RSA SECURID® ACCESS
Implementation Guide

Preempt Security
Preempt Behavioral Firewall 2.3

Daniel R. Pintal, RSA Partner Engineering
Last Modified: January 24, 2018

RSA READY

Solution Summary

Preempt Behavioral Firewall integrates with RSA SecurID to provide OTP as a Multi-Factor Authentication method.

RSA SecurID Access Features Preempt Behavioral Firewall 2.3	
On Premise Methods	
RSA SecurID	✓
On Demand Authentication	✓
Risk-Based Authentication (AM)	-
Cloud Authentication Service Methods	
Authenticate App	-
FIDO Token	-
SSO	
SAML SSO	-
HFED SSO	-

Identity Assurance	
Collect Device Assurance and User Behavior	-

Supported Authentication Methods by Integration Point

This section indicates which authentication methods are supported by integration point. The next section (Configuration Summary) contains links to the appropriate configuration sections for each integration point.

Preempt Behavioral Firewall integration with RSA Cloud Authentication Service

Authentication Methods	IDR SAML	Cloud SAML	HFED	REST	RADIUS
RSA SecurID	-	-	-	-	-
LDAP Password	-	-	-	-	-
Authenticate Approve	-	-	-	-	-
Authenticate Eyeprint ID	-	-	-	-	-
Authenticate Fingerprint	-	-	-	-	-
Authenticate Tokencode	-	-	-	-	-
SMS Tokencode	-	-	-	-	
Voice Tokencode	-	-	-	-	
FIDO Token	-	-	-		

Preempt Behavioral Firewall integration with RSA Authentication Manager

Authentication Methods	UDP Agent	TCP Agent	REST	RADIUS
RSA SecurID	-	✓	-	-
AM RBA	-			-

✓ Supported
\- Not supported
n/t Not yet tested or documented, but may be possible

RSA SecurID Access Server Side Configuration

All of the supported use cases of RSA SecurID Access with Preempt Behavioral Firewall require both server-side and Preempt Behavioral Firewall -side configuration. This section of the guide includes links to the appropriate sections for configuring both sides for each use case.

RSA SecurID and/or **On Demand Authentication** – Preempt Behavioral Firewall can be configured with RSA SecurID Authentication in the following way:

RSA Authentication Manager Configuration

TCP Agent

To configure your RSA Authentication manager for use with a TCP-based agent, you must configure an agent host record in the Security Console of your Authentication Manager and download its configuration file (sdconf.rec).

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Preempt Behavioral Firewall with RSA SecurID Access. 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 Preempt Behavioral Firewall components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Preempt Behavioral Firewall Configuration

Configuration Overview

1. To create the Preempt Connector, staff will need the following 4 items related to their SecurID deployment:
    a. SecurID Agent String
    b. Sdconf.rec (64-bit encoded file)
    c. Password to decrypt the node secret file (optional)
    d. Nodesecret (64-bit encoded file, optional)

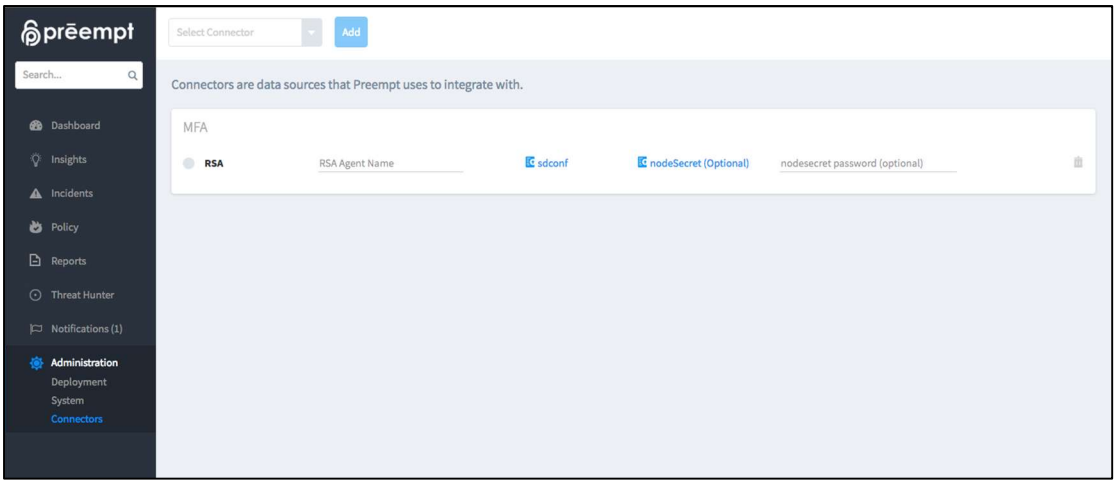
For more information on obtaining these files, please refer to the links provided below:

https://community.rsa.com/docs/DOC-54841

https://community.rsa.com/docs/DOC-53762

https://community.rsa.com/docs/DOC-53930

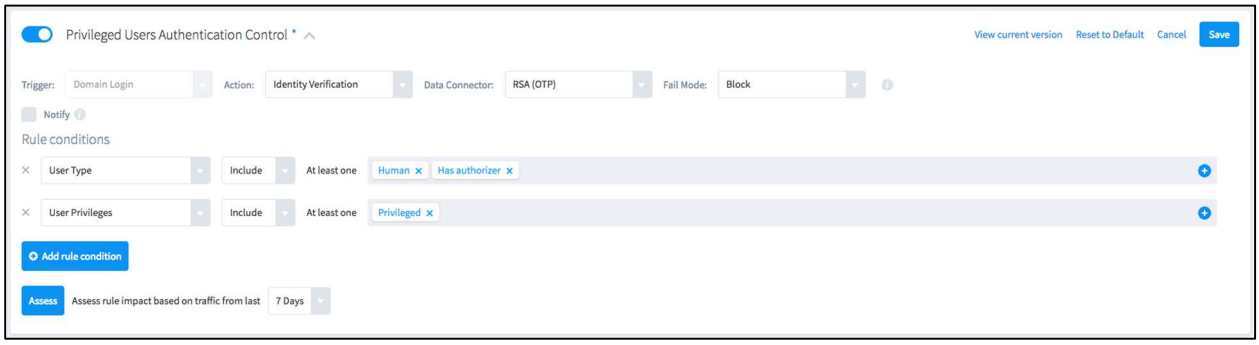
2. Connect to the Preempt user interface. Go to Administration/Connectors. Select RSA SecurID connector from the dropdown list and click on Add. The Data Connector is now added.



3. Enter the Agent Name and password collected in Step 1.
4. Click the links to the right of the Agent Name to upload the appropriate files collected in Step 1.
5. Once completed, click the Save button. Configuration of the Data Connector is now completed.

Apply Control to Security Rule

1. In Preempt UI, select Policy from the main menu.
2. Select the policy rule or rules you want to control with RSA SecurID and then click Edit. Select the action and Data Connector as shown in the screenshot below.



3. Toggle the policy on. Click Save and then Apply all changes.
4. Integration completed. Note: you can add conditions to force the policy on specific users based on membership in OU, Site, Group or Department as well as specific names or other attributes as needed.

Test the Integration

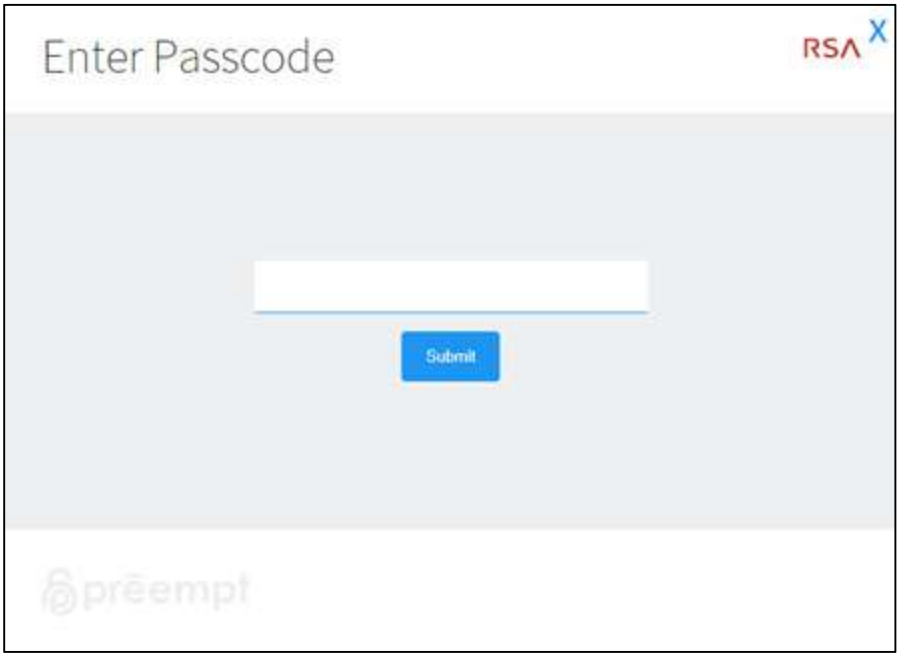
1. Choose a user who is enrolled to RSA SecurID
2. Have the user attempt to connect to an asset specified in the policy (domain, application, etc).
3. Verify the on-screen notification is presented to the user on the machine they used.

