SSH Communications Security Corp.

Tectia ConnectSecure 6.0

RSA SecurID Ready Implementation Guide

Last Modified: May 5, 2008

Partner Information

Product Information	
Partner Name	SSH Communications Security
Web Site	www.ssh.com
Product Name	SSH Tectia ConnectSecure
Version	6.0.1.16
Product Description	SSH Tectia ConnectSecure provides tools for replacing plaintext FTP with secure alternatives. SSH Tectia ConnectSecure has been designed for server-to-server communications. The main features of SSH Tectia ConnectSecure are FTP-SFTP conversion, enhanced file transfer services, transparent FTP tunneling, and transparent TCP tunneling.
Product Category	Remote Access

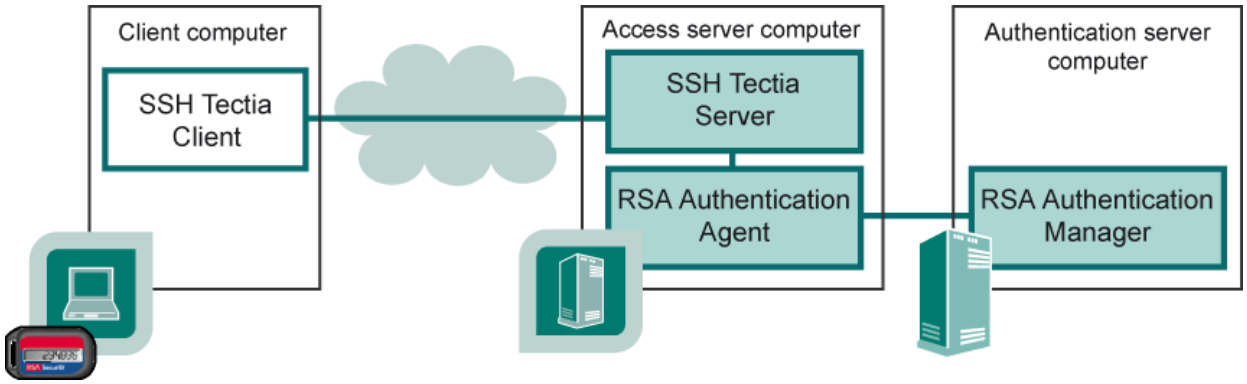
Solution Summary

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication
List Library Version Used	Library Version # 5.2 (Unix), 5.3.4 (Unix/PAM), 6.0 (Windows), 6.1 (Windows)
RSA Authentication Manager Name Locking *	Yes
RSA Authentication Manager Replica Support *	Full Replica Support
Secondary RADIUS Server Support	No
Location of Node Secret on Agent	Depending of the Agent installation directory
RSA Authentication Agent Host Type	Net OS, UNIX
RSA SecurID User Specification	Designated Users, All Users
RSA SecurID Protection of Administrative Users	No
RSA Software Token and SD800 Automation	No
Use of Cached Domain Credentials	No

SSH Tectia ConnectSecure Client and Server form an enterprise-class Secure Shell solution for securing system administration, file transfer, and application connectivity in heterogeneous enterprise networks. SSH Tectia ConnectSecure Client and Server are based on the IETF standard Secure Shell (version 2) protocol.

SSH Tectia ConnectSecure Client and Server support using RSA SecurID for two-factor authentication. SSH Tectia ConnectSecure Client forwards the SecurID passwords using a method called keyboard-interactive. It enables implementation of new authentication schemes based on keyboard interaction without the need to modify the client side.

SSH Tectia ConnectSecure Server includes support for RSA Authentication Agent API. The RSA Authentication Agent software is installed on the same server. The Agent connects to the RSA Authentication Manager that performs the user identity validation against the one-time password generated by the SecurID token.



SSH Tectia ConnectSecure and RSA SecurID system diagram

Product Requirements

Partner Product Requirements: SSH Tectia ConnectSecure Client, SSH Tectia Server	
CPU	POWER, PA-RISC, x86, x86-64, SPARC
Memory	128 Mbytes
Storage	100 Mbytes
Operating System	
Platform	**Version (Patch-level)**
IBM AIX 5L	5.2, 5.3
HP-UX	11i, 11i v2, 11i v3
SUSE LINUX Enterprise Server	9.10
Red Hat Enterprise Linux	3, 4, 5, 5.1
Sun Solaris	8, 9, 10
Microsoft Windows	2000 (SP4) , XP, Vista, Server 2003 (SP2)

Agent Host Configuration

To facilitate communication between the SSH Tectia 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 SSH Tectia Server within its database and contains information about communication and encryption.

