



## RSA SecurID Ready Implementation Guide

Last Modified: August 04, 2008

### Partner Information

---

Product Information	
Partner Name	Oracle PeopleSoft
Web Site	<a href="http://www.oracle.com">www.oracle.com</a>
Product Name	PeopleSoft 8.9
Version & Platform	8.9
Product Description	<p>Oracle's PeopleSoft Enterprise applications are designed to address the most complex business requirements. They provide comprehensive business and industry solutions, enabling organizations to:</p> <ul style="list-style-type: none"><li>• Significantly improve performance</li><li>• Web services integration that fit seamlessly into a heterogeneous applications environment</li><li>• A broad choice of technology infrastructure</li></ul>
Product Category	Web Application & ERP

The Oracle logo is the word 'ORACLE' in a bold, red, sans-serif font. A registered trademark symbol (®) is located at the top right of the letter 'E'.



## Solution Summary

This integration allows PeopleSoft users to authenticate securely with RSA SecurID tokens and RSA Authentication Manager technology. In order to implement the solution, you will set up a web server proxy to the application server hosting PeopleSoft. An RSA Authentication Manager Web Server Agent will be installed on the web server to monitor requests for resources, and Authentication Manager will be configured to protect all private PeopleSoft applications. Finally, you will configure the PeopleSoft server to trust users who have authenticated with RSA SecurID tokens.

When a user has been authenticated, the RSA Authentication Manager agent writes the username to an HTTP header variable and forwards the request to the PeopleSoft server. PeopleSoft establishes the identity of the user by parsing the HTTP header and running a simple script that creates a new session.

Step	Component	Description
1	Browser	User clicks on a link to the PeopleSoft application: <a href="http://servername/ps/ps/?cmd=start">http://servername/ps/ps/?cmd=start</a>
2	Web Server	The RSA Authentication Manager Web Server Agent intercepts the request for the URL, authenticates the user. The SID redirect script writes the authenticated username to an HTTP header variable.
3	Servlet	The PeopleSoft servlet receives the HTTP request and connects to the application server using the User ID and Password set in the "Public Users" credentials in the current Web Profile. See below for details.
4	Application Server	The application server authenticates the connection from the web server by checking these credentials. The user ID and password must be valid in order for the connection to succeed and for Signon PeopleCode to execute.
5	Signon PeopleCode	The Signon PeopleCode reads the authenticated username from the HTTP request and creates a new PeopleSoft session.

*A step-by-step example of a PeopleSoft logon configured to trust RSA SecurID two-factor authentication.*

Partner Integration Overview	
<b>Authentication Methods Supported</b>	Native RSA SecurID Authentication
<b>List Library Version Used</b>	Library Version #5.3.3.378
<b>RSA Authentication Manager Replica Support *</b>	Full Replica Support
<b>Secondary RADIUS Server Support</b>	N/A
<b>RSA Authentication Agent Host Type</b>	Net OS
<b>RSA SecurID User Specification</b>	All Users
<b>RSA SecurID Protection of Administrative Users</b>	No
<b>RSA Software Token and RSA SecurID 800 Automation</b>	No



## Product Requirements

---

Please consult the PeopleSoft application release notes and upgrade notes for possible support restrictions. Not all PeopleSoft applications support every combination supported on PeopleTools.

### Partner Product Requirements: PeopleSoft 8.9

#### System

Please consult the PeopleSoft application release notes and upgrade notes for possible support restrictions.

### Partner Product Requirements: PeopleTools 8.47

Please consult the PeopleTools application release notes and upgrade notes for possible support restrictions. Not all PeopleSoft applications support every combination supported on PeopleTools

## Agent Host Configuration

---


To facilitate communication between PeopleSoft HRMS and RSA Authentication Manager, an RSA Agent Host Record must be added to the RSA Authentication Manager database. This record identifies the PeopleSoft Server to Authentication Manager and contains information about communication and encryption as well.

To create the Agent Host Record, you will need the following information.

