Attachmate

Reflection for Secure IT 8.2 Server for Windows

RSA SecurID Ready Implementation Guide

Last Modified: September 3, 2014

Partner Information

Product Information	
Partner Name	Attachmate
Web Site	**www.attachmate.com**
Product Name	Reflection for Secure IT Server for Windows
Version & Platform	8.2
Product Description	Reflection for Secure IT for Windows is a family of Secure Shell clients and servers for Windows and UNIX—all designed to protect data in motion. With Reflection for Secure IT encryption, authentication, and logging features, you can safely transfer files, manage remote servers, and access corporate applications over encrypted connections. These features can also help you comply with stringent data security regulations.

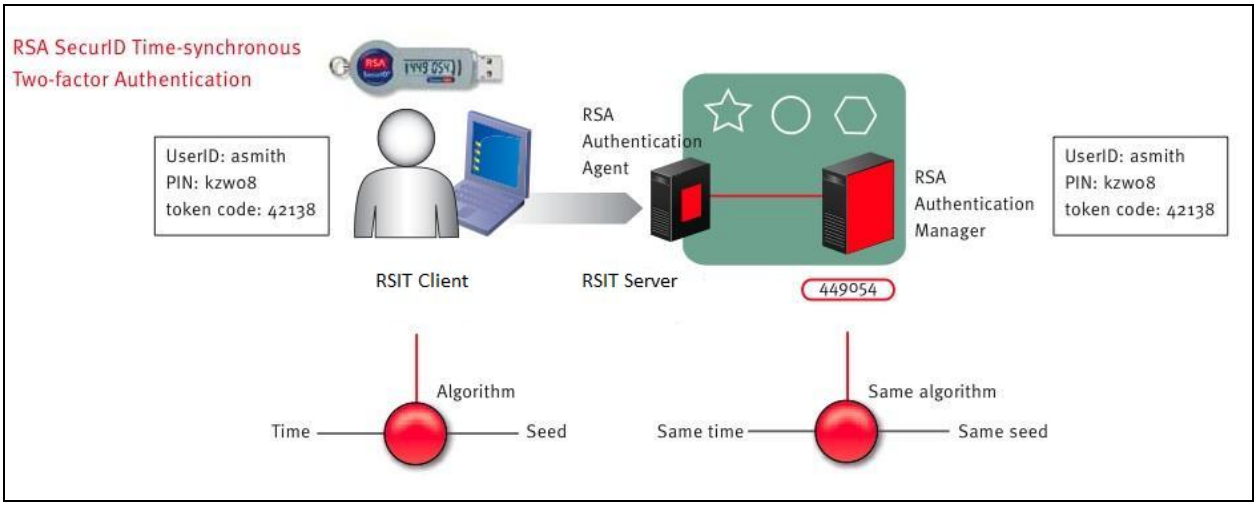
Solution Summary

Reflection for Secure IT (RSIT) enables remote administration of critical servers with the robust SSH protocol suite, which includes SSH, SFTP, and SCP. The Reflection for Secure IT, SSH-based clients and servers use strong authentication and encryption methods to shield data from spies, hackers and other security threats.

RSIT works with an array of authentication and authorization methods, and provides interoperability to new and existing security frameworks. It supports RSA SecurID two-factor authentication with the aid of the Secure Shell keyboard-interactive protocol and the RSA Authentication Agent API.

RSA Authentication agents receive authentication requests from RSIT servers, prompt users for RSA SecurID authentication credentials and forward the credentials to RSA Authentication Manager servers for authentication.

RSA SecurID supported features Reflection for Secure IT Server for Windows	
RSA SecurID Authentication via Native RSA SecurID Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	No
On-Demand Authentication via Native SecurID Protocol	Yes
RSA Authentication Manager Replica Support	Yes
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No



Agent Host Configuration

RSA Authentication Agents are custom or ready-made software applications that securely pass user authentication requests to and from RSA Authentication Manager. RSA provides a variety of out-of-the-box agents for protecting access to various operating systems and web resources, and an Authentication API for building custom agents.

