

# Product Guide

SECURE  
COMPUTING



# SAFEWORD®

For use with Microsoft Active Directory



## Copyright

© 2005 Secure Computing Corporation. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Secure Computing Corporation.

## Trademarks

Secure Computing, SafeWord, Sidewinder, Sidewinder G2, SmartFilter, Type Enforcement, SofToken, Enterprise Strong, Mobile Pass, G2 Firewall, PremierAccess, SecureSupport, SecureOS, Bess and Strikeback are trademarks of Secure Computing Corporation, registered in the U.S. Patent and Trademark Office and in other countries. G2 Enterprise Manager, SmartReporter, On-Box, Application Defenses, RemoteAccess, Sentian, Securing connections between people, applications and networks are trademarks of Secure Computing Corporation. All other trademarks, tradenames, service marks, service names, product names, and images mentioned and/or used herein belong to their respective owners.

## SafeWord Software License Agreement

The following is a copy of the Software License Agreement as shown in the software:

CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE LOADING THE SOFTWARE. BY CLICKING “YES” BELOW, OR BY INSTALLING, COPYING, OR OTHERWISE USING THE SOFTWARE, YOU ARE SIGNING THIS AGREEMENT, THEREBY BECOMING BOUND BY ITS TERMS. IF YOU DO NOT AGREE WITH THIS AGREEMENT, THEN CLICK “NO” BELOW AND RETURN ALL COPIES OF THE SOFTWARE AND DOCUMENTATION TO SECURE COMPUTING CORPORATION (“SECURE COMPUTING”) OR THE RESELLER FROM WHOM YOU OBTAINED THE SOFTWARE.

**1. Software Products Definition.** “Software Product(s)” means (i) the machine-readable object-code versions of the SafeWord software contained in the media (the “Software”), (ii) the published user manuals and documentation that are made available for the Software (the “Documentation”) and (iii) any updates or revisions of the Software or Documentation that you may receive (the “Update”). Under no circumstances will you receive any source code of the Software.

**2. Grant of License.** Secure Computing grants to you, and you accept, a non-exclusive, and non-transferable license (without right to sub-license) to use the Software Products as defined herein on a single SafeWord system.

**3. Limitation of Use.** You may not: 1) copy, except to make one copy of the Software solely for back-up or archival purposes; 2) transfer, distribute, rent lease or sublicense all or any portion of the Software Product to any third party; 3) translate, modify, adapt, decompile, disassemble, or reverse engineer any Software Product in whole or in part; or 4) modify or prepare derivative works of the Software Products. You agree to keep confidential and use your best efforts to prevent and protect the contents of the Software Product from unauthorized disclosure or use.

The Software Product is licensed for use with the specified SafeWord tokens accompanying and bundled with the Software Product. The Software Product may not be used with SafeWord tokens purchased separately, or tokens manufactured by other vendors.

**4. Limited Software Product Warranty.** Secure Computing warrants that the medium/media 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. If you do not receive media which is free from defects in materials and workmanship during the 90-day warranty period, you will receive a refund for the amount paid for the Software Product returned.

**5. Hardware Token Warranty.** For a period of one (1) year from date of shipment, Secure Computing warrants that the SafeWord tokens sold with the Software Product will be free from defects in material and workmanship under normal use. This warranty does not cover lost or stolen tokens.

**6. 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.

**7. Term and Termination.** This license is effective until terminated. You may terminate it at any time by destroying the Software Product, 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 Product and erase all copies residing on computer equipment.

**8. Ownership.** This 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 Products are and will remain the property of Secure Computing or its licensors, whether or not specifically recognized or protected under local law. You will not remove any product identification, copyright notices or other legends set forth on the Software Product.

**9. Export Restrictions.** You agree to comply with all applicable United States export control laws, and regulations, as from time to time amended, including without limitation, the laws and regulations administered by the United States Department of Commerce and the United States Department of State. You have been advised that Software Products are subject to the U.S. Export Administration Regulations. You shall not export, import or transfer Software Products contrary to U.S. or other applicable laws, whether directly or indirectly, and will not cause, approve or otherwise facilitate others such as agents or any third parties in doing so. You represent and agree that neither the United States Bureau of Export Administration nor any other federal agency has suspended, revoked or denied Your export privileges. You agree not to use or transfer the Products for end use relating to any nuclear, chemical or biological weapons, or missile technology unless authorized by the U.S. Government by regulation or specific license.

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

**11. Entire Agreement.** This Agreement is our offer to license the Software Product to you exclusively on the terms set forth in this Agreement, and is subject to the condition that you accept these terms in their entirety. If you have submitted (or hereafter submit) different, additional, or other alternative terms to Secure Computing or any reseller or authorized dealer, whether through a purchase order or otherwise, we object to and reject those terms. Without limiting the generality of the foregoing, to the extent that you have submitted a purchase order for the Software Product, any shipment to you of the Software Product is not an acceptance of your purchase order, but rather is a counteroffer subject to your acceptance of this Agreement without any objections or modifications by you. To the extent that we are deemed to have formed a contract with you related to the Software Product prior to your acceptance of this Agreement, this Agreement shall govern and shall be deemed to be a modification of any prior terms in their entirety.

**12. 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. You may not assign this License or any associated transactions without the written consent of Secure Computing. This License shall be governed by and construed in accordance with the laws of California, without regard to its conflicts of laws provisions.

## 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 Technical Support directly, telephone +1.800.700.8328 or +1.651.628.1500. If you prefer, send an e-mail to [support@securecomputing.com](mailto:support@securecomputing.com). To inquire about obtaining a support contract, refer to our "Contact Secure" Web page for the latest information at [www.securecomputing.com](http://www.securecomputing.com).

## Customer Advocate information

To suggest enhancements in a product or service, or to request assistance in resolving a problem, please contact a Customer Advocate at +1.877.851.9080. If you prefer, send an e-mail to [customer\\_advocate@securecomputing.com](mailto:customer_advocate@securecomputing.com).

If you have comments or suggestions you would like to make regarding this document or any other Secure Computing document, please send an e-mail to [techpubs@securecomputing.com](mailto:techpubs@securecomputing.com).

## Printing history

Date	Part number	Software Release
May 2005	86-0944890-A	SafeWord version 2.1
July 2005	86-0944890-B	SafeWord version 2.1



# Table of Contents

---

<b>Chapter 1: Introduction</b> .....	<b>1-1</b>
Welcome to SafeWord .....	1-2
Components and functions .....	1-3
The SafeWord Server .....	1-4
The SafeWord Management Console (SMC) .....	1-4
The Auto Updater .....	1-6
The SafeWord Internet Authentication Service (IAS) Agent ..	1-6
The SafeWord Agent for Web Interface .....	1-6
The Secure Access Manager (SAM) Agent .....	1-7
The Outlook Web Access (OWA) Agent .....	1-7
 <b>Chapter 2: Installation and Configuration</b> .....	 <b>2-1</b>
Installation prerequisites and requirements .....	2-2
Network prerequisites .....	2-2
Hardware/software requirements .....	2-2
Optional Agent prerequisites .....	2-2
Installation topology rules .....	2-3
Installing SafeWord .....	2-5
If installing the SafeWord Server .....	2-8
Installing the SMC or a SafeWord Agent only .....	2-10
Finishing the installation .....	2-11
Upgrading from SafeWord 2.0.x to SafeWord 2.1.x .....	2-12
Registering and activating SafeWord .....	2-13
Locating the Software Serial Number and Token Group ID ..	2-13
Registering and activating your product .....	2-13
Additional activation steps .....	2-14
Verifying your activation .....	2-15
Subsequent token activations .....	2-15
Password security procedures .....	2-16
Changing your administrative passwords .....	2-16
Ensuring password security .....	2-18
Preparing and deploying tokens .....	2-19
Administrator-assigned tokens using the SMC .....	2-20
Self-enrollment with the User Center .....	2-22

Adding or changing PINs .....	2-24
Testing tokens .....	2-26
<b>Chapter 3: Setting up Strong Authentication .....</b>	<b>3-1</b>
The SafeWord Internet Authentication Service (IAS) Agent .....	3-2
IAS Agent default configurations .....	3-2
Launching the administration tool .....	3-3
Configuring MPPE support .....	3-3
The SafeWord Agent for Web Interface .....	3-5
Configuring the SafeWord Agent for Web Interface .....	3-5
SafeWord Secure Access Manager (SAM) Agent .....	3-7
SAM Agent default configurations .....	3-7
Configuring MSAM 4.0 .....	3-8
The Outlook Web Access (OWA) Agent .....	3-10
OWA Agent default configurations .....	3-10
Configuring the OWA Agent .....	3-11
OWA logging settings .....	3-12
Agent configurations .....	3-13
Configuring the Authentication Engine .....	3-13
Changing Logging settings .....	3-14
Configuring the Authentication Policy .....	3-15
Configuring alternative group policies .....	3-17
<b>Chapter 4: Miscellaneous Administrative Tasks .....</b>	<b>4-1</b>
Using the Auto Updater .....	4-2
Token-related tasks .....	4-3
Resynchronizing tokens .....	4-3
Searching for unassigned tokens .....	4-5
Finding users associated with specific tokens .....	4-6
Generating emergency passcodes .....	4-7
Reassigning tokens .....	4-8
Deleting token records from the database .....	4-11
Manually importing token data records .....	4-11
Manually importing token data records from a CD .....	4-13
SafeWord server-related tasks .....	4-15
Stopping and starting servers .....	4-15
Changing component ports .....	4-15
Logging server diagnostics .....	4-16
Monitoring server status .....	4-18
Adding servers to the monitored servers list .....	4-18
Removing servers from the monitored servers list .....	4-19
Cloning servers .....	4-19
Configuring the Administration Server .....	4-19



Configuring multiple servers . . . . .	4-21
SafeWord Server synchronization . . . . .	4-21
Setting up SafeWord Server synchronization . . . . .	4-21
Verifying SafeWord Server synchronization . . . . .	4-23
Managing and viewing logs . . . . .	4-25
Configuring Management Console logging . . . . .	4-25
Viewing event logs . . . . .	4-26
Database-related tasks . . . . .	4-27
Backing up the database . . . . .	4-27
Restoring the database . . . . .	4-28
Reinstalling a server or the SMC . . . . .	4-29
Running SafeWord without Active Directory . . . . .	4-30
Importing token records without Active Directory . . . . .	4-30
Configuring SafeWord to operate without Active Directory . .	4-31
<b>Chapter 5: Troubleshooting . . . . .</b>	<b>5-1</b>
Troubleshooting . . . . .	5-2
Uninstalling SafeWord . . . . .	5-4
<b>Appendix A: SafeWord Gold 3000 Tokens. . . . .</b>	<b>A-1</b>
Overview of your Gold 3000 tokens . . . . .	A-2
SafeWord Gold 3000 tokens . . . . .	A-2
Activating tokens . . . . .	A-3
Distributing the hardware PINs . . . . .	A-3
Assigning and testing tokens . . . . .	A-3
Changing PINs . . . . .	A-3
Using your token with SafeWord . . . . .	A-4
<b>Index . . . . .</b>	<b>In-1</b>



# CHAPTER 1

## Introduction

---

### About this chapter

This chapter introduces SafeWord<sup>®</sup> software, its uses, and related components.

This chapter includes the following topics:

- ◆ “Welcome to SafeWord” on page 1-2
- ◆ “Components and functions” on page 1-3

## Welcome to SafeWord

1

Welcome to SafeWord, the strong authentication solution for Microsoft Windows platforms. SafeWord is an add-on security application that provides strong authentication to users of VPNs (virtual private networks), dial-up, Outlook Web Access, RADIUS-based technologies, and Citrix applications.

SafeWord is designed to be extremely easy to install and manage. It quickly and seamlessly integrates into existing environments, immediately increasing the security of your network servers.

To get the product running in your environment, simply:

- ◆ Meet the operational prerequisites and system requirements
- ◆ Install the software
- ◆ Activate the product
- ◆ Configure the product
- ◆ Assign and distribute SafeWord tokens to your users

**Note:** If you will be using SafeWord Gold 3000 Tokens, refer to “SafeWord Gold 3000 Tokens” on page A-1.

The term “SafeWord” (used throughout this product guide) refers to all SafeWord for... product lines (e.g. SafeWord for Nortel, SafeWord for Citrix, etc.).

SafeWord comes with several informational resources for installing and configuring the product. If you are looking for quick instructions, use the Quick Start included in the product package. If you need detailed information, use this guide. For interface specific help, use the SafeWord Online Help that is included in the software.

The next section describes SafeWord components and functions.

## Components and functions

This section describes the SafeWord core and optional components and their functions. If you prefer, you can skip this section and proceed to “Installation prerequisites and requirements” on page 2-2.

---

### Core components:

---

- ◆ The SafeWord Server
- ◆ The SafeWord Management Console (SMC)
- ◆ The Auto Updater

---

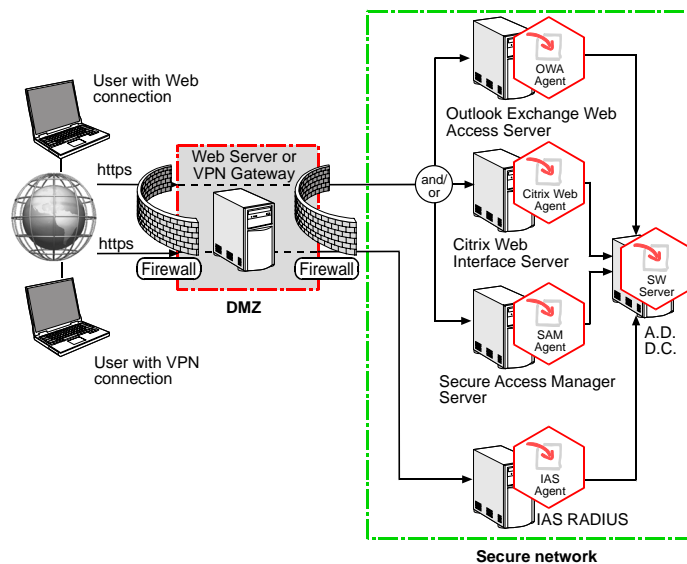
### Optional components (agents):

---

- ◆ The Internet Authentication Service (IAS) Agent
- ◆ The SafeWord Agent for Web Interface (formerly NFuse) for use with Citrix Presentation Server
- ◆ The Secure Access Manager (SAM) Agent
- ◆ The Outlook Web Access (OWA) Agent

Figure 1-1 shows a network including possible server combinations and associated SafeWord agents installed.

**Figure 1-1. Network with possible server/ SafeWord agent combinations**



These components work together to provide strong authentication for users accessing your network and applications. The sections that follow describe the functions of each of the components.

---

## The SafeWord Server

The SafeWord Server is comprised of the SafeWord database, the Authentication Engine, the Administration Service (may also be referred to as the Administration Server), and the User Center.

- ◆ The SafeWord database serves as the repository for token records.
- ◆ The Authentication Engine verifies that the passcode supplied with an authentication request is correct for the token assigned to the user being authenticated.
- ◆ The Administration Service provides the business logic for the various operations supported by the product. It is used by the SMC and the User Center to perform the tasks initiated by administrators or end users. It is also responsible for synchronizing SafeWord database data in configurations with multiple servers.
- ◆ The User Center allows end users to enroll their SafeWord tokens. It is easy to use, and saves administrative time when a large number of users will be authenticating with SafeWord tokens. The User Center also users to change or assign their PIN, resync their tokens, and test their tokens after enrollment.

---

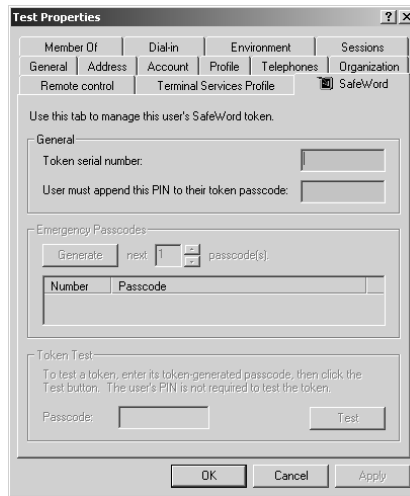
## The SafeWord Management Console (SMC)

User management occurs via the SMC, which is accessed via the standard Active Directory Users and Computers administration tool.

**Note:** *Although Active Directory is a requirement for SafeWord, you may also get a limited subset of the product's functionality without Active Directory. For details about running SafeWord without Active Directory, see "Running SafeWord without Active Directory" on page 4-30.*

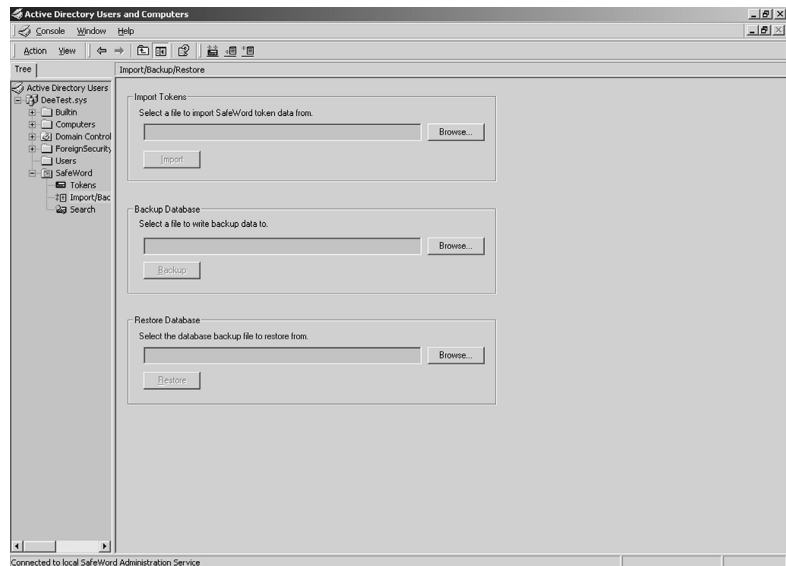
The console consists of two parts. The first part is the SafeWord tab on the standard user management dialog. Using this tab, administrators can associate Active Directory users with SafeWord tokens. They can also assign PINs, generate emergency passcodes, and test tokens assigned to individual users. Figure 1-2 shows the SafeWord tab.

