Call U Conferencing
Secure Audio Conferencing Service

RSA SecurID Ready Implementation Guide

Last Modified: June 19, 2013

Partner Information

Product Information	
Partner Name	Call U Conferencing, LLC
Web Site	www.callu.cc
Product Name	Call U Secure Conferencing
Version & Platform	Version 2.1.3
Product Description	Call U Conferencing's Secure Audio Conferencing Service requires conference participants to perform a SecurID authentication prior to being able to join the conference call.

Solution Summary

Call U Conferencing Secure Audio Conferencing allows the ability to configure higher-security conferencing by requiring SecurID two-factor authentication when joining the conference. To join a secure conference, users must first authenticate at the Call U Conferencing portal using their SecurID token.

RSA Authentication Manager supported features	
Call U Secure Conferencing 2.1.3	
RSA SecurID Authentication via Native RSA SecurID Protocol	No
RSA SecurID Authentication via RADIUS Protocol	Yes
On-Demand Authentication via Native SecurID Protocol	No
On-Demand Authentication via RADIUS Protocol	Yes
Risk-Based Authentication	No
Risk-Based Authentication with Single Sign-On	No
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

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 the Call U Portal will occur.

A RADIUS client that corresponds to the Authentication Agent must be created in the RSA Authentication Manager in order for the Call U Portal 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 RADIUS clients.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Call U Conferencing service to use RSA SecurID Authentication. Call U Conferencing only supports RADIUS authentication at this time.

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.

Call U Conferencing SecurID Features

Integration with RSA SecurID enables the service to provide a higher level of security with the Call U Conferencing service. After implementation, access to account level features from the Call U Portal is prohibited until successful authentication is completed.

This also enables a highly secure conference experience where every participant attending a secure conference call is required to authenticate prior to connection to the conference. You can read more about Secure Conferencing at **http://www.callu.cc/secure**.

Configuration Steps

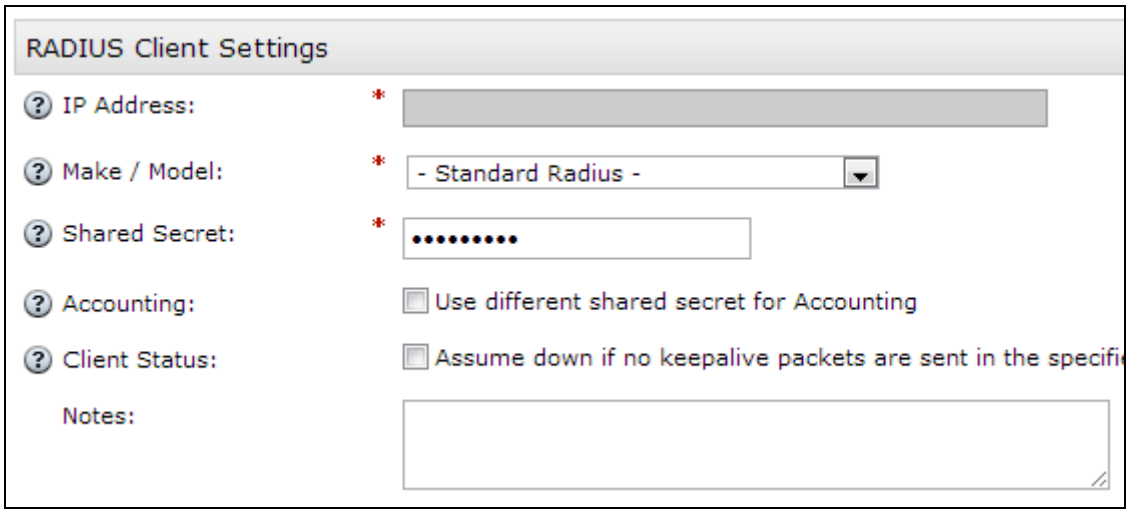
In order to implement RSA SecurID, two steps need to occur. First, your Call U Conferencing account needs to be configured to communicate with your RADIUS server(s). Second, each user under your Call U Conferencing account needs to add the RSA SecurID plug to their account and configure it.

