SEAM 1.0.1 Installation and Release Notes

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303-4900
U.S.A.

Part Number 806-4088–10
February 2000

Copyright 2000 Sun Microsystems, Inc. 901 San Antonio Road, Palo Alto, California 94303-4900 U.S.A. All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, docs.sun.com, AnswerBook, AnswerBook2, NFS, and Solaris are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc. Portions of the software copyright 1996 by the Massachusetts Institute of Technology. All rights reserved.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227–14(g)(2)(6/87) and FAR 52.227–19(6/87), or DFAR 252.227–7015(b)(6/95) and DFAR 227.7202–3(a).

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2000 Sun Microsystems, Inc. 901 San Antonio Road, Palo Alto, Californie 94303-4900 Etats-Unis. Tous droits réservés.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées du système Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, docs.sun.com, AnswerBook, AnswerBook2, NFS, et Solaris sont des marques de fabrique ou des marques déposées, ou marques de service, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.Copyright 1996 des portions du logiciel par Massachusetts Institute of Technology. Tous droits réservés.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REPONDRE A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.

Contents

1. SEAM 1.0.1 Product Overview 5

Introduction 5

Release Contents 5

SEAM 1.0.1 Product Dependencies 6

Status 6

SEAM Interoperability 6

SEAM Interoperability with MIT 6

SEAM Interoperability with NT 7

Known Bugs 7

2. SEAM Installation 13

SEAM Package Contents 13

SEAM Client Packages 13

Slave KDC Packages 14

Master KDC Packages 14

Patches 14

SEAM Installation Task Map 14

Installing SEAM Software 15

▼ How to Copy the SEAM Image to a Local File System 16

▼ How to Mount a Writable File System on the Admin Pack CD 18

▼ How to Preconfigure SEAM Installations 19

▼ How to Install SEAM Software Using the GUI 23

▼ How to Install SEAM Clients Without the GUI 26

▼ How to Fix an Unconfigured System 26

Uninstalling SEAM 27

Additions to the Solaris Management Console 27

CHAPTER 1

SEAM 1.0.1 Product Overview

This chapter provides a general overview of the Sun™ Enterprise Authentication Mechanism (SEAM) 1.0.1 product. The following topics are covered:

- "Release Contents" on page 5
- "SEAM 1.0.1 Product Dependencies" on page 6
- "Status" on page 6
- "Known Bugs" on page 7

Introduction

The SEAM 1.0.1 release is designed to improve system security by supporting Kerberos V5 authentication, privacy, and integrity. Security should also be improved by allowing single network sign-on when using the kerberized login mechanisms and by providing kerberized NFS™ services.

Release Contents

This release includes the following:

- Key distribution center (KDC)
- KDC services
  - `kadmind` and `krb5kdc`

- KDC administration utilities
  - `kadmin`, `kadmin.local`, and `gkadmin`
  - `kpropd`
- Kerberized utilities and daemons
  - `ftp`, `rcp`, `rlogin`, `rsh`, and `telnet`
  - `ftpd`, `rlogind`, `rshd`, and `telnetd`
- Documentation including:
  - *Sun Enterprise Authentication Mechanism 1.0.1 Guide*
  - *SEAM Installation and Release Notes* (this document)
  - Man pages

SEAM 1.0.1 Product Dependencies

The Solaris 8 release must be installed for this product to function. XFN and JDK™ 1.1 must also be installed.

Status

SEAM is an evolving specification and is subject to change.

SEAM Interoperability

SEAM interoperability has been tested against both MIT Kerberos V5 1.0 and NT 5.0 installations.

SEAM Interoperability with MIT

SEAM interoperates with an MIT installation with the following caveats:

1. gkadmin and kadmin do not work against MIT KDCs. The reason for this failure is that gkadmin and kadmin use the RPCSEC_GSS protocol to secure the connection to the KDC. The MIT Kerberos V5 1.0 installation uses a non-standard AUTH_GSSAPI protocol to provide security. Because these two protocols are different, you cannot use gkadmin and kadmin with an MIT KDC.
2. SEAM does not include the ksu command. Instead, PAM is used to let su do most of what ksu does. One area that is different is that ksu looks at the .k5login file to see if the user using su is allowed to do so without a password, if he has Kerberos V5 credentials. This check is not done in SEAM.
3. SEAM and MIT Kerberos V5 code are not intended to co-exist on the same host. While this is theoretically possible, it is not supported.
4. SEAM requires that rpcbind be run. This is not a requirement of the MIT Kerberos V5 installation.

SEAM Interoperability with NT

Information about SEAM interoperability with NT can be found at: http://www.connectathon.org/seam1.0. This site contains up-to-date information about the results of the testing and procedures that can be used to allow SEAM to interoperate with NT.

