SafeNet Authentication Manager

Integration Guide

SAM using RADIUS Protocol with Tectia SSH

Document Information

Document Part Number	007-012886-001, Rev. A
Release Date	December 2014

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Tectia SSH.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

SafeNet Authentication Manager (SAM) is a versatile authentication solution that allows you to match the authentication method and form factor to your functional, security, and compliance requirements. Use this innovative management service to handle all authentication requests and to manage the token lifecycle.

Enterprises and government organizations around the world use Tectia SSH client and server to secure their critical IT processes, including impromptu and automated file transfers, as well as remote systems administration. Tectia SSH offers the features, reliability, and manageability that are simply not available with the open source solutions.

ConnectSecure is an advanced Tectia SSH client that makes automation easy. ConnectSecure is ideal for adding encryption to the existing automated file transfer processes and makes it easy for your application developers to use encryption. ConnectSecure is fully interoperable with open source Secure Shell and other standards compliant implementations—so no worries about connecting with business partners or within a heterogeneous network.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in Tectia SSH using SafeNet OTP tokens managed by SafeNet Authentication Manager.
- Configure Tectia SSH to work with SafeNet Authentication Manager in RADIUS mode.

It is assumed that the Tectia SSH environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager, and that the SafeNet Authentication Manager OTP plug-in for Microsoft RADIUS Client was installed as part of the simplified installation mode of SAM. For more information on SafeNet Authentication Manager Installation modes, refer to the *SafeNet Authentication Manager 8.2 Administrator's Guide*.

Tectia SSH can be configured to support multi-factor authentication in several modes. The RADIUS protocol will be used for the purpose of working with SafeNet Authentication Manager.

Applicability

The information in this document applies to:

- **SafeNet Authentication Manager** - A server version of SAM that is used to deploy the solution on-premises in the organization.

Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Manager 8.2 HF 493** - A server version of SAM that is used to deploy the solution on-premises in the organization.
- **Tectia SSH 6.4.6.215**
- **Tectia SSH ConnectSecure Client 6.4.6.215**

Audience

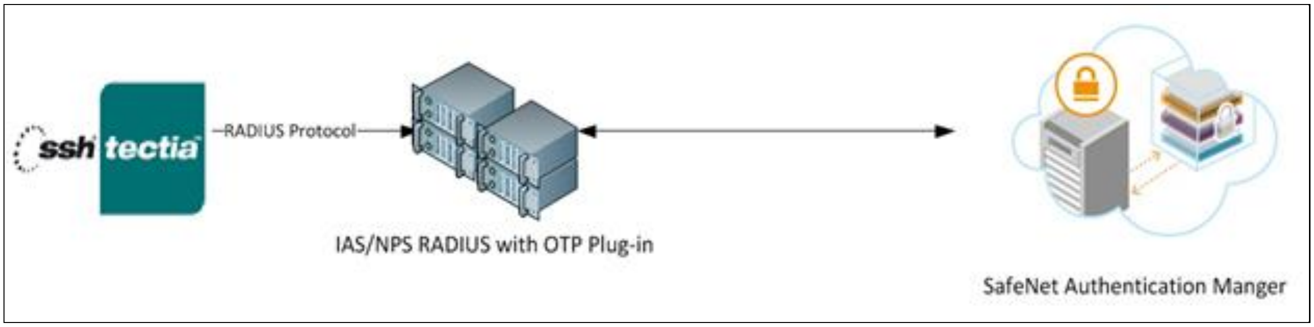
This document is targeted to system administrators who are familiar with Tectia SSH and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Manager.

RADIUS-based Authentication using SAM

SafeNet's OTP architecture includes the SafeNet RADIUS server for back-end OTP authentication. This enables integration with any RADIUS-enabled gateway or application. The SafeNet RADIUS server accesses user information in the Active Directory infrastructure via SafeNet Authentication Manager (SAM).

SAM's OTP plug-in for Microsoft RADIUS Client works with Microsoft's IAS or NPS, providing strong authenticated remote access through the IAS or NPS RADIUS server.

