# Microsoft
## Unified Access Gateway 2010

# RSA SecurID Ready Implementation Guide

Last Modified: March 26, 2013

## Partner Information

| Product Information | |
|---|---|
| **Partner Name** | Microsoft |
| **Web Site** | www.microsoft.com |
| **Product Name** | Unified Access Gateway |
| **Version & Platform** | 4.0.1773 on Windows Server 2008 R2 |
| **Product Description** | Forefront Unified Access Gateway 2010 (UAG) delivers comprehensive, secure remote access to corporate resources for employees, partners, and vendors on both managed and unmanaged PCs and mobile devices. Utilizing a combination of connectivity options, ranging from SSL VPN to DirectAccess, as well as built in configurations and policies, UAG provides centralized and easy management of an organization's complete anywhere access offering. Integrating a deep understanding of the applications published, the state of health of the devices being used to gain access, and the user's identity – UAG enforces granular access controls and policies to deliver comprehensive remote access, ensure security, and reduce management costs and complexity. |

Microsoft Forefront Unified Access Gateway 2010

# Solution Summary

Microsoft Unified Access Gateway (UAG) 2010 provides network administrators with the tools necessary to secure hosted applications and control data streams passed to the host server.

UAG 2010 utilizes RSA SecurID authentication to provide two-factor authentication and a higher level of security to users attempting to access network resources. UAG can also be configured to use RSA Risk-Based Authentication (RBA). When RBA is configured, users attempting access a trunk's login page are redirected to the RSA Secure Logon page. The user authenticates to the system using the username and either a password or a SecurID passcode. If RSA Authentication Manager determines the access attempt to be low-risk, the user is immediately granted access after validating their credentials. If the access attempt is deemed high-risk, the user is challenged with life questions or On-Demand Authentication (ODA) to an out-of-band device to further verify their identity.

| RSA Authentication Manager supported features | |
|---|---|
| **Microsoft Unified Access Gateway 2010** | |
| **RSA SecurID Authentication via Native RSA SecurID Protocol** | Yes |
| **RSA SecurID Authentication via RADIUS Protocol** | Yes |
| **On-Demand Authentication via Native SecurID Protocol** | Yes |
| **On-Demand Authentication via RADIUS Protocol** | Yes |
| **Risk-Based Authentication** | Yes |
| **Risk-Based Authentication with Single Sign-On** | Yes |
| **RSA Authentication Manager Replica Support** | Yes |
| **Secondary RADIUS Server Support** | Yes |
| **RSA SecurID Software Token Automation** | No |
| **RSA SecurID SD800 Token Automation** | No |
| **RSA SecurID Protection of Administrative Interface** | No |

**Note: When configuring KCD for Single Sign-On with Risk-Based Authentication, the usernames in your Authentication Manager Internal Database must match the usernames in your Active Directory domain. This can be managed easily by linking your Active Directory as the Identity Source for your Authentication Manager deployment.**

**Kerberos Constrained Delegation (KCD) is a complex topic. For details on configuring KCD for UAG, refer to Microsoft's documentation.**

**For details on linking an Active Directory Identity Source in Authentication Manager, refer to RSA's administration guide.**

# 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 Unified Access Gateway will occur.

A RADIUS client that corresponds to the Authentication Agent must be created in the RSA Authentication Manager in order for Unified Access Gateway to communicate with RSA Authentication Manager. RADIUS clients are managed using the RSA Security Console.

The following information is required to create a RADIUS client:

- Hostname
- IP Addresses for network interfaces
- RADIUS Secret

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

Please refer to the appropriate RSA documentation for additional information about creating, modifying and managing Authentication Agents and RADIUS clients.

# RSA SecurID files

| RSA SecurID Authentication Files | |
|---|---|
| **Files** | **Location** |
| sdconf.rec | %SystemRoot%\System32 |
| Node Secret | %SystemRoot%\System32 |
| sdstatus.12 | %SystemRoot%\System32 |
| sdopts.rec | %SystemRoot%\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 generate an integration script using 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 prior to generating the integration script.

