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, SmartFilter, PremierAccess, SofToken, Type Enforcement, and Strikeback are trademarks of Secure Computing Corporation, registered in the U.S. Patent and Trademark Office and in other countries. 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.

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. Secure Computing reserves all rights that are not expressly granted to you.

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. 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.

6. 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.

7. Protection of Confidential Information. The Software Product is delivered to you on a confidential basis and you are responsible for employing reasonable measures to prevent the unauthorized disclosure or use thereof, which measures shall not be less than those measures employed by you in protecting its own proprietary information. You may disclose the Software Product to your employees as necessary for the use permitted under this Agreement. You shall not remove any trademark, trade name, copyright notice or other proprietary notice from the Software Product.

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. 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>February 2000</td>
<td>86-0933996-A</td>
<td>SafeWord Authentication Agent for Windows NT Domains, Version 1.0.1</td>
</tr>
<tr>
<td>June 2000</td>
<td>86-0933996-B</td>
<td>SafeWord Authentication Agent for Windows NT Domains, Version 1.0.1</td>
</tr>
<tr>
<td>February 2001</td>
<td>86-0933996-C</td>
<td>SafeWord Agent for Windows Domains, Version 2.0</td>
</tr>
<tr>
<td>September 2001</td>
<td>86-0933996-D</td>
<td>SafeWord Agent for Windows Domains, Version 2.0.0.18</td>
</tr>
<tr>
<td>October 2001</td>
<td>86-0933996-E</td>
<td>SafeWord Agent for Windows Domains, Version 2.0.0.19</td>
</tr>
<tr>
<td>May 2002</td>
<td>86-0933996-F</td>
<td>SafeWord Agent for Windows Domains, Version 2.1</td>
</tr>
<tr>
<td>September 2004</td>
<td>86-0933996-G</td>
<td>SafeWord Agent for Windows Domains, Version 2.4</td>
</tr>
<tr>
<td>December 2004</td>
<td>86-0933996-H</td>
<td>SafeWord Agent for Windows Domains, Version 2.4</td>
</tr>
<tr>
<td>November 2005</td>
<td>86-0933996-I</td>
<td>SafeWord Agent for Windows Domains, Version 2.4.1</td>
</tr>
</tbody>
</table>
About this document

This document describes how to set up and use the SafeWord® Agent for Windows Domains. This document is intended for use by the person responsible for administering their organization’s network and its users.

This document contains the following topics:

- “Introducing SafeWord Agent for Windows Domains” on page 2
- “How the SafeWord Agent works” on page 4
- “Requirements” on page 5
- “Installing the SafeWord Agent for Windows Domains” on page 6
- “Configuring for Smart Card Login” on page 25
- “Removing SafeWord Agent for Windows Domains” on page 26
- “Domain Agent operating notes” on page 27
- “Troubleshooting” on page 30

Note: Throughout this manual, the term “Windows” is used as a blanket term that refers to Windows 2000, Windows 2003, and Windows XP. Areas of the documentation that are specific to one operating system will be specified as such.
Introducing SafeWord Agent for Windows Domains

The SafeWord Agent for Windows Domains enables a company to secure access to its Windows Domain-based network using PremierAccess® authentication technology. The agent consists of the following components that you can install separately or in combination with each other:

- **Service Agent**
  The Service Agent component is usually installed on Windows domain controllers. This component validates a user against a PremierAccess server. After obtaining the user’s PremierAccess information from a Workstation Agent, it attempts to authenticate the user with PremierAccess. If the PremierAccess authentication fails, the Sub-authentication Filter returns a failure result to the standard Windows domain logon subsystem.

  The Service Agent component is usually installed on a secure computer on the network, and is usually the same computer on which the Sub-authentication Filter is installed. The Service Agent needs to be configured with the IP address (or hostname) and port of the PremierAccess server it should use for authentication.

- **Sub-authentication Filter**
  The Sub-authentication Filter portion of the SafeWord Agent for Windows domains must be installed on every domain controller in a Windows domain network. This component allows PremierAccess to perform additional authentications once a user has been successfully validated by a standard Windows domain logon mechanism. It must be installed on computers designated as Windows domain controllers. When users log on to a Windows domain, those designated as members of a previously set up PremierAccess user group are prompted for their PremierAccess credentials and are only allowed to log on if the credentials are correct. The Sub-authentication Filter works in combination with the Service Agent, and must be configured with the name of a Service Agent computer to function properly.
**Workstation Agent**

The Workstation Agent component must be installed on every computer in the domain where domain access is intended to be protected by PremierAccess authentication. This is a client-side component in the system. It is responsible for communicating with the Service Agent or smart card provider, and for prompting the user for his or her PremierAccess password. It is installed on the individual workstations.

*Note:* The term "workstation" is a blanket term for any computer that is not a domain controller.