When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

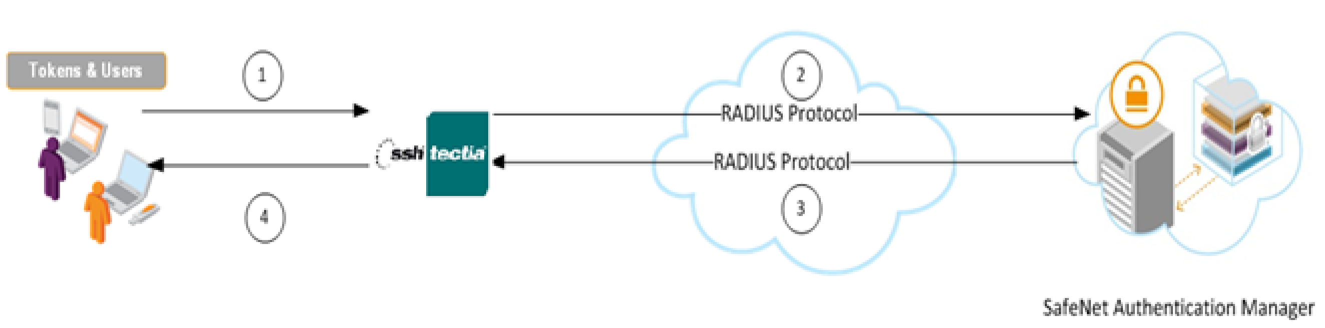

ssh tectia
RADIUS Protocol
IAS/NPS RADIUS with OTP Plug-in
SafeNet Authentication Manger

For more information on how to install and configure the SafeNet OTP plug-in for Microsoft RADIUS Client, refer to the *SafeNet Authentication Manager 8.2 Administrator`s Guide*.

RADIUS Authentication Flow using SAM

SafeNet Authentication Manager communicates with a large number of VPN and access-gateway solutions using the RADIUS protocol.

The image below describes the dataflow of a multi-factor authentication transaction for Tectia SSH.



1. A user attempts to log on to Tectia SSH using an OTP token.
2. Tectia SSH sends a RADIUS request with the user’s credentials to SafeNet Authentication Manager for validation.
3. The SAM authentication reply is sent back to Tectia SSH.
4. The user is granted or denied access to Tectia SSH based on the OTP value calculation results from SAM and is connected to Tectia SSH.

RADIUS Prerequisites

To enable SafeNet Authentication Manager to receive RADIUS requests from Tectia SSH, ensure the following:

- End users can authenticate from the Tectia SSH environment with a static password before configuring Tectia SSH to use RADIUS authentication.
- Ports 1812/1813 are open to and from Tectia SSH.
- A shared secret key has been selected, providing an added layer of security by supplying an indirect reference to a shared secret key. It is used by a mutual agreement between the RADIUS server and the RADIUS client for encryption, decryption, and digital signature purposes.

Configuring SafeNet Authentication Manager

The deployment of multi-factor authentication using SAM with Tectia SSH using the RADIUS protocol requires the following:

- Synchronizing User Stores to SafeNet Authentication Manager, page 7
- Configuring SAM’s Connector for OTP Authentication, page 7
- Token Assignment in SAM, page 8
- Adding Tectia SSH as a RADIUS Client in IAS/NPS, page 8
- SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration, page 10

Synchronizing User Stores to SafeNet Authentication Manager

SAM manages and maintains OTP token information in its data store, including the token status, the OTP algorithm used to generate the OTP, and the token assignment to users. For user information, SAM can be integrated with an external user store. During the design process, it is important to identify which user store the organization is using, such as Microsoft Active Directory.

If the organization is not using an external user store, SAM uses an internal ("stand-alone") user store created and maintained by the SAM server.

