

   If you do not remove the old SKIP keys and certificates, when the software is reinstalled multiple Screen identities will be created. To remove the SKIP identities completely, read more about `skiplocal` and `skipdb` in the *SunScreen SKIP 1.5 User's Guide.*

APPENDIX **A**

# Using the Command Line For Installing SunScreen EFS 3.0

This Appendix contains procedures for installing using the command line. These procedures can be used when installing SunScreen EFS 3.0 in:

- Routing mode with remote administration.
- Stealth mode.

Command line installation is provided as an alternative to using the installation wizard. Command line installation is intended for expert system administrators.

Before installing, review the *SunScreen EFS 3.0 Release Notes* for the latest information about this product.

## ▼ To Install the Software on the Administration Station Using the Command LineTo Install the Software on the Administration Station Using the Command Line

This procedure requires the use of `pkgadd`.

**1. Open a terminal window on the Administration Station and become root.**

**Caution -** Ensure that the OpenWindows File Manager is not running because it interferes with the operation of the `volcheck` command used for installation.

2. **Insert the SunScreen EFS 3.0 CD-ROM into the Administration Station's CD-ROM drive.**

3. **Mount the CD-ROM by typing:**

```
# volcheck
```

4. **Add the software by typing:**

```
For SPARC systems:
# pkgadd -d /cdrom/cdrom0/sparc

For x86 systems:
# pkgadd -d /cdrom/cdrom0/i386
```

For SPARC systems, you are prompted with a menu of packages to install:

```
The following packages are available:
1  SUNWbdc       SKIP Bulk Data Crypt  1.5 Software
                   (sparc) 1.5
  2  SUNWbdcx      SKIP Bulk Data Crypt (64-bit) 1.5 Software
                   (sparc) 1.5
  3  SUNWdthj      HotJava Browser for Solaris
                   (sparc) 1.1.5,REV=1998.12.03
  4  SUNWes        SKIP End System  1.5 Software
                   (sparc) 1.5
  5  SUNWesx       SKIP End System (64-bit) 1.5 Software
                   (sparc) 1.5
  6  SUNWfwcnv     SunScreen Firewall conversion
                   (sparc) 3.0
  7  SUNWhttp      Sun WebServer daemon and supporting binaries
                   (sparc) 2.0
  8  SUNWicgSA     SunScreen Administration Software
                   (sparc) 3.0
  9  SUNWicgSD     SunScreen online documentation
                   (sparc) 3.0
 10  SUNWicgSM     SunScreen man pages
                   (sparc) 3.0

... 7 more menu choices to follow;
<RETURN> for more choices, <CTRL-D> to stop display:


 11  SUNWicgSS     SunScreen Firewall
                   (sparc) 3.0
```

**(continued)**

**(Continuation)**

```
 12  SUNWkeymg     SKIP Key Manager Tools 1.5 Software
                   (sparc) 1.5
 13  SUNWkisup     SKIP I-Support module 1.5 Software
                   (sparc) 1.5
 14  SUNWrc2       SKIP RC2 Crypto Module
                   (sparc) 1.5
 15  SUNWrc4       SKIP RC4 Crypto Module  1.5 Software
                   (sparc) 1.5
 16  SUNWrc4x      SKIP RC4 Crypto Module (64-bit) 1.5 Software
                   (sparc) 1.5
 17  SUNWsman      SKIP Man Pages 1.5 Software
                   (sparc) 1.5

Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:
```

For x86 systems, you are prompted with a menu of packages to install:

```
The following packages are available:
1  SUNWbdc       SKIP Bulk Data Crypt  1.5 Software
                   (i386) 1.5
  2  SUNWdthj      HotJava Browser for Solaris
                   (i386) 1.1.5,REV=1998.12.03
  3  SUNWes        SKIP End System  1.5 Software
                   (i386) 1.5
  4  SUNWfwcnv     SunScreen Firewall conversion
                   (i386) 3.0
  5  SUNWhttp      Sun WebServer daemon and supporting binaries
                   (i386) 2.0
  6  SUNWicgSA     SunScreen Administration Software
                   (i386) 3.0
  7  SUNWicgSD     SunScreen online documentation
                   (i386) 3.0
  8  SUNWicgSM     SunScreen man pages
                   (i386) 3.0
  9  SUNWicgSS     SunScreen Firewall
                   (i386) 3.0
 10  SUNWkeymg     SKIP Key Manager Tools 1.5 Software
                   (i386) 1.5

... 4 more menu choices to follow;
<RETURN> for more choices, <CTRL-D> to stop display:


 11  SUNWkisup     SKIP I-Support module 1.5 Software
                   (i386) 1.5
 12  SUNWrc2       SKIP RC2 Crypto Module
                   (i386) 1.5
 13  SUNWrc4       SKIP RC4 Crypto Module  1.5 Software
```

**(continued)**

```
                  (i386) 1.5
 14  SUNWsman     SKIP Man Pages 1.5 Software
                  (i386) 1.5

Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:
```

1. **For SPARC systems, enter: 1-5, 8, 10, 12-17 For x86 systems, enter: 1-3, 6, 8, 10-14**

2. **Follow the program prompts, answering all the questions with** `y`**.**
   When completed, you return to the same menu of packages.