---

**Figure 1. Sample installation configuration**

- Windows 2003 workstation
- Windows XP workstation
- Windows 2000 workstation
How the SafeWord Agent works

Upon receipt of a login or protected resource access request from a workstation, a domain controller in a Windows domain that is protected by SafeWord Agent for Windows Domains, contacts the Sub-authentication Filter to initiate a PremierAccess authentication sequence. The Sub-authentication Filter passes the request on to the Service Agent component. The Service Agent component determines which SafeWord agent-equipped computer started the login sequence, or initiated a resource request.

The Service Agent directs the Workstation Agent to prompt the user for a PremierAccess password or smart card provider and PIN, and checks these credentials or the certificate against the PremierAccess database. If the credentials are valid, the Service Agent loads a cryptographically-secure voucher on the Workstation Agent and informs the Sub-authentication Filter that the authentication has succeeded. Upon successful authorization, the domain controller completes the login sequence and grants access to the user.

If the SafeWord agent-equipped computer has already successfully logged in, and the user requests a secure resource from the domain controller (e.g., access to a shared network drive), the Sub-authentication Filter once again prompts the Service Agent for authentication. The Service Agent component prompts the Workstation Agent component for the secure voucher. If the Workstation Agent responds with a valid voucher, the Service Agent validates the resource request to the Sub-authentication Filter, and the domain controller grants the user's request. If not, (e.g., if the voucher has expired), the user is again prompted for his or her PremierAccess credentials.

When the secure voucher is about to expire, the Workstation Agent warns the user of the impending expiration. When the voucher finally expires, the user's machine will automatically lock and require SafeWord credentials to unlock. Once the user enters valid SafeWord credentials, the machine is unlocked and the user receives another secure voucher.

The Service Agent can send optional custom prompts for the PremierAccess password, as well as the custom text that displays on the bottom of the dialog. This text is stored in the registry, and updated with each PremierAccess authentication request.
Requirements

End users have the ability to enter PremierAccess credentials in the Logon or Locked Workstation dialog boxes. If this information is correct, subsequent PremierAccess credential dialog boxes do not display. If the credentials are invalid, the machine locks automatically and the user will have to enter valid PremierAccess credentials to unlock the machine. For detailed information about locked workstations and SafeWord Agent-protected domains, see “Domain Agent operating notes” on page 27.

Requirements

The following items are required for use with the SafeWord Agent for Windows Domains:

- A Windows 2000, Windows 2003, or Windows Advanced Server configured as a domain controller, running TCP/IP.
- A SafeWord PremierAccess 3.0 server or later.
- Computers with the Service Agent component installed must have TCP/IP installed as one of the network protocols. The same rule applies for the client computers.
- To allow users to log on using smart cards, you will need a smart card reader (integrated or external), a Cryptographic Service Provider (CSP) for the smart card you will be supporting, and a digital certificate.
Installing the SafeWord Agent for Windows Domains

This section outlines the initial installation procedures for the SafeWord Agent for Windows Domains. Components and procedures vary depending on whether you are installing on a domain controller, on a member server, or on a workstation. Consult Table 1 to determine which components you must install and which are optional. Once the initial installation process is complete, refer to the installation instructions specific to the type of machine to which you are installing (domain controller or member server).

Table 1. Component Installation Options

<table>
<thead>
<tr>
<th>Machine to which you are installing</th>
<th>Sub-auth Filter</th>
<th>Service Agent*</th>
<th>Workstation Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Controller(s)</td>
<td>X</td>
<td>X (optional)</td>
<td>X (optional)</td>
</tr>
<tr>
<td>Member Server(s)</td>
<td></td>
<td>X (optional)</td>
<td>X (optional)</td>
</tr>
<tr>
<td>Workstation(s)</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

*Note: An * indicates that the component must be installed on at least one machine. We recommend that the Service Agent and the PremierAccess Sub-authentication Filter reside on the same computer.*

If you are installing the software from a stand-alone package that was downloaded from our Web site, locate the zipped installation files, extract the files, and run Setup. When complete, continue to step 4 on page 8 of the installation procedure.

To install the SafeWord Agent for Windows Domains from the Deployment CD, insert the PremierAccess Deployment CD in your computer’s disk drive. `Setup.exe` automatically launches and the Deployment CD Main window appears.
1. Select **Install Products**. The Install Products window appears.

2. Select **Agents for use with SafeWord® PremierAccess™**. The Agents for PremierAccess window appears.
3. Select **SafeWord Agent for Windows Domains**. Files needed for this installation will be extracted. This will take a moment. When the files are extracted, the Welcome Wizard window appears.

![Figure 5. Welcome Wizard window](image)

4. Click **Next**. The License Agreement window appears.

![Figure 6. License Agreement window](image)

5. Read the license agreement carefully, then click **Yes** to accept the terms of the license.
Installing on a domain controller

If you are installing the SafeWord Agent for Windows Domains on a domain controller, after accepting the license agreement, the Select Components window appears. If you are installing on a member server, skip to “Installing on a member server” on page 20.