Known Bugs

This is a list of the known bugs in SEAM 1.0. Each item includes the bug number and bug synopsis, as well as a short description of the bug.

4143644: Kerberized rsh -f did not work correctly

If the user explicitly asks for forwardable credentials, rsh should fail if there are no forwardable credentials.

4159036: "telnet> encrypt enable DES_OFB64" hung the session

The encryption type DES_OFB64 cannot be used for data encryption in telnet. The only encryption that can be used is DES_CFB64, which is also the default encryption type.

4159419: gkadmin should try to consult policy if possible when generating random passwords

When a user uses gkadmin to generate a random password for a principal, the tool should try to consult the policy being applied to decide the number of characters and character classes to be used. This will result in the first generated password being accepted by the kadmin API, in most cases.

4170403: Kerberized rlogin in cross-realm does not fail with incorrect password

When Kerberized `rlogin` is enabled in `inetd.conf` and not enabled in `pam.conf` (on a host running an `rlogin` server), a user is authenticated correctly using Kerberos V5 when using `rlogin` between realms. However, if the user is prompted for a password, any password is accepted. This is not a security hole, since the user has been authenticated using Kerberos V5. Avoid disabling kerberized `rlogin` in `pam.conf` if enabling it in `inetd.conf`.

4172240: when -r option is used to telnet, telnet reports escape character as ^]

The escape character is ~, as described in the man page.

4177603: kprop command returns "Broken Pipe" when kpropd.acl is missing entry for master

If `/etc/krb5/kpropd.acl` is not set up properly on a slave KDC, the `kprop` command on the client fails with "Broken Pipe."

4178210: gkadmin: when the ticket expires it should return to login window for re-authentication

When the credential of the admin who is currently logged in `gkadmin` is expired, it would be nice if `gkadmin` would pop up the message saying the "Ticket/ credential is expired"; then after the admin clicks on the "OK" button, `gkadmin` should close the current "SEAM Administration Tools" window and return the admin user to the "SEAM Administration Login" window with the prompt active on the "Password:" field to imply that the admin user needs to enter password for re-authentication.

4179331: gkadmin: Can not change the Principal/Policy name

`gkadmin` does not support the ability to change a principal's name or policy. To achieve the same effect, the principal or policy should be copied to the new name using the "Duplicate" button, then the old one should be deleted.

4184145: gkadmin: Some GUI items inside Properties window are missing some edges

The "..." button of "List Cache Timeout" is missing the right side. Also, after selecting "Show List" or "Cache Lists Forever", the hghlighted rectangle that surrounds these selectable buttons is missing the LEFT edge.

4188923: gkadmin: some minor problems with SEAM Print Helper

The SEAM Print Helper can display data entered before hitting "Cancel." Cancel should discard changes and restore whatever was there prior to that. Also, the text field of File Name in the SEAM Print Helper window does not clear properly.

4188935: gkadmin: Dismiss button does not work correctly on some Help windows

When xhosting the SEAM GUI Administration tool, the Dismiss button does not work correctly on some Help screens.

4189590: kadmin and gkadmin should print alternate string when lifetimes are 2^31-1

When the user creates a new principal wanting ticket lifetimes to be set on the KDC side, the values 2147483647 = 2^31-1 gets stored in the principal database. When viewing a principal, the CLI and GUI should not display the value 2147483647 (GUI) or 24855 days 03:14:07 (CLI) but instead show a more user friendly string. This sort of check is already being done in the case when the date 0 is printed out as "Never."

4189642: garbage in the kerberized rsh usage message

`rsh`, `rlogin`, and `rcp` print out the option string for illegal options. They should print out the program name.

4191906: The time on the warning msg when the credential is expired is misleading

If the initial ticket expiration is less than the warning threshold in `/etc/krb5/warn.conf`, then the warning message that is sent out says that the ticket will expire within the time specified in `warn.conf` file and not the ticket expiration time.

4191933: service tickets do not get stored in ticket cache when kinit is used with a lifetime of less than 30 minutes

When a user acquires credentials (a ticket granting ticket) using `kinit -l` with a lifetime of less than 30 minutes, any service tickets derived from the credential do not show up in the ticket cache. The reason is that after a renewable credential has less than 30 minutes of lifetime, SEAM attempts to automatically renew the credential to maximize ease of use. Renewing a credential causes the previous credential and service tickets derived therein to be removed. There is no other impact, because any session created using the old service ticket lasts for the ticket lifetime. Do not invoke `kinit` with a `-l` option specifying a ticket lifetime of less than 30 minutes.

4193608: kinit -s has some issues

A user cannot use `kinit` to acquire a postdated ticket with a start time more than 19 days from today's date.

