RSA Ready Implementation Guide for

RSA SecurID

Siemens RUGGEDCOM CROSSBOW 4.4

Daniel Pintal, RSA Partner Engineering
Last Modified: March 25, 2016

RSA READY

Solution Summary

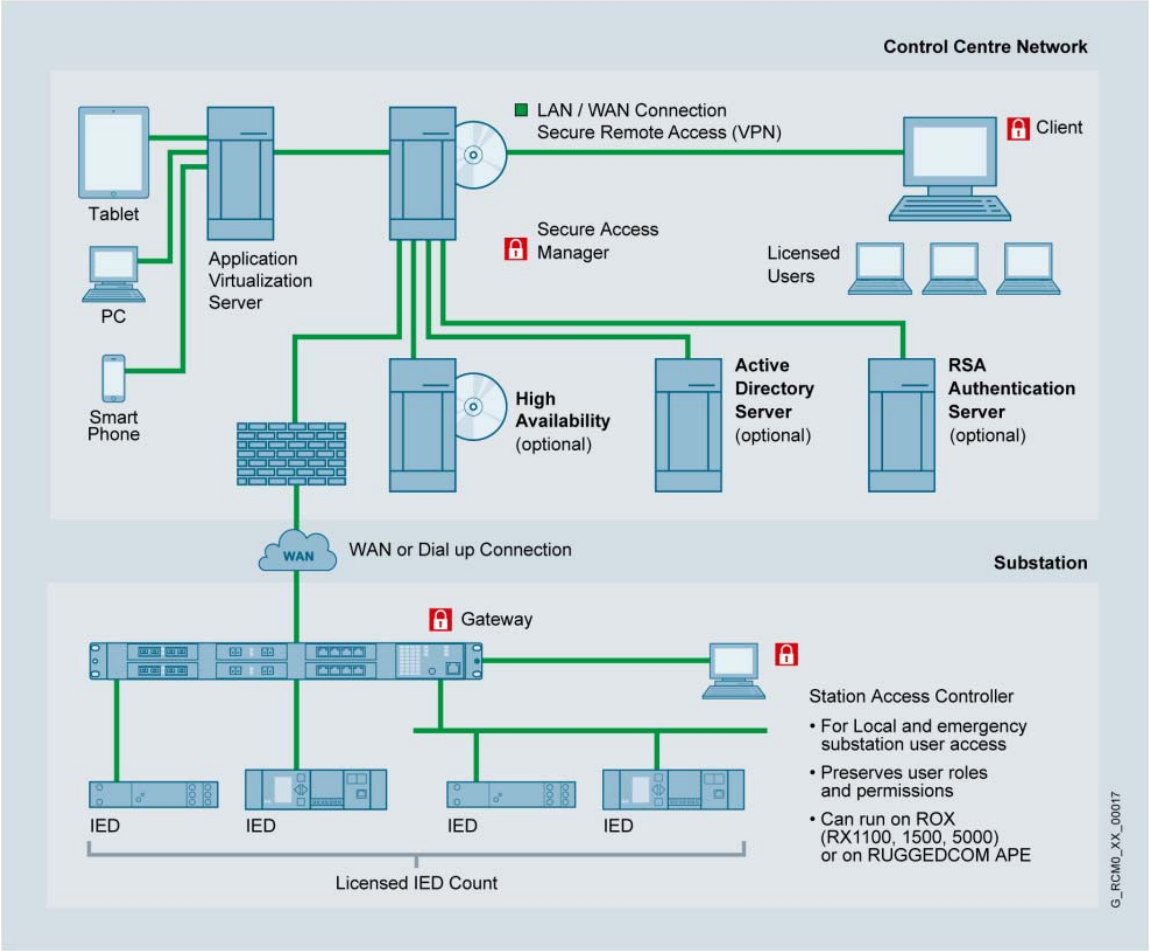
Siemens RUGGEDCOM's CROSSBOW application facilitates interactive communication with remote field IEDs (Intelligent Electronic Devices) using the IED manufacturer's proprietary maintenance applications. Data traffic is tunneled over a variety of communications media to the actual IED in the field. To the manufacturer's application, CROSSBOW appears as the IED.