1. Select the components you want to install by checking the appropriate check boxes on the Select Components window, then click Next.

2. (Conditional) If you installed the Service Agent, the Authentication Server Configuration window appears. Continue to the next step. If you did not install the Service Agent, continue to “Client Message settings” on page 13.

3. Enter the Hostname or TCP/IP Address of the PremierAccess server that the Service Agent will authenticate.

4. Enter the port number on which the PremierAccess server will listen in the Port field, then click Add.

**Note:** The Sub-authentication Filter option only appears when you are installing on domain controllers. If you are installing on a workstation, the option is unavailable.
5. Click **Next**. The SafeWord Agent for Windows Domains Configuration window appears with the **Service Agent** tab displayed.

### Service Agent settings

The Service Agent tab consists of the Key pane and the PremierAccess pane. It allows you to create private keys and to configure the agent so users can reauthenticate after failed authentication attempts.

**Tip:** Clicking **Apply** on any of the tabs activates your choices and keeps the current window open. Clicking **OK** ends the displayed portion of the setup and starts the next one. Do not click **OK** until you have completed the displayed setup.

![Figure 8. Service Agent tab](image)

#### Creating private keys

Specify a new private key in the **Private Key** field. The private/public key-pairs encrypt information passed between the Service Agent and the Sub-authentication Filter. A **public key** based on the private key you enter here is generated and exported to a file that is then imported during the Sub-authentication Filter part of the setup. The public key is imported on all domain controllers in the network because the Sub-authentication Filter must be installed on every domain controller. Private keys can be any combination of characters and digits, and can be any length.

**Note:** If the private key is modified after the initial installation, you must restart the SafeWord Agent for Windows Domains service.

If your Sub-authentication Filters are installed on machines other than the machine to which you are currently installing the software, you must manually export the public key that was generated. To export public keys manually, refer to “Exporting the public key” on page 11.
Important: If you install Service Agents on multiple machines, and then you point multiple Sub-authentication Filters to some of them, all the Service Agents must share the same private key.

Exporting the public key

If you have Sub-authentication Filters installed on machines other than this machine, on the Service Agent tab click the Export key button. A prompt for a file name with a .pky extension appears. This is your public key file. (This is only required if Sub-authentication Filters are installed on multiple machines). This public key will be used for all domain controller Sub-authentication Filter installations. To export the public key file, enter a File Name. Ensure the name has a .pky extension. After naming the key file, save it to a cd or floppy disk, or to a network location where it can be accessed by the Sub-authentication Filter machines during installation.

Reauthentication without required credentials

A SafeWord user accessing a domain resource is prompted for their SafeWord password if their voucher has expired. If the password is incorrect, the user must re-access the resource for the prompt to reappear. Enabling this option allows the user to re-enter their password without re-accessing the resource. To allow users to reauthenticate to PremierAccess after failed authentication attempts, under the PremierAccess pane, select the Allow reauthentication tries to PremierAccess on failure check box.

Note: Due to the characteristics of Active Directory, enabling this option may cause minor delays in the Active Directory operation. This option is not recommended for large Active Directory domains. Furthermore, the option to enable SafeWord authentication retries is not applicable when you initially log on to a SafeWord-protected domain (via the initial Windows Logon dialog). In this case, the agent does not retry SafeWord authentication.

Caution: Selecting this option offers ease of use at the expense of security. When users are prompted for PremierAccess credentials on failed authentication attempts, a would-be attacker may be able to conclude that it was the PremierAccess credentials, not the operating system credentials, that were invalid. Your organization’s security policy should be considered when deciding which option to use.

When you are finished configuring the Service Agent, select the Client Voucher tab.
Client voucher settings

The Client Voucher tab allows you to set voucher lifetimes. It also allows you to configure the Workstation Agent, to warn users before their voucher expires, and to lock the workstation upon expiration.

Kerberos service ticket lifetimes and Domain Agent voucher lifetimes

Kerberos is the authentication protocol that is used to authenticate access to Windows 2000 and Windows 2003 domains. If a Kerberos user ticket lifetime is set to be longer than the Domain Agent’s voucher lifetime, it is possible for a user to continue to access domain resources after her voucher has expired without being challenged for a new set of SafeWord credentials. To properly protect domain resources with the Domain Login Agent, it is important to do one of the following, either:

- Enable **Lock client workstation when voucher expires** so that the user is unable to actively access domain resources until they reauthenticate. This does not prevent processes currently running on behalf of the user from continuing to access the same domain resources.
- Set the Domain Login Agent voucher expiration to be the same as or longer than the Kerberos user ticket lifetime.

