

# **RSA Secured Partner Certification Portal Guide**

**Enabling Partner Products for RSA SecurID Two Factor  
Authentication**

Last Updated: February 15, 2007



# Table of Contents

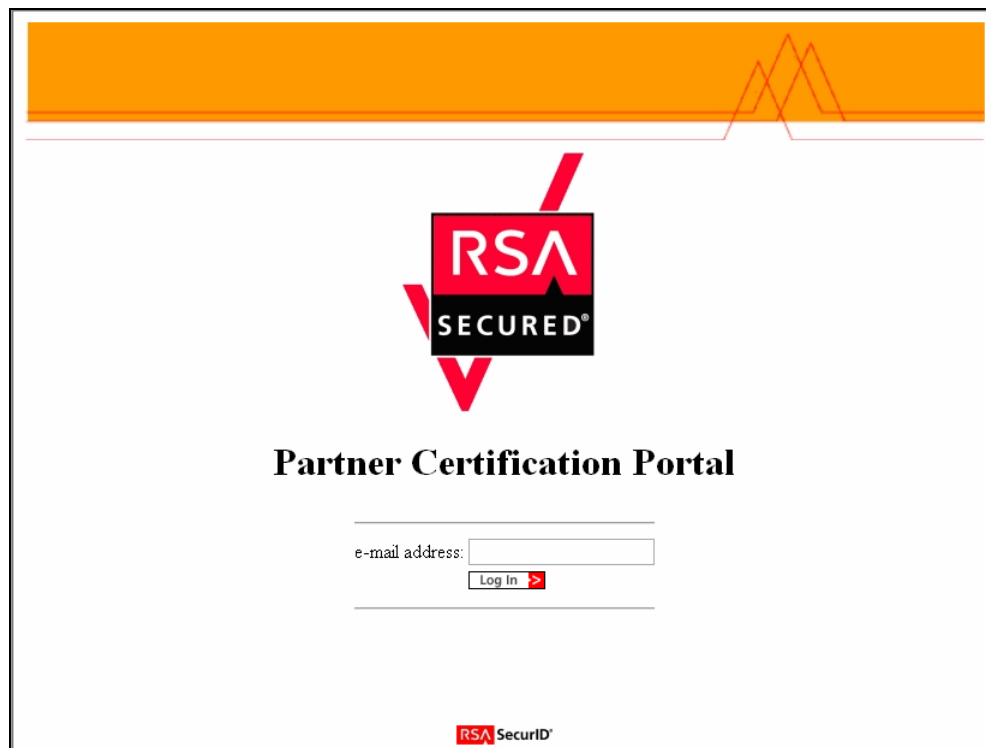
Completing RSA Secured Certification Testing.....	3
What is the Partner Certification Portal? .....	3
Problems, Questions, Comments and Failures .....	4
Accessing the Portal .....	5
Logging in for the First Time.....	6
Logging out of the Portal .....	7
Inactivity Timeout .....	7
Changing the Profile .....	8
Testing Overview .....	9
Running the Tests .....	9
Deploying the Default Java Token.....	9
Completing Certification .....	10
Mandatory Functionality Testing .....	11
Test #1 .....	11
Test #2 .....	11
Test #3 .....	11
Test #4 .....	12
Test #5 .....	13
Test #6 .....	13
Appendix.....	15
Supported Software .....	15
Web Browser(s).....	15
Java VM .....	15
Profile Configuration .....	15
Downloading sdconf.rec .....	15
Adding Agent Host Record(s).....	16
Clearing the Agent Host Node Secret .....	17
Uploading new Seed Record(s).....	18
Changing Serial Number(s) .....	19
RADIUS Testing Information .....	20
RADIUS Client Setup .....	20
RADIUS Server Configuration .....	20
Retrieving the RSA Authentication Manager Server Logs .....	21
Session Logs.....	21
Test Logs .....	22
Refreshing the Log .....	23
Restarting Tests.....	23

# Completing RSA Secured Certification Testing

This document describes how the partner should prepare for and perform the tests necessary to complete the RSA SecurID Ready checklist using the RSA Secured Partner Certification Portal. These steps are listed in order and should guide you through the testing procedures in an efficient manner.

To document results, print out the RSA SecurID Ready Checklist which is located at the end of the RSA SecurID Ready Implementation Guide template.

## What is the Partner Certification Portal?



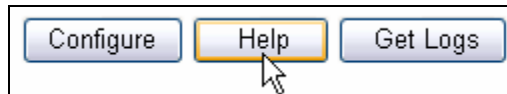
### *The Partner Certification Portal*

The Partner Certification Portal is a web based portal that allows RSA Technology Partners to perform RSA SecurID certification testing via the Internet. The portal controls the Authentication Manager servers such that the user and test parameters are configured at the back-end. For a partner to perform the testing to achieve certification status, the following prerequisites must be satisfied:

- The end user must have Internet access and a supported web browser (See **Appendix: Supported Software**) with the Java plug-in, JavaScript and Cookie support enabled.
- The end user must have the most recent Java VM installed. (See **Appendix: Supported Software**).
- The device or software being tested must have a valid hostname.
- The device or software being tested must be routable to a public IP address.

## Problems, Questions, Comments and Failures

Any issues encountered during certification testing that prove difficult to troubleshoot should be reported to the Partner Development Engineering group by clicking the **Help** button on the main page.



*The help button is located on the main page.*

On clicking the **Help** button the partners e-mail client is invoked with a recipient and subject auto populated. The partner must enter their company name into the subject line by overwriting the label <COMPANY NAME>.



*Pressing the Help button invokes e-mail.*

In the situation where help is needed, the partner should include a detailed description of the problem including steps to recreate the issue and the dates and times the error occurred. Any additional information such as screenshots or debug output can also be attached to the message.