To create the Agent Host record, you will need the following information.

- Hostname
- IP Addresses for all network interfaces
- RADIUS Secret (When using RADIUS Authentication Protocol)

When adding the Agent Host Record, you should configure the SSH Tectia Server as Net OS. This setting is used by the RSA Authentication Manager to determine how communication with the SSH Tectia Server will occur.

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

Please refer to the appropriate RSA Security documentation for additional information about Creating, Modifying and Managing Agent Host records.

Partner Product Configuration

Before You Begin

This section provides instructions for integrating the SSH Tectia 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 vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Documenting the Solution

This section contains the following instructions:

- SSH Tectia Server configuration on Windows
- SSH Tectia ConnectSecure Client configuration on Windows

Depending on your client and server platforms, carry out the steps on each client and server you wish to enable SecurID authentication on.

SSH Tectia Server Configuration

The keyboard-interactive authentication with the SecurID submethod is used to enable RSA SecurID authentication on SSH Tectia Server.

The Secure Shell client cannot request any specific keyboard-interactive submethod if the Secure Shell server allows several optional submethods. The order in which the submethods are offered depends on the server configuration. However, if the server allows, for example, the two optional submethods SecurID and password, the user can skip SecurID by pressing enter when the server offers SecurID. The user will then be prompted for a password.

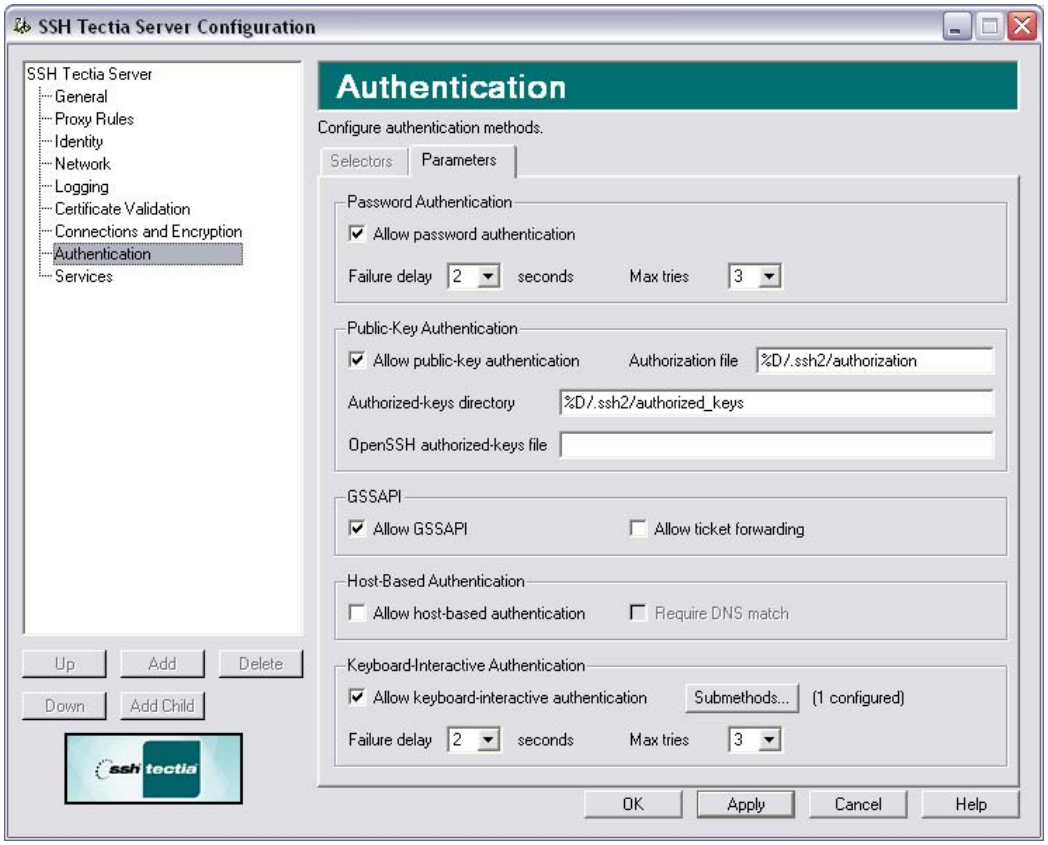
Important: An identical user record has to be defined both in the RSA Authentication Manager and the operating system (local or domain).

