RSA ACE/Agent 5.2 for Web
Installation and Configuration Guide

Contact Information

See our web sites for regional Customer Support telephone and fax numbers.

RSA Security Inc.	RSA Security Ireland Limited
www.rsasecurity.com	www.rsasecurity.ie

Trademarks

License agreement

Note on encryption technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when exporting this product.

Distribution

Limit distribution of this document to trusted personnel.

First printing: December 2003

Contents

1 Overview

The RSA ACE/Agent 5.2 for Web allows you to use RSA SecurID to protect selected web pages.

The RSA ACE/Agent 5.2 for Web software, residing on a web server, intercepts all user requests for protected web HTML or WML pages. If a URL is protected by RSA SecurID, and the Web Agent software determines that a user is not authenticated, it requests the username and passcode and passes them to the RSA ACE/Server for authentication. When a user authenticates successfully, the Web Agent stores this information in a cookie in the user's browser. As long as the cookie remains valid, the user is granted access to web pages.

Note: Web access authentication protects **http** and **https** URLs. Because of security risks associated with **ftp** file transfers across the Internet (for example, anonymous user access), Web access authentication does **not** protect files on an **ftp** server. In addition, Web access authentication does not support gopher, news, ftp, wais, or telnet protocols.

Security Features

The following table describes some of the security features that the RSA ACE/Agent 5.2 for Web provides to protect your web resources.

Security Feature	Description
Two-factor authentication	To gain access to a protected web page, a user must enter his or her username and a valid RSA SecurID passcode, which consists of • A secret, memorized personal identification number (PIN). • The tokencode currently displayed on an RSA SecurID token.
Support for SSL	This feature establishes a private communication channel between the user and the web server, preventing third parties from eavesdropping.

Security Feature	Description
Tamper-evident cookies	The cookie that the Web Agent distributes to a user's browser contains • Information indicating the user has successfully authenticated. • An encrypted data string. The encrypted string is used to detect whether someone has altered the cookie contents. Any tampering is logged in the system Web Agent audit files. In addition, to help protect the URL if the user walks away from his or her computer, cookies have set expiration times.
Name locking	This feature prevents an intruder from detecting a legitimate login attempt, intercepting the user's passcode, and using the passcode to log in.
Auditing	The Web Agent records • Access attempts • Status of connections • Any instances of cookie tampering in audit logs on the Agent Host

Types of User Access

You can configure the Web Agent to protect URLs on the local server on which it is installed. In addition, you can configure the Web Agent to allow users access to URLs on other servers that the Agent protects in the same domain or in multiple domains.

For each access type, the Web Agent distributes a cookie(s) to the user's browser that provides single sign-on access, meaning the user does not have to re-authenticate to each protected resource during a browser session.

Note: On Windows machines, you can configure single sign-on access for web applications. For more information, see the appendix "Configuring the Server for Single Sign-On Access (Windows 2003 Only)" in this book.

The following table describes the different types of user access.

Access Type	Cookie(s) Distributed to User's Browser Upon Successful Authentication	Protected URLs the User Can Access	Configuration Instructions
Local	Local Cookie	Protected URLs on the local web server	• UNIX: "Using the Setup Menu" on page 16 • Windows: "Configuring Web Access Authentication Cookies" on page 34
Domain	Domain Cookie	Protected URLs on all web servers in the domain	• UNIX: "Using the Domain and Multi-Domain Menu" on page 18 • Windows: "Configuring Multi-Server and Multi-Domain Authentication" on page 38
Multi-Domain	Domain cookies from each domain	Protected URLs on web servers in multiple domains	• UNIX: "Using the Domain and Multi-Domain Menu" on page 18 • Windows: "Configuring Multi-Server and Multi-Domain Authentication" on page 38

Getting Started

For Apache or Sun ONE

- For instructions on installing or upgrading, see the chapter "Installing the RSA ACE Agent for Web (UNIX)" in this book.
- For instructions on configuring Web access authentication cookies, protecting resources, configuring advanced settings, and setting up multi-server and multi-domain authentication, see the chapter "Configuring Web Access Authentication Settings (UNIX)" in this book.
- For information about customizing HTML or WML templates, see the chapter "Customizing Templates and Message Strings" in this book.
- For troubleshooting information, see the chapter "Troubleshooting (UNIX and Windows)" in this book.

For Windows 2000 Server or Windows 2003 Server

- For instructions on installing or upgrading, see the chapter "Installing the RSA ACE/Agent for Web (Windows)" in this book.
- For instructions on configuring Web access authentication cookies, protecting resources, configuring advanced settings, and setting up multi-server and multi-domain authentication, see the chapter "Configuring Web Access Authentication Settings (Windows)" in this book.
- For information about customizing HTML or WML templates, see the chapter "Customizing Templates and Message Strings" in this book.
- For troubleshooting information, see the chapter "Troubleshooting (UNIX and Windows)" in this book.

Getting Support and Service

RSA SecurCare Online	**https://knowledge.rsasecurity.com**
Customer Support Information	**www.rsasecurity.com/support**

Make sure that you have direct access to the computer running the RSA ACE/Agent 5.2 for Web software.

Please have the following information available when you call:

- ❑ RSA ACE/Server software version number.
- ❑ The make and model of the machine on which the problem occurs.
- ❑ The name and version of the operating system under which the problem occurs.

2 Installing the RSA ACE Agent for Web (UNIX)

Installation Requirements

Note: Make sure the web server machine is located in a secure area so that only trusted personnel can access the Web Agent.

Supported Platforms and Web Servers

- Sun ONE Web Server 6.0 on Solaris 8 and 9 on Sun UltraSparc workstations

  Note: The RSA ACE/Agent for Web does not support wireless access protocol on Sun ONE Web Servers.

- Apache Web Server 1.3.27 with mod_ssl2.8.14 on Solaris 8 on Sun UltraSparc workstations and Red Hat Linux 7.3 on an Intel Pentium or higher
- Stronghold Web Server 4.0 with Apache 1.3.x on Solaris 8 on Sun UltraSparc workstations and Red Hat Linux 7.3 on an Intel Pentium or higher

Client System Requirements

Users accessing protected web pages must have one of the following web browsers installed on their computers:

- Microsoft Internet Explorer 5.5 and 6.0
- Netscape Navigator 7.1

RSA SecurID Web authentication through wireless access protocol requires the following WAP 1.1 and 1.2.1 specifications:

- Caching of cookies
- WML Document Type Definition (DTD) version 1.1

RSA SecurID users must enable the cookie acceptance feature in their browsers. They must also use web browsers that support FORMs and Persistent Client State HTTP Cookies.

Additional Requirements

The RSA ACE/Agent 5.2 for Web works in conjunction with RSA ACE/Server 5.x or later. The Web Agent administrator should be familiar with the RSA ACE/Server system and its features.

In addition, make sure the RSA ACE/Server administrator has registered the RSA SecurID users in the RSA ACE/Server database and distributed tokens.

Pre-Installation Tasks

Before you install the Web Agent, you need to configure your web server and RSA ACE/Server environments to work with the Agent.

If you are using an Apache Web Server, go to the following section, "Enabling the Apache Web Server to Work with the Agent."

If you are using a Sun ONE Web Server, go to "Adding the Web Server to the RSA ACE/Server Environment" on page 12.

Enabling the Apache Web Server to Work with the Agent

The Apache server binaries must have module **mod_so** enabled. This module supports loading shared objects into the server at start-up or restart time.

If your Apache web server is already installed and configured, use the following procedure to check whether this module is enabled.

1. Change to the Apache server installation directory. For example:

   ```
   cd /usr/local/apache/bin
   ```

2. Type this command to list the Apache web server modules that are enabled.

   ```
   ./httpd -l
   ```

3. Look for **mod_so.c** in the output.

   If **mod_so** is not listed, you must recompile the Apache web server binaries with this module enabled. For instructions, refer to your Apache documentation.

Go to the following section, "Adding the Web Server to the RSA ACE/Server Environment."

Adding the Web Server to the RSA ACE/Server Environment

To add the Web Server to the RSA ACE/Server environment:

1. Add the web server to the RSA ACE/Server as an Open Agent Host. Ask your RSA ACE/Server administrator for assistance.
2. Obtain the **sdconf.rec** file from your RSA ACE/Server administrator, and place the file in a directory that is accessible to the web server and RSA ACE/Agent for Web software (for example: **var/ace**).

   The Web Agent software uses the **sdconf.rec** file to locate the RSA ACE/Server on the network.
3. Log into an account on the web server machine that has write permissions to the web server root directory. This is the web server user account designated in your web server configuration file.

4. Add a VAR_ACE environment variable to your web server configuration file so it is set whenever the web server runs. This environment variable identifies the location of the **sdconf.rec** file. For example:

```
setenv VAR_ACE /var/ace
```

Note: Make sure the user who owns the web server has write permissions to the directory specified by VAR_ACE. By default, this user is "nobody."

Installing the Web Agent Software

The Web Agent software requires approximately 10 MB of free disk space.

Note: RSA Security recommends that you stop your web server before installing the Web Agent. However, if you have web sites that cannot be taken out of service, the Agent will install with http services running.

To install the RSA ACE/Agent 5.2 for Web software:

1. Log into an account that has write permissions to the web server root directory.
2. Change to the directory you created when you downloaded the software, and run the install script by typing

   ```
   ./install
   ```

   When prompted to specify where you obtained your Web Agent product, if you obtained it from somewhere other than the countries listed, type **n**. Otherwise, press ENTER.
3. Accept the License Terms and Conditions by typing **A**.
4. If the **sdconf.rec** path is correct, press ENTER.

   The pathname entered for the VAR_ACE environment variable is displayed. If the pathname is not correct, it may not be correctly defined in the variable. For information about this setting, see the preceding section, "Adding the Web Server to the RSA ACE/Server Environment."
5. For each of the remaining installation prompts, press ENTER to accept the default value, or type in a different path.

   Note: If you are installing on Sun ONE, you must accept the defaults.

The install script creates a backup of the **.conf** files, using the format ***file*.conf.*date***, where *date* is the date and time the backup was created.

The configuration script starts automatically. For directions, see "Configuring the Software" on page 15.

Upgrading From RSA ACE/Agent 5.0 or 5.1 for Web

Important: Before upgrading, make backup copies of any customized HTML or WML files, and store the backup copies outside of the */Web_Agent_installation_directory*/**templates** directory. After you complete the upgrade tasks, you must configure the Web Agent to point to the customized templates. For directions, see "Specifying the Location of Customized Templates on UNIX Agent Hosts" on page 46.

Install the RSA ACE/Agent 5.2 for Web according to the instructions in the preceding section, "Installing the Web Agent Software."

The software installation makes a copy of your current configuration file (**.conf.old**) and your current **.ini** file (**.ini.old**). After the software installation is complete, the configuration script begins automatically and reads in your current configuration settings.

To keep your current settings, press ENTER at each of the configuration menus. To make changes to your configurations, select the appropriate menu item. For detailed directions, see "Configuring the Software" on page 15.

Uninstalling the Web Agent

Note: RSA Security recommends that you stop your web server before uninstalling the Web Agent. However, if you have web sites that cannot be taken out of service, you can uninstall the Agent with http services running.