Additionally, if you have the Domain Login Workstation Agent installed on any Windows 2003 member servers, you must ensure the the Domain Login Agent voucher expiration is the same as the Kerberos user ticket renewal lifetime. This ensures that the user remains strongly authenticated throughout the entire lifetime of the...
Kerberos user ticket. Windows 2003 servers require this setting because Kerberos user tickets on Windows 2003 platforms are renewed silently for the duration of the renewal lifetime without requiring reauthentication. (The Kerberos user ticket lifetime and the user ticket renewal lifetime are configured in the Kerberos policy of the Default Domain Security Policy or the Kerberos account policy of the GPO that is in effect for your domain users. The default for the Kerberos user ticket lifetime is 10 hours and the default user ticket renewal lifetime is seven days.) For additional information about Kerberos, refer to the Secure Computing Knowledge Base, which is available from www.securecomputing.com.

To set a client voucher lifetime, on the Client Voucher pane specify in **hours** and **minutes** the Client voucher lifetime, or use the defaults. This is the duration before the PremierAccess user needs to reauthenticate on the workstation after successfully being authenticated the first time (unless the user reboots, or logs out and logs in again). When a voucher expires and the user tries to access a protected network resource, they will be prompted for their PremierAccess password again. Minimum voucher lifetime is one hour. You must synchronize the clocks on all of the computers running the Service Agent. For details about synchronizing, see “Troubleshooting” on page 30.

**Note:** *If the voucher lifetime is modified after the initial installation, you must restart the SafeWord Agent for Windows Domains service.*

To configure voucher expiration behavior just prior to and upon expiration, on the Voucher Expiration Behavior pane, select the upper check box to **lock the client workstation** when a voucher expires. Select the lower check box to **display a warning to the user prior to the voucher expiration.** When complete, **select** the Client Message tab.

### Client Message settings

The Client Message tab allows you to enter custom messages users see when they log on. Credential prompt messages display in the Logon dialog box above the PremierAccess password prompt. Text messages appear on the lower portion of the window.
Credential Prompt messages: Enter your credential prompt in the Credentials Prompt pane. Messages entered here display above the PremierAccess Password field when users log onto the server.

Text Messages: Enter a Client Message in the Text Message pane. Messages entered under Text Messages display in the lower portion of the Logon Information dialog box when a user logs onto the server as a PremierAccess-protected user a second time. The message can be up to 2400 characters (approximately 30 lines). It will display on the Client Messages display. Administrators can change the messages as often as they wish. The messages update each time a user logs on as a PremierAccess user after their second logon. When you are done, select the Workstation Agent tab.
Workstation Agent settings

The Workstation Agent tab is used for designating the port on which Workstation Agents will listen for connections from the Service Agent.

![Figure 11. Workstation Agent tab](image)

In the **Port** field, enter the port number on which the Workstation Agents will listen for connections. The default is 9999. We recommend leaving the default setting as the port. If you change the port number here, you must change it on every machine on which the Workstation Agent is installed. For detailed information about changing the ports on machines where the Workstation Agent is installed, see “Changing ports on Workstation Agent machines” on page 22.

When you are finished with this configuration, select the Logging tab.

Logging component data

The **Logging** tab is used to designate the components for which you wish to log data, and to designate the type of data to store. Logging options are available when you install the Service Agent component and the Sub-authentication Filter component together, or when you install the Sub-authentication Filter component alone. The procedure that follows applies to both configurations.

**Note:** If the logging options are modified after the initial installation, you must restart the SafeWord Agent for Windows Domains service.
To designate the components and messages to log:

1. In the **Max. file size in Kb** field, enter the desired maximum log file size (in kilobytes), or use the default file size. The default is 100 Kb. The current file will be renamed and a new one created when it reaches the specified size.

2. Select the component check boxes for which you wish to log data.

3. In each **Filename** field, enter the file names of the components that you have chosen to log or **Browse** to the files.

4. Select the check boxes for the type of data to log. You may choose to log errors, errors and information, or errors, information and diagnostics. When your finished, click **OK**.

If you are not installing the Sub-authentication Filter, the Installation Complete window appears. Continue to step 5 below to finish the installation. If you are installing the Sub-authentication Filter, the Sub-authentication Filter tab appears. Skip to “Sub-authentication Filter settings” on page 17 to configure it.

5. Select **Yes, I want to restart my computer now**.

6. Remove any disks from their drives on the computer, and then click the **Finish** button.

**Important:** You must restart your computer before using the SafeWord Agent for Windows Domains program.
**Sub-authentication Filter settings**

This tab is used to designate hosts for the Service Agent, and to import public keys. The Sub-authentication Filter intercepts authentication requests and forwards them to the Service Agent program.

⚠️ **Important:** You must install Sub-authentication Filters for each domain controller in your network.

![Figure 13. Sub-authentication tab](image)

**Configuring Service Agent hosts**

The Service Agent information pane allows you to add, delete, and test hosts for the service agent.