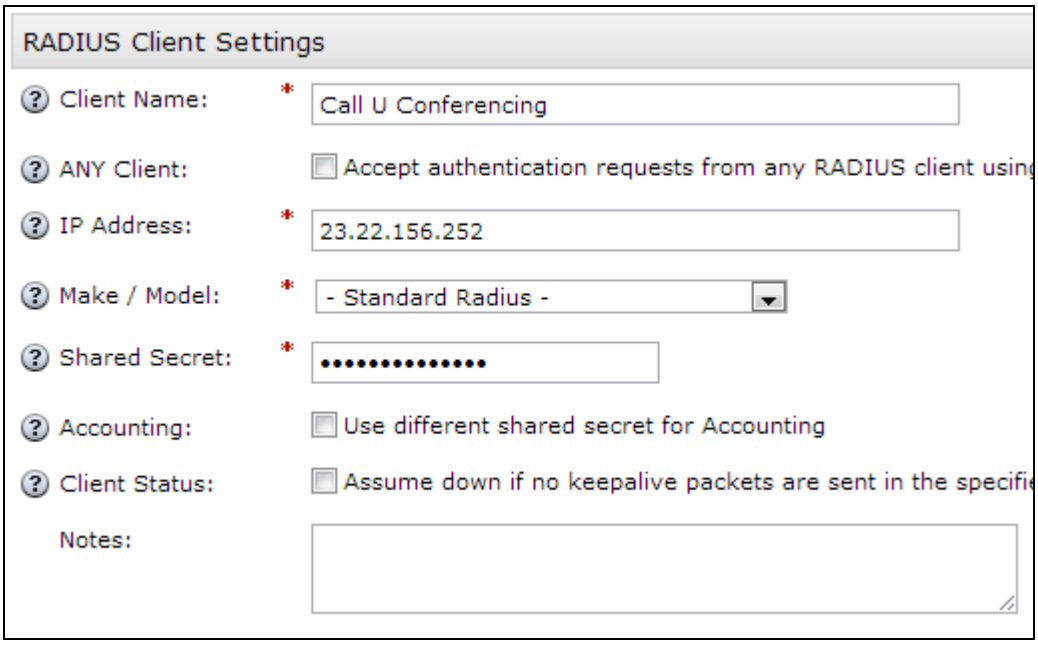
Configure Call U Conferencing

When supporting RSA SecurID, the Call U Conferencing service will communicate directly with the RADIUS service provided by your RSA Authentication Manager.

In order to support RADIUS authentication, you need to enable the RADIUS Authentication Agent from the RSA Security Console and then create a RADIUS Client from the RSA Security Console.

The RADIUS Client should have **Standard Radius** as the **Make / Model** and either accept connections from any IP address or be restricted to requests coming from IP Address **23.22.156.252** as shown below:





Call U Conferencing supports up to three different RADIUS URLs or IP addresses for redundancy and default to port 1812. You should also ensure that your RADIUS server(s) are accessible through your firewall.

Once you have configured your RADIUS servers, gather the following information about your RADIUS installation. Remember to specify the port number if it is different from the default.

- RADIUS Server 1 URL _____ Port _____
- RADIUS Server 2 URL _____ Port _____
- RADIUS Server 3 URL _____ Port _____
- RADIUS Shared Secret _____
- Call U Conferencing Primary Account Email _____

Email this information to **security@callu.cc** along with your contact information. Upon receipt, we will contact the primary account holder for the account you identify to confirm approval to implement this feature. Upon confirmation, the configuration will be completed within two (2) business days and we will contact you to arrange testing.

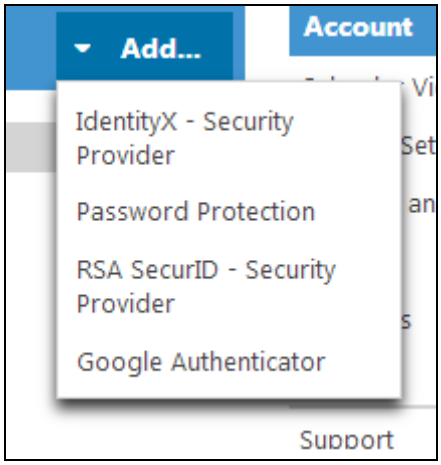
Note: You will not be able to proceed with any other steps until you receive a response from Call U Conferencing that your account has been configured to communicate with your RADIUS servers.

Important: Once your account has been configured and your users have configured their RSA SecurID Plug Ins, any changes to your RADIUS environment or unavailability of your RADIUS / RSA SecurID infrastructure will limit the functionality of the Call U Portal until such time as your RADIUS service is accessible.