To uninstall the Web Agent:

1. Change to the web server directory.
2. Run the uninstall script from the web server directory by typing

   ```
   rsawebagent/uninstall
   ```

3. (Not applicable for Linux) Remove the **rsawebagent** directory by typing

   ```
   rm -rf rsawebagent
   ```

Next Steps

- For administration tasks such as managing URLs and changing configuration settings, see the chapter "Configuring Web Access Authentication Settings (UNIX)" in this book.
- To customize the HTML and WML pages included with this Web Agent product, see the chapter "Customizing Templates and Message Strings" in this book.

3 Configuring Web Access Authentication Settings (UNIX)

You administer the Web access authentication settings of your web servers through a utility that allows you to quickly add, remove, and view URLs from the protected resource list, without having to directly access all of the configuration settings.

With the utility, you can

- Configure Web access authentication cookies
- Protect entire sites, individual directories, or individual files
- Configure advanced settings
- Set up multi-server and multi-domain authentication

Note: When you make changes to the Web access authentication properties of a virtual server, a directory, or a file, you must restart the web server.

Configuring the Software

The initial configuration sets default attribute values in the Web Agent configuration file. Once this configuration is complete, run the configuration script again if you want to make changes to individual virtual servers set up on this web server. For more information, see "Changing Configuration Settings" on page 20.

The configuration program is grouped into the following menus:

Setup Menu. Used to configure how the Agent interacts with the browser. Includes:

- Adjusting cookie validity time
- Changing the SSL port number
- Changing the WebID URL
- Changing the location of the HTML and WML templates

Configuration Menu. Used to configure access to protected URLs. Includes:

- Redirecting URLs to secure ports
- Using separate pages for username and passcode
- Using the name locking feature

Domain and Multi-Domain Menu. Used to configure for which domain(s) an authentication cookie is valid and generate a new domain secret for use on other Web Agents.

Using the Setup Menu

The Setup menu displays automatically following a successful installation.

To accept the defaults, press ENTER. Otherwise, type the line number of the option you want to change.

The following table describes the options.

Line Option	Description
1 Idle Cookie Expiration	Set the amount of time, in minutes, that an idle cookie is valid. When the cookie expires, the user must authenticate again. Setting a value that is greater than the Cookie Expiration value deactivates this feature.
2 Cookie Expiration	Set the length of time, in minutes, that an active cookie is valid. When the cookie expires, the user must authenticate again to get a new cookie.
3 SSL Port Number	Type in the SSL port number to be used for secure data transfer.
4 WebID URL	Accept the default name, unless you have an existing URL with the same name.
5 HTML/WML Templates	Accept the default. After the initial installation and configuration, you may customize the templates. Once you do so, run the configuration script again to designate the new location of your customized templates.

Using the Configuration Menu

The Configuration menu displays automatically after you complete the Setup menu.

To accept the defaults, press ENTER. Otherwise, type the line number of the option you want to change.

The following table describes the options.

Line Option	Description
1 Agent Protection	Accept the default. **Important**: Disable the Web Agent only when it is absolutely necessary to temporarily halt protection of all URLs on this web server for troubleshooting purposes. When the Web Agent is disabled, your valuable data is unprotected.

Line Option	Description
2 Name Locking	The Web Agent locks the user's name while waiting for the passcode so the name cannot be used elsewhere during the authentication process. **Note**: If your RSA ACE/Server is a pre- 5.0 version, this feature is not supported, and you need to disable it.
3 Separate Pages	The Web Agent uses separate HTML or WML pages to request the user's name and passcode. If you disable this feature, the username and passcode are sent across the Internet together.
4 Require SSL Connection	The Web Agent connects to protected URLs through an SSL port. If you disable this feature, data passed over the Internet is unprotected, meaning cookies can be seen in plain text.
5 Redirect	When a user attempts to access a protected URL through an unprotected page, the Web Agent redirects the user to an authentication page. If you disable this feature, the user receives an RSA Security message and a link to a secure connection. **Note:** This option does not appear if option 4, Require SSL Connection, is disabled.
6 Caching Pages	The Web Agent prevents the browser from caching protected URLs on the local PC. If you disable this feature, protected URLs may be cached on the local hard drive.
7 Auto Submit	After the user enters authentication information on the Web page, the Agent automatically presents the next screen so the user does not have to click CONTINUE.
8 JavaScript Pop-up	The web Agent allows the use of JavaScript Pop-up Windows for web pages that use frames. By default, this feature is disabled.
9 Ignore Browser Address	By default, this feature is disabled so that the Web Agent uses the browser IP address to sign the cookie. However if there is a proxy or a firewall between the browser and the Agent, the IP address used may be the same. If you have web sites that are accessed through load balanced proxy servers, meaning that the browser IP addresses may change, you may want to enable this feature. Otherwise, the user may have to authenticate quite frequently.

Line Option	Description
10 Current Domain Access	Once a user is authenticated, the user can access URLs on any of the web servers in the current protected domain. If you disable this feature, the user is asked to authenticate each time a protected URL is accessed on a different web server.
11 Multi-Domain Access	Once a user is authenticated, the user can access URLs on any web server in the multi-domain list. If you disable this feature, the user is asked to authenticate each time a protected URL is accessed on a web server that is outside the current domain.

Using the Domain and Multi-Domain Menu

If you enabled number 10 (Current Domain Access) or 11 (Multi-Domain Access) in the Configuration menu, the Domain and Multi-Domain Configuration menu displays automatically.

The following table describes the Domain and Multi-Domain Configuration menu options.

Line Option	Description
1 Generate Domain Secret	A domain secret was automatically generated when you installed the Web Agent. Use this option to generate a new domain secret. You may need to do this to be in accordance with company security procedures, for example.
2 Generate and Export Domain Secret	If you have multiple web servers on which users will be able to access protected URLs, each web server within the domain must have the same domain secret. Use this option to generate and export the domain secret to a file so you can import it to all other web servers at your site that will issue and accept domain cookies. You must name and create a password for the export file. The file is then stored in the Web Agent directory (the default is **rsawebagent**).
3 Import Domain Secret	If you are configuring protected URL access in a domain environment, use this option to import the domain secret from other Agent-protected web servers. You are asked for the file name and file password that you set up in option 2.

Line Option	Description
Current Domain Options	**The options below appear only if you chose number 10 (Current Domain Access) in the Configuration menu.**
4 Domain Name	Use this option to create subdomains. For example, suppose you have http://server1.domain1.domain.com http://server2.domain1.domain.com http://server3.domain2.domain.com http://server4.domain2.domain.com and you want to protect URLs on all of these servers. By entering **domain.com** as the Domain Name, you create a subdomain which includes all of the web servers above. You must enter a domain name.
5 Cookie Name	Use this option to change the default cookie name (rsacookie). Maximum name length is 30 characters.
Multi-Domain Options	**The options below appear only if you chose number 11 (Multi-Domain Access) in the Configuration menu.**
6 Add to Multi-Domain List	Enter the Agent-protected web servers on which you want all users to access protected URLs once they have authenticated. Use the format http://*server1.domain1.com*. You must enter a domain name.
7 Remove from Multi-Domain List	The Multi-Domain List of Agent-protected web servers displays. Choose the number of the web server you want to remove from the list. (This option does not appear if there are no hosts in the Multi-Domain List.)
8 View Multi-Domain List	View the list of Agent-protected web servers you entered with option 6 for the Multi-Domain List. (This option does not appear if there are no web servers in the Multi-Domain List.)

CAUTION: If you have separate web servers that authenticate users to separate RSA ACE/Server databases, specify different domain secrets for the different domain cookies. Otherwise, users might gain unauthorized access to protected URLs.

After you have configured the Agent for the first time following installation, the product registration web page opens. If you choose not to register now, you can access the page at your convenience, or you can run the registration script (**./registerWA**) from the Web Agent installation directory.

Changing Configuration Settings

You may need to make adjustments to the default configurations for the Web Agent. For example, you may find that you need a longer cookie expiration time.

To change configuration settings:

1. Run the configuration script in the Web Agent installation directory. Type

   `/web_server_directory/rsawebagent/config`

   A list of the current web server and any virtual servers you have set up in the web server configuration file displays.

2. Choose the server(s) you want to configure. You can make changes to the default settings applied to all servers, or you can make changes to an individual server.

For details about the different configuration menus, see the preceding section, "Configuring the Software."

Managing URLs

By default, the Web Agent protects all URLs on the web server on which the Agent is installed. The **protectURL** utility is an interactive menu from which you can add, remove, or unprotect individual URLs. The **protectURL** utility is located in the default Web Agent directory. Type

```
./protectURL
```

You can also manage the protected resource list by importing a list of URLs from a file. To add URLs to the protected resource list, type

```
./protectURL -a -f listURL
```

where *listURL* is a text file that contains a list of URLs, with one URL per line, that you want to add to the resource list.

To remove protected URLs from the resource list, type

```
./protectURL -d -f listURL
```

All of the URLs listed in the file are removed from the protected resource list.

Important: When you unprotect a URL, all URLs under it are also unprotected.

Advanced UNIX administrators can manage the protected resource list using command line only operations. Type

```
./protectURL -h
```

for a list of options and syntax.

Adding and Removing Virtual Web Servers

To add additional virtual servers to the Web Agent configuration:

1. Run the configuration script with the name of the virtual web server. Type

   ```
   ./config server.domain.com
   ```

2. Verify that you want to create the new server.
   The Setup menu displays.

For details about the different configuration menus, see the preceding section, "Configuring the Software."

You can add as many virtual servers as you like. However, if you want access to protected URLs to function the same way on all virtual web servers, you need to make changes to your default web server rather than individual virtual servers.

To remove a virtual server from the Web Agent configuration file:

Use the -d option by typing

```
./config -d server.domain.com
```

Note: Removing a virtual server from the configuration file does not remove or disable the web server or the Web Agent.

Using the Log Out URL to Invalidate Web Access Authentication Cookies

The Log Out URL enables you to set up a link on a web page that automatically invalidates users' Web access authentication cookies and prompts users to authenticate.

To set up the Log Out URL, add the following URL to a link on your web pages:

http://www.*domain*.com/webauthentication?logoff?referrer=/*sample*.html

where ***domain*** is the domain name and ***sample*.html** is the web page.

Important: If you do not provide an argument to **referrer=**, users are sent to the root directory on the virtual Web server.

Using Auto-Redirect Scripts to Enforce RSA SecurID Authentication

The Web Agent includes an auto-redirect script that enables you to require users to authenticate before accessing a URL that is not formally protected by RSA SecurID. The URL does not have to be hosted on the same server or be within the same domain as the server on which the Web Agent is installed.

You use the customized redirect URL from the script as the hyperlink to the unprotected site. When a user clicks on the HTML link to the URL that you want to protect, the script is invoked, and the user is forced to authenticate before gaining access to the site.

The Perl script included with the Web Agent is a sample script only. To use it, you must first customize it with your own code.

To customize an auto-redirect script:

1. Copy the Perl sample script (**PerlScriptRedirect.pl**) from the **/cgi_scripts** directory of your Web Agent installation, and store it in the web server's **/cgi-bin** directory.
2. Customize the script with your own code.

   Important: RSA Security strongly recommends that your script contain a list of URLs that users are allowed to access using the redirect URL. The script's input argument should be compared to the list of allowed URLs before any redirect takes place. Any user who attempts to access the redirect hyperlink can see the link definition and could potentially use the redirect script to access the authentication cookie. By implementing a URL comparison list, you minimize the security risk.