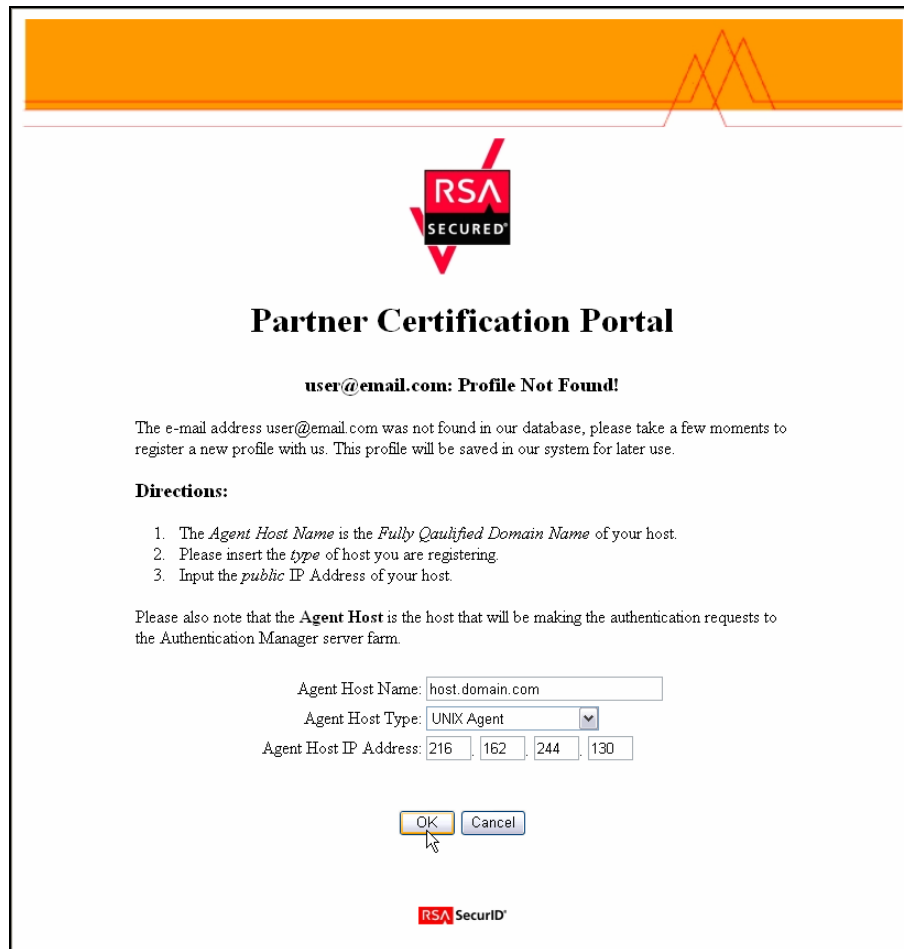
## Accessing the Portal

With a supported web browser (See **Appendix**) navigate to: <https://pe006.pe-lab.com/PEClient/> and log in using a valid e-mail address.



**IMPORTANT: Install the Root Certificate for the RSA Partner Portal Application Server before logging into the Portal.**

## Logging in for the First Time



The screenshot shows the RSA SecurID Partner Certification Portal. At the top is the RSA SecurID logo. Below it, the title "Partner Certification Portal" is centered. A message states: "user@email.com: Profile Not Found!". Below this, a paragraph explains that the email address was not found in the database and that a new profile should be registered. A section titled "Directions:" lists three steps: 1. The Agent Host Name is the Fully Qualified Domain Name of your host. 2. Please insert the type of host you are registering. 3. Input the public IP Address of your host. Below the directions, a note states: "Please also note that the Agent Host is the host that will be making the authentication requests to the Authentication Manager server farm." A registration form follows with three fields: "Agent Host Name" with the value "host.domain.com", "Agent Host Type" with a dropdown menu showing "UNIX Agent", and "Agent Host IP Address" with four input boxes containing "216", "162", "244", and "130". At the bottom of the form are "OK" and "Cancel" buttons. The RSA SecurID logo is at the very bottom of the page.

### *Example of logging in for the first time*

The first time entering the Portal, the partner will be greeted and asked for a valid e-mail address. The e-mail address will act as a label for the partner profile. The profile will store information about the partner's environment necessary for testing. The RSA Authentication Manager servers need to know the location information of the device or software being tested and the serial numbers for the hardware authenticators. Have the following information handy to answer the following questions to become registered:

- The Agent Host Fully Qualified Domain Name of software or device.
- The Agent Host IP Address of software or device.
- The Agent Host Type of software or device.
- Unique serial numbers for RSA Hardware Authenticators (**OPTIONAL**: Shipped from RSA).

**IMPORTANT: If the device or software being tested uses the RADIUS protocol to communicate with the RSA Authentication Manager servers, please contact the Partner Development Engineering group via the Help button as some back-end configuration must be performed.**

## Logging out of the Portal

The Portal must be logged out of once the partner is ready to end their session. To log out, simply click the button labeled **Logout**.

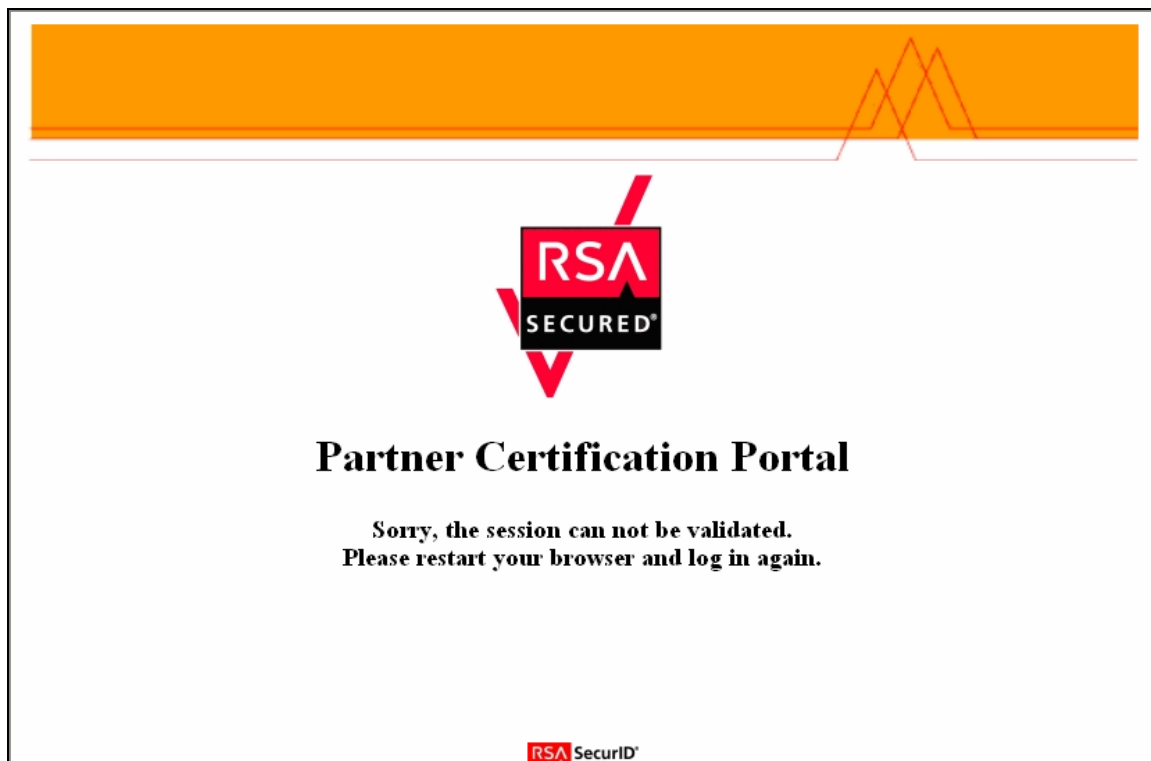


*Click the Logout button at the top of the main menu*

**IMPORTANT:** Do not just close out the web browser to end the user session, click the button labeled Logout located at the top of the main menu to avoid potentially becoming locked out of the Portal. If it is suspected that the partner is locked out please contact the Partner Development Engineering group via the Help button.

## Inactivity Timeout

The Portal tracks the partner's activity and will timeout if no activity is generated. When a timeout occurs the partner session is destroyed resulting in the partner becoming logged off the portal. The partner has an allowance of 30 minutes of inactivity before becoming logged off. When a timeout happens, the partner is not immediately notified. The next button the partner clicks on will result in the error message that is pictured below. At this point the partner must log back into the Portal.