You must register authentication agents with RSA Authentication Manager in order for the server to locate them and establish secure communication channels with them. Use the RSA Security Console to register an agent for your Attachmate RSIT host.

You will need the following information in order to do so:

- the hostname of your Attachmate RSIT server
- IP address for all of your Attachmate RSIT server host's network interfaces

Set each of your Authentication Agent's type to *Standard Agent*.

Note: Each agent hostname must resolve to one or more valid IP addresses on the local network.

RSA SecurID files

RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	%windir%\system32
Node Secret	%windir%\system32
sdstatus.12	%windir%\system32
sdopts.rec	%windir%\system32

Note: The **appendix** of this document contains more detailed information regarding these files.

Partner Product Configuration

Before You Begin

This document provides instructions for enabling RSA SecurID two-factor authentication for Attachmate Reflection for Secure IT for Windows users. You should have working knowledge of RSA Authentication Manager and RSIT, as well as access to the appropriate end-user and administrative documentation. Ensure that that both products are running properly prior to configuring the integration.

Note: This document is not intended to suggest optimal installations or configurations.

Reflection for Secure IT Server for Windows Configuration

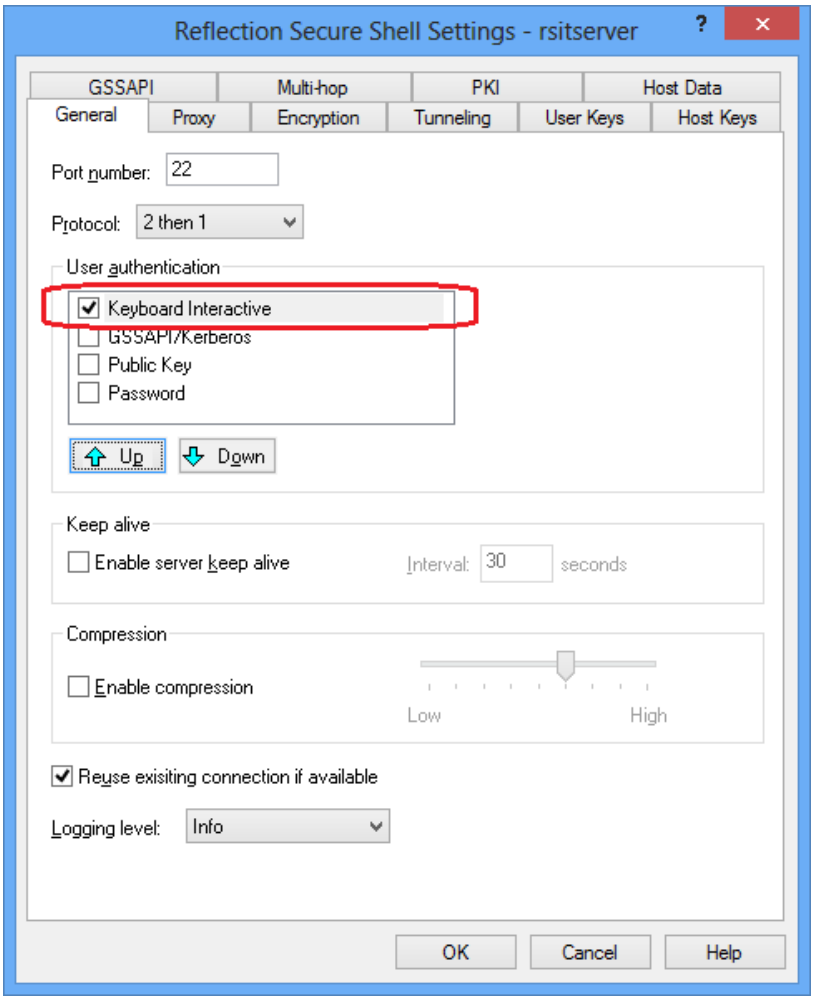
The following two sections contain instructions for configuring Attachmate RSIT to use RSA SecurID authentication:

- **Client Configuration**
- **Server Configuration**

Reflection for Secure IT Client Configuration

To configure the Reflection for Secure IT client:

1. Launch the Reflection for Secure IT client.
2. Select ***Connection > Connection Setup…***
3. Enter your RSIT server's hostname in the **Hostname** field, enter a username in the **Username** field and click the ***Security*** button.
4. Check the ***Keyboard-Interactive*** checkbox. (This is the default setting for all Reflection clients.)