- Download the integration script template for the Unified Access Gateway from the following link: **https://sftp.rsa.com/human.aspx?Username=partner&password=rsasecured&arg01=708679776&arg12=downloaddirect&transaction=signon&quiet=true**
- 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 Unified Access Gateway 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 Unified Access Gateway components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

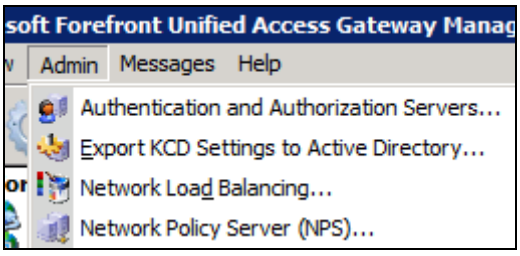
## *Overview*

Configuring Unified Access Gateway to utilize RSA SecurID authentication is performed over several steps. First, you must configure your RSA Authentication Manager instance as an authentication server in UAG using either the native SecurID protocol or RADIUS. Second, you must configure one or more trunks to use Authentication Manager as the authentication server for users accessing the trunk. Finally, if Risk-Based Authentication is in scope for your deployment, you must customize the trunk's logon page to enable RBA. Optionally, you may wish to take advantage of Kerberos Constrained Delegation to provide Single Sign-On to users accessing protected resources. This requires additional configuration, and abbreviated instructions are provided later in this guide.

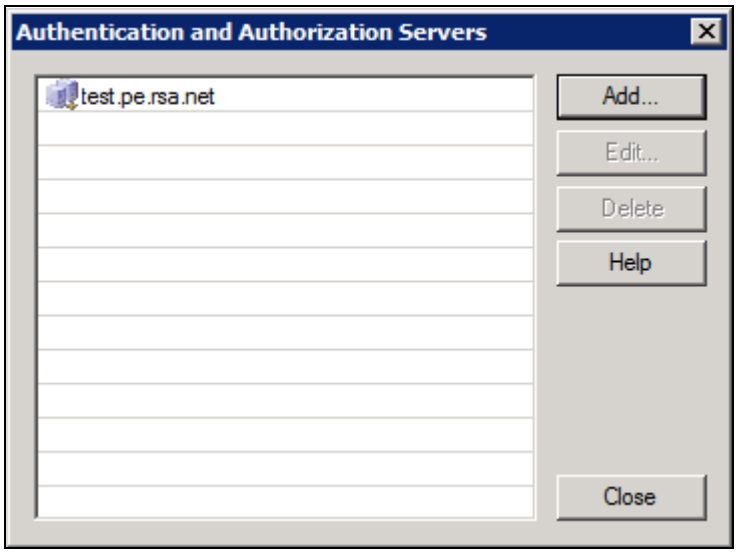
### Configure Authentication Manager as an Authentication Server

> **Note: By default, the UAG array does not contain a firewall access rule to allow the SecurID protocol. You must create this rule using the Forefront TMG Management Console, or this step will fail. For information on firewall access rules, refer to Microsoft's documentation for Threat Management Gateway 2010.**

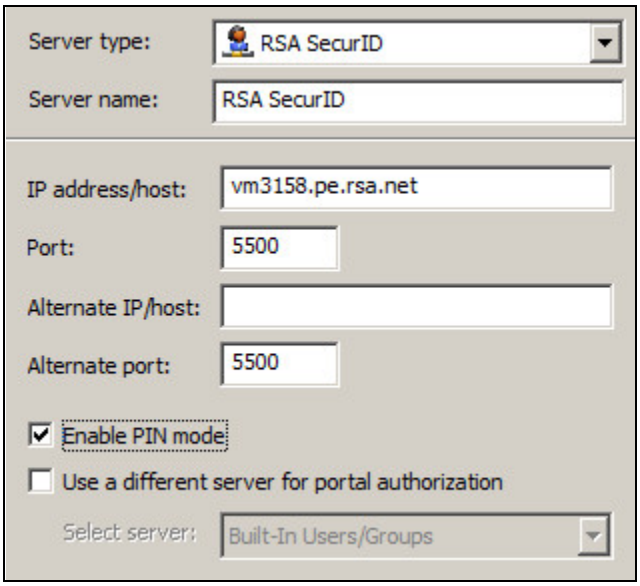
1. Prior to starting, copy the **sdconf.rec** file obtained from your Authentication Manager instance to **%SystemRoot%\system32** on your UAG server.
2. In the Forefront UAG Management console, click the **Admin** menu and select **Authentication and Authorization Servers…**



