Citrix Systems, Inc.
Web Interface

RSA SecurID Ready Implementation Guide

Last Modified: July 22, 2014

Partner Information

Product Information	
Partner Name	Citrix Systems, Inc.
Web Site	www.citrix.com
Product Name	Web Interface
Version & Platform	5.4 for Windows
Product Description	Citrix Web Interface provides users with access to Citrix XenApp or XenDesktop Server applications and content through a standard Web browser or through the Program Neighborhood Agent, and allows you to configure sites for Citrix Conferencing Manager Guest Attendee log in. The Web Interface employs Java and .NET technology executed on a Web server to dynamically create an HTML depiction of server farms for Citrix XenApp or XenDesktop sites. Users are presented with all the applications published in the server farm(s) you have made available. You can create standalone Web sites for application access or Web sites that can be integrated into your corporate portal.

Solution Summary

Citrix Web Interface integrates with RSA Authentication Manager for both SecurID and Risk-Based Authentication (ODA).

When RSA SecurID has been configured, Web Interface users will be challenged for their username, windows password and SecurID passcode. Web Interface also supports the RSA Password Integration feature to improve the end user experience. When enabled, the user will only be prompted to enter their password the first time and when it has changed. For subsequent logins, the users will only be prompted for their username and SecurID passcode. The password will be retrieved from the RSA Authentication Manager automatically.

When Risk-Based Authentication has been configured, Web Interface users will be redirected to the RSA Authentication Manager's Secure Logon page for authentication. If RSA Authentication Manager determines that the login is low risk, the user will be logged into the Citrix Web Interface, and published applications will be enumerated. If RSA Authentication Manager determines that a login is high risk, the user can be challenged with life questions or On-Demand Authentication to further authenticate the user.

RSA Authentication Manager supported features	
Citrix Web Interface 5.4	
RSA SecurID Authentication via Native RSA SecurID UDP Protocol	Yes
RSA SecurID Authentication via Native RSA SecurID TCP Protocol	No
RSA SecurID Authentication via RADIUS Protocol	No
RSA SecurID Authentication via IPv6	No
On-Demand Authentication via Native SecurID UDP Protocol	Yes
On-Demand Authentication via Native SecurID TCP Protocol	No
On-Demand Authentication via RADIUS Protocol	No
Risk-Based Authentication	Yes
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

Agent Host Configuration

To facilitate communication between Citrix Web Interface and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies Citrix Interface and contains information about communication and encryption.

RSA Authentication Manager 8.0 introduced a new TCP-based authentication protocol and corresponding agent API. RSA Authentication Manager 8.0 and newer also maintains support for the existing UDP-based authentication protocol and agents. The agent host records for TCP and UDP agents are configured similarly, but there are some important differences.

Include the following information when configuring a UDP-based agent host record.

- Hostname
- IP addresses for network interfaces

> **Note: The UDP-based authentication agent's hostname must resolve to the IP address specified.**

Include the following information when configuring a TCP-based agent host record.

- RSA agent name (in the hostname field)

> **Note: The RSA agent name is specified in the rsa_api.properties file.**

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 Citrix Web Interface will occur.

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 Citrix Web Interface from the following link: **https://sftp.rsa.com/human.aspx?Username=partner&password=rsasecured&arg01=688816961&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.

Note: Risk-Based Authentication is not compatible with IPv6 agents.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Citrix Web Interface 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 Citrix Web Interface components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Install RSA Authentication Agent for Windows

Citrix Web Interface relies on certain files contained in the RSA Authentication Agent for Windows to enable RSA SecurID functionality. Because of this, the RSA Authentication Agent (Local Authentication Client) must be installed prior to Citrix Web Interface.

Depending on which version of Windows and which RSA Authentication Agent you are using, some additional configuration may be necessary. These steps should also be performed prior to installing Web Interface. Refer to Citrix KB article CTX125097 for more information.

