

FORUM SYSTEMS SENTRYTM VERSION 9.1 RSA SECURID INTEGRATION GUIDE



Legal Marks

No portion of this document may be reproduced or copied in any form, or by any means – graphic, electronic, or mechanical, including photocopying, taping, recording, or information retrieval system – without expressed permission from Forum Systems, Inc.

FORUMOS[™] Firmware, Forum Systems XMLSec[™] WebAdmin, Forum Systems XML Security Appliance[™], Forum Sentry[™], Forum Presidio[™], Forum XWall[™] Forum Sentry[™] Web Services Gateway, Forum Presidio[™] OpenPGP Gateway, Forum FIA Gateway[™], Forum XWall Type-PCI[™], Forum XWall[®] Web Services Firewall and Forum XRay[™] are trademarks and registered trademarks of Forum Systems, Inc.

All other products are trademarks or registered trademarks of their respective companies.

Copyright © 2002-2020 Forum Systems, Inc. – All Rights Reserved.

Forum Systems Sentry™ Version 9.1 RSA SecurID Integration Guide, published January 2021.

D-ASF-SE-029972

Table of Contents

INTRODUCTION TO THE RSA SECURID INTEGRATION GUIDE	1
Audience for the RSA SecurID Integration Guide	1
Conventions Used	1
RSA SecurID Background	2
RSA SecurID Support on the System	3
RSA SecurID Concepts and Definitions	3
RSA SECURID CONFIGURATION WITH FORUM SENTRY	4
Authentication Agent Configuration	4
Configure Sentry with RSA SecurID	4
RSA SecurID Policy Creation Screen Terms	6
RSA SecurID Access Examples	6
WebAdmin Administration with RSA SecurID	7
Initial Login for Web Admin User Accounts	9
Using RSA SecurID User for Runtime Access1	1
APPENDIX	3
Appendix A - RSA SecurID References1	3

INTRODUCTION TO THE RSA SECURID INTEGRATION GUIDE

Audience for the RSA SecurID Integration Guide

The Forum Systems Sentry[™] Version 9.1 RSA SecurID Integration Guide is for System Administrators and policy developers who will manage access control to the Forum Sentry WebAdmin interface and build runtime policies using two factor authorization/authentication leveraging Sentry's integration with RSA SecurID.

Conventions Used

A red asterisk (*) aligned with a field term means that this field is required. In this and other documentation, the Web Administration Interface is referred to as the WebAdmin and the Forum Sentry API Gateway[™] is referred to as the 'device', 'product' or 'system'.

In this document, all data or commands that must be entered or selected are displayed in boldface. Example:

User name: **johnsmith** Password: *******

UI screens which display a STATUS column represent the following states:

- Green status light = enabled policy.
- Red status light = disabled policy.

Throughout this and other documents in the Documentation Set, repetitive actions not always shown, this includes:

- View / edit a policy
- Enable / disable a policy
- Delete a policy
- Rename a policy
- Limit display of policies with Search or Max Results fields.

For more information, refer to the Common Operations section of the *Forum Systems Sentry*[™] Version 9.1 Web-based Administration Guide.

Customers with plug-in licenses on the system, confirm that your Integration License is visible on the General Info screen under the SUPPORTED FEATURES section.

Any specifications and constraints referenced in this volume appear in the Appendices of this volume.

RSA SecurID Background

RSA SecurID is a mechanism developed by RSA Security for performing two-factor authentication for a user to a network resource. The RSA SecurID authentication mechanism consists of:

- 1) A "token" generator either hardware or software
- 2) Authentication Agents
- 3) RSA SecurID Server

Authentication Agents are records in the RSA Authentication Manager database that contain information about the systems for which RSA SecurID authentication is provided. For the purposes of this document, Forum Sentry instances are the Authentication Agents.

The token generator is assigned to a user and generates an authentication code at fixed interval (usually 60 seconds) using a built-in clock and factory encode random key (seed). The seed is different for each and is loaded into the corresponding RSA SecurID server.

The RSA SecurID Server is used to manage authentication agents, user accounts and token generator assignments.