Windows Server

To enable SecurID authentication on SSH Tectia Server on Windows, do the following steps:

1. Perform a standard installation of the RSA ACE Client. Reference the RSA product documentation for details.
2. Launch the SSH Tectia Server Configuration tool from the Start menu, Programs > SSH Tectia Server > SSH Tectia Server Configuration.

3. From the tree view on the left, select Authentication.

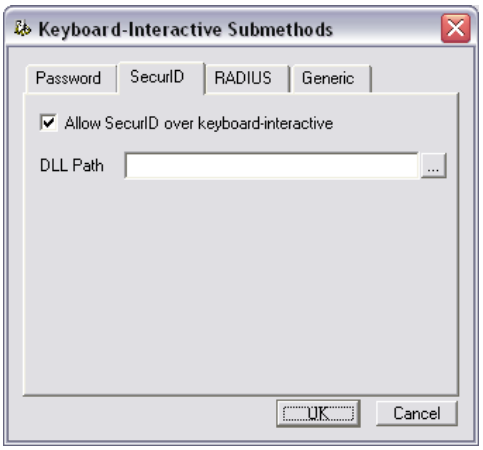


SSH Tectia Server Configuration – Authentication page

4. Make sure the Allow keyboard-interactive authentication check box is selected (it is by default).

   Also other authentication methods are allowed by default. To disable any of them, clear the corresponding check boxes.

5. Click the Submethods button. The Keyboard-Interactive Submethods dialog box opens.



Keyboard-Interactive Submethod's – SecurID

6. The password submethod is enabled by default. To disable it, clear the check box on the Password tab.

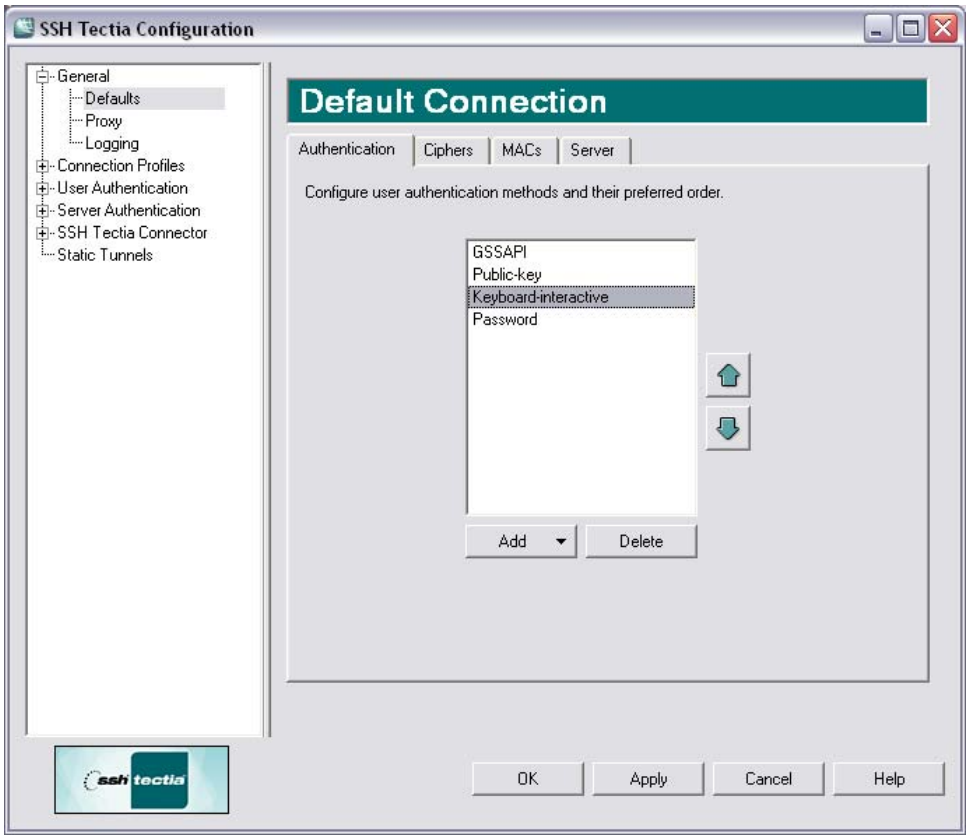
7. Select the SecurID tab, and select the Allow SecurID over keyboard-interactive check box. Giving the DLL path is not necessary. SSH Tectia Server will find the installed SecurID libraries automatically. Click OK.
8. Back on the Authentication page, click OK or Apply.

