SECURE
COMPUTING

Administration Guide

SafeWord Web Access for NES

Version 1.2

Copyright notice

Trademarks

Secure Computing Corporation Software License Agreement

CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE LOADING THE SOFTWARE. BY LOADING THE SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT, AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

1. Grant of License

a. *Authorized Use.* Secure Computing grants to you, and you accept, a non-exclusive, and non-transferable license (without right to sub-license) to use the Software as defined herein.

b. *Restrictions.* You may not transfer any Software to any third party. You may not copy, translate, modify, sub-license, adapt, decompile, disassemble, or reverse engineer any Software in whole or in part except to make one copy of the Software solely for back-up or archival purposes. You agree to keep confidential and use best efforts to prevent and protect the contents of the Software from unauthorized disclosure or use.

2. Definition of Software

"Software" means collectively (i) the machine-readable object-code versions of Secure Computing's SafeWord™ client contained in the media, (ii) the published user manuals and documentation that is made available for the Software (the "Documentation"), and (iii) any updates or revisions of the Software or Documentation that you may receive. Under no circumstances will you receive any source code of the Software. Software provided for use as "backup" in the event of failure of a primary unit may be used only to replace the primary unit after a failure in fact occurs. They may not be used to provide any capability in addition to the functioning primary system that they backup.

3. Limited Software Warranty

Secure Computing warrants that the disk(s) or tape(s) on which its Software is recorded is/are free from defects in material and workmanship under normal use and service for a period of ninety (90) days from the date of shipment to you.

Secure Computing does not warrant that the functions contained in the Software will meet your requirements or that operation of the program will be uninterrupted or error-free. The Software is furnished "AS IS" and without warranty as to the performance or results you may obtain by using the Software. The entire risk as to the results and performance of the Software is assumed by you.

4. Disclaimer of Warranty And Limitation of Remedies

THE WARRANTIES STATED HEREIN ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES AND COUNTRIES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS WHICH VARY BY STATE OR COUNTRY.

SECURE COMPUTING'S AND ITS LICENSORS ENTIRE LIABILITY UNDER, FOR BREACH OF, OR ARISING OUT OF THIS AGREEMENT, IS LIMITED TO A REFUND OF THE PURCHASE PRICE OF THE PRODUCT OR SERVICE THAT GAVE RISE TO THE CLAIM. IN NO EVENT SHALL SECURE COMPUTING OR ITS LICENSORS BE LIABLE FOR YOUR COST OF PROCURING SUBSTITUTE GOODS. IN NO EVENT WILL SECURE COMPUTING OR ITS LICENSORS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL, EXEMPLARY, OR OTHER DAMAGES WHETHER OR NOT SECURE COMPUTING HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

5. Term and Termination

This license is effective until terminated. You may terminate it at any time by destroying the Software, including all computer programs and documentation, and erasing any copies residing on computer equipment. This Agreement also will automatically terminate if you do not comply with any terms or conditions of this Agreement. Upon such termination you agree to destroy the Software and erase all copies residing on computer equipment.

6. Ownership

The Software is licensed (not sold) to you. All intellectual property rights including trademarks, service marks, patents, copyrights, trade secrets and other proprietary rights in or related to the Software are and will remain the property of Secure Computing or its licensors, whether or not specifically recognized or protected under local law.

7. Export Restrictions

You agree to comply with all applicable United States export control laws and regulations, including without limitation, the laws and regulations administered by the United States Department of Commerce and the United States Department of State.

8. U.S. Government Rights

Software furnished to the U.S. Government are provided on these commercial terms and conditions as set forth in DFARS 227.7202-1(a).

9. General

Any waiver of or modification to the terms of this Agreement will not be effective unless executed in writing and signed by Secure Computing. If any provision of this Agreement is held to be unenforceable, in whole or in part, such holding shall not affect the validity of the other provisions of this Agreement. In the event of any inconsistency between this Agreement and any other related agreements between you and Secure Computing, the terms of this Agreement shall prevail.

Technical Support Information

Secure Computing works closely with our Channel Partners to offer worldwide Technical Support services. If you purchased this product through a Secure Computing Channel Partner, please contact your reseller directly for support needs.

To contact Secure Computing directly or inquire about obtaining a support contract, refer to our “Contact Secure" Web page for the latest contact information at *www.securecomputing.com*. Or if you prefer, send us an email at *support@securecomputing.com*.

Printing history

Date	Part number	Software Release
June 2000	86-0934246-A	SafeWord Web Access for IIS, Version 1.2

TABLE OF CONTENTS

Preface: About this Guide. v
Purpose of this guide v
Who should read this guide v
Using this guide vi
About printing this document vi
How this guide is organized vi
Finding additional information vii
Typographic Conventions viii

Chapter 1: SafeWord Web Access for NES. 1-1
About NES 1-1
Requirements 1-2
NES 1-2
SafeWord Web Access 1-2
SafeWord Web Access overview 1-3
Authenticating a user 1-4

Chapter 2: Installing and Configuring SafeWord Web Access 2-1
Installation overview 2-2
Installing the SafeWord Web Access plugin 2-3
Manually editing the plugin's configuration file 2-8
Configuring the obj.conf and obj.conf directives list 2-8
Form-based authentication 2-9
Advanced feature: SafeWord Web Access plugin config file (*config.data*) 2-11
File editing conventions 2-11
Config.data parameters 2-11
Advanced feature: roles 2-13
Methodology 2-13
Adding roles in the authentication server 2-14
Adding roles in SafeWord Web Access plugin config file (*config.data*) 2-19
Using roles to protect web resources (obj.conf) 2-20

Advanced feature: configure the SafeWord Web Access EASSP configuration file (*swwa.cfg*) 2-20
SafeWord authentication server 2-21
Other *swwa.cfg* configurations 2-23
The *swec.md5* file 2-24
Starting the Web server 2-25
Customizing HTML forms 2-26
Logging 2-26
Uninstalling SafeWord Web Access 2-27

Chapter 3: Custom Authentication 3-1
Out of the box 3-1
Creating your own authentication Web pages 3-2
Guidelines for customization 3-2
Using built-in authentication pages 3-3
SafeWord Web Access Web pages 3-3
HTML forms 3-4
HTML pages 3-4
Creating custom authentication pages 3-5
Adding custom login forms to SafeWord Web Access 3-5
Initiating a SafeWord authenticated session 3-6

Chapter 4: Troubleshooting 4-1
Errors during installation 4-1
Errors starting the server(s) 4-3
Verifying that SafeWord Web Access is enabled 4-3
Single sign-on server errors 4-3

PREFACE

About this Guide

Introduction

This preface introduces this guide and contains the following sections:

- "Purpose of this guide" on page v
- "Using this guide" on page vi
- "How this guide is organized" on page vi
- "Finding additional information" on page vii

Purpose of this guide

This guide provides information about installing and managing SafeWord Web Access for Netscape Enterprise Server (NES).

Who should read this guide

This guide is intended for network and system administrators, SafeWord administrators, and anyone else who needs to install and configure SafeWord Web Access to work with NES.

IMPORTANT: *You must have NES and SafeWord installed before you can install SafeWord Web Access.*

This guide does not explain NES or SafeWord; information about those products are contained in their respective manuals. However, this guide does contains enough information about these products to enable you to configure them to work with SafeWord Web Access.

For more information about NES and SafeWord, see "Finding additional information" on page vii.

Using this guide

This manual is in Acrobat (softcopy) format only and does not contain an index. However, you can use Acrobat's **Find** feature to search for every instance of any word or phrase that you want. Using the Find feature allows you to decide what is relevant.

You may find, when you view this document online in PDF format, that the screen images are blurry. If you need to see an image more clearly, you can either enlarge it (which may not eliminate the blurriness) or you can print it out. (The images are very clear when printed out.)

About printing this document

For the best results, print this document using a PostScript printer using a PostScript driver.

- If your printer understands PostScript but does not have a PostScript driver installed, you need to install a PostScript driver. You can download one from **www.adobe.com**.
- If your printer is not a PostScript printer, and your document does not print out as expected, turn the **Print as Image** option to **ON** and then try printing.

