Forum Systems
Forum Sentry

RSA SecurID Ready Implementation Guide

Last Modified: December 15th, 2014

Partner Information

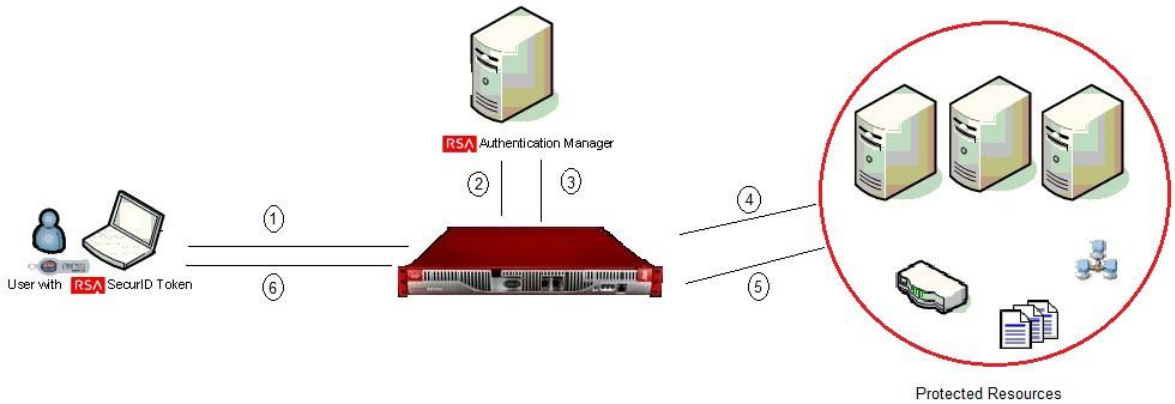
Product Information	
Partner Name	Forum Systems
Web Site	www.forumsys.com
Product Name	Forum Sentry
Version & Platform	8.3 for Windows and Linux
Product Description	Forum Sentry – deployed as a hardware appliance, software gateway or a Cloud-based instance – seamlessly controls access to services, protects information through data-level encryption, ensures the integrity of a message through signatures, and controls corporate information flow. Forum Sentry industry specific solutions include: government compliance, secure electronic forms, secure partner integration, secure partner collaboration, electronic notary, and evidence repository within a Service Oriented Architecture.

Solution Summary

XML Gateways are central to Service Oriented Architecture (SOA) for their ability to integrate services securely. Typically deployed as a hardware appliance, an XML Gateway seamlessly controls access to services, protects information through data-level encryption, ensures the integrity of a message through signatures, and controls corporate information flow. HTML/JSON traffic from portals as well as XML/ SOAP messages from application-to-application communication are protected via XML Gateways, sometimes also referred to as SOA Gateways.

This document provides an overview of configuring Forum Sentry for use with RSA SecurID Authentication. In this solution, Forum Sentry is configured as an Authentication Agent on the RSA Authentication Server to manage end user access to back end web services, applications or any number of back end resources that need to be exposed and controlled.

RSA Authentication Manager supported features	
Forum Systems Forum Sentry 8.3	
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



Agent Host Configuration

To facilitate communication between Forum Sentry 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 Forum Sentry 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

> **Note: 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 Forum Sentry will occur.

