Radiant Logic
Cloud Federation Service

RSA SecurID Ready Implementation Guide

Last Modified: December 26, 2014

Partner Information

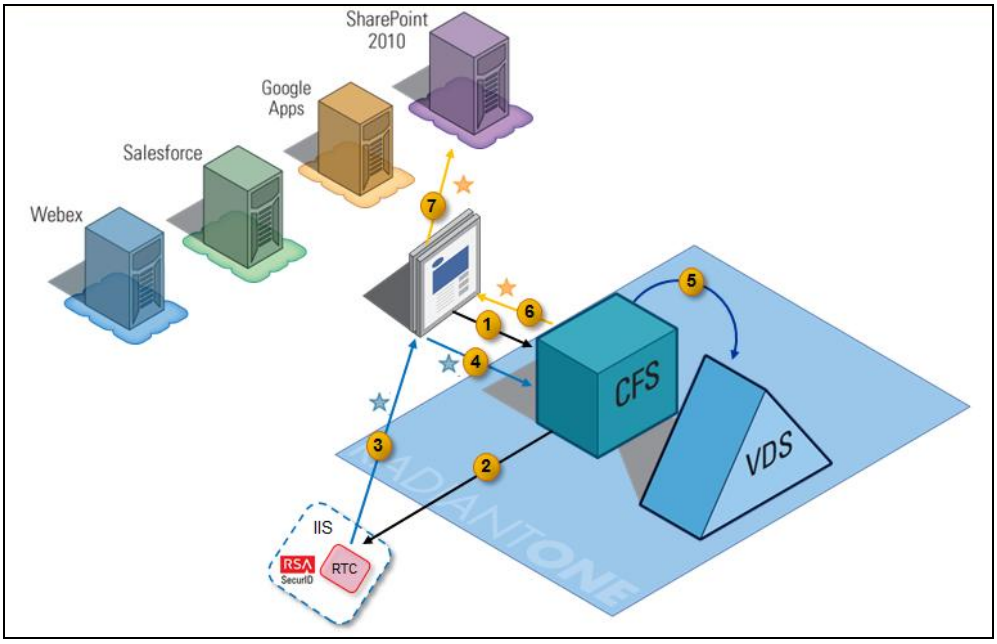
Product Information	
Partner Name	Radiant Logic
Web Site	www.radiantlogic.com
Product Name	CFS
Version & Platform	V3.3
Product Description	The RadiantOne Cloud Federation Service (CFS), powered by identity virtualization, is the latest component of the RadiantOne suite. Together with the RadiantOne virtual directory server, CFS delegates the task of authenticating against all your identity stores to one common virtual layer, and shields your external and cloud applications from the complexity of your identity systems. VDS virtualizes the authentication, validating the user against a variety of sources—including multiple Active Directory domains and forests, LDAP, databases, and web services—then CFS acts as a secure token service, (STS), gathering the requested attributes and building an encrypted claim in the form that the application understands. CFS can securely deliver claims to many of today's mission-critical applications, including but not limited to WebEx, SharePoint 2010/2013, Google apps, and Salesforce.

Solution Summary

RadiantOne Cloud Federation Service (CFS) integrates with RSA SecurID using a custom Radiant Trust Connector (RTC) and an RSA Authentication Agent. Once the integration has been configured, users may choose to authenticate with RSA SecurID two-factor authentication in order to access protected applications. This process is depicted in the diagram below.

CFS also supports RSA Risk-Based Authentication (RBA). RBA strengthens RSA SecurID authentication and password-based authentication by analyzing a user's behavior and device to identify fraudulent authentication attempts. If the assessed risk is unacceptable, RSA Authentication Manager will challenge the user with a secondary authentication method to further confirm the user's identity.

RSA SecurID Authentication Flow-of-Events



1. A user navigates to the CFS portal to access an application, and CFS redirects the client to the appropriate RTC application which displays a login page.
2. The user chooses to authentication with RSA SecurID, and an RSA Authentication Agent prompts the user for credentials. The agent submits the user's credentials to an RSA Authentication Manager server for authentication.
3. The RTC creates a SAML token that contains the authentication results, passes the token to the browser and redirects the user to CFS.
4. CFS requests additional user attributes from a Radiant Logic Virtual Directory Server (VDS) based on a pre-defined user ID mapping.
5. CFS repackages the attribute values in a new token, encrypts the token using the requested application's certificate and passes it to the application.
6. The application uses CFS's public key to decrypt the token and evaluates its attribute values to determine if the user is authorized to access the requested resource.

Supported Features

RSA SecurID Supported Features	
CFS v3.3	
RSA SecurID Authentication via Native RSA SecurID Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	No
On-Demand Authentication via Native SecurID Protocol	Yes
Risk-Based Authentication	Yes
RSA Authentication Manager Replica Support	Yes
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No

Authentication Agent Configuration

RSA Authentication Agents are custom or ready-made software applications that securely pass user authentication requests to and from RSA Authentication Manager. RSA provides the RSA Authentication Agent API for building custom agents, as well as a variety of out-of-the-box agents for protecting access to various operating systems and web resources.

Note: The RadiantOne Cloud Federation Service integration uses the RSA Authentication Web Agent for Microsoft Internet Information Services (IIS).

All RSA authentication agents must be registered with RSA Authentication Manager in order for the server to locate them and establish secure communication channels with them. Use the RSA Security Console to register an agent for each RTC website in your environment.

You need the following information to register an agent:

- the hostname of the RTC site's IIS server
- IP addresses for all of the IIS server host machine's network interfaces

When you register an authentication agent set the agent's type to *Web Agent*.

Note: Hostnames must resolve to valid IP addresses on the local network.

RSA SecurID files

RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	The RSA Web agent installation directory.
Node Secret	The RSA Web agent installation directory.
sdstatus.12	The RSA Web agent installation directory.
sdopts.rec	The RSA Web agent installation directory.

Partner Product Configuration

Before You Begin

This section provides instructions for enabling RSA SecurID two-factor authentication and RSA RBA for Radiant Logic Cloud Federation Service users. You should have working knowledge of CFS and RSA Authentication Manager, as well as access to the appropriate end-user and administrative documentation. Ensure that that both products are running properly prior to configuring the integration. In addition, you must install an RSA Authentication Web Agent for IIS and a RadiantOne RTC an IIS server, and map all RSA users to VDS users before proceeding. Consult your CFS and VDS documentation for details.