How this guide is organized

This manual contains the following information.

Chapter Title	Description
Chapter 1: SafeWord Web Access for NES	Provides an overview and general information on SafeWord Web Access for NES.
Chapter 2: Installing and Configuring SafeWord Web Access	Provides information on installing and configuring SafeWord Web Access.
Chapter 3: Custom Authentication	Provides information on customizing authentication and html pages.
Chapter 4: Troubleshooting	Provides information on testing and verifying SafeWord Web Access.

Finding additional information

For additional information about SafeWord, other Secure Computing products, NES, and basic network security, refer to the following:

For information on...	Refer to ...
SafeWord Plus	All SafeWord Plus technical documentation is included in PDF format on the product CDs. For information on installing and configuring SafeWord Plus, see the following (also provided in hard copy): ◆ *SafeWord Plus Installation Guide* ◆ *SafeWord Plus Administration Guide* For a list of what is new in this release and know technical issues, see: ◆ *release notes.txt* file ◆ *known_issues.txt* file For detailed installation and configuration procedures for a particular SafeWord agent, see the appropriate PDF document on the Deployment CD.
Secure Computing	For the latest information about SafeWord/Plus and other network security products from Secure Computing, access our home page at: **http://www.securecomputing.com**
Netscape Enterprise Server	Go to **www.netscape.com** and search for "NES."
Basic network security	◆ *Computer Security Basics*, by Deborah Russell and G. T. Gangemi Sr. (O'Reilly and Associates, Inc., 1991). ◆ *Internet Security for Business*, Terry Bernstein, Anish B. Bhimani, Eugene Schultz, Carol A. Siegel (John Wiley & Sons, Inc., 1996). ◆ *Windows NT Security Handbook*, by Tom Sheldon (Osborne McGraw-Hill, 1997). This book is a great resource for almost any NT security issue.

Typographic Conventions

Note: *Throughout this manual, the term "SafeWord" is used as a blanket term that refers to SafeWord 5.x or SafeWord Plus. Areas of the documentation that are specific only to one version (i.e., SafeWord 5.x or SafeWord Plus) will be specified as such.*

This manual uses the following typographic conventions:

- **User input**

  The names of commands you type at the UNIX prompt appear in a **`boldface Courier`** font. For example, the following line of text contains a command name:

  Type **`whereami`** at the UNIX prompt.

  In commands, words that appear in *`Courier italic`* font are place holders for text you type. Words that appear in square brackets (`[` and `]`) are place holders for optional text. For example:

  `do.restore` *`filenum`* `[`*`device`*`]`

  In this example, *`filenum`* refers to the number assigned to the file system when it was backed up; you type this number following the command. For the optional **`[`***`device`***`]`** parameter, you might type, for example, **`/dev/rst0`**.

- **Line wrapping**

  When a command does not fit on one line on a page in this manual, it wraps to the next line and the wrapped line is indented. The backslash (\) is used at the end of the line, as shown below.

  ```
  cf ftp add message [msgfile=file_name] \
  [dir=directory_name] [type=entry_type]
  ```

- **Console output**

  Text displayed on a computer screen is shown in `plain Courier` font. For example:

  Upon completion, the Sidewinder displays the message "`DUMP IS DONE`."

- **File , directory, and role names**

  The names of files and directories appear in *plain text italics*. Words that appear in angled brackets <> are placeholders for text you type. For example:

  Put your image files in the *<your_NES_plugins_dir>/SafeWord/html/Images* directory.

CHAPTER 1

SafeWord Web Access for NES

SafeWord Web Access for NES is an NSAPI plugin that lets you use SafeWord authentication with Netscape's Enterprise Server.

This chapter contains the following topics:

- "About NES" on page 1-1
- "Requirements" on page 1-2
- "SafeWord Web Access overview" on page 1-3
- "Authenticating a user" on page 1-4

About NES

Netscape Enterprise Server (NES) enables organizations to share their information resources inside and outside the company, and deploy applications that can enhance communication, streamline processes, and reduce costs. By supporting multiple platforms, databases, and document types, NES leverages existing investments in hardware, applications, and information. It goes beyond existing Web servers by providing both advanced information services for content management and network-centric applications that can dramatically improve a company's ability to communicate and share information.

Requirements

The following requirements are considered to be the minimum acceptable requirements for hardware and software support.

NES

NES requires specific software and hardware. Before you can install a server, your system must meet the following requirements:

- Any CPU with access to a CD-ROM running **Sun Solaris 2.6**.
- 32 MB of RAM (64 MB is recommended for machines running database-intensive applications, which have many open database connections).
- 100 MB hard disk space.
- Swap space at least as large as the amount of RAM (twice the amount of RAM is recommended).
- Netscape Communicator 4.6 or higher, or Internet Explorer 4.01 or higher. Cookies must be enabled in the client software before you can administer your server.

SafeWord Web Access

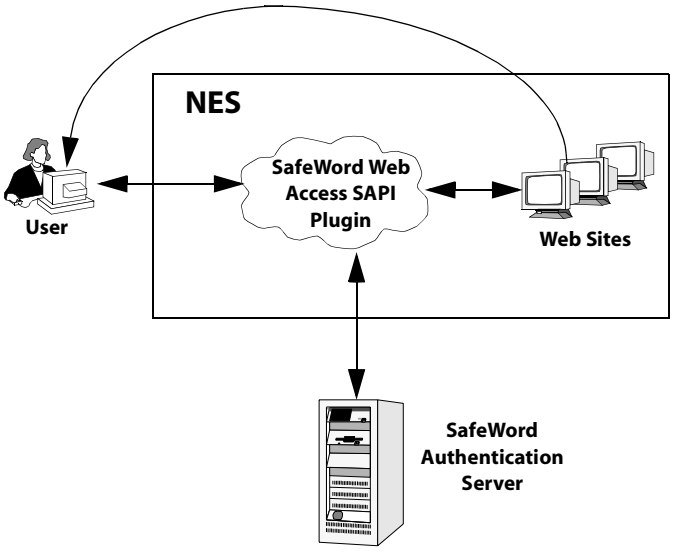
Before you can install SafeWord Web Access, your system must meet the following requirements:

- 2 MB of free space on your hard drive.
- SafeWord authentication server must be installed on your system.

SafeWord Web Access overview

The SafeWord Web Access plugin takes advantage of NES's openness to user-customizable API's, which are loaded and invoked during different stages of HTTP request processing. SafeWord Web Access allows you to more tightly define your own customized authentication methods and requirements, create your own set of permissions, or access privileges to resources.

Figure 1-1. SafeWord Web Access for NES plugin overview



1. When a user tries to access a Web resource, the request is received by the SafeWord Web Access NSAPI plugin.
2. If the Web resource is protected by SafeWord Web Access, it requests the user's identity (either using a digital certificate or SafeWord Web username) and password(s) for authentication.

   If the user's SafeWord Web identity and password(s) fail authentication, access is denied, the user is notified, and the process stops.
3. Once the user passes SafeWord authentication, SafeWord Web Access verifies that the user has the proper role to access the Web resource.

   If the user role doesn't have the authority to access the Web resource, access is denied, the user is notified, and the process stops.

Authenticating a user

A user authenticates using HTML forms. As shown in Figure 1-2, a user is first prompted for his or her identity (either by certificate or username).

Figure 1-2. SafeWord Web Access username form

After the certificate or user name is entered, the user may be prompted for one or more authenticator forms, as shown in Figure 1-3.

Figure 1-3. SafeWord Web Access password form (dynamic)

These forms are always present when you use SafeWord Web Access to protect your web resource. These forms may be customized to better suit the needs of your organization. For information on customizing Web pages, refer to Chapter 3, “Custom Authentication.”