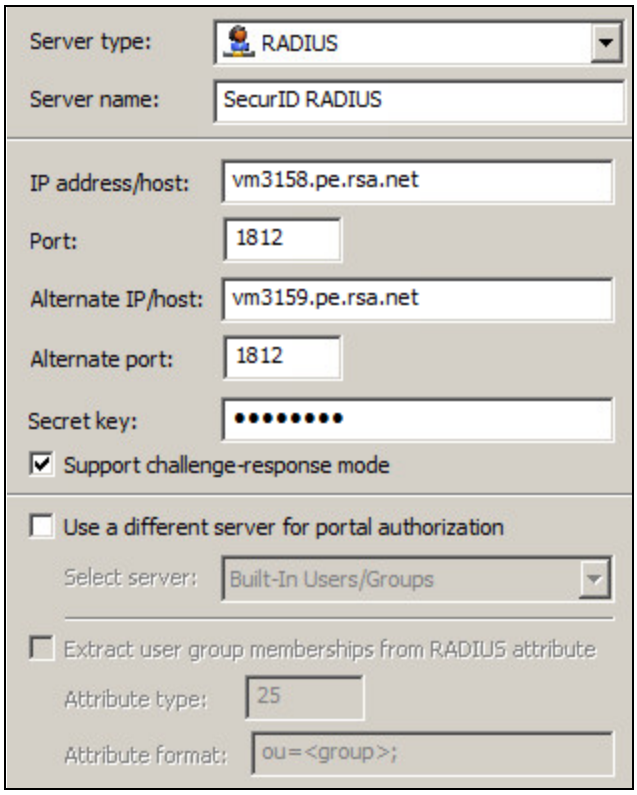
3. Your existing authentication servers are displayed in a list. Click the **Add…** button to add a new authentication server set.



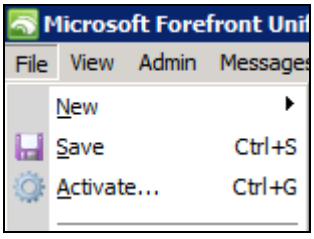

4. Select **RSA SecurID** as the server type and give a name to the configuration. Provide the hostname or IP address of your Authentication Manager primary instance. You do not need to provide information for the replica instance—this information will be read from the sdconf.rec file you provided. Ensure that **Enable PIN mode** is checked. Click **OK** to save the configuration.



5. To configure Authentication Manager as an authentication server using **RADIUS**, the process is identical, except that you choose **RADIUS** as the server type. Specify the **hostname** or **IP address** of your Authentication Manager primary and replica instance, if applicable. Enter **1812** as the **Port** for both servers. Supply a **secret key**. This key must match what was configured in Authentication Manager when the RADIUS client was created. Finally, ensure that **Support challenge-response mode** is **checked**. Click **OK** to save the server configuration.

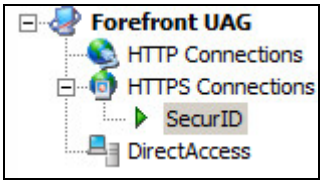



6. Click the **File** menu and select **Activate…** to activate your UAG configuration. This commits the changes made to the configuration storage and synchronizes the changes to any UAG array members. The activation process may take several minutes to complete.