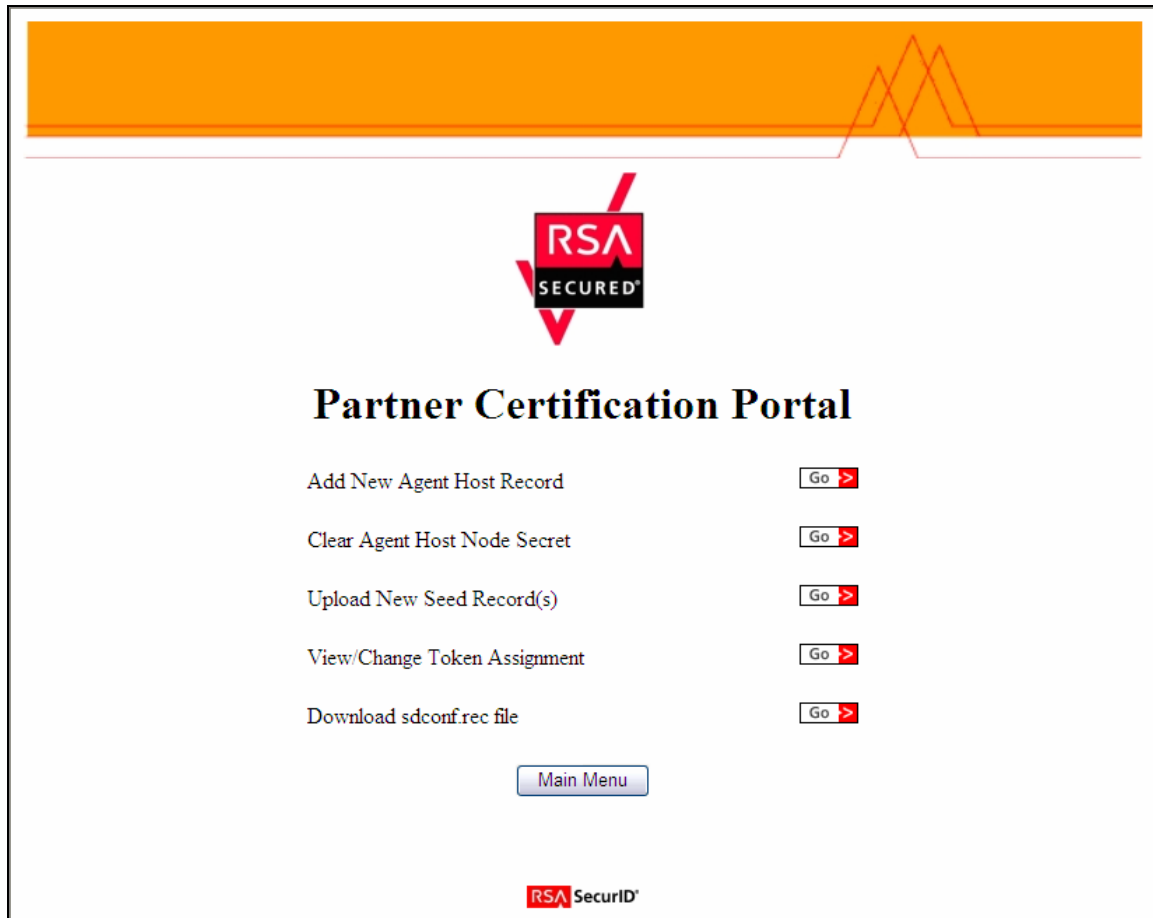


*The session has timed out.*

**IMPORTANT:** If a partner is logged off due to portal inactivity during a certification testing, the procedure must be restarted from the beginning. This means the partner must not resume testing from the point at which they became inactive but instead start testing back at Test #1.

## Changing the Profile

Clicking on the button labeled **Configure** at the top of the main menu allows the partner to adjust their profile. The configuration options include adding new Agent Host records to the RSA Authentication Manager Servers, uploading new Seed Records, changing the Serial Numbers for the token used in testing, or the download of the sdconf.rec file (See **Appendix**).




*The main screen for Configure Profile*

## Testing Overview

### Running the Tests

It is required that each test suite be run in order from Test #1 to Test #6 in one session to complete certification. The partner is free to run tests in any order for testing purposes, but must log out and back in for certification. The entire process should take no longer than 1 hour however it is likely only 30-45 minutes will be needed. Please make sure that the required time is set aside for testing. Start a test suite by clicking the button labeled "Start" to the right of the test description as pictured below.

Test Title	Test Description	Action
Test #1	PROCEDURE: user authenticates using the assigned token.  TESTS: Force Authentication after New PIN System Generated PIN Name Locking Enabled	

***Click Start to begin the test procedure***

Clicking start takes the partner into a new screen that displays the steps of the test. The tests must be run in chronological order in order to be run successfully. For the partner, the steps that complete each test are labeled as such, refer to the example below.

5. The user should enter the passcode and then be successfully connected. [Test Passed: Force Authentication after New PIN and Name Locking Enabled]
--

***The steps are labeled to show a test pass***

Above the test procedure are quick directions showing the partner which user to use for testing as well as what type of Authenticator (ex. Token or Password). If a Token is being used, the serial number will be displayed to the right of the Authenticator type in brackets. If an error occurs at the RSA Authentication Manager Server when setting up the Token for the user the error message will display instead of the serial number in brackets.

<b>DIRECTIONS:</b> Authenticator => token [Bad Token Serial]
---

***Error setting the token for the test***

### Deploying the Default Java Token

Click the **Launch Token** button to deploy the Java based software token to begin testing.



***Launch the default Java token***

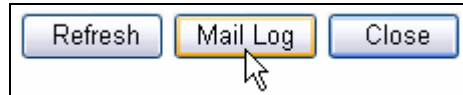
When the button has been clicked a Java applet will deploy to the partners desktop in a separate browser window. This token will be the default token used for testing.



***The default Java Token running***

## Completing Certification

Once all of the test suites have been passed, the partner must return to the main menu, get the logs and copy them into an e-mail to be sent off to the Partner Development Engineering group along with a completed Implementation Guide.



*The Mail Log button is located in the log window*

Begin by retrieving the session logs (See **Appendix: Session Logs**) and then click the **Mail Log** button located in the log window.



*The Mail Log button invokes e-mail*

By clicking the **Mail Log** button the partners e-mail client is invoked with an auto populated recipient and subject line. Complete the subject by inserting a company name in for the label <COMPANY NAME>. Next paste the contents of the session log into the e-mail body along with contact information such as full name and phone number with extension. Lastly attach the completed Implementation Guide to the e-mail and send it off to the Partner Development Engineering group.

## Mandatory Functionality Testing

**IMPORTANT: The user name for all tests is 'user'. Make sure that a token serial number appears at the top of test before starting a test.**

### Test #1

1. Begin the authentication process.
2. The user will be prompted to input *user name* and *PASSCODE* and should then enter the current tokencode on the token.
3. Accept the System Generated PIN.



**This completes the System-generated PIN.**

4. The user should be prompted to wait for the tokencode to change and enter the passcode.
5. The user should enter the passcode and then be successfully connected.



**This completes the Force Authentication after New PIN and Name Locking Enabled.**

### Test #2

1. Begin the authentication process.
2. The user will be prompted to input *user name* and *PASSCODE* and should then enter the current tokencode on the token.
3. The user creates a new PIN of **abcd**.
4. The user should be prompted to wait for the tokencode to change and enter the passcode.
5. The user should enter the passcode and then be successfully connected.