Access to such devices must be closely controlled, so user authentication is required. Though a user may (and probably will) be on a remote client machine, all communication to the field must pass through the central CROSSBOW server. Before any communications is allowed, a client must logon to the server. RSA SecurID strong two-factor authentication is used to authenticate all users if the installed server is Siemens RUGGEDCOM's CROSSBOW Server (Product Number 6GK6000-2CA00-0AA0). This document applies to configurations using that server.

Once authenticated, an internal database on the server is consulted to determine what devices that user will be granted access to. Upon selecting a device, a communication session to the selected device is established, and the user can access it as if the device were locally connected to their computer.

RSA Authentication Manager supported features	
CROSSBOW 4.4	
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	No
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

- **Refer to Note below graphic on next page**



Important: The administrative interface in CROSSBOW clients is protected by RSA SecurID. The CROSSBOW server direct administrative interface is not protected by RSA SecurID.

RSA Authentication Manager Configuration

Agent Host Configuration

To facilitate communication between the Siemens RUGGEDCOM CROSSBOW Server 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 the Siemens RUGGEDCOM CROSSBOW Server and contains information about communication and encryption.

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

- Hostname
- IP addresses for network interfaces

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

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 Siemens RUGGEDCOM CROSSBOW Server will occur.

Partner Product Configuration

Before You Begin

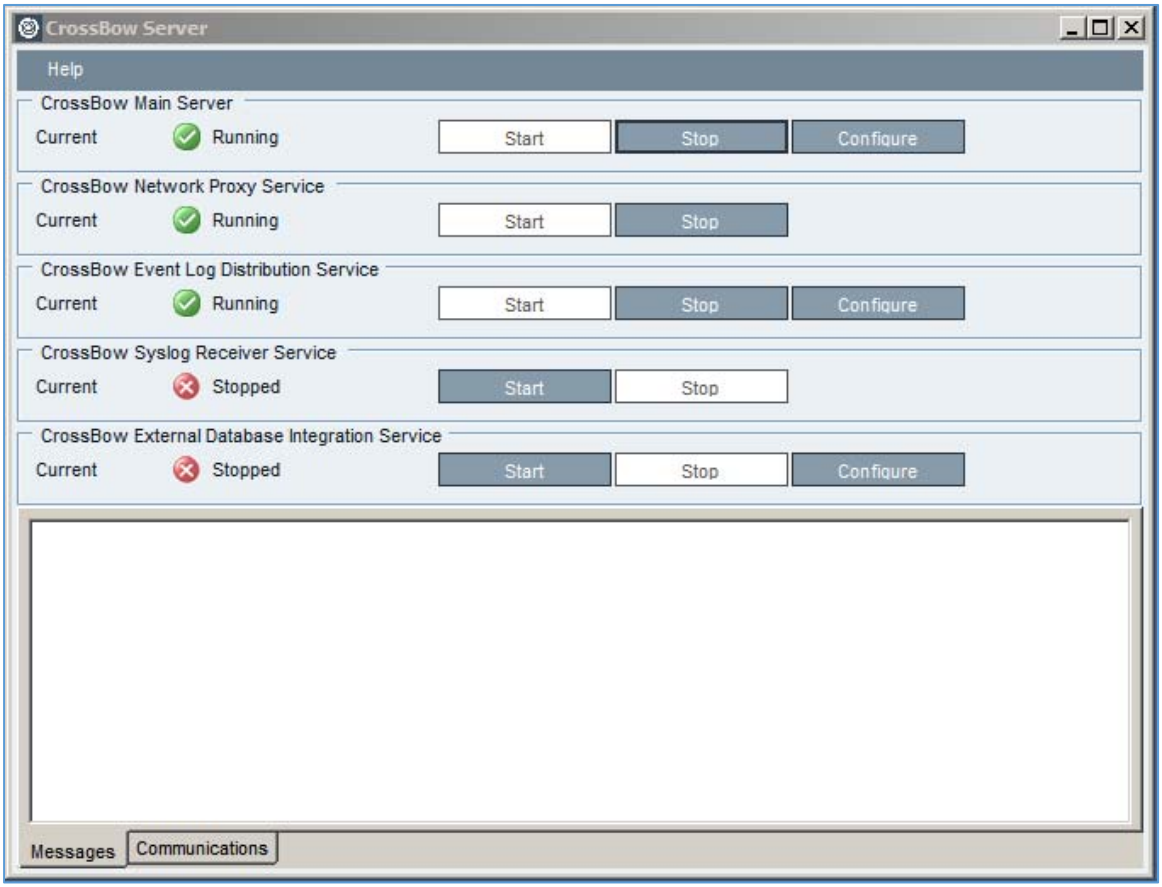
This section provides instructions for configuring the CROSSBOW Server with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

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.