3. Use the customized redirect URL from the script as the hyperlink to the unprotected site.

An example redirect URL looks like this:

http://<*protectedHostname*>/webauthentication?referrer=/cgi-bin/PerlScriptRedirect.pl?target=http://<*unprotectedHostname*>/new_application.jsp

- **/webauthentication/** is the virtual Web Agent reference. It ensures that a user attempting to access the unprotected URL is prompted to authenticate.
- **/cgi-bin/PerlScriptRedirect.asp** is the script that performs the redirect to the input argument.
- **http://<*unprotectedHostname*>/new_application.jsp** is the input argument, or unprotected URL.

For more information about customizing auto-redirect scripts, see the directions included in each script.

Configuring the Agent for Proxy Servers

To be able to authenticate through a proxy server, change the value of WebID_URL on the remote Agent-protected web server from the default value of **/webauthentication** to

https://proxyserver.domain.com/xxx/webauthentication

where **https://*proxyserver.domain.com*/xxx/** is the path to the root directory of the remote Agent-protected web server. To make the change, run the Web Agent configuration script on the remote Agent-protected web server. The WebID URL option is in the Setup menu of the configuration program.

4 Installing the RSA ACE/Agent for Web (Windows)

Installation Requirements

Supported Platforms

The RSA ACE/Agent for Web 5.2 is qualified to run on the following platforms:

- Windows Server 2003, Enterprise Edition, with Internet Information Server (IIS) 6.0
- Windows 2000 Server with Service Pack 4 and Internet Information Server (IIS) 5.0

Note: The machine cannot be an RSA ACE/Server Primary or Replica. Running both IIS and RSA ACE/Server on the same machine may result in a decrease in performance.

Host System Requirements

Your system must meet the following minimum requirements:

- Intel Pentium or higher.
- 32 MB of RAM.
- 10 MB of free disk space.
- TCP/IP networking.
- The disk partition containing the web server directories must be an NTFS partition.The FAT file system is not supported.
- Secure Sockets Layer (SSL) certificate.

  For more information about how to obtain an SSL certificate from a Certificate Authority, such as VeriSign, visit the VeriSign web site at **http://www.verisign.com**.
- If users access protected web pages through a proxy server, the proxy must support the passing of cookies.

Client System Requirements

Users accessing protected web pages must have one of the following web browsers installed on their computers:

- Microsoft Internet Explorer 5.5 and 6.0
- Netscape Navigator 7.1

RSA SecurID Web authentication through wireless access protocol requires the following WAP 1.1 and 1.2.1 specifications:

- Caching of cookies
- WML Document Type Definition (DTD) version 1.1

RSA SecurID users must enable the cookie acceptance feature in their browsers. They must also use web browsers that support FORMs and Persistent Client State HTTP Cookies.

Additional Requirements

The RSA ACE/Agent 5.2 for Web works in conjunction with RSA ACE/Server 5.x or later. The Web Agent administrator should be familiar with the RSA ACE/Server system and its features.

In addition, make sure the RSA ACE/Server administrator has registered the RSA SecurID users in the RSA ACE/Server database and distributed tokens.

Note: If you intend to use the Web Agent software to protect the files of multi-homed servers, you must account for the extra IP addresses in the RSA ACE/Server database. The RSA ACE/Server administrator has to define a secondary node for each additional IP address used on the Agent Host. In addition, you should specify an IP address override on the **Advanced** tab of the RSA ACE/Agent control panel; the override address should exactly match the network address specified for the Agent Host in the Server database. For instructions on how to define secondary nodes, consult the RSA ACE/Server documentation.

Compatibility with Other RSA ACE/Agents

You can run the RSA ACE/Agent 5.2 for Web on the same machine as the RSA ACE/Agent 5.5 or later for Windows.

Pre-Installation Tasks

Tasks for the RSA ACE/Server Administrator

The RSA ACE/Server administrator must complete the following tasks before you install the Web Agent:

- Register the RSA ACE/Agent Host as an Agent of the RSA ACE/Server. The Agent type must be **Net OS Client**.
- Register RSA SecurID users in the RSA ACE/Server database and distribute RSA SecurID tokens to those users.

Tasks for the Web Agent Administrator

You must complete the following tasks before you install the Web Agent:

- Obtain the RSA ACE/Server configuration file (**sdconf.rec**) from the RSA ACE/Server administrator. Copy the **sdconf.rec** to the ***%SYSTEMROOT%*\system32** directory of the Agent Host.
- Ask your RSA ACE/Server administrator if the usernames in the RSA ACE/Server database records have the user's Windows domain name attached (for example, **DOMAIN\username**). If so, you must select the **Send domain and username to RSA ACE/Server** option when you enable RSA ACE/Agent authentication.

  For more information about this option, see "Using Advanced Configuration Options" on page 35 in the chapter "Configuring Web Access Authentication Settings (Windows)" in this book.

Installing the Web Agent Software

The directions in this section apply to new installations on Windows 2000 Server and Windows 2003 Server.

To install the Web Agent software:

1. Log in to the machine as a local administrator.
2. Browse to the directory you created when you downloaded the software, and double-click **setup.exe**.
3. Follow the prompts until the sdconf.rec Location dialog box opens. Specify the location of the configuration file you obtained from your RSA ACE/Server administrator.
4. Follow the prompts to complete the installation.

After you finish installing the Web Agent, you must configure the Microsoft Internet Service Manager. For instructions, see the following section, "Configuring the Microsoft Internet Service Manager."

Configuring the Microsoft Internet Service Manager

To configure ISM, you must complete the following tasks:

- Install a Secure Sockets Layer (SSL) certificate on the web server. If you do not have an SSL certificate installed, the Web access authentication username and passcode will not be encrypted before transmission.

  For more information about how to obtain an SSL certificate from a Certificate Authority, such as VeriSign, see the Microsoft Internet Service Manager Help, or visit the VeriSign web site at **http://www.verisign.com**.

- Configure the Password Authentication settings of the ISM. For instructions, see the following section, "Configuring ISM Password Authentication Properties."
- Make sure the RSA SecurID ISAPI filter and the Watchdog ISAPI filter have priority over all other ISAPI filters. For instructions, see "Setting the Priority Level for the RSA SecurID ISAPI Filter" on page 29 and "Setting the Priority Level for the Watchdog ISAPI Filter" on page 30.

After you have installed the Web Agent and configured the Microsoft Internet Service Manager, you must configure the RSA SecurID Web access authentication settings of your IIS web servers.

For instructions, see the chapter "Configuring Web Access Authentication Settings (Windows)" in this book.

Configuring ISM Password Authentication Properties

To configure your IIS password authentication properties:

1. To open the Internet Service Manager (ISM), click **Start > Settings > Control Panel**, and double-click **RSA Web Agent**.
2. In the left pane of the MMC, right-click the name of the web site that you want to protect, and then click **Properties**.
3. Click the **Directory Security** tab, and in the **Anonymous Access and Authentication Control** (Windows 2000) or **Authentication and access control** (Windows 2003) area, click **Edit**.
4. To activate Windows password authentication for users accessing the web server, go to step 5. Otherwise, to permit anonymous users to browse the web server directories using the default anonymous login username and password (usually IUSR_*machinename* in the User Manager)
   - Select **Anonymous Access** on Windows 2000 or **Enable anonymous access** on Windows 2003.

     Note: Selecting this option does not bypass Web access authentication on protected files or directories, nor does it bypass the file- and directory-level security permissions that have been set using the Windows access control tools.

   - Proceed to step 6.

5. In the **Authenticated access** area, to activate Windows password authentication for users accessing the web server, check one of the following options:

   - **Basic authentication (password is sent in clear text)**. Provides Windows username and password authentication for all brands of web browsers. If you choose this option, RSA Security strongly recommends that you have an SSL certificate installed on the web server and that you select the **Require secure connection to access protected pages** option on the RSA SecurID Web access authentication properties sheet in the ISM. Otherwise, the usernames and passwords are transmitted as unencrypted clear text, which is a high security risk.

     Users in a Windows Domain environment must append their Domain name to their username at the password prompt.

   - Integrated Windows Authentication allows Microsoft Internet Explorer users who are logged in to the Windows Domain or a Workgroup to access the web server without being prompted for a username and password.

   If you do not select either option, users accessing protected pages with Microsoft Internet Explorer receive the **A required header is missing/not found** error and cannot be authenticated.

   If your organization uses more than one type of web browser, check both **Basic authentication (password is sent in clear text)** and **Integrated Windows Authentication**.

   Note: Do not enable Windows Challenge/Response if a user's Windows login username is different from the user's RSA SecurID username recorded in the RSA ACE/Server database.

6. Click **OK** to return to the Properties window, and then click **OK** to save the property settings.

Setting the Priority Level for the RSA SecurID ISAPI Filter

To give the RSA SecurID Watchdog ISAPI filter priority over all other filters:

1. Click **Start > Settings > Control Panel**, and double-click **RSA Web Agent**.
2. In the left panel, right-click the name of the Agent Host machine, and click **Properties**.
3. In the **Internet Information Services** tab, under Master Properties, click **Edit**.
4. Click the **ISAPI Filters** tab.
5. If the RSA SecurID ISAPI filter is not displayed at the top of the list, move it to the top using the arrow on the left-hand side of the filter list.
6. Click **Apply**, and then click **OK**.
7. Click **OK** again.
8. Restart the web server.

Setting the Priority Level for the Watchdog ISAPI Filter

To give the RSA SecurID Watchdog ISAPI filter priority over all other filters:

1. Click **Start > Settings > Control Panel**, and double-click **RSA Web Agent**.
2. In the left panel, double-click the name of the Agent Host machine to display its list of virtual web servers.
3. Right-click the name of the virtual server whose properties you want to view, and click **Properties**.
4. Click the **ISAPI Filters** tab.
5. If the Watchdog ISAPI filter is not displayed at the top of the list, move it to the top using the arrow on the left-hand side of the filter list.
6. Click **Apply**, and then click **OK**.
7. Restart the web server.

Upgrading from RSA ACE/Agent 5.0 for Windows (Windows 2000 Only)

To upgrade from the RSA ACE/Agent 5.0 for Windows on a Windows 2000 Server to the RSA ACE/Agent 5.2 for Web, you must perform the following tasks:

- **Task 1**: Make a backup copy of any customized HTML or WML files and store the backup copies outside of the /***Web_Agent_installation_directory***/templates directory.

  Note: After you complete the upgrade tasks, you must configure the Web Agent to point to the customized templates. For directions, see "Specifying the Location of Customized Templates on Windows Agent Hosts" on page 46.

- **Task 2**: Install the RSA ACE/Agent 5.2 for Web, which will upgrade the web component of the Agent. For instructions, see "Installing the Web Agent Software" on page 27.
- **Task 3**: Through Add/Remove Programs, uninstall the RSA ACE/Agent 5.0 for Windows.
- **Task 4**: To reconcile the removal of shared code, run the Web Agent installation in Repair Mode. For instructions, see "Running the Web Agent Install in Repair Mode" on page 31.
- **Task 5 (Optional)**: Install RSA ACE/Agent 5.5 for Windows. For instructions, see the RSA ACE/Agent 5.5 for Windows documentation.

  Note: The RSA ACE/Agent 5.5 for Windows installation replaces the RSA ACE/Agent Control Panel with its own version. However, your configurations settings remain intact.

Note: The RSA ACE/Agent for Web 5.2 cannot co-exist with versions of the RSA ACE/Agent for Windows prior to 5.5. In addition, if you later uninstall RSA ACE/Agent 5.5 for Windows, you must run the Web Agent 5.2 installation in Repair Mode. For instructions, see "Running the Web Agent Install in Repair Mode" on page 31.