3. **Enter** `q` **to quit** `pkgadd`**.**

4. **Set the** `PATH` **and** `MANPATH` **by editing your shell initialization file (such as** `.profile` **or** `.login` **file).**
   a. **Set the** `PATH` **for the Bourne shell by typing:**
      ```
      PATH=/opt/SUNWicg/SunScreen/bin:$PATH
      PATH=/usr/dt/bin:$PATH
      export PATH
      ```
   b. **Set the** `MANPATH` **for the Bourne shell by typing:**
      ```
      MANPATH=$MANPATH:/opt/SUNWicg/SunScreen/man
      export MANPATH
      ```

5. **Eject the CD-ROM from the CD-ROM drive by typing**

```
# eject cdrom0
```

:

6. **Install any SKIP upgrades (Export Controlled [1024–bit] or U.S. and Canada Use Only [2048–bit] keys) as instructed in the documentation that is included with the upgrade SKIP CD-ROM.**

7. **Reboot by typing:**

```
# sync; init 6
```

The software packages have been installed. You continue the installation process on the machine that is the Administration Station.

# Installing Certificates on the Administration Station

To obtain encrypted communication between the Administration Station and the Screen, certificates must be installed on both machines. This can be done by either using self-generated certificates or by installing issued certificates. Both methods are done on the Administration Station.

## ▼ Option 1: To Create a Self-Generated Certificate on the Administration StationOption 1: To Create a Self-Generated Certificate on the Administration Station

1. **Open a terminal window and create the required SKIP directories by typing:**

```
# skiplocal -i
```

2. **Create the self-generated certificate on the Administration Station by typing:**

```
# skiplocal -k -f -V
```

   The local certificate ID appears. It is the Administration Station's 32-character certificate ID (MKID).

3. **Write down the certificate ID, which begins with 'Ox'.**

4. **Add SKIP to all the interfaces by typing:**

```
# skipif -a
```

5. **Reboot to complete the installation by typing:**

```
# sync; init 6
```

The Administration Station's certificate ID has been generated. You next move to the Screen to install the SunScreen software.

## ▼ Option 2: To Install the Issued Certificate on the Administration Station Using Command LineOption 2: To Install the Issued Certificate on the Administration Station Using Command Line

To do this procedure, you will need the Key and Certificate floppy diskette.

1. **Open a terminal window on the Administration Station and become root.**

**Caution -** Ensure that the OpenWindows File Manager is not running because it interferes with the operation of the `volcheck` command used for installation.

2. **Create the required SKIP directories by typing:**

```
# skiplocal -i
```

3. **Insert the Key and Certificate diskette into the Administration Station's floppy drive.**

4. **Mount the CD-ROM by typing:**

```
# volcheck
```

5. **Install the SKIP keys by typing:**

```
# install_skip_keys -icg /floppy/floppy0
```

6. **Start the SKIP daemon by typing:**

```
# skipd_restart
```

7. **Eject the Key and Certificate floppy diskette by typing:**

```
# eject floppy0
```

8. **Write down the certificate ID, which is eight characters long.**

9. **Add SKIP to all the interfaces by entering:**

```
# skipif -a
```

10. **Reboot to complete the installation by entering:**

```
# sync; init 6
```

The Administration Station's certificate ID has been installed. You next move to the Screen to install the SunScreen software.

# Installing on the Screen Via The Command Line

You can install the required SunScreen EFS packages on the Screen by:

1. Using `pkgadd` to install the software packages from the SunScreen EFS CD-ROM.
2. Reboot.
3. Run `ss_install` on the Screen.

4. Reboot.

## ▼ To Install The Software on the Screen Using the Command LineTo Install The Software on the Screen Using the Command Line

**1. Open a terminal window on the Screen and become root.**

**Caution -** Ensure that the OpenWindows File Manager is not running because it interferes with the operation of the `volcheck` command used for installation.

