Microsoft
Active Directory Federation Services (AD FS) 2.0

RSA SecurID Ready Implementation Guide

Last Modified: 3/20/2013

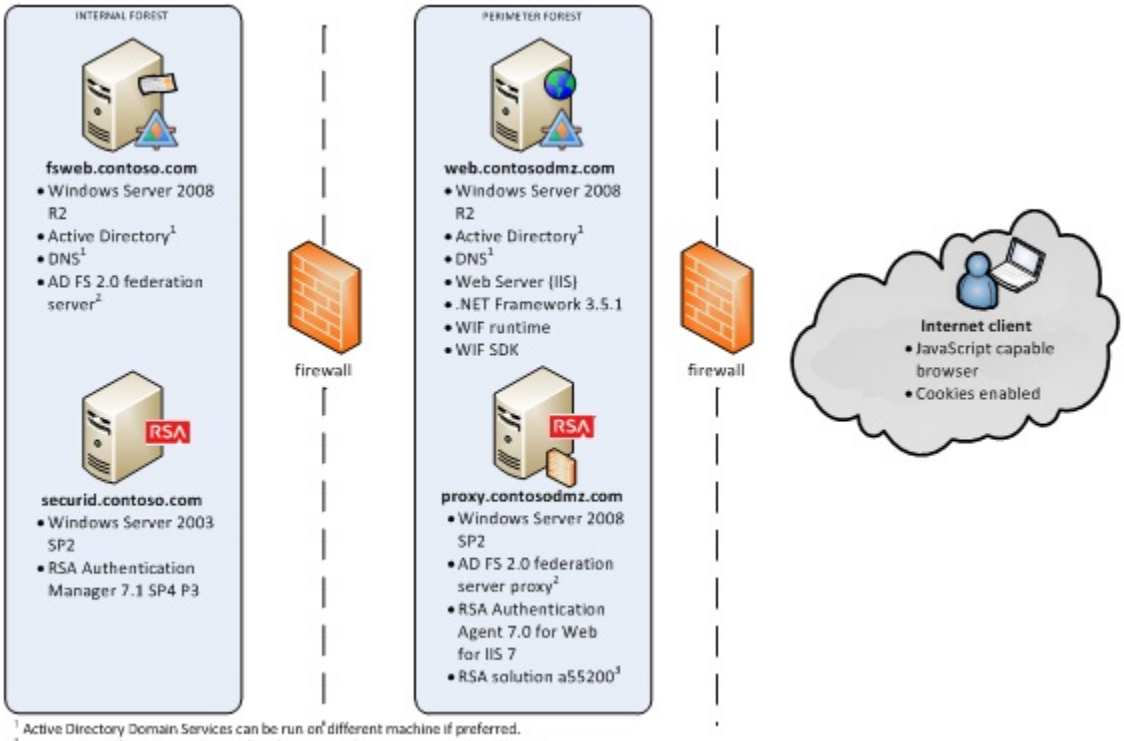
Partner Information

Product Information	
Partner Name	Microsoft
Web Site	www.microsoft.com
Product Name	Active Directory Federation Services
Version & Platform	2.0
Product Description	Microsoft Active Directory Federation Services (AD FS) 2.0 is a security token service (STS) that enables *identity federation*, extending the notion of centralized authentication, authorization and SSO to Web applications and services.

Solution Summary

This document provides an overview of the integration between RSA Authentication Manager and Microsoft Active Directory Federation Services (AD FS) 2.0 enabling two factor authentication for web based applications and services.

RSA Authentication Manager supported features	
AD FS 2.0	
RSA SecurID Authentication via Native RSA SecurID Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	No
On-Demand Authentication via Native SecurID Protocol	Yes
On-Demand Authentication via RADIUS Protocol	No
Risk-Based Authentication	Yes
Risk-Based Authentication with Single Sign-On	No
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	No
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No



[1] Active Directory Domain Services can be run on different machine if preferred.
[3] AD FS 2.0 Install automatically installs other required components not listed here.
[4] Solution iterates RSA web agent build number to 411.

Authentication Agent Configuration

Authentication Agents are records in the RSA Authentication Manager database that contain information about the systems for which RSA SecurID authentication is provided. All RSA SecurID-enabled systems require corresponding Authentication Agents. Authentication Agents are managed using the RSA Security Console.