- To add a host, enter the **Hostname(s)** of the machine(s) running the Service Agent, then click the **Add** button.
- To delete a host, highlight its name, then click the **Delete** button.
- To test a host, highlight its name, then click the **Test** button. Public keys must be imported before testing the host. If you are installing the Sub-authentication filter on the same machine as the Service Agent, this key is automatically imported and it is displayed in the Import Key field. If a public key is not displayed, refer to “Importing public keys” on page 18.
Tip: We recommend that, in addition to the Sub-authentication Filter, each domain controller have a copy of the Service Agent installed on it. The Sub-authentication Filter on that machine should then, at the very least, point to that local copy of the Service Agent. Additionally, each Sub-authentication Filter can also point to Service Agents running on the other domain controllers. With this network topology, even if the local Service Agent is stopped, authentications will be allowed to continue. Sub-authentication Filters will automatically attempt to connect to these additional Service Agents, adding fault tolerance to the system.

Caution: It may sometimes be tempting to have Sub-authentication Filters from multiple domain controllers pointing to the same single Service Agent. This topology, however, has the disadvantage of leaving the entire network dependent on a single machine. It is not recommended.

Importing public keys

The lower pane of the Sub-authentication Filter tab allows you to import the public key that was exported to a file during the Service Agent installation. If you are installing the Sub-authentication Filter on the same machine as the Service Agent, this key is automatically imported. You will see the public key displayed in the Import Key field. Otherwise, to import a public key:

1. Click the Import key button.
2. Enter the file name and path of the public key file saved during the Export key portion of the Service Agent installation.

Tip: If you have forgotten where your .pky file is, check the SafeWord Agent for Windows Domains Configuration shortcut by clicking Start -> All Programs -> Secure Computing -> SafeWord Agent for Windows Domains -> SafeWord Agent for Windows Domains Configuration. On the window that displays, select the Service Agent tab, and then click the Export key button on the machine where you installed the Service Agent.

3. Click the Test button to trigger a contact attempt with the selected Service Agent. You are notified that the Service Agent is actually running on the specified host. The test checks to see if the Service Agent is running. It does not detect key mismatches or other problems.

Important: If you just installed the Service Agent, and you have not restarted your computer, this function will always fail verification. You must restart the computer first.

If you wish to exclude hosts from PremierAccess authentication, select the Host Exclusion tab and continue to the next section.
Host Exclusion settings

Host exclusions are the hostnames that are to be excluded from PremierAccess authentication. Adding an entry to the list enables the client to skip the PremierAccess part of the incoming authentication requests. It assumes that authentication will be performed by another program. Normal Windows authentication remains in place.

To add an entry to the exclusion list, in the Host Name field, enter the hostname(s) to be excluded from PremierAccess authentication, then click Add.

Important: This list must be entered on all controllers in the domain to be protected by PremierAccess. If the domain controllers are not included, it is possible that hosts in the list may not be excluded from PremierAccess authentication. Other programs that depend on this option may fail to work properly.

Select the Logging tab if you wish to configure data to log.

Logging data

The Logging tab is used to designate the components for which you wish to log data. To configure logging, refer to “Logging component data” on page 15.
Installing on a member server

If you are installing the SafeWord Agent for Windows Domains on a member server, after accepting the license agreement, the Select Components window appears.

![Select Components window](image)

**Note:** The Sub-authentication Filter option only appears when you are installing on domain controllers. If you are installing on a workstation, the option is unavailable.

To install the Service Agent and/or the Workstation Agent at the same time, continue to “Installing the Service Agent and/or the Workstation Agent on a member server” on page 20. If you are only installing the Workstation Agent, refer to “Installing the Workstation Agent as a standalone component” on page 21.

Installing the Service Agent and/or the Workstation Agent on a member server

To install the Workstation Agent and the Service Agent on a member server, select the **Service Agent** check box and the **Workstation Agent** check box, then click **Next**. The SafeWord Agent for Windows Domains Configuration **Service Agent** tab appears.
The Service Agent tab allows you to create private keys and to configure the software to allow users to reauthenticate after failed authentication attempts. Refer to “Service Agent settings” on page 10 for configuration instructions.

---

### Installing the Workstation Agent as a standalone component

You can install the Workstation Agent as a standalone component on member servers or on workstations. To install the Workstation Agent on a member server, refer to “Installing the Workstation Agent on a member server” below. To install the Workstation Agent on a workstation, refer to “Installing the Workstation Agent on a workstation” below.

### Installing the Workstation Agent on a member server

If you are installing the Workstation Agent on a member server, after accepting the license agreement, select the **Workstation Agent** check box and then click **Next**. You will be prompted to restart your computer. Select **Yes, I want to restart my computer now**. The InstallShield Wizard Complete window appears, indicating that the Workstation Agent has been successfully installed. Click the **Finish** button.
Installing the Workstation Agent on a workstation

If you are installing the Workstation Agent on a workstation, after accepting the license agreement, you are prompted to restart your computer. Select Yes, I want to restart my computer now. The InstallShield Wizard Complete window appears, indicating that the Workstation Agent has been successfully installed. Click the Finish button.