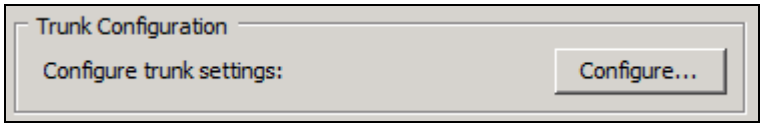


## Configure Trunks for SecurID Authentication

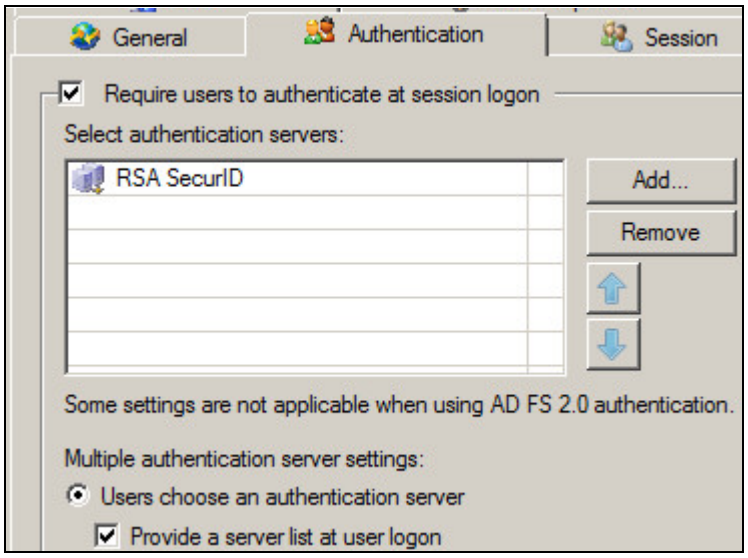
1. Using the Forefront UAG Management console, select the trunk for which you want to configure SecurID Authentication.



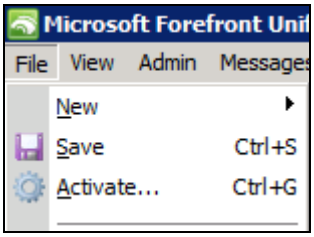

2. In the right panel that appears, locate the **Trunk Configuration** section and click the **Configure…** button.




3. On the **Authentication** tab, remove your old authentication server setting (if any) and add the SecurID or RADIUS authentication servers you configured in the previous section.

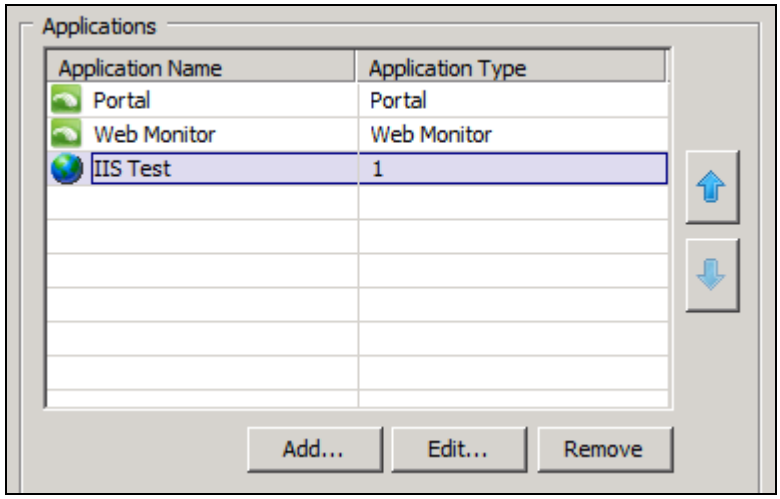



4. Click **OK** to save the trunk configuration.
5. Click the **File** menu and select **Activate…** to activate your UAG configuration. This commits the changes made to the configuration storage and synchronizes the changes to any UAG array members. This process may take several minutes to complete. Once activated, users accessing the UAG portal via this trunk will be prompted to authenticate using their SecurID usernames and passcodes.