The following information is required to create an Authentication Agent:

- Hostname
- IP Addresses for network interfaces

Set the Agent Type to "Standard Agent" when adding the Authentication Agent. This setting is used by the RSA Authentication Manager to determine how communication with Microsoft AD FS 2.0 will occur.

RSA SecurID files

RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	%windir%\system32
Node Secret	%windir%\system32
sdstatus.12	%windir%\system32
sdopts.rec	%windir%\system32

Note: The appendix of this document contains more detailed information regarding these files.

Risk-Based Authentication Integration Script

To protect a web-based application with Risk-Based Authentication (RBA), you must download the appropriate integration script from the RSA Security Console, and deploy it to the applications default logon page. The script redirects the user from the web-based application's default logon page to a customized logon page that allows RSA Authentication Manager to authenticate the user with RBA.

The following steps should be taken.

- Download and install the RSA Web Agent for IIS.
- Verify that the most recent RBA integration script template is installed on your Authentication Manager system by comparing the header of the installed integration script template to the header of the downloaded integration script template.
- Install the downloaded integration script template if it is newer than the installed script template, or if the script template for your agent is not installed.

Please refer to RSA documentation for more information on RBA integration scripts.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Microsoft AD FS 2.0 with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

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

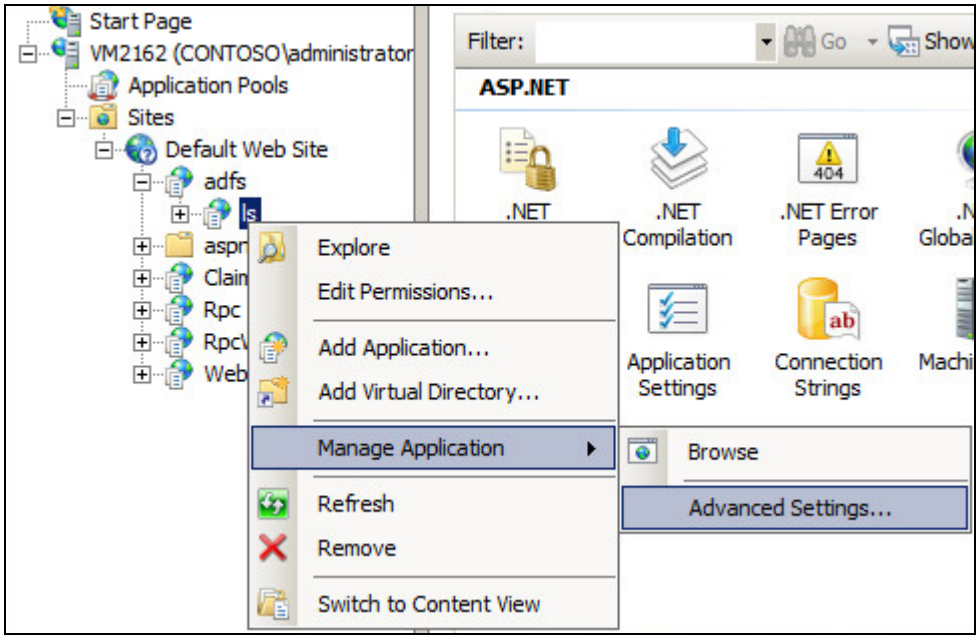
All Microsoft AD FS 2.0 components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