SAM 8.2 supports the following external user stores:

- Microsoft Active Directory – 2003, 2008, and 2008 R2
- Novell eDirectory
- Microsoft ADAM/AD LDS
- OpenLDAP
- Microsoft SQL Server 2005 and 2008
- IBM Lotus Domino
- IBM Tivoli Directory Server

Configuring SAM's Connector for OTP Authentication

SafeNet Authentication Manager is based on open standards architecture with configurable connectors. This supports integration with a wide range of security applications, including network logon, VPN, web access, one-time password authentication, secure email, and data encryption.

If you selected the **Simplified OTP-only** configuration, SafeNet Authentication Manager is automatically configured with a typical OTP configuration, providing a working SafeNet Authentication Manager OTP solution.

The **Simplified OTP-only** configuration is as follows:

- **Connectors** - SAM Connector for OTP Authentication is installed
- **SAM Backend Service** - Activated on this server; scheduled to operate every 24 hours

In addition, the SAM default policy is set as follows:

- OTP support (required for OTP) is selected in the **Token Initialization** settings.
- The SAM Connector for OTP Authentication is set, by default, to enable enrollment of OTP tokens without requiring changes in the TPO settings. For more information on how to install and configure the SafeNet Authentication Manager for simplified installation, refer to the *SafeNet Authentication Manager 8.2 Administrator's Guide*.

Token Assignment in SAM

SAM supports a number of OTP authentication methods that can be used as a second authentication factor for users authenticating through Tectia SSH.

The following tokens are supported:

- eToken PASS
- eToken NG-OTP
- SafeNet GOLD
- SMS tokens
- MobilePASS
- SafeNet eToken Virtual products
- MobilePASS Messaging
- SafeNet Mobile Authentication (iOS)
- SafeNet eToken 3400
- SafeNet eToken 3500

Tokens can be assigned to users as follows:

- **SAM Management Center:** Management site used by SAM administrators and the help desk for token enrollment and lifecycle management.
- **SAM Self-Service Center:** Self-service site used by end users for managing their tokens.
- **SAM Remote Service:** Self-service site used by employees not on the organization's premises as a rescue website to manage cases where tokens are lost or passwords are forgotten.

For more information on SafeNet's tokens and service portals, refer to the *SafeNet Authentication Manager 8.2 Administrator's Guide*.

Adding Tectia SSH as a RADIUS Client in IAS/NPS

For Windows Server 2003, the Windows RADIUS service is Internet Authentication Service (IAS). The IAS is added as the RADIUS server in Tectia SSH.

For Windows Server 2008 and above, the Windows RADIUS service is the Microsoft Network Policy Server (NPS). The NPS server is added as the RADIUS server in Tectia SSH.

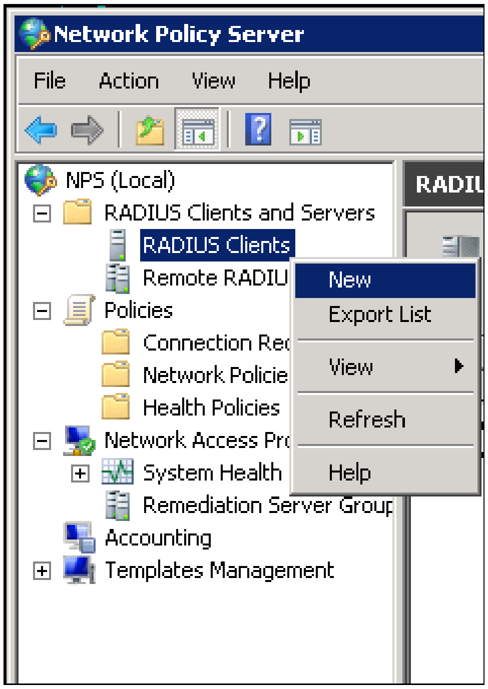
Tectia SSH must be added as a RADIUS client on the IAS/NPS server so that IAS/NPS will authorize Tectia SSH for authentication.

NOTE: It is assumed that IAS/NPS policies are already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager.

The details below refer to NPS, and are very similar to IAS.