4193925: gkadmin: inconsistency of Enter key behavior when creating a new policy

Currently, after entering a policy name in the "Policy Details" panel with the default parameter values, hitting the Enter (Return) key does not automatically create the policy. Enter/Return key should have equivalent action as clicking the Done button.

`4194001: gkadmin: "Last Changed By:" field does not display the full name`

The “Last Changed By” field does not display the instance name so admin principals are not properly identified.

`4206443: Document the lifetime and renewable lifetime negotiation in kinit man page`

When a user specifies lifetime in the command line, the actual lifetime of the ticket obtained is the minimum of the following:

- Value specified in the command line
- Value specified in the KDC configuration file
- Value specified in the Kerberos data base for the server principal; in the case of `kinit` it is `krbtgt/`*<realmname>*.
- Value specified in the Kerberos database for the user principal

`4210970: gkadmin: Date/Time Helper doesn’t change Feb 29 to Feb 28 if year is changed`

Changing the year on the Date/Time Helper does not recalculate the maximum allowable date for that month.

`4211978: gkadmin: Password Expires: field displayed misleading info`

When `gkadmin` is used to change the password, the password expiration time changes, because it gets the expiration time from a policy assigned to the principal. The GUI does not make it obvious that the expiration time is coming from a policy. The effect on password expiration is true, regardless whether the password is changed with `kadmin`, `kadmin.local`, `gkadmin`, `kpasswd`, or `passwd`.

The users need to be aware that a there are two choices every time they change the password: either empty out the password expiration field to make the server fill it in by consulting the policy, or leave the field with a date in it to set the expiration date explicitly.

`4218214: gkadmin: "Return" key doesn’t work on highlighted GUI buttons`

While mouse-clicking worked on GUI buttons, unfortunately pressing the "Enter" or "Return" key on the highlighted button does not work.

4220042: "kadmin: add_principal -expire "1/1/2000 7:00am" xhu" doesn't work

The -expire option to the add_principal command of kadmin does not work when an a.m. time is specified. For example:

```
kadmin: add_principal -expire "9/1/1999 7:00am" xhu
Invalid date specification "9/1/1999 7:00am".
```

Using "pm" works. To get an a.m. time do not include "am" in the time specification for times before noon. The way to add this principal is:

```
kadmin: add_principal -expire "9/1/1999 7:00"
```

4245090: document how to add principals when not using DNS

The procedures in the SEAM documentation was written, based on using DNS, so all of the host and service principals use fully-qualified domain names. If you are not using DNS, then do not include the domain name when creating principals. As an example, kdc1.acme.com would be kdc1.

4245982: error response for "mdtm" not consistent with other non-supported ftp commands

Attempting to use the unsupported mdtm subcommand prints a different error message than the also-unsupported size command, and the error is printed twice.

4247366: kdb5_util create command does not work correctly with -r option specified

The kdb5_util create command does not handle the -r [*realm*] argument correctly, so /etc/krb5/krb5.conf must be configured for the desired realm before the Kerberos database is created.

4248395: gkadmin: auto wrap feature is not fit for Japanese language.

The gkadmin context-sensitive help breaks lines in a way that is incorrect for Japanese locales, resulting in ragged lines.

4249206: date parser has some i18n problems

Some date parsing strings are not correctly internationalized, leading to different behavior in non-English locales. Also, some assumptions are made about abbreviations and prefixes which are not correct in non-English locales. The parser may assume an abbreviation even when one is not used. This bug is related to 4220042.

`4250805: SEAM, l10n_euro, i18n, Admin tool, entry box does not accept extended chars`

A policy name which contains extended 8-bit characters is rejected when entered into gkadmin. Use 7–bit policy names.

`4258360: SEAM is not able to display certain localized messages`

Several error messages were found to be not localizable in system test; these messages display in English despite the availability of a translation.

`4260991: inconsistent error message from rcp command`

The Kerberos-enabled `rcp` command produces a different and more confusing error message than the regular `rcp` in the Solaris 8 release, when it does not have write permission to a target file.

`4284200: SEAM uninstall leaves configuration files behind`

Uninstalling SEAM leaves configuration files in place without asking the user if this is the desired result. You might need to edit `/etc/pam.conf`, `/etc/krb5/warn.conf`, `/etc/krb5/krb5.conf`, and `/etc/inet/inetd.conf` to complete the uninstall process.

`4291596: Kerberized ftpd does not support PAM`

The SEAM `ftpd` does not support the PAM framework like the Solaris version does.