System Configuration

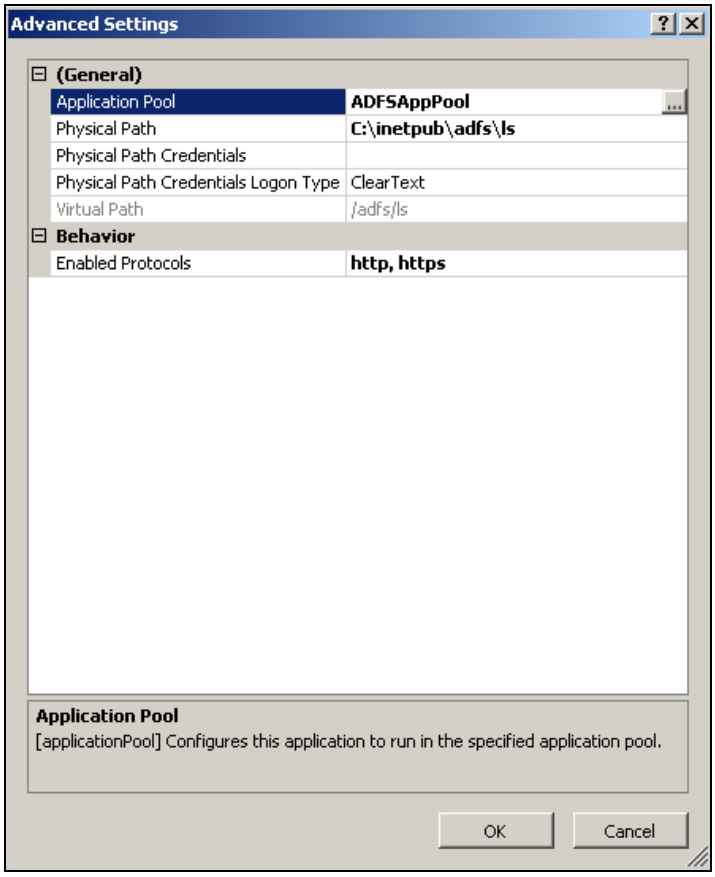
This document is intended to validate and qualify the integration between Microsoft AD FS 2.0, RSA Web Agent and the RSA Authentication Manager 8. Details of the Microsoft portion of the installation and configuration can be found on the Microsoft website.

RSA Web Agent Installation

1. Download and install the RSA Web Agent for IIS.
2. Open Microsoft IIS 7.5 and expand the web site from the Start Page to **adfs/ls**. Right click **ls > Manage Application > Advanced Settings**.

