Cryptzone
AppGate Security Server

RSA SecurID Ready Implementation Guide

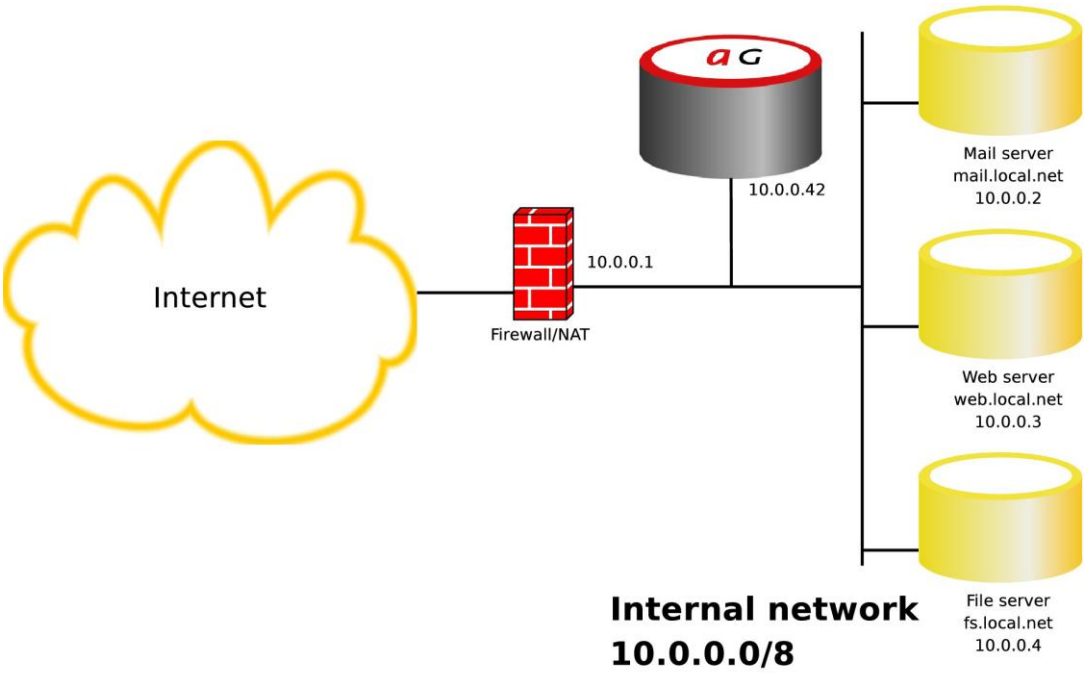
Last Modified: January 14, 2014

Partner Information

Product Information	
Partner Name	Cryptzone
Web Site	www.cryptzone.com
Product Name	AppGate Security Server
Version & Platform	10.2.1
Product Description	The Cryptzone AppGate Security Server (AGSS) allows secure and controlled access to resources on protected servers regardless of client location. All access to the servers is done through the AGSS which encrypts all traffic between the AGSS and the client while granting access to those who should have it, essentially acting as a gateway.

Solution Summary

RSA SecurID supported features	
Cryptzone AppGate Security Server v10.2.1	
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
On-Demand Authentication via API	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	Yes



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 AppGate Security Server will occur.

A RADIUS client that corresponds to the Authentication Agent must be created in the RSA Authentication Manager in order for AppGate Security Server 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	/var/ace/sdconf.rec
Node Secret	/var/ace/securid
sdstatus.12	/var/ace/sdstatus.12
sdopts.rec	Not Implemented

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

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the AppGate Security Server with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