Running the Web Agent Install in Repair Mode

Repair Mode reconciles the addition or removal of code that the Web Agent shares with another RSA ACE/Agent, such as the RSA ACE/Agent for Windows.

To run the Web Agent installation in Repair Mode:

1. In the Windows Control Panel, click **Add/Remove Programs**.
2. Under **Currently Installed Programs**, click **RSA ACE/Agent for Web**, and then click **Change**.
3. In the Welcome dialog box, click **Next**.
4. In the Program Maintenance dialog box, select **Repair**, and click **Next**.
5. Follow the prompts to complete the installation.

Next Steps

After you upgrade the Web Agent, even though your configuration settings and protected URLs are preserved, you must re-enable RSA Web Access protection on the site level. For instructions, see the Help topic "Enabling Web Access Authentication."

Uninstalling the RSA ACE/Agent for Web

To uninstall RSA ACE/Agent 5.2 for Web:

1. In the Windows Control Panel, click **Add/Remove Programs**.
2. Scroll down and click **RSA ACE/Agent for Web**.
3. Click **Remove**.

5 Configuring Web Access Authentication Settings (Windows)

Opening the Web Access Authentication Properties Sheet

You administer the Web access authentication settings of your IIS web servers locally or remotely through an Internet Service Manager (ISM) that has been extended with the RSA SecurID Web access authentication property sheet.

From the ISM, you can

- Configure Web access authentication cookies
- Protect entire sites, individual directories, or individual files
- Configure advanced settings
- Specify the location of customized templates
- Set up multi-server and multi-domain authentication

Note: When you make changes to the Web access authentication properties of a virtual server, you must restart the virtual server from the ISM.

To display the RSA SecurID Web access authentication properties sheet:

1. To open the ISM, click **Start > Settings > Control Panel**, and double-click **RSA Web Agent**.
2. Double-click the name of the Agent Host machine to display its list of virtual web servers.
3. Right-click the name of the virtual server whose properties you want to view, and click **Properties**.
4. Click the **RSA SecurID** tab.

Configuring Web Access Authentication Cookies

Each time an RSA SecurID user enters a valid passcode at the Web access authentication prompt, the web server stores a Web access authentication cookie in the user's web browser. The cookie passes the user's authentication information to the server when the user browses to a protected file or directory on that server. As long as the cookie is still valid, the user does not have to authenticate again during the current session. A cookie is valid only during the browsing session for which it was created. If the user closes the web browser, he or she must re-authenticate to get a new cookie.

For instructions on setting cookie expiration times, see the Help topics "Controlling Cookie Expiration Times" and "Setting Cookie Expiration Times." For information about cookies that are valid on multiple servers in a domain or on multiple domains, see "Configuring Multi-Server and Multi-Domain Authentication" on page 38.

Note: You can use the RSA ACE/Agent Web Authentication API to add information, which you extract at a later time, to the cookie. For more information, see the *RSA ACE/Agent Web Authentication API Guide*.

Protecting Resources

The following table describes the different options for protecting resources. For instructions, see the related Help topic for each option.

Protection Option and Related Help Topic	Notes
Protecting an Entire Site	By protecting the virtual server, you are protecting the root directory and everything contained by it. Do not attempt to protect only the **default.htm** file. Instead, protect the entire virtual web server, but remove the protection settings on specific directories or files that you want to make available for access by anyone. **Note**: The Web Agent supports multiple virtual servers on the same physical machine.
Protecting Individual Directories	RSA Security recommends that you protect entire directories. Any files or sub-directories that you add to the directory after you change its Web access authentication settings will automatically inherit those settings, unless you change the settings on a specific file or directory.

Protection Option and Related Help Topic	Notes
Protecting Individual Files	Web access authentication provides the ability to protect individual virtual web server files, but this option is not as efficient as protecting the entire directory that contains the file. When you protect a directory, any files or subdirectories you add to the directory later are protected automatically. Protecting files instead of specific directories creates additional administrative overhead. With individual file protection, you must enable URL protection on a per-file basis, which may result in some files being overlooked and left unprotected.

Using Advanced Configuration Options

The following table describes the configuration options available through the RSA SecurID Web access authentication properties sheet. For instructions, see the related Help topic for each option.

Configuration Option and Related Help Topic	Description
Using SSL Connections	A Secure Socket Layer certificate prevents unauthorized users from monitoring the connection, intercepting a user's passcode, and gaining access to protected pages. RSA Security strongly recommends that you enable SSL.
Controlling Redirection of HTTP Connections	If you enable SSL, clients that connect using a non-SSL (HTTP) connection are redirected to a page with a link to the HTTPS server. Rather than display a page with a link, you can automatically redirect users to the secure server. For example, if a user attempts to access a protected resource at **http://www.exampledomain.com/sales_figures/**, the user's request would be redirected automatically to **https://www.exampledomain.com/sales_figures/** (note use of the **HTTPS** protocol).

Configuration Option and Related Help Topic	Description
Disabling the IIS Server If the Agent Fails to Initialize	If the Web access authentication feature set fails to load properly during web service startup, the IIS server is disabled and all users who try to access URLs on the server see an error page. The server is disabled to ensure that unauthorized users do not gain access to protected resources. RSA Security recommends that you enable this feature for optimum protection of web resources. If you do not disable the virtual web server, in the event of a failure all protected resources are fully available to any person who gains access to the server.
Enabling Group Security	The Group Security feature allows you to control group access to protected web resources. For more information, see "Controlling Group Access to Protected Web Resources" on page 39.
Sending the Domain Name with the Username	If your RSA ACE/Server database records have users' domain names appended to their usernames (for example, **DOMAIN\jsmith** instead of simply **jsmith**), you can configure Web access authentication to send the full domain\username string during authentication to the RSA ACE/Server. To use this feature, you must have password authentication enabled on your web server. For more information, see the Microsoft Internet Information Server (IIS) documentation. When RSA SecurID users attempt to access a page that is protected by Web access authentication, they must first enter their Windows usernames and passwords. You must instruct users to always enter their domain names with their usernames (for example, **DOMAIN\jsmith**). When the RSA SecurID passcode authentication prompt displays, the full domain\username string is inserted automatically in the **Username** field.
Preventing Caching of Protected Pages	If an RSA SecurID user's browser is left unattended, an unauthorized user can view pages that are stored in the cache long after the user has quit his or her browsing session. When you prevent the caching of protected pages, you minimize the security risk.
Authenticating Through a Firewall (Ignore Browser IP Address for Cookie Validation)	If you have a firewall and some users are being prompted to authenticate every time they attempt to access a protected page, you must configure the Web Agent to authenticate through a firewall.

Configuration Option and Related Help Topic	Description
Enabling Name Locking	Name locking protects against the danger that someone might observe a user entering the passcode and present the same passcode on a different Agent Host in the realm. With name lock, the Agent Host sends the user's login name and passcode to the RSA ACE/Server separately. If someone attempts to use the same username and passcode, the Server refuses the authentication request.
Using Separate Username and Passcode Pages	If you enabled name locking, you can also configure the Web Agent to display separate username and passcode pages to the user.
Using a JavaScript Pop-up Window to Authenticate in Frames	If the protected web site uses HTML frames, oftentimes the passcode prompt ends up being too small to read clearly. To avoid this problem, the passcode prompt can be displayed in a JavaScript pop-up window.
Enabling Auto Submit (avoid having to click Continue after successful Auth)	By default, after a user authenticates successfully, the Web Agent displays a success page on which the user must click **Continue** in order to access the desired URL. When you enable Auto Submit, after a user authenticates successfully, the desired URL opens without the user having to click **Continue**.
Using Text Link Authentication Mechanism for Multi-Domain WML Access	During multi-domain authentication, the Web Agent attempts to get an image from each of the domains to verify that it has made a connection. Some cell phones display the image even though the Web Agent has not connected successfully. Once the user has authenticated in a multi-domain environment and then attempts to access a URL in another domain, he or she is prompted to authenticate again. This option forces the user to manually click on a text link for each domain instead of attempting to automatically make the connection using images.
Disabling Cookie API Processing	This option allows you to disable any cookie API processing that you have implemented. **Note**: If you enable single sign-on, cookie API processing is automatically enabled.

Configuration Option and Related Help Topic	Description
Using the Standard Page Cache Prevention Mechanism for WML Access	Because many cell phones do not respond to the standard method of preventing page caching, the Web Agent uses an alternative method for WML access. However, the standard method is more efficient. This option configures the Web Agent to attempt to use the standard method of preventing page caching. To use this feature, you must first enable **Prevent Caching of Protected Pages on Clients**, and the user's cell phone must be capable of using the standard no cache method.

Configuring Multi-Server and Multi-Domain Authentication

The Web Agent offers the ability for RSA SecurID users to authenticate on virtual web servers across multiple web domains. A user enters his or her passcode only once to authenticate to each of the participating web servers. After authenticating successfully, the user has access to protected resources in the participating web servers' domains.

Important: Domain cookies bypass a workstation's Agent Host activations in the RSA ACE/Server database. RSA SecurID users whose browsers use a domain cookie from one server might gain access to information on other servers that they are usually not allowed to view. Restrict access to confidential directories by assigning **Read** permission only to the appropriate RSA SecurID users. For information on setting security permissions, see the Windows 2000 or Windows 2003 documentation.

For instructions on setting up multiple server or multiple domain authentication, see the Help topics "Setting Up Multiple Server Authentication: Overview" and "Setting Up Multiple Domain Authentication: Overview."

Using the RSA ACE/Agent Control Panel

The RSA ACE/Agent control panel contains the tools you need to perform test authentication and configure advanced security settings.

Important: The configuration settings on the Advanced properties sheet of the RSA ACE/Agent control panel are set to work in most installations of the Agent. You should not reset them unless doing so will improve performance.

To open the RSA ACE/Agent control panel:

In the Windows Control Panel, double-click the **RSA ACE/Agent** icon.

For instructions on configuring advanced security settings, see the RSA ACE/Agent Control Panel Help.

Testing Authentication

Before you deploy tokens to users, use the RSA ACE/Agent Control Panel to test that Web Agent authentication has been correctly implemented. The test verifies that

- The **sdconf.rec** file you installed on the Agent Host points to the appropriate RSA ACE/Server database.
- The host has a valid node secret file.
- Your system is configured properly for authentication.

For testing purposes, use a token that already has a PIN. For directions, see the RSA ACE/Agent Control Panel Help topic “Testing Authentication.”

Controlling Group Access to Protected Web Resources

The Group Security feature allows you to control group access to protected web resources.

When you enable Group Security, during user authentication, the Web Agent stores the list of group memberships from the user’s RSA ACE/Server record in the user’s Web access authentication cookie. Once the user is authenticated, the system compares the Windows group permissions of the requested resource to the groups listed in the user’s cookie. If a valid match is found, the user gains access to the resource. If no valid match is found, the user is denied access to the resource.

For example, you want only managers to be able to gain access to the Inet451 directory on the web server. By enabling the Group Security feature, you can ensure that

- The Inet451 directory is protected by Web access authentication.
- Only users who have Manager in the Shell field of their RSA ACE/Server database record can gain access to the directory.

Note: If the IIS machine is a PDC (primary domain controller) or BDC (backup domain controller), you cannot create a local non-domain group. Therefore, you cannot use the Group Security feature on a PDC or BDC.