- The PeopleSoft Server Hostname
- IP Addresses for all network interfaces

When adding the Agent Host Record, you should configure PeopleSoft HRMS as a Net OS agent. This setting is used by the RSA Authentication Manager to determine how communication with the PeopleSoft Server will occur.

---

 *Note: Hostnames within RSA Authentication Manager must resolve to valid IP addresses on the local network.*

---

Please refer to the appropriate RSA Security documentation for additional information about creating, modifying and managing Agent Host Records.



## Partner Product Configuration

---

### ***Before You Begin***

This section provides instructions for integrating PeopleSoft HRMS 8.9 with RSA SecurID. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of each products and the ability to perform the tasks outlined in this section. Administrators should have access to all product documentation in order to install the required components.

All components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

### ***Configuration Overview***

Once you have configured the PeopleSoft Server as an Agent Host within RSA Authentication Manager, you must perform the following steps to configure HRMS for SecurID two-factor authentication.

- A. [Create a PeopleSoft user default user](#)
- B. [Disable the PeopleSoft logon page](#)
- C. [Create a PeopleCode Signon script for RSA](#)
- D. [Activate the PeopleCode Signon script for RSA](#)
- E. [RSA Authentication Manager configuration](#)
- F. [Logout Screens](#)
- G. [Logon Screens](#)


#### ***G. Create a PeopleSoft default user***

A PeopleSoft user must establish a secure connection to the PeopleSoft application server before the authenticated user's session can be created. This user is referred to as the default user. Log in to

The default user will only be granted permission to connect to the HRMS application. PeopleSoft recommends creating a long and difficult-to-guess password. However, "PASSWORD" is used in this example for simplicity's sake. "DEFAULT\_USER" is used for a user ID.

- Log in to PeopleSoft and create a default user.

---

 *Note: PeopleSoft user IDs and passwords are case-sensitive. Both must be set in uppercase.*

---



### G. Disable the PeopleSoft logon page

The RSA Authentication Manager logon prompt replaces the PeopleSoft prompt in this integration. You must disable PeopleSoft logon so your users aren't prompted twice.

- Log into the HRMS system and navigate to *PeopleTools* → *Web Profile* → *Web Profile Configuration* → *<Profile>* → *Security*, where *<Profile>* is the current environment's Web Profile.
- Check the Allow Public Access checkbox.
- Set *User ID* and *Password* to the values set in [Step A](#) and click *Save*.

<input type="checkbox"/> PIA use HTTP Same Server ?	<input checked="" type="checkbox"/> Allow Unregistered Content ?	<b>SSL</b> <input type="checkbox"/> Secured Access Only ? <input checked="" type="checkbox"/> Secure Cookie with SSL ?
<b>Authenticated Users</b>		
<b>Inactivity Warning:</b> <input type="text" value="1,080"/> Seconds ?	<b>HTTP Session Inactivity:</b> <input type="text" value="0"/> Seconds ?	
<b>Inactivity Logout:</b> <input type="text" value="1,200"/> Seconds ?		
<b>Timeout Warning Script:</b> WEBLIB_TIMEOUT.PT_TIMEOUTWARNING.FieldFormula.IScript_TIMEOUTWARNING	<input type="button" value="Override"/>	?
<b>Public Users</b>		
<input checked="" type="checkbox"/> Allow Public Access ?	<b>User ID:</b> <input type="text" value="DEFAULT_USER"/> ?	
	<b>Password:</b> <input type="text" value="*****"/> ?	
	<b>HTTP Session Inactivity:</b> <input type="text" value="1,200"/> Seconds ?	
<b>Web Server Jolt Settings</b>		<b>XML Link</b>
<b>Disconnect Timeout:</b> <input type="text" value="0"/> Seconds ?	<b>User ID:</b> <input type="text" value="VP1"/> ?	
<b>Send Timeout:</b> <input type="text" value="50"/> Seconds ?	<b>Password:</b> <input type="text" value="***"/> ?	
<b>Receive Timeout:</b> <input type="text" value="600"/> Seconds ?	<input checked="" type="checkbox"/> XML Link Use HTTP Same Server ?	