CHAPTER 2

Installing and Configuring SafeWord Web Access

This chapter contains the procedures for installation. It includes the following topics:

- "Installation overview" on page 2-2
- "Installing the SafeWord Web Access plugin" on page 2-3
- "Configuring the obj.conf and obj.conf directives list" on page 2-8
- "Advanced feature: SafeWord Web Access plugin config file (config.data)" on page 2-11
- "Advanced feature: roles" on page 2-13
- "Advanced feature: configure the SafeWord Web Access EASSP configuration file (swwa.cfg)" on page 2-20
- "The swec.md5 file" on page 2-24
- "Starting the Web server" on page 2-25
- "Customizing HTML forms" on page 2-26
- "Logging" on page 2-26
- "Uninstalling SafeWord Web Access" on page 2-27

Installation overview

After you install NES and verify the server is working correctly, you can install the SafeWord Web Access plugin. Installation is accomplished by following the prompts from the installation script, which results in the following actions:

- Expands *tar* file into the appropriate directories
- Sets up links from <*your_NES_install_dir*>*/docs* directory to the required HTML files
- Sets permissions for the above files so the Web server can access them
- Creates a *swwa.cfg* file
- Creates plugin configuration files
- Adds plugin information into the Web server configuration

You should have the following information on hand when installing the SafeWord Web Access plugin:

- Hostname (or IP Address) for one or more SafeWord servers, and port number(s). Verify the servers are working correctly, and that they contain a valid username and password for testing. For example: **server1.mycompany.com, port number**
- NES plugin directory. For example: */usr/netscape/suitespot/plugins*
- NES docs directory (for installation of HTML files). For example: */usr/netscape/suitespot/docs*
- NES Web server root directory. For example: */usr/netscape/suitespot/https_SERVER1*

Installing the SafeWord Web Access plugin

To install SafeWord Web Access plugin, follow the steps below.

1. Download the compressed file from **www.securecomputing.com.**
2. Uncompress the file using the **`uncompress`** *`filename`***`.Z`** command.
3. Extract the file using **`tar -xvf *.tar`** command.

IMPORTANT: *You need to run the installation script as "root." The installation script requires read/write permissions to change owner and group names of the files to be owner and group of the web server.*

4. Run the **`./install`** script from within the directory created in step 3.
5. Specify the type of authentication server you will be using:
   - SafeWord 5.x or earlier
   - SafeWord Plus, old protocol
   - SafeWord Plus, new protocol (default)
6. Type the name of SafeWord server 1 (primary server).

   You need to supply a fully-qualified hostname or IP address for the primary server on which SafeWord is running. For example: **server1.mycompany.com**.
7. Type the port number of the primary server.

   This is the port number of the SafeWord server you set during the installation. The default port number will vary depending on the type of authentication server you selected in step 5:

   - SafeWord 5.x or earlier default = 7482
   - SafeWord Plus, old protocol default = 5030
   - SafeWord Plus, new protocol default = 5031
8. Enter the Client Type that you want the Web plugin to appear as.

   The Client Type, or Internet Server Name, is an ASCII string that tells SafeWord what type of client this is. Common values are SID, WWW, TELNET, etc. If you hit **Return** without specifying a Client Type, this line will be commented out in the configuration file, and SafeWord will match the request against a default ACL or PassAction.

IMPORTANT: *Selecting "yes" in the next step requires that the server is running and has at least one stored user with which you can authenticate and test the connection to the server.*

9. If you want to test the connection to the primary server, select **Yes**.

If you select **Yes** to test the server connection, you are prompted for username and password. The result of the test is displayed on screen; you must determine if the test was successful. If not, you are taken back to step 6.

10. If you want to add a second SafeWord server, select **Yes**. If you do not want to add any additional servers, proceed to step 13.

You need to supply a fully-qualified hostname or IP address for a secondary server on which SafeWord is running. For example: **server1.mycompany.com**.

11. Type the port number of the secondary server.

This is the port number of the second SafeWord server you set during the installation. The default port number is 7482.

IMPORTANT: *Selecting* **Yes** *in the next step requires that the server is running and has at least one stored user with which you can authenticate and test the connection to the server.*

12. If you want to test the connection to secondary server, select **Yes**.

If you select **Yes**, you are prompted for a username and password. The result of the test is displayed on screen; you must determine if the test was successful. If not, you are taken back to step 10.

13. Type the idle timeout for default user role.

The timeout values in the range of 0 to 604,800 seconds (1 week) allow you to set time limits for sessions. This is the maximum amount of time allowed between successive requests for uncached pages. If you enter **0** (zero) for the timeout value, the timeout will NOT be enforced.

The default is 900 seconds (15 minutes).

Note: *Disabling the idle timeout can be useful for limiting the number of authentication cookie updates, which may also slightly improve your browser's network performance.*

14. Type the session timeout for default user role.

The timeout values in the range of 0 to 604,800 seconds (1 week) allow you to set time limits for sessions. This is the total time allowed from the moment of successful authentication until a user is required to reauthenticate. If you enter **0** (zero) for the timeout value, the timeout will NOT be enforced.

The default is 3600 seconds (one hour).

15. To allow users to change their fixed passwords during authentication, select **Yes**.

Note: *Allowing users to change their password will eliminate the need for you, the administrator, to periodically change a user's password.*

16. If you want to use single sign-on, select **Yes**. If you do not want to use single sign-on, select **No** and go to step 19.

You can designate a group of multiple hosts that will share a single key for access. This is called a "single sign-on group."

If you selected **Yes** when prompted for a decision on whether there are other Web servers that comprise a single sign-on group, you need to supply domain names for those other servers. For example, a domain name of **.xyz.com** allows all hosts that contain **.xyz.com** to use the SafeWord Web Access single sign-on. All servers in the single sign-on group must share the same application ID encryption key, which is described next.

17. Type the domain name for web servers to share SafeWord Web Access single sign-on.

Note: *Domain names in the single sign-on group must start with a period (.). For example ".xyz.com".*

18. Type the application ID encryption key for encrypting browser cookies.

IMPORTANT: *If this is NOT the first installation SafeWord Web Access, you should type the same encryption key you entered when you installed the first SafeWord Web Access server.*

This is the key that is used to encrypt/decrypt browser cookies. You can use the randomly-generated default key (e.g., 45 37 c3 1f 84 7f 15), or one of your own.

19. Type the full pathname to NES server plugin location.

During installation, the script installs a SafeWord Web Access plugin to this directory.

Example: `/usr/netscape/suitespot/plugins/`

Note: *If you have previously installed SafeWord Web Access, the install script denotes this and reminds you to backup your data files prior to continuing with the installation.*

20. Type the full pathname to the NES HTML file location.

This directory creates a symbolic link from the *<SafeWord_Web_Access_plugin>/html/* directory to the web server *docs* directory (i.e., "document root"). This symbolic link is created so the SafeWord Web Access HTML files (e.g., authentication, logout, etc.) can be accessed by your web server without having to make duplicate copies of these files.

Pathname example: `/usr/netscape/suitespot/docs/`

21. Type the full pathname to the Web server.

This is the directory that contains the Web server's startup and stop scripts (**`./start`** and **`./stop`**), as well as Web server configuration information (e.g., *config/obj.conf*) and log files (e.g., *logs/errors*). The script needs to back up the Web server configuration (and optionally auto-edit it as well) so the *config/obj.conf* file must exist under the Web server's directory path.

For example: `/usr/netscape/suitespot/https-SERVER1/`

22. Type the username for server running NES.

This is the username (e.g., "nobody") that you designated during the NES installation on the target server. You should consider restricting the server's access to your system resources and running under a non-privileged system user account. This is because the account needs *read* permissions for the configuration files and *write* permissions for the logs it creates. For security reasons, the account shouldn't have write permissions to some of the configuration files because if the server is compromised, no one can write to those configuration files.

Note: *A username of "nobody" will not work on systems that assign a user ID of -2 for user "nobody". A user ID less than 0 creates an error during installation. Check the* /etc/passwd *file to determine the userid for "nobody," and make sure it's greater than 0.*

23. Type the group name.

Group names (e.g., "nobody") are assigned using NES's server Admin window. Group names are linked to the username that you designated during the NES installation. If the group name is incorrect, the server may fail due to problems with file permissions.

Note: *See your UNIX administrator if you are unable to determine what the group name should be.*

24. Back up the Web server configuration file.

The script will automatically back up *config/obj.conf* to *config/obj.conf.bak.pre-SWWA*. If you later choose to uninstall this plugin, the backed-up file can be used to restore *obj.conf*.