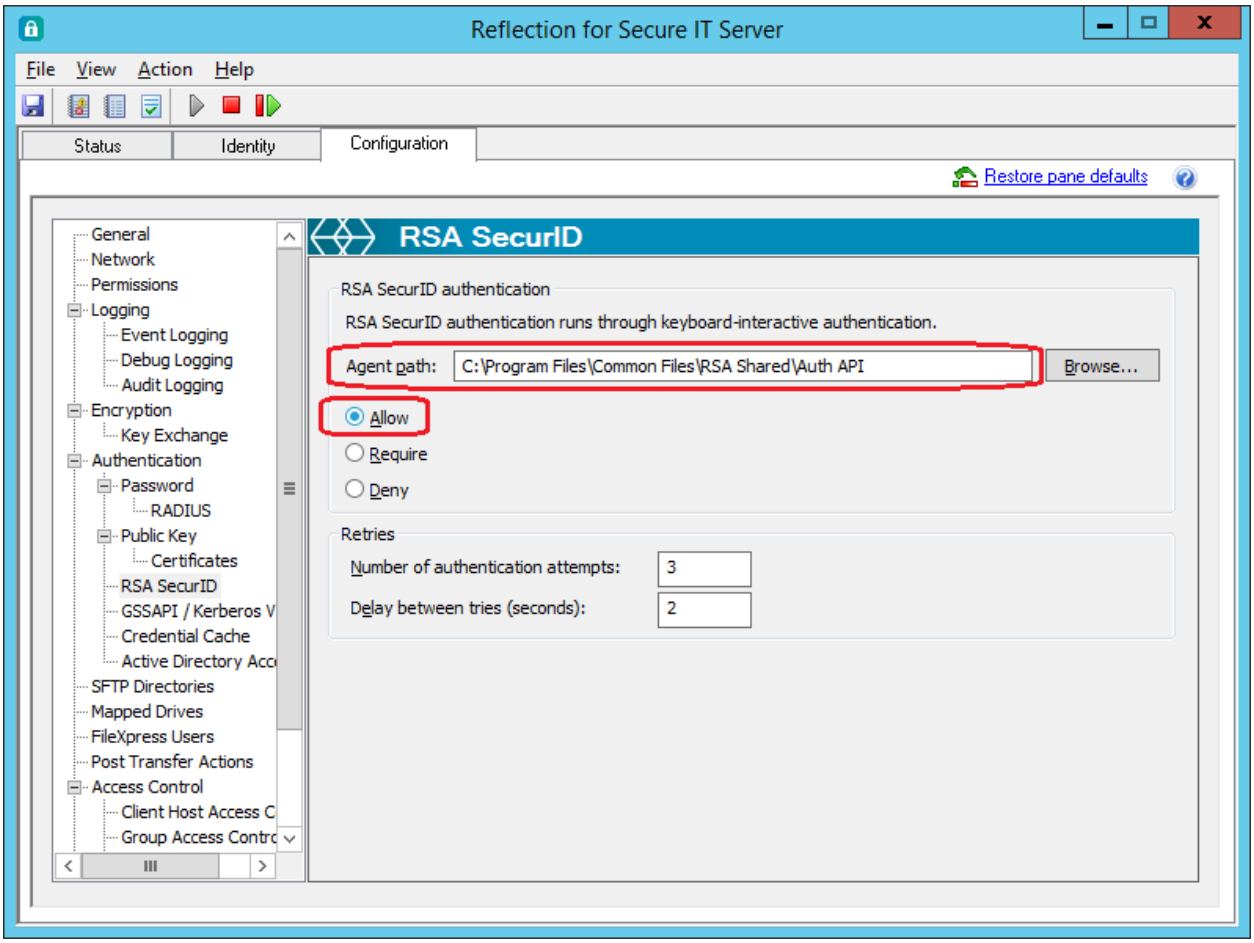


Reflection SSH Client Configuration

Reflection for Secure IT Server for Windows Configuration

To configure the Reflection for Secure IT Server for Windows:

1. Install the RSA SecurID Authentication Agent on the RSIT host.
2. Launch the **Reflection for Secure IT Server console** and select the **Configuration** tab.
3. Select the **RSA SecurID** tree node.
4. Specify the path to the directory that contains *aceclnt.dl* library in the **Agent path** field.
5. Select either the **Allow** or **Require** radio buttons to enable RSA SecurID authentication.