**Figure 1-2. SafeWord tab on the standard user management dialog**



The other part is a separate SafeWord section added to the left pane of the same tool. The controls in that section allow administrators to list tokens, view and search for user/token associations, and import new token records into the system. They can also backup and restore the SafeWord database here. The SafeWord section is shown in Figure 1-3.

**Figure 1-3. The SafeWord section in Active Directory Users and Computers**



---

## The Auto Updater

SafeWord's Auto Updater allows you to automatically update your SafeWord software with new features and patches as they become available. The feature installs on every host in the distributed system. When updates are available, a message displays to notify the user. The user will only be notified if there are updates that do not already exist on their system. The Auto Updater runs automatically when the SafeWord Management Console is accessed. On other SafeWord components, it can be launched manually. The Auto Updater allows you to view, download, and install the available updates (if there are any) whenever you desire. Only the updates that you have not already installed will be visible in the list of available updates.



**Important:** *Manual downloading and installing of updates is not recommended, as it can leave your system in an unstable state. If you download and run the updates manually, be sure to install them in the order in which they are listed in the Auto Updater.*

---

## The SafeWord Internet Authentication Service (IAS) Agent

SafeWord provides strong authentication to industry-leading IPsec VPNs, SSL VPNs, commsservers, and other RADIUS (Remote Authentication Dial-In User Service) devices. Simply install and configure SafeWord's IAS Agent, which works with Microsoft's IAS RADIUS, to provide strong authentication to RADIUS devices through the Microsoft IAS RADIUS server.

Once the IAS Agent is installed and configured, VPN and RADIUS users who access their network remotely will be required to enter a SafeWord token-generated passcode in order to access the network. Detailed information and configuration instructions for the IAS RADIUS Agent are contained in Chapter 3 of this guide.

---

## The SafeWord Agent for Web Interface

The SafeWord Agent for Web Interface is for use with Citrix. It resides on the same Citrix server on which the Citrix Web Interface is installed, and provides the link to the SafeWord Server. It intercepts user access requests and routes them to the Authentication Engine for user name and passcode verification. Once properly authenticated, users are allowed access; otherwise access is denied. Configuration instructions and details can be found in Chapter 3 of this guide.



---

## **The Secure Access Manager (SAM) Agent**

SafeWord adds strong authentication to Secure Access Manager features through the SafeWord Secure Access Manager Agent. The agent uses the standard SafeWord administration tools, and installs directly on top of your Citrix Secure Access Manager installation. Configuration instructions and details about SAM support can be found in Chapter 3 of this guide.

---

## **The Outlook Web Access (OWA) Agent**

SafeWord's Outlook Web Access Agent works with the Microsoft Exchange Server to provide SafeWord strong authenticated access through the Microsoft Exchange Outlook Web Access (OWA) component. When this option is chosen at installation, users who access their e-mail account remotely using Outlook Web Access will be prompted for a SafeWord token-generated passcode in order to access the network. If you will be using the Outlook Web Access Agent, complete installation and configuration information is available in Chapter 3 of this guide.



# Installation and Configuration

---

## About this chapter

This chapter describes the process of installing and registering your SafeWord software.

This chapter includes the following topics:

- ◆ “Installation prerequisites and requirements” on page 2-2
- ◆ “Installing SafeWord” on page 2-5
- ◆ “Upgrading from SafeWord 2.0.x to SafeWord 2.1.x” on page 2-12
- ◆ “Registering and activating SafeWord” on page 2-13
- ◆ “Password security procedures” on page 2-16
- ◆ “Preparing and deploying tokens” on page 2-19

## Installation prerequisites and requirements

# 2

The following are the prerequisites necessary to install, configure, and use this product. Some components are required for all configurations, others are required only if you will be using a specific agent. For specific component information, refer to Chapter 3 of this guide.

---

### Network prerequisites

Before installing SafeWord your users must be able to make a successful connection to secure network resources by a secure Web or VPN session. Your network must also have the following required components:

- ◆ Windows 2000/2003 domain controller
- ◆ Active Directory populated with users

**Note:** Although Active Directory is a requirement for all SafeWord features, a limited subset of functionality is available without Active Directory. For details about running SafeWord without Active Directory, see “Running SafeWord without Active Directory” on page 4-30.

- ◆ Internet access

---

### Hardware/software requirements

Table 2-1 lists minimum system hardware and software (operating system) requirements for installing and running SafeWord.

**Table 2-1. Hardware/software requirements**

Component	Specification
CPU	Pentium III @ 550 MHz (or better)
OS	Windows 2000/2003 Server Edition (with latest service pack)
RAM	256 MB (min) 512 MB (recommended)
Disk Space	300 MB (min) 3 GB (recommended)

---

### Optional Agent prerequisites

Table 2-2 lists the prerequisites for installing and using SafeWord components and the available optional agents.

Table 2-2. Component and optional Agent prerequisites

To install...	...you must also have
SafeWord Server	This component is always available as an installation option. If you install it on a non-domain controller, you must provide domain administrator credentials that have the privilege to log on as a service.
SafeWord Management Console (SMC)	This component is only available when the installation machine is part of a domain.
IAS Agent	No specific requirements
SafeWord Agent for Web Interface	<ul style="list-style-type: none"> <li>◆ Web Interface 2.0 or 3.0 installed</li> <li>◆ Internet Explorer 5.5 or higher (for configuring the agent)</li> </ul>
OWA Agent	Microsoft Exchange Server 2000 or 2003  <b>Note:</b> You must be logged on as a domain administrator for this agent to be available during installation.
SAM Agent	Citrix Secure Access Manager (2.x or 4.0) installed  <b>Note:</b> The SAM Agent is protected when using CSG for authentication. The agent software must be installed where CSG is installed.



**Important:** For hierarchical domain topologies, you must be logged on as a parent domain administrator.

## Installation topology rules

SafeWord offers a variety of options for installing and using its components to best suit existing installation topologies.

You may install all SafeWord components on one machine (if that machine has the capacity to handle the authentication and management load of your organization), or components can be installed on separate machines if you want to spread the operational load among several machines. The SafeWord installer program will not allow you to install a component if it cannot correctly operate on the target machine. All other installation combinations are supported, as long as they conform to the following rules.

---

### Rules governing component installation.

---

- ◆ **Rule 1:** The SafeWord Agents must be installed on the same machine as the component they're designed to protect. The agents are tightly integrated with their respective component and cannot operate as a standalone piece.



**Important:** *If your network contains multiple component installations (OWA, IAS, Web Interface, etc.), each installation must also have its corresponding SafeWord Agent installed on the same machine.*

- ◆ **Rule 2:** Because of the tight integration of the SMC with the standard Windows Active Directory management tool, the SMC must be installed on a domain controller that also has the standard Active Directory Users and Computers management tool installed on it.

**Note:** *The SMC is installable on Windows XP as long as the Windows Server 2003 Administration Tools Pack (Adminpak.msi) is installed. The pack can be downloaded from [www.microsoft.com](http://www.microsoft.com).*

## Installing SafeWord

Installing SafeWord is quick and easy. The software will not interfere with your existing topology. You can install it directly in your existing environment.

Once you have verified that your server environment meets the operational prerequisites and system requirements outlined in the previous section of this guide, follow the steps below to install SafeWord.

1. Insert the SafeWord Installation CD into the CD-ROM drive of the computer where you are installing SafeWord. The installer starts automatically.

The Welcome to SafeWord window appears.

**Figure 2-1. Welcome to SafeWord window**



2. Enter your product serial number.

The product serial number, located on the back of your product package and/or on the Activation Certificate, should begin with two letters (e.g. RA, SC, etc.), and is in the format (RAxx-xxxx-xxxx-xxxx).

**Note:** The *View Documentation* button only becomes active once all serial number digits are entered.

3. Click **OK**.
4. When the Welcome screen appears, click **Next**.
5. When the License Agreement window appears, review the license agreement, then click **Yes** to accept it.

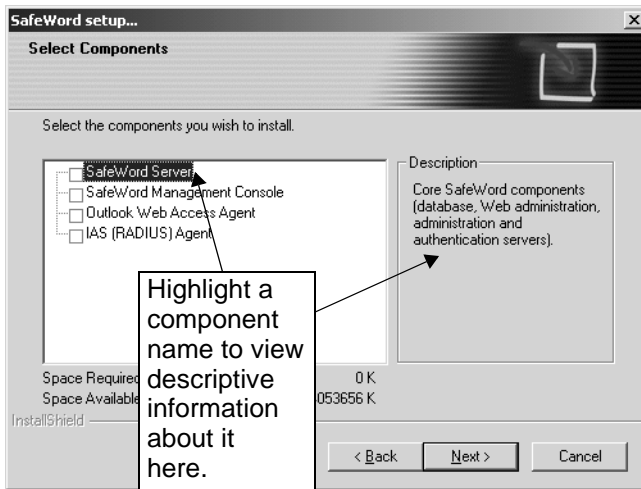


**Important:** You must accept the license to continue the installation process.

6. When the Choose Destination Location window appears, accept the default installation location (or browse/select another), then click **Next**.

The Select Components window appears.

**Figure 2-2. Select Components window**



In Figure 2-2 none of the components are selected for installation. If you are unsure about which components to install, refer to Table 2-2 on page 2-3.



**Tip:** If a component cannot be installed on a given machine, it will not be listed in the window displayed in Figure 2-2.

---

### Continuing the installation

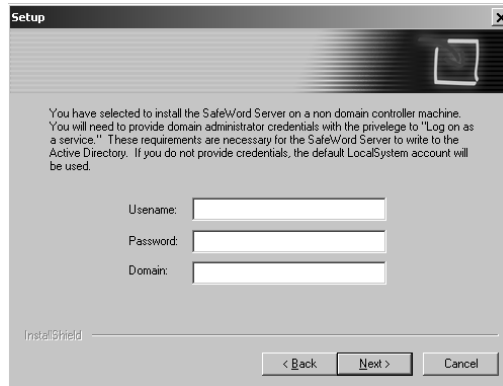
---

7. If you are installing the SafeWord server on a machine that is not a domain controller, skip to step 10.
8. If you are installing the SafeWord Server on a machine that is not a domain controller, a Setup window appears requesting domain administrator credentials with the privilege to log on as a service. In this case, continue to the next step to provide the proper credentials.

**Note:** Domain administrator credentials and the privilege to log on as a service are required so the SafeWord Server can write to Active Directory.



**Figure 2-3. Administrator Credentials window**



9. Enter your account ID (user name with the required credentials), account password, and domain (to which this machine will log-in) in the appropriate fields.



**Important:** *If no credentials are specified, the local system credentials will be used. Clicking Next will cause the Choose Destination window to appear.*

10. Click **Next**.
11. When the Select Program Folder window appears, click **Next**.
12. When the Start Copying Files window appears, click **Next**.

Installer-related windows will flash on and off as the program installs the software, initializes components, and starts servers and/or services.

- ◆ If you are installing the SafeWord Server, continue to the section, “If installing the SafeWord Server”.
- ◆ If you are installing the SMC or a SafeWord Agent only, proceed to “Installing the SMC or a SafeWord Agent only” on page 2-10.

## If installing the SafeWord Server

If you are installing the SafeWord Server, the Server Components window appears. In this window, you will identify the ports over which the SafeWord components will communicate and specify unique encryption and signing keys.

By default, SafeWord installs with the following port/key settings:

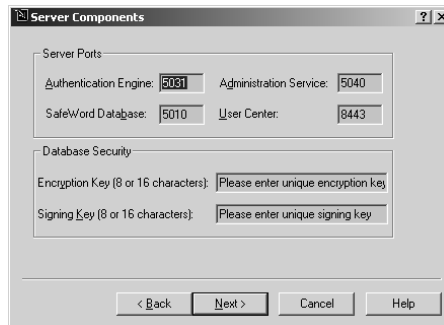
**Table 2-3. Default SafeWord port/key settings**

Parameter	Setting (default)
Authentication Engine	Port 5031
SafeWord Database	Port 5010
Administration Service	Port 5040
User Center	Port 8443
Encryption Key	Please enter unique encryption key
Signing Key	Please enter unique signing key



**Important:** The User Center is a public access resource for end user token management. It is available in the form of a URL, for example: **https://machinename:port/usercenter**.

**Figure 2-4. Server Components window**



**Tip:** If you see a small exclamation point displayed next to a Port field, the port you have chosen is already in use by another process. In this situation, you must choose a different port for the component you are currently configuring.

1. Keep the default ports, or specify different port numbers for the **Authentication Engine**, the **SafeWord Database**, the **Administration Service**, and the **User Center**.
2. Personalize your SafeWord installation by defining a unique **Encryption**

**Key** and **Signing Key** on the Database Security pane. The keys can be 8 or 16 characters in length.

**Note 1:** If you are installing multiple servers, they must all have the same keys as are used here.

**Note 2:** If the key string you enter is less than 16 characters in length, DES will be used as the encryption algorithm. While faster, it is not as secure as 3DES, which would be used for a full 16 character key string.



**Security Alert:** It is important to enter your own custom encryption key and signing key for your SafeWord database. This helps to insure the integrity of data, uniquely distinguishing it from all other SafeWord installations.

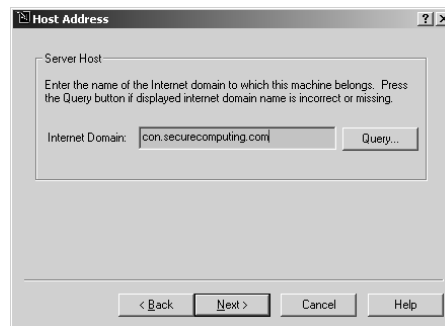


**Important:** Once the encryption key is entered in this window, it must remain the same for the life of the installation.

3. Click **Next**.

The Host Address window appears.

**Figure 2-5. Host Address window**

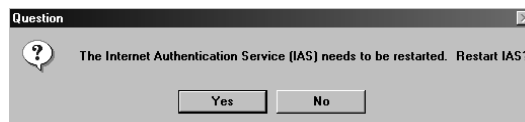


4. In the **Internet Domain** field, enter the Fully Qualified Domain Name to which this machine belongs. If you do not know the domain, click the **Query** button to get it from your DNS server.
5. Click **Next**.

### If installing the IAS Agent

6. If you are installing the IAS Agent on a machine where Microsoft IAS is already installed, a window appears indicating that you must restart IAS. If the Restart window does not appear, skip to step 8.

**Figure 2-6. Restart IAS window**



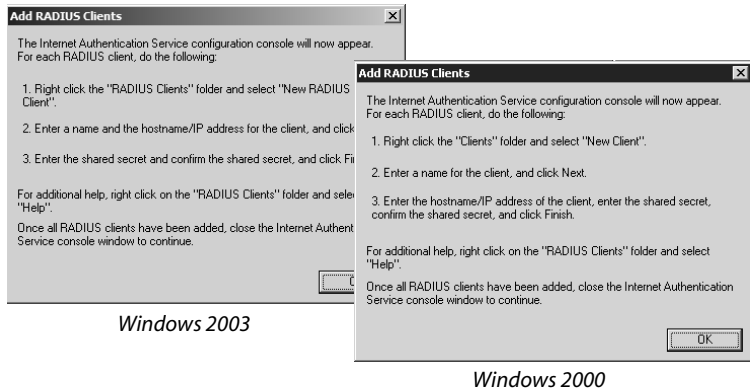
7. Click **Yes** to restart the Internet Authentication Service.

If you are installing the IAS Agent on a machine that did not already have IAS running on it, a Question window appears indicating that you must add RADIUS clients to the client's list. If this window does not appear, skip to step 10. Otherwise, continue to the next step.

8. To add RADIUS clients to the client's list, click **Yes**.

The Add RADIUS Clients window appears.

**Figure 2-7. Add RADIUS Clients window**



9. When the IAS configuration console appears, follow the instructions on the interface to add the RADIUS clients.

10. Click **OK**.

Proceed to "Finishing the installation" on page 2-11.

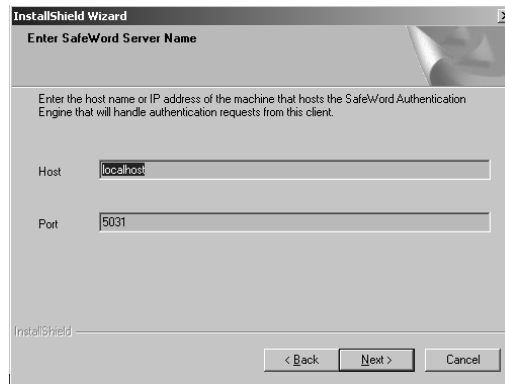
---

## Installing the SMC or a SafeWord Agent only

If you are installing the SMC or a SafeWord Agent only, you will be asked to specify the name and port number for the Authentication Engine.

The Enter SafeWord Server Name window appears before the installation reaches 100 percent.

**Figure 2-8. Enter SafeWord Server Name window**



The fields in this dialog box correspond to the Authentication Engine port setting you entered in step 1. The default setting is 5031.

11. Enter the **Host** and **Port** of the machine where the SafeWord Server is installed.
12. Click **OK**.

---

## Finishing the installation

During installation, a number of windows appear and disappear. This portion of the installation may take several minutes to complete.

When the installation is finished, the InstallShield Wizard Complete window appears.

13. Click **Finish**.

Before you can use your SafeWord software, you must register and activate it. Refer to the next section, “Registering and activating SafeWord” on page 2-13.

## Upgrading from SafeWord 2.0.x to SafeWord 2.1.x

To upgrade your SafeWord 2.0.x system to SafeWord 2.1.x, do the following:

1. Insert the SafeWord 2.1.x CD into the system containing the SafeWord 2.0.x software.
2. If you have no internet access, you will need to acknowledge the warning dialog and choose **Continue** to proceed with the installation.  
The installer will detect the older SafeWord version, and ask if you want to upgrade your existing installation.
3. Select **Yes** to perform the upgrade.
4. (Optional: preview the product documentation) Select **OK** to proceed with the installation.
5. If you have internet access, run the SafeWord Auto Update Agent to check for the most current product updates.

Before you can use your SafeWord software, you must register and activate it. Refer to the next section, “Registering and activating SafeWord” on page 2-13.

## Registering and activating SafeWord

SafeWord must be registered and activated after installation. Upon successful registration, a SafeWord activation key and token data records are downloaded for you and placed in their proper directory. This unlocks and enables full software functionality.

The Activation Certificate that came with your software contains the SafeWord Software Serial number and Token Group ID number that allow you to download the activation key and token data records.