To add a RADIUS client:

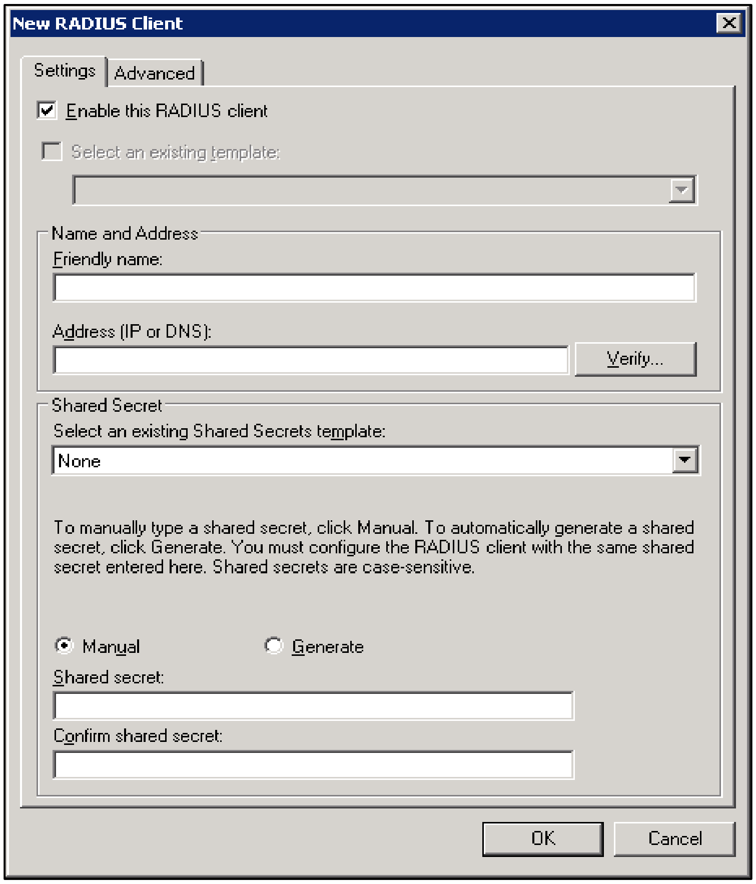
1. Click **Start > Administrative Tools > Network Policy Server**.
2. From the NPS web console, in the left pane, expand **RADIUS Clients and Servers**, right-click **RADIUS Clients** and then click **New**.



(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

3. On the **New RADIUS Client** window, complete the following fields on the **Settings** tab:

Enable this RADIUS client	Select this option.
Friendly name	Enter a RADIUS client name.
Address (IP or DNS)	Enter the IP address or DNS of Tectia SSH.
Manual/Generate	Select **Manual**.
Shared secret	Enter the shared secret for the RADIUS client. The value must be the same when configuring the RADIUS server in Tectia SSH.
Confirm shared secret	Re-enter the shared secret to confirm it.



☑ Enable this RADIUS client

□ Select an existing template:

Select an existing Shared Secrets template: None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

4. Click **OK**.

   Tectia SSH is added as a RADIUS client in NPS.

SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration

RADIUS protocol is used for authentication and authorization. The SafeNet OTP solution supports the Microsoft IAS service (used in Windows 2003) and Microsoft NPS service (used in Windows 2008 and later) as Windows services running a RADIUS server. These services may be extended by adding plug-ins for the authentication process.

SAM's OTP plug-in for Microsoft RADIUS Client works with Microsoft’s IAS or NPS to provide strong, authenticated remote access through the IAS or NPS RADIUS server. When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet Authentication Manager OTP plug-in, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