**Important:** You must restart your computer before using the SafeWord Agent for Windows Domains program.

Changing ports on Workstation Agent machines

If you are not using the default port as the port on which machines where Workstation Agents are installed will listen for requests, you must change the port number on every machine where the Workstation agent is installed. To do so, select Start -> All Programs -> Secure Computing -> SafeWord Agent for Windows Domains -> SafeWord Agent for Windows Domains Configuration. On the window that displays, select the Workstation Agent tab. Enter the port on which the machine will listen, then click OK. Repeat this process on every machine where the Workstation Agent is installed, then restart the Workstation for these changes to take effect.

Reconfiguring the Windows firewall to operate with the Workstation Agent

If you are installing the Workstation Agent on a machine running Windows XP Service Pack 2, and the Microsoft firewall is enabled, you must reconfigure the firewall in order for the Workstation Agent to operate properly. To do so, log on to the machine as an administrator, and then do the following:

2. Select the Exceptions tab, and then click the Add Port button.
3. Enter an appropriate port name and the port number on which the Workstation Agent will operate. The default port is 9999.
4. Select the UDP option, click OK, then click OK again to close the window.
5. Restart the Workstation for the changes to take effect.
Configuring Windows Domain users for PremierAccess authentication

For a Windows Domain user to be protected by PremierAccess, there must be a PremierAccess user configured with the same name in the PremierAccess user database unless Windows group checking is enabled. The Windows user name must be identical to the PremierAccess UserID.

**Note:** Currently, only SafeWord Gold 3000/Platinum (synchronous mode), SafeWord Silver 2000, and non-expiring fixed passwords are supported. Asynchronous mode (challenge-response) authenticators, authenticator combinations, and expiring fixed passwords are not supported.

To configure Windows 2000 and Windows 2003 environments, use the **Active Directory Users and Computers** utility to:

1. Create a global group called SAFEWORD_USERS. The name of the group must be typed in uppercase.

2. Add any users who should be authenticated by PremierAccess to the “SAFEWORD_USERS” group.

**Caution:** Do not add non-PremierAccess users here. The group creator is automatically added to the group they create. If their name is not in PremierAccess, they will fail PremierAccess authentication and a Bad User ID will show up in the PremierAccess logs.
The SafeWord Agent for Windows Domains utility

Use the **SafeWord Agent for Windows Domains Configuration utility** to change prompts, to customize text, or to change the Service Agent public key, Sub-authentication Filter public key, voucher lifetime, CSP, or default smart card CSP. You can also set the smart card logon option with this utility.

To access the utility, from the Windows Start menu, select **Programs -> Secure Computing -> SafeWord Agent for Windows Domains -> SafeWord Agent for Windows Domains Configuration**.

When you modify the values of the public/private key, the voucher lifetime, or the logging setting, you must restart the SafeWord Agent for Windows Domains Service.

PremierAccess Authentication server configuration

To configure the PremierAccess Authentication server or to add an additional server to your configuration, select **Programs -> Secure Computing -> SafeWord Agent for Windows Domains -> Edit PremierAccess Servers**. The **safeinfo.cfg** file displays. Line 02 displays the IP address and port number of the current Authentication server, and it can be modified in order to change the location of the Authentication server or to add an additional server.

---

**Miscellaneous configuration information**

The following options are available for customizing application settings post installation.
Configuring for Smart Card Login

PremierAccess allows your users to optionally logon using Smart Cards in place of passwords. If you will be using smart cards, you will need to install the CSP software that accompanies your smart card reader on each of the machines where users will be using smart cards. You may install that software now, or after you complete this configuration procedure. Users will only be able to logon with smart cards after you have installed the reader software, configured the smart card logon feature, obtained a digital certificate, and enrolled that certificate into PremierAccess.

To configure your application to allow smart card logon on a domain controller or a server, from the Windows Start menu, select Programs -> Secure Computing -> SafeWord Agent for Windows Domains -> SafeWord Agent for Windows Domains Configuration. If the agent is installed on a workstation, run the sccconfig utility from the Run command in the Start menu. The Smart Card Login tab appears.

![Figure 17. Smart Card Login window](image)

1. Select the Use a Smart Card check box.
2. (Optional) If you installed your reader software and provided CSPs at that time, they display in the Options list. If you set a CSP to display automatically, that CSP appears as the default provider. Select a CSP from the drop-down list.
3. Click OK.
4. If you have not already done so, install your smart card reader software and obtain a digital certificate for use with smart cards.

**Note:** Your digital certificate must be enrolled into PremierAccess before it can be used.
Removing SafeWord Agent for Windows Domains

To remove the SafeWord Agent for Windows Domains from the machines in the domain, run the Uninstaller on all the machines. To run the Uninstaller:

1. From the Windows Start menu, select Settings -> Control Panel.
2. Double-click the Add/Remove Programs icon.
3. Select SafeWord Agent for Windows Domains from the list of programs.
4. Click the Add/Remove button.
   - On Workstations, removal is complete.
   - On the domain controller, the InstallShield Wizard displays.
5. (Conditional) Select the Remove button, and click Next.
6. Restart your machine.
While most aspects of this operation are intuitive, a few areas warrant further discussion. The following sections contain that material.