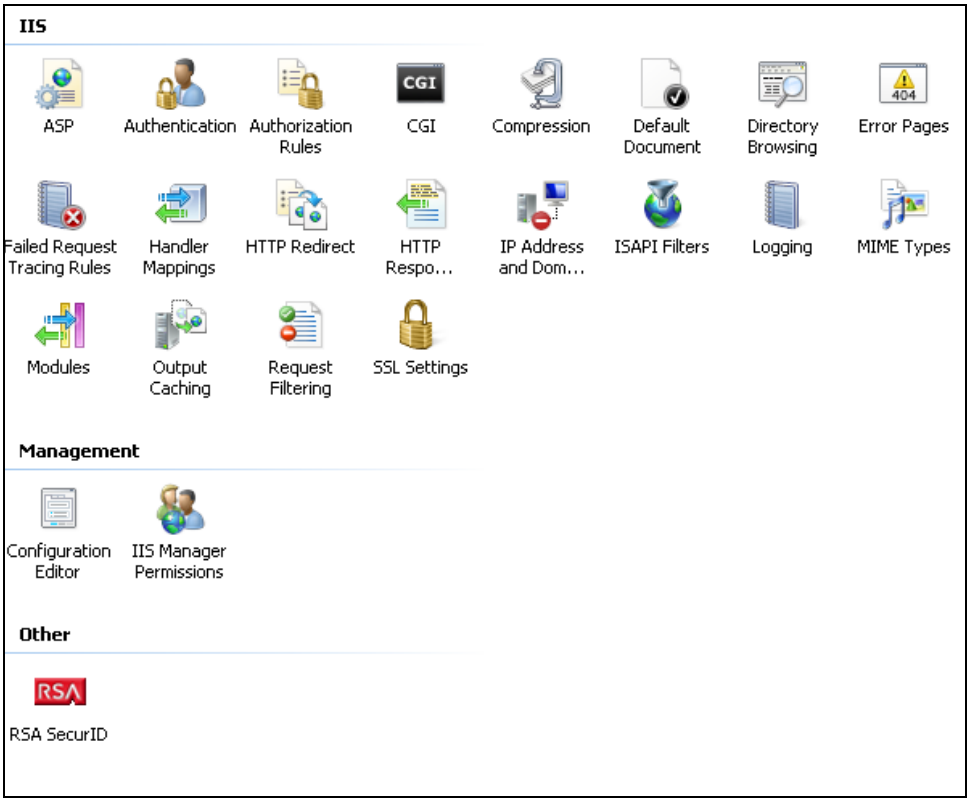


3. Modify the Application Pool properties for this resource setting the value to **ADFSAppPool**.

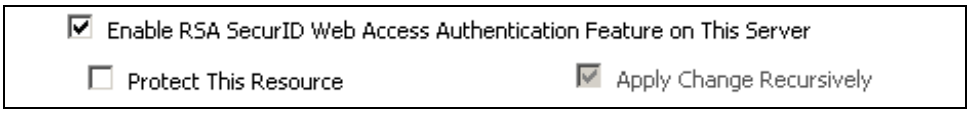


4. Repeat steps 1 & 2 for /ClaimsAwareWebAppWithManagedSTS and /WebID.

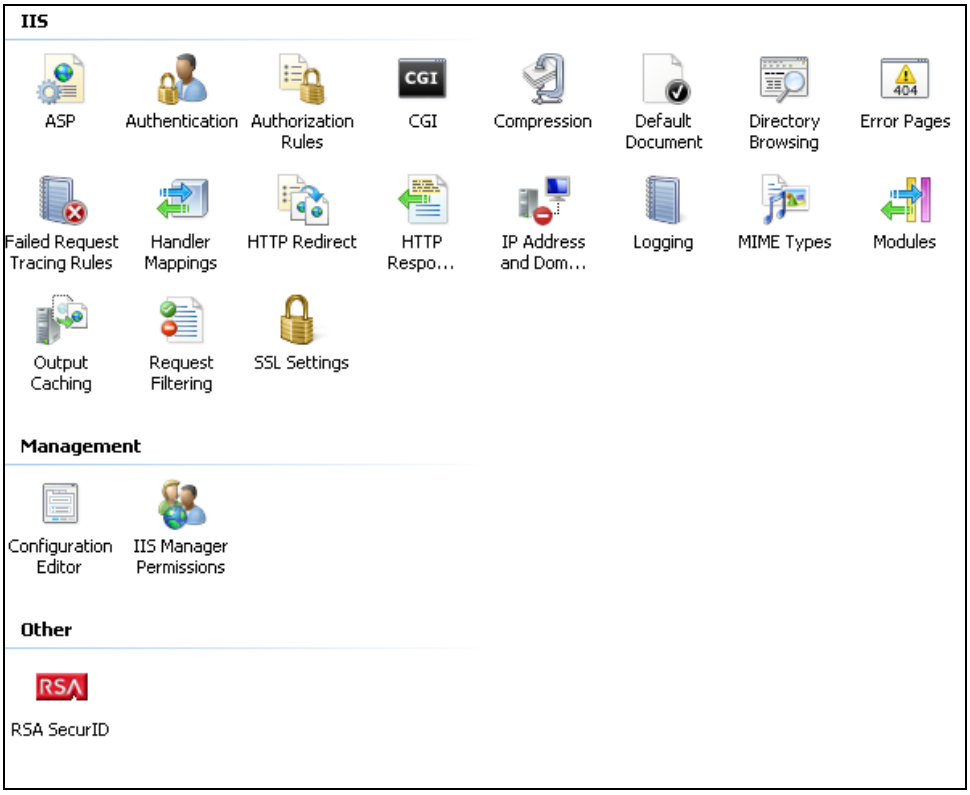
5. Open IIS Manager and select **Default Web Site**. In the center pane scroll down to Other and locate the RSA SecurID icon.



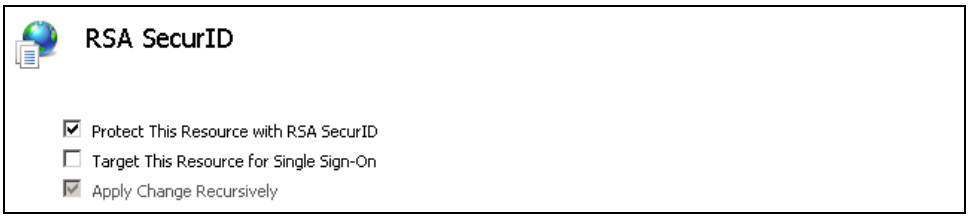
6. Double click the icon to open the RSA SecurID properties page and check **Enable RSA SecurID Web Access Authentication Feature on This Server** to enable the RSA Web Agent.