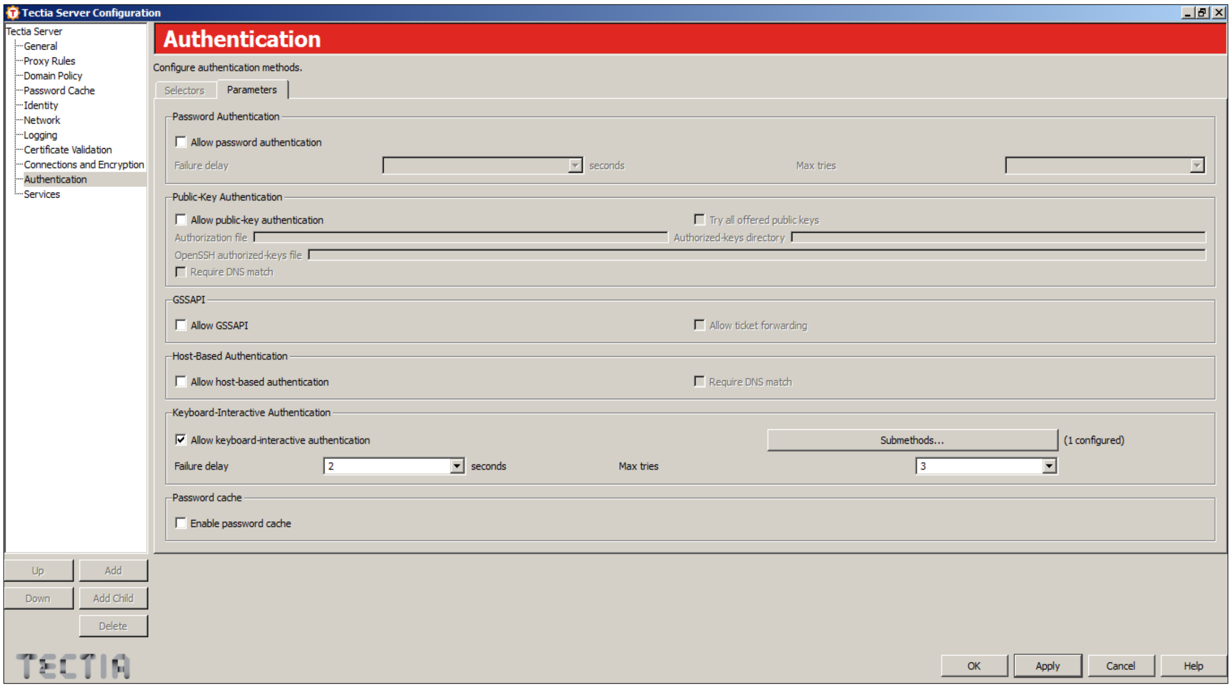
Configuring Tectia SSH

Configuring Tectia SSH for RADIUS authentication requires configuring the SSH Tectia server on Windows.

Configuring SSH Tectia Server on the Windows Platform

The Keyboard-Interactive Authentication with the RADIUS submethod is used to enable SafeNet Authentication Manager authentication on the SSH Tectia server. The Tectia SSH Client cannot request any specific Keyboard-Interactive submethod if the Tectia SSH server allows several optional submethods. The order in which the submethods are offered depends on the server configuration.

1. Create a text file (for example, **secret.txt**) on the local computer containing the RADIUS server shared secret, and then save the file.
2. Launch the **Tectia Server Configuration** tool from **Start > Programs > SSH Tectia Server > SSH Tectia Server Configuration**.
3. On the **Tectia Server Configuration** window, in the left pane, click **Authentication**.



Configure authentication methods.

Password Authentication
☐ Allow password authentication
Failure delay seconds Max tries

Public-Key Authentication
☐ Allow public-key authentication ☐ Try all offered public keys
Authorization file Authorized-keys directory
OpenSSH authorized-keys file
☐ Require DNS match