Logging on in Windows environments

When a user logs into a PremierAccess-protected domain, and he erroneously enters invalid PremierAccess credentials, the user is granted access to the desktop only. Although it appears they have successfully logged in, they will not be able to access protected domain resources, and the PremierAccess password prompt will display again so they can retry logging into the domain.

Locking and unlocking the workstation

When the workstation is locked by the screen saver, by voucher expiration, or explicitly by the user, the user will be required to provide PremierAccess credentials upon unlocking. If invalid PremierAccess credentials are entered, the workstation will immediately lock again. The user is only granted access if they provide a valid password or a smart card CSP with the correct smart card PIN. To disable this behavior, create a RequireAuthOnUnlock registry key in DWORD value under <HKEY_LOCAL_MACHINE>/Software/SecureComputing/SafeWord/AGENT_SERVICE and set it to 0. Whenever this value is changed, the SafeWord Agent for Windows Domains service must be restarted.

The public key prompt

The first time a user logs on to a SafeWord Agent-protected domain, the following Public Key dialog box displays.
This is a normal process that serves as a security measure to prevent potential attacks on the network. If this is the first time a user has logged on to the domain, they should click **Yes** to accept the new key.

If this is not the first time a user has logged on to the domain, the dialog box indicates that the Administrator has changed the private key in the Service Agent. Administrators should inform their users in advance that they have changed the private key. It is also helpful to provide users with the first four digits of the new public key. This allows users to verify receipt of a new public key.

If the dialog box displays even though the private key has not been changed, in configurations with multiple domain controllers and Service Agents, this indicates that there may be a key mismatch between the Service Agents.

Finally, if the dialog displays upon subsequent logins, and the private key has not been changed, nor are there multiple domain controllers and Service Agents creating a key mismatch, this may indicate that network security has been compromised. In this case, users should contact their system administrators and report the behavior.

---

**Logging on to Windows XP through Remote Desktop**

The agent also allows SafeWord-protected logons through Remote Desktop to Windows XP machines with the Workstation Agent installed. Users will be required to enter valid domain and SafeWord credentials just like an interactive logon at the machine’s console.

**Note:** Before users can log onto SafeWord’s protected Windows XP machines through Remote Desktop, the agent’s public key must be accepted with a log on at the machine’s console in order to interact with a public key prompt.

---

**Logging on via Terminal Services**

Although it is possible to use this agent to log on to Windows via a Terminal Services session, doing so is not recommended. Demands on a multi-session, multi-user environment such as Terminal Services are quite different from those of the standard Windows Domain Login environment. If strong authentication for Terminal Services is desired, the SafeWord Agent for Terminal Services should be deployed.
WINS and DHCP addresses

In configurations that incorporate the Windows Internet Networking Service (WINS) or Dynamic Host Control Protocols (DHCP), it is possible that a workstation may have different IP addresses at different times. For workstations with dynamic IP addresses, or laptops with docking stations where both the laptop and the docking station have a network interface card, you should set up the Name Resolution for the workstation, so it is always possible to access the machine by name. Use the ‘ping’ utility to ping the workstation by name from a different machine. If these machines are configured in a way that allows them to incorrectly cache an "old" workstation IP address, the SafeWord Agent will be unable to contact the workstation, and authentication will fail. For detailed information about configuring WINS and DHCP, see the Windows Server Configuration Guide.

The effects of domain trust relationships on the Agent operation

When a domain does not have any kind of trust relationship set up, users must provide separate sets of credentials for each domain in order to gain access to their resources. If one or both domains are protected by the SafeWord Agent for Windows Domains, attempts to gain access predictably result in the PremierAccess prompt appearing on the user’s workstation.

However, if two domains have a two-way trust relationship, and the user has already successfully authenticated to one of the domains, accessing resources on the other domain may not trigger authentication by the second domain controller. The user is allowed access because he or she has already successfully authenticated to the domain that the second domain trusts. Because of this trust relationship, you must install the SafeWord Agent components on all domain controllers in all domains that have trust relationships with the domain that needs to be protected by PremierAccess. If this is not done, there is no way to guarantee that access will not be granted by another domain that has a trust relationship with the PremierAccess-protected domain. For more information on trust relationships in Windows domains, see one of the many books that are available on the topic of Windows System Administration.
Troubleshooting

When troubleshooting, ensure that the logging option for the Sub-authentication Filter, the Service Agent, and any agents in questions are set to Errors, Info, and Diagnostics.