On Screen Notifications

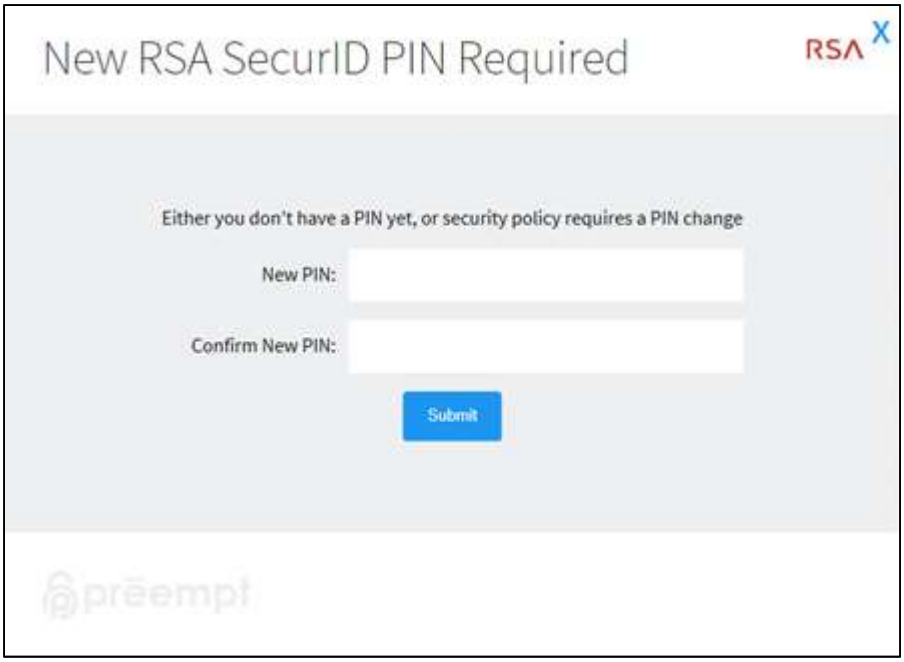
- Domain Admin rights are needed for on screen notifications to be presented
- Supported on Windows 7 / Windows Server 2008 R2 and above.
- When two or more users simultaneously are in the middle of an active logon screen on same terminal server, On Screen Notification will display only on the first terminal window. This is an extreme case.
- Will not present on endpoints behind NAT or VPN unless network firewall properly configured to allow such traffic. See Preempt knowledge base if needed.