For Windows Server 2008 R2 and RSA Agent 7.x:

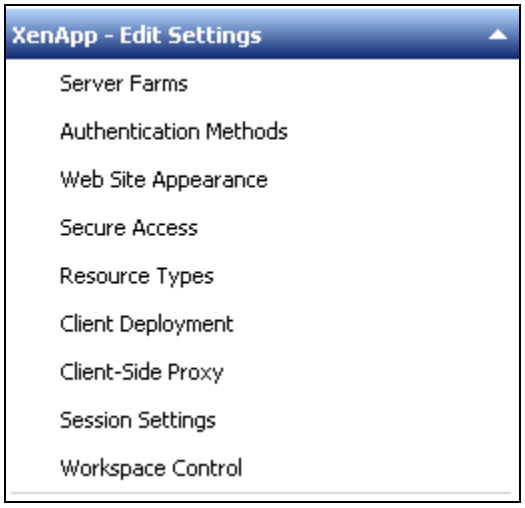
1. Perform a test authentication in the RSA agent to generate the node secret (securid) file.
2. Copy the following files from C:\program files\common files\rsa shared to C:\windows\system32
    - sdconf.rec
    - securid
    - sdstatus.12
    - aceclnt.dll
    - sdmsg.dll
3. Open the IIS Management MMC snap-in and navigate to the CitrixWebInterface Application Pool.
4. Open the advanced settings and set “Enable 32-Bit Applications” to False.

A regular installation of Citrix Web Interface can be performed after the RSA Authentication Agent has been installed.

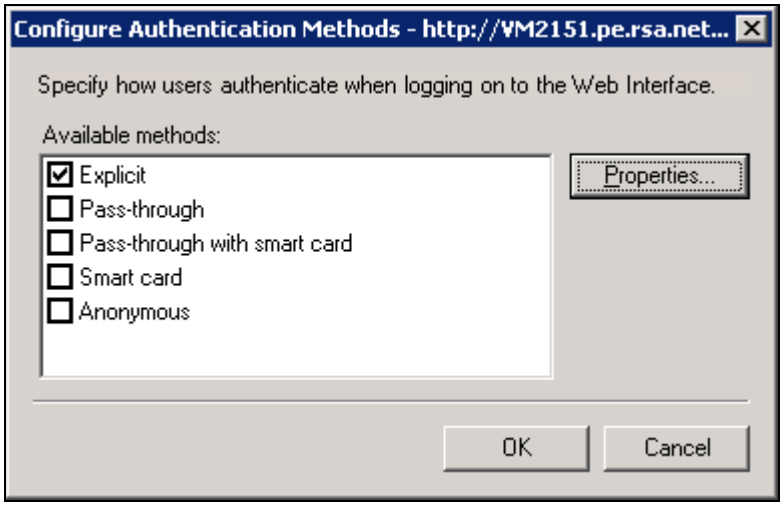
Configure Web Interface for RSA SecurID Authentication

Perform the following steps:

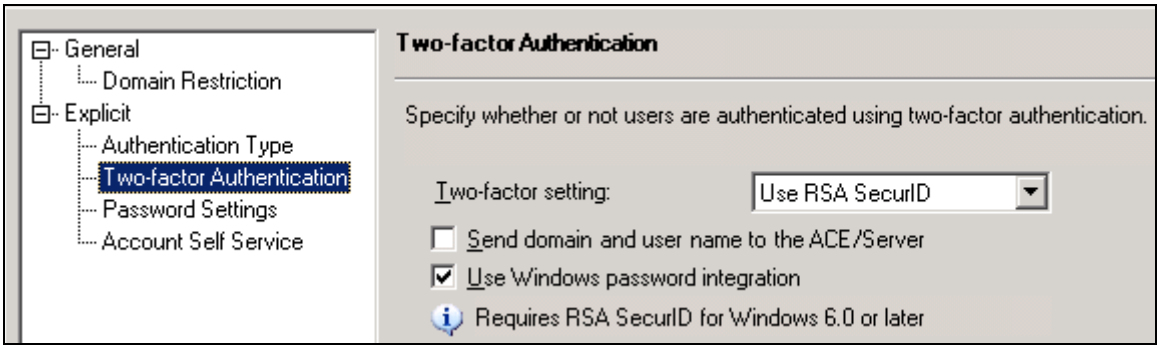
1. From the Web Interface configuration settings, select **Configure Authentication Methods**.