**2. Insert the SunScreen EFS 3.0 CD-ROM into the Screen's CD-ROM drive.**

**3. Mount the CD-ROM by typing:**

```
# volcheck
```

**4. Add the software by typing:**

```
For SPARC systems:
# pkgadd -d /cdrom/cdrom0/sparc

For x86 systems:
# pkgadd -d /cdrom/cdrom0/i386
```

For SPARC systems, you are prompted with a menu of packages to install:

```
The following packages are available:
1  SUNWbdc       SKIP Bulk Data Crypt  1.5 Software
                   (sparc) 1.5
  2  SUNWbdcx      SKIP Bulk Data Crypt (64-bit) 1.5 Software
                   (sparc) 1.5
  3  SUNWdthj      HotJava Browser for Solaris
                   (sparc) 1.1.5,REV=1998.12.03
  4  SUNWes        SKIP End System  1.5 Software
                   (sparc) 1.5
  5  SUNWesx       SKIP End System (64-bit) 1.5 Software
                   (sparc) 1.5
  6  SUNWfwcnv     SunScreen Firewall conversion
```

**(continued)**

**(Continuation)**

```
                  (sparc) 3.0
  7  SUNWhttp      Sun WebServer daemon and supporting binaries
                  (sparc) 2.0
  8  SUNWicgSA     SunScreen Administration Software
                  (sparc) 3.0
  9  SUNWicgSD     SunScreen online documentation
                  (sparc) 3.0
 10  SUNWicgSM     SunScreen man pages
                  (sparc) 3.0

... 7 more menu choices to follow;
<RETURN> for more choices, <CTRL-D> to stop display:


 11  SUNWicgSS     SunScreen Firewall
                  (sparc) 3.0
 12  SUNWkeymg     SKIP Key Manager Tools 1.5 Software
                  (sparc) 1.5
 13  SUNWkisup     SKIP I-Support module 1.5 Software
                  (sparc) 1.5
 14  SUNWrc2       SKIP RC2 Crypto Module
                  (sparc) 1.5
 15  SUNWrc4       SKIP RC4 Crypto Module  1.5 Software
                  (sparc) 1.5
 16  SUNWrc4x      SKIP RC4 Crypto Module (64-bit) 1.5 Software
                  (sparc) 1.5
 17  SUNWsman      SKIP Man Pages 1.5 Software
                  (sparc) 1.5

Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:
```

For x86 systems, you are prompted with a menu of packages to install:

```
The following packages are available:
1  SUNWbdc       SKIP Bulk Data Crypt  1.5 Software
                   (i386) 1.5
  2  SUNWdthj      HotJava Browser for Solaris
                   (i386) 1.1.5,REV=1998.12.03
  3  SUNWes        SKIP End System  1.5 Software
                   (i386) 1.5
  4  SUNWfwcnv     SunScreen Firewall conversion
                   (i386) 3.0
  5  SUNWhttp      Sun WebServer daemon and supporting binaries
                   (i386) 2.0
  6  SUNWicgSA     SunScreen Administration Software
                   (i386) 3.0
  7  SUNWicgSD     SunScreen online documentation
                   (i386) 3.0
```

**(continued)**

**(Continuation)**

```
  8  SUNWicgSM     SunScreen man pages
                   (i386) 3.0
  9  SUNWicgSS     SunScreen Firewall
                   (i386) 3.0
 10  SUNWkeymg     SKIP Key Manager Tools 1.5 Software
                   (i386) 1.5

... 4 more menu choices to follow;
<RETURN> for more choices, <CTRL-D> to stop display:


 11  SUNWkisup     SKIP I-Support module 1.5 Software
                   (i386) 1.5
 12  SUNWrc2       SKIP RC2 Crypto Module
                   (i386) 1.5
 13  SUNWrc4       SKIP RC4 Crypto Module  1.5 Software
                   (i386) 1.5
 14  SUNWsman      SKIP Man Pages 1.5 Software
                   (i386) 1.5

Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:
```

1. **For SPARC systems, enter: 1-2, 7-16 For x86 systems, enter: 1, 5-13**

2. **Follow the program prompts, answering all the questions with y.**
   When completed, you return to the same menu of packages.

3. **Enter q to quit** `pkgadd`**.**

4. **Set the** `PATH` **and** `MANPATH` **by editing your shell initialization file (such as** `.profile` **or** `.login` **file).**
   a. **Set the** `PATH` **for the Bourne shell by typing:**
   ```
   PATH=/opt/SUNWicg/SunScreen/bin:$PATH
   PATH=/usr/dt/bin:$PATH
   export PATH
   ```
   b. **Set the** `MANPATH` **for the Bourne shell by typing:**
   ```
   MANPATH=$MANPATH:/opt/SUNWicg/SunScreen/man
   export MANPATH
   ```

5. **Eject the CD-ROM from the CD-ROM drive by typing**

```
# eject cdrom0
```

6. **Install any SKIP upgrades (Export Controlled [1024–bit] or U.S. and Canada Use Only [2048–bit] keys) as instructed in the documentation that is included with the upgrade SKIP CD-ROM.**

7. **Reboot by typing**:

```
# sync; init 6
```

8. **Open a terminal window and become root, if not already.**

9. **Complete installation by typing**:

```
# ss_install
```

Answer the questions that appear. The questions and text are similar to the panels that appear when installing using the installation wizard. Review the procedures for installing the software on the Screen in Chapter 4 or 5 if more detail is needed.