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 enable two factor authentication to the Sentry WebAdmin interface or 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 SecurID Support on the System

Sentry's WebAdmin portal can be used to manage RSA SecurID configuration and supports RSA SecurID tokens for both administrative and run-time access to policies in Sentry. The WebAdmin is a web-based management interface used for monitoring as well as configuring all aspects of Forum Sentry including server, security and network policies.

RSA SecurID Concepts and Definitions

The following table defines various RSA SecurID terms and concepts:

CONCEPT	DEFINITION
Sdconf.rec	The RSA Authentication Manager configuration file.
token	Hardware or software generated and assigned to a user which generates an authentication code.
Sdopts.rec	RSA Authentation Manager optional configuration file.
Authentication agent	Records in the RSA Authentication Manager database that contain information about the systems for which RSA SecurID authentication is provided.
RSA Authentication Manager	The server where RSA Authentication Console has been installed on and is used to manager RSA users, agents, and tokens. It is expected that the reader has access to and working knowledge of the RSA Server.

RSA SECURID CONFIGURATION WITH FORUM SENTRY

Configuring Forum Sentry for use with RSA SecurID involves creating an authentication agent in RSA SecurID that corresponds to the Forum Sentry instance, creating user accounts, and assigning tokens to the user accounts. Forum Sentry is then configured to reference the RSA SecurID server. Lastly, RSA policies are created in Forum Sentry for either runtime or administrative access.

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:

Forum Sentry Hostname Forum Sentry IP Addresses

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.

Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.

Configure Sentry with RSA SecurID

1. Log on to the WebAdmin and navigate to ACCESS → User Policies → RSA SecurID. On the RSA POLICIES screen, select the New button to create RSA Policy.

FORUMSERER	يًا ا	> API S	ECURITY GATEW	AY	€¢ F	ORUMSYS	LEMS 🕑
IDP			-				*
ACCESS	R	SA POLI	CIES				
Runtime Access User ACLS IP ACLS XACML Admin Access Domains Roles User Policies Users Cache User Groups Active Users LDAP RSA SecurID Kerberos SiteMinder TAM WebSeal Oracle AM ClearTrust HP SelectAccess		NAME No items to disp	STATU S play	SERVERS	PORT	PROTOCOL	New
2001-2014 FORUM SYSTEMS, INC.		English	T		Active	Domain: Default 🔻	(LOGONT 🥚

2. On the RSA Policy creation screen, enter the RSA Server Manager information.

FORUMSERERY	🛱 > API SECURI	TY GATEWAY		C FORUMSYSLEM	is 🕐
ACCESS					Ê
Runtime Access	RSA POLICIES >	RSA POLICY			
IP ACLS	R SA POLICY				
XACML	Name*:				
Admin Accoss	Privileged Access:				
Domains	Enable Debug:				
Roles	Restrict Menus:				
User Policies	Role Policy:	•			
Cache User Groups	sdconf.rec*:	Choose File No file chosen			
Active Users	ADVANCED				
RSA SecurID	Rsa Agent Host:				
Kerberos SiteMinder	sdopts.rec:	Choose File No file chosen			
TAM	SERVER CONFIGURAT	ION			
WebSeal Oracle AM	Configuration Version:	0			
ClearTrust	Client Retries:	0			
HP SelectAccess	Client Timeout:	0			
WS-Trust	Port:	0			
OpenAM DEST	Service:				
Sentry	Procotol:				
Custom	Release:	0.0.0.0			
SYSTEM			<u>C</u> reate		
PARTNERS					-
© 2001-2014 FORUM SYSTEMS, INC.	English	•		Active Domain: Default 🔻	106017 🔴

The required options are the Name and sdconf.ref file. Refer to the following table for a detailed description of all options on the RSA Policy creation screen. When creating an RSA policy for WebAdmin administrative account, check the "Privileged Access" option. Otherwise, leave this option unchecked when creating an RSA policy for runtime access.