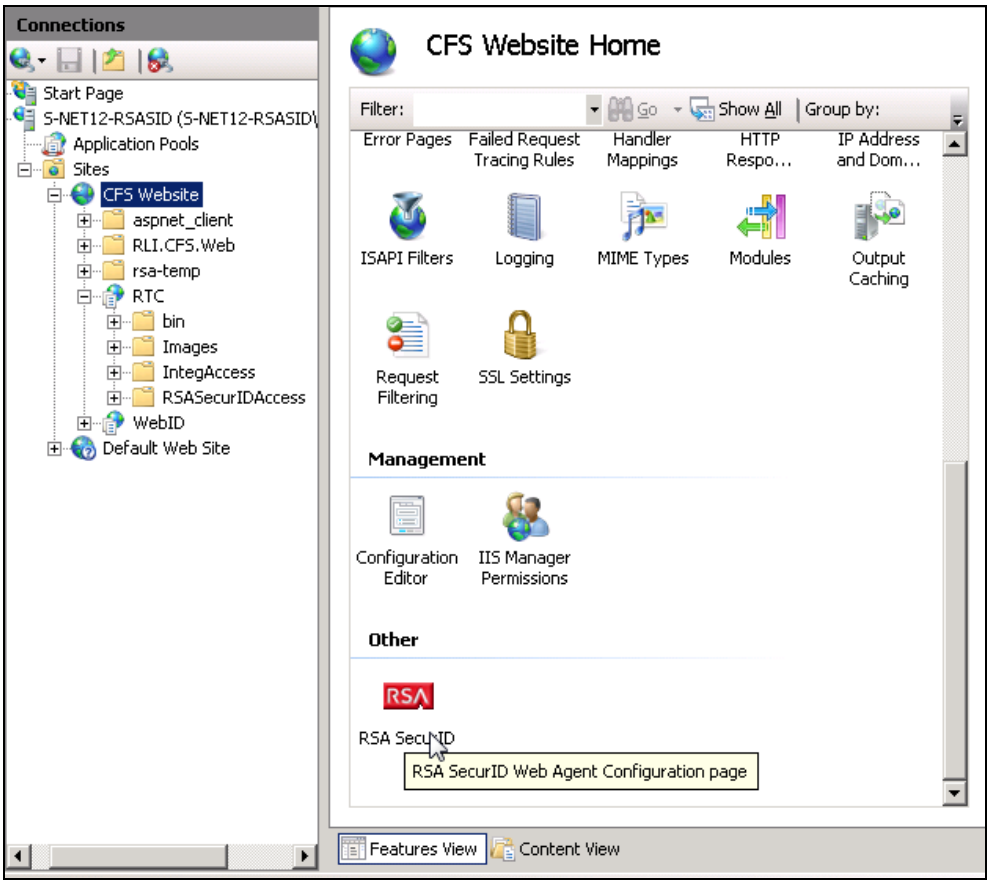
Note: This document is not intended to suggest optimal installations or configurations.

Configure RSA SecurID Authentication for CFS

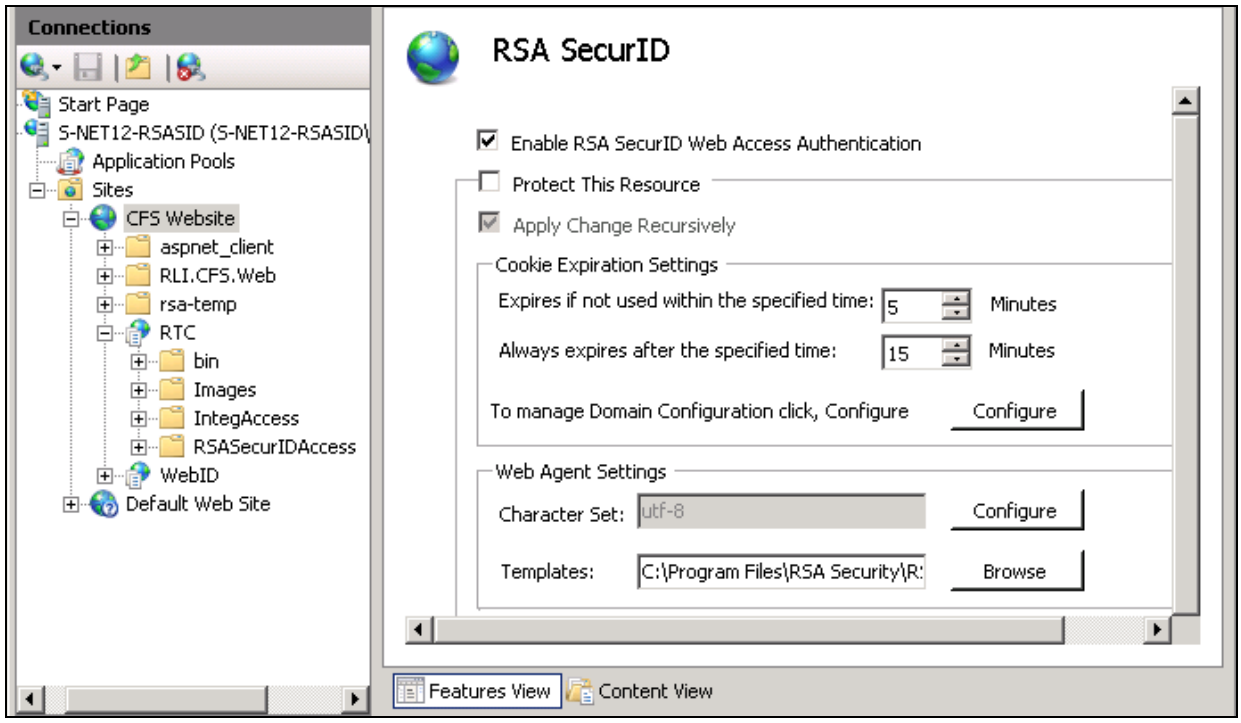
Configure the RadiantOne RTC

Follow the instructions below to enable RSA SecurID authentication for RTC on a given IIS web server. You must perform these steps for each RSA web agent you install.