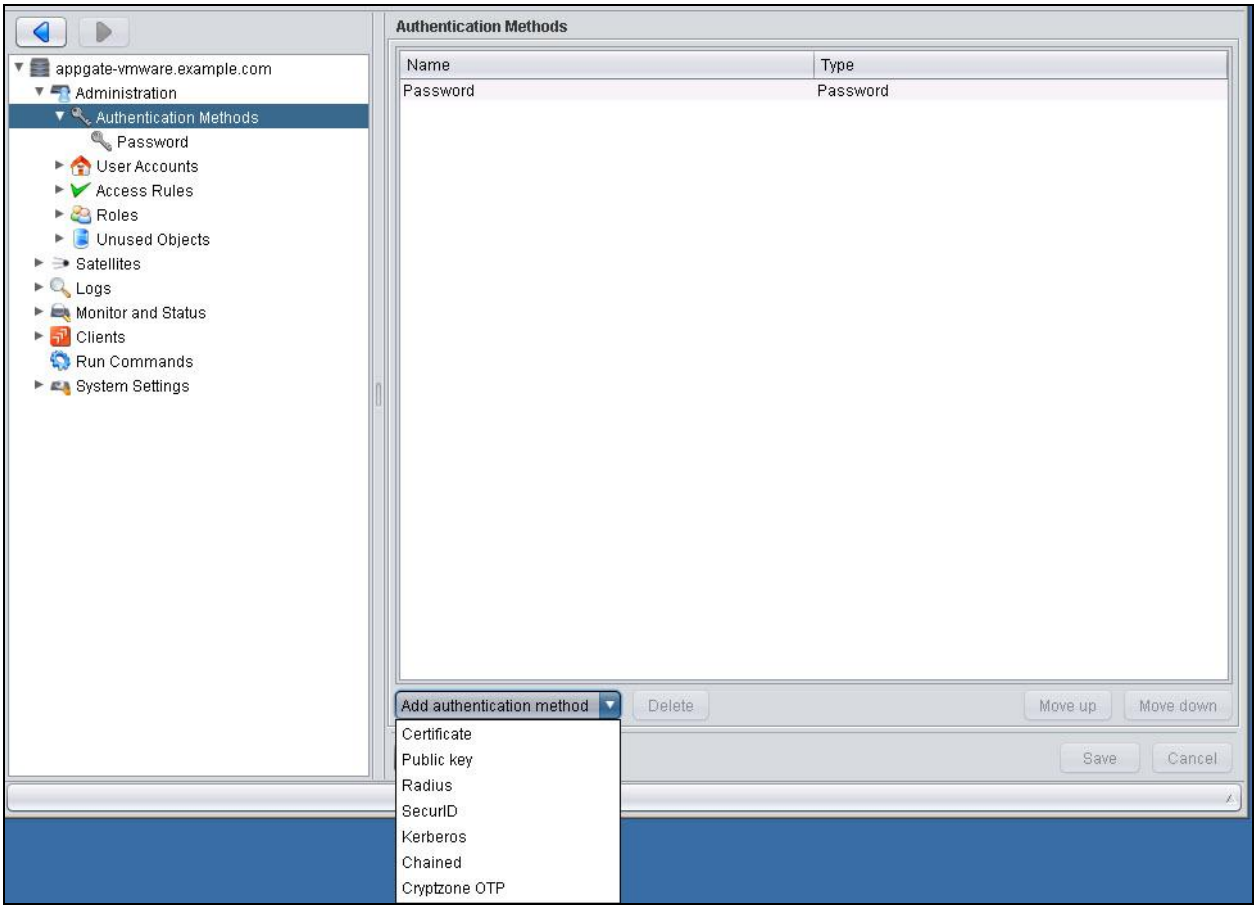
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All AppGate Security Server components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuring RSA SecurID

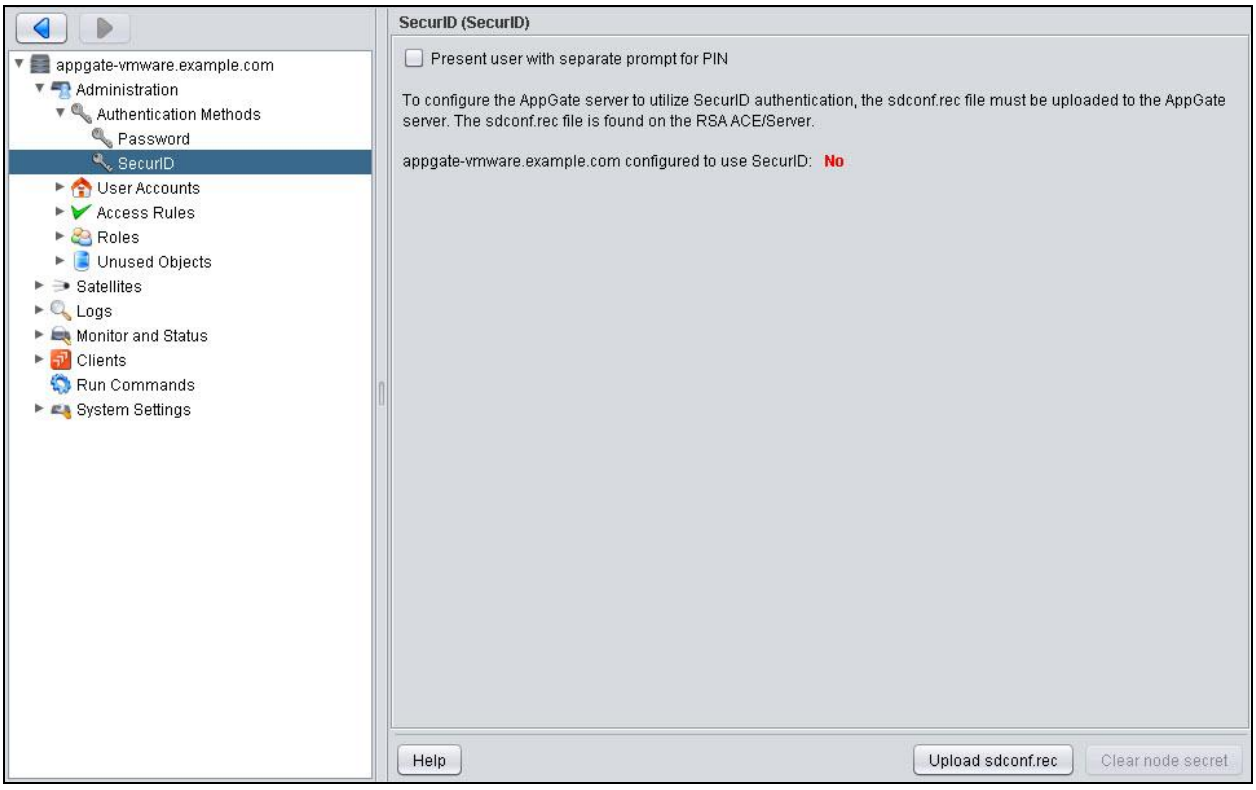
This guide provides configuration information for native RSA SecurID as well as RSA RADIUS Authentication.