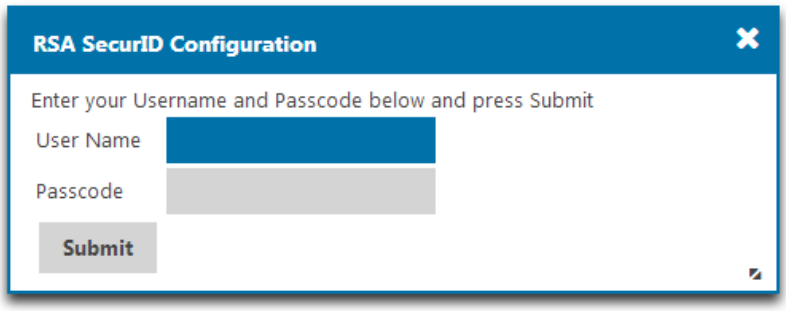
RSA SecurID Plug In Configuration

Once you have a RADIUS client configured and have contacted Call U Conferencing with your RADIUS server information, you are ready to configure the SecurID Plug In.

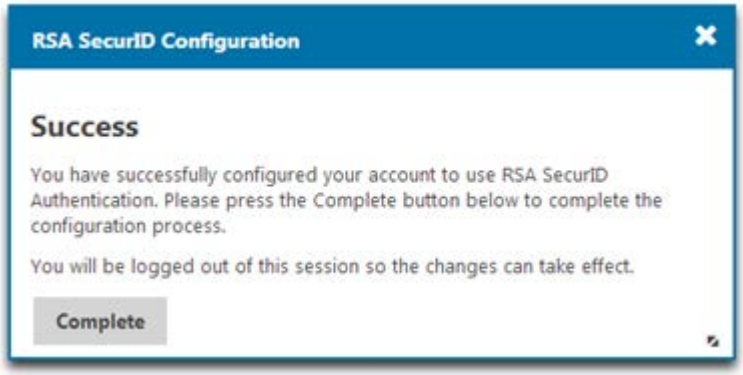
1. Navigate to the **Plug Ins** page on the Call U Portal and click **Add…** to add a new Plug In. Select the **RSA SecurID – Security Provider Plug In**.



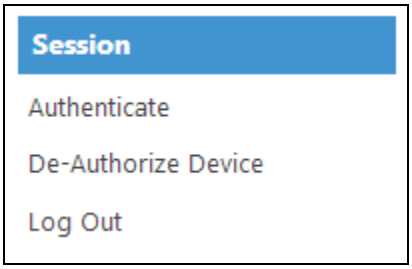
2. You will be prompted for you SecurID User Name and Passcode. Follow normal procedures for entering your Passcode depending on the type of token you are using and the status of your account.



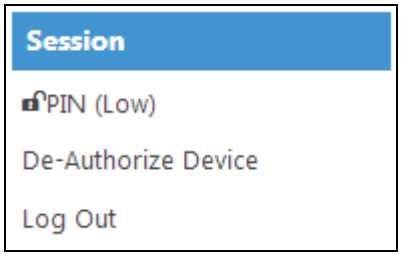
3. The Call U Conferencing service will attempt to contact your RADIUS server and authenticate your SecurID Passcode. If successful, you will be shown a success message and the SecurID Plug In is now active. If you receive an error, check your RADIUS server logs for more information.



4. To authenticate your portal session, browse to the Call U Portal and select **Authenticate** from the right-hand menu.

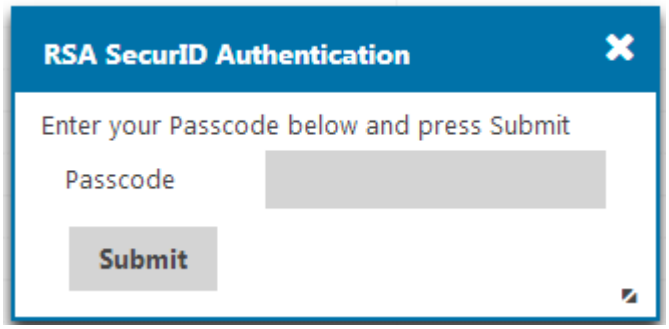


5. The Call U Conferencing service will contact your RADIUS server to authentication your SecurID Passcode. Upon success, you will be returned to the Call U Portal with the appropriate authentication message displayed in the Menu.