**This completes the User Defined (4-8) Alphanumeric.**

1. Restart the authentication process.
2. The user will be prompted to input *user name* and *PASSCODE* and should then enter the password **12345**.
3. The user creates a new PIN of **1234**.
4. The user should be prompted to wait for the tokencode to change and enter the passcode.
5. The user should enter **1234** and then be successfully connected.



**This completes the 4 Digit Password.**

### Test #3

1. Begin the authentication process.
2. The user will be prompted to input *user name* and *PASSCODE* and should then enter the password **12345**.
3. The user creates a new PIN of **abcde**.
4. The user should not be successfully connected.



**This completes the Deny Alphanumeric PIN.**

1. Restart the authentication process.
2. The user will be prompted to input *user name* and *PASSCODE* and should then enter the password **12345**.
3. The user creates a new PIN of **1234**.
4. The user should not be successfully connected.



**This completes the part 1 of 2 for Deny 4 and 8 digit PIN.**

1. Restart the authentication process.
2. The user will be prompted to input *user name* and *PASSCODE* and should then enter the password **12345**.
3. The user creates a new PIN of **12345678**.
4. The user should not be successfully connected.



**This completes the part 2 of 2 for Deny 4 and 8 digit PIN.**

1. Restart the authentication process.
2. The user will be prompted to input *user name* and *PASSCODE* and should then enter the password **12345**.
3. The user creates a new PIN of **12345**.
4. The user should be prompted to wait for the tokencode to change and enter the passcode.
5. The user should enter **12345** and then be successfully connected.



**This completes the User Defined (5-7 Numeric).**

#### **Test #4**

1. Begin the authentication process.
2. The user will be prompted to input *user name* and *PASSCODE* and should then enter the current tokencode on the token.
3. The user creates a new PIN of **abcd**.
4. The user should be prompted to wait for the tokencode to change and enter the passcode.
5. The user should enter the passcode and then be successfully connected.



**This completes the part 1 of 2 for User Selectable.**

1. Restart the authentication process.
2. The user will be prompted to input *user name* and *PASSCODE* and should then enter the password **12345**.
3. The user creates a new PIN of **12346**.
4. The user should be prompted to wait for the tokencode to change and enter the passcode.
5. The user should enter **1234** and then be successfully connected.



**This completes the part 2 of 2 for User Selectable.**

1. Begin the authentication process.
2. The user will be prompted to input *user name* and *PASSCODE* and should then enter the password **123456789**.
3. The user should not be successfully connected.
4. Repeat steps 1-3 for two more iterations.

The Token should be set to Next Tokencode Mode [See Log]

1. Restart the authentication process.
2. The user will be prompted to input *user name* and *PASSCODE* and should then enter the current passcode.
3. The user should be prompted to wait for the tokencode to change and enter the next passcode.
4. The user should enter the current passcode and then be successfully connected.



This completes the Next Tokencode Mode.

### Test #5

1. Begin the authentication process.
2. The user will be prompted to input *user name* and *PASSCODE* and should then enter the current tokencode on the token.
3. The user creates a new PIN of **12345678**.
4. The user should be prompted to wait for the tokencode to change and enter the passcode.
5. The user should enter the passcode and then be successfully connected.



This completes the 16-Digit Passcode.

### Test #6

1. Stop the primary server authentication service by clicking the **Stop** Action button for the primary server.

The Status should change to Stopped and the Button change to Start.

2. Begin the authentication process.
3. The user will be prompted to input user name and PASSCODE and should then enter the current tokencode on the token.
4. The user should enter the passcode and then be successfully connected.



This completes the part 1 of 3 for Failover (3-10 Replicas).

5. Stop the first replica authentication by clicking the **Stop** Action button for the 1st replica server.

The Status should change to Stopped and the Button change to Start.

6. Restart the authentication process.
7. The user will be prompted to input user name and PASSCODE and should then enter the current tokencode on the token.

8. The user should enter the passcode and then be successfully connected.



**This completes the part 2 of 3 for Failover (3-10 Replicas).**

9. Stop the second replica authentication by clicking the **Stop** Action button for the 2nd replica server.

**The Status should change to Stopped and the Button change to Start.**

10. Restart the authentication process.

11. The user will be prompted to input user name and PASSCODE and should then enter the current tokencode on the token.

12. The user should enter the passcode and not be successfully connected.



**This completes the part 3 of 3 for Failover (3-10 Replicas).**

13. Start again all authentication servers by clicking the **Start** Action button for the all of the servers.

**The Status' should change to Running and the Buttons change to Stop for all servers.**

14. Restart the authentication process. .

15. The user will be prompted to input user name and PASSCODE and should then enter the current tokencode on the token.

16. The user should enter the passcode and then be successfully connected.



**This completes the No RSA Authentication Manager.**

# Appendix

## Supported Software

### Web Browser(s)

- Internet Explorer 6.0 SP2\*
- Mozilla Firefox 1.x\*

### Java VM

- Sun Microsystems Java 1.5 or greater\*\*

\*Must have the Java Plug-in, JavaScript 1.3 and Cookie support.

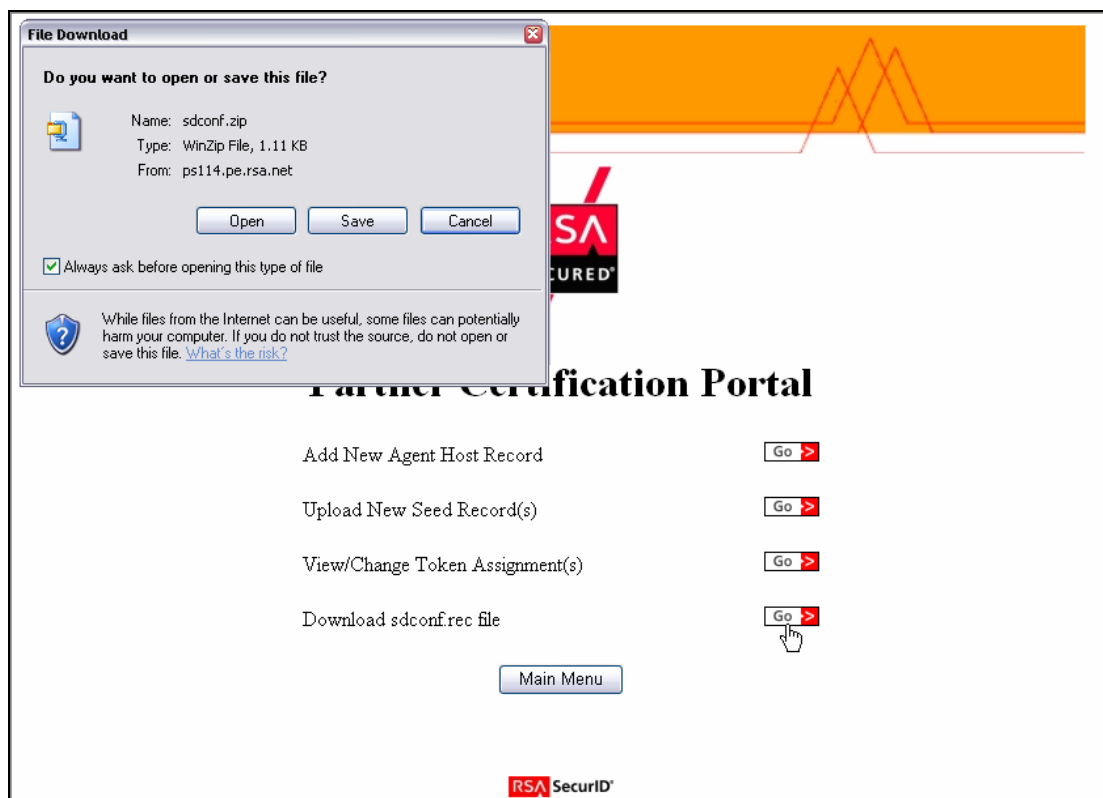
\*\*All Patch levels are supported by the portal.