CHAPTER 2

SEAM Installation

This chapter includes the steps necessary to install the SEAM product and should be used by anyone doing an installation. The procedures to preconfigure and install SEAM are included in this chapter. The first procedure allows for the preconfiguration of much of the site-specific data so that files need not be manually edited as part of the install process; it also includes a local installation. The second procedure actually adds all of the SEAM software using the preconfiguration information.

These topics are covered in this chapter:

- "SEAM Package Contents" on page 13
- "Installing SEAM Software" on page 15
- "Uninstalling SEAM" on page 27

SEAM Package Contents

The SEAM software can be installed on either a client, a KDC slave server, or a KDC master server. Any other types of servers (such as a SEAM application or SEAM NFS server) are configured after the client software packages are installed. Each type of installation adds one or more packages, some of which change files that are important to system security.

SEAM Client Packages

The client packages install the SEAM man pages, the administrative applications (`kadmin` and `gkadmin`), as well as the kerberized daemons and utilities (`ftp` and `ftpd`, for example). During the install process the following files are edited: `/etc/`

`inetd.conf`, `/etc/services`, `/etc/pam.conf`, and `/etc/krb5/krb5.conf`. If you have site-specific alterations to these files, you should check the file contents after the installation.

Slave KDC Packages

The slave KDC installation process installs all of the client packages, as well as an additional package that includes the utilities needed by any KDC server. A start-up script is installed in `/etc/init.d/kdc`, which starts the slave KDC daemons. Also, the `/etc/krb5/kdc.conf` and `/etc/inetd.conf` files are edited.

Master KDC Packages

The master KDC installation process installs all of the client packages, the slave KDC package, and a package that includes the files and utilities needed only on the master KDC server. The process edits the crontab file for `root` and installs a start-up script in `/etc/init.d/kdc.master`. A file to control access to the KDC, `/etc/krb5/kadm5.acl`, and a file to control the propagation of the KDC database, `/etc/krb5/kpropd.acl`, are added. Securing these files is important for the security of the KDC database.

Patches

The SEAM 1.0 release included many patches which fixed the Solaris 2.6 or Solaris 7 releases. There are no patches for the SEAM 1.0.1 release.

SEAM Installation Task Map

To best utilize SEAM, the product installation should be done in a specific order. You can alter this order if you need to, but some steps might have to be repeated or you might need to make manual changes to the configuration files.

TABLE 2–1 First Steps: SEAM Configuration Order

Task	Description	For Instructions, Go To ...
1. Plan for your SEAM Installation	Consider configuration issues and make decisions about them before starting the software installation process.	"Planning for SEAM" in *Sun Enterprise Authentication Mechanism 1.0.1 Guide*
2. (Optional) Install NTP	In order for SEAM to work properly, the clocks on all systems in the realm must be kept in sync.	"Synchronizing Clocks between KDCs and SEAM Clients" in *Sun Enterprise Authentication Mechanism 1.0.1 Guide*
3. (Optional) Run SEAM preconfiguration procedure	To make the installation of a site with many hosts easier, the procedure can be run to store much of the installation information on an NFS server. This information can then be used during installation.	"How to Preconfigure SEAM Installations" on page 19
4. Run SEAM software installation procedure	To install the SEAM software packages on a client or a server	"How to Install SEAM Software Using the GUI" on page 23
5. Configure the master KDC server	Steps to configure and build the master KDC server and database for a realm.	"Configuring KDC Servers" in *Sun Enterprise Authentication Mechanism 1.0.1 Guide*
6. Additional steps to configure SEAM	Steps to configure slave KDCs, SEAM clients, SEAM NFS servers, and other useful tasks	"SEAM Configuration Task Map" in *Sun Enterprise Authentication Mechanism 1.0.1 Guide*

Installing SEAM Software

The installation process is best done using the following procedures. The first step is to establish a writable area to place files that are used during the configuration process. This writable file system and an image of the SEAM packages should be exportable to all systems that need SEAM installed. You can choose to either:

1. Copy the Solaris 8 Admin Pack CD to a local disk on an NFS server that can be exported — see "How to Copy the SEAM Image to a Local File System" on page 16.
2. Mount a writable file system on the CD and export both — see "How to Mount a Writable File System on the Admin Pack CD" on page 18.

After a writable area is prepared, the next step is to define needed information for the configuration files, so you don't need to enter this information manually. This is called the preconfiguration procedure. The last procedure installs the SEAM software using the preconfiguration information, if available.

The procedure to establish configuration files for the master KDC, slave KDCs, and SEAM clients is optional, but in sites with many systems, using the configuration files has many advantages.

1. The data needs to be entered only once, so the installations run faster
2. Since the configuration files are shared by all of the installations, the chances of making an error during the installation are reduced.

The tool used in this process gathers information such as the realm name, the KDC server names, and other important information, and stores it.