Partner Product Configuration

Before You Begin

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

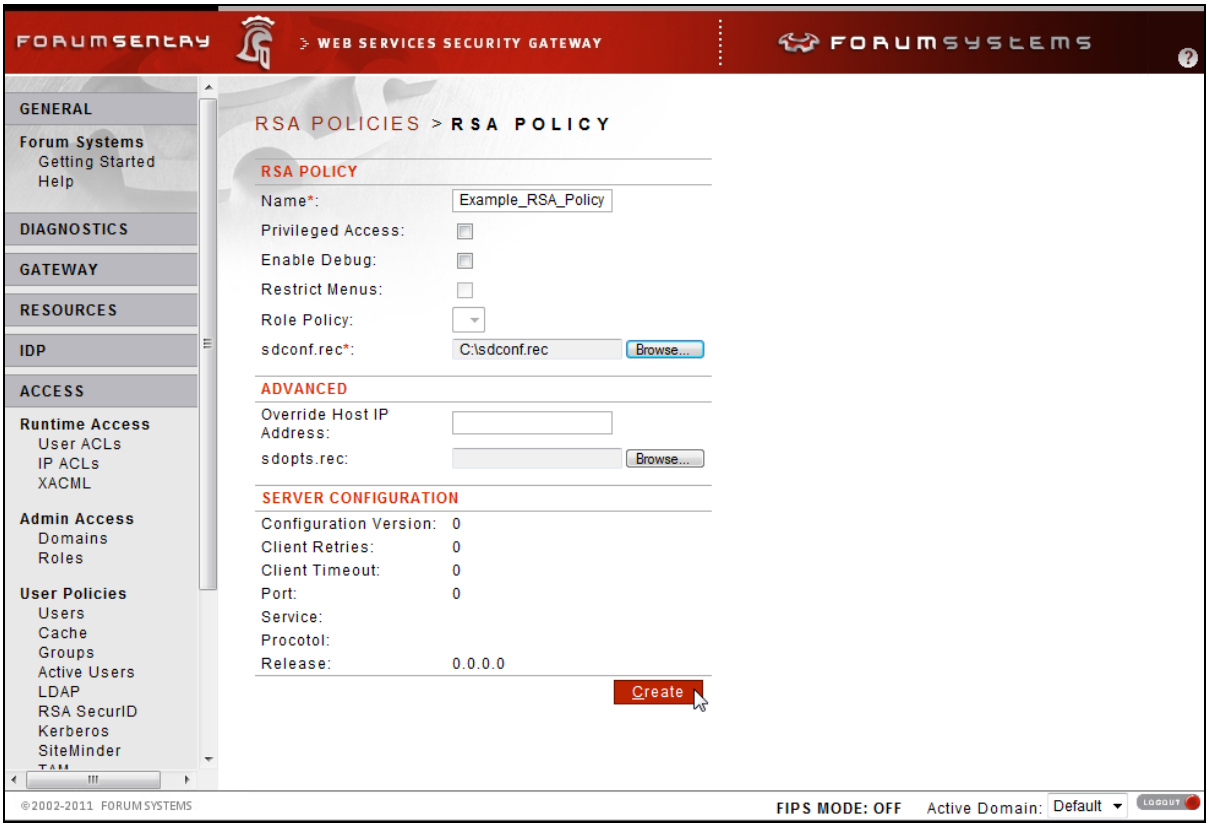
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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

Configure Forum Sentry for RSA SecurID Authentication

1. Logon to the Forum Systems Forum Sentry web administrative interface using an administrative account and browse to **ACCESS** > **User Policies RSA SecurID** and click **New**.

2. Configure the **RSA Policy** and click **Create** to save it.

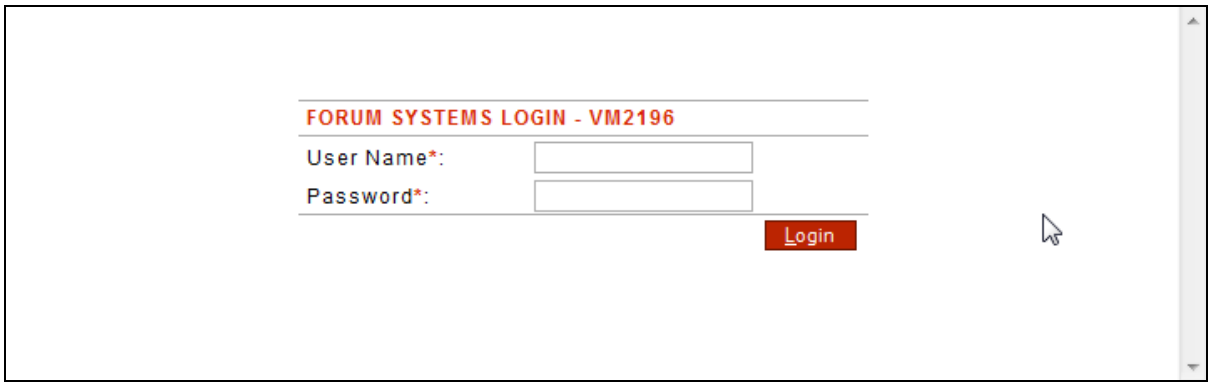


- Enter the policy name in the **Name** field.
- Browse to the location of the **sdconf.rec** configuration file.
- Enter an IP address in **Override Host IP Address** to manually set the IP the RSA library binds to.

The green STATUS light indicates that the RSA Policy is now active and is ready to perform RSA SecurID Authentications.