25. Modify the *obj.conf* file.

Before using this plugin, you first need to hook it into the Web server's configuration file, and define roles and resource/role permission mappings. You may do these configurations manually, or allow the install script to do this for you.

If you choose to manually edit the file, the script will remind you of the necessary changes, and exit. Refer to "Manually editing the plugin's configuration file" on page 2-8.

If you choose to allow the script to make the necessary changes, the script will add the two required "Init" lines on page 2-8, as well as the one required Object stanza on page 2-10.

26. Add resource/role entries.

The script will repeatedly prompt the user for resource and role specifications to indicate what resources (e.g., Web pages, directories, etc.) are protected by which roles. The resource is entered as a full filepath, such as:
`/usr/netscape/suitespot/docs/some_private_page.html`

The roles are a comma-separated list of role names with NO extraneous whitespace, indicating the roles that are allowed access to the specified resource. For example, `role1,role2,role3`. For each role that has not yet been defined in the plugin's configuration file, the install script asks the user if that role should be added to the plugin's configuration file. The user may specify the timeouts for each of these roles.

27. The plugin is now installed and configured. You must restart the Web server for the plugin to take effect.

Manually editing the plugin's configuration file

If you want to manually edit the plugin's configuration, follow the steps below:

1. Add configuration/directive lines to *obj.conf* and *obj.conf* directives list. Refer to "Configuring the obj.conf and obj.conf directives list" on page 2-8.
2. (Advanced feature) Configure the *config.data* file. Refer to "Advanced feature: SafeWord Web Access plugin config file (config.data)" on page 2-11.
3. (Advanced feature) Configure the *swwa.cfg* file. Refer to "Advanced feature: configure the SafeWord Web Access EASSP configuration file (swwa.cfg)" on page 2-20.

Configuring the obj.conf and obj.conf directives list

These files insert initialization lines and directives into NES that are specific to the SafeWord Web Access plugin.

The *obj.conf* file tells NES to load and initialize the SafeWord Web Access plugin. Format for the directive is:

```
Init fn="load-modules" funcs="wa_init,wa_service"
    shlib="<your_NES_server_dir>/SafeWord/lib/swwa.so"

Init fn="wa_init" loglevel="normal"
    rootDir="<your_NES_server_dir>/SafeWord/"
```

Note: *These text strings are wrapped, but must all be entered on the same line. The init string is on its own line.*

The *obj.conf* directives list allows you to specify the kind of authentication option for resources you want to protect.

IMPORTANT: *The order of NSAPI directives must occur as follows: AuthTrans, NameTrans, PathCheck, ObjectType, Service, AddLog. Additionally, if the Service line for SafeWord Web Access is not the first service line in the obj.conf file, the plugin will not be called when a request comes in.*

Form-based authentication

Form-based authentication (see Figure 2-2) uses an HTML page to obtain username and password. When you use form-based authentication, the text strings are wrapped, but must each be entered on the same line. You may find it most convenient to append the entries to the bottom of your *obj.conf* file.

You may add the protection line to existing objects, or as shown in the following example, create new objects for this purpose. The general format is as follows:

```
Service fn="wa_service" authMethod="EASSP"
    allowedRoles="list_of_roles"
```

Please note the following details:

- Each service function protects a single `<Object>..</Object>` stanza (corresponding to a particular file or directory path.) Therefore, you can configure several different directories or files to be protected.
- Also, for each `<Object>`, you can choose a list of one or more roles that have access to this resource. Upon successful authentication, the authentication server returns a list of roles in which this user may participate; the role names configured here should coincide with these roles. The SafeWord Web Access plugin is initially configured only with the “default” role, but you can add more roles, as discussed in "Advanced feature: roles" on page 2-13.
- The “list_of_roles” is a comma-separated list of role names with NO spaces. For example:

  ```
  allowedRoles="role1,role2,role3"
  ```

The following <Object>…</Object> stanza is *required* in order for the SafeWord Web Access plugin to be available to perform authentication, logins and logouts:

```
######### /SafeWord/ directory access ##########
# This one Object stanza handles all /SafeWord/*
# requests.
########################################
<Object ppath="<your_NES_docs_dir>/SafeWord/*">
Service fn="wa_service" authMethod="EASSP"
     allowedRoles="default"
</Object>
```

For each file or directory branch you want to protect, you may include an <Object>…</Object> stanza to protect that resource. The following examples illustrate their use:

```
## Only users in roles "engineer_role" or
##"admin_role" may access this page.
<Object ppath="<your_NES_docs_dir>/suppliers/
  list.html">
Service fn="wa_service" authMethod="EASSP"
     allowedRoles="engineer_role,admin_role"
</Object>

## Only users in the "finance_role" may access
## this directory branch.
<Object ppath="<your_NES_docs_dir>/financial/*">
Service fn="wa_service" authMethod="EASSP"
     allowedRoles="finance_role"
</Object>

## Anyone that can successfully SafeWord
## authenticate, regardless of what roles they are
## granted, may access this directory.
## (All authenticated users are automatically
## given the "default" role.)
<Object ppath="<your_NES_docs_dir>/
     employee_contact_info/">
Service fn="wa_service" authMethod="EASSP"
        allowedRoles="default"
</Object>
```

Advanced feature: SafeWord Web Access plugin config file (*config.data*)

This file provides the plugin with important run-time information, such as which authentication methods are available, authentication server addresses and ports, and which roles are configured.

File editing conventions

This file can be edited using any text editor. All values are case sensitive. Lines beginning with a pound (#) sign are treated as comments (# must be the first character of the line).

Each line in the file has two parts:

- **Parameter descriptor**

  A two character ID (e.g., 10) at the beginning of the line, followed by a space and documentary text.

- **Value/setting**

  Actual parameter values that control the behavior of SafeWord Web Access. If a value field contains multiple parts, you may separate the parts with space characters. Unless stated otherwise, you should have no more than one occurrence of each parameter.

Config.data parameters

- **AUTH_TYPES**

  This parameter specifies what types of authentication the plugin is capable of performing. Currently, only EASSP (SafeWord authentication protocol) is supported. For example:

  ```
  AUTH_TYPES;EASSP
  ```

- **ROLE**

  Note: *You may have up to 50 instances of this parameter.*

  This parameter defines a role and its associated timeouts (in seconds.) Timeout values may range from 0 to 604,800 seconds (one week.) A timeout value of 0 will cause that timeout NOT to be enforced. **enableTimeout** is a boolean indicating whether to enforce that role's timeouts (usually TRUE); legal values are “true” or “false” (case-insensitive.) The “default” role is required, and you may add up to 49 additional roles.

The format of a ROLE entry is:

```
ROLE;rolename,idleTimeout,sessionTimeout,enableTimeout
```

In the following example, a user in the "overseas_role" role has an idle timeout of 5 minutes and a session timeout of 30 minutes. A local worker may not require such frequent authentication, so you can create a role such as "local_engr_role" in which the timeouts are more relaxed, providing a one-hour idle timeout and an eight-hour session timeout.

```
ROLE;overseas_role,300,1800,TRUE

ROLE;local_engr_role,3600,28800,TRUE
```

- **ENCRYPTION_KEY**

  This parameter (also referred to as the Application ID) defines the key used to encrypt/decrypt the browser cookies. For all servers within a "single sign-on group" you should set each plugin's key to the same value, so the other Web servers can understand and create shareable cookies. The format is 8 hexadecimal octets (case-insensitive), separated by spaces.

  Example:

  ```
  ENCRYPTION_KEY ; a4 5f cc 70 b2 b7  1 25
  ```

- **DOMAIN_NAME**

  This parameter defines the domain to which SafeWord Web Access cookies are sent. (Without this parameter, a browser would only send cookies to the particular server from which they originated, thus preventing single sign-on.) If you do not require single sign-on, type `<HOSTNAME>`. Otherwise, type the domain in which the group of web servers reside.