3. Select the Create button to create the RSA policy.

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

FORUMSERERS	a 🤉 web services secur	ITY GATEWAY		😂 FOR	umsyst	EMS	8
GENERAL Forum Systems	RSA POLICIES						
Getting Started	NAME	STATUS	SERVERS		PORT	PROTOCOL	
Therp	Example_RSA_Policy		ps032.pe.rsa.net(1	10.100.50.32)	5500	udp	
DIAGNOSTICS			<u>C</u> lear Node Secret	De <u>l</u> ete	<u>E</u> nable <u>D</u>	isable <u>N</u> ew	
GATEWAY							

RSA SecurID Policy Creation Screen Terms

The RSA SecurID configuration screen includes the following terms and definitions:

TERM	DEFINITION
Name	The name this RSA SecurID policy will be referenced by.
Privileged Access	When enabled, the user has access to the WebAdmin as a super user.
Enable Debug	Enables debug log level logs to be created.
Restrict Menu	Enables restricting menus for WebAdmin users.
Role Policy	When restricting menus, the Role Policy dictates which menus the WebAdmin users have access to.
sdconf.rec	The Choose File button allows for the RSA Authentication Manager Configuration file to be selected and uploaded to Sentry. It is also made available for download from Sentry once imported.
RSA Agent Host	Indicates the IP address of the agent host in the Authentication Manger database.
sdopts.rec	The Choose File button allows for the RSA Authentication Manager optional configuration file to be uploaded to Sentry. It is also made available for download from Sentry once imported.
Configuration Version	The version of the sdconf.rec file that is in use. For Authentication Manager 5.1 or later, this number is 14.
Client Retries	The number of times the agent sends authentication data to the Authentication Manager before a timeout occurs.
Client Timeout	The amount of time (in seconds) that the agent waits before resending authentication data to the Authentication Manager.
Port	UDP port of the Authentication Manager authentication service
Service	Name of the RSA Authentication Manager authentication service
Release	The version number of the RSA Authentication Manager
Servers	The IP address that the agent uses to communicate with the server. This address could be the actual IP address of the server you have selected, or it could be an alias IP address assigned to the server. An IP address of 0.0.0.0 indicates that the agent has not yet received communication from the server.

RSA SecurID Access Examples

Examples for working with RSA SecurID access include:

- Accessing Forum Sentry WebAdmin using RSA SecurID user with token generator
- Using RSA SecurID(with token) user for runtime access

Note: RSA SecurID user accounts can also be configured for runtime or administrative access to Sentry without the use of tokens. When the user account is configured this way, authentication is achieved using the user account name and password (RSA pin) only without a token.

WebAdmin Administration with RSA SecurID

 To use an RSA policy for WebAdmin administration, ensure that the "Privileged Access" option is enabled in the RSA policy (note that the "Privileged Access" option enables full access, it is also possible to provided limited access). Then log into the Sentry WebAdmin interface and navigate to Access → Admin Access → Domains.

FORUMSERLAY	🚡 > API SECURITY GATEWAY	🛠 FORUMSYSLEMS	?
RESOURCES IDP ACCESS Runtime Access User ACLs IP ACLS XACML Admin Access Domains Roles User Policies Users	PI SECURITY GATEWAY D O MAIN MANAGEMENT CREATE NEW DOMAINS Add one Domain name per line	S FORUMSYSLEMS	
Cache User Groups Active Users LDAP RSA SecurID Kerberos SiteMinder TAM WebSeal Oracle AM ClearTrust HP SelectAccess WS-Trust OpenAM REST Sentry Custom	Delete		
PARTNERS			•

On the DOMAIN MANAGEMENT screen, select or create the Domain to use for WebAdmin administration.

2. On the DOMAIN DETAILS screen, note that an RSA group has automatically been created and added to the listing of available groups to select. The group name will be the name of the RSA policy that was created prefixed with "RSA-".

FORUMSERLAY	🛱 > API SECURITY GATI	EWAY		🛠 FORUMSYSLEMS	?
RESOURCES	DOMAIN MANAGEMEN	NT > DOMA	IN DETAI	LS	-
IDP	DOMAIN DETAILS				
ACCESS	Domain Name: Default				
Runtime Access User ACLs IP ACLs XACML	Restrict Menus: 📄 Role policy: 🔽				
Admin Access	# GROUP	READ WR	TE		
Domains	1 🖶 <u>RSA-RSA SecurID</u>)		
Roles	2 🛧 Local Admins	 Image: A start of the start of)		
User Policies Users Cache User Groups Active Users LDAP RSA SecurID Kerberos SiteMinder TAM WebSeal Oracle AM ClearTrust HP SelectAccess WS-Trust OpenAM REST Sentry Custom		<u>S</u>	IVE		
PARTNERS					+
© 2001-2014 FORUM SYSTEMS, INC.	🔚 English 🔻			Active Domain: Default ▼	60UT 🔴

Select the READ and/or WRITE check box(es) next to the RSA group to enable the appropriate administrative access for the RSA user accounts. Select the Save button to commit the changes.