Login Screenshots

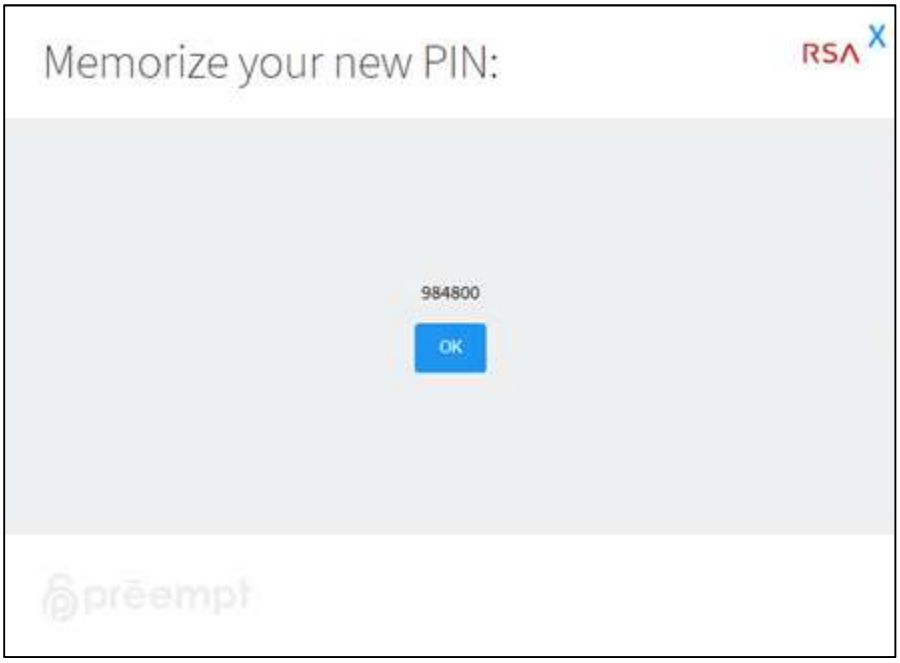
Login screen



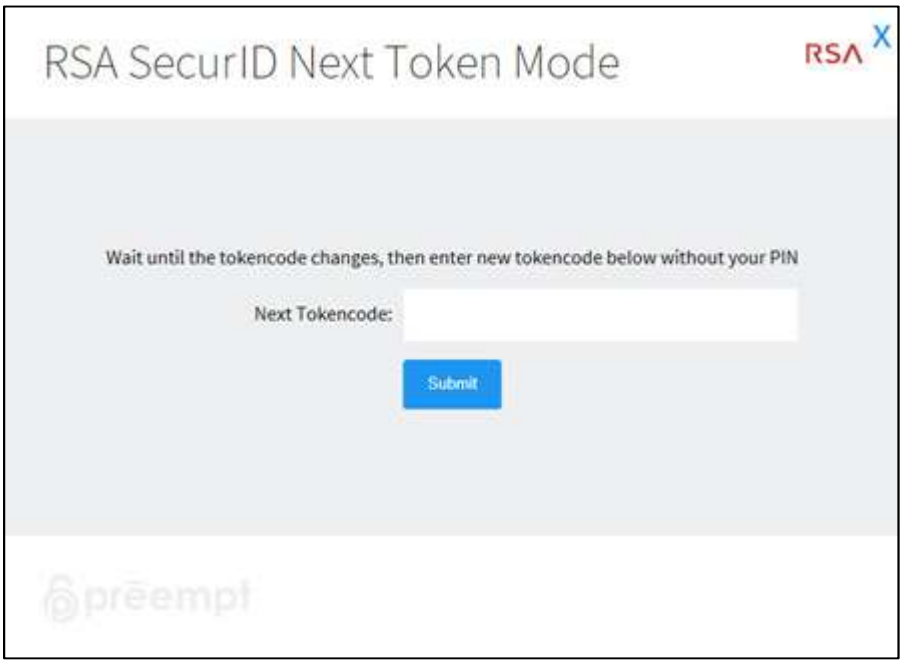
User-defined New PIN



System-generated New PIN



Next Tokencode



Certification Checklist for RSA SecurID Access

Certification Environment Details:

RSA Authentication Manager 8.2, Virtual Appliance

Preempt Behavioral Firewall 2.3, Virtual Appliance

RSA Authentication Manager

Date Tested: January 24, 2018

Authentication Method	REST Client	UDP Agent	TCP Agent	RADIUS Client
RSA SecurID	-	-	✓	-
RSA SecurID Software Token Automation	-	-	✓	-
On Demand Authentication	-	-	✓	-
Risk-Based Authentication		-		-

✓ = Passed, **X** = Failed, **-** = N/A

Appendix

RSA SecurID AccessIntegration Details

Partner Integration Details	
RSA Authentication Agent API (TCP)	Java 8. SDK v8.6
RSA SecurID User Specification	Designated Users, All Users, Default Method
Display RSA Server Info	No
Perform Test Authentication	No – but health check is available
Agent Tracing	No

RSA Authentication Agent Files (C and Java Agents only)

RSA SecurID Authentication Files	
TCP Agent Files	**Location**
rsa_api.properties	Modification not supported
sdconf.rec	/data/rsa-files
sdopts.rec	Not supported
Node secret	/data/rsa-files (encrypted)

API Details:

Removing the connector will delete all files related to RSA SecurID integration from Preempt Behavior Firewall.