## Profile Configuration

During any point in the profile configuration, a **Cancel** button when clicked will return the partner to the main menu of the Portal.

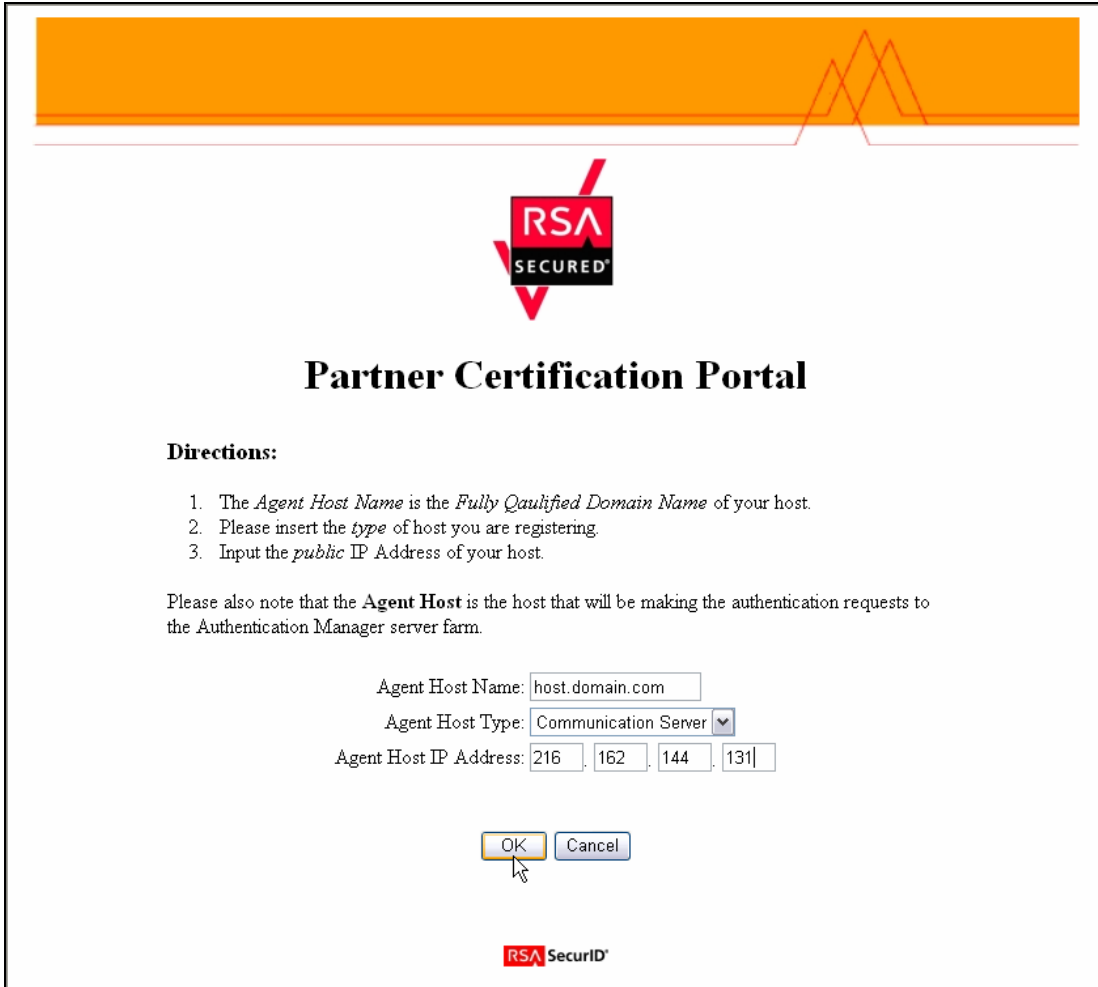
### Downloading sdconf.rec

To download the sdconf.rec, navigate to the configuration menu and click the **Go** button next to the **Download sdconf.rec** label. Refer to the Partner Development Guide for more information on the sdconf.rec file.



## Adding Agent Host Record(s)

- Click on the **Go** button for **Add New Agent Host Record**.
- Fill in the form making sure the prerequisites for the Portal listed in the first section of the Partner Certification Portal Guide.



The screenshot shows the RSA SecurID Partner Certification Portal. At the top is an orange header bar. Below it is the RSA SECURED logo, which consists of a red square with 'RSA' in white and a black square with 'SECURED' in white, flanked by two red arrows pointing towards each other. The title 'Partner Certification Portal' is centered below the logo. Underneath the title is the section 'Directions:' followed by a numbered list of three steps. Below the list is a paragraph of text. Then there is a form with three fields: 'Agent Host Name' with the value 'host.domain.com', 'Agent Host Type' with a dropdown menu showing 'Communication Server', and 'Agent Host IP Address' with four input boxes containing '216', '162', '144', and '131'. At the bottom of the form are 'OK' and 'Cancel' buttons. The RSA SecurID logo is at the very bottom of the window.

**Partner Certification Portal**

**Directions:**

1. The *Agent Host Name* is the *Fully Qualified Domain Name* of your host.
2. Please insert the *type* of host you are registering.
3. Input the *public* IP Address of your host.

Please also note that the **Agent Host** is the host that will be making the authentication requests to the Authentication Manager server farm.

Agent Host Name:

Agent Host Type:

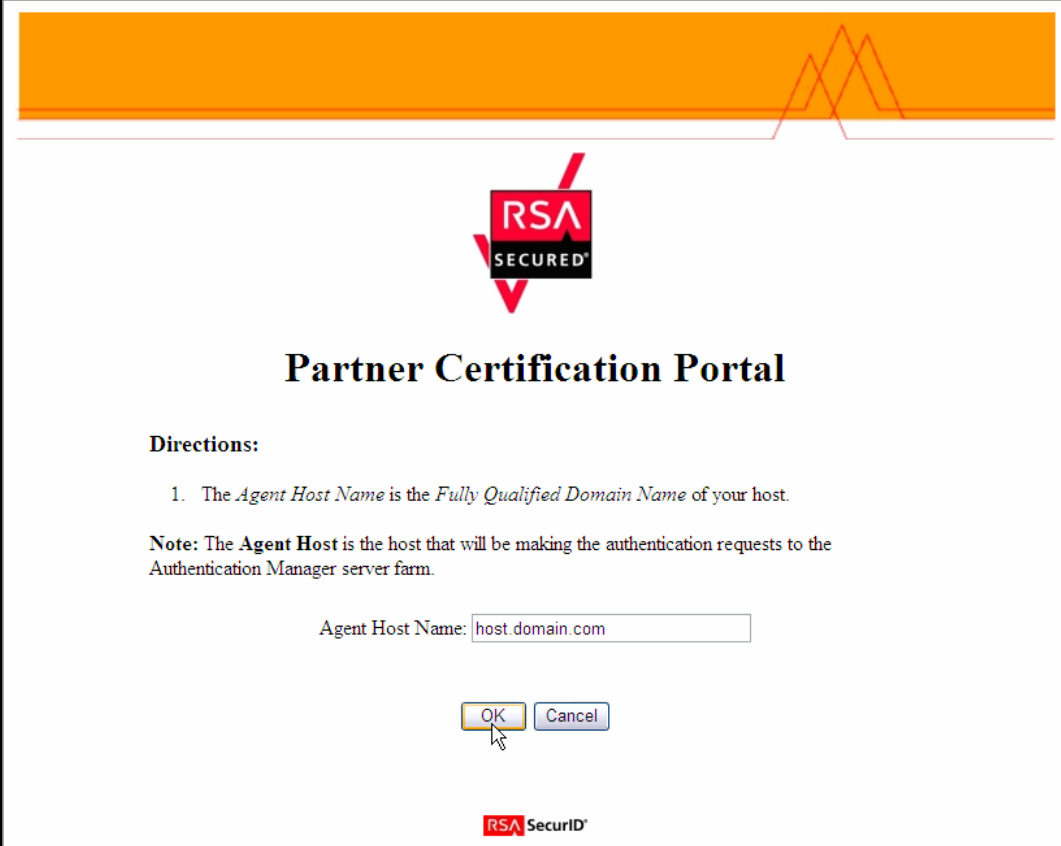
Agent Host IP Address:

**RSA SecurID**

***Example of adding a new Agent Host record to RSA Authentication Manager***

## Clearing the Agent Host Node Secret

- Click on the **Go** button for **Clear Agent Host Node Secret**.
- Fill in the text box with the **Fully Qualified Domain Name** of the **Agent Host** that will have the node secret cleared.
- Click the **OK** button

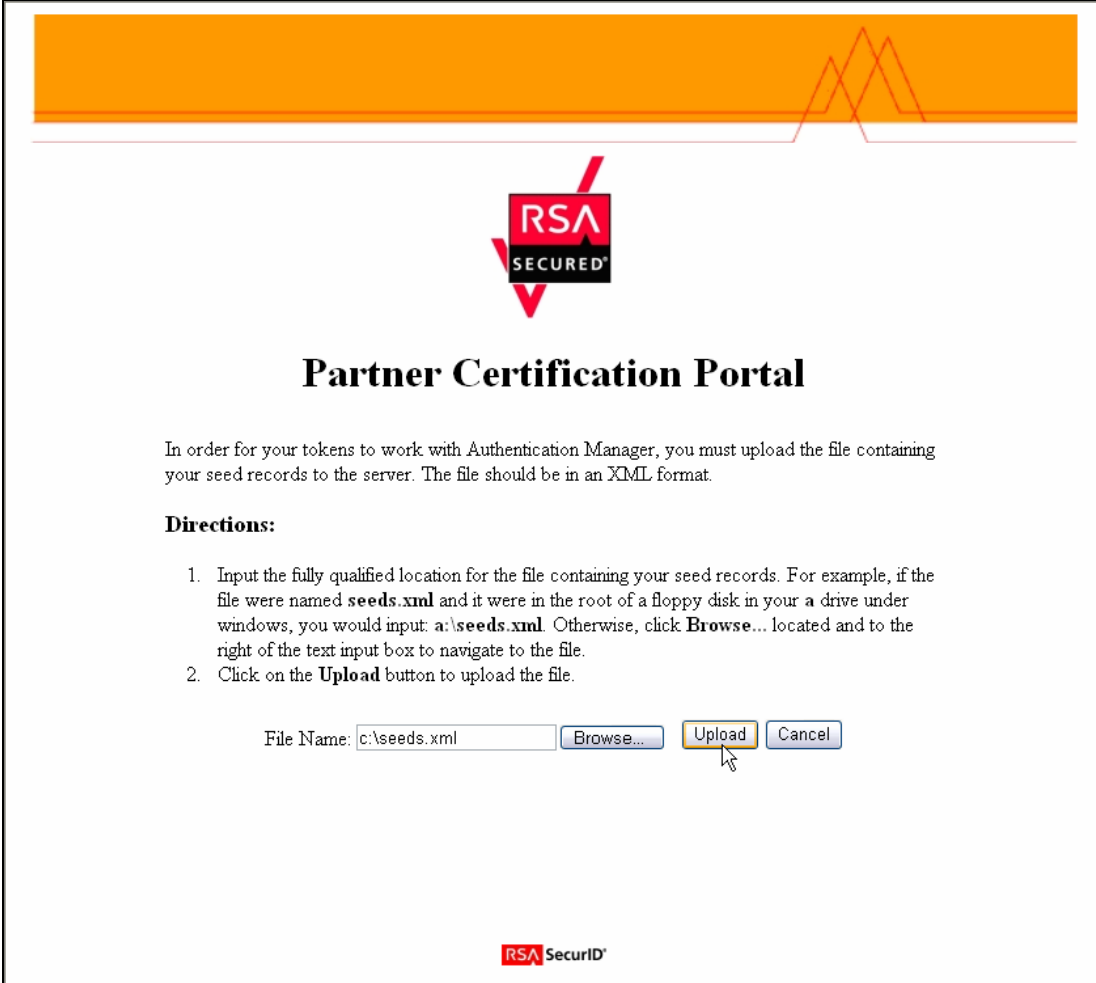


The screenshot shows the RSA SecurID Partner Certification Portal. At the top is an orange header bar. Below it is the RSA SECURED logo, which consists of a red square with 'RSA' in white and 'SECURED' in black, with a red checkmark above it. The main title is 'Partner Certification Portal'. Underneath is the section 'Directions:' followed by a numbered list: '1. The *Agent Host Name* is the *Fully Qualified Domain Name* of your host.' Below this is a 'Note:' stating: 'The **Agent Host** is the host that will be making the authentication requests to the Authentication Manager server farm.' There is a text input field labeled 'Agent Host Name:' containing the text 'host.domain.com'. Below the input field are two buttons: 'OK' and 'Cancel'. A mouse cursor is pointing at the 'OK' button. At the bottom of the portal is the RSA SecurID logo.

***Example of clearing the node secret for an Agent Host***

## Uploading new Seed Record(s)

- Click on the **Go** button for **Upload New Seed Record(s)**.
- Fill in the text box with the Fully Qualified location (example: C:\Seeds.xml) of the XML file containing the valid Seed Records or click the **Browse** button and navigate to the file.
- Click the **Upload** button.




The screenshot displays the RSA SecurID Partner Certification Portal. At the top, there is an orange header bar. Below it, the RSA SECURED logo is centered. The main heading is "Partner Certification Portal". A paragraph of text states: "In order for your tokens to work with Authentication Manager, you must upload the file containing your seed records to the server. The file should be in an XML format." Below this, the "Directions:" section lists two steps: 1. Input the fully qualified location for the file containing your seed records. For example, if the file were named **seeds.xml** and it were in the root of a floppy disk in your a drive under windows, you would input: **a:\seeds.xml**. Otherwise, click **Browse...** located and to the right of the text input box to navigate to the file. 2. Click on the **Upload** button to upload the file. Below the directions, there is a form with a "File Name:" label, a text input box containing "c:\seeds.xml", and three buttons: "Browse...", "Upload", and "Cancel". A mouse cursor is pointing at the "Upload" button. At the bottom of the form, the RSA SecurID logo is displayed.