---

### Locating the Software Serial Number and Token Group ID

Your Software Serial Number and Token Group ID are found on the Activation Certificate in the following formats:

- ◆ **SafeWord Software Serial Number**—The serial number is a 16-digit alphanumeric code in the form of this example: RAXx-xxxx-xxxx-xxxx. You will need the serial number to obtain your product activation key.
- ◆ **Token Group Identifier**—Your Token Group ID is also a 16-digit alphanumeric code in the form of this example: TKxx-xxxx-xxxx-xxxx. Entered on the same Web page as the SafeWord Software Serial Number, it allows you to obtain the data records for your tokens.



**Important:** Keep your Activation Certificate in a safe location where you can find it in the future. You will need the SafeWord Software Serial Number when/if you purchase additional SafeWord tokens.

---

### Registering and activating your product

Activation is required before you can use your SafeWord software and tokens. When you complete the activation form, your information will be verified, and registration key and token records will be downloaded and installed automatically. Registering the product occurs from within the SafeWord Management Console.



**Security Alert:** The prompt that allows you to download the activation key and token data records is a one-time only prompt. For security reasons, you are only allowed one attempt to download these files. If your download is unsuccessful, contact Customer Service at 1.800.700.8328 or 1.651.628.1500 to request a CD of these records.

To register and activate the product:

1. Locate the SafeWord Product Serial Number and the Token Group Identifier included on your Activation Certificate.
2. Launch the SafeWord Management Console by selecting **Start-> Programs -> Administrative Tool -> Active Directory Users and Computers**.

**Note:** You will be prompted to enter an administrative password. See "Changing your administrative passwords" on page 2-16.

3. Right-click on the SafeWord folder.
4. Select **Activate Product**, and the activation form appears.
5. Complete the activation form by entering all required information.



**Important:** If you have more than two token group IDs, enter all of them at this time to download the token data records for all tokens. If you do not enter an ID for a package of tokens, you will not be able to download the data records for those tokens at this time. To download token data later, refer to "Manually importing token data records" on page 4-11.

6. Click the **Submit** button.

You will see a message that SafeWord activation and token import is in progress. A list of steps for the license and tokens also appears. When the processes are complete, you will see a message that SafeWord is activated and the token data download is complete.

7. Click **OK**.



**Important:** While your activation is completing, a key file and an import file are downloaded and stored automatically in `Install_directory`. The key file is required to enable SafeWord, and the import file contains token data records. You may choose to access and save either or both of these files separately. A dialog box that appears during this stage of the activation allows you to choose to save the files separately.

---

## Additional activation steps

If the Management Console is installed on a machine different than the machine on which the SafeWord Server is running, the following additional activation steps are necessary:

1. On the system where the SMC is installed, browse to the location where the **key.html** file is stored (`Install_directory\SERVERS\AdminServer\activation`).
2. Copy **key.html** into the following subdirectory on the SafeWord system: `Install_directory\SERVERS\AdminServer\activation`.





**Important:** Ensure the file name is **key.html**. Using any variation (*key.htm* or *key.html.html* for instance) will cause the activation to fail.

3. Restart the SafeWord Administration Service by doing the following:
  - a. Select **Start -> Programs -> Administrative Tools -> Services**.
  - b. Right click **SafeWord Administration Service** and select **Restart**.

The successfully processed license file will be renamed **key.activated.html**.

---

## Verifying your activation

Your SafeWord registration and activation are complete, but you may verify the success of the activation by doing the following:

1. Launch the SafeWord Management Console by selecting **Start-> Programs -> Administrative Tool -> Active Directory Users and Computers**.
2. Right-click the SafeWord folder in the Console.
3. Select **About SafeWord Management**.
4. Verify the Product Serial Number in the Serial Number field is correct.
5. Browse to **Install\_directory\SERVERS\AdminServer\activation** where you installed the SafeWord Server component.



**Tip:** If you choose the default installation location, you will browse to *C:\Program Files\Secure Computing\SafeWord\SERVERS\Admin Server\activation*.

The successfully processed license file is now renamed **key.activated.html**.

---

## Subsequent token activations

When you purchase additional tokens, you activate them using the original Product Serial number and the Token Group identifier from the newly purchased token pack. Follow the same steps outlined in the activation instructions, “Registering and activating SafeWord” on page 2-13. In this case, even if the Management Console is installed separately from the SafeWord server, it is not necessary to activate the server using the **key.html** file.

## Password security procedures

This section contains post installation procedures that help ensure security of the SMC and user center.

---

### Changing your administrative passwords

The first time you start the SMC and the User Center, you must customize your installation by changing the default password for each of them. These are **not** passcodes generated by a SafeWord token. They are passwords that the SMC and the User Center use to connect to the Administration Service.



**Tip:** For security purposes, it is important that you use passwords that consist of mixed case letters and numbers.

---

### Changing your SMC default password

You must customize your SMC password before you can use the SafeWord software. The first time you use the SMC, the **Enter an Administration Password** window appears prompting you to change your administration password. Do the following to customize your installation with a password:



**Important:** You will only need to change the administration password the first time SafeWord is started. If you plan to install multiple management consoles, you will need to specify the same password for all installations.

**Figure 2-9. Enter an Administration Password window**



1. Enter and re-enter the desired password, then click **OK**.
2. When the Success window appears, Click **OK**.



**Tip:** To change the administration password again, you can use the Active Directory Users and Computers tool. To open the **Change Administration Password** dialog box, launch the **Active Directory Users and Computers tool**, right-click the **SafeWord** folder under the tree directory, and select **Change Administration Password**.

## Changing the User Center default password

Before giving users access to the User Center, you should access it yourself to customize your administrative password. The first time you access the User Center, you will automatically be prompted to change its default password. It is highly recommended that you change this password, as the default password is the same for every installation of SafeWord, and is therefore insecure. You will only have to change this password the first time you open the User Center. You can only change the administration password from the machine where the User Center is installed.

To customize the administration password, do the following:

1. Open the User Center by selecting **Start -> Programs -> Secure Computing -> SafeWord -> User Center**, or by launching the Web page: *https://localhost:**port**/usercenter*.



**Important:** Only administrators can access the User Center from the Start menu. Your users must use the URL and browse to it.

**Note:** Boldface text in the URL indicates text that will vary based on the machine and port being used.

The Change your administration password window appears.

**Figure 2-10. Change Your Administration Password window**



2. Enter and re-enter the new password in the appropriate fields, then click **Submit** to complete the password change.

---

## Ensuring password security

In order to allow the SafeWord components to connect to the Administration Service automatically, the passwords that you just changed are stored as part of the component's configuration. Because of this, the physical and network security of the computers where you install the SafeWord components is of paramount importance. You must ensure that these machines are physically secure and that they do not have any publicly-accessible directories.

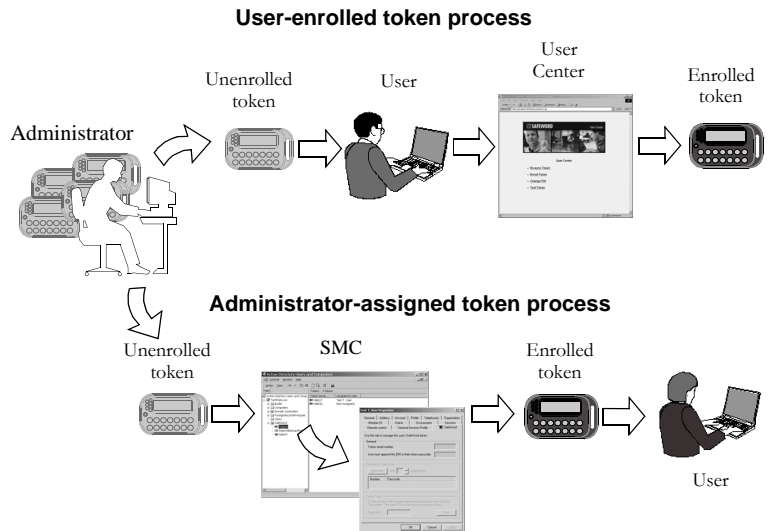


**Security Alert:** *Physical security must be maintained specifically on the C:\winnt\ScCADUserExt directory, on any machine where you have installed the SMC, and the C:\Program Files\<<INSTALL\_DIR>\SERVERS\Web\Tomcat\ directory.*

## Preparing and deploying tokens

There are two available paths for deploying tokens. The first lets your users enroll their own tokens using the SafeWord User Center (see User-enrolled token process in Figure 2-11). This option removes the burden of manual entry by you, and is described in “Self-enrollment with the User Center” on page 2-22.

**Figure 2-11. Token deployment processes**



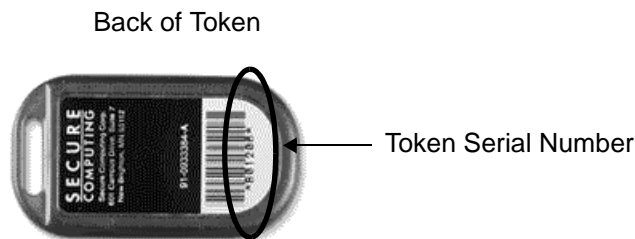
In the second path, you can enroll and assign tokens using the SMC tool (see Administrator-assigned token process in Figure 2-11). This option is described in “Administrator-assigned tokens using the SMC” on page 2-20.



**Security Alert:** Directories where you have installed the User Center must **NOT** be accessible to the public.

Each token has a serial number on its back that SafeWord uses to create an association between the token and a user (see Figure 2-12).

**Figure 2-12. SafeWord token**



## Administrator-assigned tokens using the SMC

If you prefer to assign tokens to users, do the following:

1. Launch the Active Directory Users and Computers tool by selecting **Start -> Programs-> Administrative Tools-> Active Directory Users and Computers**.
2. On the left side of the window, select the **Users** folder. A list of users appears on the right side of the window.



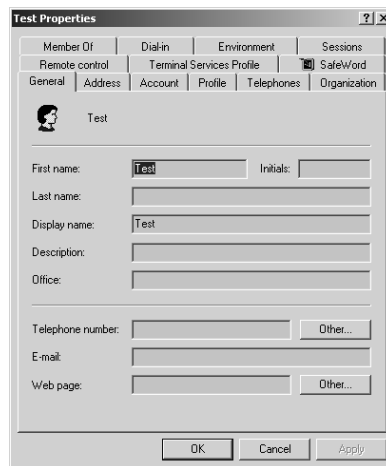
**Important:** You may choose to have users in a container other than the default Users folder. This container is sometimes referred to as an “organizational unit” and it is special because it has a security boundary. You can delegate administration of this organizational unit, whereas administration of the default Users folder cannot be delegated. The default Users folder is a regular container and is named Users. Creating user accounts in containers other than the default Users folder is your prerogative.

3. Locate the user to whom you will be assigning a token, then right-click the user’s name and select **Properties** to display the user’s Properties window.



**Tip:** If some of your users will share a token, assign the same token serial number to each user who will share it.

**Figure 2-13. User Properties window**



4. Click the **SafeWord** tab.

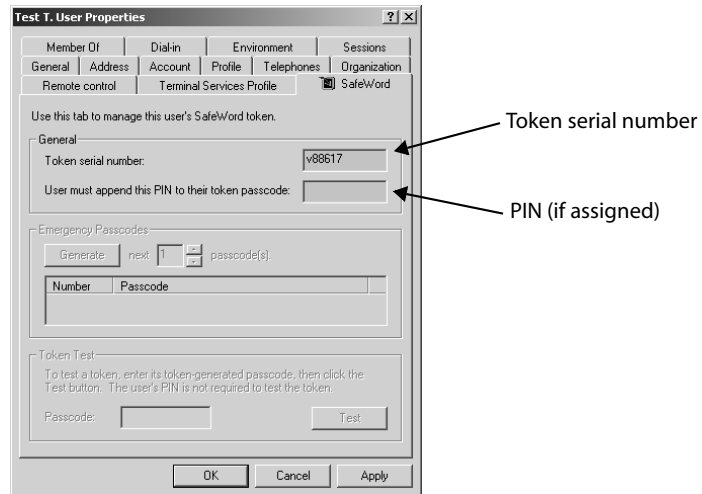


**Tip:** If you get an error while attempting to view the SafeWord tab for a user, the administration service has rejected the user’s client certificate. This occurs when the SMC has been re-installed. Remove the user’s client certificate to access the SafeWord tab of their Properties window (see “Reinstalling a server or the SMC” on page 4-29).

5. Select a SafeWord token, and locate the serial number on the back.

- In the **Token serial number** field (found in the General section of the SafeWord tab), enter the token's serial number.

**Figure 2-14. Populated  
Token Serial Number  
field**



Requiring a PIN with a user passcode adds a second layer of security to your system. If you will require users to authenticate with a token passcode and PIN, they must append the PIN to the end of the passcode. If they do not know their PIN, they will be denied access.



**Tip:** Users can change their PIN by choosing **Change PIN** from the User Center (see “Adding or changing PINs with the User Center” on page 2-25).

- If you will be assigning a PIN to this user, enter a four-digit PIN in the field labeled **User must append this PIN to their token passcode**. Otherwise, leave the field empty.
- Click **Apply**. Clicking Apply activates the lower portion of the window, allowing you to generate emergency passcodes or test the token.
  - If you will not be generating emergency passcodes or testing the token at this time, click **OK** to close the window.
  - If you want to generate emergency passcodes, see “Generating emergency passcodes” on page 4-7.
  - If you want to test this token, see “Testing tokens with the SafeWord Management Console” on page 2-26.
- Distribute this token to the appropriate user. Be sure to tell them if they will need to append a PIN to the end of their passcode.
- Repeat the procedure for each SafeWord token user.

## Self-enrollment with the User Center

Users can self-enroll their tokens and add or change their PIN by using the User Center. This saves you time and provides users the opportunity to test their token. Since users must browse to the User Center, they will need to know the User Center URL in the following format:

*https://**machinename:port**/usercenter.*

**Note:** Boldface text in the URL indicates text that will vary based on the machine and port being used.



**Tip:** Administrators can access the User Center by selecting **Start -> Programs -> Secure Computing -> SafeWord -> User Center** or by browsing to it using the URL.



**Important:** Only administrators can access the User Center from the Start menu.

To enroll their tokens instruct your users to:

1. Open the User Center by launching the following Web site:  
*https://**machinename:port**/usercenter*

**Note:** In the URL, **machinename** is the computer where the SafeWord Server is installed, and **port** is the port on which the User Center is installed. The default port is 8443.



**Tip:** As an alternative, you can use the IP address in place of the machine name in the URL.

The User Center Home Page appears.

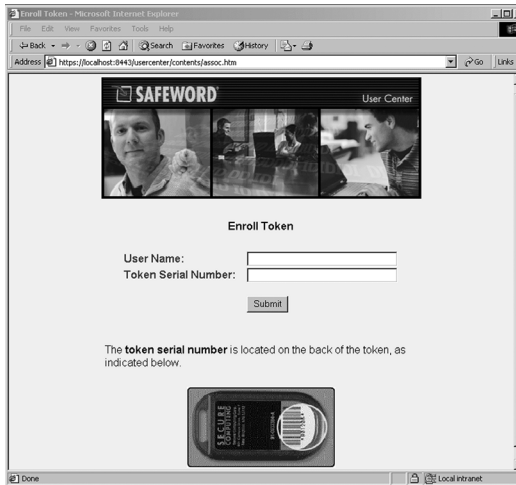
**Figure 2-15. User Center Home Page window**



2. Click **Enroll Token**. The User Token Enrollment window appears.



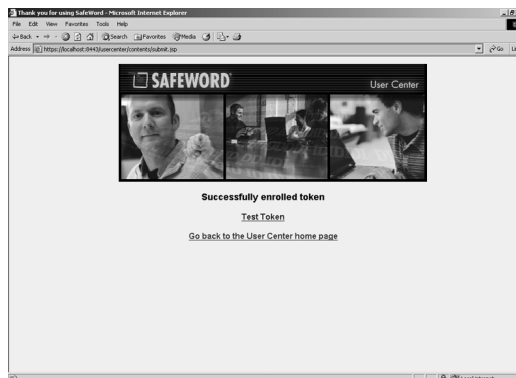
**Figure 2-16. User Token Enrollment window**



3. Enter your user name in the **User Name** field.
4. Enter the token serial number found on the back of the token into the **Token Serial Number** field.
5. Click the **Submit** button.

The Successfully Enrolled Token window appears.

**Figure 2-17. Successful Enrollment window**



The token is now enrolled in SafeWord. You may also choose to test the token from this window.

6. To test the token, click **Test Token** and go to "Testing tokens with the User Center" on page 2-27.

---

## Adding or changing PINs

Once a token is enrolled into SafeWord, you may also choose to use a PIN along with token-generated one-time passcodes. PINs add another layer of security to your system.

Choosing to add a PIN means that each time users authenticate using a one-time passcode generated by their token, they must append their PIN to the end of their passcode. PINs can be added by administrators or by users. If your users will be adding their own PINs, see the section called “Adding or changing PINs with the User Center” on page 2-25. If you will be assigning PINs to users, continue to the next section.

---

### Adding or changing PINs with the SafeWord Management Console

---

As the administrator, you can use either the SafeWord Management Console or the User Center to add or change PINs for users.

You can add PINs for all users, or you can give all or some of them the option to decide for themselves whether or not they want to use a PIN. To add or change a PIN with the SafeWord Management Console, do the following:

1. Open the Active Directory Users and Computer tool by selecting **Start -> Programs -> Administrative Tools -> Active Directory Users and Computers**.
2. Click the **Users** folder on the left side of the window.
3. Double click the name of the user for whom you are assigning a PIN.
4. When the user’s Properties window appears, select the **SafeWord** tab.
5. To assign a new PIN or change an existing one, enter the desired PIN in the field labeled **User must append this PIN to their token passcode**.
6. Click **Apply** or **OK**.

The PIN is now required each time this user authenticates using passcodes generated with their assigned token.

To specify that the user does not need to use a PIN, simply clear the existing PIN from the field labeled **User must append this PIN to their token passcode**.

## Adding or changing PINs with the User Center

As the administrator, you can add or change PINs for users with the User Center. If you will allow your users set their own PIN, you must supply them with the URL for the User Center. If the user already has a PIN associated with their token, they will also need the current PIN in order to change to a new PIN.

