Administration Guide

SafeWord® for Citrix® MetaFrame®
Secure Access Manager Agent

Version 2.0
Copyright

© 2004 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, SmartFilter, SofToken, Type Enforcement, and Strikeback are trademarks of Secure Computing Corporation, registered in the U.S. Patent and Trademark Office and in other countries. PremierAccess, G2 Firewall, G2 Enterprise Manager, Gauntlet, SecureOS, and MobilePass 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 "I ACCEPT" 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 "I DO NOT ACCEPT" 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.

Secure Computing Corporation ("Secure Computing") provides its software and licenses its use either directly or through authorized dealers. You assume responsibility for the selection of the programs to achieve your intended results, and for the installation (unless installation is purchased from Secure Computing or an authorized dealer), use and results obtained from the programs.

1. 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.

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

3. 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.

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

Secure Computing does not warrant that the functions contained in the Software will meet your requirements or that operation of the program will be uninterrupted or error-free. The Software is furnished “AS IS” and without warranty as to the performance or results you may obtain by using the Software. The entire risk as to the results and performance of the Software is assumed by you. 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 Warranty. Secure Computing agrees to assign to You all supplier warranties, remedies and software licenses for hardware supplied hereunder to the extent permitted by the applicable supplier. You agree to pursue warranty claims directly with the manufacturer where possible.

For a period of three (3) years from date of shipment, Secure warrants to You that the SafeWord tokens will be free from defects in material and workmanship under normal use.
6. Limitation Of Warranty And 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, including without limitation, the laws and regulations administered by the United States Department of Commerce and the United States Department of State.

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. General. Any waiver of or modification to the terms of this Agreement will not be effective unless executed in writing and signed by Secure Computing. If any provision of this Agreement is held to be unenforceable, in whole or in part, such holding shall not affect the validity of the other provisions of this Agreement. In the event of any inconsistency between this Agreement and any other related agreements between you and Secure Computing, the terms of this Agreement shall prevail. 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. To inquire about obtaining a support contract, refer to our "Contact Secure" Web page for the latest information at 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.

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.
## Printing history

<table>
<thead>
<tr>
<th>Date</th>
<th>Part number</th>
<th>Software release</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 2003</td>
<td>86-0943397-A</td>
<td>SafeWord for Citrix MetaFrame Secure Access Manager Agent, Version 1.1</td>
</tr>
<tr>
<td>September 2004</td>
<td>86-0943397-B</td>
<td>SafeWord for Citrix MetaFrame Secure Access Manager Agent, Version 2.0</td>
</tr>
</tbody>
</table>
# Table of Contents

Welcome .................................................. 1  
Pre-installation requirements .......................... 2  
Installing the Secure Access Manager Agent ........ 4  
Configuring the Secure Access Manager Agent ........ 7  
  Configuring the Authentication Engine .............. 7  
  Changing default logging settings .................. 9  
  Defining groups for token authentication .......... 10  
Removing the Agent .................................. 12
Welcome

The Secure Access Manager Agent is an optional add-on component from Secure Computing Corporation for use with SafeWord PremierAccess and the MetaFrame Secure Access Manager. The agent uses the standard SafeWord for Citrix administration tools, and installs directly on top of your SafeWord for Citrix MetaFrame installation.

About this guide

This guide is written specifically for the person who is assigned to administer SafeWord PremierAccess servers running the MetaFrame Secure Access Manager. It includes the following sections:

- “Pre-installation requirements” on page 2
- “Installing the Secure Access Manager Agent” on page 4
- “Configuring the Secure Access Manager Agent” on page 7
- “Removing the Agent” on page 14

The next section describes the pre-installation requirements for the Secure Access Manager Agent.
Pre-installation requirements

Before installing and running the Secure Access Manager Agent, your system environment must meet the following operational and system requirements:

- Microsoft Windows 2000 or 2003 with the latest available service pack installed
- 256 MB RAM (minimum); **512 MB** (recommended)
- 3 MB of disk space (minimum); **10 MB** (recommended)
- SafeWord PremierAccess installed on at least one server in your network
- Citrix MetaFrame Secure Access Manager with Secure Gateway installed
- Internet Explorer version 5.5 or greater
- Users successfully authenticating using MetaFrame Secure Access Manager

When your system meets these requirements, you are ready to install your agent from the Deployment CD. You can install the agent on any server that meets the system environment requirements and communicates with the SafeWord for PremierAccess Authentication Engine.
Figure 1 shows the Secure Access Manager Agent installed in a typical SafeWord PremierAccess environment. Your organization’s environment may not look exactly like the one depicted in the graphic, but it must at least meet all the pre-installation and operating system requirements outlined in this guide.
Installing the Secure Access Manager Agent

Before beginning this installation, you must have SafeWord PremierAccess and Citrix MetaFrame Secure Access Manager installed and running in your network. When both of these programs are operating, you are ready to install the MetaFrame Secure Access Manager Agent. If you have not installed the other applications, you cannot install the agent software. Refer to the SafeWord PremierAccess and the Citrix MetaFrame Secure Access Manager documentation for specific installation instructions.

If you are ready to install the SafeWord MetaFrame Secure Access Manager Agent, do the following:

1. Insert the Deployment CD into the target computer’s CDROM drive.
2. When the Installer Main Window appears, click the Install Products link.
3. When the available products window appears, click the Agents for use with SafeWord® PremierAccess™ link.
   The installer window will display a list of all available agents.
4. Click the SafeWord® RemoteAccess Agents link.
   Several InstallShield windows will appear and disappear as the installer checks your system configuration.
5. When the Serial Number window appears, enter your product serial number, then click OK.

![Figure 2. Serial Number prompt window]

6. When the Welcome window appears, click Next.
7. When the License Agreement window appears, you must click Yes to continue with the installation.
   The Select Destination window appears.
8. Either accept the default installation destination, or use the Browse button to change the destination. When your choice has been made, click Next.

The Select Components window appears.

9. Select MetaFrame Secure Access Manager Agent, then click Next.

10. Review the information in the Program Folder window, then click Next.

11. Review the information in the Start Copying files window, then click Next.

The SafeWord Server Name window appears.
12. Enter the Host name (or IP address) and Port number for the SafeWord Authentication Engine location. The default location is localhost.

13. Click Next to complete the installation.
Configuring the Secure Access Manager Agent

When you install the Secure Access Manager Agent, its Authentication Engine, logging functions, and authentication group policy are configured as follows:

- the Authentication Engine runs on the host machine that was chosen when the agent was installed
- logging is disabled
- the authentication group policy is set for all users to authenticate using SafeWord

The sections that follow explain how to reconfigure these settings using the Secure Access Manager Agent configuration tool.

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

Configuring the Authentication Engine

To launch the administration tool and reconfigure the Authentication Engine, do the following:


2. When the Agent Configuration window appears, click the Authentication Engine button. The Authentication Engine tab appears.

3. Enter the Host name or IP address of the machine to which the agent will send authentication requests in the Host name/IP address field.
4. Enter the Port number on which the Authentication Engine will listen for requests in the Port field. This port number must match the port number specified for the Authentication Engine when you installed SafeWord PremierAccess.

5. Click the Save button. The server appears in the list of configured locations.

6. To remove servers from the Configured Locations list, select the server name from the list and click the Remove button.

7. Click OK.

Important: If you are configuring multiple servers, repeat the same steps for each server you are configuring. For more information about configuring multiple servers, refer to the SafeWord PremierAccess Product Guide.
Changing default logging settings

Logging functions are disabled by default when the Secure Access Manager Agent is installed. You must enable logging to define which events to log, and where to log them. You may view and manage log records using Windows Event Viewer. You may also view and manage log records in 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.
   
   The Configure Logging window appears.