1. Open the IIS Manager Console, expand the **Sites→CFS Website→RTC→RSASecurIDAccess**, and double-click the **RSA SecurID** icon



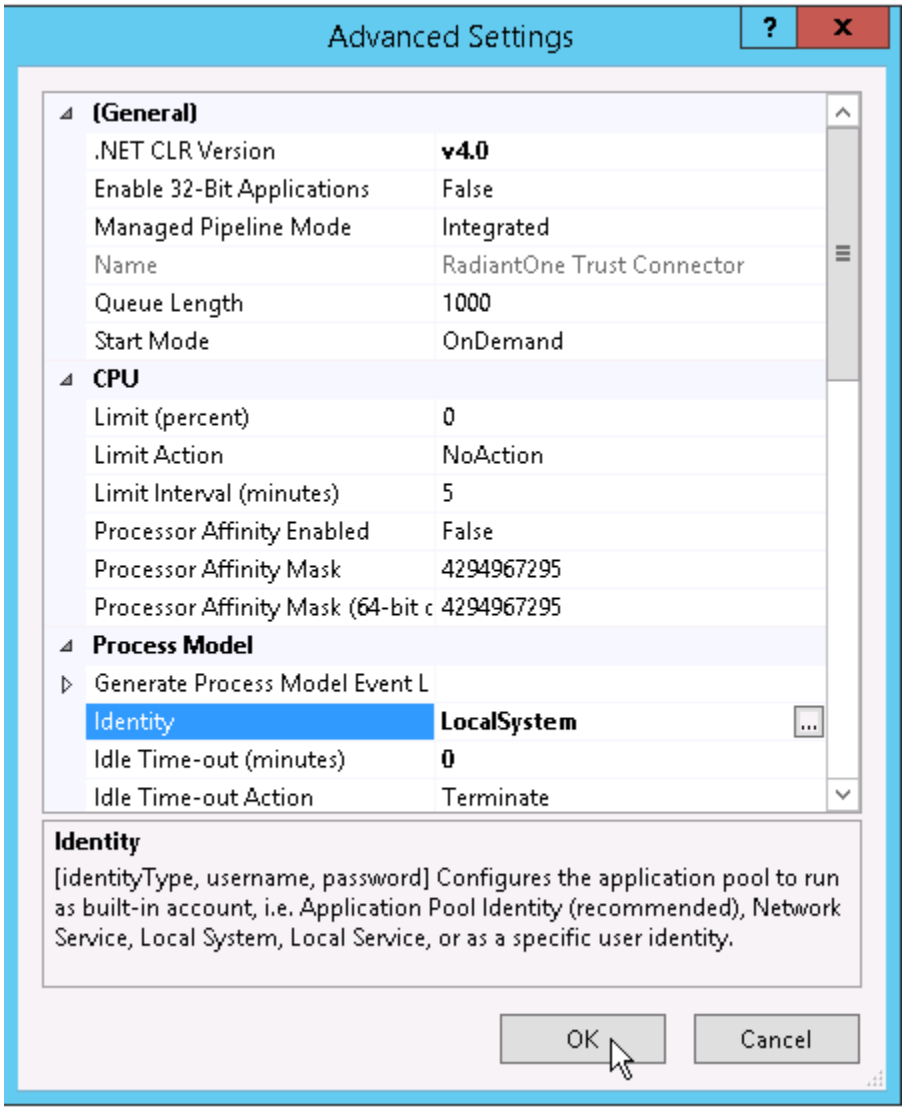
2. Select the **Enable RSA SecurID Web Access Authentication** checkbox.
3. If you don't want to protect the entire website, uncheck the **Protect This Resource** checkbox.



4. Expand the **RTC** tree to the **RSASecurIDAccess→RSA SecurID** node, check the **Protect This Resource with RSA SecurID** checkbox and click the **Apply** button.

5. Expand the Application Pools, right-click on the CSF website's application pool and click the **Advanced Settings** menu item.
6. Expand the **General** section. choose *v4.0* in the .**NET CLR Version** field and choose *Integrated* in the **Managed Pipeline Mode** field.

7. Expand the **Process Model** section and choose *LocalSystem* in the **Identity** field.
8. Click the **OK** button.



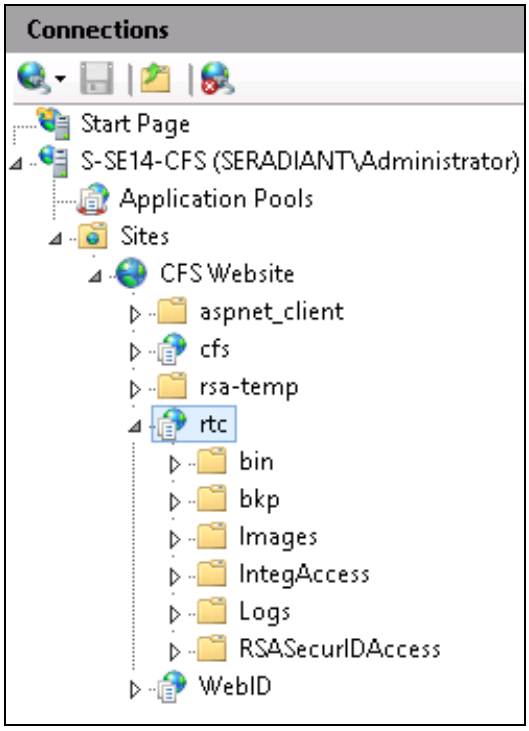
Export the Radiant Trust Connector Certificate for RSA SecurID

The RTC installer generates a certificate that it needs in order to communicate with CFS. You must export the certificate and copy it to your CFS host machine so that you can import it when you configure the RSA SecurID in CFS. There are two ways to export the certificate:

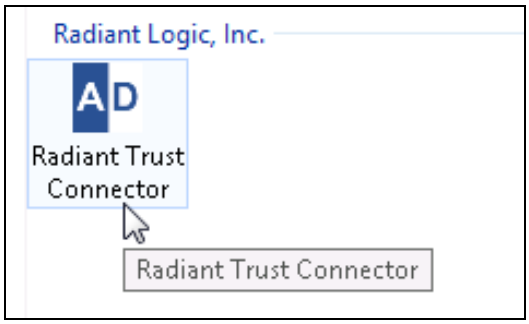
- Export the Certificate from the RTC Machine
- Export the Certificate from a Web Browser

Export the Certificate from the RTC Machine

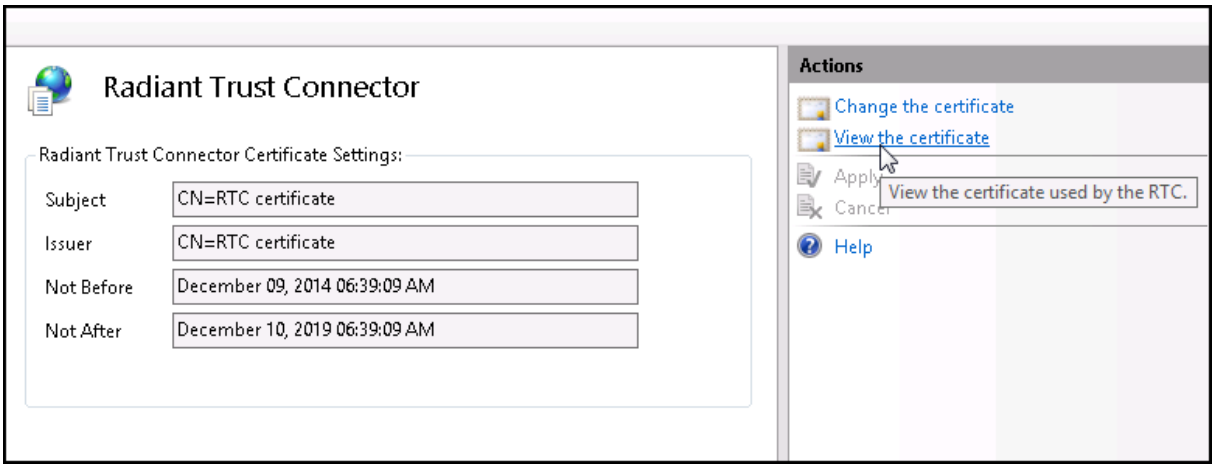
1. If you are on the machine where the RTC is installed, open the IIS Manager console, expand the **CFS Website** and click on the **RTC** application.