If you are using issued certificates, you need your all your certificate diskettes.

---

**Note -** The SKIP command to run on the Administration Station is displayed at the end. It is contained in the `AdminSetup.readme` file, found in the directory `/etc/opt/SUNWicg/SunScreen`. Write this command down for use in the following procedure.

---

---

**Tip -** If you trust that the network between the Screen and the Administration Station is secure, you can ftp the `AdminSetup.readme` file from the Screen to the Administration Station. This saves you the task of writing down the information which is required in the next procedure.

---

10. **Reboot by typing**:

```
# sync; init 6
```

## ▼ To Use Command-Line SKIP on the Administration StationTo Use Command-Line SKIP on the Administration Station

1. **On the Administration Station, open a terminal window and become root.**

2. **To enable unencrypted communication from the Administration Station to all hosts other than the Screen, type:**

```
# skiphost -a default
```

3. **Add a rule so that encrypted communication is possible between the Administration Station and the Screen by typing:**

```
# skiphost command_from_ss_install
```

This command is in the `AdminSetup.readme` file. The command is in the following form, which has been divided into lines for readability:

skiphost -a *name_of_Screen* -r *NSID_type*

-R *Screen's_certificate_ID* -s *NSID_type*

-S *Administration_Station's_certificate_ID*

-k *key_encryption_algorithm*

-t *data_encryption_algorithm* -m *MAC_algorithm*

1. **Turn on SKIP by typing:**

```
If Screen has only one interface:
# skiphost -o on
If Screen has more than one interface, for each interface:
# skiphost -i name_of_interface -o on
```

**Note -** To display the interfaces, if forgotten, type `ifconfig -a`.

2. **Save the SKIP settings by typing:**

```
# skipif -i all -s
```

3. **Restart the SKIP daemon by typing:**

```
# skipd_restart
```

Refer to the *SunScreen SKIP 1.5 User's Guide* for more information on operating SKIP, if needed.

**Note -** After configuring SKIP, check that the encryption parameters and 32-character certificate ID (MKID) values match on both the Administration Station and the Screen.

1. **To configure and manage your SunScreen from your Administration Station, run a Java-enabled Web browser compliant with JDK 1.1.3 or later, and launch the Administration GUI by typing the following URL:**

```
http://Name_of_Screen:3852/
```

.

See the *SunScreen EFS 3.0 Administration Guide* for instructions on how to use the Administration GUI.

APPENDIX **B**

# Upgrading Crypto Modules

Use the following table when you want to add additional Crypto modules to your SKIP configuration. For example, SunScreen EFS 3.0 ships with the Global version of SKIP, which only contains the RC2 and RC4(x) Crypto modules. To add additional modules, for example DES, you must take some care to install only the packages you need.

**Note -** The End System SKIP modules (`SUNWes` and `SUNWesx`) should not be added to a SunScreen EFS 3.0 Screen.

When upgrading from SKIP Crypto Global version, add the following packages:

| **Add these packages to upgrade to the Export Controlled version...** | **Add these packages to upgrade to the Domestic version...** |
|---|---|
| `SUNWkusup`SKIP U-Support module | `SUNWkdsup`SKIP D-Support module |
| `SUNWdes` SKIP DES Crypto Module | `SUNWdes`SKIP DES Crypto Module |
| `SUNWdesx` SKIP DES Crypto Module (64-bit in SPARC only) | `SUNWdesx`SKIP DES Crypto Module (64-bit in SPARC only) |
| | SUNW3des SKIP 3DES Crypto Module |
| | SUNW3desx SKIP 3DES Crypto Module (64-bit in SPARC only) |
| | SUNWrc4s SKIP RC4-128 Crypto Module |
| | SUNWrc4sx SKIP RC4-128 Crypto Module (64-bit in SPARC only) |

| Add these packages to upgrade to the Export Controlled version... | Add these packages to upgrade to the Domestic version... |
|---|---|
| | SUNWsafe SKIP SAFER Crypto Module<br><br>SUNWsafex SKIP SAFER Crypto Module (64-bit in SPARC only) |