 **Note:** The default user never signs in to a PeopleSoft application. PeopleSoft initiates a secure connection to the application server with the default user's credentials. The server then reads the RSA SecurID-authenticated username from an HTTP header and uses it to create a new session.



**G. Create a PeopleCode Signon script for RSA**

After each successful RSA SecurID authentication, PeopleSoft will run a script that reads the authenticated username from an HTTP header variable and use it to create a session. Log in to PeopleTools Application Designer and enter the following script (or a variation<sup>1</sup>) into an Application Designer record. A variable value in the script is set to the default user ID "DEFAULT\_USER". [If you chose to create a user with a different UID, you must change the "SignonUserId" variable's value in the script.](#)

```

/*//////////////////////////////////////////////////////////////////////////

RSA_SID. This function sets the CT_REMOTE_USER header variable to the value of the
authenticated user. PeopleSoft reads this value and changes the session id to match this user.
UserIDs have to match in both PeopleSoft and RSA Authentication Manager. You must change
the value of the SignonUserId variable if your default username isn't "DEFAULT_USER".

/*//////////////////////////////////////////////////////////////////////////

Function RSA_SID()


    If %PSAuthResult = True And &authMethod <> "WWW" And &authMethod <> "LDAP"
    And
        &authMethod <> "SSO" Then
        getWWWAuthConfig();

    If %SignonUserId = "DEFAULT_USER" Then
        &userID = %Request.GetHeader("ct-remote-user");
        If &userID <> "" Then
            SetAuthenticationResult( True, Upper(&userID), "", False);
            &authMethod = "RSA";
        End-If;
    End-If;
    End-If;

End-Function;

/*//////////////////////////////////////////////////////////////////////////

```

 **Note:** The default username must match the value of the "SignonUserId" variable.

**If your default username isn't "DEFAULT\_USER", you must modify the script by replacing "DEFAULT\_USER" with the appropriate UID (in quotation marks) in the following line:**

```
If %SignonUserId = "DEFAULT_USER" Then
```

<sup>1</sup> Only modify the Signon script if your default username isn't "DEFAULT\_USER". To do this, follow the above instructions. Be careful not to change the script in any other way.



You can either place the code into an existing record or use Application Designer to create a new one. Consult your PeopleCode documentation for instructions on how to access and edit Application Designer records.

In this example, the script was added to an existing record called “FUNCLIB\_LDAP”. Paste the code into the ‘FUNCLIB\_LDAP’ record in PeopleSoft Application Designer. (On Windows: *Start* → *Programs* → *PeopleTools Installation* → *Application Designer*). Make sure that you have permission to modify the ‘FUNCLIB\_LDAP’ record before logging into Application Designer.

### G. Activate the PeopleCode Signon script for RSA

Open the Signon PeopleCode page (PeopleTools → Security → Security Objects → Sign On PeopleCode) and do the following:

- Set the *Invoke as User ID* and *Password* fields with PeopleSoft credentials. The user must have permission to execute PeopleSoft Signon code. The “PS” UID is used in the following example.
- Create a new line by clicking on the ‘+’ button to the far right. Set the ‘Function Name’ column to ‘RSA\_SID’. Enter the same parameter values you used for the ‘FUNCLIB\_LDAP’ record.
- Enable this new line by checking the *Enable* box.
- The *Exec Auth Fail* checkbox must not be checked.
- Click *Save*.

## Signon PeopleCode

Signon

Invoke as user signing in

Invoke as User ID:  Password:

*Sequence	Enabled	*Record	*Field Name	Event Name	Function Name
1	<input type="checkbox"/>	FUNCLIB_PWDCNTL	PWDCNTL	FieldChange	Password_Controls
2	<input type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	WWW_AUTHENTICATION
3	<input type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	LDAP_AUTHENTICATION
4	<input type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	SSO_AUTHENTICATION
5	<input type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	LDAP_PROFILESYNCH
6	<input checked="" type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	RSA_SID



### G. RSA Authentication Manager Configuration

The RSA Web Agent doesn't populate an HTTP header variable with authenticated usernames. You must follow the instructions in this section to add this functionality. Once Authentication Manager has authenticated a user and written populated a header variable with the user's UID, the PeopleCode Signon script can access the UID and use it to create a PeopleSoft session.