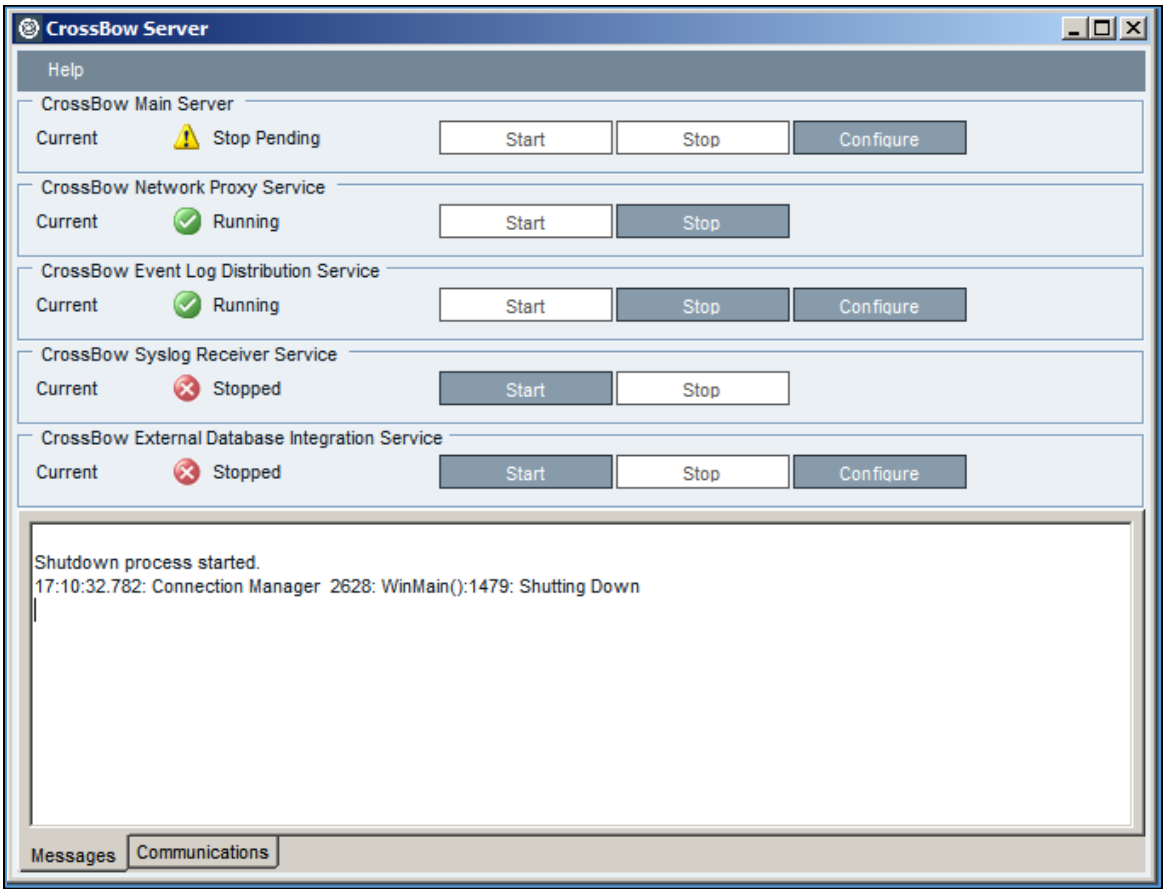
All CROSSBOW Server components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Siemens RUGGEDCOM CROSSBOW Server Configuration