3. Once the domain has been modified or created, navigate to the System → Settings → System and select that domain under the Web Admin Domain Policy field.

FORUMSERERY	🔓 > API SECURITY GATE	VAY	C FORUMSYSLEMS	?
DIAGNOSTICS	SYSTEM SETTINGS			Î
GATEWAY	WEB ADMIN SETTINGS			
RESOURCES	Web Admin Port*:	5050		
IDP	Web Admin Domain Policy*: Web Admin IP ACL Policy*:	Default View Edit		
ACCESS	GLOBAL DEVICE MANAGEMENT	(GDM) SETTINGS		
SYSTEM	GDM Port*:	5070		_
Settings System Control	GDM Domain Policy*: GDM IP ACL Policy*:	Default v Edit Unrestricted v Edit		
Preferences	SSH SETTINGS			

8 I Forum Systems Sentry[™] Version 9.1 RSA SecurID Integration Guide

Initial Login for Web Admin User Accounts

For new RSA user accounts that have not been initialized – a PIN has not been generated for the user account – the user account can be initialized via the Sentry WebAdmin interface. There are two options for initializing an RSA user account via the WebAdmin interface:

- 1. The PIN can be entered by the user during initial login.
- 2. A PIN can be generated by the RSA system and presented to the user during the initial login,

Note: RSA SecurID user accounts can also be configured for administrative access to Sentry without the use of tokens. When the user account is configured this way, authentication is achieved using the user account name and password (RSA pin) only without a token.

Login Screen:

Once the RSA Policy has been created, an RSA Server Manger account can be used to log into Forum Sentry at the login prompt per the figure below.

FORUM SYSTEMS LC)GIN -	
User Name*:	username]
Password*:]
		Login

User-defined New PIN:

If the RSA Server is configured to allow users to generate their own PIN's, an initial password set by the RSA Server administrator should be used with the user account to first log into Forum Sentry. Subsequently, obtain the initial PIN from the RSA Server administrator.

Log into Forum Sentry with the username and the initial PIN provided by the RSA Server administrator. A prompt will be displayed to create and confirm a new user PIN. Any PIN restrictions regarding PIN length or usable characters is also displayed.

Enter a new pin.The pin numbers	should be between 4 a	nd 8 letters or
FORUM SYSTEMS LOGI	N -	
New Pin*:]
Confirm Pin*:		
		New Pip

Enter a new PIN and then select the *New Pin* button to confirm and create the user PIN. You will then be returned to the Forum Sentry login page to use the user account name, PIN and token pass code to log in.

Note: The user account password is now the combination of both the PIN and the token pass code. For instance, if the user account PIN is "abc1234", and the current token pass code is "6633 7639", then the password is "abc123466337639".

System-generated PIN:

For system generated PIN's, log into Forum Sentry using the assigned username and just the current token code only. A new system generated PIN will be displayed which must be used with all subsequent logins. Record the PIN when displayed as this is the only time Forum Sentry will present the system generated PIN.

 Memorize your new Pite: TIAL Wait for the next tokencode to login 						
FORUM SYSTEMS LOGIN -						
User Name*:	username					
Password*:						
		Login				

Using RSA SecurID User for Runtime Access

Runtime Access

User ACLs IP ACLs

Admin Access

Domains Roles

User Policies Users

 To use and RSA policy for runtime access, ensure that the "Privileged Access" option is NOT enabled in the RSA policy. Then log into the Sentry WebAdmin interface and navigate to Access → Runtime Access → User ACLs.