1. Start the AppGate Console by launching a web client and enter the IP address of the AppGate Security Server.
2. Navigate the left hand tool bar to **Administration > Authentication Methods** and select **SecurID** and/or **Radius** from the **Add Authentication Method** pull down.

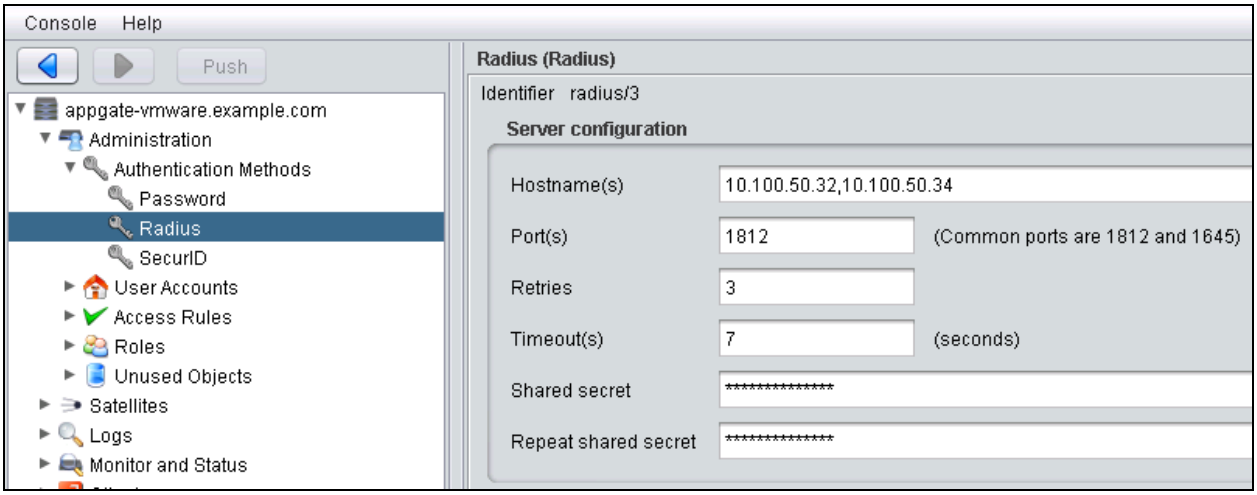


3. Click **Save** at the bottom right hand corner.

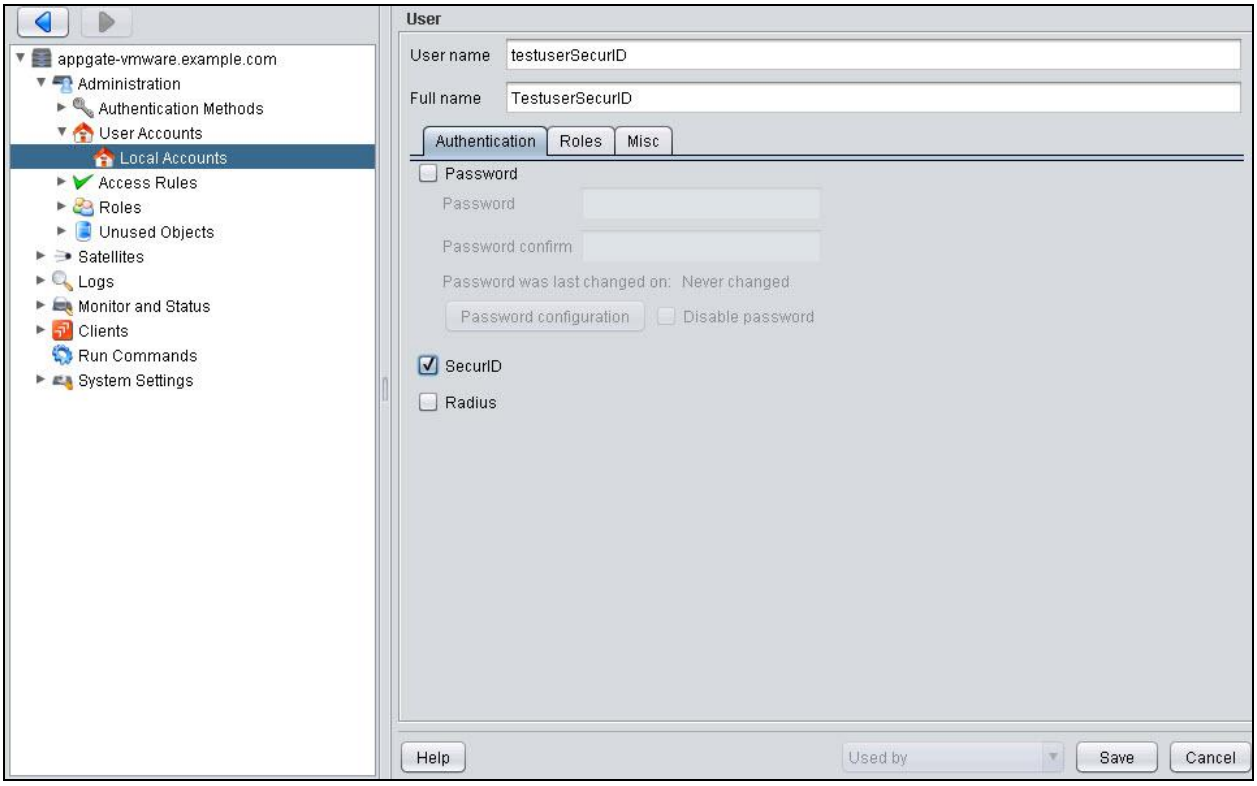
4. If configuring for native SecurID go to the SecurID screen and upload the **sdconf.rec** file you downloaded from the RSA Authentication Server.



5. If configuring for Radius go to the Radius screen and configure the **Hostname(s)** with the primary and secondary Radius servers' addresses separated by a comma. Configure the **Shared secret** and click **Save**.