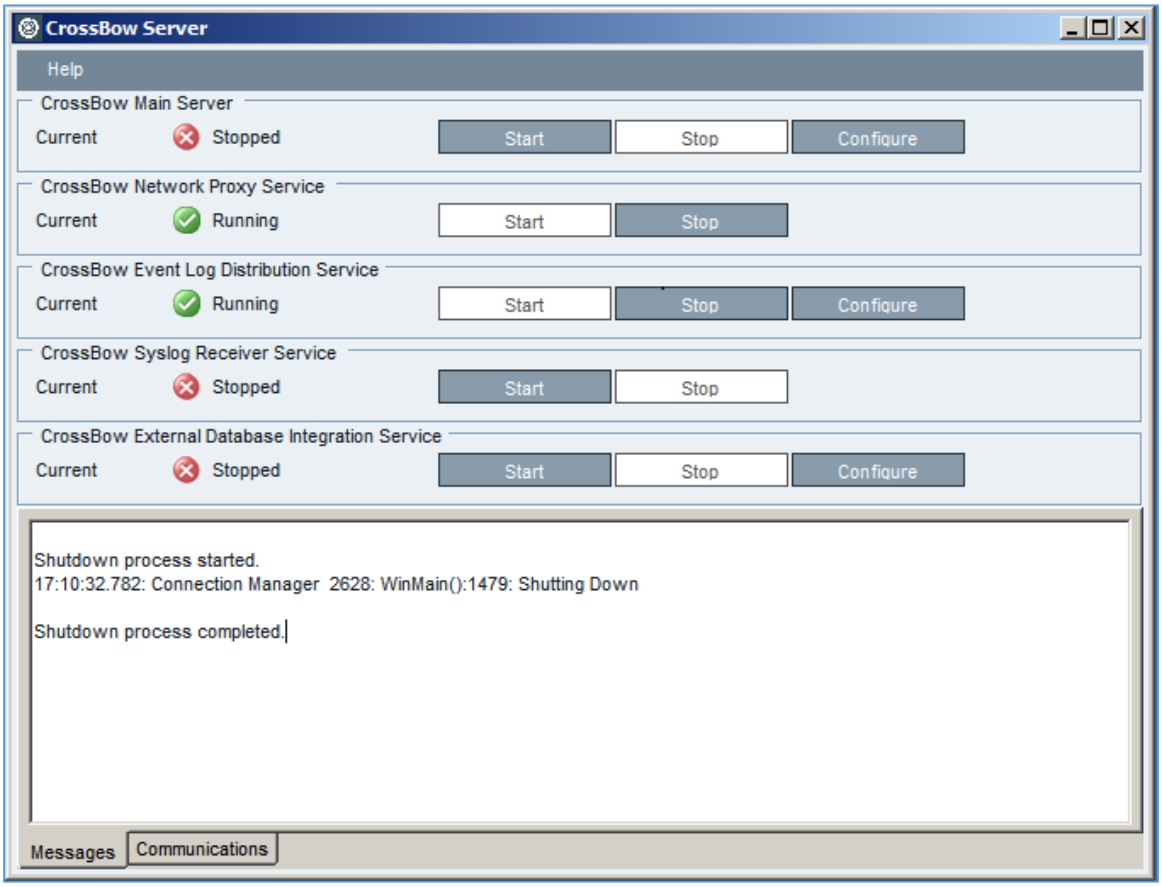
1. Copy the sdconf.rec file generated by the RSA Authentication Manager server into the C:\Windows\SysWOW64 directory on the CROSSBOW Server machine.
2. Open the CROSSBOW Server GUI.