The next step is to install the SEAM product. Before attempting to install, you need to determine what type of system you need. The installation process allows you to select a master KDC installation, a slave KDC installation, or a SEAM client installation. The master KDC packages should only be included on the KDC master server; likewise, the slave KDC packages should only be installed on KDC slave servers (see "How to Install SEAM Software Using the GUI" on page 23).

The SEAM client packages should be installed on any host that requires SEAM. These hosts can include network application servers, NFS servers, and all clients. A simpler procedure can be used for installing the SEAM clients if the preconfiguration process has been completed (see "How to Install SEAM Clients Without the GUI" on page 26).

The last procedure in this section explains how to fix a system that had all of the software installed before the preconfiguration step was completed. This can happen when the default Solaris 8 Admin Pack installation is done without doing the preconfiguration process first. Refer to "How to Fix an Unconfigured System" on page 26 for a complete explanation.

▼ How to Copy the SEAM Image to a Local File System

If you do not want to leave the Solaris 8 Admin Pack CD mounted on a server while SEAM installations are occurring, then copying the packages from the Admin Pack CD is the best way to make the SEAM image available. The packages require about

50MB. This procedure requires that you have the Admin Pack CD available on the server.

1. **Become root on an NFS server.**

2. **Copy the SEAM image from the Admin Pack CD to a local file system.**

```
# cd /export
# mkdir SEAM
# cd /cdrom
# find .install components/Sun_Enterprise_Authentication_Mechanism -print|
        cpio -dump /export/SEAM
```

Note - The last line is split on two lines to make it readable, but should be entered as one command.

3. **Export the file system.**

   To make the configuration files available for all installations, `/export` or `/export/SEAM` needs to be NFS-mountable by all hosts.

   a. **Edit the** `/etc/dfs/dfstab` **file.**

      Add an entry for either `/export` or `/export/SEAM` if one does not exist.

```
share -f nfs -ro /export/SEAM
```

   b. **Start the NFS services.**

      If this is the first `share` command or set of `share` commands that you have initiated, the NFS daemons are probably not running. The following commands kill the daemons and restart them.

```
# /etc/init.d/nfs.server stop
# /etc/init.d/nfs.server start
```

Where to Go From Here

Now that an area has been prepared to store the configuration file, you can follow the steps in "How to Preconfigure SEAM Installations" on page 19.

▼ How to Mount a Writable File System on the Admin Pack CD

If you want to leave the Solaris 8 Admin Pack CD on a server while SEAM installations are occurring, then you need to mount a writable file system onto of the CD to provide an area for the preconfiguration information to be stored. This procedure requires that you have the Admin Pack CD available on the server.

1. **Become root on an NFS server.**

2. **Create a file system for the preconfiguration files.**

```
# cd /export
# mkdir SEAM_preconfig
```

3. **Mount the file system on the Admin Pack CD.**

```
# SEAM=/cdrom/components/Sun_Enterprise_Authentication_Mechanism/\
> .install/pkgutil/siteconfig_response
# mount -F lofs /export/SEAM_preconfig $SEAM
```

4. **Export the file system.**

   To make the configuration files available for all installations, `/export` or `/export/SEAM` needs to be NFS mountable by all hosts.

   a. **Edit the** `/etc/dfs/dfstab` **file.**

      Add an entry for `/cdrom` and for the new directory `/export/SEAM_preconfig`, if one does not exist.

```
share -f nfs -ro /cdrom
share -f nfs -ro /export/SEAM_preconfig
```

b. Start the NFS services.

If this is the first `share` command or set of `share` commands that you have initiated, the NFS daemons are probably not running. The following commands kill the daemons and restart them.

```
# /etc/init.d/nfs.server stop
# /etc/init.d/nfs.server start
```

Where to Go From Here

Now that an area has been prepared to store the configuration file, you can follow the steps in "How to Preconfigure SEAM Installations" on page 19.

▼ How to Preconfigure SEAM Installations

This procedure can be followed to preconfigure much of the information needed when configuring either the KDCs or the SEAM clients. If preconfiguration is needed, a writable file system must be available for the preconfiguration information (see "How to Copy the SEAM Image to a Local File System" on page 16 or "How to Mount a Writable File System on the Admin Pack CD" on page 18). The information stored on the NFS file system can be accessed by each host in the realm during the installation procedure. This process is optional, but should be very helpful for large sites.

Note - This procedure will install SEAM on the NFS server using the preconfiguration information, but none of the SEAM applications will work until at least a KDC master is installed.