***Example of uploading more Seed Records to RSA Authentication Manager***

## Changing Serial Number(s)

- Click the **Go** button for **View/Change Token Assignment**.
- Input the new Serial Number for their respective User.



The screenshot shows the RSA SecurID Partner Certification Portal. At the top is an orange header bar. Below it is the RSA SECURED logo. The main heading is "Partner Certification Portal" followed by "Assign Tokens". Under "Directions:", there is a list item: "1. Please input the *unique* token serial number." Below this is a note: "Note: The serial number for the default token is: 000030463563". There is a text input field labeled "User Token:" containing the value "000030463563". Below the input field are "OK" and "Cancel" buttons. At the bottom of the page is the RSA SecurID logo.

### *Example of changing the RSA hardware authenticators used during tests*

Note: RSA Hardware Authenticator Serial Numbers may be up to 12 digits in length, however most are not. The RSA Authentication Manager Server requires that all Serial Numbers contain 12 digits. This is achieved by padding the Serial Number with leading 0's and is reflected to the user in this configuration form. It is considered valid input with or without the leading 0's by the partner as the Partner Certification Portal will provide the padding to the RSA Authentication Manager Servers.

## RADIUS Testing Information

### RADIUS Client Setup

If the partner product has been implemented using the RADIUS protocol, please contact the RSA Partner Development group at [RSASelfCert@rsa.com](mailto:RSASelfCert@rsa.com). Include the following information in your e-mail so that a RADIUS client will be setup for testing:

- Public host name and IP address of the RADIUS client that will communicate with RSA servers.
- Private host name and IP address of the RADIUS client that will communicate with RSA Servers.  
[OPTIONAL]

### RADIUS Server Configuration

The partner product RADIUS configuration will need to be configured to authenticate using the addresses listed below:

**SERVER 1:** pe006.pe-lab.com [216.162.248.6]

**SERVER 2:** pe007.pe-lab.com [216.162.248.7]

**SERVER 3:** pe008.pe-lab.com [216.162.248.8]

The RADIUS secret to be used is:

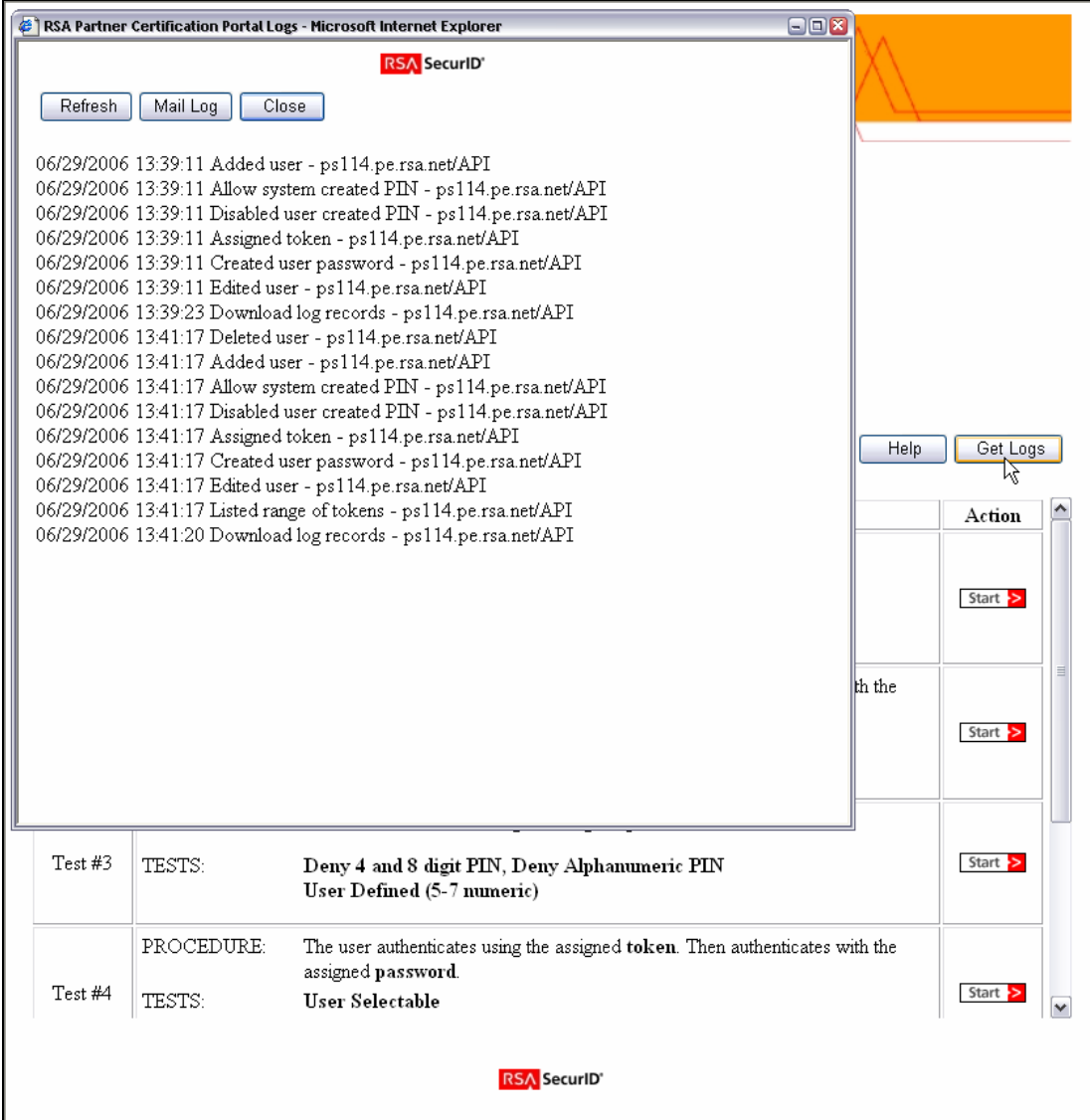
**SECRET:** 12345678

**Note:** It is the responsibility of the partner to implement failover when using the RADIUS protocol.

## Retrieving the RSA Authentication Manager Server Logs

### Session Logs

The partner may request the RSA Authentication Manager Server Logs at any point during their connection to the Partner Certification Portal. To retrieve the logs, click the **Get Logs** button located at the top of the **Main Menu**. Clicking this button will get the partner the entire logs for their current session only. If the partner requires back logs, please contact the Partner Development Engineering group via the **Help** button with the desired date(s) and time(s) for the log.