  For example, the following entry will allow servers www.xyz.com, www1.xyz.com, and www.abc.xyz.com to share credentials:

  ```
  DOMAIN_NAME ; .xyz.com
  ```

  If you do not require single sign-on, use the following:

  ```
  DOMAIN_NAME ; <HOSTNAME>
  ```

- **EASSP_TIMEOUT**

  This parameter defines a SafeWord EASSP authentication protocol detail for determining a timed-out authentication connection (in seconds). For example:

  ```
  EASSP_TIMEOUT ; 10
  ```

- **CHANGE_PWD**

  This parameter defines whether users are allowed to change their fixed password(s). Valid values are TRUE or FALSE.

Advanced feature: roles

This section explains in more detail the function and use of roles within SafeWord Web Access.

Methodology

1. When a user first attempts to access a Web page or directory that is protected by SafeWord Web Access, no SafeWord Web Access cookie will be present in the request headers, and they will first be forced to authenticate. Upon successful authentication, the authentication server will return a list of (zero or more) roles in which this user may act. The SafeWord Web Access plugin then constructs a cookie which includes these roles and their respective timeouts. Each role has two timeouts associated with it:

   - **Idle timeout**—indicates the maximum amount of time between HTTP accesses.
   - **Session timeout**—indicates the maximum amount of time since authentication.

   When constructing the cookie, the plugin will put fresh timestamps on the timeouts of the roles it is aware of (from *config.data*), and puts zero timestamps in all other timeouts.

2. Upon subsequent HTTP accesses to this server (or others within the single sign-on group), the browser will prepend the cookie to the request headers.

3. The SafeWord Web Access plugin examines the cookie's list of roles and their timeouts, comparing them against the information in this plugin's *config.data* file. (Each SafeWord Web Access plugin instance may have different timeouts for the same roles, if so desired; Therefore, a timed-out role on one Web server may still be valid on another.) If this cookie contains any valid (non-timed-out) roles that coincide with the list of allowed roles for that resource (as found in *obj.conf*), the user will be granted access to the resource. For each of those valid roles that coincide with the list of allowed roles, the idle timeouts are updated. Continue at Step 2.
4. If this cookie contains only timed-out roles that coincide with the list of allowed roles for that resource, then the current cookie is erased, and the user must again authenticate. Continue at Step 1.
5. If this cookie contains no roles that coincide with the list of allowed roles for that resource, then the current cookie is not updated or erased, but an "Access Forbidden" page is returned to the browser. Continue at Step 2.

Adding roles in the authentication server

There are several ways to add roles to a user record, depending on what combination of authentication servers you are using. The following example should clarify how user roles are configured and used within a SafeWord server. In the following example, the role "default" has been explicitly included; however, all users implicitly inherit the "default" role, so it's unnecessary to type in this role, except for the sake of clarity.

User authentication and authorization information is stored in a user database entry on a SafeWord authentication server. On a SafeWord 5.x server, the list of roles is entered as a comma-separated list (e.g., `role1,role2,role3`) under "Pass Actions." This ASCII string usually contains a command that should be executed upon successful authentication, often a shell like */bin/csh*.

Roles example for SafeWord 5.x

To add a list of roles to a user entry:

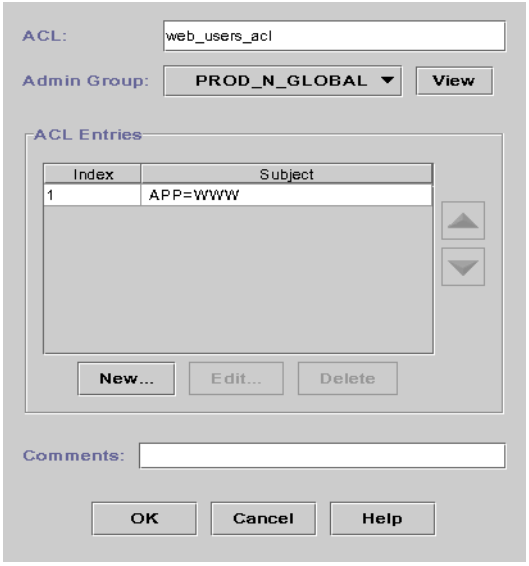
1. Run **`idutil`** to edit the SafeWord User database.
2. Select a user record to edit.
3. Select the **Pass Actions** field.
4. Under the Hosts column, type **default**.
5. Under the Action column, type the comma-separated list of roles (e.g., role1,role2,default).

Roles example for SafeWordPlus

If you have existing ACLs, Roles, or Users, you can edit existing entries. The following instructions assume that you are starting from scratch.

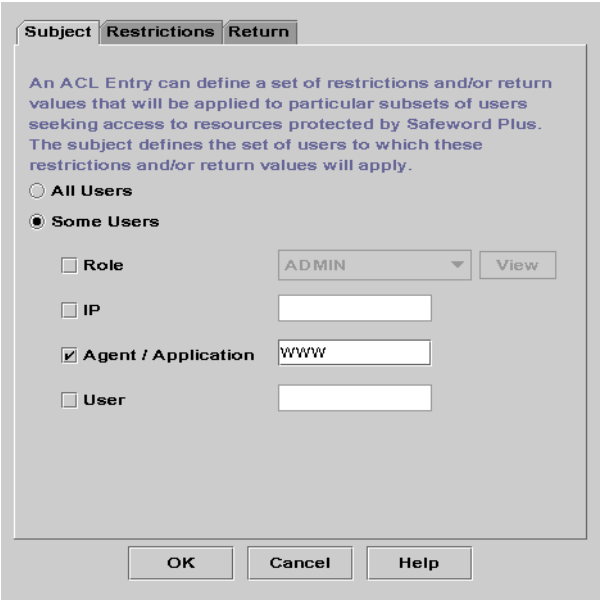
Creating an ACL

1. Log in to the Admin Console.
2. From the main menu, select **Insert** -> **ACL**. The following window appears.



3. Type a name for the new ACL in the ACL textbox.

4. Click **New** to create a new ACL Entry. The following window appears.



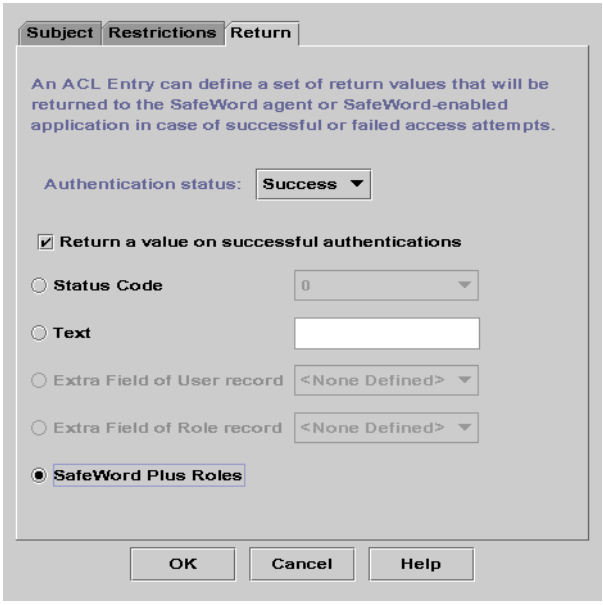
5. In the Subject tab, if you entered a Client Type during the Web plugin installation (see step 8 on page 2-3), then do the following:

   a. Select the **Some Users** radio button

   b. Select the **Agent/Application** checkbox

   c. Enter the same string that you entered during the plugin installation in the Agent/Application textbox.

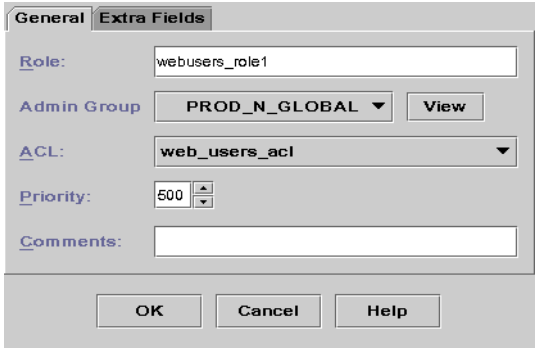
6. Select the Return tab. The following window appears.



7. Select **Success** in the Authentication status drop-down list.
8. Select the **Return a value on successful authentications** checkbox.
9. Select the **SafeWord Plus Roles** radio button.
10. Click **OK** to save the ACL entry, then **OK** again to save the ACL.