In this procedure the following configuration parameters are used:

hardware configuration = SPARC

realm name = `ACME.COM`

DNS domain name = `acme.com`

master kdc = `kdc1.acme.com`

slave kdc = `kdc2.acme.com`

answerbook server = `denver`

online help URL = `http://denver:8888/ab2/coll.384.2/SEAM/@AB2PageView/8897`

file system holding SEAM packages = `/export/SEAM`

1. **Become root on an NFS server.**

2. **Start the install process.**

```
# cd /export/SEAM/components/Sun_Enterprise_Authentication_Mechanism
# ./installer
```

Note - If you are using the CD for package installations instead of using an NFS server, then installer is found in: /net/denver/cdrom/components/Sun_Enterprise_Authentication_Mechanism.

---

3. **Click Next in the Welcome screen.**

4. **Select the type of installation.**

   The next screen asks you to select a default installation or a custom installation. Select the custom installation to get to the preconfiguration screens. Click Next to proceed.

5. **Click Next in the Locale Selection screen.**

6. **Select the software components to be installed.**

   If the NFS server is not going to be a SEAM client or if you are just collecting preconfiguration information, then none of the components need to be selected. For a Solaris 8 NFS server that is going to provide Kerberized NFS support, the only components that should be selected are 5.8 Kernel Module and SEAM Client. Click Next to proceed.

7. **Define site configuration information.**

   The next screen allows you to select the configuration procedure as well as entering configuration information.

   a. **Select the configuration procedure.**

The top part of the screen allows you to select how the machine will be configured. For this procedure you should select "Re-configure site information." You can select to:

- Use previously configured site information — Use after the preconfiguration process has been completed
- Configure site information — Use this to enter new information
- Configure just this machine — Use to enter new information for this host
- Configure this machine later — Use when you are not sure about all of the configuration parameters, but want to install the packages anyway

b. Identify the site configuration directory.

The path should be to a file system that is mountable by all of the systems that require SEAM installations.

c. Specify the realm name.

By convention, the realm name is capitalized to help differentiate it from other domain names. For this example, the domain name is `ACME.COM`.

d. Identify the master KDC and slave KDC server names.

Use fully-qualified host names. For this example, the host names are `kdc1.acme.com` for the master and `kdc2.acme.com` for the slave. You can add as many slaves as needed.

e. Enter the DNS domain name for this realm.

f. Specify the URL for online help.

This URL is used by the SEAM Administration Tool, so the URL should be defined properly to enable the "Help Contents" menu to work. The web version of this manual can be installed on any appropriate AnswerBook2 server. You will need to change the `localhost` entry and add information after the `SEAM` portion of the address.

For this example, the URL should point to `http://denver:8888/ab2/coll.384.2/SEAM/@AB2PageView/6685`, unless another location is more appropriate. The section titled "SEAM Administration Tool" in the "Administering Principals and Policies" chapter of the *Sun Enterprise Authentication Mechanism Guide* is the suggested location to use.

You can verify the URL by entering the URL into any web browser and verifying that the page is available. Make sure that the Solaris 8 Admin Pack documentation has been installed before attempting to verify the URL.

g. Identify the maximum lifetime for tickets.

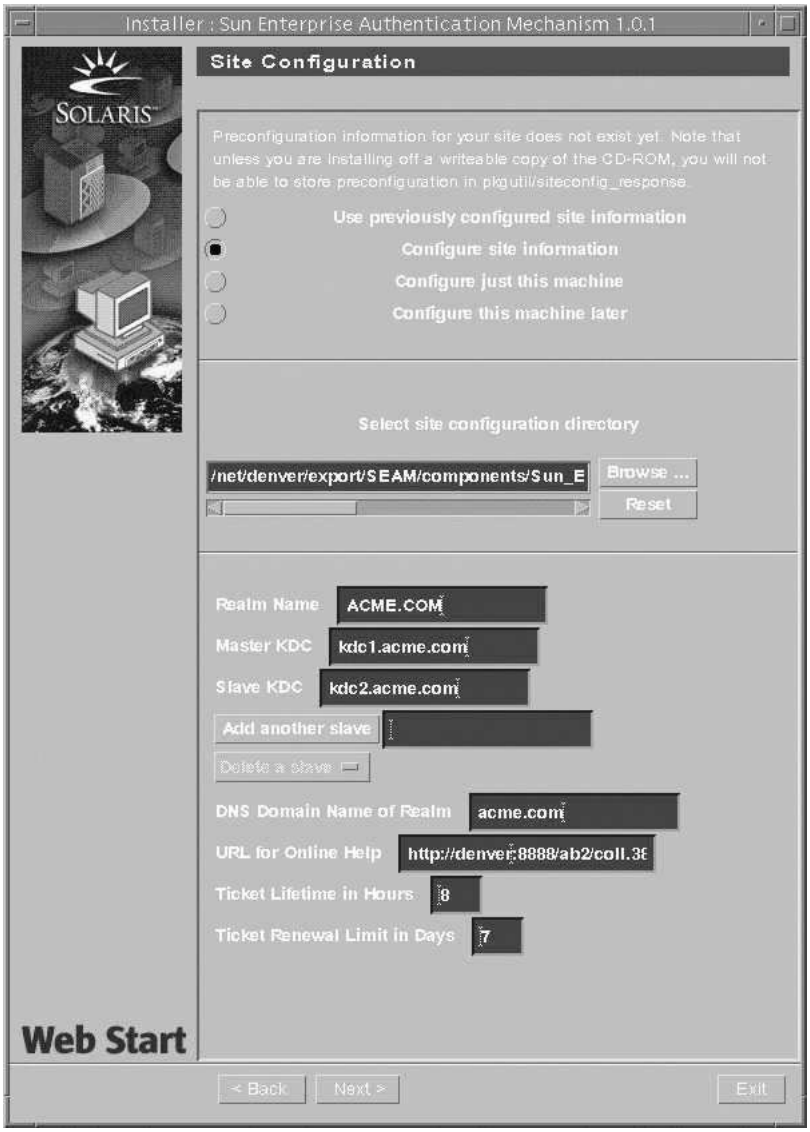
If the default value is acceptable, do not change it.