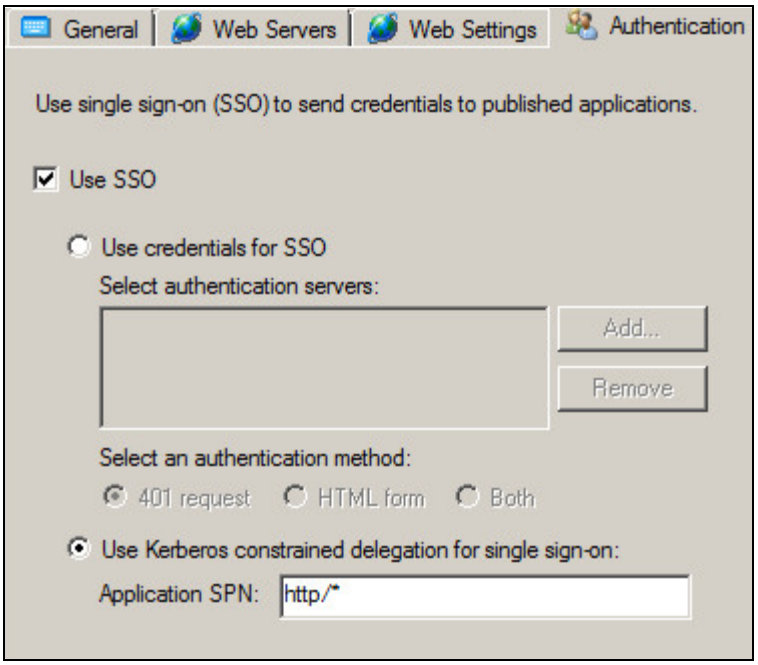


## Configure UAG for Kerberos Constrained Delegation (KCD)

1. Locate the resource for which you would like to configure KCD. Click the **Edit…** button.




2. On the **Authentication** tab, click the checkbox for **Use SSO** and select the radio button for **Use Kerberos constrained delegation for single sign-on**. Leave the default SPN unless you configured a custom SPN, such as in the case of a load-balanced scenario.




3. Activate your UAG configuration to apply these changes.
4. You must now configure the Active Directory computer account as explained below. Note that The UAG Management Console provides a feature that will generate an export file that can be used to automatically import these changes to Active Directory. To use this feature, open the **Admin** menu and select **Export KCD Settings to Active Directory…**

## Configure Constrained Delegation on Active Directory

This section contains abbreviated instructions for configuring Constrained Delegation on Active Directory and Web Application Servers. Please refer to Microsoft's documentation for detailed configuration instructions for specific products and versions.

1. Within the UAG Computer Account Properties in Active Directory, click the Delegation tab and configure the following options.
   - Select the **Trust this computer for delegations to the specified services only** option.
   - Select the **Used and authentication protocol** option.
   - Add the **Service Type** and **Computer Account** name for the system which will host the delegated service and click **OK**.
2. Configure the Web Application Server.
   - From the IIS Manager, open the properties for which website you want constrained delegation enabled.
   - Click **Edit** from the **Directory Security** tab.
   - Clear the checkbox for **Enable anonymous access**.
   - Mark the checkbox for Integrated Windows authentication.

## Customize Trunks for Risk-Based Authentication

**! Important: Microsoft UAG is a powerful product that supports many different configurations. This guide illustrates how to customize the default UAG portal for RBA. Additional customizations may be needed for advanced UAG deployments. You should fully understand how UAG's CustomUpdate mechanism works and have a backup of your configuration before attempting these customizations.**

1. Using the RSA Security Console, download an RBA integration script for your Agent Host. Be sure to select the script template for Microsoft Unified Access Gateway 2010. Save this file as **am_integration.js**.

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

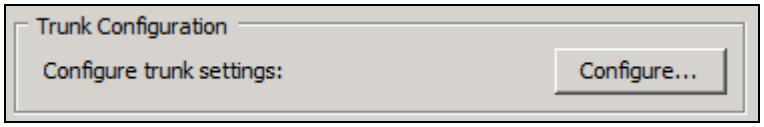
2. On the UAG server, copy **am_integration.js** to ***[UAG_INSTALL]*\von\InternalSite\scripts\CustomUpdate**. *[UAG_INSTALL]* is the directory where Microsoft UAG was originally installed.
3. On the UAG server, copy **bottomText.inc** from ***[UAG_INSTALL]*\von\InternalSite\samples** to ***[UAG_INSTALL]*\von\InternalSite\inc\CustomUpdate**.
4. Edit the version of **bottomText.inc** in the CustomUpdate folder to include the following customization. This code should be inserted at the very top of the include file. Be sure to **save** this file after editing it.

```
<%'include file for bottom text%>
<script src="/InternalSite/Scripts/CustomUpdate/am_integration.js"
type="text/javascript"></script>
<script type="text/javascript">
	if (document.getElementById('form1'))
	{
		if (get_cookie("dwLastDetectionTimestamp") == "")
		{
			window.onload = redirectToIdP;
		}
	}
</script>
```

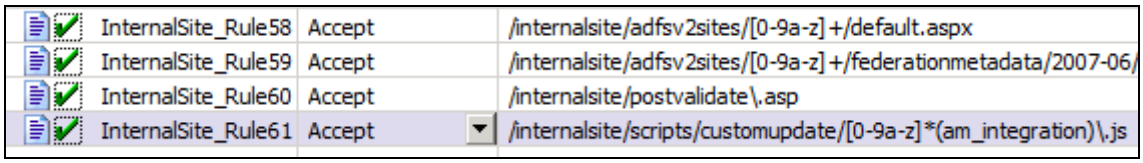
5. This customization will cause the RBA Integration script to be invoked whenever the InternalSite's login page is reached.