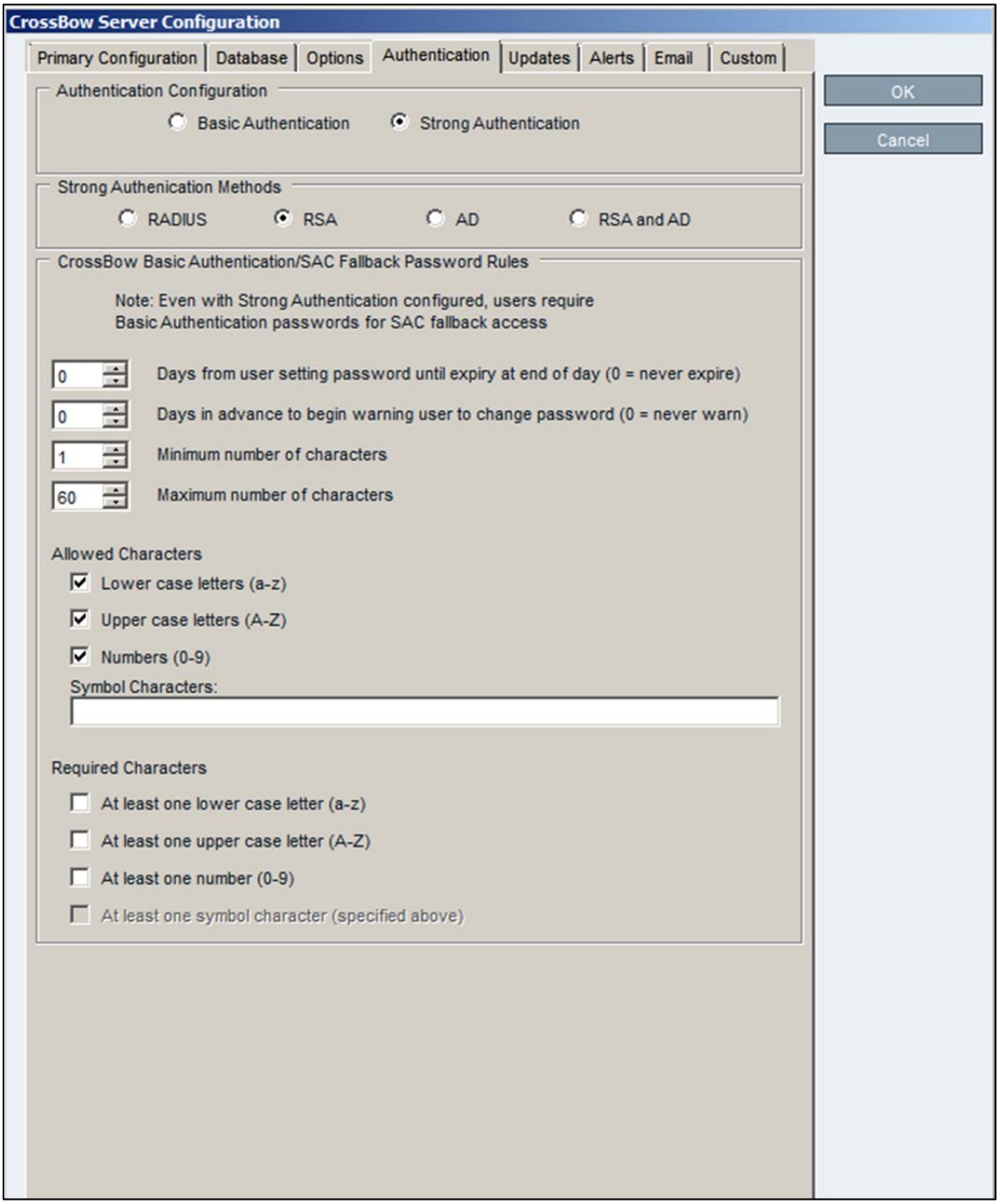
3. If the CROSSBOW Main Server status shows Running, click the **Stop** button for the CROSSBOW Main Server and wait for the status to change to Stopped.



