Communication Devices, Inc.
Port Authority

RSA SecurID Ready Implementation Guide

Last Modified: December 3rd, 2012

Partner Information

Product Information	
Partner Name	Communication Devices, Inc.
Web Site	www.commdevices.com
Product Name	Port Authority
Version & Platform	10.10
Product Description	The Port Authority provides MultiPath plus Encrypted Side Band access to Routers, Firewalls, VOIP switches, and other network elements when conditions on the network deteriorate via an encrypted side channel or a secondary network, including Ethernet, analog telco circuits, or a cellular GPRS network.

Solution Summary

The Port Authority connects directly to a number of console ports and provides the highest level of protection regardless of the state of the network. This is done by maintaining an internal security database that is updated by a central database on an "as needed" basis. This internal database provides fast, reliable, two factor RSA SecurID authentication every time a technician accesses the router.

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication
List SAE Library Version Used	SAE 2.3
RSA SecurID User Specification	Designated Users
RSA SecurID Protection of Administrative Users	No
Issue RSA Software Token	No
RSA Software Token and RSA SecurID 800 Automation	No

Partner Authentication Agent Configuration

Before You Begin

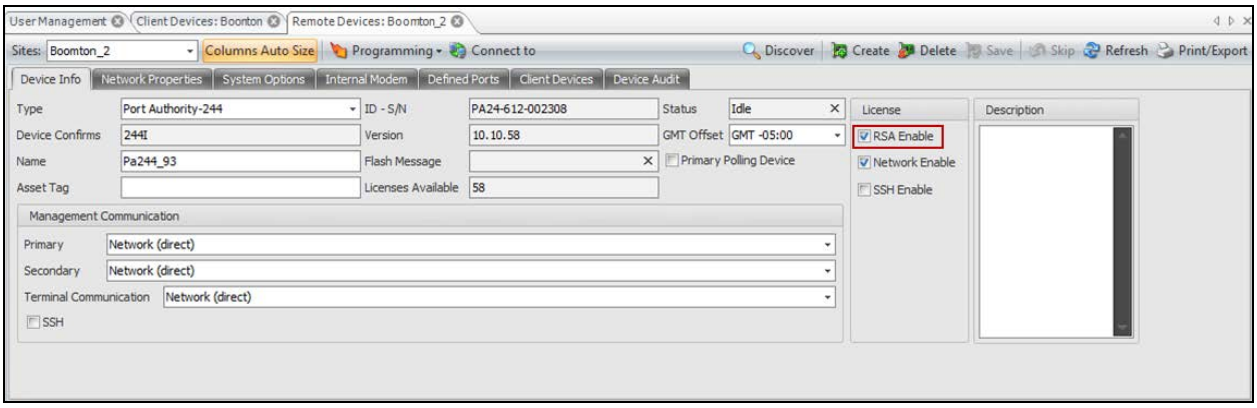
This section provides instructions for integrating the partners' product with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

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 vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuring the Port Authority Device

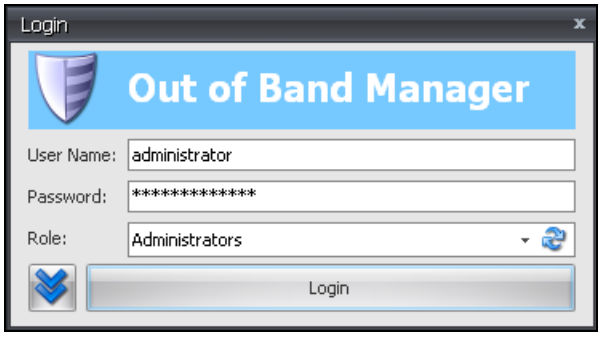
Before assigning RSA SecurID tokens to users on the Port Authority device, the device must be enabled for RSA SecurID. Please refer to the Port Authority product documentation for more information.



Configuring PIN Parameters

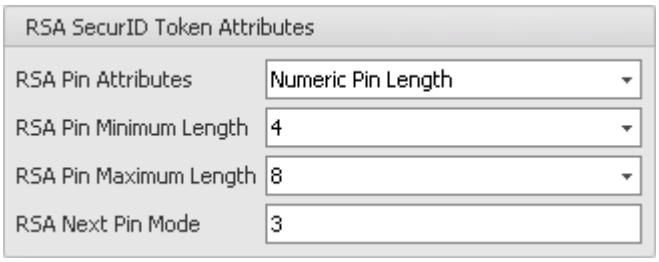
The attributes for the RSA PIN can be modified with the **Out of Band Manager**. To modify the PIN requirements, perform the following steps.