- After installing the web agent, you need to install/enable the web agent's API. Please consult the *Web Authentication Developer's Guide* for platform-specific instructions. You'll find the guide in the *doc* directory of your agent's installation distribution.

See the Appendix for an example of enabling the API on Windows IIS.

- After RSA Authentication Manager authenticates a PeopleSoft user, the web agent creates an encrypted cookie that contains information about the user. Once you've enabled the web agent's API, you can use it in a script to read the username from this cookie and write it to the "CT\_REMOTE)USER" HTTP header variable. Please consult the *Web Authentication Developer's Guide* for platform-specific instructions.<sup>2</sup>

See the Appendix for an example for Windows IIS.

### F. Logout Screens

- The standard PeopleSoft "Logout" link must be modified or disabled. The following example sets the link to point to an HTML page that will close the browser.
- Navigate to %PEOPLETOOLS\_PORTAL\_HOME%\WEB-INF\psftdocs\ps and make a backup copy of signin.html. Copy the following code to a file named signin.html and replace the new file with the original file.

```
<html><head><body>

    <SCRIPT LANGUAGE="JavaScript">
        window.opener = top; window.close();
    </SCRIPT>

</body></html>
```

- Restart the servers.


---

<sup>2</sup> RSA provides APIs in many programming languages (Java, C, ASP, Perl, etc.) . Your *Web Authentication Developer's Guide* list the APIs available on your platform.



## G. Logon Screens

Once the integration is complete, RSA Authentication Manager will prompt PeopleSoft users for SecurID tokencodes before granting them access to requested resources.



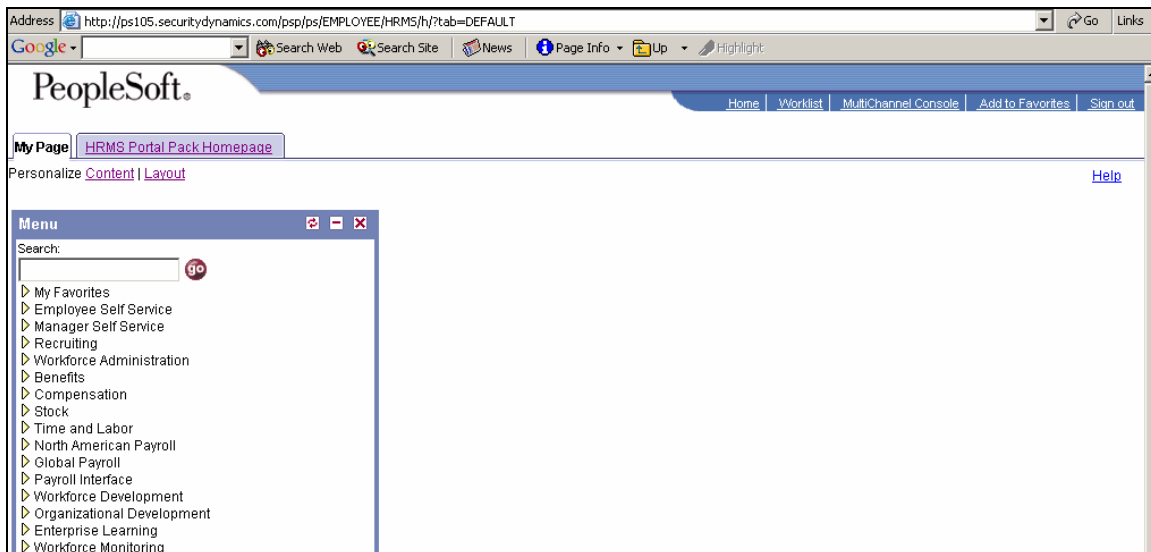
---

### RSA SecurID Username Request

The page you are attempting to access requires you to authenticate using your SecurID token.  
Enter your username and click **Send**.  
Click **Reset** to clear the field if you make a mistake.