SafeWord Agent for Windows Domains version 2.4 provides a feature that allows users to enter their PremierAccess credentials on the same screen where they enter their Windows credentials. When troubleshooting installations, we recommend that end-users do not fill in their PremierAccess credentials on the initial login screen. By doing so, the Agent brings up a separate PremierAccess prompt once a connection between the Agent and the Agent Service is established, making it easier to determine the cause of problems that may be encountered.

Table 2. Troubleshooting Information

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Possible cause</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>On a workstation running Windows 2000/2003/XP, user is prompted for PremierAccess credentials on initial login dialog; login attempt fails and user is never prompted for PremierAccess credentials in a separate dialog.</td>
<td>The Workstation Agent is not installed on the workstation.</td>
<td>Install the Workstation Agent component on the workstation.</td>
</tr>
<tr>
<td></td>
<td>There is a port mismatch between the Workstation Agent on that workstation and the Service Agent.</td>
<td>Use the SCCCONFIG utility to configure the port correctly. Specify the port entered on the Client Port tab on both the Workstation Agent and Service Agent machines.</td>
</tr>
</tbody>
</table>

More...
<table>
<thead>
<tr>
<th>Symptom</th>
<th>Possible cause</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Sub-authentication Filter on the domain controller authenticating the user is not pointing to a valid Service Agent.</td>
<td>Use the SCCCONFIG utility to configure the filter correctly. Specify the correct Service Agent on the Sub-auth Filter tab in the utility. Remember to press the <strong>Add</strong> button to add the machine to the list.</td>
<td></td>
</tr>
<tr>
<td>The Sub-authentication Filter and the Service Agent that it points to do not share the same private/public key pair.</td>
<td>Use the SCCCONFIG utility to configure the filter correctly. You can verify that the key is correct by exporting it from the Service Agent, examining the contents of the resulting .pky file, and then comparing them to the public key displayed on the Sub-auth Filter tab of the configuration utility. If necessary, export the key from the Service Agent, and import it into all Sub-authentication Filters in the domain. <strong>Note:</strong> The Service Agent will detect this situation, and log an error message in the Event Log.</td>
<td></td>
</tr>
<tr>
<td>The Sub-authentication Filter and the Service Agent that it points to run on different machines and do not share common networking protocols.</td>
<td>Ensure that there is a shared networking protocol installed on both machines.</td>
<td></td>
</tr>
<tr>
<td>Either the Workstation Agent machine or the Service Agent machine does not have TCP/IP installed.</td>
<td>Ensure that TCP/IP is installed on both machines.</td>
<td></td>
</tr>
</tbody>
</table>
### Troubleshooting

#### On the Workstation Agent machine, the user is prompted for PremierAccess credentials; login attempt fails even though correct PremierAccess credentials are entered.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Possible cause</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Service Agent is not configured to point to a valid PremierAccess server.</td>
<td>Check your PremierAccess server configuration to make sure that the machine (or IP address) and port specified there are correct.</td>
<td></td>
</tr>
<tr>
<td>The PremierAccess server is not running.</td>
<td>Start the PremierAccess server.</td>
<td></td>
</tr>
<tr>
<td>The user name is not in the PremierAccess database.</td>
<td>Add the user to the PremierAccess database.</td>
<td></td>
</tr>
<tr>
<td>The <code>swec.dat</code> or <code>swec.md5</code> file is no longer in sync with the PremierAccess database.</td>
<td>Remove the <code>swec.dat</code> or <code>swec.md5</code> file from the WINNT\System 32 directory. The next successful authentication will create a new valid <code>swec.dat</code> or <code>swec.md5</code> file.</td>
<td></td>
</tr>
</tbody>
</table>

#### User expecting to be authenticated by PremierAccess is allowed to log in without being prompted for PremierAccess credentials.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Possible cause</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>User is not a member of SAFEWORD_USERS group.</td>
<td>Make user a member of SAFEWORD_USERS group.</td>
<td></td>
</tr>
<tr>
<td>Not all domain controllers in the domain have the Sub-authentication Filter installed.</td>
<td>Install and correctly configure the Sub-authentication Filter on all domain controllers in the domain.</td>
<td></td>
</tr>
</tbody>
</table>

#### User designated as a member of SAFEWORD_USERS group is granted access in spite of missing or invalid PremierAccess credentials.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Possible cause</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not all domain controllers in the domain have the Sub-authentication Filter installed.</td>
<td>Install and correctly configure the Sub-authentication Filter on all domain controllers in the domain.</td>
<td></td>
</tr>
</tbody>
</table>

More...
On the Agent (client) machine, the user is prompted for PremierAccess credentials several times in a row, even though correct PremierAccess credentials were entered the first time.

Clock discrepancy between computers running the Service Agent prevents the voucher from being accepted immediately after it has been issued.

Synchronize computer clocks between all computers running the Service Agent. This can be done by running the command: `net time \MACHINE_NAME\set\y` where MACHINE_NAME is the name of one of the computers running the Service Agent. If more than two machines are involved, they should all be synchronized to each other. Synchronization should be done periodically by running the above command in the startup script of each machine.