The server is now ready to accept connections using SecurID authentication.

Windows Client

To enable SecurID authentication on SSH Tectia ConnectSecure Client on Windows, do the following steps:

1. Launch the SSH Tectia ConnectSecure Configuration tool from the SSH Tectia ConnectSecure tray icon short menu by clicking Configuration.
2. From the tree view on the left, select General > Defaults.
3. On the Authentication tab, make sure the Keyboard-interactive method is shown on the list selected (it is by default). If keyboard-interactive is not on the list, add it by clicking the Add button and clicking Keyboard-interactive from the drop-down list.
4. Other authentication methods are allowed by default. To disable any of them, use the Delete button. To change the order in which the methods are attempted, use the arrow buttons.



SSH Tectia ConnectSecure Configuration – Default Connection, Authentication tab

5. SSH Tectia ConnectSecure Client can have connection profiles that define customized connection settings for different Secure Shell servers. To customize the authentication settings in the connection profiles, select the profile under Connection Profiles and make the appropriate settings on the Authentication tab.

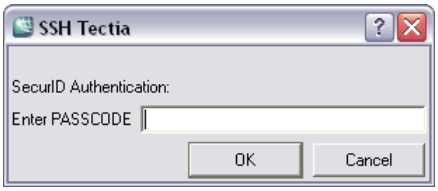
   For servers that allow only SecurID authentication, you can create profiles that have all other authentication methods except keyboard-interactive disabled.

6. Click OK to take the changed configuration in use.

7. The client is now ready to use SecurID authentication.

To test the connection, start SSH Tectia ConnectSecure Client from the Start menu, Programs > SSH Tectia ConnectSecure Client > SSH Tectia Client. Click Quick Connect to connect without profiles, or click Profiles and select a profile for the connection.

Once the SSH Tectia Server accepts keyboard-interactive as the authentication method, SSH Tectia ConnectSecure Client will prompt the user for the RSA SecurID PASSCODE.



SecurID authentication – Enter PASSCODE

If set in the user's SecurID profile, SSH Tectia ConnectSecure Client may prompt for creating the PIN code with the following dialogs.

Certification Checklist for RSA Authentication Manager 6.1

Date Tested: May 5, 2008

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	6.1 [295]	Windows Server 2003 SP1
RSA Authentication Agent	6.0.2 / 6.1	Windows Server 2003 SP1
SSH Tectia Server	6.0.1.16	Windows Server 2003 SP1
SSH Tectia ConnectSecure Client	6.0.1.16	Windows XP SP2

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
User Selectable	✓	User Selectable	N/A
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	N/A
Deny Alphanumeric PIN	✓	Deny Alphanumeric PIN	N/A
PASSCODE			
16 Digit PASSCODE	✓	16 Digit PASSCODE	N/A
4 Digit Password	✓	4 Digit Password	N/A
Next Tokencode Mode			
Next Tokencode Mode	✓	Next Tokencode Mode	N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	N/A
Name Locking Enabled	✓	Name Locking Enabled	
No RSA Authentication Manager	✓	No RSA Authentication Manager	N/A

Additional Functionality			
RSA Software Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
RSA SD800 Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
Domain Credential Functionality			
Determine Cached Credential State	N/A	Determine Cached Credential State	
Set Domain Credential	N/A	Set Domain Credential	
Retrieve Domain Credential	N/A	Retrieve Domain Credential	

DRP

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

Certification Checklist for RSA Authentication Manager 7.1

Date Tested: April 30, 2008

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1	Windows Server 2003 SP1
RSA Authentication Agent	6.1 (bld 293)	Windows Server 2003 SP1
SSH Tectia Server	6.0.1.12	Windows Server 2003 SP1
SSH Tectia ConnectSecure Client	6.0.1.16	Windows XP SP2

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
PIN Reuse	✓	PIN Reuse	N/A
Passcode			
16 Digit Passcode	✓	16 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
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	N/A
No RSA Authentication Manager	✓	No RSA Authentication Manager	N/A

Additional Functionality			
RSA Software Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
PIN Expiration	N/A	PIN Expiration	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
RSA SecurID 800 Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
PIN Expiration	N/A	PIN Expiration	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A

DRP

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

Known Issues

Solaris x86-64: RSA SecurID cannot be used with SSH Tectia Server on Solaris x86-64, because RSA SecurID offers only a 32-bit PAM library. SSH Tectia Server expects a 64-bit pam_securid.so.