7. Expand the **adfs** and **ls** folders and in the center pane scroll down to Other and locate the RSA SecurID icon.



8. Double click on the RSA SecurID icon to open the properties page and check **Protect This Resource with RSA SecurID**.



9. Test access to the resource by browsing to the protected resource page.

Configure ADFS for Risk-Based Authentication

1. Using the RSA Security Console, download an RBA integration script for your Agent Host. Be sure to select the script template for RSA Authentication Agent for Web. Save this file as **am_integration.js**.

> **Note: Refer to RSA's documentation for Authentication Manager for more information on generating RBA integration scripts.**

2. Locate C:\Program Files\RSA Security\RSAWebAgent\templates\useridandpasscode.htm and modify the file properties.
3. Right-click **useridandpasscode.htm** and select **Properties** and deselect **Read-only**, and click **OK**.

> **Note: In case of an international locale, the useridandpasscode.htm file is also found in:**
>
> **C:\Program Files\RSA Security\RSAWebAgent\templates\nls\en-securid.**

4. Make a backup copy of the **useridandpasscode.htm** file.
5. Open the am_integration.js and copy the contents below the comments section starting with:

```
function toAbsolutePath(url) {
```

6. Open the useridandpasscode.htm file and paste the text that you copied from am_integration.js immediately before the </script> HTML tag.
7. In the useridandpasscode.htm file locate the <BODY> tag and modify as follows:

- Change the text from:

```
<BODY language="JavaScript" onload="initPage()" onunload="check_cancel()">
```

- To:

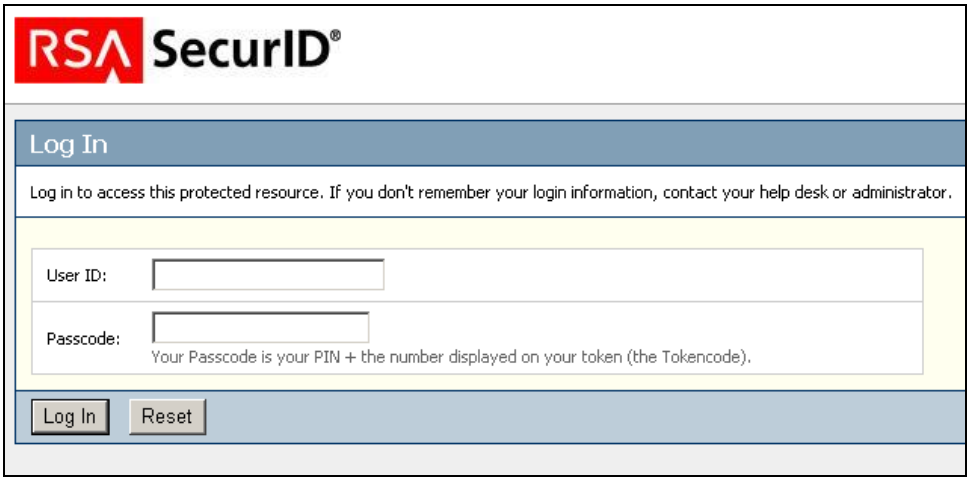
```
<BODY language="JavaScript" onload="redirectToIdP()">
```

> **Note: For the useridandpasscode.htm file, inside en-securid, change the <BODY> tag as change the text from:**
>
> **<body language="JavaScript" onload="authenticate()">**
>
> **To:**
>
> **<BODY language="JavaScript" onload="redirectToIdP()">**