To add or change a PIN using the User Center:

1. Open the User Center by launching the following Web page:  
*https://**machinename**:**port**/usercenter.*

**Note 1:** In the URL, **machinename** is the name of the computer where the SafeWord Server is installed, and **port** on which the User Center is installed. The default port number is 8443.

**Note 2:** Boldface text in the URL indicates text that will vary based on the machine and port being used.

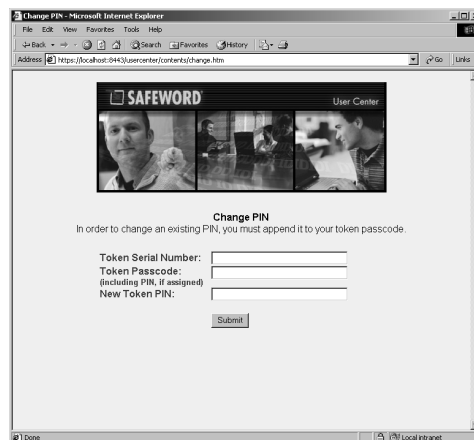


**Tip:** As an alternative, you can use the IP address in place of the machine name in the URL.

2. When the User Center Home Page window appears, click **Change PIN**.

The Change PIN window appears.

**Figure 2-18. Change PIN window**



3. Enter the Token Serial Number from the back of your token into the **Token Serial Number** field.
4. Enter a Token Passcode in the **Token Passcode** field. Be sure to include your PIN if applicable.
5. Enter your desired four-digit PIN in the **New Token PIN** field.
6. Click the **Submit** button.

The Successfully changed PIN window appears. You must use the new PIN when logging in with token-generated passcodes.

**Figure 2-19. Successful PIN Change window**



If your users will test tokens with the User Center, provide them with the information found in the next section. If you prefer to test a token yourself, see “Testing tokens with the SafeWord Management Console”.

---

## Testing tokens

Once a token has been assigned and enrolled, it should be tested. As with most procedures in SafeWord, you may choose to test tokens yourself with the SafeWord Management Console, or you may allow users to test them with the User Center. The sections that follow explain both procedures.

---

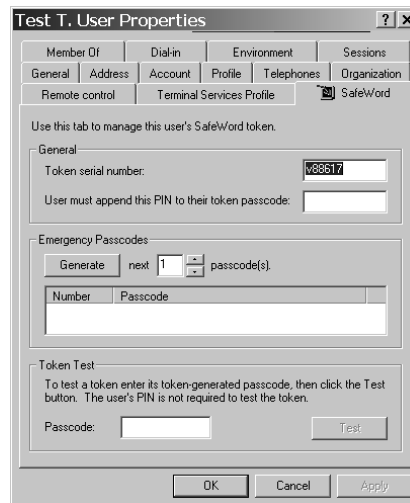
### Testing tokens with the SafeWord Management Console

---

As the administrator, you can choose to test a token before distributing it to a user. A token test option is located on the SafeWord tab of the Active Directory Users and Computers tool. To test a token, do the following:

1. Launch Active Directory from **Start -> Programs -> Administrative Tools -> Active Directory Users and Computers**.
2. Select the **Users** folder on the left side of the window.
3. Right click the user whose token you are testing, then select **Properties**.
4. Click the **SafeWord** tab.

**Figure 2-20. Testing tokens with the Active Directory Users and Computers tool**



5. Confirm that the **Token serial number** field is populated with the serial number of the token you are testing.
6. Generate a one time passcode using the token and enter it in the **Passcode** field under Token Test.
 

**Note:** You do not need to append a PIN to the end of the Passcode in the Management Console, even if the user requires a PIN to log in.
7. Click the **Test** button.
 

A window appears indicating the token has been tested successfully.
8. Click **OK**.

---

## Testing tokens with the User Center

---

Your users can test their token using the User Center. To test a token with the User Center, instruct your users to do the following:

1. Open the User Center by launching the following Web page:  
[https://\*\*machinename\*\*:\*\*port\*\*/usercenter](https://machinename:port/usercenter).
 

**Note 1:** In the URL, **machinename** is the computer where the SafeWord Server is installed, and **port** is the port on which the User Center is installed. The default port number is 8443.

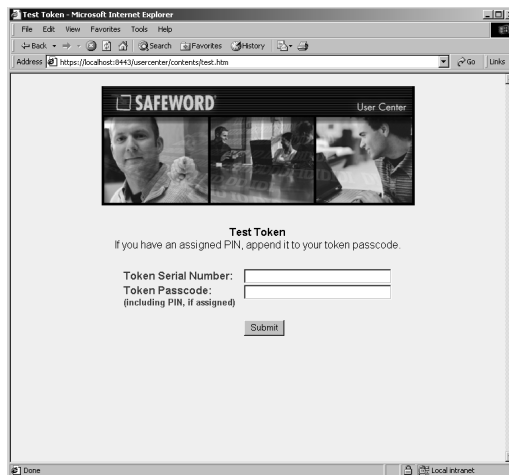
**Note 2:** Boldface text in the URL indicates text that will vary based on the machine and port being used.
2. When the User Center Home Page window appears, click **Test Token**.

**Figure 2-21. User Center Home Page window**



The Test Token window appears.

**Figure 2-22. Test Token window**



3. Enter the Token Serial Number in the **Token Serial Number** field.
4. Enter a token-generated passcode in the **Token Passcode** field. Remember that if a PIN has been added to this token, it must be appended to the end of the passcode on this field.
5. Click the **Submit** button.

A Successful Token Test window appears, informing you that this token has been successfully tested.

# Setting up Strong Authentication

---

## About this chapter

This chapter provides information on configuring the SafeWord agent(s) you selected during installation.

This chapter includes the following topics:

- ◆ “The SafeWord Internet Authentication Service (IAS) Agent” on page 3-2
- ◆ “The SafeWord Agent for Web Interface” on page 3-5
- ◆ “SafeWord Secure Access Manager (SAM) Agent” on page 3-7
- ◆ “The Outlook Web Access (OWA) Agent” on page 3-10
- ◆ “Agent configurations” on page 3-13
- ◆ “Configuring alternative group policies” on page 3-17

## The SafeWord Internet Authentication Service (IAS) Agent

3

SafeWord's IAS Agent works with Microsoft's IAS RADIUS to provide SafeWord strong authenticated remote access through the Microsoft IAS RADIUS server. Once configured, users who access their network remotely will be required to enter a SafeWord token-generated passcode in order to access the network.

The SafeWord IAS Agent is available as one of the SafeWord installation options, and supports the following password protocols:

- ◆ PAP
- ◆ CHAP
- ◆ MS-CHAP version 1
- ◆ MS-CHAP version 2

The agent comes with an administration tool that is used for configuring the authentication engine, logging parameters, group authentication policies, and MPPE support. This section describes how to configure the authentication engine, change logging settings, set authentication policies, and configure Microsoft Point-To-Point Encryption (MPPE) support.

---

### IAS Agent default configurations

If the SafeWord IAS Agent was installed as part of the SafeWord installation, its default configuration options were set as follows:

**Table 3-1. Default IAS agent settings**

Attribute	Default setting
Authentication Engine	On host machine chosen during installation
Authentication Group Policy	All users authenticate using Safeword
MPPE Support	Enabled
Logging	Disabled

**Note:** Errors are logged to the Windows Event Viewer, even if logging functions are disabled.

You can change any of these settings using the administration tool as described in the following sections.



## Launching the administration tool

To launch the administration tool do the following:

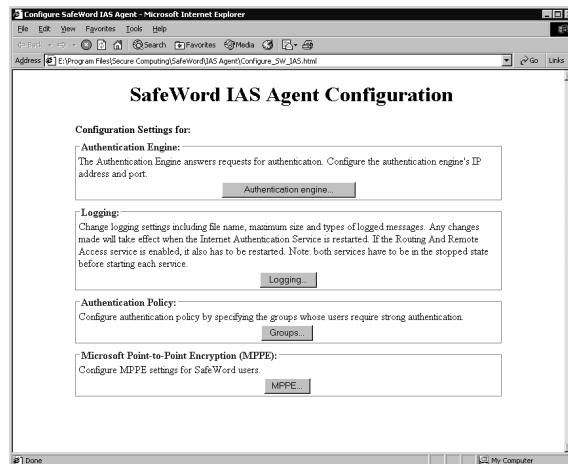


**Important:** You must configure the SafeWord IAS Agent from the machine where it is installed. You cannot configure it remotely.

1. Go to the machine on which the agent is installed.
2. Select **Start -> Programs -> Secure Computing -> SafeWord -> IAS Agent -> Configure IAS Agent**.

The Agent Configuration window appears.

**Figure 3-1. Agent Configuration window**



To configure the Authentication Engine, Logging, and Authentication Policy, see “Agent configurations” on page 3-13 of this guide.

## Configuring MPPE support

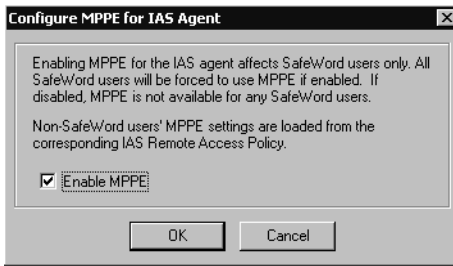
The IAS agent supports the MPPE protocol when using MS-CHAP version 1 or 2 to authenticate. MPPE is enabled by default for SafeWord users. Non-SafeWord users will still use the corresponding SafeWord Policy MPPE settings.

To configure MPPE support, do the following:

1. On the SafeWord IAS Agent Configuration window, click the **MPPE** button.

The Configure MPPE for IAS Agent window appears. By default MPPE is enabled.

**Figure 3-2. Configure MPPE for IAS Agent window**



2. To disable MPPE, clear the check box.
3. Click **OK**.

To configure the Authentication Engine, Logging, and Group Authentication Policies, see "Agent configurations" on page 3-13.

## The SafeWord Agent for Web Interface

The SafeWord Agent for Web Interface is the strong authentication component you install on your Citrix Web Interface server. It provides the link to the SafeWord Server by routing user access requests to the Authentication Engine which verifies user names and passcodes. Once authenticated, users are allowed access, otherwise access is denied.

### Configuring the SafeWord Agent for Web Interface

In order for your Citrix users to strongly authenticate with SafeWord, you must configure the SafeWord Agent for Web Interface. When the SafeWord Agent is installed on Citrix Web Interface 2.0, the SafeWord configuration options for the Authentication Engine, Logging, and Authentication Policy are a part of the Web Interface Administration tool.



**Important:** You can only configure the SafeWord Agent for Web Interface at the machine where Citrix is installed. You cannot configure these settings remotely. When the SafeWord Agent is installed on Citrix Web Interface 3.0, the SafeWord configuration options for the Authentication Engine, Logging, and Authentication Policy are not part of the Web Interface Administration Tool.

To set up strong authentication, do the following:

1. Launch the administration tool by starting Internet Explorer on the computer where you have installed the Citrix component.



**Important:** You must use Internet Explorer to configure the Web Interface for Citrix Administration tool. You cannot configure it using Netscape Communicator.

2. Browse to the Web Interface Admin page.
3. Select **Authentication**.

The Authentication Settings window appears.

4. Scroll down to the Explicit login settings pane.
5. Enable the following:
  - a. for Web Interface 2.0, enable (check) **Use SafeWord for strong authentication**.
  - b. for Web Interface 3.0, enable **Enforce 2-factor authentication** and select the **SafeWord** option.

**Note:** All SafeWord authentication configuration is set within the Explicit login settings pane of the Authentication Settings window.

**Note:** If you are using Citrix Web Interface version 3.0, access the Authentication Engine

configuration options by selecting **Start -> All Programs -> Secure Computing -> SafeWord -> Configure Web Interface Agent**. On the window that displays, select the **Authentication engine** button. To continue the procedure, skip to step 6.

6. To configure the location of the Authentication Engine that the agent will use, select the **Authentication engine** button.

To configure the Authentication Engine, Logging, and Authentication Policy, see "Agent configurations" on page 3-13.

## SafeWord Secure Access Manager (SAM) Agent

The SafeWord SAM Agent is an optional add-on component used with SafeWord for Citrix and the Secure Access Manager. The agent installs directly on top of your SafeWord for Citrix installation.

### SAM Agent default configurations

When you installed the Agent, its default settings are as follows:

Table 3-2. Default SAM agent settings

Attribute	Default setting
Authentication Engine	On host machine chosen during installation
Logging	Disabled
Authentication Policy	All users authenticate using Safeword

**Note:** Errors are logged to the Windows Event Viewer, even if logging functions are disabled.

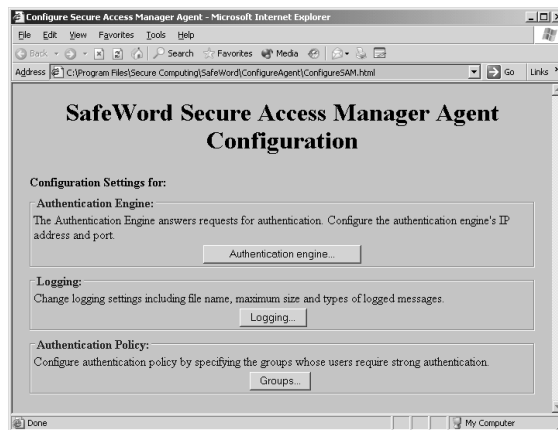


**Important:** You must configure the Secure Access Manager Agent from the machine where it is installed. You cannot configure it remotely.

### Launching the administration tool

1. Select **Start -> Programs -> Secure Computing -> SafeWord -> Configure Secure Access Manager Agent**.

Figure 3-3. Agent Configuration window



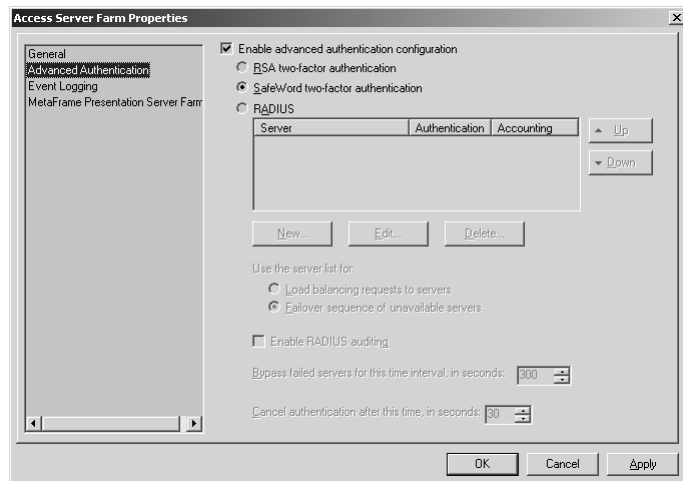
For information on configuring the Authentication Engine, Logging, and Authentication Policy, see “Agent configurations” on page 3-13.

## Configuring MSAM 4.0

If you are running MSAM 4.0, and want to enable SafeWord authentication for a given logon point, the configuration process is as follows:

1. Launch the Management Console by selecting **Start -> Programs -> Citrix -> Management Consoles -> Access Suite Control**.
2. In the left pane of the Management Console, right-click on the **MSAM Farm** icon, then select **Edit Farm Properties**.
3. In the Access Server Farm Properties window, click (highlight) **Advanced Authentication** (see Figure 3-4).

**Figure 3-4. Access Server Farm Properties window**



4. Select the **Enable Advanced Authentication** check box, then select **SafeWord two-factor authentication**.
5. Click **Apply**, then click **OK**.

This enables advanced authentication for the given server farm, and specifies that SafeWord will be used for authentication.

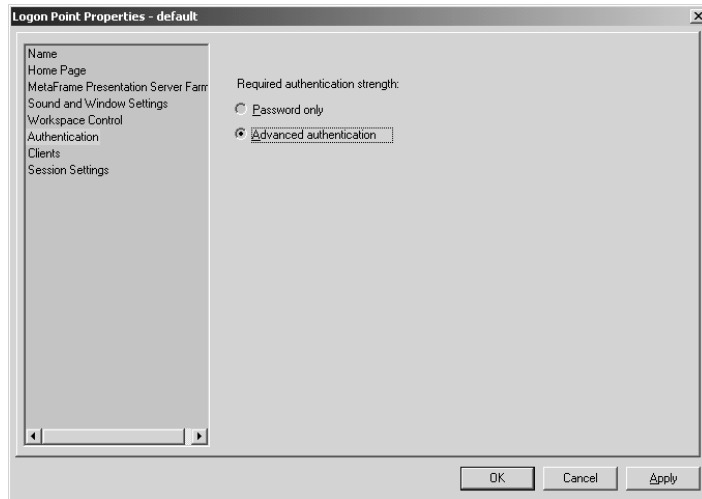
Next, you will specify that SafeWord authentication will be used to protect a given logon point.

**Note:** Any logon point requiring SafeWord advanced authentication must have the SafeWord SAM Agent present on the machine that you want to protect.

6. In the Management Console left pane, expand the Policies node, then expand the Logon Points node.

7. Highlight the default (user -assigned) Logon node, then select **Edit Logon Point** (see Figure 3-5).

**Figure 3-5. Logon Point Properties page**



8. In the Logon Point Properties page, highlight **Authentication**, then select **Advanced Authentication**.

## The Outlook Web Access (OWA) Agent

SafeWord's OWA Agent works with the Microsoft Exchange Server to provide strong authenticated access through the Microsoft Exchange OWA component. When installed, users who access their e-mail remotely using OWA will be prompted for a SafeWord token-generated passcode in order to access the network.

**Note:** When installing the OWA Agent in an Exchange front-end back-end network topology, only the front-end server needs to have the OWA Agent installed on it.

The SafeWord OWA agent uses an administration tool for configuration, and installs on the same machine hosting Exchange OWA (typically a Windows 2000/2003-based Web server).



**Important:** The SafeWord OWA Agent does not currently support Microsoft Exchange 2003's native forms-based authentication mode.

---

### OWA Agent default configurations

When you install the SafeWord OWA Agent, its default configurations are set as follows:

**Table 3-3. Default OWA agent settings**

Attribute	Default setting
Authentication Engine	On host machine chosen during installation
Authentication Policy	All users authenticate using Safeword
Session and idle timeouts	Enabled at 3600 and 300 seconds respectively
Logging	Enabled for errors
Require SSL connections	Enabled by default

**Note:** Errors are logged to the Windows Event Viewer, even if logging functions are disabled.

Agent parameters are configured using the administration tool. The following sections explain how to reconfigure these settings.