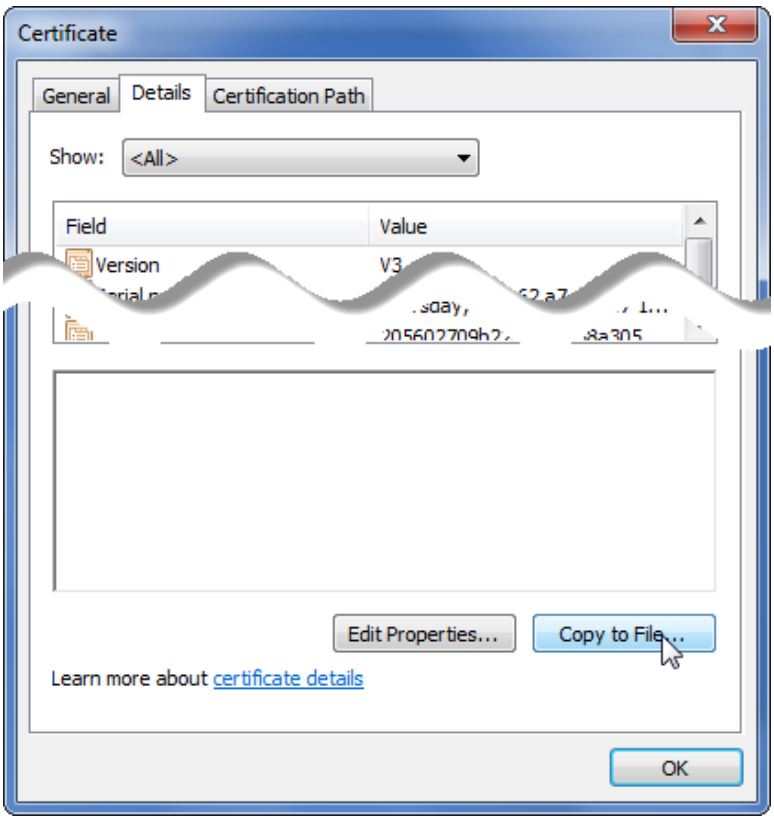
2. Double-click on **the Radiant Trust Connector** icon on the right.



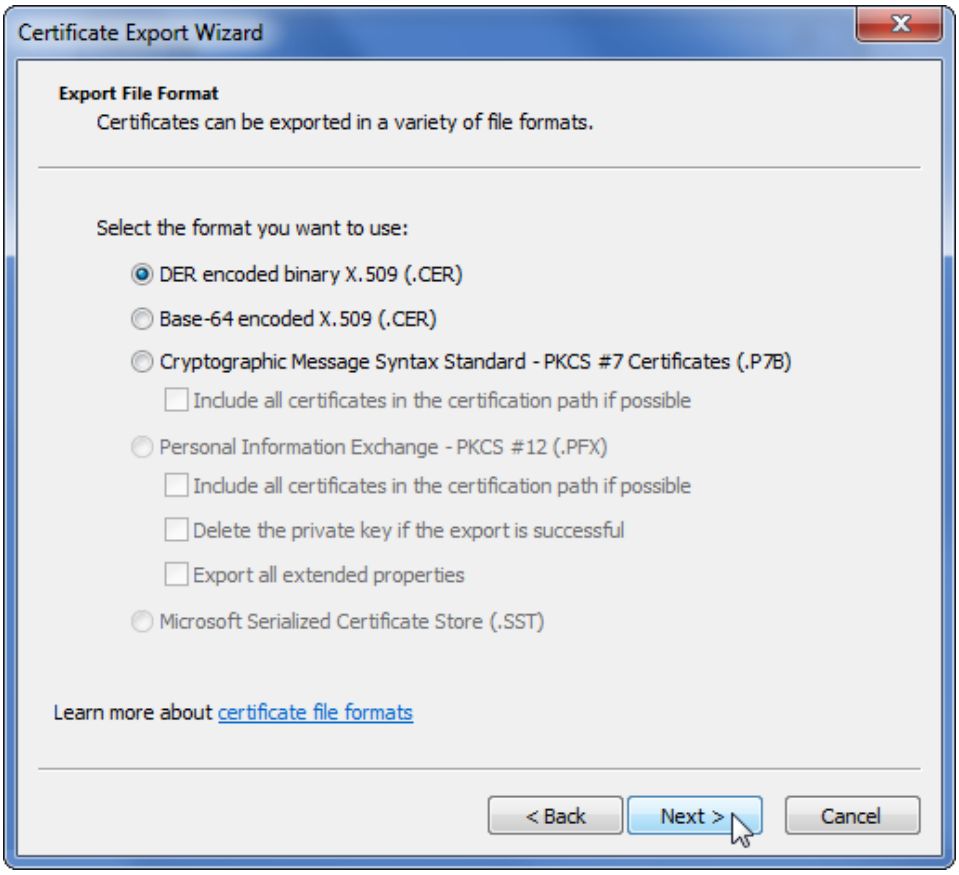
3. Click the **View the Certificate** link on the far right of the screen.



4. Windows will open your server's root **Certificate** dialog box. Click the **Details** tab and click the **Copy to File** button.