Username:

After a successful authentication, PeopleSoft creates a new session for the user.



Address: <http://ps105.securitydynamics.com/psp/ps/EMPLOYEE/HRMS/h?tab=DEFAULT>

PeopleSoft. Home | Worklist | MultiChannel Console | Add to Favorites | Sign out

My Page: [HRMS Portal Pack Homepage](#)

Personalize [Content](#) | [Layout](#) [Help](#)

Menu

Search:

- My Favorites
- Employee Self Service
- Manager Self Service
- Recruiting
- Workforce Administration
- Benefits
- Compensation
- Stock
- Time and Labor
- North American Payroll
- Global Payroll
- Payroll Interface
- Workforce Development
- Organizational Development
- Enterprise Learning
- Workforce Monitoring

# Certification Checklist for RSA Authentication Manager 6.x

Date Tested: August 3, 2008

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.1	Windows 2003
RSA Authentication Agent	5.2	IIS 6.0
PeopleSoft HRMS	8.9	Windows 2003
PeopleTools	4.7	Windows 2003

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
<b>New PIN Mode</b>			
Force Authentication After New PIN	<input checked="" type="checkbox"/>	Force Authentication After New PIN	<input type="checkbox"/> N/A
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input type="checkbox"/> N/A
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input type="checkbox"/> N/A
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input type="checkbox"/> N/A
User Selectable	<input checked="" type="checkbox"/>	User Selectable	<input type="checkbox"/> N/A
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input type="checkbox"/> N/A
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input type="checkbox"/> N/A
<b>PASSCODE</b>			
16 Digit PASSCODE	<input checked="" type="checkbox"/>	16 Digit PASSCODE	<input type="checkbox"/> N/A
4 Digit Password	<input checked="" type="checkbox"/>	4 Digit Password	<input type="checkbox"/> N/A
<b>Next Tokencode Mode</b>			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input type="checkbox"/> N/A
<b>Load Balancing / Reliability Testing</b>			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input type="checkbox"/> N/A
Name Locking Enabled	<input checked="" type="checkbox"/>	Name Locking Enabled	<input type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input type="checkbox"/> N/A
<b>Additional Functionality</b>			
<b>RSA Software Token Automation</b>			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input type="checkbox"/> N/A	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
<b>RSA SecurID 800 Token Automation</b>			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input type="checkbox"/> N/A	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
<b>Domain Credential Functionality</b>			
Determine Cached Credential State	<input type="checkbox"/> N/A	Determine Cached Credential State	<input type="checkbox"/>
Set Domain Credential	<input type="checkbox"/> N/A	Set Domain Credential	<input type="checkbox"/>
Retrieve Domain Credential	<input type="checkbox"/> N/A	Retrieve Domain Credential	<input type="checkbox"/>

JGS

✓ = Pass ✗ = Fail N/A = Non-Available Function

# Certification Checklist for RSA Authentication Manager 7.1

Date Tested: June 30, 2008

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.1	Windows 2003
RSA Authentication Agent	5.2	IIS 6.0
PeopleSoft HRMS	8.9	Windows 2003
PeopleTools	4.7	Windows 2003