---

## Launching the administration tool

---

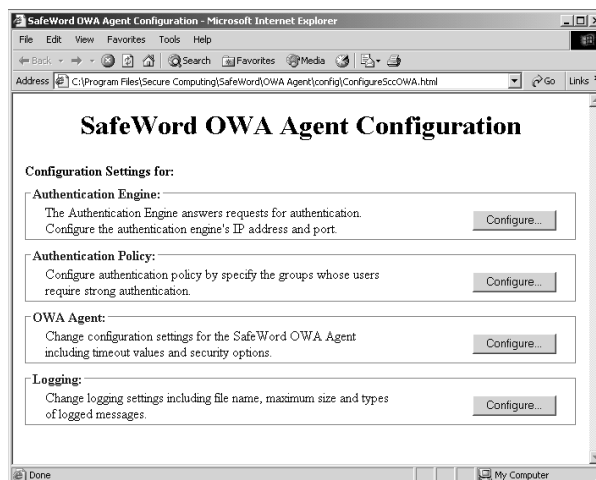


**Important:** You must configure the SafeWord OWA Agent from the machine where it is installed. You cannot configure it remotely.

1. Go to the machine on which the agent is installed.
2. Select **Start -> Programs -> Secure Computing -> SafeWord -> OWA Agent -> Configure OWA Agent**.

The Agent Configuration window appears.

**Figure 3-6. Agent Configuration window**



For information on configuring the Authentication Engine and Authentication Policy settings, see “Agent configurations” on page 3-13 of this guide.

For specific details on configuring Logging for the OWA Agent, please see “Changing Logging settings” on page 3-14 of this guide.

---

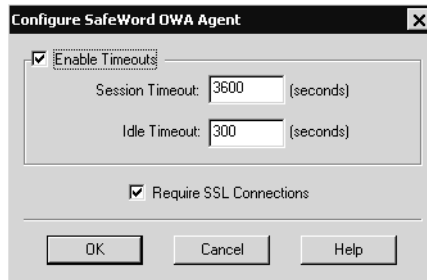
## Configuring the OWA Agent

To configure the OWA Agent, do the following:

1. In the Agent Configuration Window, click the **OWA Agent** button.

The Configure OWA Agent window appears.

**Figure 3-7. Configure OWA Agent window**



2. Modify the following fields as needed:
  - ◆ **Enable timeouts** (selected by default -- click to clear): enables or disables time limits for an active or idle (inactive) session.
  - ◆ **Session timeout** (3600 seconds default): the duration (in seconds) for a single session.
  - ◆ **Idle timeout** (300 seconds default). the duration (in seconds) of an idle (inactive) session.
  - ◆ **Require SSL connections** (selected by default): requires that all login attempts are via SSL (https) connection.

**Note:** The *Require SSL Connections* option is enabled only if a certificate is present in the Exchange OWA site, in which case the option will be automatically turned on at installation time.



**Security Alert:** Operating an Exchange OWA site without a server certificate and SSL is not recommended.

3. When done, click **OK**.
4. Restart the IIS service.

For details on obtaining and installing a server certificate, please refer to the IIS and Microsoft Exchange OWA documentation.

---

## OWA logging settings

The SafeWord OWA agent logging function records two types of logs: Extension and Filter logs. Filter logs are created every time a user accesses an Exchange resource. Extension logs are generated when a non-credentialed user attempts to access an Exchange resource and is required to authenticate.

**Note:** Under certain circumstances, only one set of logs will be created for the OWA Agent. In this case, both the Filter and Extension logs will be combined into one file.

## Agent configurations

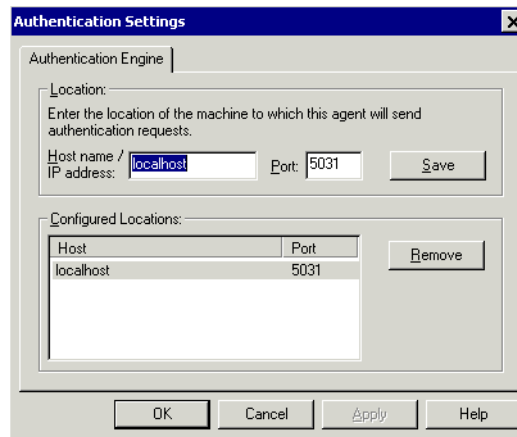
This section contains information on configuring the Authentication Engine, Logging, and Authentication Policy.

### Configuring the Authentication Engine

1. Click the **Authentication Engine** button.

The Authentication Engine window appears.

**Figure 3-8. Authentication Engine window**



2. In the **Host name/IP address** field, enter the Host name or IP address of the machine to which the agent will send authentication requests.
3. In the **Port** field, enter the Port number on which the Authentication Engine will listen for requests.

This port number must match the port number specified for the Authentication Engine.

4. Click the **Save** button. The server appears in the list of configured locations.
5. To remove servers from the Configured Locations list, select the server name from the list and click the **Remove** button.
6. Click **OK**.
7. Restart the IIS service (only required for OWA Agent).



**Important:** If you are configuring multiple servers, repeat the same steps for each server you are configuring.

## Changing Logging settings

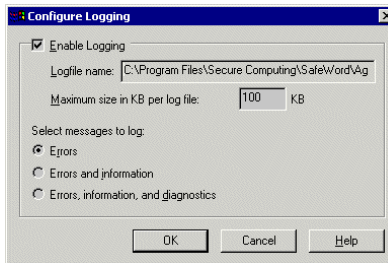
By default, logging functions are enabled for errors. You can modify which events are logged, and where to log them. You may view and manage log records using Windows Event Viewer, or as text files.

**Note:** Errors are logged to the Windows Event Viewer, even if logging functions are disabled.

To configure logging, do the following:

1. Click the **Logging** button on the Agent Configuration window.

**Figure 3-9. Configure Logging windows**



2. Select the **Enable Logging** check box to activate the window.

**Note:** By default, logs are stored in <install\_dir>/SafeWord/Agentlogs).

3. Select the types of messages to log from the following options:
  - ◆ Errors
  - ◆ Errors and information
  - ◆ Errors, information, and diagnostics



**Important:** Login diagnostic information may result in extremely voluminous output. Unless you are troubleshooting a problem, diagnostic logging should be disabled.

4. Click **OK**, then do a service restart as follows:

**Table 3-4. Agent/service restarts**

Agent	Restart...
IAS Agent	IAS Service
Web Agent	IIS Service
SAM Agent	None required
OWA Agent	IIS Service

**Note:** If Routing & Remote Access Server (RRAS) is on the same machine, stop the IAS service and RRAS, restart RRAS, then restart IAS.

## Configuring the Authentication Policy

SafeWord allows you to designate special groups of users who will be required to log on to the system using a SafeWord token. While you could force all your users to use tokens when logging in, this approach may not be flexible enough for your environment.

Instead, you can force a specific Windows group to log in using tokens by using the native Windows user and group management tools to create a global group called `SAFEWORD_USERS` (see Figure 3-10). This is the group into which you would assign specific users to log in using SafeWord tokens.



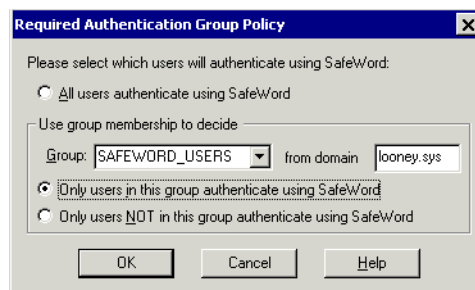
**Important:** You must create global groups before you can apply authentication policies to specific users.

Once users are placed in this special group, you must tell the agent what the group is, and how to treat users in it. The following instructions describe how this is done.

1. Click the **Groups** button on the Agent Configuration window.

The Required Authentication Group Policy window appears.

**Figure 3-10. Required Authentication Group Policy window**



2. You may designate users from specific groups and/or domains who will use SafeWord tokens.

**Note:** This group configuration only affects the groups associated with the SafeWord Agents.



**Important:** Windows 2000 can be installed in either Windows 2000 native mode or pre-2000 compatibility mode. If the operating system was installed in Windows 2000 native mode, the group **Domain Users** must be added to the global group called **pre-2000 Compatible Access** in order for domain queries to be successful.

3. To require all users authenticate using SafeWord strong authentication, select **All users authenticate using SafeWord** then continue to step 5
4. If the group's domain is different from the one displayed in the Internet

Domain field, enter the group's domain in the **from domain** field, then

- ◆ Select a **Group** from the Group list. This will most likely be the global group you created for this purpose.
- ◆ Select either:
  - Only users in this group authenticate using SafeWord

Or

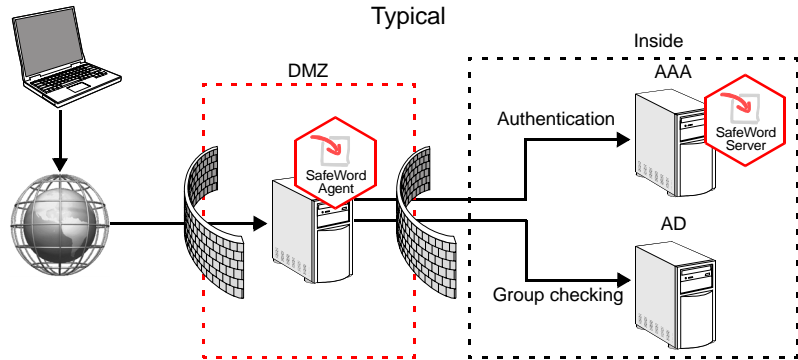
- Only users NOT in this group authenticate using SafeWord

**5.** Click **OK**.

## Configuring alternative group policies

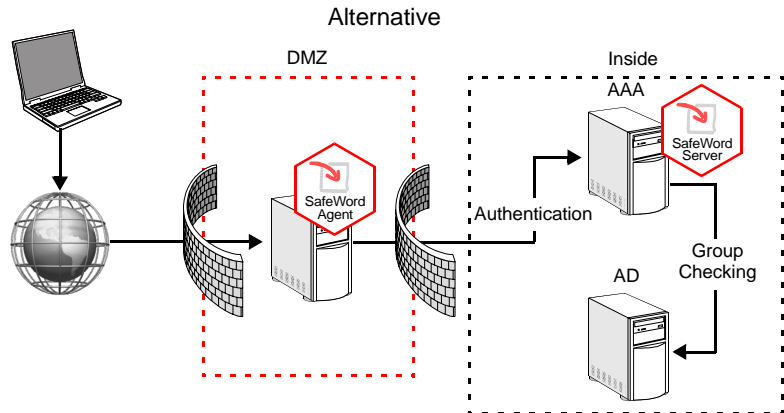
SafeWord's default configuration should suit the majority of network topologies and use cases. The SafeWord Agent is responsible for checking group membership and submitting authentication requests to the authentication engine (see Figure 3-11).

**Figure 3-11. Typical network setup**



Occasionally, the default configuration may not fit a particular network topology or management policies. If computers in a network DMZ do not have anonymous access to Active Directory, the SafeWord Agent is unable to contact Active Directory and read group membership information in order to determine which users require SafeWord authentication. You can configure SafeWord to handle such a scenario (see Figure 3-12).

**Figure 3-12. Alternative network topology**



In this configuration, group membership checking is done by the SafeWord server (rather than the agent). Since the server will typically be running inside the trusted network, it should have no difficulty obtaining the necessary information from Active Directory.

To configure the alternative network topology, do the following:

1. On the computer in the DMZ running the SafeWord agent, use the group configuration window (refer to “Configuring the Authentication Policy” on page 3-15) to force **all users to authenticate using SafeWord**. This will forward ALL authentication requests to the SafeWord server.
2. On the computer inside the network running the SafeWord server, locate the file `INSTALL_DIRECTORY\SERVERS\Shared\scservers.ini`.
3. Locate the line that starts with  

```
#GroupsAuthenticationRequiredClass=securecomputing.yellowstone...
```
4. Modify the line by removing the “#” sign from the beginning of that line.
5. Navigate to  
`INSTALL_DIRECTORY\SERVERS\AAAServer\GroupDiscrimination`.
6. Locate and open the HTML file called `ConfigureGroupPolicy.html`.

**Figure 3-13. Group Discrimination configuration page**



This page will launch configuration dialogs to specify logging and authentication policy settings. This enables the server, if configured, to decide the authentication policy that determines a user's need for authentication. To enable this functionality you must edit the `<INSTALLDIR>\SERVERS\Share\dScServers.ini` file and uncomment the line that specifies the setting for `GroupsAuthenticationRequiredClass`.

**Configuration Settings for:**

**Logging:**  
 Change logging settings including file name, maximum size and types of logged messages.

**Authentication Policy:**  
 Configure authentication policy by specifying the groups whose users require strong authentication.

7. Change the logging and group policies as needed. Refer to “Configuring the Authentication Policy” on page 3-15 for additional information.
8. Restart the SafeWord Authentication Engine service

**Note:** Please note that in this topology it is vital that your SafeWord Authentication Engine service is up and running constantly; otherwise, neither the SafeWord nor the non-SafeWord users will be able to log on to your system. The best way to ensure this is to set up your system with multiple SafeWord servers, as described in section “Configuring multiple servers” on page 4-21.



## CHAPTER 4

# Miscellaneous Administrative Tasks

---

### About this chapter

This chapter provides information on working with the SafeWord database, server management, reinstallation procedures, and running SafeWord in a non-Active Directory environment.

This chapter includes the following topics:

- ◆ “Using the Auto Updater” on page 4-2
- ◆ “Token-related tasks” on page 4-3
- ◆ “SafeWord server-related tasks” on page 4-15
- ◆ “Configuring multiple servers” on page 4-21
- ◆ “Reinstalling a server or the SMC” on page 4-29
- ◆ “Running SafeWord without Active Directory” on page 4-30

## Using the Auto Updater

# 4

The Auto Updater allows you to view and/or automatically update your SafeWord software with new features and patches as they become available. It runs automatically when the SMC is accessed, and only if updates are available. On other SafeWord components, it can be launched manually. You can download and install any or all the updates at anytime.



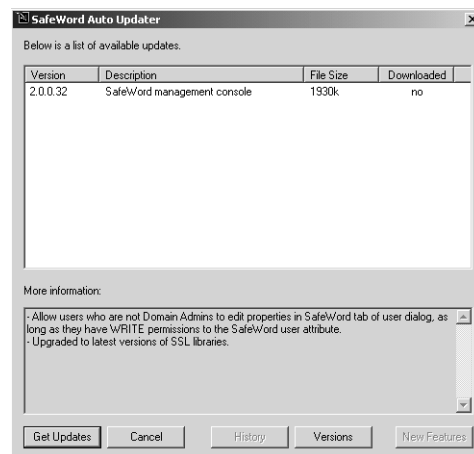
**Important:** *Manual downloading and installing of updates is not recommended, as it can leave your system in an unstable state. If you download and run updates manually, be sure to install them in the same order in which they are listed in the Auto Updater.*

To manually run the Auto Updater or view the available updates, do the following:

1. Select **Start -> Programs -> Secure Computing -> SafeWord -> AutoUpdater -> Update Secure Computing Products.**

**Note:** *If a new version of AUA is available, you will be prompted to download the newer version.*

**Figure 4-1. Update Agent window**



2. Check the update list to determine if an update is needed.
3. Click the **Get Updates** button.

The updates are downloaded to your computer. When the download is complete, a Download Complete window appears.

**Note:** *Selecting Get Updates will download all available updates. The Auto Updater does not allow a user to choose which updates to download.*

4. To install the updates, click **OK**.
5. To find the list of updates that have been installed on your system, click the **History** button.

## Token-related tasks

This section contains user management information, including how to search for specific token information, create emergency passcodes, and view and delete token records.

If you are going to use SafeWord Gold 3000 tokens, refer to “SafeWord Gold 3000 Tokens” on page A-1.

---

### Resynchronizing tokens

There are occasions when a SafeWord token will get out of synchronization and its generated passcodes will not function properly. If this occurs, you will need to resync the token. To resync a token, do the following:

1. Launch the User Center.

**Figure 4-2. User Center main menu**



2. On the main menu, select **Re-sync Token**. The **Re-sync Token** window appears.

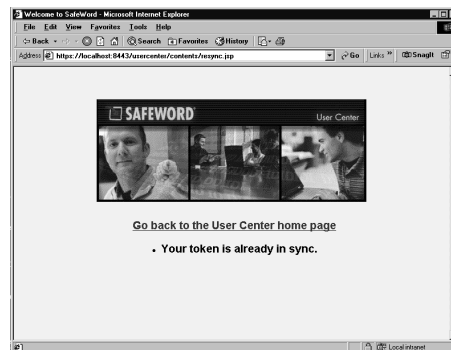
**Figure 4-3. Re-sync Token window**



3. Enter the out-of-sync token's serial number in the Token Serial Number field.
4. Generate a passcode and enter it in the first Token Passcodes field. If this token has a PIN assigned to it, append it to the end of the passcode.
5. Generate a second passcode and enter it in the second Token Passcodes field. Append a PIN if applicable.
6. Click the **Submit** button.

The token is now synchronized.

**Figure 4-4. Token in Sync window**

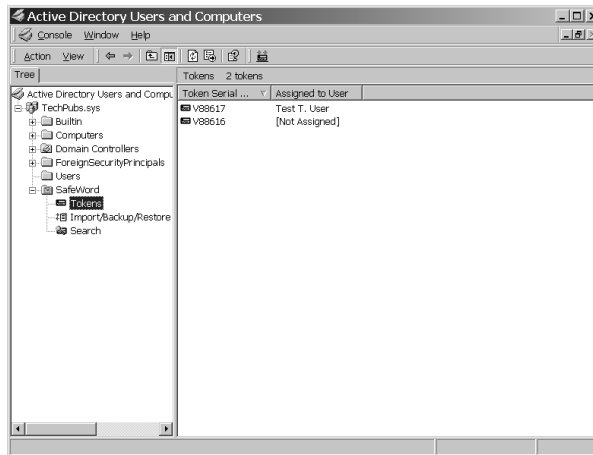


## Searching for unassigned tokens

To search for unassigned tokens, do the following:

1. Open Active Directory Users and Computers tool by selecting **Start -> Programs -> Administrative Tools -> Active Directory Users and Computers**.
2. Expand the **SafeWord** folder at the bottom of the tree on the left side of the window.
3. Click the **Tokens** icon.