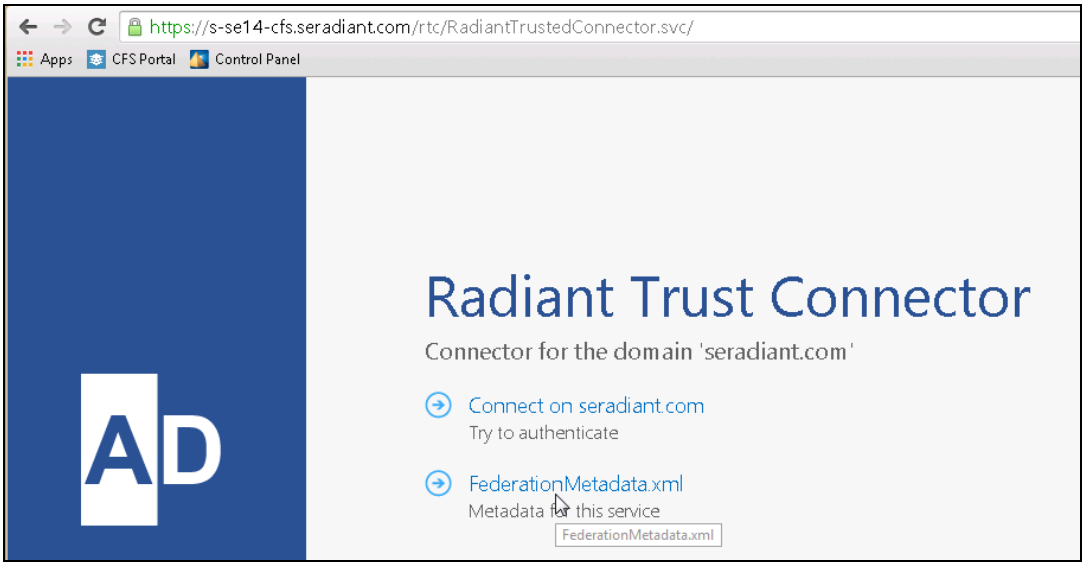
5. Windows will open the **Certificate Export Wizard**. Click the **Next** button on the **Welcome** page.
6. Select the **DER encoded binary X.509 (.CER)** radio button on the **Export File Format** page.
7. Click the **Next** button.



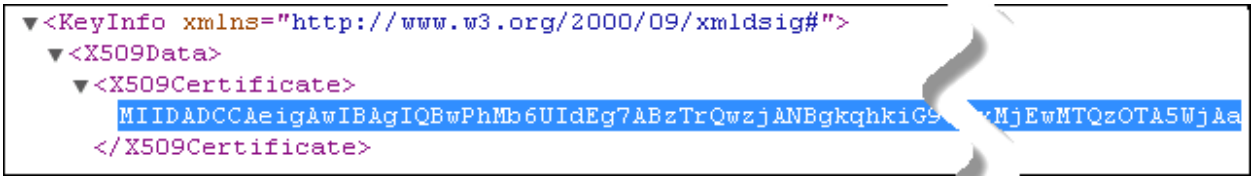
8. Click the **Browse** button on the **File to Export** page.
9. Expand the **Browse Folders** section at the bottom of the **Save As** dialogue box, locate and select a temporary folder and specify a name for the root certificate file in the **File name** text field.
10. Click the **Save** button.
11. Copy the certificate to a directory on your CFS machine. You will need to access it when you configure the RTC in the CFS tenant dashboard.

Export the Certificate from a Web Browser

1. If you are not on the RTC host machine, navigate to the RTC URL from a web browser (e.g. https://s-se14-cfs.seradiant.com/rtc/RSASecurIDAccess/) and click the **FederationMetadata.xml** link.

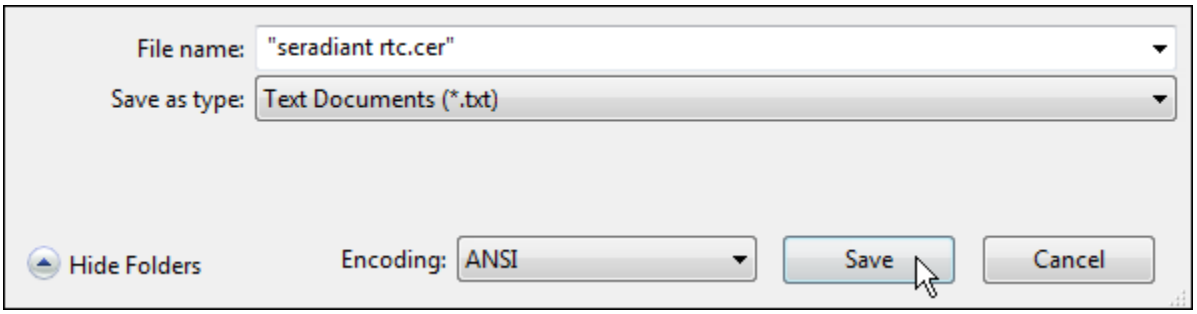


2. Copy the <*X509Certificate*> element's value.



3. Open text editor, paste the <*X509Certificate*> element's value into a new document and save the file with a *.cer* or *.der* extension.

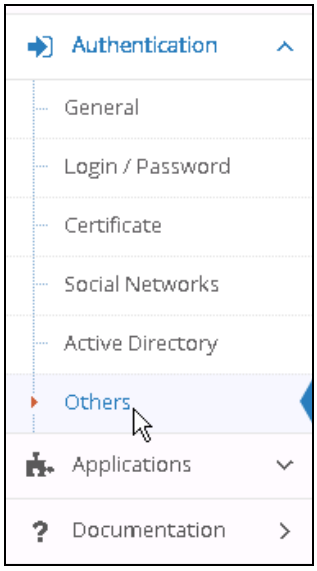
Important: Make sure your file has a *.cer* or *.der* extension. You may need to enclose the filename in double quotes to prevent your text editor from appending a *.txt* extension.



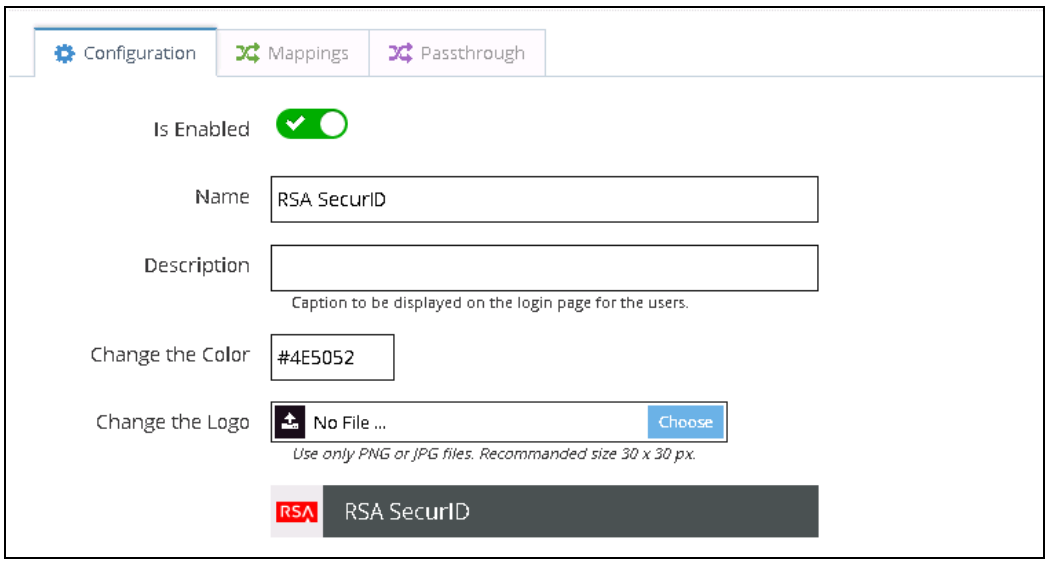
4. Copy the certificate to a directory on your CFS machine. You will need to access it when you configure the RTC in the CFS tenant dashboard.