GSSAPI
☐ Allow GSSAPI ☐ Allow ticket forwarding

Host-Based Authentication
☐ Allow host-based authentication ☐ Require DNS match

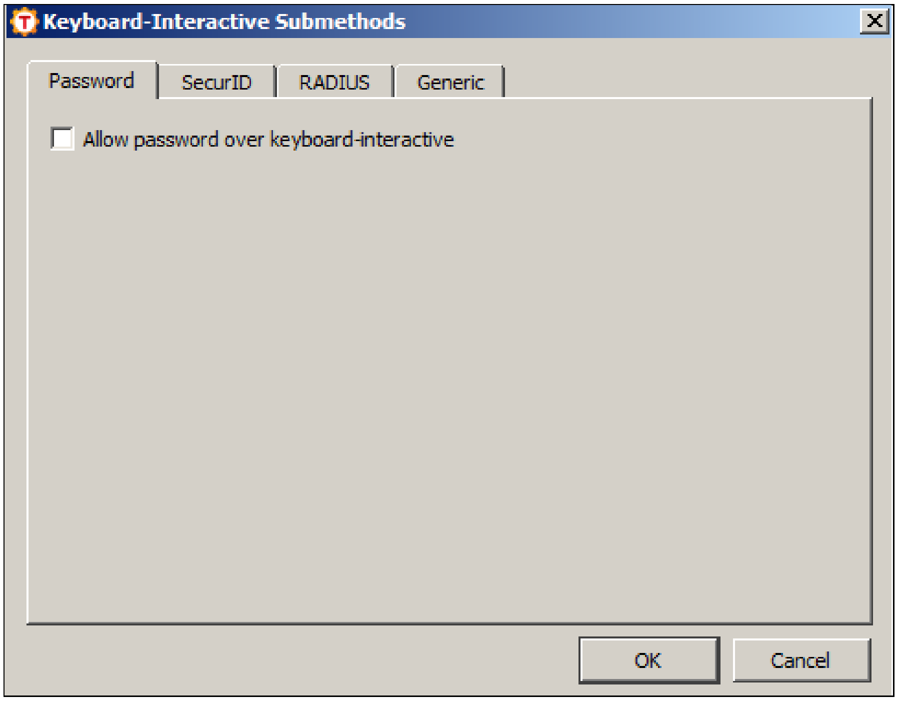
Keyboard-Interactive Authentication
☑ Allow keyboard-interactive authentication Submethods... (1 configured)
Failure delay 2 seconds Max tries 3

Password cache
☐ Enable password cache

(The screen image above is from SSH Communications Security software. Trademarks are the property of their respective owners.)

4. In the right pane, click the **Parameters** tab.
5. On the **Parameters** tab, under **Keyboard-Interactive Authentication**, perform the following steps:
    a. Ensure that **Allow keyboard-interactive authentication** is selected (the default mode), and that other authentication methods are not selected.
    b. Click **Submethods**.

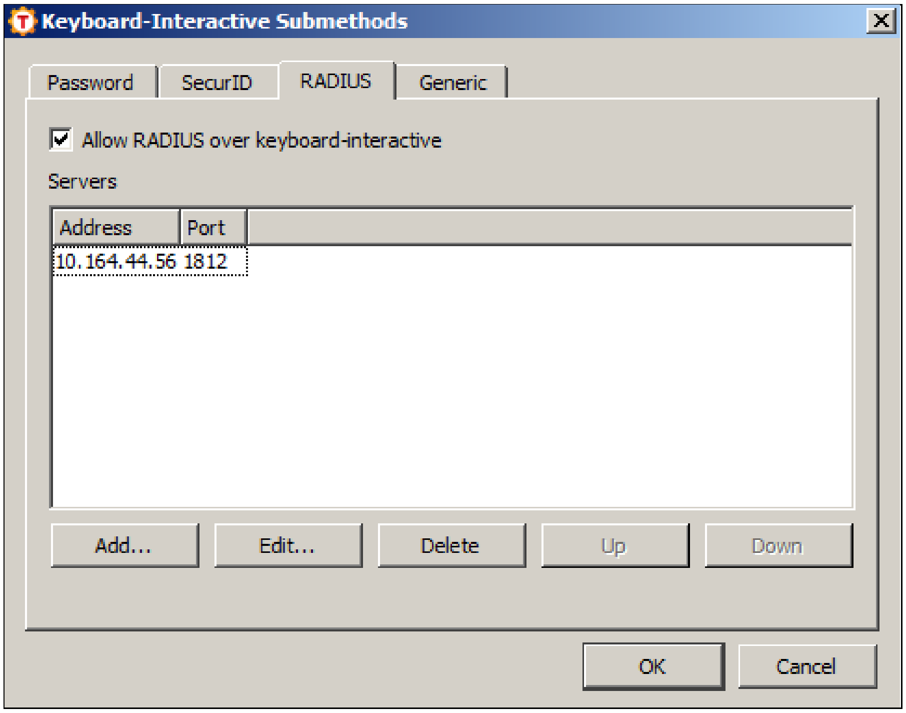
c. On the **Keyboard-Interactive Submethods** window, click the **Password** tab, and then clear **Allow password over keyboard-interactive**.