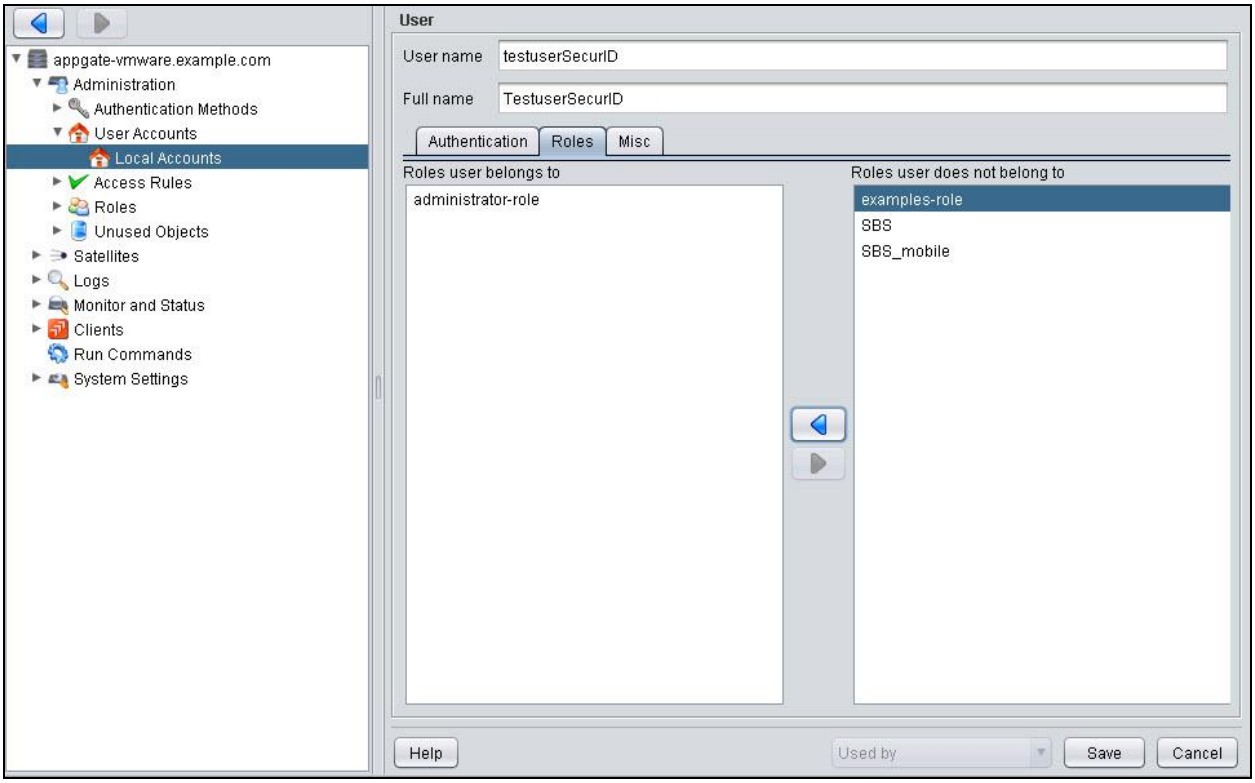


6. Navigate to **Administration > User Accounts > Local Accounts** and click **New**. Fill in the **User name** field and check **Radius** or **SecurID** under the Authentication tab.



Note: The user account must be defined in both the RSA Server and AppGate Server.

7. Select the **Roles** tab and assign at least one to the **Roles user belongs to** column.
8. Click **Save**.

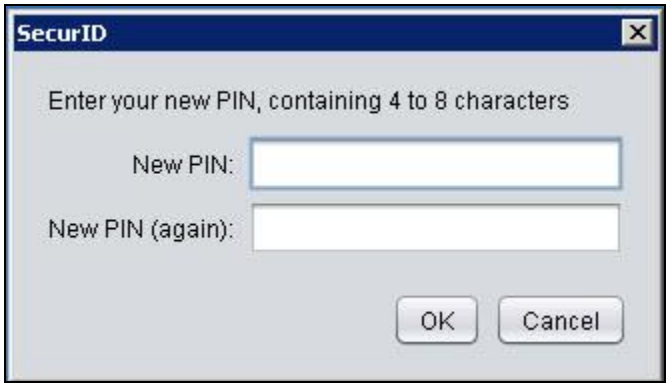


9. Open a web browser to the AGSS and download the AGSS client to the user's desktop.
10. Launch the AGSS client and select the authentication method. Enter the user's RSA credentials.

Screens

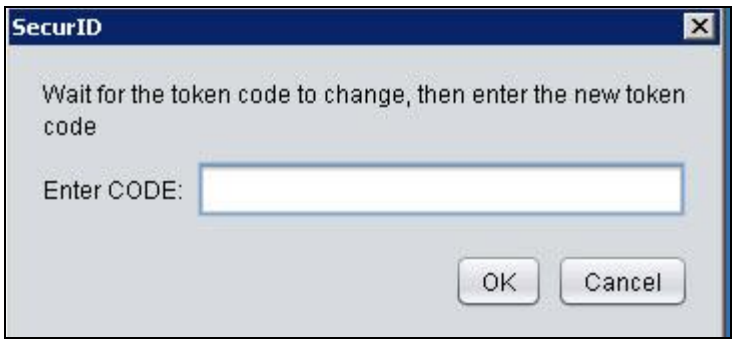
Login screen:

User-defined New PIN:



System-generated New PIN:

Next Tokencode:



Certification Checklist for RSA Authentication Manager

Date Tested: January 14, 2014

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.0	Virtual Appliance
Cryptzone AppGate Security Server	10.2.1	Proprietary
Cryptzone AppGate Client	10.2.1	Windows 7

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	✓

GLS

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

Appendix

Partner Integration Details	
RSA SecurID API	5.0.3
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	Designated Users
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	No

Node Secret:

To clear the node secret navigate the left hand tool bar to **Administration > Authentication Methods**.
Select **SecurID** and click on **Clear node secret** at the bottom of the screen.