Configure RSA SecurID Authentication for CFS

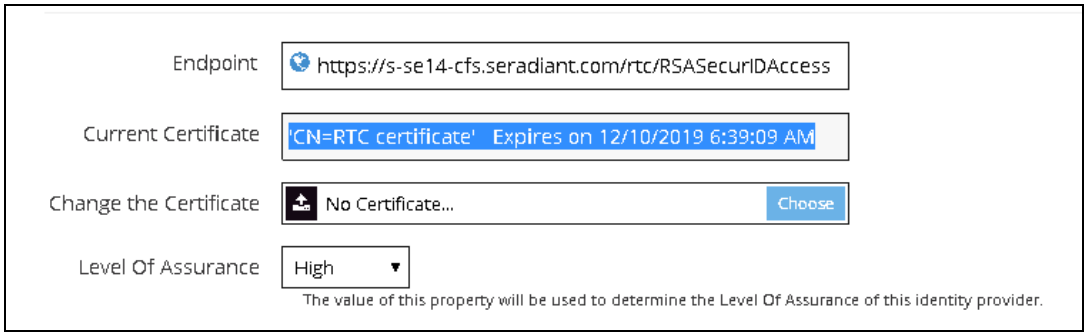
1. Login the CFS Tenant Administration Dashboard as a tenant administrator, open the **Administration** section, expand the **Authentication** tree and select the **Others** node.



2. Click the **New Trusted Identity Provider** button and select the **Configuration** tab.
3. Click the **Is Enable** toggle button so that the check mark is exposed on the left.
4. Enter a name to identify the RSA SecurID authentication method in the **Name** field.
5. Optionally, enter a description of the method in the **Description**.
6. If you want to select an RSA SecurID logo to display on the CFS portal login page, click the **Choose** button, locate and select a logo, and click the **OK** button.

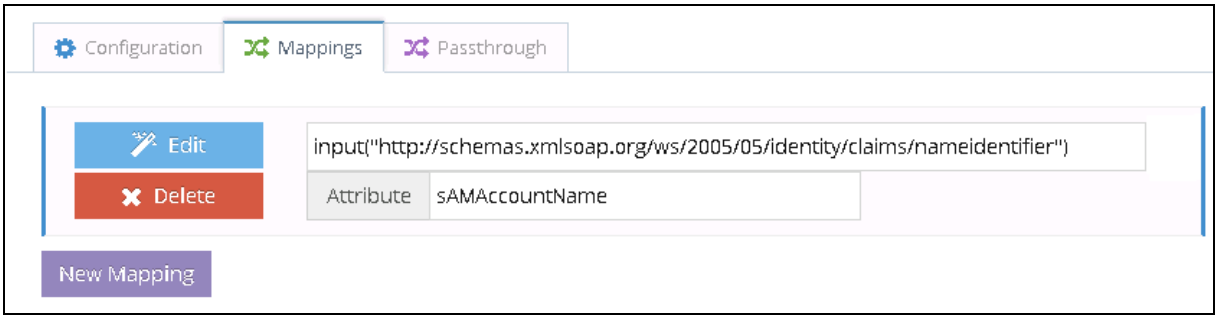


7. Enter the RTC endpoint URL in the **Endpoint** field.
8. Click **Choose** buton to the right of the **Change the Certificate** field, locate and select the RTC certificate you exported and click the **OK** button.
9. Based on your requirements, select the level of assurance for a successful RSA SecurID authentication from the **Level of Assurance** dropdown list.
10. Click **Save** button.



11. Select the **Mappings** tab.
12. Whenever an RSA SecurID user authenticates, CFS will look up their user's identity in VDS based on a pre-defined user ID mapping. The example below uses the *sAMAccountName* attribute to map RSA users to CFS identities. To edit this criteria, click the **Edit** button.

Important: You must map each user's identity in your RSA Authentication Manager identity store to an identity in your CFS VDS identity store. Consult your CFS and VDS documentation for details.



13. Click **Save** button.

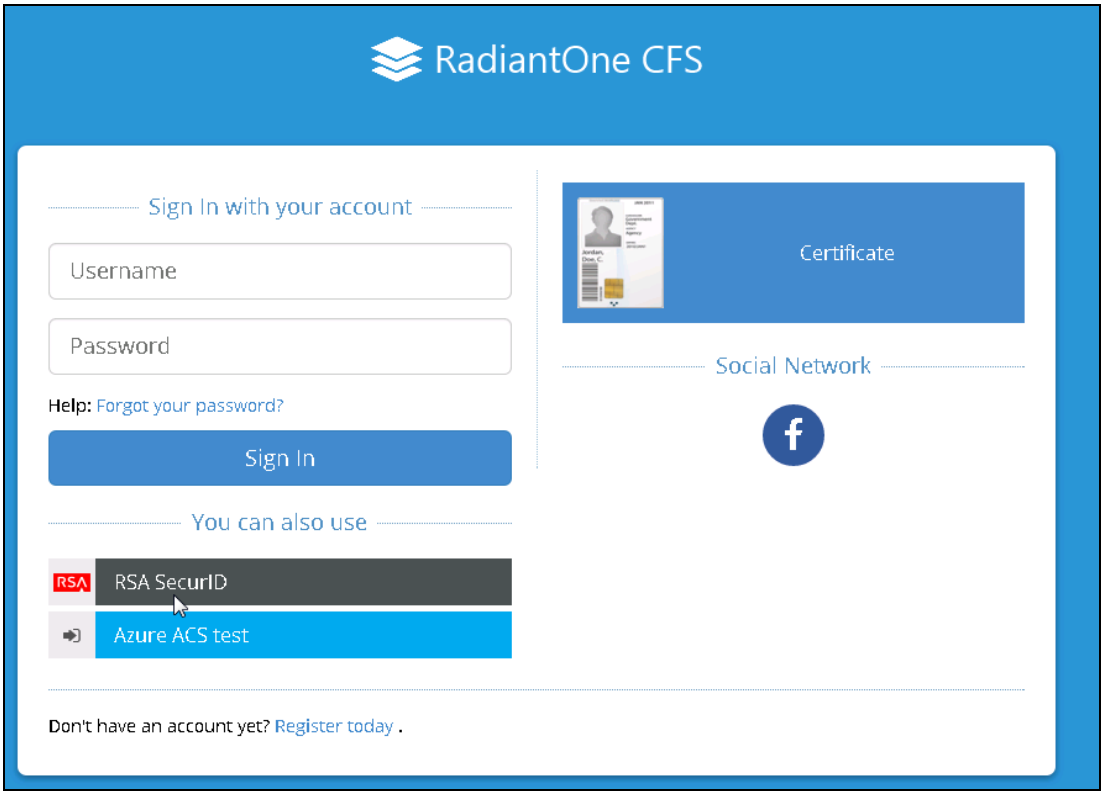
Risk-Based Authentication Configuration

If you plan to enable RSA Risk-Based Authentication (RBA) for a CFS, you have to configure RSA SecurID authentication first. Once you have done so, follow the instructions in your RSA Authentication Web Agent documentation to configure Risk-based Authentication.