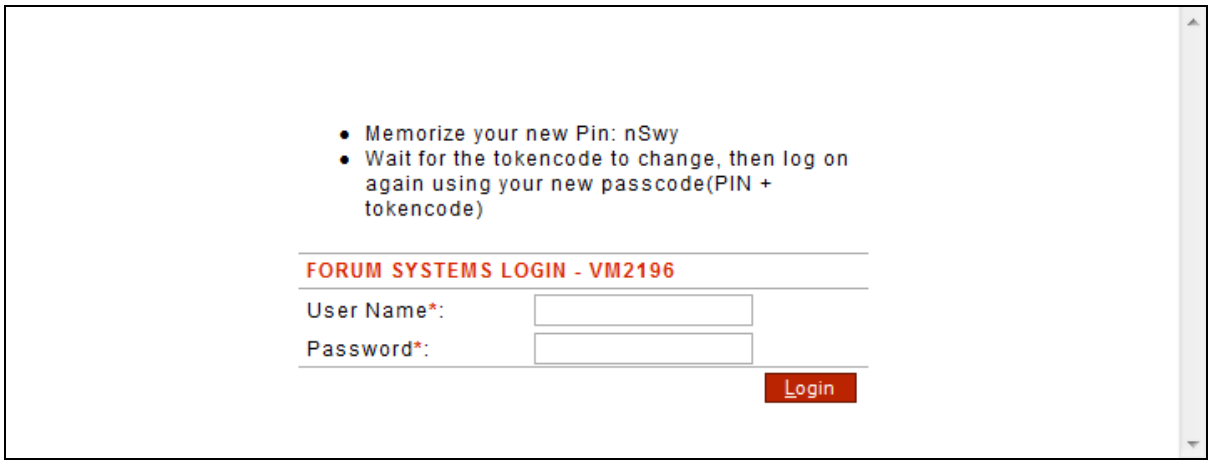
RSA SecurID Login Screens

Login screen:

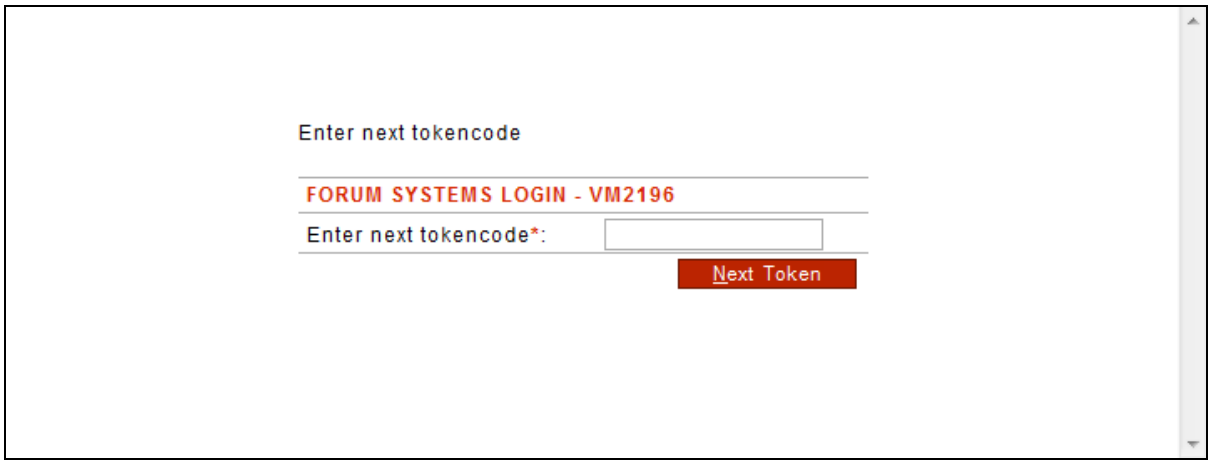


User-defined New PIN:

System-generated New PIN:



Next Tokencode:



Certification Test Checklist for RSA Authentication Manager

Certification Environment

Product Name	Version Information	Operating System
RSA Authentication Manager	8.1	Virtual Appliance
Forum Systems Forum Sentry	8.3.386 64bit	Windows Server 2012

RSA SecurID Authentication

Date Tested: December 15th, 2014

Mandatory Functionality	RSA Native UDP Agent	RSA Native TCP Agent	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

PEW

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

Appendix

RSA SecurID Authentication Files

RSA SecurID Authentication Files	
UDP Agent Files	**Location**
sdconf.rec	In memory
sdopts.rec	In memory
Node secret	In memory
sdstatus.12 / jastatus.12	In memory

Partner Integration Details

Partner Integration Details	
RSA SecurID UDP API	8.1.1 for Java
RSA SecurID TCP API	N/A
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	All users
Display RSA Server Info	Yes
Perform Test Authentication	No
Agent Tracing	Yes

Node Secret:

To clear the node secret, logon to the Forum Systems Forum Sentry web administrative interface using an administrative account and browse to **ACCESS** > **User Policies** > **RSA SecurID.** Mark the checkbox for your RSA Policy and click **Clear Node Secret**. Reboot the system or restart the Forum Sentry service to reinitialize the RSA agent.

sdconf.rec:

To manage the sdconf.rec configuration file, logon to the Forum Systems Forum Sentry web administrative interface using an administrative account and browse to **ACCESS** > **User Policies** > **RSA SecurID.** Click **Delete** to remove or open the **RSA Policy** and browse to and upload a new **sdconf.rec** file. Reboot the system or restart the Forum Sentry service to reinitialize the RSA agent.

sdopts.rec:

To upload an sdopts.rec file, logon to the Forum Systems Forum Sentry web administrative interface using an administrative account and browse to **ACCESS** > **User Policies** > **RSA SecurID**. Open your RSA Policy and click **Browse** to upload an **sdopts.rec** file**.** Reboot the system or restart the Forum Sentry service to reinitialize the RSA agent.