   If this customization is to apply to all trunks, leave the file as is. If the customization is to apply to specific trunks only, rename the file with the convention *<Trunk_Name><Secure*(0=no/1=yes*)><Original_Filename.ext>*. For example, if the customization were only to apply to the trunk in this example, the file should be renamed to **SecurID1bottomText.inc**. This would cause the customized include file to be loaded only when the 'SecurID' trunk is accessed.

6. Most UAG configurations will not allow am_integration.js to be loaded by default. In order to allow this, a URL rule must be created in the trunk configurations for which this customization will apply. In the Forefront UAG Management console, access the advanced trunk properties for your trunk by clicking the trunk, and then locating the **Trunk Configuration** section and clicking the **Configure…** button.




7. On the **URL Set** tab, a list of URL rules is displayed. Click the **Add Primary** button to create a new rule.

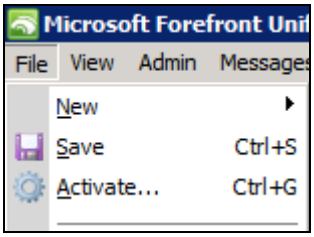



8. Supply the following information for the new rule:

   - **Name:** The name of the rule matters because it determines which application it governs. Name your rule with the convention **InternalSite_RuleX**, where X is a number.
   - **Action:** Determines if a matching URL is accepted or rejected. Set this to **Accept**.
   - **URL:** This is a regular expression that specifies a pattern of URLs that you want to match. Specify a pattern of **/internalsite/scripts/customupdate/am_integration\.js**, making sure to include the backslash in the file name.
   - **Parameters:** This option determines whether parameters passed as part of the URL are rejected, handled, or ignored. Set this option to **Ignore**.
   - **Note (optional):** Optional information about the rule.
   - **Methods:** specifies which HTTP methods are allowed for the URL pattern. Set this option to **GET**.

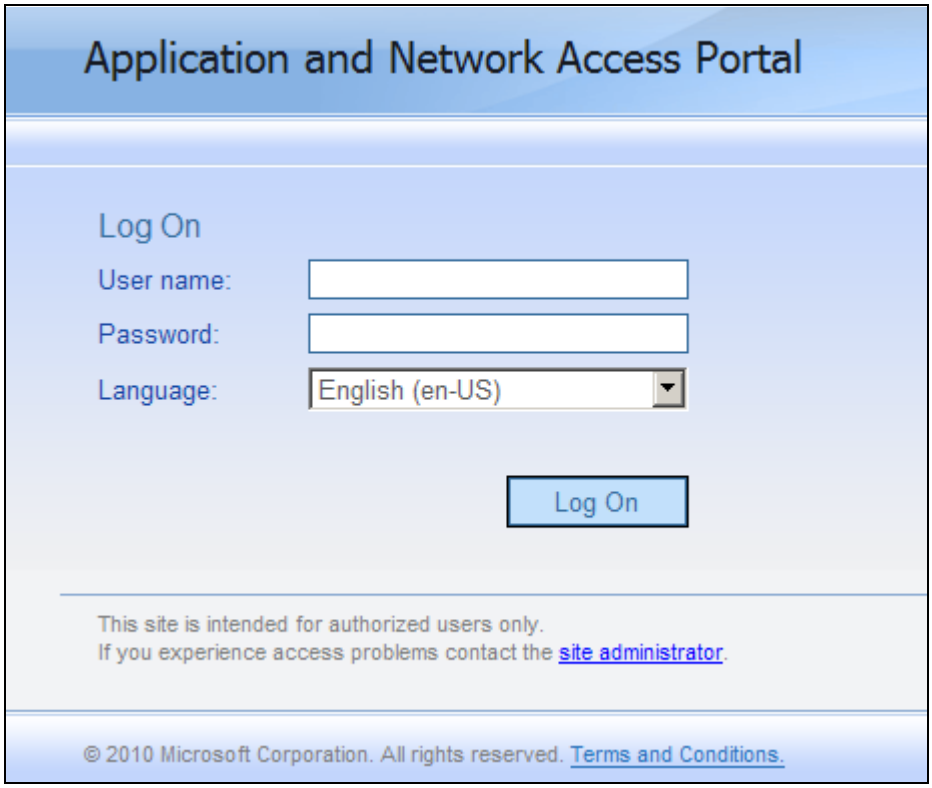
> **Note: Not all UAG configurations will require you to configure this rule. The default URL set is determined based on which application type you selected when you created the trunk. Some types allow all URLs by default, while others are more locked down for security. If in doubt, create this rule. If, after configuring RBA, users are not being redirected to the RSA Secure Logon page, check the UAG web monitor for Security events that indicate am_integration.js is being blocked from loading. This will indicate the necessary rule is missing or incorrectly configured.**
>
> **Refer to Microsoft's documentation for complete details on URL rules.**