**Figure 4-5. Unassigned Tokens window**



Your token serial numbers and assigned users appear in the right pane. Unassigned tokens appear with **[Not Assigned]** under the Assigned to User list.

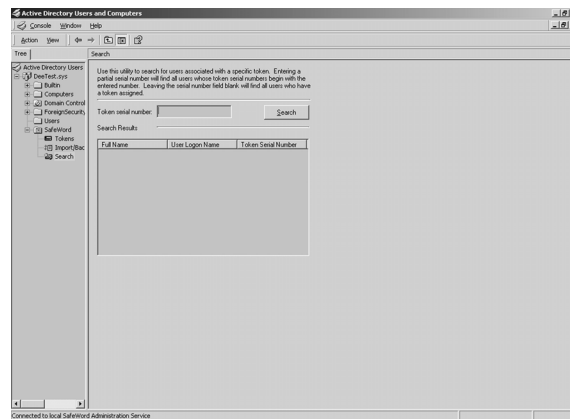
## Finding users associated with specific tokens

There may be times when you will need to find users associated with specific tokens. SafeWord includes a Search utility to help you find the users and their tokens. To use the Search utility, do the following:

1. Open the Active Directory Users and Computer tool by selecting **Start -> Programs -> Administrative Tools -> Active Directory Users and Computers**.
2. Expand the **SafeWord** folder on the left side of the window.
3. Click **Search** on the left side of the window.

The Search Utility window appears. The Search utility allows you to search for users using a specified token serial number.

**Figure 4-6. Search Utility window**



4. Enter the token serial number in the **Token serial number** field.



**Tip:** Entering a partial token serial number will find all users whose token serial numbers begin with the entered number. Leaving the field blank will retrieve all users who have tokens assigned.

5. Click the **Search** button.

The Search Results list the Full Name, User Logon Name, and Token serial numbers.

## Generating emergency passcodes

Emergency passcodes should be used when a user cannot generate passcodes with their token. You can generate emergency passcodes for the user until they are again able to use their token. Emergency passcodes are appropriate if a user forgets their token, or is simply having a problem authenticating using a token-generated passcode.

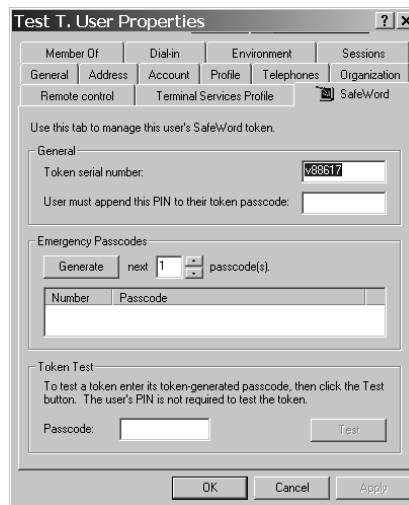


**Important:** When you use an emergency passcode for a user who has forgotten their token (or whose token passcode is not working properly), the user will need to manually resynchronize the token when it is retrieved or fixed. If you have generated five emergency passcodes, the token will produce five identical passcodes when it is used again. The user should generate the same number of token passcodes as emergency codes generated for them. Generating these passcodes with their token without using the passcodes will resynchronize their token.

To generate emergency passcodes for a user, do the following:

1. Open the Active Directory Users and Computer tool by selecting **Start -> Programs -> Administrative Tools -> Active Directory Users and Computers**.
2. Click the **Users** folder on the left side of the window.
3. Double click the user's name that requires an emergency passcode(s) from the list of users on the right side of the window.
4. Click the **SafeWord** tab.

**Figure 4-7. Properties window**



5. Select the number of one-time passcodes to generate. You can generate up to nine emergency passcodes.

**Note:** *The same sequence of passcodes is generated every time you press the Generate button until one of them is successfully used for authentication.*

6. Under Emergency Passcodes, click the **Generate** button.

**Note:** *SafeWord automatically generates the number of passcodes you request, and they appear in the order in which they must be used in the list below the **Generate** button.*

7. Inform the user of their emergency passcodes.



**Important:** *Emergency passcodes must be used in the same sequential order in which they were generated. Emergency passcodes are exactly like token-generated one-time passcodes, and cannot be used more than once.*

---

## Reassigning tokens

When a user leaves your organization, or no longer needs to authenticate using SafeWord strong authentication, they should surrender their SafeWord token. You can reassign the token and its records to another user. You reassign tokens by removing the token serial number from the departing user's properties on the SafeWord tab in the Active Directory Users and Computers tool, adding that serial number to the new user's properties, and distributing the token to the new user. Removing a serial number disassociates the token records from the user. It does not remove that information from your database. When you assign the token serial number to a new user, a new association is created. Once the token is given to the new user, they can generate passcodes for authentication to access your protected resources.



**Important:** *When a token is lost, stolen, or broken, you must completely remove the token records from your database. The records are obsolete without the token. See "Deleting token records from the database" on page 4-11 for information about deleting token records.*

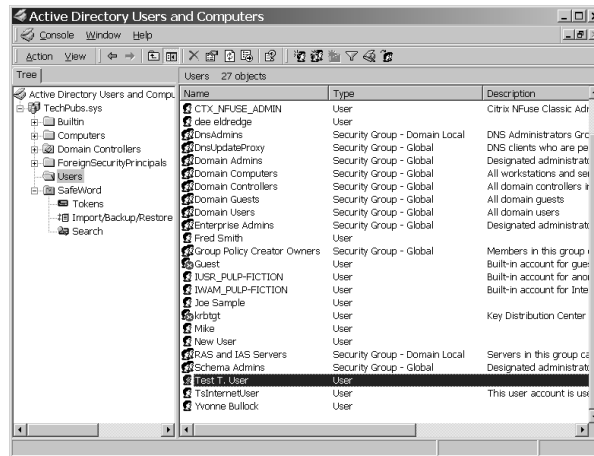
To reassign token records using the Active Directory Users and Computers tool, do the following:

1. Obtain the token from the user who is being disassociated from SafeWord.
2. Open the Active Directory Users and Computers tool by selecting **Start -> Programs -> Administrative Tools -> Active Directory Users and Computers**.



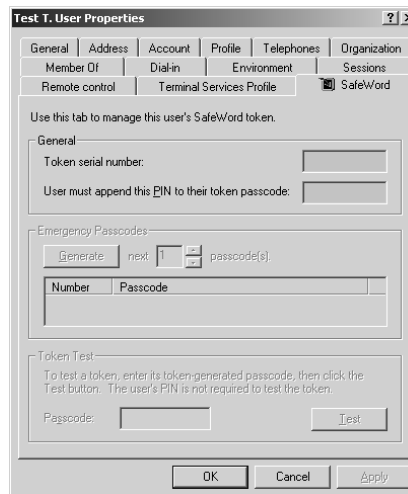
3. Select the **Users** folder.

**Figure 4-8. List of Users window**



4. Right click on the user **Name** for whom you are disassociating token records.
5. Select the **SafeWord** tab in the user's **Properties** window.

**Figure 4-9. User properties with serial number cleared**



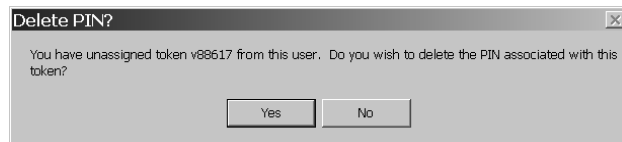
6. Clear the serial number from the **Token serial number** field.
7. Click the **Apply** button.

If you did not delete the PIN assigned to this user, you will be asked if you wish to delete the PIN associated with this token. Deleting a token PIN gives that user the option to add a new PIN when they receive their

new token. If you do not delete the PIN from a user's Properties, they will need to use the assigned PIN even when they receive a new Token.

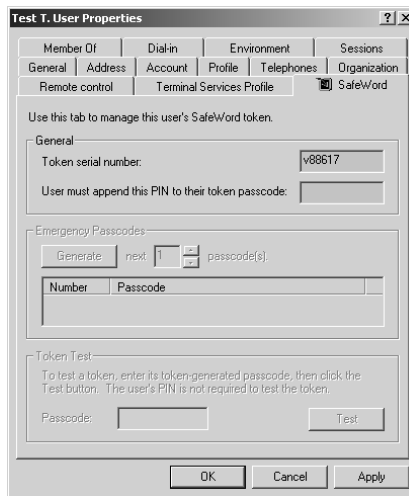
8. If the Delete PIN window appears:
  - a. Click **Yes** to delete the PIN associated with this token.
  - b. Click **No** to leave the PIN assigned to the user from whom this token is being disassociated.
9. Click **OK**.
10. If the Delete PIN window does not appear, skip to step 11.

**Figure 4-10. Delete token window**



11. Open the Properties window for the user to whom you are reassigning the token.
12. Enter the serial number from the back of the token into the **Token serial number** field.

**Figure 4-11. New user with assigned token**



13. Click **OK**.  
You have now created a new association between this user and the token records.
14. Distribute the token to its new user.

## Deleting token records from the database

There are situations when you will need to delete token records from the database. If a token is lost, stolen, or broken, its token records are obsolete since you will not be able to reassign the token to another user. You should delete obsolete token records from your database. Deleting them provides space to add new token records when your organization purchases additional SafeWord tokens. You delete token records using the Active Directory Users and Computers tool.

1. Open the Active Directory Users and Computers tool by selecting **Start -> Programs -> Administrative Tools -> Active Directory Users and Computers**.
2. Expand the **SafeWord** folder on the left side of the window.
3. Click the **Tokens** icon.
4. From the **Token serial number** list on the right side of the window, select one or more tokens to delete and right click the selection.
5. Select **Delete**. If the token is already assigned to a user, the **Token Assigned** message appears to confirm that you really want to delete the token record.



**Important:** If you delete tokens at this point, and then restore the database, all token user associations will be lost.

6. Click **Yes**.

The token records are deleted from the database. If you want to unassign the token without removing the records from the database, see "Reassigning tokens" on page 4-8.



**Tip:** Multiple token records can be selected and deleted simultaneously. You can also highlight a token and use the **Delete** button on the toolbar to delete token records.

## Manually importing token data records

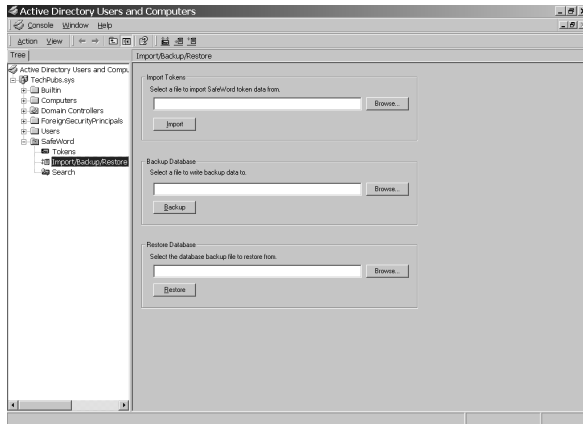
When you registered and activated SafeWord, an **import\_XXXXXXXXX.dat** file (where x is the download time stamp) that contains the programming and data records needed by your tokens was automatically installed on your computer. Once the software and token activation were complete, the token data records were installed in the database and ready for use.

If for some reason you need to manually import token data records, the

process is as follows:

1. Launch the Active Directory Users and Computers tool by selecting **Start -> Programs-> Administrative Tools-> Active Directory Users and Computers**. The Active Directory Users and Computers tool appears.
2. Select the SafeWord folder in the directory tree.

**Figure 4-12. Import/Backup/Restore window**



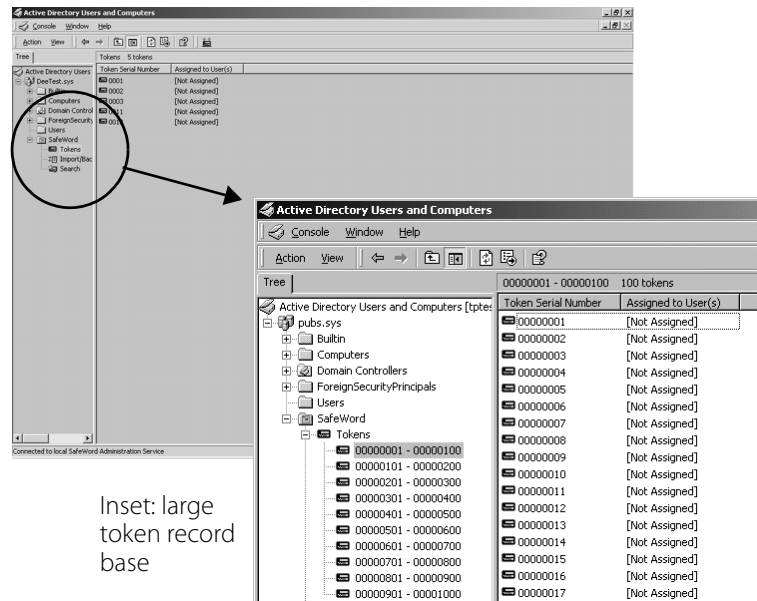
3. Click the **Import/Backup/Restore** option in the left pane of the window.
4. Under Import Tokens, click the **Browse** button.



**Tip:** You can also import tokens by selecting the *Import Tokens* icon on the toolbar.

5. Locate the directory where you saved the files you downloaded during registration and activation.
6. Select **import0.dat**.
7. Click **Open**.
8. When the token data file name appears, click the **Import** button.  
Upon successful import, an Import Successful window appears.
9. Click **OK**.
10. On the left pane of the window, click the **Tokens** icon.

**Figure 4-13. Imported Token Records window**



Inset: large token record base

A list of token serial numbers appears in the right pane of the window. Notice that the tokens have not been assigned to users yet. The inset image shows how the token records are organized into ranges when the total number of imported token records exceeds 500. The ranges are created to simplify management tasks. The grouping is based on the token serial number.

## Manually importing token data records from a CD

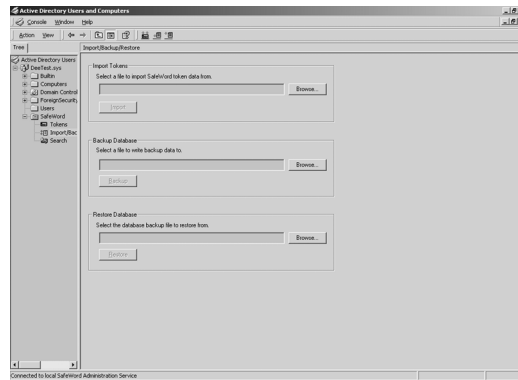
If you do not wish to download your token data records from the Internet, you may request a CD from Secure Computing by contacting Customer Service at 1.800.700.8328 or 1.651.628.1500 (for international callers). You import token records from a Token Data CD using the Active Directory Users and Computers tool.

To import the token data records from a CD, do the following:

1. Insert the Token Data CD into the CD-ROM drive of the computer where you installed the SMC.
2. Open Active Directory Users and Computers by selecting **Start -> Programs-> Administrative Tools-> Active Directory Users and Computers**.
3. Select the SafeWord folder.

**Figure 4-14. Import/Backup/Restore window**

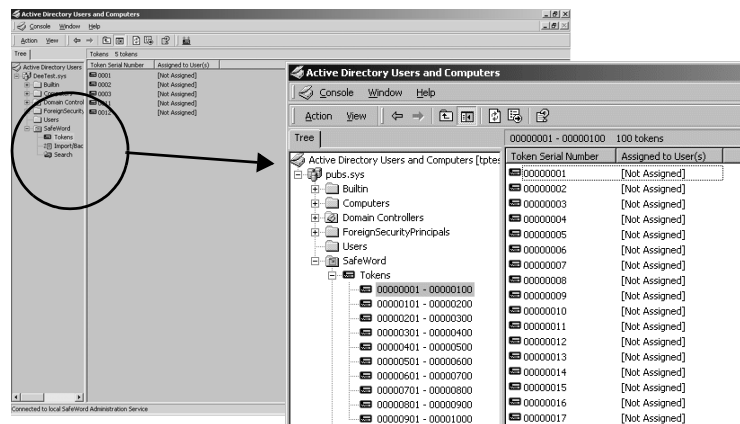
The Active Directory Users and Computers window appears.



4. Click the **Import/Backup/Restore** option in the left pane of the window.
  5. Under Import Tokens, click the **Browse** button.
- ➡ **Tip:** You can also import tokens by selecting the **Import Tokens** icon on the toolbar.
6. Locate the directory on the Token Data CD that contains the import file.
  7. Select **import0.dat**.
  8. Click **Open**.
  9. When the token data file name appears, click the **Import** button.
  10. When the Import Successful window appears, click **OK**.
  11. On the left pane of the window, click the **Tokens** icon.

A list of unassigned token serial numbers appears in the right pane. The inset image shows how the records are organized into ranges - based on serial number - when the number of token records exceeds 500.

**Figure 4-15. Imported Token Records window with large token record base (inset)**



## SafeWord server-related tasks

As the administrator, you can change component ports, audit system events, view event logs, set up a different administration server, setting up logging, and configuring SafeWord servers.

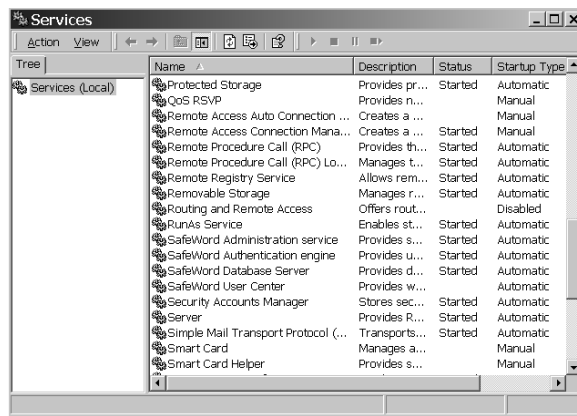
### Stopping and starting servers

If you need to manually stop or start a SafeWord server, do the following:

1. Select **Start -> Programs -> Administrative Tools -> Services**.

The Services utility opens.

**Figure 4-16. Services with SafeWord servers running**



2. Highlight the name of the SafeWord server you want to stop or start.
3. From the File menu, select **Action -> Start or Stop**.
4. Double-click the server's name in the list to display its Properties window.
5. Click the Service Status **Start or Stop** button.