1. Login to the **Out of Band Manager**.



2. Select the **Common** tab → **System Settings** → **Global System Settings** tab → **Common System Settings** tab.

3. In the middle column, locate the **RSA SecurID Token Attributes** window.

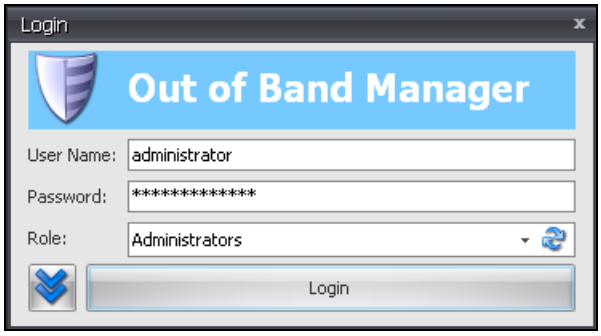


4. Make the appropriate changes and then select the **SaveChanges** button in the upper-right of the **Common System Settings** tab.

> **Note: Next Tokencode mode is referred to as "RSA Next Pin Mode" within the CDI software.**

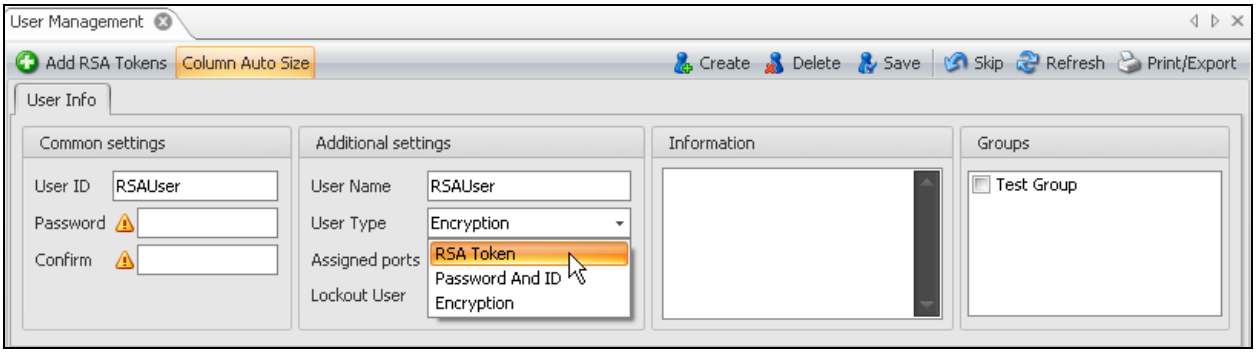
Assigning an RSA Token

1. Login to the **Out of Band Manager**.

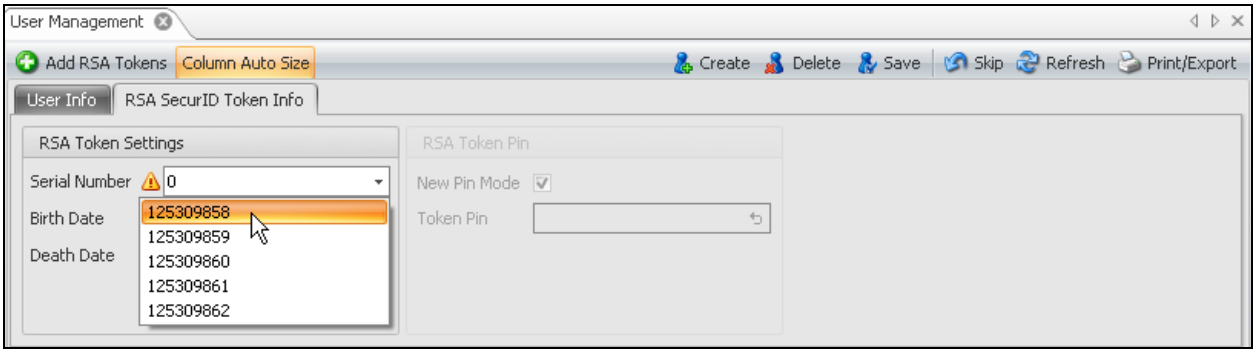


2. Select the **Security** tab →**Users** icon → **User Management** tab. Select an existing user by clicking on the username or create a new user by clicking the **Create** button.