To enable the Group Security feature, you must perform the following tasks:

- **Task 1:** Create a local group. Perform this procedure on the web server.
- **Task 2:** Activate a user on the Agent Host. Perform this procedure through the RSA ACE/Server Database Administration application.
- **Task 3:** Associate the local group with a file protected by RSA SecurID. Perform this procedure on the web server.
- **Task 4:** Enable group security. Perform this procedure on the web server.

Task 1: Creating a Local Group

To create a local group:

1. On the web server, click **Start > Programs > Administrative Tools > Computer Management**.
2. Double-click **Local Users and Groups**.
3. Right-click **Groups**, and select **New Group**.
4. Fill in the appropriate name and description, and click **Create**.

   Note: You do not need to fill in the **Members** field.

5. Repeat step 4 for each group you want to create.

Task 2: Activating a User on the Agent Host

Note: The following procedure describes how to activate a user directly on an Agent Host. The RSA ACE/Server also allows you to activate users on Agent Hosts through RSA ACE/Server groups. If a user is activated on a Agent Host both directly and through a group with the same username but different **Shell** fields, the direct **Shell** field overrides the group **Shell** field.

To activate a user on the Agent Host:

1. From the RSA ACE/Server Database Administration application, open the appropriate user record.
2. Click **Agent Host Activations**.
3. In the Available Agent Hosts panel, select the web server, and click **Activate on Agent Hosts**.
4. In the Activate User dialog box, do the following:
   - In the **Login** field, type the appropriate username.
   - In the **Shell** field, type the name of the local group you created on the web server.

     Note: If you are entering multiple group names in the **Shell** field, you must separate the names by a comma, but do not insert any spaces in the field. For example, Sales,Marketing,HQ.

   - Click **OK**.

Task 3: Associating the Local Group with a File Protected by RSA SecurID

To associate the local group with a file protected by RSA SecurID:

Note: You must perform this procedure through Windows Explorer, **not** the ISM.

1. On the web server, open Windows Explorer, and browse to the file you want to associate with the local group.
2. Right-click the file, and select **Properties**.
3. From the **Security** tab, add the local group(s) you created on the web server, and assign the appropriate permissions.
4. Click **OK**.

Task 4: Enabling Group Security

To enable Group Security

1. To open the ISM, click **Start > Settings > Control Panel**, and double-click **RSA Web Agent**.
2. Double-click the name of the Agent Host machine to display its list of virtual web servers.
3. Right-click the name of the virtual server whose properties you want to view, and click **Properties**.
4. Click the **RSA SecurID** tab.
5. Under **Advanced Settings**, check **Enable Group Security**.

Using the Log Out URL to Invalidate Web Access Authentication Cookies

The Log Out URL enables you to set up a link on a web page that automatically invalidates users' Web access authentication cookies and prompts users to authenticate.

To set up the Log Out URL, add the following URL to a link on your web pages:

http://www.*domain*.com/WebID/IISWebAgentIF.dll?logoff?referrer=/*sample*.html

where ***domain*** is the domain name and ***sample*.html** is the web page.

Note: If you do not provide an argument to **referrer=**, users are sent to the root directory on the virtual Web server.

Using Auto-Redirect Scripts to Enforce RSA SecurID Authentication

The Web Agent includes auto-redirect scripts that enable you to require users to authenticate before accessing a URL that is not formally protected by RSA SecurID. The URL does not have to be hosted on the same server or be within the same domain as the server on which the Web Agent is installed.

You use the customized redirect URL from the script as the hyperlink to the unprotected site. When a user clicks on the HTML link to the URL that you want to protect, the script is invoked, and the user is forced to authenticate before gaining access to the site.

The ASP and Perl scripts included with the Web Agent are sample scripts only. To use them, you must first customize them with your own code.

To customize an auto-redirect script:

1. Copy either the ASP sample script (**AspScriptRedirect.asp**) or the Perl sample script (**PerlScriptRedirect.pl**) from the **/scripts** directory of your Web Agent installation, and store it in the web server scripts directory (usually **/inetpub/scripts**).
2. Customize the script with your own code.

   Important: RSA Security strongly recommends that your script contain a list of URLs that users are allowed to access using the redirect URL. The script's input argument should be compared to the list of allowed URLs before any redirect takes place. Any user who attempts to access the redirect hyperlink can see the link definition and could potentially use the redirect script to access the authentication cookie. By implementing a URL comparison list, you minimize the security risk.

3. Use the customized redirect URL from the script as the hyperlink to the unprotected site.

An example redirect URL looks like this:

http://<*protectedHostname*>/WebID/IISWebAgentIF.dll?referrer=/Scripts/AspScriptRedirect.asp?target=http://<*unprotectedHostname*>/new_application.jsp

- **/WebID/IISWebAgentIF.dll** is the virtual Web Agent reference. It ensures that a user attempting to access the unprotected URL is prompted to authenticate.
- **/Scripts/AspScriptRedirect.asp** is the script that performs the redirect to the input argument.
- **http://<*unprotectedHostname*>/new_application.jsp** is the input argument, or unprotected URL.

For more information about customizing auto-redirect scripts, see the directions included in each script.

Configuring the Agent for Microsoft Proxy Server

Microsoft Proxy Server 2.0 is installed as a filter extension of the default web site on the proxy host. After you install the Web Agent on the proxy host, set up the proxy service to work in reverse proxying with Web access authentication.

During reverse proxying, the proxy server host

- Filters incoming requests from the Internet for web site resources
- Directs the requests either to a local IIS virtual web server or to another internal web server

To an Internet user, the proxy server appears to be one web server, but the proxy server host is actually handling requests for any number of web servers that are behind the proxy.

When a request comes in for a web site resource that is protected by RSA SecurID, the Agent on the proxy server host gets the request and challenges the user for his or her RSA SecurID passcode.

To handle the requests for protected resources, you configure the default web site on the proxy host to contain mapped URLs for each of the web server resources that RSA SecurID protects.

Note: Microsoft Proxy Server does not support Group Security.

To set up the Agent to work with the proxy service:

1. On the proxy host, click **Start > Programs > Microsoft Proxy Server > Microsoft Management Console**.
2. Right-click the default web site, and click **Properties**.
3. In the **RSA SecurID** tab, check **Enable Web Access Authentication Feature Set on This Server**, but *do not* check **Protect This Resource**.
4. Click **Apply**.
5. With the default web site still selected, add each resource that you want to protect with RSA SecurID as a folder or file to the default web site.

   To add a resource to the default web site:

   - Right-click the default web site, and click **Explore**.
   - In the Exploring wwwroot window, click **Inetpub\wwwroot**.
   - Click **File > New > Folder**.
   - Give the new folder the same name as the actual resource to be protected. It does not matter that the folder is empty. For example, if you want to protect a URL named **/Mktg/Promotions**, add a folder named Mktg. Under that folder, add a folder named Promotions.
   - When you are finished adding the resources, click **File > Close**.
   - Refresh the view in the ISM.
6. In the default web site list of resources, right-click a resource that you have just added, and click **Properties**.
7. In the **RSA SecurID** tab, check **Protect This Resource**, and click **OK**.

6 Customizing Templates and Message Strings

When users authenticate using a web browser or a wireless device microbrowser, the RSA ACE/Agent 5.2 for Web software prompts users for their username and RSA SecurID passcode and informs them about the success of the authentication attempt. For standard browsers, the system returns these messages as HTML pages. For wireless device microbrowsers, the system returns messages in WML format.

The Web Agent software provides default versions of HTML and WML templates and messages. However, the HTML and WML templates and messages can be customized to reflect your company's image and administrative needs. You can edit the HTML and WML forms and supporting files to

- Add a custom greeting message
- Add your own custom graphics
- Change standard HTML and WML buttons to custom graphics
- Display Web access authentication prompts in a language other than English
- Customize the Web access authentication messages

Important Guidelines

To ensure that the templates will function properly after you have made changes, adhere to the following rules:

- Copy the templates into a new directory before making changes to them. If any templates are missing from this new directory, the Web Agent automatically defaults back to the original templates.
- Use a text editor to make changes. Programs such as FrontPage and HomeSite tend to add unnecessary additional HTML/WML tags to templates. There is also a possibility that these programs may alter the substitution strings that are necessary in the templates.
- After you have completed your changes, test the templates to make sure they are functioning properly. For information on utilities you can use to troubleshoot problems, see "Troubleshooting (UNIX and Windows)" on page 55.

Important: Do not alter any of the substitution strings in the templates or message text files (**webagent.msg** and **strings.txt**). These strings begin with two "at" signs (@@). The substitution strings are used to include error messages and text from the RSA ACE/Server and provide place holders for graphics and message strings.

Customizing Templates

Specifying the Location of Customized Templates on UNIX Agent Hosts

During the Agent installation, the default Web access authentication HTML and WML templates are copied into the **/templates** directory of your Web Agent installation. If you decide to use customized templates, you must store them in a different directory.

To access the templates and text strings, log in as a web server user as defined in the web server configuration file.

To specify the location of a virtual server's customized HTML or WML templates, run the Web Agent Setup configuration script. For directions, see "Using the Setup Menu" on page 16.

Specifying the Location of Customized Templates on Windows Agent Hosts

During the Agent installation, the default Web access authentication HTML and WML templates are copied into the **/templates** directory of your Web Agent installation. If you decide to use customized templates, you must store them in a different directory.

To access the templates and text strings, log in as a web server user as defined in the web server configuration file.

To specify the location of a virtual server's customized HTML or WML templates, see the Help topic "Specifying the Location of Customized Templates."

Modifying Static Text

You can change the static text that appears in Web access authentication templates, or you can add your own static text.

To modify the text in a Web access authentication template:

1. Using a text editor, open one of the HTML or WML templates in the directory. The templates are listed in "List of HTML and WML Templates" on page 51.

   Important: When editing HTML or WML templates, avoid altering the contents of substitution strings. These strings begin with two "at" signs (@@).

2. Delete the static text you want to change, and add the new text.

   For example, the tag **<H1>Welcome to Widgets, Inc.</H1>**, when placed in the **passcode.htm** or **passcode.wml** file, changes the text of the first heading in that page from "RSA SecurID passcode Request" to "Welcome to Widgets, Inc."

3. Save and close the file.

Adding Custom Graphics

You can add one or more custom graphics to the Web access authentication templates.

Note: WAP/WML devices usually have limited display space for graphics. Be sure the use of graphics is appropriate for your WAP devices before using them.

To add a custom graphic to a Web access authentication template:

1. Using a text editor, open one of the HTML or WML templates in the directory. The templates are listed in "List of HTML and WML Templates" on page 51.
2. Decide where you want the image to be placed on the page, then insert the appropriate tag in the HTML or WML markup pointing to the image file. Use one of the following methods for naming graphic files:
   - A substitution macro (@@URL?GetPic?image=) works with HTML and WML. With WML, the images must be WBMP. With HTML, the images must be JPG. Substitution macros cannot have absolute paths. The images must be in the same directory as the templates, and you must omit the filename extension from the file specification as in the following example:

     ```
     <IMG src="@@URL?GetPic?image=logo" ALIGN="left">
     ```

   - You can use HTTP URLs instead of substitutions if the image files reside in an area of the server that is unprotected by RSA SecurID authentication, or on a separate server hosting the URL. HTTP URLs are always absolute; relative URLs cannot be used in templates. The image types for HTTP URLs can be **.jpg**, **.gif**, or **.wbmp** as in the following example:

     ```
     <IMG src="http://server.domain.com/img/logo.jpg"
     ALIGN="left">
     ```

     Note: When using HTTP URLs, ensure the image file you point to in the **src** path is in a directory that is not protected by RSA SecurID and that you always specify a fully qualified path to the image file.
3. Save and close the file.
4. Stop and restart the web server for the changes to take effect.
   The web authentication prompt displays the new graphic.