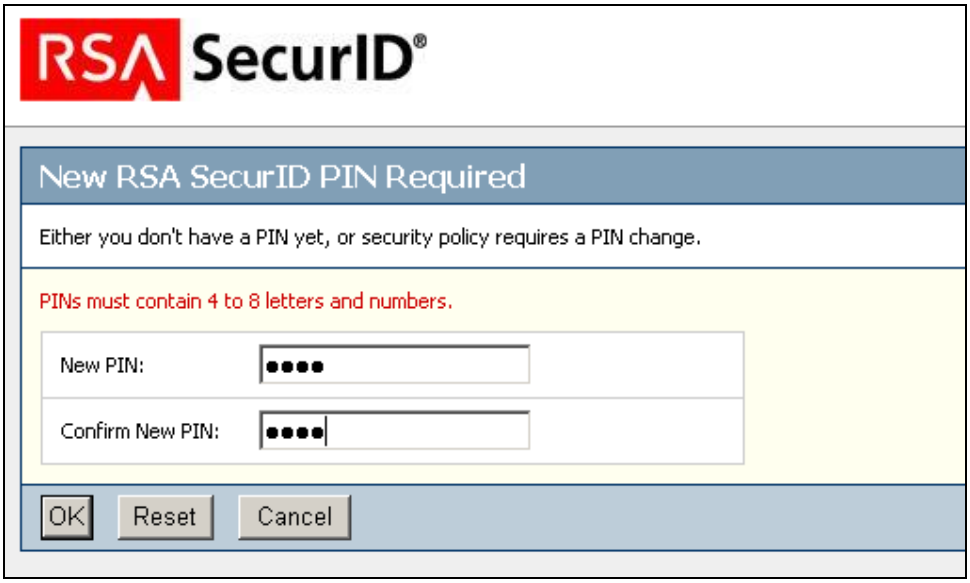
8. Save the useridandpasscode.htm file.
9. Restart the Web server.

RSA SecurID Login Screens

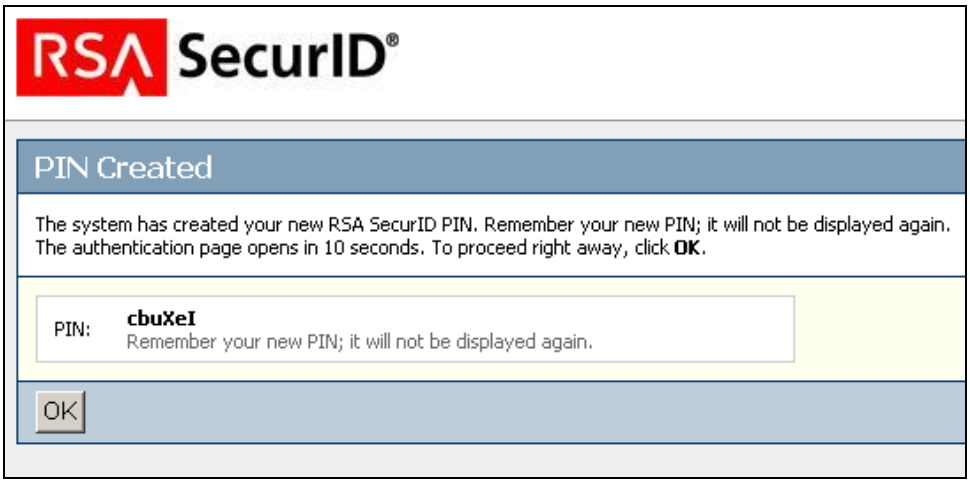
Login screen:



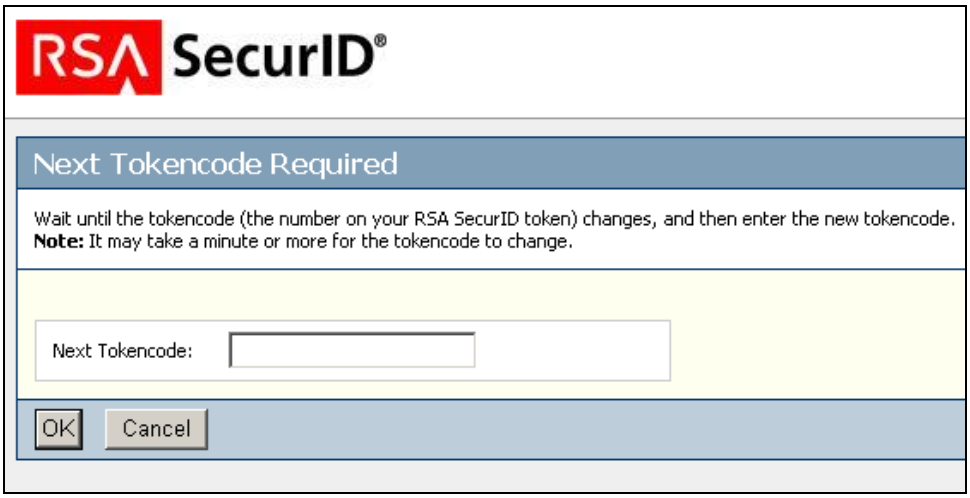
User-defined New PIN:



System-generated New PIN:



Next Tokencode:



Certification Checklist for RSA Authentication Manager

Date Tested: 3/20/2013

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.0	Virtual Appliance
RSA Authentication Web Agent	7.0.2 Build 411	Windows 2008 R2 x64
Windows Identity Foundation SDK	3.5	Windows 2008 R2 x64
Active Directory Federation Services	2.0	Windows 2008 R2 x64

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	✓	Force Authentication After New PIN	N/A
System Generated PIN	✓	System Generated PIN	N/A
User Defined (4-8 Alphanumeric)	✓	User Defined (4-8 Alphanumeric)	N/A
User Defined (5-7 Numeric)	✓	User Defined (5-7 Numeric)	N/A
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	N/A
Deny Alphanumeric PIN	✓	Deny Alphanumeric PIN	N/A
Deny PIN Reuse	✓	Deny PIN Reuse	N/A
Passcode			
16-Digit Passcode	✓	16-Digit Passcode	N/A
4-Digit Fixed Passcode	✓	4-Digit Fixed Passcode	N/A
Next Tokencode Mode			
Next Tokencode Mode	✓	Next Tokencode Mode	N/A
On-Demand Authentication			
On-Demand Authentication	✓	On-Demand Authentication	N/A
On-Demand New PIN	✓	On-Demand New PIN	N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	N/A
No RSA Authentication Manager	✓	No RSA Authentication Manager	N/A

DRP

✓ = Pass ✗ = Fail N/A = Not Applicable to Integration

RSA Risk-Based Authentication Functionality			
RSA Native Protocol		RADIUS Protocol	
Risk-Based Authentication			
Risk-Based Authentication	✓	Risk-Based Authentication	N/A
Risk-Based Authentication with SSO	N/A	Risk-Based Authentication with SSO	N/A

DRP

✓ = Pass ✗ = Fail N/A = Not Applicable to Integration

Appendix

Partner Integration Details	
RSA SecurID API	7.02 build 411
RSA Authentication Agent Type	Web Agent
RSA SecurID User Specification	All Users
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	Yes

Node Secret:

Is located in the c:\windows\system32 folder and can be deleted to clear the node secret on the Agent Host.

sdconf.rec:

The installation of the RSA Authentication Web Agent places the sdconf.rec file in the c:\windows\system32 folder.

sdopts.rec:

Place the sdopts.rec if required in the c:\windows\system32 folder.

sdstatus.12:

Created by the agent and located within the c:\windows\system32 folder.

Agent Tracing:

To enable tracing, registry edits must be made on the Microsoft Windows system on which the RSA ACE/Agent is loaded.

1. Run the registry editor.
2. Under [HKEY_LOCAL_MACHINE] [SOFTWARE] [SDTI] [ACECLIENT] add the following two values, by doing [edit] [add value]:

```
Value Name: TraceLevel
    Data Type:   REG_DWORD
    Click OK
    Select hex in the DWORD Editor
    Data: f
```

3. Click OK.

```
Value Name: TraceDest
    Data Type:   REG_DWORD
    Click OK
    Select hex in the DWORD Editor
    Data: 6
    Click OK
```

> **Note: that the TraceDest parameter is a bit map as follows:**
>
> **"1" --> Windows Event Log**
>
> **"2" --> stdout (screen output)**
>
> **"4" --> <WINDOWS_HOME>\aceclient.log**
>
> **E.g. using the value "6" will direct the debug trace to the aceclient.log file and to the console.**

4. Reboot the Windows machine.

```
Optional parameters are as follows:

    Value Name: TraceFile
    Data Type:   REG_SZ
    Click OK
    Enter the path and filename for the logfile to create (default %SYSTEM
ROOT\aceclient.log)

    Value Name: TraceSize
    Data Type:   REG_DWORD
    Click OK
    Select a format in the DWORD Editor
    Data: Enter the desired file size in Bytes
    Click OK
```

> **Note: Using the SDITRACE_CONSOLE value can cause the service applications to access violate during logoff. Use only for real time debugging situations.**