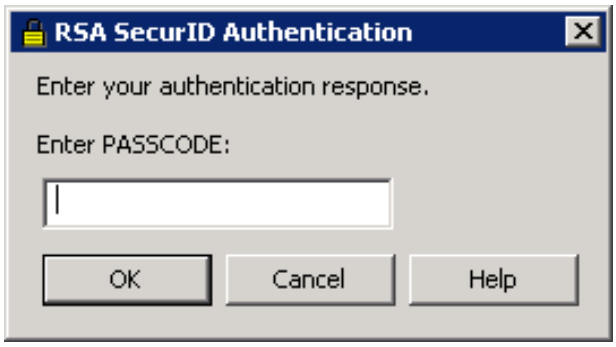


Reflection for Secure IT Server Console

Logon Screen Examples

Once you have configured the Reflection for Secure IT client and server for RSA SecurID authentication, users will authenticate with RSA SecurID. Below is an example of the logon process from the Reflection for Secure IT client:

1. Prompt for PASSCODE:



2. Prompt for system to generate PIN:

3. Prompt for system to display PIN:

4. Prompt for next PASSCODE:

5. Prompt to enter new PIN:

6. Prompt to re-enter PIN:

Certification Checklist for RSA Authentication Manager 8.0

Date Tested: September 3, 2014

Certification Environment		
Product Name	**Version**	**Operating System**
RSA Authentication Manager	8.0	SLES 11
RSA Authentication Agent	7.2.1	Windows 2012 R2
Reflection for Secure IT Server for Windows	8.2	Windows 2012 R2
Reflection for Secure IT Client	7.2 SP3	Windows 2012 R2

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	✓	Force Authentication After New PIN	N/A
System Generated PIN	✓	System Generated PIN	N/A
User Defined (4-8 Alphanumeric)	✓	User Defined (4-8 Alphanumeric)	N/A
User Defined (5-7 Numeric)	✓	User Defined (5-7 Numeric)	N/A
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	N/A
Deny Alphanumeric PIN	✓	Deny Alphanumeric PIN	N/A
Deny Numeric PIN	✓	Deny Numeric PIN	N/A
Deny PIN Reuse	✓	Deny PIN Reuse	N/A
Passcode			
14 Digit Passcode	✓	14 Digit Passcode	N/A
4 Digit Fixed Passcode	✓	4 Digit Fixed Passcode	N/A
Next Tokencode Mode			
Next Tokencode Mode	✓	Next Tokencode Mode	N/A
On-Demand Authentication			
On-Demand Authentication	✓	On-Demand Authentication	N/A
On-Demand New PIN	✓	On-Demand New PIN	N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	N/A
No RSA Authentication Manager	✓	No RSA Authentication Manager	N/A

JGS

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

Known issues

Attachmate Reflection for Secure IT Server for Windows doesn't report PIN reuse errors.

Appendix

Partner Integration Details	
RSA SecurID API	7.2.1 (Windows Agent library)
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	All Users
Display RSA Server Info	Yes
Perform Test Authentication	Yes
Agent Tracing	Yes

Node Secret:

Copy the node secret to the %windir%\system32 directory on the RSIT Windows server host.

sdconf.rec:

Copy the *sdconf.rec* file to the %windir%\system32 directory on the RSIT Windows server host.

sdopts.rec:

Copy the *sdopts.rec* file to the %windir%\system32 directory on the RSIT Windows server host.

sdstatus.12:

Copy the *sdopts.rec* file to the %windir%\system32 directory on the RSIT Windows server host.