**Tip:** Restarting the Database Server will start all the SafeWord Services.

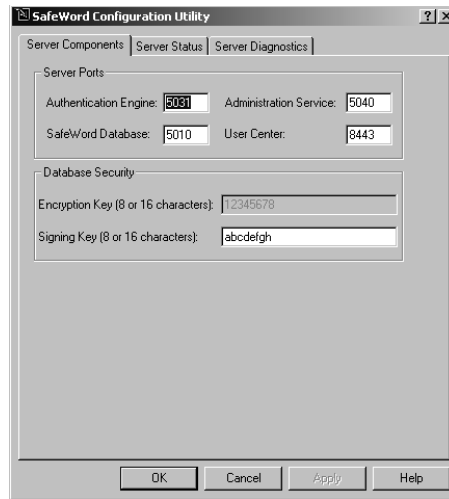
### Changing component ports

You can change the ports over which your SafeWord components are communicating using the SafeWord Configuration Utility. To change ports:

1. Launch the SafeWord Configuration Utility by selecting **Start -> Programs -> Secure Computing -> SafeWord -> SafeWord Configuration**.

**Figure 4-17. Server Components tab of the Configuration Utility**

The SafeWord Configuration Utility window appears.



You may change the ports and signing key that the SafeWord components are using on the Server Components tab.

2. To change a value that is not grayed out, highlight the existing value and enter a new one.
3. When finished using the Configuration Utility, click **OK** to exit.
4. If you want to set up logging of diagnostics information, click the **Server Diagnostics** tab, and continue to the next section.

**Note:** Restart all the SafeWord Services for changes to take effect. For details about starting services, see "Configuring multiple servers" on page 4-21.

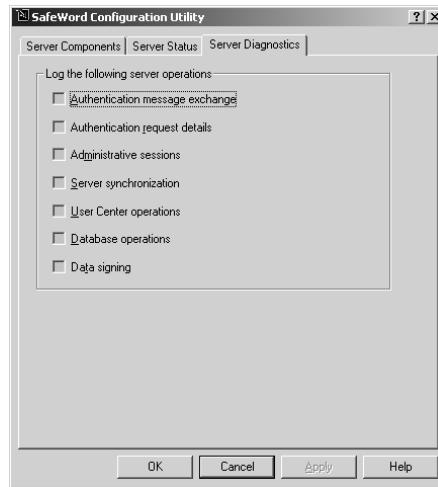
## Logging server diagnostics

Occasionally it is useful to view a detailed log of operations to the various SafeWord components. To turn on detailed diagnostic logging, do the following:

1. Launch the SafeWord Configuration Utility by selecting **Start -> Programs -> Secure Computing -> SafeWord -> SafeWord Configuration**.
2. Select the **Server Diagnostics** tab.



**Figure 4-18. Server Diagnostics tab of the Configuration Utility**



3. Select the check box for any of the following events you want to log:
  - ◆ Authentication message exchange
  - ◆ Authentication request details
  - ◆ Administrative sessions
  - ◆ Server synchronization
  - ◆ User Center operations
  - ◆ Database operations
  - ◆ Data signing
4. When done, click **OK**.

Table 4-1 specifies the locations of the generated diagnostic logs.

**Table 4-1. Server Diagnostic File Locations**

Event Type	File Location
Authentication-related events	<b>InstallationDirectory</b> \SERVERS\AAAAServer\ScsAAA SrvrLog.txt
Administration and server synchronization events	<b>InstallationDirectory</b> \SERVERS\AdminServer\ScsAdSrvrLog.txt
Database and signing events	Files will be distributed between the two locations listed above depending on which component performed the operation
User Center logs	<b>InstallationDirectory</b> \SERVERS\Web\Tomcat\ScsUserCenterLog.txt



**Important:** Restart all the SafeWord Services for changes to take effect. For details

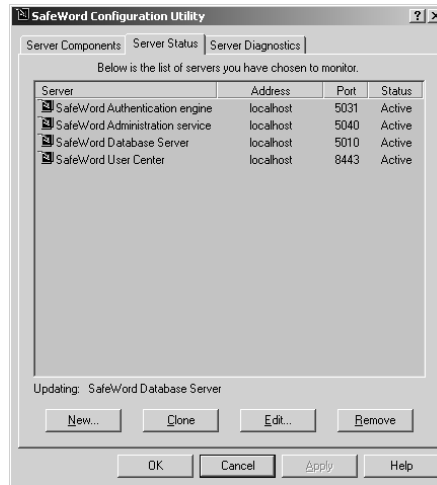
about starting services, see “Configuring multiple servers” on page 4-21.

## Monitoring server status

To check the status of servers you have selected to monitor, do the following;

1. From the SafeWord Configuration Utility, click the **Server Status** tab.

**Figure 4-19. Server Status tab of the Configuration Utility**



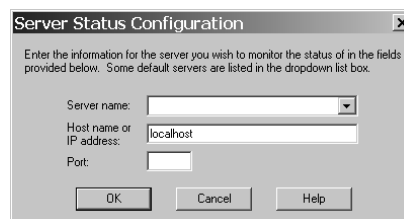
The server name, its address, port and status of the servers you chose to monitor are displayed in the active window.

## Adding servers to the monitored servers list

You can add servers to be monitored using the Server Status tab of the Configuration Utility. To add a server to the monitored server list;

1. On the Configuration Utility’s Server Status tab, click the **New** button.

**Figure 4-20. Server Status Configuration window**



2. In the **Server name** field, enter the name of the server you wish to monitor or choose a server from the drop down list.
3. If the server is not installed on the local machine, enter its host name or IP address and a port number.
4. Click **OK**.  
You are returned to the Server Status tab. The new server name, its address, port and status are displayed in the list of servers.

---

## Removing servers from the monitored servers list

You can remove servers from the monitored list using the Server Status tab of the Configuration Utility. To remove a server from the monitored list, select a server to remove, then click the **Remove** button to remove the server from the list.

---

## Cloning servers

You can clone (copy) servers with their settings to use as templates to create new servers to monitor on the Server Status tab of the Configuration Utility. To clone a server:

1. From the server list, select a server whose settings are similar to those you want to apply to a new server.
2. Click the **Clone** button. The new cloned server appears in the server list.
3. To change settings for the newly cloned server, highlight the server and click the **Edit** button.
4. Edit the cloned server's name, host name or IP address, and port number.
5. Click **OK**.

---

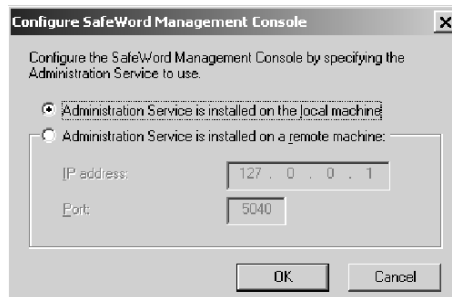
## Configuring the Administration Server

The SMC must access the SafeWord Administration Server. Because you can install the SafeWord Server on a different machine from the SMC, you may have to configure the console to point to the correct Administration Server.

To do this, do the following:

1. Open the Active Directory Users and Computer tool by selecting **Start -> Programs -> Administrative Tools -> Active Directory Users and Computers**.
2. Right click the **SafeWord** folder.
3. Select **Configure SafeWord Management Console**.

**Figure 4-21. Configure SafeWord Management Console**



4. If the Administration Service is on the local machine, select **Administration Service is installed on the local machine** and click **OK**.
5. If the administration service is installed on a remote machine:
  - a. Select the **Administration Service is installed on a remote machine** option.
  - b. Enter the **IP address and Port** for the machine where the SafeWord Servers are installed.
  - c. Click **OK**.



**Important:** *The port used for configuring the Administration Service must match the port specified as Administration Service when the SafeWord Server was installed.*

## Configuring multiple servers

SafeWord allows you to specify that multiple authentication engines can be used to process user login attempts. This setup improves system reliability and increases fault-tolerance. When multiple servers are specified, the first server in the list is tried first, and continues to be used as long as it is available. If it fails to respond within 30 seconds of the authentication request, the next specified server in the list is used, and so forth.

---

### SafeWord Server synchronization

When SafeWord is installed on multiple machines, and SafeWord Server synchronization is enabled, your environment is protected with load balancing, automatic failover, automatic backup of token records, and synchronization of the built-in administrative account between multiple SafeWord Server instances. If Server synchronization is not enabled, load balancing, automatic failover, and automatic backup are inoperative, and your system may encounter problems as a result of token records being out of synchronization.

SafeWord implements server synchronization based on a bi-directional ring topology in which each machine in the ring communicates with its neighbor in the ring. Each server has up to two neighbors: a logical 'next' server, and a logical 'previous' server. These neighboring servers are also known as peers.



**Tip:** For best performance SafeWord recommends running no more than six servers in your synchronization ring.

---

### Setting up SafeWord Server synchronization

SafeWord Server synchronization is performed by the Administration Service, which was installed as part of the SafeWord Server. Therefore, the Administration Service and the SafeWord Database Service must be running for SafeWord Server synchronization to occur.



**Important:** It is strongly recommended that you run synchronization over a VPN link. If not run over a VPN link, server synchronization traffic is not encrypted.

To configure SafeWord or Server synchronization, you must complete the following steps on every server that will participate in Server synchronization:

**Note:** It does not matter if the servers belong to the same or different Windows or DNS domains, you simply must ensure that each domain can talk to the other.

1. (If not already done) Install the SafeWord Server. For details about installing components, see "Installation topology rules" on page 2-3.
2. Stop the SafeWord Administration Service and the SafeWord Authentication Engine for all servers in the ring. If you are unsure about how to stop servers, see "Configuring multiple servers" on page 4-21.



**Important:** Do not stop the SafeWord database.

3. Edit the **Install\_Directory**\SERVERS\Shared\sccservers.ini file by doing the following:
  - a. Locate and uncomment the line starting with **DBActionListenerClass** by removing the first # character.
  - b. Locate and uncomment the line starting with **ReplNext\_JDBC\_URL**.
  - c. Replace the **NEXT\_HOST** on that line with the name or IP address of the peer that will serve as the logical 'next' peer in the ring.

The next two steps only apply to SafeWord Server synchronization rings consisting of more than two peers.

- d. Locate and uncomment the line starting with **ReplPrev\_JDBC\_URL**.
  - e. Replace **Prev\_Host** on that line with the name or IP address of the peer that will serve as the logical 'previous' peer in the ring.
4. Save the file.
  5. Open a command window and change to directory **Install\_Directory**\SERVERS\Database\bin.
  6. For each neighbor of this host, run batch file **AddReplPeer<machine name>.bat** (where <machine name> specifies the IP address of the neighbor). For example, if you are setting up peer MACHINE1 and its neighbor is MACHINE2, then on MACHINE1 you will run **AddReplPeer machine2.domain.sys**. Do this for each peer in the ring. This tells the database to accept connections from the neighbor peers whose names you specify as command line arguments.
  7. Start the SafeWord Administration Service and the Authentication Engine for all servers in the ring.
  8. If the User Center Service was running before, you must restart that service now.

**Note:** SafeWord Management Console configuration (the window that displays when you right-click the SafeWord folder from the Active Directory Users and Computers tool) is not synchronized to other machines in the domain. So if you have two domain controllers on a single domain, you can point each of the domain controllers to two different administration servers.

---

## Verifying SafeWord Server synchronization

To verify that server synchronization is working, perform the following tests on any system in the server synchronization ring.

---

### Importing tokens test

---

1. Select **Import/Backup/Restore** under the SafeWord folder.
2. Browse or specify a path to the token data records file, then select the **Import** button.
3. To verify that the import has completed successfully, connect to the Administration server running on a machine different from the one where you just did the import.
4. Select **Tokens** under the SafeWord folder.
5. Verify that the list of newly imported token serial numbers appears in the right pane of the window.
6. Verify that the newly imported token data is synchronized on all the other server(s) in the ring.



**Important:** *The procedure for testing the token import process is only applicable when you are initially setting up two or more machines. Do not use this process if you have already associated tokens to users.*

---

### PIN assignment test

---

1. Select the **Users** folder on the Active Directory Users and Computers window.
2. Highlight a user who has a SafeWord token assigned.
3. From the Action menu, select **Properties**.
4. Select the SafeWord tab.
5. Assign a **PIN** if there is not already one assigned, or clear the existing one.
6. Close the User Properties window by clicking **OK**.
7. Select the **SafeWord** folder under the domain tree.
8. Reconfigure the SMC to access the other servers in the synchronization ring. (See "Configuring the Administration Server" on page 4-19.)
9. Verify that the token PIN on the other server(s) was correctly added or cleared.

---

## Checking server synchronization

---

To confirm that SafeWord Server synchronization is in a steady state (meaning all changes are synchronized) do the following:



**Important:** *You must perform the following procedure on each server in the ring.*

1. Open a command window and change to directory ***Install\_Directory***\SERVERS\Database\bin.
2. Run the batch file called **QueryChangeLog**. This check should be performed on all servers in the ring.
3. The system has reached steady state once the output reads: **Empty set**.



## Managing and viewing logs

SafeWord records various events to logs that you can view for troubleshooting or server maintenance.

### Configuring Management Console logging

You may choose to log specific information from one of the SafeWord Agents, the SafeWord Server components (the Authentication Engine, the Administration Service, and the User Center), or from the SMC.

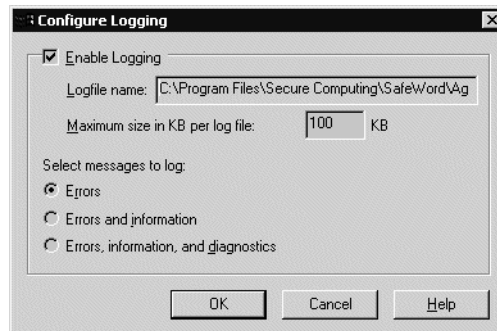
To view event logs from the SafeWord Server components, see “Viewing event logs” on page 4-26.

To set up logging for connections of the SafeWord Management Console to the Administration Service, do the following:

1. Right click the **SafeWord** folder in the Active Directory Users and Computers tool.
2. Select **Logging Settings**.

The Configure Logging window appears.

**Figure 4-22. Configure Logging window**



3. Click the **Enable Logging** check box.

**Note:** By default, logs are stored in <install\_dir>/SafeWord/Agentlogs.

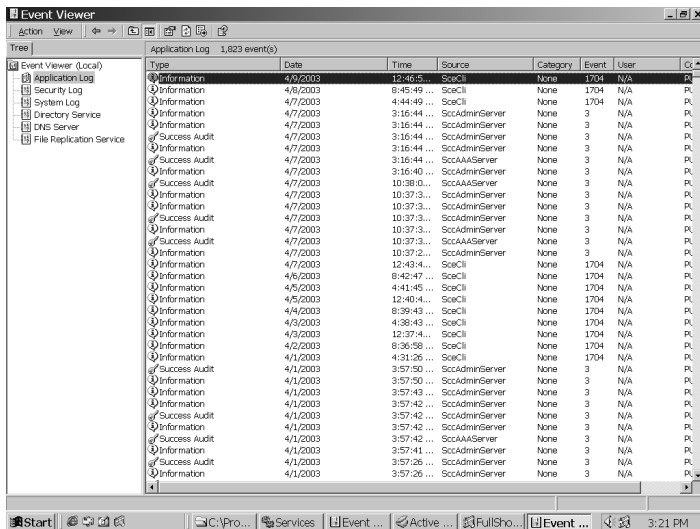
4. Select the types of messages to log from the following options:
  - ◆ Errors
  - ◆ Errors and information
  - ◆ Errors, information, and diagnostics
5. Click **OK**.

## Viewing event logs

You can audit various system authentication and administrative events such as authentication attempts, the starting and ending of administrative sessions, and modifications to entries in the SafeWord database. Viewing these event records is done using the standard Windows Event Viewer. SafeWord logs are placed in the Application section of the Event Log. To view the logs, do the following:

1. Open the Event Viewer by selecting **Start -> Programs -> Administrative Tools -> Event Viewer**.
2. Select **Application Log** from the left pane of the window.

**Figure 4-23. Event Viewer window**



SafeWord events are listed in the right pane with other Windows events.

## Database-related tasks

The SafeWord database serves as a repository for token records, and should be backed up on a regular basis, or anytime a change has been made to token records.

### Backing up the database

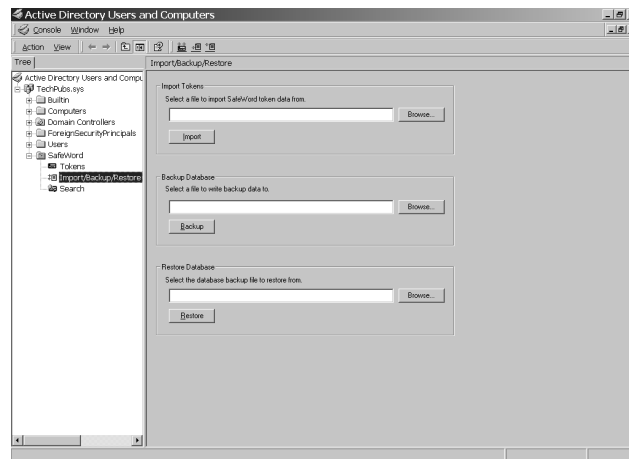
To back up your SafeWord database, do the following:

1. Open the Active Directory Users and Computer tool by selecting **Start -> Programs -> Administrative Tools -> Active Directory Users and Computers**.
2. Select the SafeWord folder.
3. Select **Import/Backup/Restore** under the SafeWord folder.



**Tip:** You can also back up your database by selecting the **Backup Database** icon on the toolbar.

**Figure 4-24. Import/Backup/Restore window**



4. Under **Backup Database**, click the **Browse** button to locate the file to write backup data to.
5. When the file name appears in the field labeled **Select a file to write Backup data to** click the **Backup** button.
6. Click **OK** upon successful backup.