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
<b>New PIN Mode</b>			
Force Authentication After New PIN	<input checked="" type="checkbox"/>	Force Authentication After New PIN	<input type="checkbox"/> N/A
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input type="checkbox"/> N/A
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input type="checkbox"/> N/A
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input type="checkbox"/> N/A
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input type="checkbox"/> N/A
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input type="checkbox"/> N/A
Deny Numeric PIN	<input checked="" type="checkbox"/>	Deny Numeric PIN	<input type="checkbox"/> N/A
PIN Expiration	<input checked="" type="checkbox"/>	PIN Expiration	<input type="checkbox"/> N/A
PIN Reuse	<input checked="" type="checkbox"/>	PIN Reuse	<input type="checkbox"/> N/A
<b>Passcode</b>			
16 Digit Passcode	<input checked="" type="checkbox"/>	16 Digit Passcode	<input type="checkbox"/> N/A
4 Digit Fixed Passcode	<input checked="" type="checkbox"/>	4 Digit Fixed Passcode	<input type="checkbox"/> N/A
<b>Next Tokencode Mode</b>			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input type="checkbox"/> N/A
<b>Load Balancing / Reliability Testing</b>			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input type="checkbox"/> N/A
Name Locking Enabled	<input checked="" type="checkbox"/>	Name Locking Enabled	<input type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input type="checkbox"/> N/A
Additional Functionality			
<b>RSA Software Token Automation</b>			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
<b>RSA SecurID 800 Token Automation</b>			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A

JGS

✓ = Pass ✗ = Fail N/A = Non-Available Function



## Known Issues

---

### Setting Cookie Expiration Times

A Web access authentication cookie is valid only during the browsing session for which it was created. If the user exits the Web browser, the cookie expires, and the user must get a new cookie during the next authentication session.

Before enabling Web access authentication cookies, decide what expiration constraints, if any, to place on the cookies you distribute to RSA SecurID users. For example, you can configure cookies to always expire during a browsing session.

If a cookie is replaced before a customized Web access authentication browser cookie expires, the replacement cookie supersedes the customized cookie. As a result, you lose any third-party data you are setting using the Web Authentication API. To prevent the loss of third-party data, use the following guidelines to configure your Web Agent cookie expiration times so that you have an appropriate window for setting third-party data:

- If the expiration time for idle cookies is greater than the overall cookie expiration time, the idle cookie feature becomes invalid, and the cookie is not replaced.
- If the expiration time for idle cookies is less than three minutes and less than the overall cookie expiration time, the cookie is replaced every 30 seconds.
- If the expiration time for idle cookies is greater than three minutes but less than the overall cookie expiration time, the cookie is replaced every 60 seconds.
- To configure cookie expiration times, see the Web Agent Help topics “Controlling Cookie Expiration Times” and “Setting Cookie Expiration Times.”



## Appendix

---

### Enabling the Web Authentication API on Windows

Supported Platforms for this example:	
Operating System	Web Server
Windows Server 2003, Standard Edition	IIS 6.0
Windows Server 2003, Enterprise Edition	IIS 6.0
Windows 2000 Server with Service Pack 4	IIS 5.0

The RSA Authentication Agent 5.3 for Web automatically installs the **rsacookieapi.dll** in the web server **%SystemRoot%\system32** directory. Before you can use the **rsacookieapi.dll**, however, you must enable the use of the Web Authentication API.

To enable the Web Authentication API:

1. Open the ISM by clicking Start > Settings > Control Panel, and double-clicking 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 Options, clear Disable Cookie API.
  6. Click Apply, and then click OK.
  7. Restart the virtual server from the ISM.
-



## Enabling the Web Authentication API on Windows

### Supported Platforms for this example:

Operating System	Web Server
Windows Server 2003, Standard Edition	IIS 6.0
Windows Server 2003, Enterprise Edition	IIS 6.0
Windows 2000 Server with Service Pack 4	IIS 5.0

RSA Authentication Agent for Web does not populate the HTTP header variable REMOTE\_USER; the field may be populated by the web server or another application. For example, if the resource is also protected by NTLM/IWA, then the value will be populated with the name used for the NTLM/IWA authentication. For security reasons, the HTTP header variable REMOTE\_USER must not be used to verify the SecurID user name.

To obtain the RSA SecurID authenticated user name, use the RSA Authentication Agent for Web API. Examples of how to do this in CGI, JScript, and VBScript are provided with the agent installation media. An example of how to call the user name in ASP is given below:

```
<% Dim RSACookieAPI
Set RSACookieAPI = Server.CreateObject("Rsacookieapi.RSACookie") %>
<%Response.AddHeader "CT_REMOTE_USER", RSACookieAPI %>
```