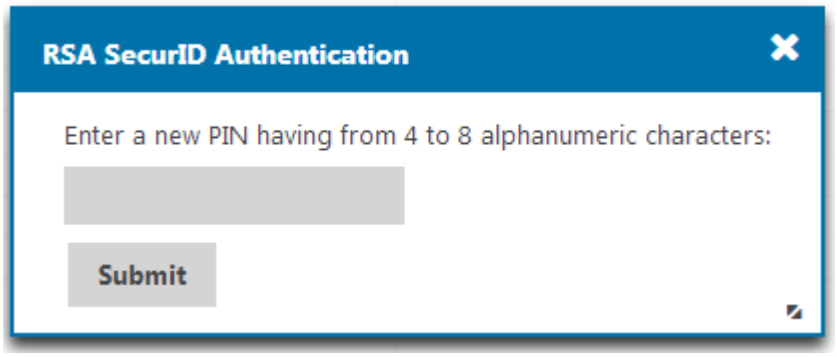


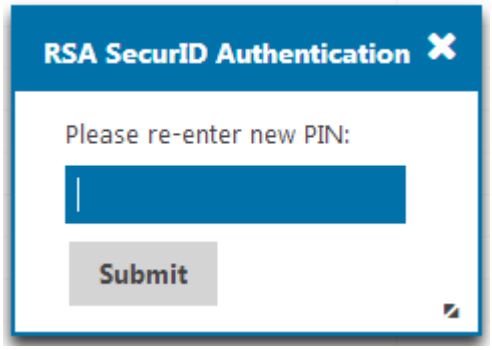
RSA SecurID Login Screens

Login screen:

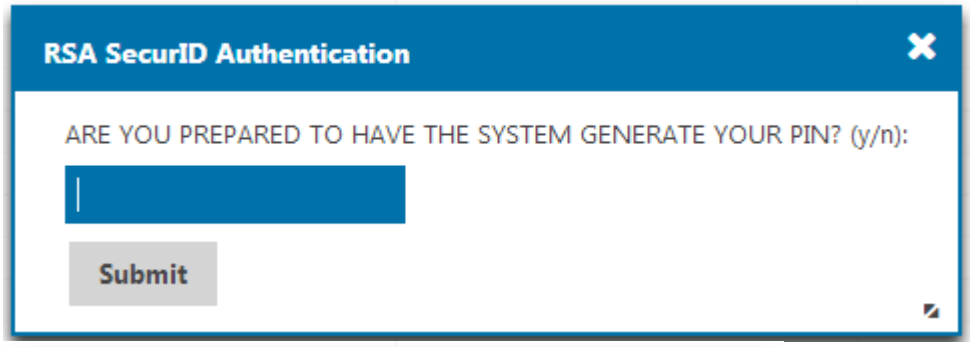


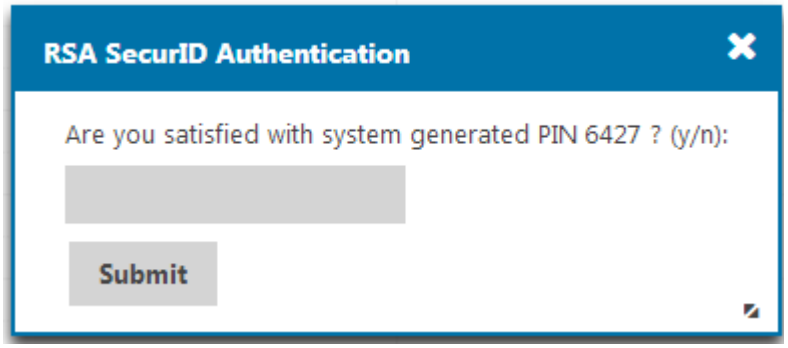
User-defined New PIN:



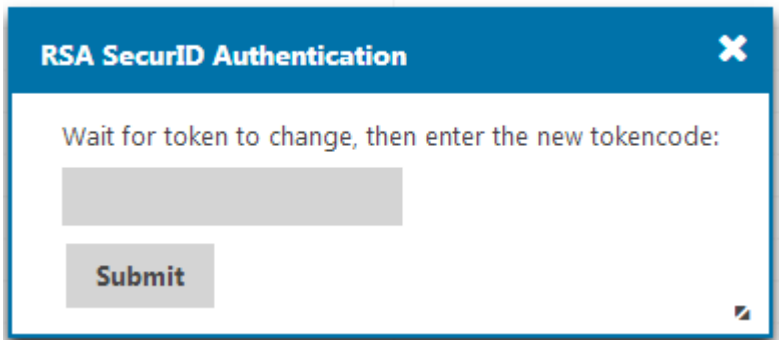


System-generated New PIN:





Next Tokencode:



Certification Checklist for RSA Authentication Manager

Date Tested: June 19, 2013

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.0	Virtual Appliance
Call U Secure Conferencing	2.1.3	Hosted Service

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

MRQ / PAR

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