2. Under **Available methods**, check **Explicit**, click **Properties**.



3. Under the **Explicit** heading, highlight **Two-factor Authentication**.



4. Select the **Send domain and user name to the ACE/Server** box if you have user accounts in different Domains and need to pass your usernames to the Authentication Manager server in the DOMAIN\USERNAME format.
5. If you select the **Use Windows password integration box**, the Citrix Web Interface server will only prompt for a username and PASSCODE after the first successful authentication. If the user's Domain password is available from the RSA Authentication Manager, then it will be retrieved by the Web Interface server. If the password is not available or is invalid, the Web Interface server will prompt to store the password on behalf of the user to allow for future logins with just a PASSCODE.

> **Note: If you are unable to log on to the Web Interface using RSA Windows Agent 7.x, additional configuration may be necessary. Please refer to Citrix Document ID: CTX125097.**

Citrix Web Interface is now configured for RSA SecurID Authentication.

Configure Web Interface for Risk-Based Authentication

The Risk-Based Authentication (RBA) functionality is dependent upon Web Interface acting as an RSA SecurID authentication agent. You must first complete the RSA SecurID configuration including Windows Password Integration in the "Configure Web Interface for RSA SecurID" section of this guide before proceeding.

1. Download the RBA integration script (am_integration.js) from the RSA Authentication Manager Security Console.

> **Important: Perform step 2 only if you are integrating with Citrix Web Interface 5.4**

2. If you are using Citrix Web Interface 5.4, you must modify the RBA Integration script file (am_integration.js). Complete the following steps to make the necessary changes.
    1. Open the am_integration.js file with a text editor.
    2. Search for the string "changeLoginBtnColor(false);" and delete that line of code.
    3. Exit the text editor saving your change.

Citrix Web Interface can be configured for RBA so that either the administrator sets the domain during RBA configuration or so that the end user enters the domain during the logon process.

Administrator-specified domain

Configure Citrix Web Interface for RBA using an Administrator-specified domain by completing the steps below.

Note: All directories are in relation to the website directory for which you are enabling for RBA. The default website is c:\inetpub\wwwroot\citrix\xenapp\

1. Copy the RBA Integration script into the following directory on the Citrix Web Interface site:

```
auth\clientscripts\
```

2. Add the following line of code:

```
<!--#include file="am_integration.js"-->
```

   To:

```
auth\clientscripts\loginClientScript.ascx
```

3. Add the following line of code, replacing <domain> with your domain name:

```
<script type="text/javascript">
       var isRadius = false;
       var preserve_password_flag = true;
       var domain = "<domain>";
       initRBASupport(isRadius);
</script>
<script type="text/javascript">window.onload=redirectToIdP;</script>
```

   To the bottom of:

```
auth\login.aspx
```

Citrix Web Interface is now configured for Risk-Based Authentication.

User-specified domain

Configure Citrix Web Interface for RBA using a domain specified by the end user by completing the following steps:

1. Copy the RBA Integration script into the following directory on the Citrix Web Interface site:

   ```
   auth\clientscripts\
   ```

2. Add the following line of code:

   ```
   <!--#include file="am_integration.js"-->
   ```

   To:

   ```
   auth\clientscripts\loginClientScript.ascx
   ```

3. Add the following line of code:

   ```
   <script type="text/javascript">
          var isRadius = false;
          var preserve_password_flag = true;
          var domain = "";
          initRBASupport(isRadius);
   </script>
   ```

   To the bottom of:

   ```
   auth\login.aspx
   ```

4. For Citrix Web Interface 5.3 or earlier, open the following file:

   ```
   app_data\include\loginMainForm.inc
   ```

   For Citrix Web Interface 5.4, open the following file:

   ```
   app_data\include\loginMainFormFoot.inc
   ```

   Search the file for the following string:

   ```
   href=”javascript:submitForm()”
   ```

   And replace it with:

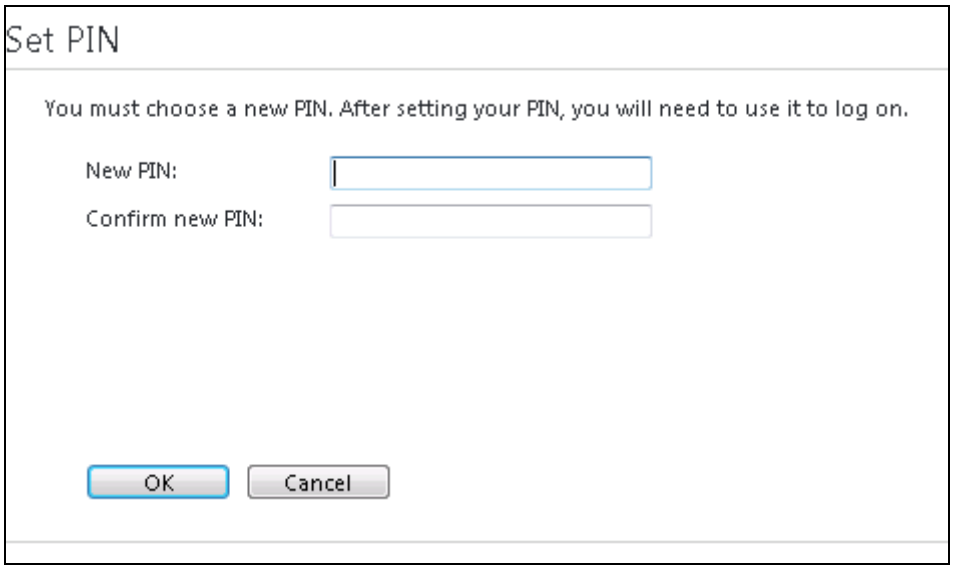
   ```
   href="javascript:redirectToIdP()"
   ```

Citrix Web Interface is now configured for Risk-Based Authentication.

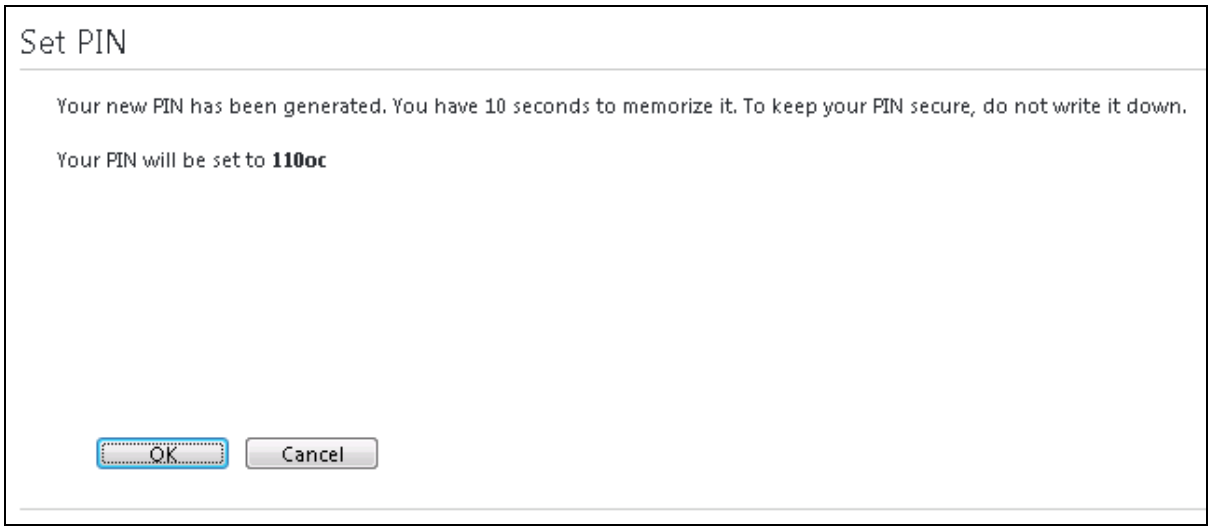
RSA SecurID Login Screens

Login screen:

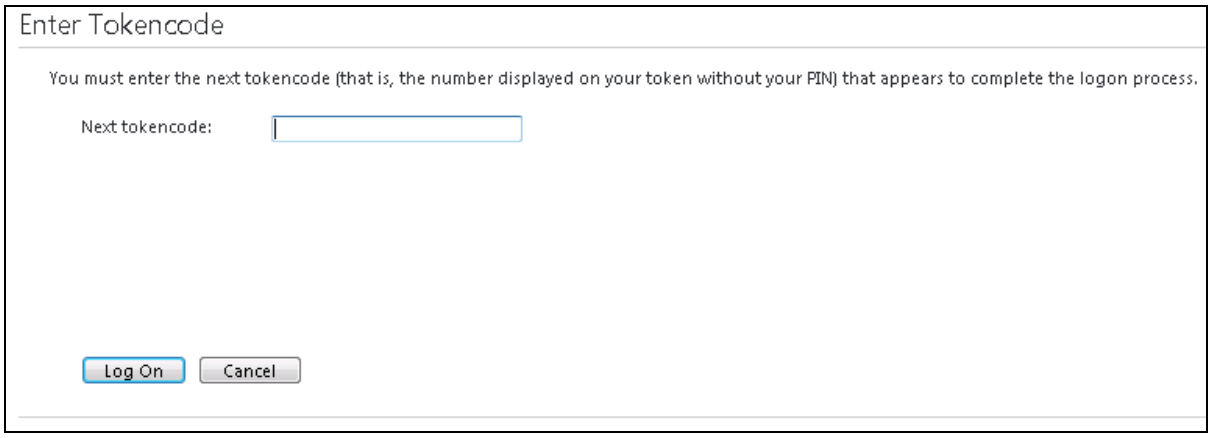
User-defined New PIN:



System-generated New PIN:



Next Tokencode:



Certification Test Checklist for RSA Authentication Manager

Certification Environment

Product Name	Version Information	Operating System
RSA Authentication Manager	8.1	Virtual Appliance
RSA Authentication Agent	7.2	Windows Server 2008 R2
Citrix Web Interface	5.4	Windows Server 2008 R2

RSA SecurID Authentication

Date Tested: July 22, 2014

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

PEW

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

Certification Test Checklist for RSA Authentication Manager

Risk-Based Authentication

Date Tested: July 22, 2014

Mandatory Functionality	RSA Native UDP Agent	RSA Native TCP Agent	RADIUS Client
Risk-Based Authentication			
Risk-Based Authentication	✓	N/A	N/A

Appendix

RSA SecurID Authentication Files

RSA SecurID Authentication Files	
UDP Agent Files	**Location**
sdconf.rec	C:\Windows\System32
sdopts.rec	C:\Windows\System32
Node secret	C:\Windows\System32
sdstatus.12 / jastatus.12	C:\Windows\System32
TCP Agent Files	**Location**
rsa_api.properties	N/A
sdconf.rec	N/A
sdopts.rec	N/A
Node secret	N/A

Partner Integration Details

Partner Integration Details	
RSA SecurID UDP API	Dependent on version of RSA Agent
RSA SecurID TCP API	N/A
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	All users
Display RSA Server Info	Yes; via RSA Security Center
Perform Test Authentication	Yes; via RSA Security Center
Agent Tracing	Yes; via RSA Security Center

Node Secret:

Refer to documentation for the version of RSA Authentication Agent for information regarding Node Secret.

sdconf.rec:

Refer to documentation for the version of RSA Authentication Agent for information regarding sdconf.rec configuration file.

sdopts.rec:

Refer to documentation for the version of RSA Authentication Agent for information regarding sdopts.rec configuration file.

sdstatus.12:

Refer to documentation for the version of RSA Authentication Agent for information regarding sdstatus.12 configuration file.

Agent Tracing:

Refer to documentation for the version of RSA Authentication Agent for information regarding Agent Tracing.