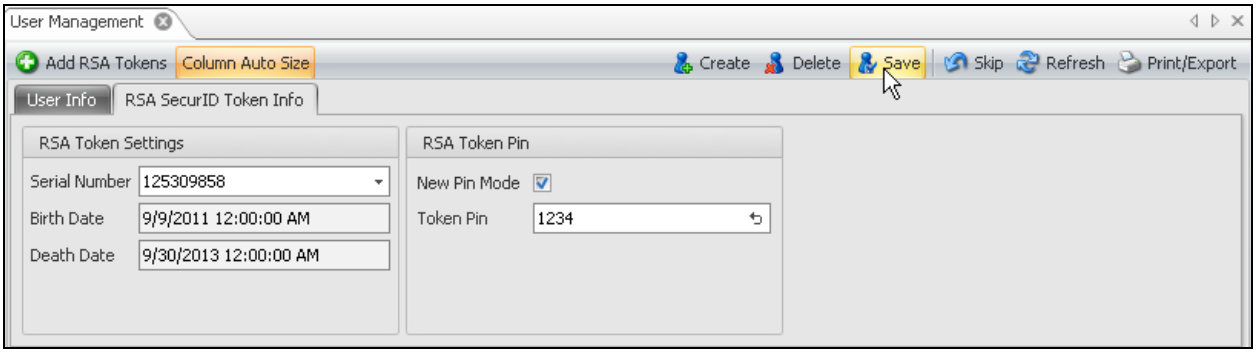
3. Once you have created or selected an existing user, in the **User Info** tab → **Additional settings**, pull down the **User Type** box and select **RSA Token**.



4. Next, select the **RSA SecurID Token Info** tab. Pull down the **Serial Number** box to the token you wish to assign to the user.



5. Check the **New Pin Mode** box. In **Token Pin**, enter a PIN for the user or select the back arrow ↩ to system generate a PIN.



6. Click the **Save** button

Note: The data must be synchronized between the Out of Band Manager Database and the device in order for the user to be prompted for SecurID authentication. Please use the "Program-Reload Device" option within the Out of Band Manager before attempting to authenticate.

Certification Checklist

Date Tested: December 3rd, 2012

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Engine	2.3	Microsoft Windows 7
CDI Port Authority	PA-244, 10.10.58	Proprietary
CDI Out of Band Manager	6.0.1.36B	Microsoft Windows 7

Authentication Functionality	
New PIN Mode	
Force Authentication After New PIN	✓
System Generated PIN	✓
User Defined (4-8 Alphanumeric)	✓
User Defined (5-7 Numeric)	✓
User Selectable	✓
Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	✓
PASSCODE	
16-Digit PASSCODE	✓
4-Digit Password	✓
Next Tokencode Mode	
Next Tokencode Mode	✓
Load Balancing / Reliability Testing	
Failover	✓
No Server available	✓

Administrative Functionality	
Server Down	
Client reports status message	✓
Client times out	✓
Administrative Functions	
Import tokens from XML file no password	✓
Import tokens from XML file with password	✓
Disable Token	✓
Assign a token	✓
Un-assign a token	✓
Auditing	
Audit record creation	✓
Successful authentication	✓
Failed authentication	✓
Report generation	✓

JJO / PAR

✓ = Pass ✗ = Fail N/A = Non-Available Function

Appendix

RSA Next Tokencode Mode vs. CDI RSA Next Pin Mode

RSA Next Tokencode Mode is a technology found in the RSA Authentication Manager product. CDI RSA Next Pin Mode is a technology implemented in the CDI products. When in RSA Next Tokencode mode, the user is required to input the next Tokencode generated after the valid PASSODE is accepted by the RSA Authentication Manager. When in CDI RSA Next Pin Mode, the user is required to input the next PASSCODE after the first valid PASSCODE is accepted by the CDI device. This differs from the RSA workflow in that the PASSCODE must be input by the user instead of just the Tokencode.