9. Click the **File** menu and select **Activate…** to activate your UAG configuration. This commits the changes made to the configuration storage and synchronizes the changes to any UAG array members. This process may take several minutes to complete. Once activated, users accessing the UAG portal via this trunk will authenticate using Risk-Based Authentication.

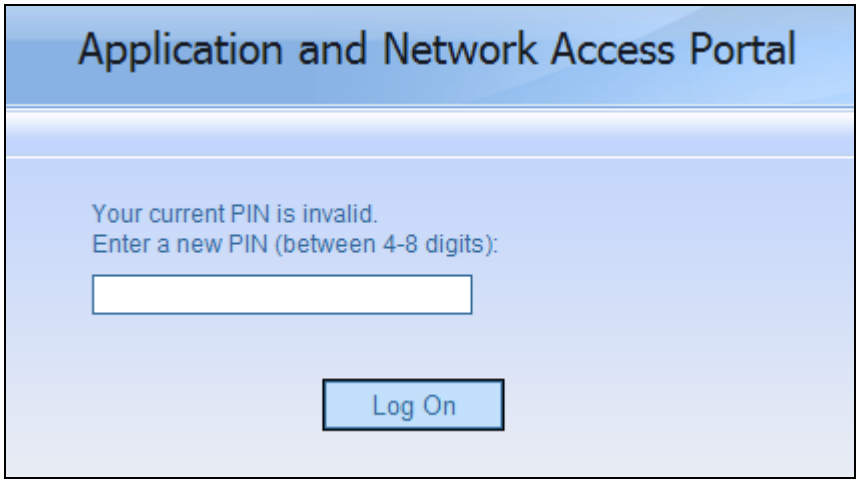


## RSA SecurID Login Screens

Login screen:

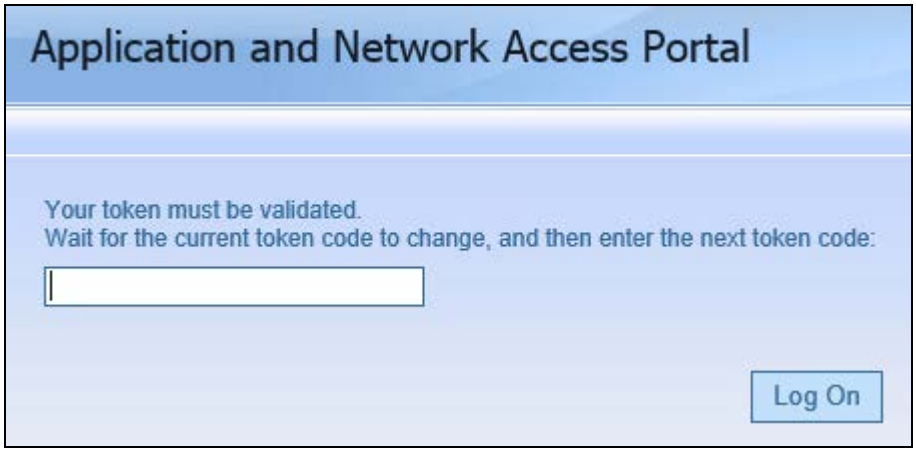



User-defined New PIN:



System-generated New PIN:


Next Tokencode:



# Certification Checklist for RSA Authentication Manager

Date Tested: March 26, 2013

| Certification Environment | | |
|---|---|---|
| **Product Name** | **Version Information** | **Operating System** |
| **RSA Authentication Manager** | 8.0 | Virtual Appliance |
| **Microsoft UAG 2010** | 4.0.1773.10100 | Windows 2008 R2 |

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

MRQ ✓ = 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 | ✓ |
| Risk-Based Authentication with SSO | ✓ | Risk-Based Authentication with SSO | ✓ |

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

# Known Issues

## Incorrect New PIN Prompts

When in new PIN mode, the UAG portal may not display the correct PIN prompt based on the user's PIN policy. For example, the test environment consistently displayed PIN settings of 4 to 8 digits even when the PIN policy was adjusted to allow 5 to 7 digits. This is mainly cosmetic—the Authentication Manager instance will accept or reject a PIN based on the user's policy settings regardless of the PIN prompt UAG has supplied.

## Session Persistence with Multi-Tab Browsers

When configured for Risk-Based Authentication, if a user logs out of their UAG session and attempts to log in again, the browser may not redirect them to the RSA Secure Logon Page. Instead, the user is presented with the normal On-Demand Authentication page for the UAG Portal. If this occurs, close all browser tabs and restart your browser. This behavior occurs due to a difference in behavior between browsers when handling expired cookies.

The RBA integration script for UAG looks for the absence of the **dwLastDetectionTimestamp** cookie to determine if it needs to redirect the user to the RSA Secure Logon page. This cookie expires with the UAG portal session, but some browsers do not remove the cookie until the browser is restarted.

# Appendix

| Partner Integration Details | |
|---|---|
| **RSA SecurID API** | 6.4.025 |
| **RSA Authentication Agent Type** | Standard Agent |
| **RSA SecurID User Specification** | Designated Users |
| **Display RSA Server Info** | No |
| **Perform Test Authentication** | No |
| **Agent Tracing** | Yes |
| | |

## *Node Secret:*

The node secret is stored in **%SystemRoot%\System32** on the UAG server. To clear the node secret from the UAG server, delete the **securid** file from this directory.

## *sdconf.rec*

The node secret is stored in **%SystemRoot%\System32** on the UAG server. If your AM configuration changes, download a new copy of this file from the RSA Security Console and replace this file.

## *Agent Tracing:*

Using Regedit locate the HKEY_LOCAL_MACHINE\Software\SDTI\ACECLIENT key and create 2 DWORD values: **tracelevel** and **tracedest.**

The value tracelevel specifies the verbosity and the categories of messages produced by the code. The value tracedest controls the output destination of the trace messages.

**tracedest** VALUES:

```
SDITRACE_EVENT_LOG  0x00000001   // messages to event log
SDITRACE_CONSOLE    0x00000002   // messages to console
SDITRACE_LOGFILE    0x00000004   // messages to logfile (aceclient.log)
SDITRACE_DEBUGGER   0x00000008   // messages to debugger output
SDITRACE_NOFILELINE 0x80000000   // no file and line information
```

The SDITRACE_NOFILELINE value can be combined with any of the other values to stop the display of file and line number information. The logfile is **%SystemRoot%\ACECLIENT.LOG** but can be changed by creating a **REG_SZ:tracefile** value and specifying the file pathname.

**tracelevel** VALUES:

```
SDITRACEING_OFF     0x000000000  // All messages off
SDITRACEING_ON      0x000000001  // All messages marked with this level on
SDITRACEING_ENTRY   0x000000002  // All entrypoints use this
SDITRACEING_EXIT    0x000000004  // All function returns use this
SDITRACEING_FLOW    0x000000008  // All logic flow control use this (ifs)
SDITRACEING_GRP1    0x000000010  // Old SDITRACE macros use this (see dbglib.h)
```

The hex value 0xF gives the complete set of tracing. The values can be combined to produce multiple sets of trace messages.

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