h. Identify the maximum lifetime for renewable tickets.

If the default value is acceptable, do not change it.

i. Review the definitions that you have set.

If the definitions are correct, click Next to proceed. When you click Next, the preconfiguration information is saved to the configuration directory.



Note - A disk space check is done after this step. If there is enough space then you should not have to do anything.

8. **Click Install Now to start the installation.**

   The screen will show the components selected. If there are no components selected and you are just collecting the preconfiguration information, you can click Exit.

9. **A summary of the installation process is displayed; click Next to proceed.**

10. **Additional information is displayed in the next screen; click Exit to finish the procedure.**

    A window is displayed asking if you want to reboot. Rebooting is not necessary until the server needs to use SEAM.

▼ How to Install SEAM Software Using the GUI

In this example, the SEAM master server installation is selected, but the process is much the same for the slave and client installations. The SEAM packages have been installed on `/net/denver/export/SEAM`, although they could be installed on a local file system or you can install using the Admin Pack CD.

SEAM client installations can be made faster by following the instructions in "How to Install SEAM Clients Without the GUI" on page 26.

1. **Start the installation script.**

```
# cd /net/denver/export/SEAM/components/Sun_Enterprise_Authentication_Mechanism
# ./installer
```

2. **Click Next in the Welcome screen.**

3. **Select the type of installation.**

   The next screen asks you to select a default installation or a custom installation. Select the custom installation. Click Next to proceed.

4. **Click Next in the Locale Selection screen.**

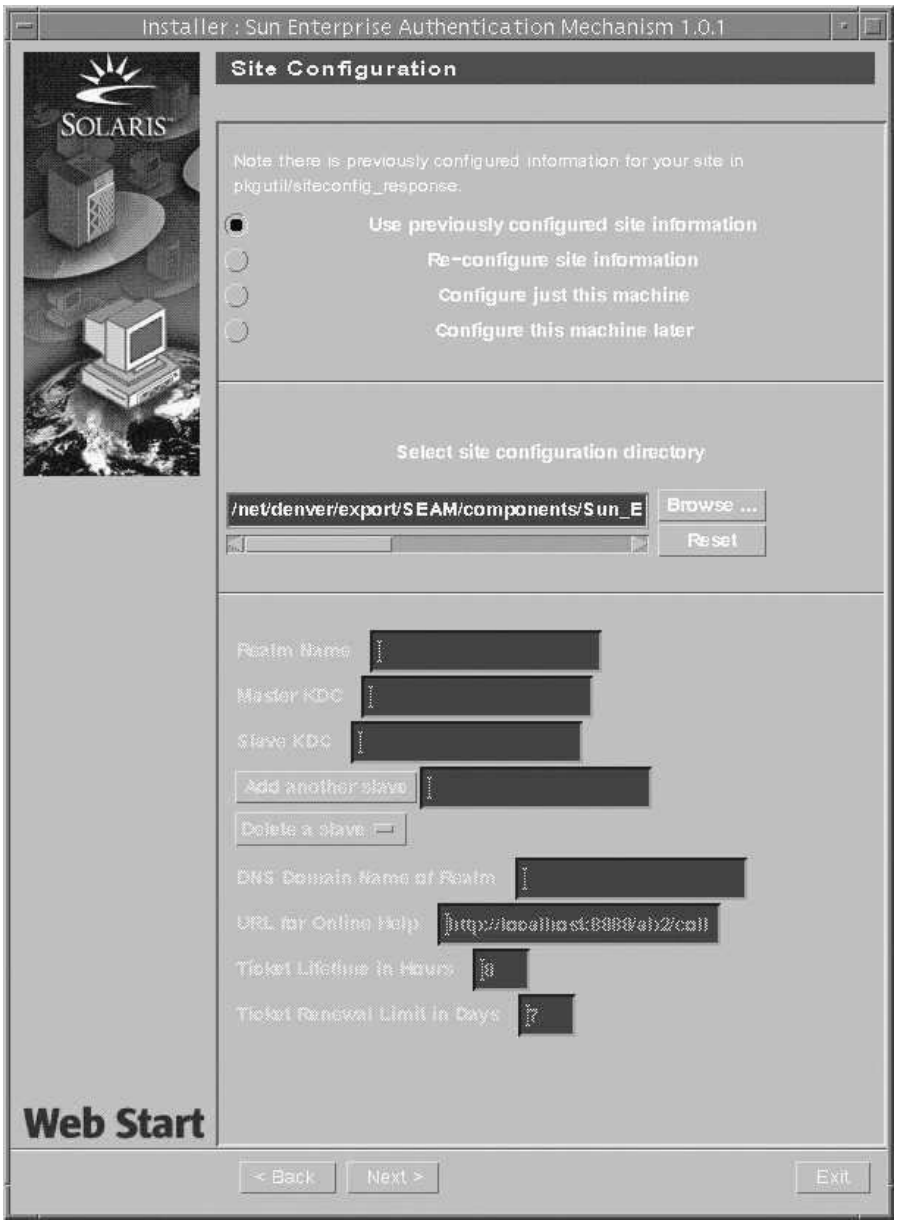
   Currently there are no locales to select in this release.