Changing the Buttons (HTML Only)

You can replace the standard Send and Reset buttons that appear in the HTML templates with custom graphics. This approach is not supported by WML.

Note: Make sure the image file you point to in the **src** path is in a directory that is not protected by RSA SecurID and that you always specify a fully-qualified path to the image file.

To change the buttons in a Web access authentication template:

1. Using a text editor, open one of the HTML templates in the directory. The templates are listed in "List of HTML and WML Templates" on page 51.
2. Scroll down to the line that reads

   ```
   <INPUT TYPE=SUBMIT VALUE="Send">.
   ```

3. Edit the line so it reads

   ```
   <A HREF="JavaScript:document.forms[0].submit()"><IMG SRC="path
   to your image" BORDER="0"></A>
   ```

   where ***path to your image*** is a fully qualified path to an image file.

   Important: Make sure the image file you point to in the **src** path is in a directory that is not protected by RSA SecurID and that you always specify a fully qualified path to the image file.

   If you also want to replace the **Reset** button, replace the line

   ```
   <INPUT TYPE=RESET VALUE="Reset">
   ```

   with

   ```
   <A HREF="JavaScript:document.forms[0].reset()"><IMG SRC="path
   to your image" BORDER="0"></A>
   ```

4. Save and close the file.
5. Stop and restart the web server for the changes to take effect.

Customizing Templates for Another Language

If you need to customize the templates for a language other than English, you must store them in a language-specific directory under the Web Agent templates directory.

On UNIX and Windows Agent Hosts, the default directory for language specific templates is **/*Web_Agent_installation_directory*/templates/nls/<*language_code*>** where *language_code* is the language preference code used by web browsers.

To find the correct language code, refer to the language preferences list of codes in the Internet Explorer or Netscape Navigator web browsers. For more information about using international character sets in HTML documents, consult an HTML reference book or visit the World Wide Web Consortium's web site at **www.w3.org/pub/WWW/International**.

Important Guidelines

- Your end users must have their browser language preference set to use the appropriate language code.
- The code must correspond to your language-customized template directory name. The new language preference must appear at the top of their web browser's list of language preferences.
- If the preference settings are not set correctly, language-customized templates do not exist, or the Agent cannot find the specified templates for a virtual web server, the browser displays the default English version of the templates.

To translate HTML and WML forms for a non-English language:

1. Create a language-specific subdirectory in the templates directory of the Web Agent.

   For example, on UNIX Agent Hosts:

   ```
   /usr/local/apache/rsawebagent/Templates/nls/fr
   ```

   where **fr** is the language preference code for French.

   On Windows Agent Hosts,

   <your_own_template_path>`\nls\de`

   where **de** is the language preference code for German

2. Copy the templates to the language-specific subdirectory that you have just created.
3. Customize the text strings within the templates.

   Note: Do not remove the substitution macros. (These macros begin with a double at sign (@@) in the text.) The macros are replaced with actual values when the text is displayed.

4. If you are using a Windows Agent Host, save and close the template file(s). If you are using a UNIX Agent Host, run the Web Agent configuration script, and update the **Template** path in the **Setup** menu to point to the language specific templates.

Customizing Message Strings

You can customize certain messages that display while users interact with the Web access authentication prompt pages that are produced from the HTML or WML templates. The message strings are contained in a file named **strings.txt** located in the */**Web_Agent_installation_directory**/**templates** directory on UNIX and Windows Agent Hosts.

For example, **strings.txt** contains passcode page errors like:

```
[Messages]
; PASSCODE page errors and messages.
1="100: Access denied. The RSA ACE/Server rejected the
PASSCODE you supplied. Please try again."
2="101: Access denied. Unexpected RSA ACE/Agent Error %d.
Please try again."
3="102: You must enter a valid PASSCODE. Please try again."
```

Important: If you modify the message strings, make certain that you do not remove or alter the position of the variable strings (**@@SUB1**, **@@SUB2**, and so on) contained in the message text. The strings are replaced by actual values when the messages are displayed.

To customize the text displayed by the **multidom.htm** or **multidom.wml** template, search for the following section in the **strings.txt** file:

```
; multiple domain authentication string
; This is HTML only
22="<strong>Requesting authentication from server
@@SUB1</strong> <img alt=failed src="@@SUB2"><br>"
; This is for WML with image tag support
23="<strong>Server @@SUB1 <img alt="failed"
src="@@SUB2"/></strong><br/>"
```

Note: If you translate the text messages in **strings.txt** into a language other than English, you must store the translated file in the same language-specific directory where other translated HTML or WML templates are stored. For more information, see "Customizing Templates for Another Language" on page 48.

List of HTML and WML Templates

The following table summarizes the purpose of each template.

Note: If you are using RSA SecurID PINPads instead of tokens, you need to change the **passcode** and/or **useridandpasscode** templates to display the correct message to your users. The correct message to display is included in the templates in a comment section.

Template	Purpose
Errors	
error.htm **error.wml**	The page that RSA SecurID users see when a fatal error occurs during authentication. The **@@sub** macro in the template substitutes the error message passed from the system or from the **strings.txt** file.
forbidden.htm **forbidden.wml**	The page that RSA SecurID users see in response to requesting a forbidden URL.
Authentication Templates	
newpin.htm **newpin.wml**	The New PIN page displayed when users are authenticating with their token for the first time. From this page, users create their own PINs.
newpin1.htm **newpin1.wml**	The New PIN page displayed to a user that will receive a system-generated PIN. This functionality is determined in the RSA ACE/Server.
newpin2.htm **newpin2.wml**	The New PIN page displayed when a user is given the choice of whether to create their own PIN or receive a system-generated PIN. This functionality is determined in the RSA ACE/Server.
nextprn.htm **nextprn.wml**	The page displayed when a token is in Next Tokencode mode. This happens when a user enters a series of incorrect passcodes during authentication. After the user finally enters a correct tokencode, the user is prompted for another correct tokencode before being allowed access.
sslredir.htm **sslredir.wml**	The page users might see momentarily with some browsers when they must use a secure channel to access protected pages. In some cases, users must click a link on the **sslredir** (**.htm** or **.wml**) page to continue.
redirect.htm/redirect-get.htm **redirect.wml**	The page displayed when users complete the authorization process or when they log off. **Note**: If you customize **redirect.htm**, you must customize **redirect-get.htm** to look the same.

Template	Purpose
redirectmanual.wml	This page is displayed to cell phone users when the cell phone does not support automatic redirection to a protected URL. The user is provided with a list of secure URLs and must manually choose one.
cancel.htm/cancel-get.htm **cancel.wml**	The page displayed to users when they cancel out of the authorization process. **Note**: If you customize **cancel.htm**, you must customize **cancel-get.htm** to look the same.
showsys.htm **showsys.wml**	The page displayed to users for ten seconds while the system generates an RSA SecurID PIN for them.
multidom.htm/multidom-get.htm **multidom.wml**	The page displayed when users are authenticating across multiple domains. **Note**: If you customize **multidom.htm**, you must customize **multidom-get.htm** to look the same.
userid.htm **userid.wml**	If you chose to present separate web pages to users to input the username and passcode, this template is used for the username. If you did not choose to present separate pages, the **useridandpasscode** template is used.
passcode.htm **passcode.wml**	If you chose to present separate web pages to users to input the username and passcode, this template is used for the passcode. If you did not choose to present separate pages, the **useridandpasscode** template is used.
useridandpasscode.htm **useridandpasscode.wml**	If you chose to present one web page to users to input both the username and passcode, this template is used. If you chose to present separate web pages to input the username and passcode, the **userid** and **passcode** templates are used.

The HTML and WML forms are supported by the following files, which are also installed into the Templates directory:

Template	Purpose
Bitmaps	
denied.jpg **denied.wbmp**	If you have configured the Web Agent to allow multiple domain authentications, the word “Denied” is displayed if a user’s authentication request to a virtual web server does not succeed.
ok.jpg **ok.wbmp**	If you have configured the Web Agent to allow multiple domain authentications, the word “SUCCESS” is displayed if a user’s authentication request to a virtual web server succeeds.
rsalogo.jpg	This is the background graphic used on the authentication pages.
securid_banner.jpg	This graphic displays the RSA SecurID banner on the authentication pages.
Other Files	
strings.txt	This file contains text strings that are used to display various messages while users interact with the Web access authentication prompt pages.
style.css	The cascading style sheet used for the web pages.

7 Troubleshooting (UNIX and Windows)

RSA ACE/Server Utilities

Use these utilities to determine communication between the Web Agent and the RSA ACE/Server.

UNIX

These utilities reside in the Web Agent directory (***/web_server_directory*/rsawebagent** is the default).

acestatus

This utility provides information about the RSA ACE/Server such as the configuration version, the server name and address, the number of client retries, and the client time-out period.

acetest

This utility allows you to authenticate to the RSA ACE/Server from the command line rather than going through authentication web pages in your browser. This will help you determine whether a problem lies with the templates or with the authentication process itself.

Windows

sdtest

This utility provides information about the RSA ACE/Server such as the configuration version, the server name and address, the number of client retries, and the client time-out period. In addition, this utility allows you to test authentication with the RSA ACE/Server.

For more information about **sdtest**, see "Using the RSA ACE/Agent Control Panel" on page 39 and the RSA ACE/Agent Control Panel Help.

Logging Authentication Attempts

Authentication attempts are logged in ***/web_server_directory*/logs/error_log** (UNIX) and the Windows Event Viewer (Windows).

Note: On UNIX machines, the different types of error messages logged can be found in the **webagent.msg** file located in the Web Agent directory (***/web_server_directory*/rsawebagent** is the default).

The following table provides a list of possible error messages and their cause:

Error Message	Possible Cause and Solution
(UNIX only) File /usr/local/web_server_directory/conf/*file*.conf isn't writable.	The user account with which you are logged in does not have write permissions. Log in with a web server user account that has write permissions to the web server root directory.
100:Access denied. The RSA ACE/Server rejected the passcode you supplied. Please try again.	The first time an authentication occurs after the Web Agent has been installed on the web server, a node secret is generated by the RSA ACE/Server and sent to the web server. This error is also received if the node secret file is missing or the node secret on the RSA ACE/Server and web server do not match. Contact your RSA ACE/Server administrator.
Unexpected RSA ACE/Agent error 103. Please try again.	This error is received when there are network problems. Contact your RSA ACE/Server administrator.
AceInitialize Failed during acetest authentication.	The **sdconf.rec** file is missing. Obtain an **sdconf.rec** file from your RSA ACE/Server administrator. Place the file in a directory that is accessible to the web server and RSA ACE/Agent for Web software. Restart the web server.
The page cannot be found.	The requested page may not present.
RSA Securid Error. 106: Web server too busy. Please try again later.	This error may occur when communication to the RSA ACE/Server is down or the **sdconf.rec** file is missing. Contact your Server administrator.
Unexpected authentication error.	This error may occur when authenticating using the **acetest** utility. Communication to the RSA ACE/Server is down. Contact your Server administrator.