Creating a Role

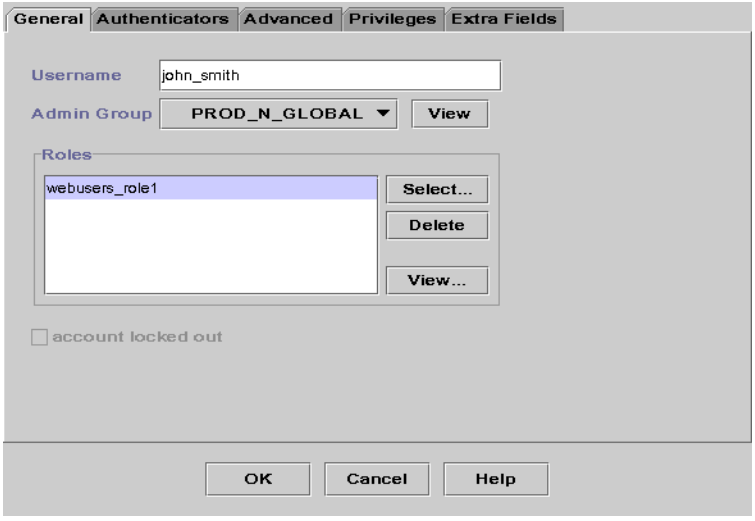
1. From the main menu, select **Insert** -> **Role**. The following window appears.



2. In the General tab, specify a Role name in the Role textbox.
3. Select the ACL you created from the ACL drop-down list.
4. Click **OK**.

Creating a User

1. From the main menu, in the left-hand pane that displays Groups, select the proper group in which to store your new user.
2. From the main menu, select **Insert** -> **User**. The following window appears.



3. In the General tab, enter a username for the user in the Username textbox.
4. Under Roles, click **Select** to assign one or more roles to this user.
5. Fill in any other information in the other tabs, such as authenticator information.
6. Click **OK**.

Adding roles in SafeWord Web Access plugin config file (*config.data*)

The roles entered in *config.data* determine which roles the plugin needs to enforce, and session and idle timeouts for each role. (For more information, refer to the description of the ROLE attribute in the "File editing conventions" on page 2-11.)

It is possible for each plugin instance in a single sign-on group to have different role configurations. In addition to some roles existing in some instances of *config.data* but not others, each instance of *config.data* could have different timeout values for the same roles. For example, within a single sign-on group, one Web server that hosts proprietary cost/pricing information may be the only Web server in the group that contains a “finance role” allowing access to client/buyer addressing information. Also, the timeouts for several roles on this Web server could be much smaller than timeouts on other Web servers, to reduce the possibility of fraudulent online orders from hijacked connections or unattended workstations.

One consequence of varying timeouts of a role within a single sign-on group is, a role that is considered “timed out” on one machine may still be considered valid on a different machine. For example, if a user's final valid role has just timed out on Server 1, which has short timeouts, normal behavior at this point would be for Server 1 to send a “timed out” cookie, thus forcing subsequent authentication. However, if the user has configured their browser to “Alert me before accepting any cookies”, they could avoid the current cookie's destruction by hitting “Cancel” on the cookie notification dialog box, and continue web surfing on Server 2, which has longer timeouts.

Using roles to protect web resources (obj.conf)

The Netscape *obj.conf* file contains (among other things) the list of directives/checks that must be successfully completed before the Web server can access the requested Web page. SafeWord Web Access protection is incorporated by adding directives to *obj.conf*, as described in the section "Configuring the obj.conf and obj.conf directives list" on page 2-8. In the Service directive you add, the allowedRoles parameter indicates which roles are sufficient in order to access the protected resource. As long as a user has at least one of the allowed roles which has not yet timed out, they are permitted access.

The allowedRoles parameter holds a comma-separated (no spaces) list of roles. If you type a role name or use a role that hasn't been defined in *config.data*, the plugin will log this error, ignore the unknown rolename, and continue processing.

Note: *Although users inherit the "default" role just by successfully authenticating, THEY DO NOT INHERIT ACCESS TO RESOURCES. If you want to grant the "default" role access privileges to a resource, you must explicitly include it in that resource's Service's allowedRoles parameter.*

Advanced feature: configure the SafeWord Web Access EASSP configuration file (*swwa.cfg*)

The SafeWord Web Access EASSP configuration file (*swwa.cfg*) determines several operating parameters for SafeWord Web Access. It can be edited using any text editor. All values are case sensitive. Lines beginning with a pound (#) sign are treated as comments (# must be the first character of the line).

Each line in the file has two parts:

- **Parameter descriptor**

  A two character ID (e.g., 10) at the beginning of the line, followed by a space and documentary text.

- **Value/setting**

  Actual parameter values that control the behavior of SafeWord Web Access.

SafeWord authentication server

The SafeWord authentication server parameter specifies one or more servers to use (you must specify at least one server). Up to three additional servers may be specified. The syntax for this configuration is:

```
02 SafeWord Authentication Server: host weight
 connections [port]
```

- **Host**

  Name or IP address where SafeWord server is located. The host name may be one of the following:

  — Host IP address (e.g., 200.2.2.27)

  — Host name (entry must be made in the */etc/hosts* file associating the IP address with the host name.)

- **Weight**

  Value used for determining priority and load balancing for multiple authentication servers. The weight value designates which servers are used and under what conditions. There are two schemes for selecting servers as they are needed:

  — **Prioritized**—This scheme specifies a primary server that is used whenever possible. If it goes down, the next server on the list is used as a backup. If that server fails, the next is used, and so on. To specify this scheme, set all the weights to 0. The priority is the order in which the servers are entered into the file; the first entry has the highest priority.

  — **Load balancing**—This scheme provides a means to distribute the client load across multiple servers. As each session requires a server, they are allocated in sequential order. For an equal balancing of all servers, type a "1" for all servers. For unequal loading, increase the weight to increase the load.

- **Connections**

  The maximum number of simultaneous connections allowed. Specify a value if you need to "throttle" swwa. This is typically set to 0, which means "no limit."

- **Port**

  Service port number of the server (optional). If omitted or set to 0, the default port number is used. Typically, it is not required. It should only be set when the default port number conflicts with an existing service. When the port number is 0 or not entered, the swwa client searches the */etc/services* file for a SafeWord entry.

  An entry would look like this:

  ```
  SafeWord 7482/tcp #SafeWord Authentication Server
  ```

  If the entry is found, the specified number is used. If no entry is found, the client uses the default number of 7482.

Sample SafeWord server configurations that use the following convention:

```
02 SafeWord Authentication Server: host weight
connections [port]
```

would look like this:

- **Single server**

  ```
  02 SafeWord Authentication Server: 222.40.23.02 0 0 7479
  ```

- **Multiple servers, primary with backups**

  ```
  02 SafeWord Authentication Server: 222.40.23.02 0 0 7479
  02 SafeWord Authentication Server: 222.40.23.02 0 0 7480
  02 SafeWord Authentication Server: 222.40.23.04 0 0 7479
  ```

- **Multiple servers, load sharing**

  ```
  02 SafeWord Authentication Server: 222.40.23.02 2 0 7479
  02 SafeWord Authentication Server: 222.40.23.03 1 0 7479
  02 SafeWord Authentication Server: 222.40.23.04 1 0 7479
  ```

Other *swwa.cfg* configurations

- **User ID source**

  swwa.cfg requires setting this as **user**.

- **Server's System Name**

  Specifies which SafeWord User database is used. SafeWord idutil can be used to setup and manage multiple user and authenticator databases. Each user database is given a "System Name." SafeWord comes with the "standard" system database already configured. You can use the standard database if you want. Make sure that the server's system name is "standard" (or matches your custom system name).

- **Data Files Path**

  This is the directory where the *swec.dat* file resides. If a custom text set is used, it is also in this directory.

  Path: `<your_NES_plugin_dir>/SafeWord/data`

- **Console Status Messages**

  swwa.cfg can send error, informational, debug, and status messages to the system console. Valid entries are the same as described for user status messages. Normally, this value is set to **error**. Valid entries are:

  — NONE: No logging is sent.