FORUMSERERY	🛱 🔅 API SECURITY GATEWAY		C FORUMSYSLEMS
GENERAL	USER ACL MANAGEMENT		
DIAGNOSTICS			
GATEWAY	CREATE NEW ACCESS CONTROL LISTS		-
GATEMAT	Add one ACL name per line		
RESOURCES	RSA_User_ACL		
IDP			
ACCESS			
Runtime Access User ACLs IP ACLs		<u>C</u> reate	
	ACCESS CONTROL LIST		_
Admin Access Domains Roles	No items to display		
		De <u>l</u> ete	
User Policies Users Cache			
FORUMSERLAY	🛱 🗇 API SECURITY GATEWAY		V FORUMSYSLEMS
GENERAL	- A MORENE		
DIAGNOSTICS	USER ACL MANAGEMENT		
GATEWAY	CREATE NEW ACCESS CONTROL LISTS Add one ACL name per line		
RESOURCES			
IDP			
ACCESS			

Select an existing user ACL or enter the name of a new ACL and select the create button.

ACCESS CONTROL LIST

RSA User ACL

Create

Delete

2. On the USER ACL DETAILS screen, note that an RSA group has automatically been created and added to the listing of available groups to select. The group name will be the name of the RSA policy that was created prefixed with "RSA-".

FORUMSERERS	API SECURITY GATEWAY	S FORUMSYSLEMS	
GENERAL			
DIAGNOSTICS	USER ACE MANAGEMENT - USER ACE DETAILS		
GATEWAY	USER ACL DETAILS ACL Name: BSA User ACL		
RESOURCES	# USER GROUP	EXECUTE	
IDP	1 + RSA-RSA SecurID	2	
ACCESS	2 🛧 Local Admins		
Runtime Access User ACLs IP ACLs XACML		<u>S</u> ave	

Select the EXECUTE check box next to the RSA user group to add it to the AC and select the Save button to commit the changes. Once created, the ACL can be added to content policy virtual directories as seen below.

GENERAL	XMI POLICIES > XMI POLICY		
DIAGNOSTICS			
GATEWAY	XML POLICY		
GATEWAT	Policy Name: RSA SecurID XML Policy		
Network Policies Network Policies Proxy Policies Cloud Policies Cache Policies	Virtual Directories Task Lists Settings IDP Rules Logging		
WSDL Policies WSDL Libraries	Virtual Directories > Virtual Directory: RSA SecurID Test		
WSDL Policies	VIRIUAL DIRECTORY		
Content Policies XML Policies	Name*: RSA SecuriD Test		
	Description:		
JSON Policies	Virtual URI: http://10.5.1.38:80/rsasecurid(/.*)?		
HTML Policies	Remote URI:		
OAuth Policies	VIRTUAL URI SETTINGS		
Tests	Listener Policy: HTTP-Listener V Edit		
Task Policies	Virtual Host:		
Task List Groups	Use virtual host as a regular expression		
Task Lists	Virtual Path: //sasecurid		
Redirect Policies	Enable Virtual Path Case Insensitivity		
Redirect Policies	Filter Expression: (/,*)?		
Request Filters	Replace Expression: \$0		
Request Filters	Request Filter Policy: Default ▼ Edit		
RESOURCES	Error Template: [From Listener Policy] V		
IDP	ACCESS CONTROL		
	IP ACL Policy: Unrestricted Edit		
ACCESS	ACL Policy: RSA_User_ACL V Edit		
Runtime Access User ACLs IP ACLs XACML	XACML Policy: [None] V		
	Password Authentication: [Specify] 🔻		
	Use basic authentication:		
Admin Access	Use digest authentication:		
Domains	Use kerberos authentication:		
	Use cookie authentication:		
User Policies	Use form post authentication:		
Cache	Username Parameter:		
User Groups	Password Parameter:		
LDAP	Require password authentication (any type):		
RSA SecurID	Password Authentication Realm:		
Kerberos SiteMinder	Redirect Policy: [None] •		
one minuer			

APPENDIX

Appendix A - RSA SecurID References

The following table lists various RSA SecurID references:

SPECIFICATION	REFERENCES SECTION OR DETAILS
RSA SecurID	http://www.emc.com/security/rsa-securid/index.htm
RSA SecurID Hardware Tokens	http://www.emc.com/security/rsa-securid/rsa-securid-hardware- tokens.htm
RSA SecurID Tokenless Authentication	http://www.emc.com/security/rsa-securid/rsa-risk-based- authentication.htm
RSA Authentication Manager	http://www.emc.com/security/rsa-securid/rsa-authentication-manager.htm
RSA SecurID Customer Support	http://www.emc.com/support/rsa/index.htm