□ Allow password over keyboard-interactive

(The screen image above is from SSH Communications Security software. Trademarks are the property of their respective owners.)

d. On the **Keyboard-Interactive Submethods** window, click the **RADIUS** tab. Select **Allow RADIUS over keyboard-interactive**, and then click **Add**.



☑ Allow RADIUS over keyboard-interactive

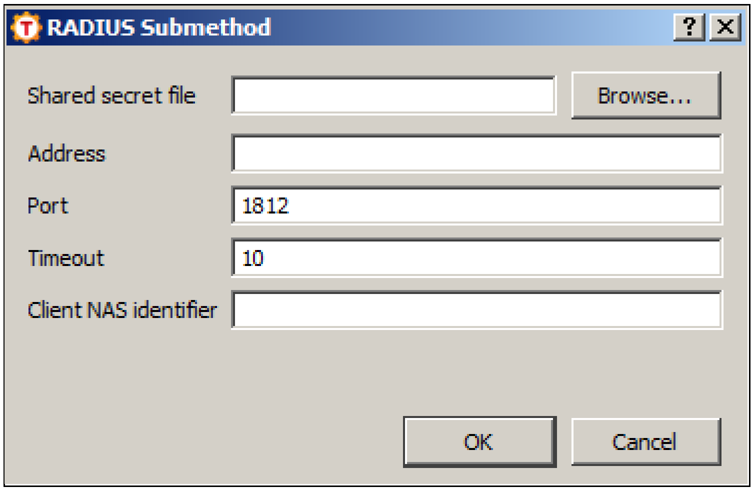
Servers

Address	Port
10.164.44.56	1812

(The screen image above is from SSH Communications Security software. Trademarks are the property of their respective owners.)

e. On the **RADIUS Submethod** window, complete the following fields:

Shared secret file	Click **Browse** and select the shared secret file.
Address	Enter the IP address of the SAM server.
Port	Enter **1812**.



Port 1812

Timeout 10

(The screen image above is from SSH Communications Security software. Trademarks are the property of their respective owners.)