## Restoring the database

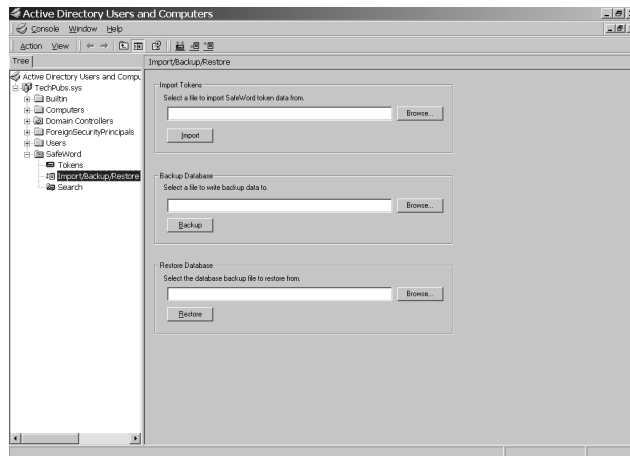
To restore the SafeWord database, do the following:

1. Open the Active Directory Users and Computer tool by selecting **Start -> Programs -> Administrative Tools -> Active Directory Users and Computers**.
2. Select the SafeWord folder.
3. Select the **Import/Backup/Restore** icon under the SafeWord folder.



**Tip:** You can also restore the database by selecting the *Restore Database* icon on the toolbar.

**Figure 4-25. Import/Backup/Restore window**



4. Under **Restore Database**, click the **Browse** button to locate the file from which to restore data.
5. Click **OK**.
6. When the file name appears in the field labeled **Select a database backup file to restore from**, click the **Restore** button.
7. Restart the Authentication Engine and the Administration Service.

When you restore the database, token records are reset back to their state at the time of the last backup and may be out of sync with their associated tokens. Sometimes the Authentication Engine is able to resynchronize the database records to the physical tokens automatically at the next authentication. Other times, the users need to login to the system twice. The first attempt to login will fail, but the second (assuming a correct one-time passcode is given) will succeed and resynchronize the token record. This behavior is by design.

## Reinstalling a server or the SMC

The SMC communicates with the SafeWord server (specifically, the Administration Service), and each generates an SSL certificate (stored with the component) to provide connection security and verify component identity. When the server and SMC are installed on the same machine, these certificates remain synchronized. However, if installed different machines and either component is reinstalled, the certificates may need to be regenerated. This typically results in an error message saying that the SMC could not connect to the server. There are two variations of this case, as described here:

### Case 1: you reinstalled the console, and kept the existing server installation

Solution: reset the server's record of the old console's certificate:

1. Locate and open (in a text editor) the file called *clients.ini* in directory `INSTALL_DIRECTORY\SERVERS\AdminServer\certificates`
2. Locate and remove the line that looks like the following:  
**HOST\_OR\_IP\_ADDRESS\CN=SccADUserExt=DB\A3\E9\4D\7A\A6\A2\8D\A5\B8\3D\4E\E0\CD\CF\D3**  
 where HOST\_OR\_IP\_ADDRESS is the location of the SMC .
3. Save the file.
4. Restart the Administration service.

### Case 2: you reinstalled the server, and kept the existing SMC installation

Solution: reset the console's record of the old server's certificate:

1. Locate and open (in a text editor) the file called *servers.ini* in directory `WINDOWS_DIRECTORY\SccCerts`  
 (WINDOWS\_DIRECTORY is the directory where Windows was installed; for example, c:\winnt)
2. Locate and remove the line that looks like the following:  
**HOST\_OR\_IP\_ADDRESS:5040=87:4d:76:49:47:a0:3b:23:e0:a8:52:2e:8f:8c:6e:d6**  
 where HOST\_OR\_IP\_ADDRESS is the location of the SafeWord server (for multiple servers, locate the line with the correct server address!). If the server was installed on a port other than 5040, then that port will appear in place of 5040.
3. Save the file.
4. Restart the SafeWord Management Console.

## Running SafeWord without Active Directory

SafeWord is optimized for seamless integration with the native Windows Active Directory management tools. However, there may be times when Active Directory integration is not practical or desirable. To support such circumstances, SafeWord supports a standalone mode of operation, not requiring Active Directory. While this mode does not provide all of the advanced management features, it does allow organizations to add strong authentication to their environments in a robust and simple fashion.

The following is a list of the features that are supported by SafeWord without Active Directory:

- ◆ The ability to associate users with tokens
- ◆ Importing token licenses into the system
- ◆ Display of user assignment in token list display
- ◆ Searches for users based on token serial numbers
- ◆ Backing up and restoring the SafeWord database
- ◆ Displaying imported token records

The following are not supported when you use SafeWord without Active Directory:

- ◆ The ability to associate users with tokens using native user management tools
- ◆ The ability to assign token PINs
- ◆ Generation of emergency passwords
- ◆ Token authentication tests
- ◆ User Center support

---

### Importing token records without Active Directory

To import token records when you are not using Active Directory, you must use the standalone SafeWord Management Console. The process is the same either with or without Active Directory.

## Configuring SafeWord to operate without Active Directory

To configure SafeWord to operate without Active Directory, do the following:

1. Edit *Install\_Directory\SERVERS\Shared\sccservers.ini* file as follows:

- a. Locate the line that matches the following:

```
IdMapperClass=securecomputing.yellowstone.authserver.ADtoTokenSNIdMapper
```

- b. Comment out the line by inserting a pound (#) sign at the beginning, as in the following:

```
#IdMapperClass=securecomputing.yellowstone.authserver.ADtoTokenSNIdMapper
```

- c. Locate the line that matches the following:

```
#IdMapperClass=securecomputing.yellowstone.authserver.PropFileIdMapper
```

- d. Uncomment the line by removing the first pound (#) sign:

```
IdMapperClass=securecomputing.yellowstone.authserver.PropFileIdMapper
```

- e. Locate the line that matches the following:

```
#PropFileIdMapperFile=c:\Program files\Secure Computing\SafeWord  
\SERVERS\AAAServer\users.map
```

- f. Uncomment the line by removing the first pound (#) sign:

```
PropFileIdMapperFile=c:\Program files\Secure Computing\SafeWord  
\SERVERS\AAAServer\users.map
```

- g. If desired, change to a file with a different name or location where you specify associations between user IDs and token serial numbers.

- h. Locate the line that begins with:

```
userDbType= . . . .
```

- i. Change the line to:

```
userDbType=securecomputing.nbt.tokenasplugin.FileUserDBMapper
```

- j. Locate and comment out (add a “#” to the beginning) the line:

```
IdMapperClass=internal
```

2. Create or edit the file by specifying user to token associations in the following format:

**userid=tokensn**

For example, to associate user **jd**oe with a token with serial number **12345678**, add the following entry to your map file:

**jd**oe=12345678

3. Add a line with user to token association for every user with a SafeWord token.

**Note:** *User IDs are not case-sensitive.*

4. Restart the Authentication Engine and the Administration Server.



# CHAPTER 5

## Troubleshooting

---

### About this chapter

This chapter contains information on troubleshooting your SafeWord system, and includes steps for uninstalling it if needed.

This chapter includes the following topics:

- ◆ “Troubleshooting” on page 5-2
- ◆ “Uninstalling SafeWord” on page 5-4

## Troubleshooting

This section contains troubleshooting information you may use if you encounter issues during installation, configuration or management of the SafeWord product.

**Table 5-1. Troubleshooting SafeWord**

Subject	Problem	Solution
<b>Installation</b>	Installation aborts	<ul style="list-style-type: none"> <li>◆ Ensure that target system meets all operational prerequisites and system requirements.</li> <li>◆ Check the install.log found in C:\Program Files\Secure Computing\installs for obvious errors.</li> </ul>
<b>Activation</b>	Activation fails	<ul style="list-style-type: none"> <li>◆ Confirm that the name key.html is being used. Any variations on this name (including key.html.html) will result in activation failure.</li> <li>◆ Contact Customer Support, provide activation key and error message.</li> </ul>
<b>Auto Updater</b>	AUA fails with error message "Error verifying signature: Class not registered [0x80040154]"	<ol style="list-style-type: none"> <li>1. Run existing AUA (which will fail).</li> <li>2. Go to Program Files\Secure Computing\SafeWord\Patches, launch <i>PatchSetup.exe</i> (manually patches AUA to newest version).</li> </ol>

**More...**

Subject	Problem	Solution
<p><b>Configuration</b></p>	<p>Error messages occur when attempting to configure the product</p>	<p>Use the Configuration Utility to turn on logging for the component you are trying to configure. (See "Logging server diagnostics" on page 4-16).</p>
	<p>Configuration was changed, but change was not reflected</p>	<p>Verify that the appropriate server(s) was restarted after the configuration was changed.</p>
	<p>Error message occurs when attempting to access the SafeWord tab from a user's Properties window</p>	<p>Confirm the status of the user's client certificate, and/or get a new certificate for a user. See "Reinstalling a server or the SMC" on page 4-29.</p>
	<p>Authentication fails</p>	<p>Confirm the IP address of the SafeWord Server is correctly entered on the proper Authentication Settings field of the Administration window. Without the IP address, authentication fails.</p>
	<p>Successful authentication, but access is denied</p>	<p>View your event logs to verify what is occurring. (See "Viewing event logs" on page 4-26).</p>
<p><b>Uninstallation</b></p>	<p>After uninstalling and reinstalling SafeWord, access to the SafeWord folder is denied</p>	<p>A simple uninstall of SafeWord may not completely remove all the files related to the software. Ensure that all directory and registry content has been removed, then reinstall the software</p>

## **Uninstalling SafeWord**

You uninstall SafeWord using the standard Windows-based Add/Remove Programs tool. To uninstall the program, select **Start -> Settings -> Control Panel -> Add/Remove Programs**. When the Add/Remove Programs window appears, select **SafeWord** and continue following the prompts to remove the software.

## APPENDIX A

# SafeWord Gold 3000 Tokens

---

### About this appendix

This appendix serves as a supplement for using SafeWord Gold 3000 tokens with your SafeWord software. It describes the tokens, and provides information and references about activating and distributing the tokens and their associated PINs.

Further information about your tokens can be found in the SafeWord Authenticator Administration Guide, located in Secure Computing's Web site at <http://www.securecomputing.com/techpubs.cfm>. You will need to enter your company ID to access the documentation area.

This appendix provides the following information.

- ◆ “Overview of your Gold 3000 tokens” on page A-2
- ◆ “Activating tokens” on page A-3
- ◆ “Distributing the hardware PINs” on page A-3
- ◆ “Assigning and testing tokens” on page A-3
- ◆ “Changing PINs” on page A-3
- ◆ “Using your token with SafeWord” on page A-4

## Overview of your Gold 3000 tokens

A


Your SafeWord software supports user authentication via SafeWord Gold 3000 tokens. The tokens are pre-programmed, each with its own unique PIN. These PINs serve only as electronic “keys” that “unlock” the token’s internal pass phrase generator, and only the correct PIN will result in correct pass phrase generation. You must activate the tokens before they can be used. After activation, you will receive a file called **ps.dat** which contains a PIN to token serial number association.

### SafeWord Gold 3000 tokens

SafeWord Gold 3000 tokens are designed in a key fob-type case design. Table A-1 lists the Gold 3000 key functions and common display messages.

**Note:** *If there is uncertainty about whether a displayed character is a number or letter, always defer to numbers. For example, use a "5" not an "S", and an "8" not a "B".*

**Table A-1. SafeWord Gold 3000 keys and common display messages**

SafeWord Gold 3000	Key	Function
	ON	Turns the token on or off.
	Clr	Clears the display.
	<<	Deletes last entered character.
	Entr	Generate a password.
	1 to 0 keys	Used to input PINs.
	PIN reset button	Allows for entering and/or changing PINs
Standard Display Prompt	Meaning	
ERASEd	Token memory has been erased.	
ENTR PIN	Enter your PIN.	

Advise your users that if they see any display messages other than those described above to contact an administrator.

## Activating tokens

Tokens are activated using the Product Serial Number code from your original software product, and the Token Group Identifier code from newly purchased token packs. For details about activating your tokens, refer to “Registering and activating your product” in your SafeWord Product Guide.



**Important:** When you are activating additional tokens purchased after activating your SafeWord software, you will not need to activate the `key.html` file. Follow the instructions for “Registering and activating your product” in your SafeWord Product Guide, but ignore the “Additional activation steps.”

## Distributing the hardware PINs

When your token pack is activated, the token PIN to serial number file (`ps.dat`) will be downloaded into the directory `<install_dir>\ImportData`. When a token is assigned to a user, they must be given the correct PIN for their assigned token. Without that PIN, they will not be able to use their token.



**Important:** Remember to inform users of their PIN when you distribute tokens to them.

## Assigning and testing tokens

Once you have activated your software and token data records, the tokens are ready to be assigned to users via the SafeWord Management Console (SMC), or users can enroll their own tokens using the SafeWord User Center. For detailed information about assigning tokens using the SMC, see “Administrator-assigned tokens using the SafeWord Management Console” in Chapter 3. If you prefer to allow your users to enroll their tokens in the User Center, see “User token self-enrollment with the User Center” in Chapter 3.



Secure Computing does NOT recommend using the PIN feature in the SMC or User Center for Gold 3000 tokens.

## Changing PINs

PINs on Gold 3000 tokens can be changed by entering the hard (pre-programmed) PIN, then pressing the PIN reset button and entering the new PIN.

If the hard PIN is changed and forgotten, the token will need to be reprogrammed.



**Important:** Gold 3000 token hard PINs can only be changed on the token itself. They cannot be changed in either the SafeWord Management Console (SMC) or the User Center.

## **Using your token with SafeWord**

The Gold 3000 token works with SafeWord in the following mode:

- ◆ Synchronous, friendly mode
- ◆ Passcode length = 6 character
- ◆ With and without Hard PIN



## REFERENCE

# Index

### A

- activation
  - certificate 2-14
  - key 2-13
  - the software 2-13
- Active Directory Users and Computers tool 4-13
- adding or changing PINs
  - with the SafeWord Management Console 2-24
- Administration Server
  - configuring 4-19
- Administration Service 1-4
- administration tool 3-3
- administrative passwords 2-16
- Agents
  - about IAS 1-6
  - about OWA 1-7
  - about SAM 1-7
  - about Web Interface 1-6
  - default settings for IAS 3-2
  - default settings for OWA agent 3-10
  - default settings for SAM Agent 3-7
- authentication
  - Engine 1-4, 3-13
  - policy, configuring 3-15
  - settings window 3-5
- Auto Updater 1-6

### B

- backing up the database 4-27

### C

- changing the User Center default password 2-17

- changing your administrative password 2-16
- changing your SMC default password 2-16
- CHAP support
  - IAS Agent and 3-2
- Citrix
  - and Web Interface 3-5
- components
  - changing ports on 4-15
  - functions 1-3
- computers in DMZ 3-17
- configuring
  - agents 3-13
  - alternative group policies 3-17
  - authentication engine 3-13
  - authentication policy 3-15
  - logging 3-14
  - the Administration Server 4-19
- configuring the MSAM 4.0 Agent 3-8

### D

- database
  - backing up 4-27
  - restoring 4-28
- default IAS setting 3-2
- default OWA setting 3-10
- default SAM setting 3-7
- deleting PINs 4-10
- diagnostic file locations 4-17
- DMZ
  - computers in 3-17
- domain administrator credentials 2-7

### E

- emergency passcodes

- generating 4-7
- encryption key 2-8
- explicit login settings 3-5

**G**

- generating emergency passcodes 4-7
- groups
  - SafeWord token and 3-15

**I**

- IAS agent default setting 3-2
- import0.dat 4-11
- importing token data records 4-11, 4-13
- Installing SafeWord 2-5

**K**

- Keys
  - encryption 2-8
  - signing 2-8

**L**

- Logging
  - configuring the management console for 4-25
  - server diagnostics 4-16
  - setting up with the Active Directory Users and Computers tool 4-25
  - settings 3-14

**M**

- Microsoft Point-To-Point Encryption (MPPE) support 3-2
- monitoring servers 4-18
- MPPE 3-2
- MPPE support
  - configuring 3-3
- MS 3-2
- MSAM 4.0 3-8
- MS-CHAP v1, 2
  - IAS Agent and 3-2

**O**

- Outlook Web Access Agent 1-7
- OWA Agent
  - extension and filter logs 3-12
  - timeouts 3-12
- OWA agent default setting 3-10

**P**

- PAP support
  - IAS Agent and 3-2
- passwords 2-16
  - administrative 2-16
  - changing the User Center default 2-17
  - security of 2-18
  - SMC default 2-16

**PINs**

- adding or changing 2-24
- adding or changing with the User Center 2-25
- changing 2-25
- deleting 4-10
- requiring 2-21

**Pins**

- users and 2-24
- privileges 2-6

**R**

- RADIUS support
  - IAS Agent and 1-6
- registering and activating 2-13
- reinstalling
  - the SafeWord Server 4-29
  - the SMC 4-29
- restoring the database 4-28

**S**

- SafeWord
  - Agents 1-6
  - database 1-4
  - installing 2-5
  - Management Console 1-4

- changing default password 2-16
- running without Active Directory 4-30
- Server 1-4
- Server synchronization 4-21
  - setting up 4-21
  - verifying 4-23
- Software Serial Number 2-13
- tab on SMC 1-4
- uninstalling 5-4
- SAM agent default setting 3-7
- searching
  - for unassigned tokens 4-5
  - results 4-6
  - utility 4-6
- servers
  - adding to monitored list 4-18
  - cloning 4-19
  - configuring multiple 4-21
  - monitoring status of 4-18
  - removing from monitored list 4-19
  - starting and stopping 4-15
  - synchronization 4-21
- setting up replication 4-21
- signing key 2-9
- SMC 1-4

## T

- testing tokens
  - with the SafeWord Management Console 2-26
- The 3-5, 3-7
- timeouts
  - OWA Agent 3-12
- tokens
  - administrator testing 2-26
  - finding users assigned specific tokens 4-6
  - icon 4-5
  - importing data records 4-11
  - importing records from the token data CD 4-13
  - reassigning 4-8
  - resynchronizing 4-3
  - search utility 4-6

- serial number 2-19, 2-23, 2-28
- testing with the SMC 2-26
- testing with the User Center 2-27
- Token Group Identifier 2-13
- unassigned 4-5
- Troubleshooting 5-2

## U

- unassigned tokens 4-5
- uninstalling SafeWord 5-4
- Upgrading from 2.0.x to 2.1.x 2-12
- User Center 1-4
  - URL for 2-25

## V

- VPN support
  - IAS Agent and 1-6

## W

- Web Interface
  - using with Citrix 3-5





Part Number: 86-0944890-B

Software Version: SafeWord, Version 2.1

Product names used within are trademarks of their respective owners.

Copyright © 2005 Secure Computing Corporation. All rights reserved.