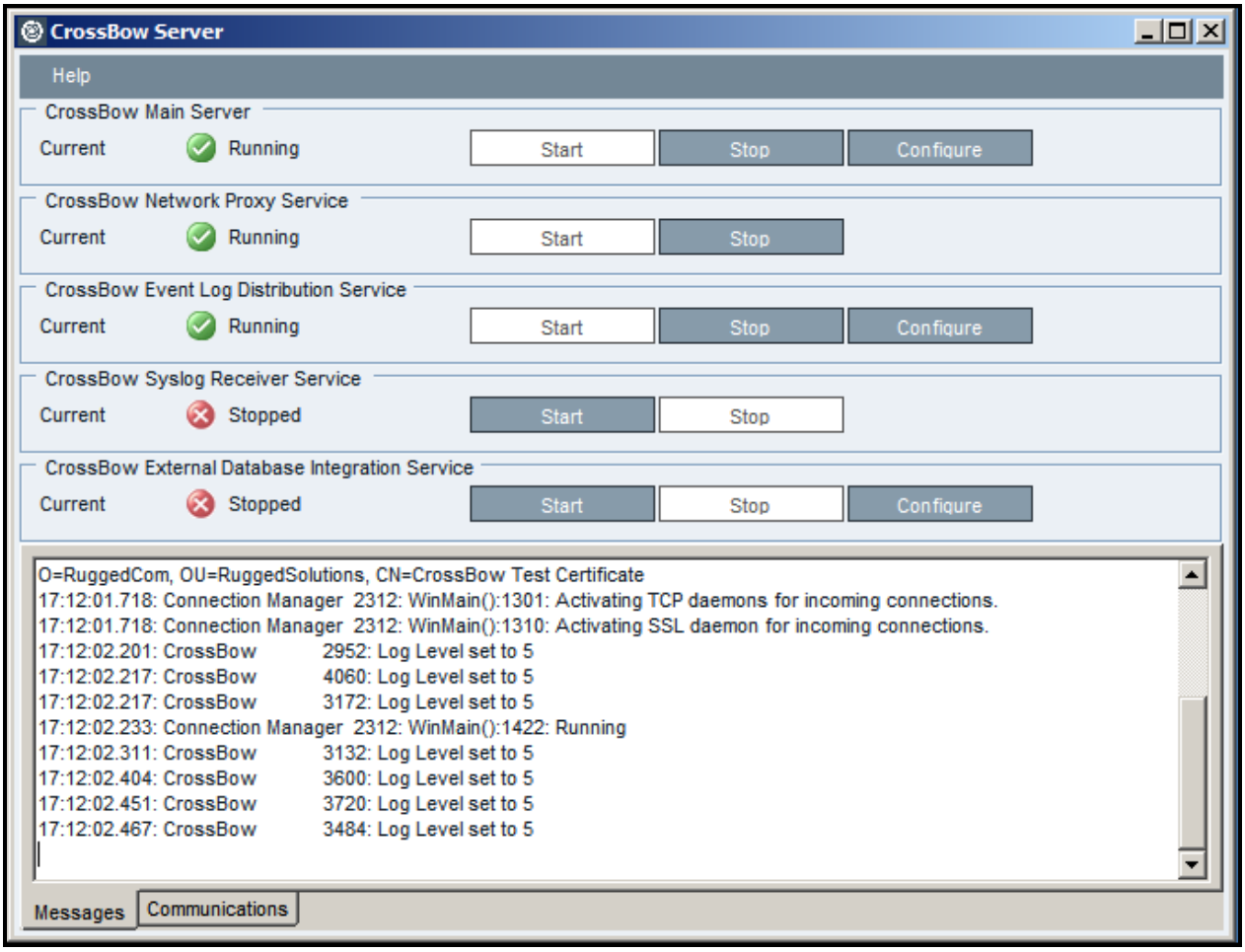
4. Click the **Configure** button to bring up the CROSSBOW Server Configuration form.



5. Click the **Authentication** tab within the CROSSBOW Server Configuration screen.
6. Click the **Strong Authentication** radio button.
7. Click the **RSA** radio button.
8. Click the **OK** button.



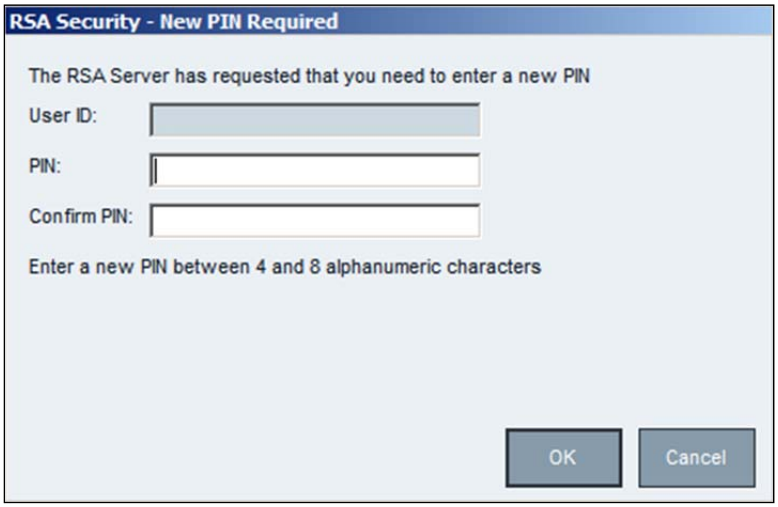
9. Click the **Start** button for the CROSSBOW Main Server in the CROSSBOW Server GUI.