Error Message	Possible Cause and Solution
The Page cannot be displayed.	There are two possible causes for this error message. • Communication to the web server is down. • The web server was started without SSL. Therefore, the Redirect Secure feature in the Web Agent is disabled. The best solution is to restart the web server with SSL. You could also have users access the page with an **https** request.
RSA Web Access Authentication Extension Error. RSA Web Access Authentication: Internal server configuration error.	The path to the HTML and WML templates is invalid. Verify the correct path in the Web Agent configuration .
For Multi-Domain Authentication: Requesting authentication from server http://server Denied.	Make sure that the same domain secret exists on each web server within the multi-domain area.

RSA ACE/Agent 5.2 for Web Error and Event Viewer Log Messages

The Web Agent logs events in the web server error log file on UNIX machines and the Windows Event Viewer Application Log under the source ACECLIENT on Windows machines.

This section lists all error and event messages alphabetically.

ACECheck processing error for userid *username*

If the **ACECheck** function returns an error, an RSA ACE/Server time-out or some other communications error has occurred.

ACEClose processing error *errornumber*

If the **ACEClose** function returns an error, an RSA ACE/Server time-out or some other communications error has occurred.

ACENext processing error for userid *username*

If the **ACENext** function returns an error, an RSA ACE/Server time-out or some other communications error has occurred.

ACEPin processing error for userid *username*

If the **ACEPin** function returns an error, an RSA ACE/Server time-out or some other communications error has occurred.

All users challenged. Passcode required.

The specified service is configured to challenge all users of the service with RSA SecurID. The **Challenge** control on the RSA ACE/Agent control panel is set to **All Users**. The user was challenged to enter a passcode.

An error occurred when accessing the Metabase.

The Agent failed while reading from or writing to the Metabase. If this message is displayed, first make sure you have the correct administrative privileges, and then reboot the Agent Host. If the error persists, reinstall the Agent to override the existing settings. If that does not resolve the situation, you will have to uninstall, and then reinstall the Agent.

Authentication failure.

The subject described in the Event Detail did not authenticate successfully and was therefore refused access.

Authentication Manager: Access Denied.

The user did not enter a valid RSA SecurID passcode.

Authentication Manager: RSA ACE/Agent Library Failure.

The RSA ACE/Agent could not load the **aceclnt.dll** library file. The file is either corrupted, has been moved to another directory, or has been deleted from the system.

If the **aceclnt.dll** file is no longer on the system, you must reinstall the RSA ACE/Agent.

Authentication Manager: Cannot resolve address IP address to a host name. The data is the Windows Sockets error.

The RSA ACE/Agent Network authentication proxy service attempted to get the workstation name, but the service could not resolve the numeric IP address to a host name because the name was not found in DNS. Make sure DNS is working properly on your network.

Authentication Manager: Failed Authentication Attempt. User *username*.

The user entered an invalid passcode, causing the “bad passcode” counter to be incremented by 1 in the Windows registry. If this counter exceeds the configured number of bad passcodes, the user’s token will be deactivated until an administrator intervenes.

The number of allowed bad passcodes is stored in the **sdconf.rec** file and can be viewed by running the **sdtest** program.

Authentication Manager: Invalid RSA ACE/Server configuration. User *username*.

The **sdconf.rec** file is not valid. The file is either corrupted, has been moved to another directory, or has been deleted from the system.

To correct the problem, get a new copy of **sdconf.rec** from your RSA ACE/Server administrator.

Authentication Manager: New PIN Accepted. User *username*.

The user successfully associated a new PIN with his or her token.

Authentication Manager: New PIN Rejected. User *username*.

The user did not successfully associate a new PIN with his or her token. If the user is attempting to create his or her own PIN, make sure the user understands the PIN length and syntax parameter settings for your RSA ACE/Server.

Authentication Manager: Next Tokencode Accepted. User *username*.

After entering a series of bad passcodes, the user was prompted to enter the next tokencode from his or her token. The next tokencode was valid and the user was authenticated successfully.

Authentication Manager: User Canceled New PIN Mode. User *username*.

The user was prompted to associate a new PIN with his or her token, but the user did not complete the new PIN procedure. Make sure the user understands how to use his or her token in New PIN mode.

Authentication Manager: User Canceled Transaction. User *username*.

The user was prompted to authenticate, but then canceled out of the Enter passcode dialog box. This is a purely informational message.

Authentication Manager: User I/O Timeout. User *username*.

The user waited too long at the **Enter passcode** prompt, so the RSA ACE/Agent canceled the transaction.

Authentication Manager: User Interface Library Failure.

The RSA ACE/Agent could not load the **sdui.dll** library file. The file is either corrupted, has been moved to another directory, or has been deleted from the system.

If the **sdui.dll** file is no longer on the system, you must reinstall RSA ACE/Agent.

Cannot create socket during initialization in RSA SecurID Authentication

Socket services may not have started. Check the Event Log to find out if there is a problem with the network card or the TCP/IP services.

Also, make sure echo services are running on your RSA ACE/Server by doing one of the following:

- If the RSA ACE/Server is running on a Windows NT machine, open the RSA ACE/Server machine Network control panel, click the **Services** tab, and make sure **Simple TCP/IP Services** are installed. If they are not, add the **Simple TCP/IP Services**.
- If the RSA ACE/Server is running on a UNIX machine, make sure the **echo** service is running on the RSA ACE/Server machine. See your UNIX operating system documentation for information about starting the echo service.

Cannot create socket during initialization.

Make sure echo services are running on your RSA ACE/Server by doing one of the following:

- If the RSA ACE/Server is running on a Windows NT machine, open the RSA ACE/Server machine Network control panel, click the **Services** tab, and make sure **Simple TCP/IP Services** are installed. If they are not, add the **Simple TCP/IP Services**.
- If the RSA ACE/Server is running on a UNIX machine, make sure the **echo** service is running on the RSA ACE/Server machine. See your UNIX operating system documentation for information about starting the echo service.

Cannot load RSA ACE/Agent DLL

Test cannot find **aceclnt.dll** in the **\system32** directory. You must install the Web Agent software in repair mode.

Cannot read server private key from file.

Make sure you have copied both the ***hostname*.crt** and the ***hostname*.key** files to the import location. In addition, make sure you are entering the certificate password correctly.

Connection attempt failed.

This results from a bad server certificate. When a user attempts to mount a network drive or printer or to test authentication in silent mode, this message is logged. During silent mode, the drive will mount successfully.

Cookie rejected. Cached client info does not match.

If a user is using more than one workstation, this message appears each time the user switches from one workstation to another.

Cookie rejected. Cookie failed MD5 test.

An unauthorized user has attempted to access the web server with a bogus Web access authentication cookie.

Cookie rejected. Expired cookie. Username *username*

A Web access authentication cookie has expired in response to the time-out values defined in the web properties sheet.

Could not initialize RSA ACE/Agent

Will be preceded by a number of RSA ACE/Agent error messages, such as **Cannot find sdconf.rec**. Try reinstalling the **sdconf.rec** file in the **%*SYSTEMROOT*%\system32** directory.

Could not initialize Cookie Cache

A memory error has occurred within an internal function. Your web server may be overloaded; you may need more physical memory.

Could not open HTML template *filename*

The HTML template file is missing.

Also check the security settings for the file. Make sure the account that the web server is running has Full Access privileges to the HTML file.

Could not open registry key *keyname*

A serious registry corruption has occurred. You must reinstall the RSA ACE/Agent software.

Could not query value *valuename*

If you have enabled the Domain Cookies feature without setting a domain secret, you might get a **valuename DomainData** message, followed by a **Domain cookies are disabled** message.

Could not read HTML template *filename*

The HTML template file is missing.

Could not resolve hostname *hostname*

The DNS function of the web server is configured incorrectly. Domain cookies cannot be used until the configuration is corrected.

Failed authentication for userid *username*.

The RSA ACE/Server did not grant the user access; the most common causes for this are wrong username or an invalid passcode.

Failed to create event.

These are internal errors. The machine may not have enough free resources to add RSA SecurID authentication. Consider moving service(s) from this machine to another one.

Failed to create service thread, aborting.

There were too many other processes running, so the service did not start.

Failed to find required service WINSOCK.

The Windows socket interface was not found. Check the event log to find out if there is a problem with WINSOCK. Ensure that TCP/IP has been enabled on the machine.

File incorrect size: sdconf.rec.

It is likely that the **sdconf.rec** file was not copied in binary or ftp mode. Ask the RSA ACE/Server administrator for a new copy of **sdconf.rec**.

File not found: aceclnt.dll.

Software may have been installed incorrectly or **aceclnt.dll** may have been deleted. Reinstall the RSA ACE/Agent software from the Microsoft Internet Information Server CD to correct the problem.

File not found: sdconf.rec.

The **sdconf.rec** file is not in the ***%SYSTEMROOT%*\system32** directory. It was either removed or never copied from the RSA ACE/Server. Ask the RSA ACE/Server administrator for a new copy of **sdconf.rec**.

Initialization of sdagent.dll library failed.

Users see this error message when there is no root certificate installed on the computer. To correct this problem, obtain a copy of the root certificate and reinstall the RSA ACE/Agent software.

New PIN accepted for userid *username*.

The RSA ACE/Server verified the RSA SecurID user's new PIN.

New PIN rejected for userid *username*.

The PIN was rejected by the RSA ACE/Server. The user must re-authenticate to set the PIN. Check the Activity Log on the RSA ACE/Server.

New PIN requested from userid *username*.

The RSA ACE/Server has prompted the RSA SecurID user to create his or her own PIN or receive a system-generated PIN.

Next code accepted for userid *username*.

The Next Tokencode was accepted by the RSA ACE/Server and access was granted.

Next code rejected for userid *username*.

The user must attempt to authenticate again.

Next code requested from userid *username*.

The user's token was in Next Tokencode mode and the RSA ACE/Server asked for the second tokencode.

No cookie or corrupted information.

This message will appear each time a new user logs in to the web server.

Out of memory in *functionname*.

A memory error has occurred within an internal function. Your web server may be overloaded; you may need more physical memory.

Passcode Incorrect (multiple instances of)

If you have both RAS authentication and web authentication enabled on a machine, the RSA ACE/Agent could be sending the encrypted RAS authentication passcode through the wrong IP address. Check the IP addresses of each service and the client nodes on the RSA ACE/Server for possible addressing errors.

Remote authentication denied for userid *username*.

Another web sever within the DNS domain has requested authentication of user *username* with a domain cookie and was not given access.

Check the security settings for the file. Make sure the account that the web server is running has Full Access privileges to the HTML file.

Remote authentication given for userid *username*.

Another web server within the DNS domain has requested authentication of user *username* with a domain cookie and was given access.

Remote authentication received deny for userid *username*.

A web server requesting authentication of a domain cookie was rejected.

Remote cookie rejected. Cookie failed MD5 test.

An unauthorized user has attempted to access the web server with a bogus Web access authentication domain cookie.

Remote: NT/RAS not available.

The machine does not meet one or more of the system or software requirements needed to enable authentication of RAS connections.

RSA ACE/Agent initialization failed

The Agent cannot make the connection to the RSA ACE/Server. Make sure the RSA ACE/Server and network are operational and that all network interface cards and cables are properly installed and in good condition.

RSA ACE/Server is not responding

There is a network communications problem between the RSA ACE/Server and the RSA ACE/Agent, the server cannot be found (because the IP address is wrong, for example), or the RSA ACE/Server daemon is not running.