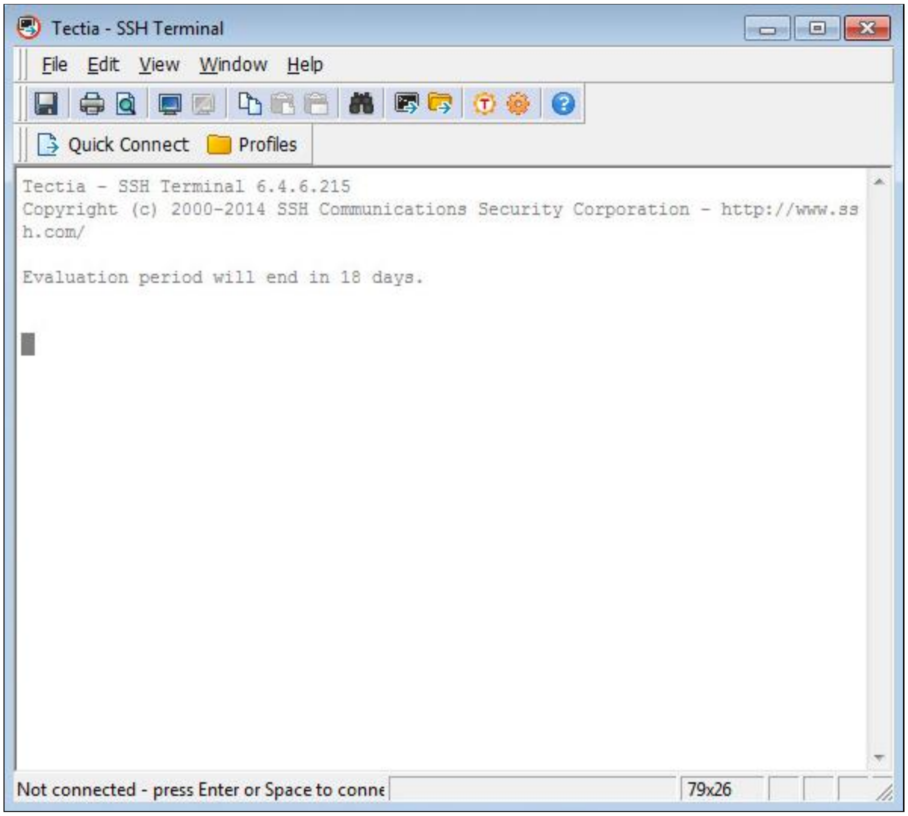
f. Click **OK** twice to return to the **Parameters** tab on the **Tectia Server Configuration** window.

6. Click **OK**.

Running the Solution

Once the configurations are completed on the Tectia SSH server, you can run the solution to check the RADIUS and Keyboard-Interactive authentication method. To test RADIUS authentication, a token should be assigned to the user in SAM.

1. Start the **Tectia SSH ConnectSecure Client** or the **Tectia SSH Client** application from **Start > Programs > Tectia ConnectSecure > Tectia SSH Terminal**.
2. On the **Tectia SSH Terminal** window, click **Quick Connect**.



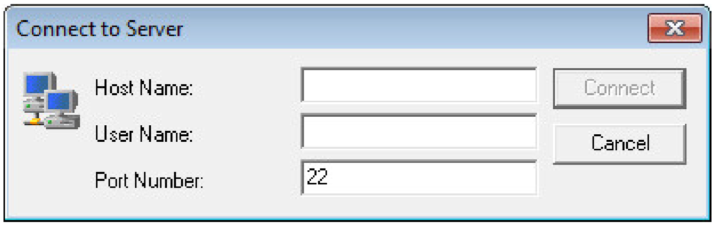
```
Tectia - SSH Terminal 6.4.6.215
Copyright (c) 2000-2014 SSH Communications Security Corporation - http://www.ss
h.com/

Evaluation period will end in 18 days.
```

Not connected - press Enter or Space to conne

(The screen image above is from SSH Communications Security software. Trademarks are the property of their respective owners.)

3. On the **Connect to Server** window, provide the following information, and then click **Connect**:

Host Name	Enter the IP address of the Tectia SSH server.
User Name	Enter the user name.



Host Name:

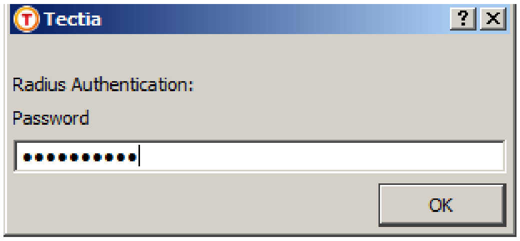
User Name:

Port Number: 22

(The screen image above is from SSH Communications Security software. Trademarks are the property of their respective owners.)

4. Once the SSH Tectia server accepts Keyboard-Interactive as the authentication method, SSH Tectia ConnectSecure Client/Tectia Client will prompt for the SafeNet token passcode.

   In the **Password** field, enter the OTP generated on the enrolled SafeNet token, and then click **OK**.



(The screen image above is from SSH Communications Security software. Trademarks are the property of their respective owners.)

The user is logged in successfully.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	