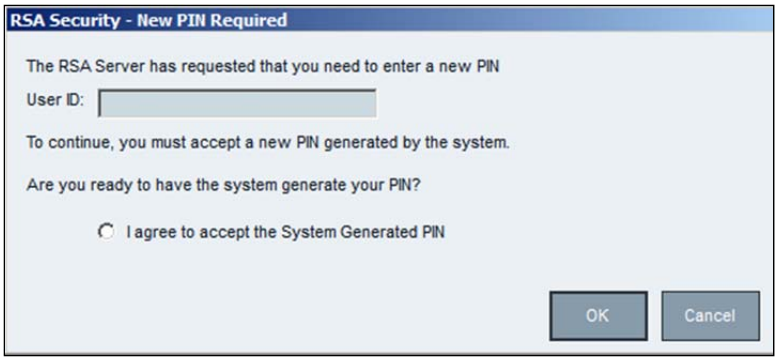
RSA SecurID Login Screens

Login screen:

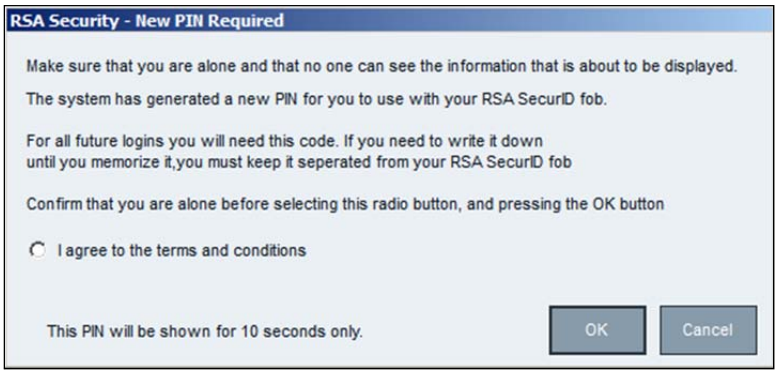
User-defined New PIN:



System-generated New PIN:



System-generated New PIN (Continued):



Next Tokencode:

Certification Checklist for RSA Authentication Manager

Date Tested: March 25, 2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.1	Virtual Appliance
CROSSBOW	v4.4	Windows Server 2008 R2

RSA SecurID Authentication

Date Tested: March 25, 2016

Mandatory Functionality	Native UDP	Native TCP	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

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

Appendix

RSA SecurID Authentication Files

RSA SecurID Authentication Files	
UDP Agent Files	**Location**
sdconf.rec	C:\Windows\SysWOW64
sdopts.rec	Not tested
Node secret	C:\Windows\SysWOW64
sdstatus.12 / jastatus.12	C:\Windows\SysWOW64

Partner Integration Details

Partner Integration Details	
RSA SecurID UDP API	8.1 C API
RSA SecurID TCP API	Not Implemented
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	All Users
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	No

Using Two RSA agents on one Agent Host

CROSSBOW can be installed alongside the RSA Control Center and either Agent may register with the Authentication Manager. The node secret file (securid) and sdconf.rec can be copied from whichever agent is first to register and be used by the other agent. Ex If RSA Control center registers first, the securid and sdconf.rec can be copied from C:\Program Files\Common Files\RSA Shared\Auth Data to C:\Windows\SysWOW64.

- Verify the agent host has been successfully registered with the authentication manager using the RSA Control Center.
- Verify the Node Secret and sdconf.rec resides in the correct directory as described below.
- Verify the RSA user exists in the CROSSBOW database.

Troubleshooting

API Details:

Node Secret:

The node secret (securid) is created after a successful authentication. The file resides in the C:\Windows\SysWOW64 directory. To clear the node secret, delete the **securid** file.

sdconf.rec:

The sdconf.rec file is copied to the C:\Windows\SysWOW64 directory on the CROSSBOW server.

sdopts.rec:

If needed, the sdopts.rec can be populated with the relevant information and resides in the C:\Windows\SysWOW64 directory.

sdstatus.12:

Sdstatus.12 is located in the C:\Windows\SysWOW64 and should be deleted if the node secret is cleared.