  — ERROR: Error messages are sent.

  — INFO: Routine informational messages are sent.

  — DEBUG: Debugging messages are sent.

  — ALL: All message types are sent.

  More than one type of message can be sent as follows:

  ```
  16 Send Status Messages to Console: ERROR INFO
  ```

- **Log File Messages**

  swwa can send error, informational, debug, and status messages to the log file. This parameter specifies what types of logs are sent to the logfile. Valid entries are the same as described for console status messages. The length of the log file defaults to 64 KB if not specified using syntax:

  ```
  Max log file length in KB (128 max)
  ```

  A log file is written until it reaches the maximum length, at which point it is renamed with a *.bak* extension, and a new file is started. If a *.bak* log already exists, it is overwritten.

The *swec.md5* file

This file is responsible for ensuring the validity (or authenticity) of the SafeWord servers. Authentication with an authenticator is required for the file to become valid. The *swec.md5* file also relies on proper synchronization with each SafeWord server key. If synchronization fails for any reason, then all authentication attempts to that server fail.

The *swec.md5* file can lose synchronization if you reinstall SafeWord Web Access, your SafeWord server software, or change its key. In these cases, an error with the *swec.md5* file can usually be cleared by deleting the file (or by hand-editing the file and deleting the entire line for that particular server), then re-authenticating with a valid username and dynamic password.

Starting the Web server

Once installation and configuration are complete, you can start the server in one of two ways:

- Using the command line, as follows:

  your_NES_server_dir`/start`

- Connecting to your Admin server; verify that the following conditions are met:
  - Server is running
  - The IP address (or server name) is correct
  - The port number of the NES server in the site window is correct

Note: *If you use the browser method, any changes you make will overwrite the obj.conf file.*

(e.g., `http://192.168.26.22:23579/https-192.168.26.22/bin/index`)

On successful startup, you should see the following:

```
[date:time]:info: successful server startup

[date:time]:info: Netscape-Enterprise/3.5.1 B<build number>

[date:time]:info: sw_access_init reports:(0)Starting...

[date:time]:info: sw_access_init reports:(0)initializing
EASSP...

[date:time]:info: sw_access_init reports: (0)Authentication
initialization for 'EASSP' was a success. AP Code: '0'
Message:Initialized and registration complete...'

[date:time]:info: sw_access_init reports:(0)Waiting for
requests...

[date:time]:info: sw_access_init reports:(0)Exiting.
```

Once you start the server, the NES Admin page appears. For further information about using the features of the NES Admin page, refer to Netscape's NES documentation.

Customizing HTML forms

You can customize the Web pages that SafeWord Web Access uses to challenge users and display status. For example:

- Change the overall look and feel
- Add your company banner or logo
- Add instructions or links to help pages
- Have login redirect to a page other than the default page

For details on how to customize Web pages, see "Creating your own authentication Web pages" on page 3-2.

Logging

Logging functions are handled by NES's native logging feature, and can be found under NES's Server Status Panel. Within this panel, you can choose to view access logs or view error logs.

If you're not using a browser, these files are located at:

<your_NES_server_dir>/logs/errors

<your_NES_server_dir>/logs/access

The Access log records all connections made to the NES server, and includes the IP address from which the connection originated; the date and time of connection, and specific Web page(s) the user connected to. The log also records the username of user who requested the resource.

The Error log records errors that occurred during a session. It includes the date and time of occurrence; the host IP address of the user who received the error; and a brief explanation of the error's cause.

The Error Log also records time user logged in and logged out.

Uninstalling SafeWord Web Access

To uninstall SafeWord Web Access, follow the steps below.

1. Stop all running Web servers associated with SafeWord Web Access.
2. Manually remove all directories created during the installation using the following command:

   rm -r *<your_NES_plugins_dir>***/SafeWord**

3. Remove the SafeWord Web Access documents symlink from your HTML server's root document directory using the following command:

   rm -r *<your_NES_docs_dir>***/SafeWord**

4. Change to your NES Web server root directory using the following command:

   cd *<your_NES_webserver_root_dir>*

5. Restore the backed-up copy of the obj.conf file using the following command:

   mv config/obj.conf.bak.pre-SWWA config/obj.conf

CHAPTER 3

Custom Authentication

This chapter provides information on using SafeWord Web Access either “out of the box” or customizing it to suit your organization.

This chapter contains the following topics:

- "Out of the box" on page 3-1
- "Creating your own authentication Web pages" on page 3-2
- "Using built-in authentication pages" on page 3-3
- "Creating custom authentication pages" on page 3-5

Out of the box

Out of the box, SafeWord Web Access performs authentication as follows:

If a client attempts to access a Web resource protected by SafeWord Web Access, the user is challenged to enter a SafeWord username and password. Upon successful authentication, they are given access to the resource.

Alternatively, if the client accesses any Web site with the URL path of */SafeWord* or */SafeWord/index.html*, they are presented with a choice of logging in or logging out. If they choose to log in, they are challenged for a SafeWord username and password. Upon successful authentication they are redirected to the **LoginSuccess.htm** page.

If, after being authenticated by SafeWord Web Access, the user attempts to access a resource protected by NES, they are challenged for their NES username and password.

3 Creating your own authentication Web pages

You can create your own HTML forms for initiating SafeWord authenticated sessions. These forms collect the SafeWord username and password, and upon successful authentication, redirect the user to some Web resource. The benefit to creating your own login pages is that they can reside anywhere on a Web site, and each Web site can have a different login page. Also, the login page can have menu options specific to the Web site.

Guidelines for customization

- **Absolute path names for local support file**

  The SafeWord Web Access HTML files are kept separate from the Web site directories. Therefore, if you wish to add links to files in the *<your_NES_plugins_dir>/SafeWord/html/* directory, you must give those files a URL path that starts with */SafeWord/*. For example, suppose you want to include your company logo on the authentication form. You would put the image file in the *<your_NES_plugins_dir>/SafeWord/html/Images/* directory. You would then include the following in the authentication form:

  ```
  <IMG SRC="/SafeWord/Images/filename">
  ```

- **Retaining existing form items unchanged**

  All the existing form items are required for proper operation. Do not change their names, and in the cases of the hidden text fields, do not change their attributes. You can, of course, change the size, location, and font. For the one exception to this rule, see the next guideline.

- **Customizing the login target page**

  The Login.htm forms default to redirecting the client to the **LoggedIn.htm** page. If you want to specify a different destination for the user upon successful authentication, you must change the value of the PassRedirect hidden text field. The default value will be */SafeWord/LoggedIn.htm,* which simply redirects to the **LoggedIn.htm** page.

- **Changing the default login link authentication form**

  When a user sends a GET request to */SafeWord/* or */SafeWord/index.html*, they get a page with links to login and logout pages. The default link for login is */SafeWord/Login.htm*, which is a SafeWord Web Access authentication only form.

Using built-in authentication pages

The built-in SafeWord Web Access authentication pages are sent by SafeWord Web Access in the following circumstances:

- The user tries to access a protected resource
- The SafeWord authenticated session times out
- A user tries to access a restricted resource for which they do not have the proper role
- A user sends a GET request to the URL path of */SafeWord* or */SafeWord/* or */SafeWord/index.html*
- A user logs out
- A user aborts a logout

The HTML files for all these situations are located in the product directory, <*your _NES_plugins_dir*>*/SafeWord/html/*. The SafeWord Web Access program requires that these filenames do not change. The Web master can customize these files but must follow the guidelines below in order to meet the minimum functional criteria for the HTML forms. It is highly recommended that you make backups of these files before modifying them. For a list of the files see "SafeWord Web Access Web pages" on page 3-3.

SafeWord Web Access Web pages

These are the Web pages required by SafeWord Web Access. These pages must be located in your web server's real documents directory. The **`./install`** script creates a symlink from <*your_NES_plugins_dir*>*/SafeWord/html* to <*your_NES_docs_ dir*>*/SafeWord/html* directory.