2. Select the **Enable Logging** check box to activate the window.
3. In the **Logfile name** field, enter the file name and path where you want to store log files. You can also use the **Browse** button to specify the file name and path.

   Your file name and path should resemble the following:
   
   `x:\path\path\...\file name.txt`

4. In the **Maximum size in KB per log file** field, enter the maximum size a log file can reach before it is archived and a new file is created.
5. Select the types of messages to log from the following options:
   - Errors
   - Errors and information
   - Errors, information, and diagnostics

⚠️ **Important:** Selecting to log diagnostic information may result in extremely voluminous output. There should be no reason to select this option unless you are troubleshooting a problem. You should disable diagnostic logging when you no longer need it.

6. Click **OK**.

For more information about logging, see the *SafeWord PremierAccess Product Guide*.

---

**Defining groups for token authentication**

SafeWord PremierAccess allows you to select groups of users who will be required to log on to the system using a SafeWord token. The simplest way to configure this is to force all your users to use tokens when logging in. Since this approach may not be flexible enough for your environment, you can also force only users belonging to a specific Windows group to use tokens. To do this, use the native Windows user and group management tools to create a global group (for example SafeWord_users) to which you will assign users who need to use a SafeWord token to log in. For more information about groups, see the *SafeWord PremierAccess Product Guide*.

Once users are made to be members of the group that will use SafeWord tokens, you will need to tell the agent what the group is, and how to treat users in it. The instructions that follow describe how this is done.
1. Click the **Groups** button on the Agent Configuration window.

   The Required Authentication Group Policy window appears.

   ![Figure 8. Required Authentication Group Policy window](image)

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

   **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.

2. To require all users authenticate using SafeWord strong authentication, select **All users authenticate using SafeWord** then continue to step 4.

3. 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
     - Only users NOT in this group authenticate using SafeWord

4. Click **OK**.

   For more information about groups, tokens and configuring strong authentication, refer to the **SafeWord PremierAccess Product Guide** located on the SafeWord PremierAccess Server CD.
Configuring alternative group policy settings

By default, SafeWord is configured so that the SafeWord MetaFrame Secure Access Manager Agent checks group membership and submits authentication requests to the authentication engine (Figure 10).

If computers in a network DMZ do not have anonymous access to your Active Directory installation, the SafeWord MetaFrame Secure Access Manager Agent is unable to contact Active Directory and read group membership information in order to determine which users require SafeWord authentication. Fortunately, you can configure SafeWord to handle such a scenario (see Figure 11).

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 above topology, do the following:

1. On the computer in the DMZ running the SafeWord agent, use the group configuration screen 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\sccservers.ini`.

3. In that file, locate the line that starts with...

   ```
   #GroupsAuthenticationRequiredClass=securecomputing.yellowstone...
   ...
   ```

   ...remove the "#" sign from the beginning of that line.

4. Navigate to `INSTALL_DIRECTORY\SERVERS\AAAServer\GroupDiscrimination`.

5. Locate and open the HTML file called `ConfigureGroupPolicy.html`. The Group Discrimination configuration page appears.

6. Change the logging and group policies as needed, then 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 the section called “Configuring multiple servers” in Chapter 4 of the SafeWord PremierAccess Administration Guide.
Removing the Agent

You remove the MetaFrame Secure Access Manager Agent using the standard Windows-based Add/Remove Programs tool. To remove the agent, do the following:

To remove the agent, do the following:

1. Select Start -> Settings -> Control Panel -> Add/Remove Programs.
2. When the Add/Remove Programs window appears, select SafeWord RemoteAccess.
3. Click the Change/Remove button.
4. A RemoteAccess screen will appear prompting to Modify, Repair, or Remove the agent.
5. Select Remove.
6. Click Next to remove the installation.
   - The agent components will be stopped automatically and the uninstallation process will occur.
   - **Note:** If shared files are detected, remove them by clicking Yes when prompted.
7. Click Finish in the Maintenance Complete window.
8. Close the Add/Remove Programs tool.
9. The uninstallation is complete.