**RSA SecurID**

Refresh Mail Log Close

06/29/2006 13:39:11 Added user - ps114.pe.rsa.net/API  
06/29/2006 13:39:11 Allow system created PIN - ps114.pe.rsa.net/API  
06/29/2006 13:39:11 Disabled user created PIN - ps114.pe.rsa.net/API  
06/29/2006 13:39:11 Assigned token - ps114.pe.rsa.net/API  
06/29/2006 13:39:11 Created user password - ps114.pe.rsa.net/API  
06/29/2006 13:39:11 Edited user - ps114.pe.rsa.net/API  
06/29/2006 13:39:23 Download log records - ps114.pe.rsa.net/API  
06/29/2006 13:41:17 Deleted user - ps114.pe.rsa.net/API  
06/29/2006 13:41:17 Added user - ps114.pe.rsa.net/API  
06/29/2006 13:41:17 Allow system created PIN - ps114.pe.rsa.net/API  
06/29/2006 13:41:17 Disabled user created PIN - ps114.pe.rsa.net/API  
06/29/2006 13:41:17 Assigned token - ps114.pe.rsa.net/API  
06/29/2006 13:41:17 Created user password - ps114.pe.rsa.net/API  
06/29/2006 13:41:17 Edited user - ps114.pe.rsa.net/API  
06/29/2006 13:41:17 Listed range of tokens - ps114.pe.rsa.net/API  
06/29/2006 13:41:20 Download log records - ps114.pe.rsa.net/API

Help Get Logs

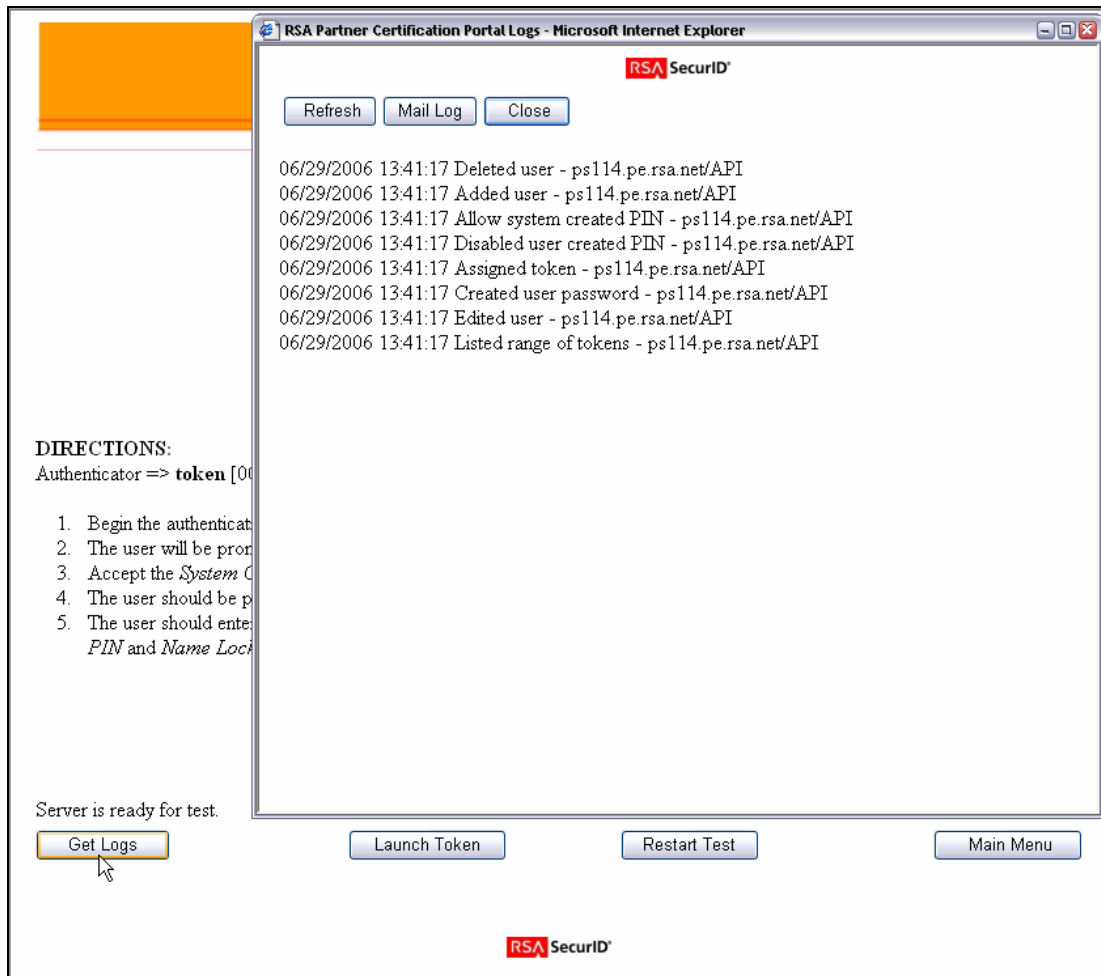
	Action
	Start >
th the	Start >
	Start >
Test #3	TESTS: Deny 4 and 8 digit PIN, Deny Alphanumeric PIN User Defined (5-7 numeric)
Test #4	PROCEDURE: The user authenticates using the assigned token. Then authenticates with the assigned password. TESTS: User Selectable

**RSA SecurID**

*Clicking on Get Logs for RSA Authentication Manager logs*

## Test Logs

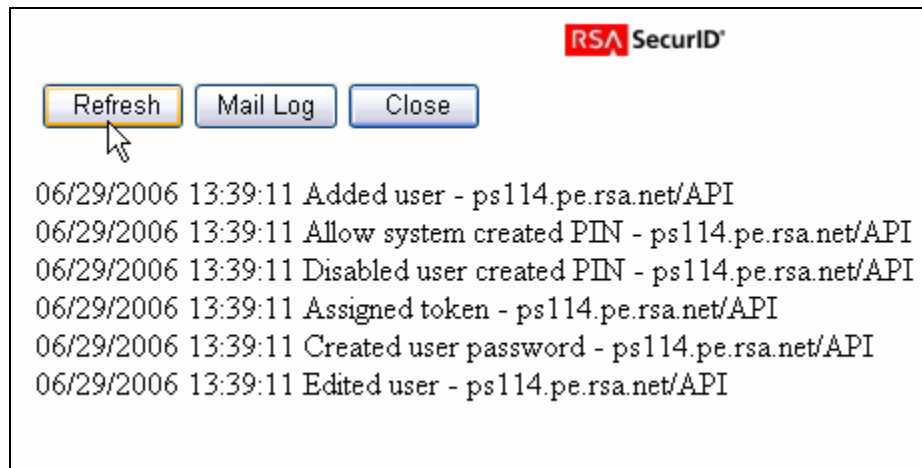
During a test unexpected results from the device or software being tested may occur. The results may have come from messages sent to the device or software from the RSA Authentication Manager Server. The partner may view the logs of the RSA Authentication Manager Server by clicking the button labeled **Get Logs** while in an active test (See picture below). Clicking this button will get the partner the entire logs for the current test only. If the partner requires back logs for the current session, return to the **Main Menu** and click the **Get Logs** button at the bottom of the menu.



**Example of getting logs during a test**

## Refreshing the Log

To get more of the log while testing click the **Refresh** button in the log window. Never close out a log window while running a test, only after a test has completed.



*Clicking the Refresh button retrieves more logs*

**IMPORTANT:** Do not close out the log window while testing. Closing out the window will clear out the logs that were retrieved for that test. If this happens the partner must return to the main menu and reenter the test to reset the logs for that test.

## Restarting Tests

When using the Portal to test an RSA SecurID enabled software application or hardware device the partner may reset a test back to defaults by clicking the **Restart Test** button. This will set the user back into New PIN mode but will not restart the test logs.



*Click Restart Test to reset the test back to defaults*