5. **Select the software components to be installed.**

   For a master, select the Master Server package. For a slave, select the Slave Server package. Other packages are added as needed. Click Next to proceed.

6. **Select the configuration procedure and directory.**

   The next screen allows you to select the configuration procedure, as well as identifying the path to the configuration files. If you have preconfigured site information, select "Use previously configured site information" and specify the directory path to the configuration files.



Note - A disk space check is done after this step. If there is enough space then you should not have to do anything.

---

7. **Click Install Now to start the installation.**

The screen will show the components selected.

8. **A summary of the installation process is displayed; click Next to proceed.**

9. **Additional information is displayed in the next screen; click Exit to finish the procedure.**

Where to Go From Here

The *Sun Enterprise Authentication Mechanism Guide* includes a list of the tasks that can be done after the SEAM software is installed.

▼ How to Install SEAM Clients Without the GUI

SEAM clients can be installed without using the GUI, after the preconfiguration process is complete. Not using the GUI means that you do not need to go through any of the screens, so the installation should run faster. Because you do not use any of the screens, you might only add client packages.

If necessary you can install all of the clients before the preconfiguration process is complete and use the script mentioned in "How to Fix an Unconfigured System" on page 26 to complete the configuration.

1. **Become `root` on the client.**

2. **Change directory to the preconfiguration area.**

```
# cd /net/denver/export/SEAM/components/Sun_Enterprise_Authentication_Mechanism
```

Note - To load packages from the CD, use the path: /net/denver/cdrom/components/Sun_Enterprise_Authentication_Mechanism.

3. **Start the installer.**

```
# ./installer -nodisplay
```

▼ How to Fix an Unconfigured System

If a full installation is done without creating the preconfiguration files first, you can correct the system using the following procedure.

1. **Become root on the system.**

2. **Run the script to fix the configuration.**

```
# cd /net/denver/export/SEAM/components/Sun_Enterprise_Authentication_Mechanism
# ./sparc/Tools/seamfixconfig
```

Note - If you are using the Solaris 8 Admin Pack CD, the path would be: /net/denver/cdrom/components/Sun_Enterprise_Authentication_Mechanism.

Uninstalling SEAM

SEAM, like other products in the Solaris 8 Admin Pack release, can be uninstalled using `prodreg`. More information about this utility can be found in "How to Uninstall a Product From the Registry" in *Solaris 8 Admin Pack Installation Guide*.

Removing the SEAM packages using `prodreg` or `pkgrm` does not make changes to several files even though these files are changed during the installation process. You might need to edit `/etc/pam.conf`, `/etc/krb5/warn.conf`, `/etc/krb5/krb5.conf`, and `/etc/inet/inetd.conf` to complete the uninstall process.

Additions to the Solaris Management Console

After SEAM has been installed, you can launch the SEAM Administration Tool from the Solaris Management Console (SMC). To start the GUI, double-click on the "security" category in the left pane of the SMC window, and double-click the SEAM icon in the right pane.