RSA ACE/Server is not responding. Run CLNTCHK to verify port and IP address of RSA ACE/Server

There is a network communications problem between the RSA ACE/Server and the RSA ACE/Agent, the RSA ACE/Server cannot be found (because the IP address is wrong, for example), or the RSA ACE/Server daemon is not running.

Session Manager: Failed to Create Server Thread.

There are too many server threads running (too many users connecting at once). Try widening the intervals at which users attempt to log in.

Session Manager: Failed to Create Socket.

This message results from a memory shortage or WINSOCK error. The cause might be too many users connecting to the server at the same time.

Session Manager: Failed to Resolve Hostname.

Most likely a configuration error. The machine that is connecting has no DNS or NetBIOS name, or has an invalid IP address. Make sure your network is configured properly and that your host file entries are correct.

Session Manager: Not Enough Memory.

The system does not have enough physical RAM, or there were too many other processes running in memory. If you receive this message often, add more physical memory to the computer.

Session Manager: Winsock startup error.

The Microsoft Windows Sockets failed to initialize. To troubleshoot WINSOCK problems, consult your Microsoft networking documentation.

Successful authentication.

The subject described in the Event Detail authenticated successfully and was granted access to the system.

The access control entry for *filename* was not found.

The Windows NT security entry for this file is corrupted. If you suspect that the ACL has become corrupted, see the Microsoft Windows NT Help, or contact Microsoft technical support.

The discretionary Access Control List for *filename* was not found.

The Windows NT security entry for this file is corrupted. If you suspect that the ACL has become corrupted, see the Microsoft Windows NT Help, or contact Microsoft technical support.

The local group *groupname* does not exist.

Indicates an incorrect implementation of the Web access authentication **Group Security** feature.

The RSA ACE/Agent could not locate one of the groups listed in the user's **Shell** field on the local machine. Make sure you created and named the group properly in the Windows NT User Manager.

The security descriptor could not be found. The file may not exist: *filename*.

A user requested a URL that does not resolve to a file on the machine. Make sure the user is entering the URL correctly.

The user connected to port *portname* has been disconnected. . .

There is a problem with RSA SecurID authentication. See the Event Detail topic for more specific information.

The user *server/username* disconnected from port *portnumber*.

The user closed the connection on the specified port.

The user *server/username* connected on port *portnumber* on date at time and disconnected on date at time. . .

A normal RSA ACE/Agent disconnection has occurred.

The user *username* has connected and been authenticated on port *portnumber*.

A normal (authenticated) RSA ACE/Agent-Server connection occurred.

Unexpected error from RSA ACE/Agent.

The value returned by the RSA ACE/Server is not valid.

User <blank> canceled out of RSA SecurID Authentication routine.

The user canceled without entering a username.

User I/O Timeout-User took too long to respond.

The Windows NT system timed out after waiting for a response from the user.

User *username* canceled out of New PIN routine.

The user canceled the authentication attempt.

User *username*: ACCESS DENIED. ATTEMPT 1.

The user was denied access. Check the RSA ACE/Server Activity Log for the specific reason.

User *username*: Access denied. Attempt to use invalid handle. Closing connection.

An internal error occurred. If the message re-occurs, call the RSA Security Customer Support Center.

User *username*: ACCESS DENIED. Next Tokencode failed.

The user must attempt to authenticate again.

User *username*: ACCESS DENIED. Server signature invalid.

This message indicates that the identity of the RSA ACE/Server could not be verified by the client. If you see this message, call the RSA Security Customer Support Center.

User *username*: ACE Check Error: Invalid group SID. Passcode required.

The user's group SID did not contain a valid group name. The user was challenged for an RSA SecurID passcode.

User *username*: canceled out of Next Tokencode routine.

The user canceled out of the Next Tokencode process.

User *username*: canceled out of RSA SecurID Authentication routine.

The user canceled after entering a username.

User *username*: Domain not found. User challenged for passcode.

The user may have entered the domain name incorrectly and will be challenged for a passcode.

User *username*: New PIN accepted.

The user's New PIN was verified.

User *username*: New PIN rejected.

The PIN was rejected by the RSA ACE/Server. The user needs to re-authenticate to set the PIN. Check the RSA ACE/Server Activity Log.

User *username*: Not found. User challenged for passcode.

The user is unknown to the system, but the user will be challenged for passcode anyway.

User *username*: Successfully logged on with Next Tokencode.

The Next Tokencode was accepted by RSA ACE/Server and access was granted to the user.

Known Problems of Third-Party Software

Netscape 7.1 Browser Issues

Unlike Internet Explorer, Netscape maintains a single browser session across multiple instances of the browser. If a user has successfully authenticated onto a protected resource in one instance of the browser, as long as that instance remains open, all other instances of the browser share the same authentication cookie. Therefore, the user does not have to authenticate again in any other instances of the Netscape browser to access protected resources.

Wireless Devices

RSA ACE/Agent and RSA ACE/Server administrators should be aware of the following items pertaining to RSA SecurID web authentication. A user could experience these scenarios when using a cellular phone equipped with a microbrowser to access protected URLs.

- If your environment includes a GSM network, your WAP connection needs to be in connection mode. Multiple domain environments require that handset devices and gateways support the receipt of cookies from multiple domains.
- Requiring an SSL connection to protected URLs creates a more secure environment. For ease of use, you can configure the Web Agent to automatically redirect the URL request to a secure connection. However, not all microbrowsers support automatic redirection. In this case you need to disable the redirect option. A web page is then presented with a link to the secure connection that users will have to manually click.
- When the Web Agent is configured to use a single web page for entering the username and passcode, the LCD on certain devices may appear to be using separate pages, one for entering the username and a second page for entering the passcode. However, the microbrowser on the device is sending the data all at once, unless you have specifically enabled the **Use Separate Username and Passcode Pages** option in the Web Agent.
- When **Name Locking** and **Use Separate Username and Passcode Pages** are enabled in the Web Agent, and the carrier signal is lost after transmitting the username, the username is locked in the Web Agent database until the Name Lock time-out expires. Instruct the user to authenticate again after the Name Lock expiration time.

- It can be difficult for users to enter the PIN and tokencode within the designated time limit (typically 60 seconds) before the tokencode changes again. Most WAP devices by default are set up for alphanumeric entries. That means the user must scroll through the letters assigned to a button before reaching the numbers. Since tokencodes are always numeric, instruct users to switch their phone to numeric entry, if their phone allows this, only after entering the PIN.
- Some gateways have very specific size limitations for WML templates. You may need to reduce the amount of information provided in the templates.
- To enable the **Redirect HTTP Connections to Secure Server** option, the cellular device and its gateway must allow for SSL redirection. RSA Security recommends that you instruct the user to refer to the documentation provided with his or her cellular device.
- Devices that allow for an image display may, during the course of an authentication, display the status "Failed" for several seconds (depending on the speed of the micro browser) until an image is shown on the LCD that indicates success. In these instances, the user should wait for several seconds until the success image is shown. If, however, the "Failed" status message is displayed for a substantial amount of time, it is most likely valid, and the user should attempt to authentication again.

Multi-Domain Issues

When connecting to multiple domains, a web page is displayed showing the domain URL and the success or failure of the connection. In some environments, the GIFs used to show "Success" or "Failed" do not appear in the web page. If this occurs, do not use **https** when you input domains in your multi-domain list, just use **http**. As far as RSA Security has been able to determine, this problem only occurs when there is no valid certificate on the web server and using some versions of Internet Explorer. Therefore, this problem will basically only occur in a test environment.

The following issues may occur when using multi-domain access on wireless devices:

- When Multi-Domain Access is enabled in the web Agent, a list of URLs for the domains is displayed. WAP devices that allow for an image display may, during the course of an authentication, display the "Failed" status for several seconds (depending on the speed of the microbrowser) until an image is shown on the LCD that indicates success. In these instances, the user should wait for several seconds until the success image is shown. However, if the "Failed" status message remains for a substantial amount of time, it is most likely valid, and the user should attempt to authenticate again.
- When multi-domain is enabled, the Web Agent attempts to get an image from each of the domains to see if it has connected. With some cell phones, the image is displayed, but the connection was never actually made. So, once the user has authenticated once in a multi-domain environment and then attempts to access a URL in another domain, the user is asked to authenticate again rather than having single sign-on.

  To work around this issue, on UNIX machines, set the variable **UseTextWML=1** in the **RSAWebAgent.ini** file located in the Web Agent installation directory (the default is **rsawebagent**). This will force the user to manually click on a text link for each domain instead of attempting to automatically make the connection using images.

On Windows machines, enable the **Using Text Link Authentication Mechanism for Multi-Domain WML Access** configuration option. For more information, see “Using Advanced Configuration Options” on page 35.

A Configuring the Server for Single Sign-On Access (Windows 2003 Only)

With Single Sign-On (SSO) access, users need only authenticate through RSA SecurID to access a web application that would normally also be protected by a windows logon. The RSA ACE/Agent for Web supports SSO access for Microsoft Outlook Web Access (OWA) only.

Requirements

To implement SSO access:

- The RSA ACE/Agent 5.2 for Web must be running on a Windows 2003 Server in an environment in which a Windows 2003 Server is the domain controller.
- You must have unique usernames across all domains. In addition, usernames in the Active Directory Server must match the usernames in the RSA ACE/Server database.
- To use SSO access for Outlook Web Access (OWA), you must install Microsoft Exchange Server 2003 and configure it to work with IIS.

Setup Tasks

To set up the web server for SSO access, you must complete the tasks described in this section.

Task 1: Configure the Domain to Run at the Windows 2003 Server Functional Level

When the domain runs at the Windows 2003 Server functional level, Windows 2003 machines cannot talk to Windows 2000 machines. This is necessary for SSO because SSO works only on Windows 2003 Servers.

To configure the domain to run at the Windows 2003 Server functional level:

1. Click **Programs > Administrative Tools > Active Directory Users and Computers**.
2. In the left pane, right-click **Active Directory User and Computer <*servername*>**, select **All Tasks**.
3. Click **Raise Domain Functional Level**.
4. In the **General** tab, click **Raise Domain Functional Level**.
5. In the Select An Available Domain Functional Level dialog box, click **Windows Server 2003**.
6. Click **OK**.

Task 2: Configure the Web Application for Anonymous Access

To configure SSO access for Outlook Web Access (OWA), you must configure the **ExchWeb/bin** directory for anonymous access.

To configure the web application for anonymous access:

1. Click **Start > Settings > Control Panel > RSA Web Agent**.
2. In the left panel, right-click the name of the web application, and click **Properties**.
3. Click the **Directory Security** tab, and in the **Authentication and access control** area, click **Edit**.
4. Make sure **Enable Anonymous Access** is the only option selected.
5. Click **OK**, and then click **Apply**.

Task 3: Enable SSO on the Virtual Directory

To configure SSO access for Outlook Web Access (OWA), you must enable SSO on the **Exchange**, **ExchWeb**, and **public** virtual directories.

To enable SSO on the virtual directory:

1. In the Internet Service Manager (ISM), double-click the appropriate virtual server.
2. Right-click the appropriate virtual directory, and click **Properties**.
3. In the **Virtual Directories** tab, under **Application Settings**, click the **Create** button next to the **Application Name** field, and click **Apply**.
4. Click the **RSA SecurID** tab.
5. Check **Protect This Resource with RSA SecurID**.
   All subdirectories and files that belong to the directory inherit this protection status.
6. Check **Target This Resource for Single Sign On**.
7. Click **OK**.

Index

V

W