Note: In order for an application to support RBA, it must also support RSA SecurID authentication. Before you configure RBA for CFS, make sure you have enabled RSA SecurID. RBA **does not** require RSA SecurID tokens.

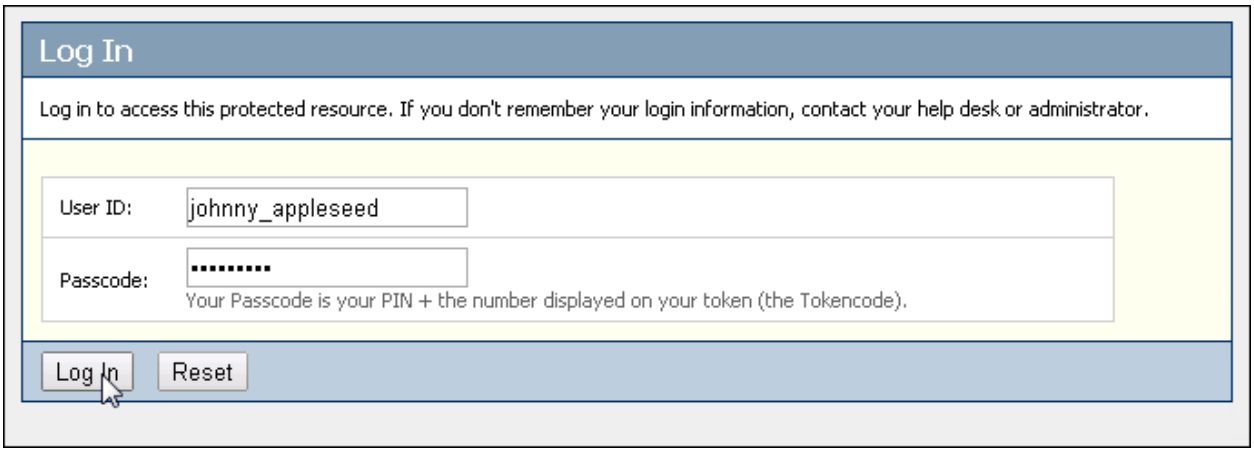
RSA SecurID and RBA Authentication Screenshots

Once you configure the integration, CFS will give users the option to authenticate with RSA SecurID.



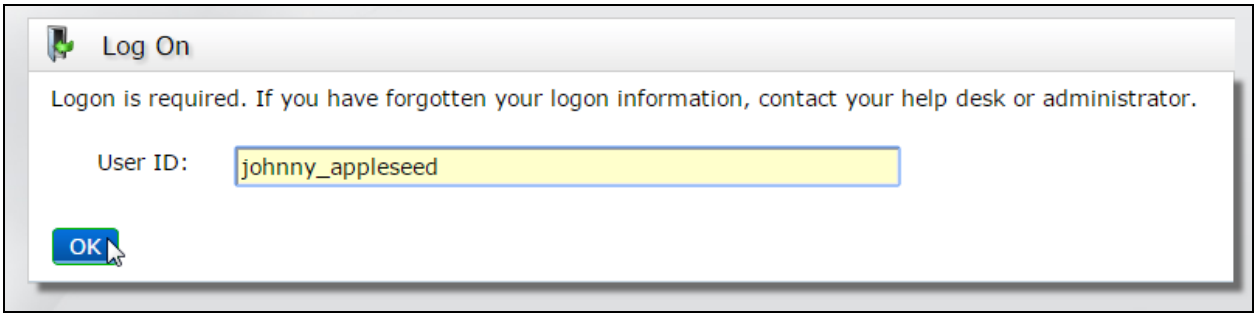
If the user clicks the RSA SecurID button, CFS will redirect the user to the RTC. If the RSA Authentication Web Agent for IIS has been configured for RSA SecurID authentication (rather than RBA), the agent will prompt the user for RSA SecurID credentials.

Standard RSA SecurID Logon Prompt:

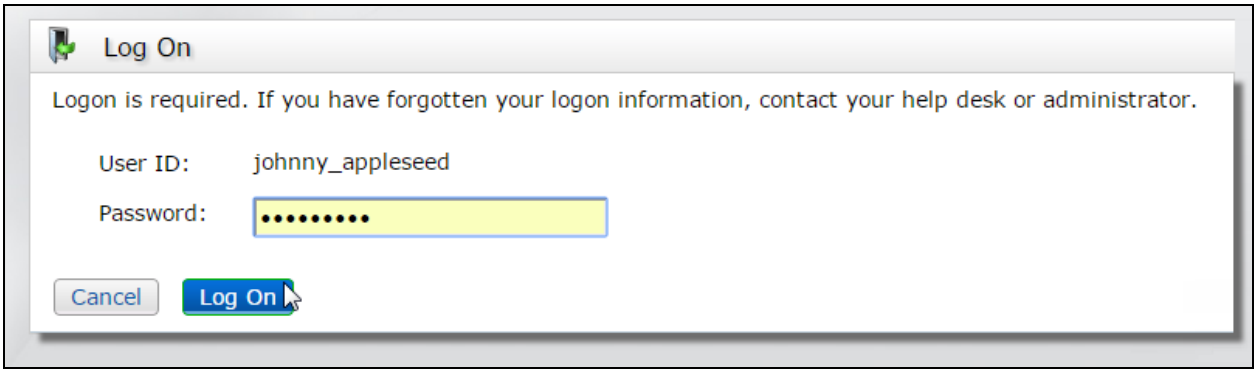


If the RSA Authentication Web Agent has been configured for RSA RBA, RSA's RBA application will prompt the user for primary credentials, and possibly secondary credentials depending on risk analysis.