******** QUESTION ********
NEED TO UPDATE THESE TABLES!

HTML forms

HTML Form	Description
Authentication.htm	SafeWord authentication: sent when the user first tries to access a SafeWord Web Access protected resource.
Reauthentication.htm	SafeWord reauthentication: sent when the user does not pass the SafeWord Web Access authentication.
TimeoutAuthentication.htm	SafeWord reauthentication: sent when the session times out.
Login.htm	SafeWord authentication: sent when the login link on the **index.html** page is clicked.
Logout.htm	Logout with confirmation: sent when you click the logout link on the **index.html** page.

HTML pages

HTML Page	Description
AccessDenied.htm	Sent when user fails authentication using the HTTP Basic Authentication method.
index.html	Contains links to login and logout: sent when URL path is */SafeWord* or */SafeWord/* and the HTTP request is a GET.
Forbidden.htm	Access forbidden message: sent when user does not have the proper role for a resource.
LoggedOut.htm	Message that the user has successfully logged out; sent after you click **Yes** on the **Logout.htm** form.
NotLoggedOut.htm	Message that the user was not logged out; sent after you click **No** on the **Logout.htm** form.
Version.htm	Informs the user as to current version number.

Creating custom authentication pages

The benefit of creating your own authentication pages is that they can be tailored to each specific Web server. You can adopt an existing Web site's "look and feel." The built-in authentication pages can be used universally for all Web servers on a machine.

You can create Web pages of your own design for:

- Initiating a SafeWord authenticated session
- Terminating a SafeWord authenticated session

You can place your authentication pages in the *<your_NES_plugins_dir>/SafeWord/html/* directory, with the following consequences:

- Your custom pages are always accessible, even if your entire Web site is protected.
- Files located in the *<your_NES_plugins_dir>/SafeWord/html/* directory have an URL that starts with */SafeWord/*.
- Links in your Web pages to local support files in the html directory must use absolute URL paths.

Adding custom login forms to SafeWord Web Access

The following procedure is an example of how to add a custom login form to the *<your_NES_plugins_dir>/SafeWord/html/* directory.

1. Create a directory in *<your_NES_plugins_dir>/SafeWord/html* directory for your Web page such as */SafeWord/html/MyLogin*.
2. Create a directory for images such as: *<your_NES_plugins_dir>/SafeWord/html/MyLogin/Images*.
3. Put your login HTML file in the *<your_NES_plugins_directory>/SafeWord/html/MyLogin* directory (example: **`login.htm`**). For details on creating this file, see the section on Initiating a SafeWord authenticated session.

4. Put your image files such as company logo in the *<your_NES_plugins_dir>/SafeWord/html/MyLogin/Images* directory (example: `myLogo.jpg`).
5. Edit the login file and set the links to the image files so that they look like this:

   ```
   <IMG SRC="/SafeWord/MyLogin/Images/myLogo.jpg">
   ```

6. Use the login form by going to the following URL:

   http://your.web.site/SafeWord/MyLogin/login.htm

Initiating a SafeWord authenticated session

To initiate a SafeWord authenticated session, create an HTML form with the following parameters:

- `Command=`**`SafeWordAuthentication`**
- `SafeWordUser=`*`username`*
- `SafeWordPassword=`*`password`*
- `PassRedirect=`*`destination URL`*

Example:

```
<FORM ACTION="/SafeWord/Command.cgi" METHOD="POST"
 ENCTYPE="application/x-www-form-urlencoded">
<P>SafeWord Username:</P>
<INPUT TYPE="TEXT" NAME="SafeWordUser">
<P>SafeWord Password:</P>
<INPUT TYPE="PASSWORD" NAME="SafeWordPassword">
<INPUT TYPE="HIDDEN" NAME="Command" VALUE="SafeWord
 Authentication">
<INPUT TYPE="HIDDEN" NAME="PassRedirect" VALUE=" /
 SafeWord/LoggedIn.htm">
<P><INPUT TYPE="SUBMIT" VALUE="Ok"></P>
</FORM>
```

The value for the PassRedirect parameter is the URL the user will be redirected to upon successful authentication.

CHAPTER 4

Troubleshooting

This chapter contains information to help you troubleshoot problems you may encounter when using SafeWord Web Access.

This chapter contains the following topics:

- "Errors during installation" on page 4-1
- "Errors starting the server(s)" on page 4-3
- "Verifying that SafeWord Web Access is enabled" on page 4-3
- "Single sign-on server errors" on page 4-3

Errors during installation

If you encountered errors during installation:

1. Check to see whether you ran the **`./install`** script as "root."

   The installer needs read/write permission to change the owner and group names of the files to be the owner and group of the Web server.
2. Verify that the target Web server is running and can be reached from your browser.
3. Make sure your SafeWord server is functioning correctly.
4. Check the error log located at *<your_NES_install_dir>/logs/errors*. Check for error messages that might help you determine the source of the error.

5. Verify that the following lines exist in the *obj.conf* file (and all text for each line is placed on a single line):

```
Init fn="load-modules" funcs="wa_init,wa_service"
shlib="<your_NES_server_dir>/SafeWord/lib/swwa.so"

Init fn="wa_init" loglevel="normal"
rootDir="<your_NES_server_dir>/SafeWord/"
```

If you are using forms, the SafeWord Web Access service directive is listed first in the service directive list

IMPORTANT: *If the Service line for SafeWord Web Access is not the first service line in the obj.conf file, the plugin will not be called when the server receives a request.*

6. Modify the *obj.conf* file to turn on logging level for debugging. Set the **loglevel** parameter in the *obj.conf* file to "**debug**"

   ```
   Init fn="wa_init" loglevel="debug"
   rootDir=<your_root_dir>"
   ```

7. If you reinstalled SafeWord Web Access, you may encounter an error in the *swec.dat* file. If this happens, delete the old *swec.dat* file, and reauthenticate with a valid username and dynamic password.

8. Error locating plugin directory: check the full pathname to the directory in which the plugins are to be written.

   Example: `/usr/netscape/suitespot/plugins/`

Errors starting the server(s)

If you encountered errors while trying to start the server:

1. For browser errors indicating that a file does not exist (for files that begin with */SafeWord/*), verify the link between your Web server's root directory and *<your_NES_plugin_dir>/SafeWord/html/*. The SafeWord Web Access plugin requires these forms to be your Web server's directory when using the service directive.

   If you have your Web server configured to disallow following symlinks, you'll need to copy the required html files to *<your_NES_plugin_dir>/SafeWord/html/*.

2. If you used a browser to connect to your admin server and make configuration changes, they may have overwritten the *obj.conf* file.

3. For errors with permissions of configuration files, check the error log found at *<your_NES_plugin_dir>/logs/errors*.

4. Verify the groupname you entered during installation is the same as the groupname you associated with the username of the NES server on which the plugin is being installed.

Verifying that SafeWord Web Access is enabled

To verify that SafeWord Web Access is enabled, check the error log file located at:

```
<your_NES_server_dir>/logs/errors
```

The entry would look something like this:

```
[date:time]:info: sw_access_init reports:(0)Waiting
for requests...
```

Single sign-on server errors

For errors starting a server that's part of a single sign-on group;

1. Verify that the *<your_NES_plugins_ dir>/SafeWord/data/config.data* file for that server contains the same shared ENCRYPTION_KEY and DOMAIN_NAME strings as the primary server.

2. Verify that the domain name was entered correctly. Also verify that the domain name you entered starts with a "." (e.g., ".xyz.com").

3. Verify that the accessed URL's hostname contains the same domain name as specified in step 1 and step 2.

   For example, `http://server1.xyz.com/index.html` will work, but `http://server1/index.html` will not, because the browser has no way of knowing that host "server1" is actually part of domain .xyz.com. Therefore, the browser will not return the cookie.

4. Verify that the *<your_NES_plugins_ dir>/SafeWord/data/config.data* file on all single sign-on servers contains the same encryption key and domain name strings. The domain name string must be the domain of the Web servers that share single sign-on, not "`<HOSTNAME>`", or the actual hostname of a server if your SafeWord Web Access plugin resides on different hosts.

5. Verify that your browser is at least Netscape Communicator 4.6 or higher, or Internet Explorer 4.01 or higher.

Part Number: 86-0934246-A
Software Version : SafeWord Web Access for NES, Version 1.2