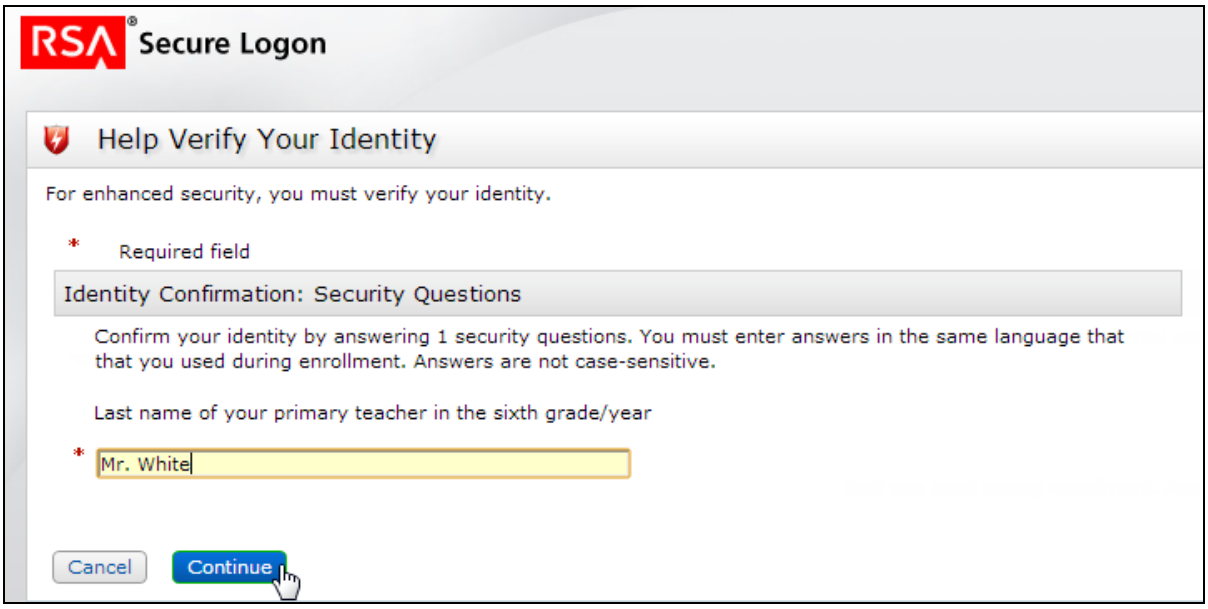
RBA User ID Logon Prompt:



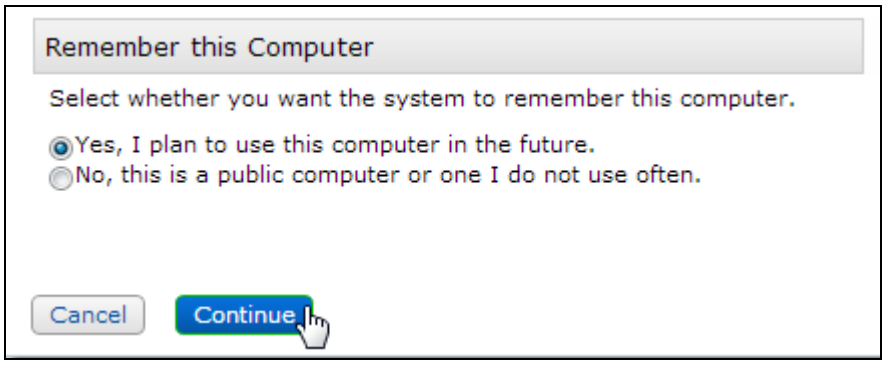
RBA Password Logon Prompt:



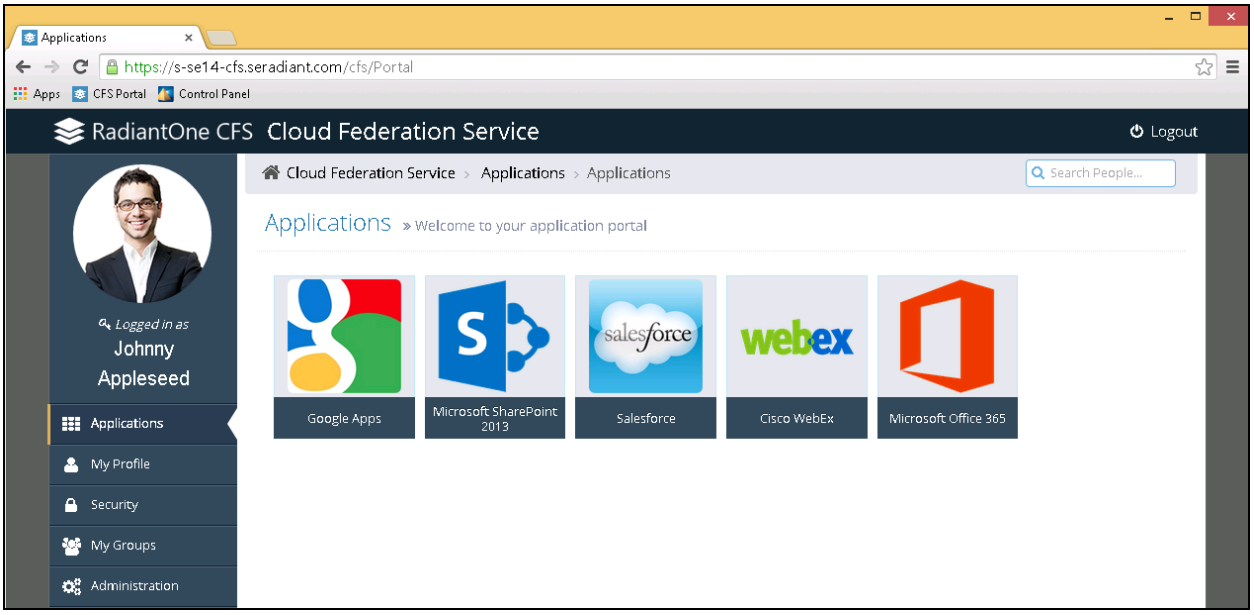
RBA Challenge Question Logon Prompt:



RBA Device-Binding Option Prompt:



After RSA authenticates the user's RSA SecurID or RBA credentials, CFS will allow the user to access applications that trust CFS as an identity provider.



Certification Checklist for RSA Authentication Manager

Date Tested: December 18, 2014

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.1	Virtual Appliance
RSA Authentication IIS Web Agent	7.1.2	Windows 2008 R2
RadiantOne Cloud Federation Service	3.3	Windows 2008 R2

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 Numeric PIN	✓		Deny Numeric PIN	N/A
Deny PIN Reuse	✓		Deny PIN Reuse	N/A
Passcode				
14 Digit Passcode	✓		14 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

JGS / PAR

✓ = 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

JGS

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