SafeNet Authentication Service

Integration Guide

SAS Using RADIUS Protocol with Tectia SSH

Document Information

Document Part Number	007-012609-001, Rev. B
Release Date	December 2014

Trademarks

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 Service delivers a fully automated, versatile, and strong authentication-as-a-service solution.

With no infrastructure required, SafeNet Authentication Service provides smooth management processes and highly flexible security policies, token choice, and integration APIs.

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 authenticators managed by SafeNet Authentication Service.
- Configure Tectia SSH to work with SafeNet Authentication Service 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 Service.

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 Service.

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)** — SafeNet's cloud-based authentication service.
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)** — A server version that is used by Service Providers to deploy instances of SafeNet Authentication Service.
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)** — A server version 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 Service (SAS)** – SafeNet's cloud-based authentication service
- **Tectia SSH Server 6.4.6.215**
- **Tectia SSH Client 6.4.6.215**
- **Tectia SSH ConnectSecure Client 6.4.6.215**

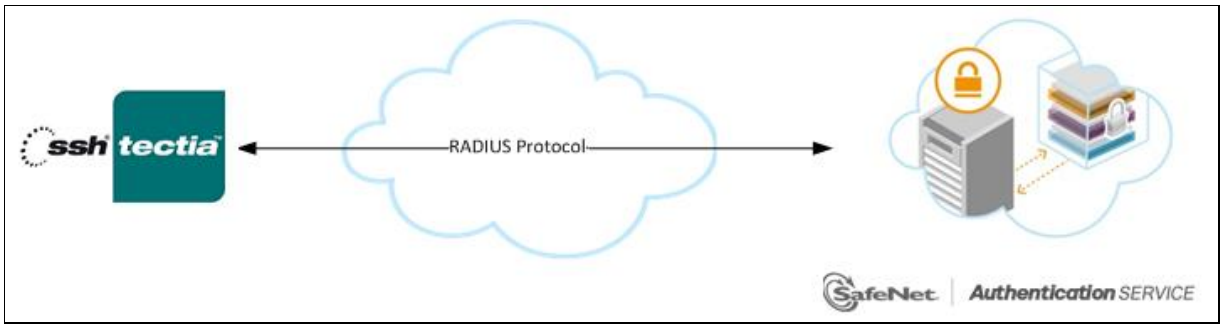
Audience

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 Service.

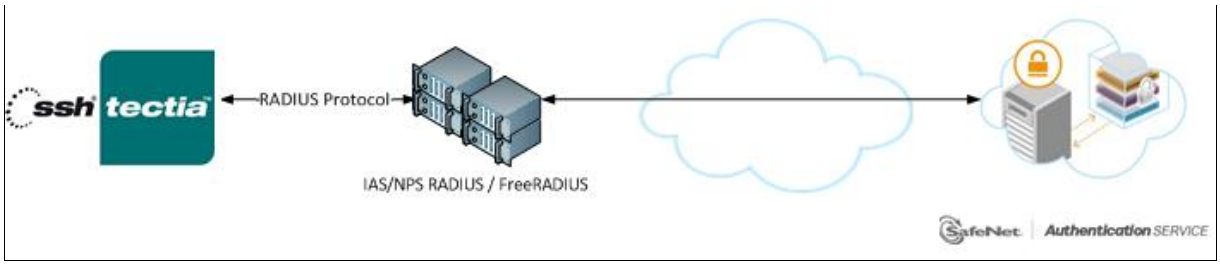
RADIUS-based Authentication using SAS Cloud

SAS Cloud provides two RADIUS mode topologies:

- **SAS cloud hosted RADIUS service** – A RADIUS service that is already implemented in the SAS cloud environment and can be used without any installation or configuration requirements.



- **Local RADIUS hosted on-premises** - A RADIUS agent that is implemented in the existing customer's RADIUS environment. The agent forwards the RADIUS authentication requests to the SAS cloud environment. The RADIUS agent can be implemented on a Microsoft NPS/IAS or FreeRADIUS server.



For more information on how to install and configure SAS Agent for IAS/NPS, refer to: http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-Agents-IASNPS.pdf

For more details on how to install and configure FreeRADIUS, refer to the *SAS FreeRADIUS Agent Configuration Guide*.

This document demonstrates the solution using the SAS cloud hosted RADIUS service.

RADIUS-based Authentication using SAS-SPE and SAS-PCE

In addition to the pure cloud-based offering, SafeNet Authentication Service comes with two on-premises versions:

- **SafeNet Authentication Service – Service Provider Edition (SPE)** – An on-premises version of SafeNet Authentication Service targeted at service providers interested in hosting SAS in their data center.
- **SafeNet Authentication Service – Private Cloud Edition (PCE)** – An on-premises version of SafeNet Authentication Service targeted at organizations interested in hosting SAS in their private cloud environment.

For both on-premises versions, SAS can be integrated with the following solutions that serve as local RADIUS servers:

- **Microsoft Network Policy Server (MS-NPS) or the legacy Microsoft Internet Authentication Service (MS-IAS)** — SafeNet Authentication Service is integrated with the local RADIUS servers using a special on-premises agent called SAS Agent for Microsoft IAS and NPS.

  For more information on how to install and configure the SAS Agent for Microsoft IAS and NPS, refer to the following document:

  http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-Agents-IASNPS.pdf

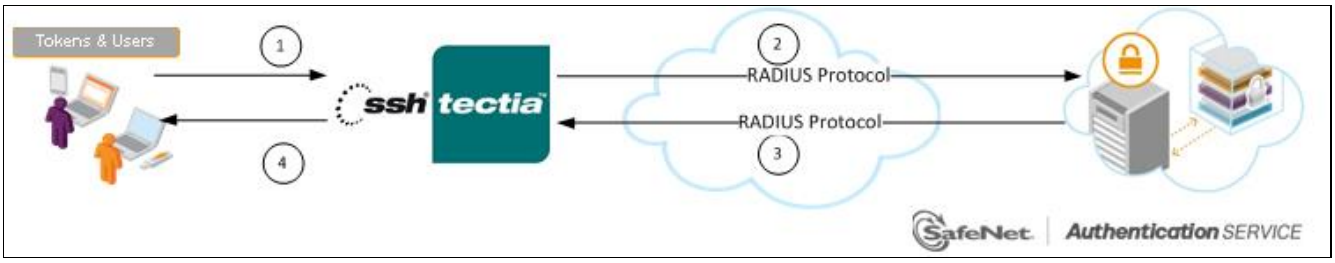
- **FreeRADIUS** — The SAS FreeRADIUS Agent is a strong authentication agent that is able to communicate with SAS through the RADIUS protocol.

  For more information on how to install and configure the SAS FreeRADIUS Agent, refer to the SafeNet Support Portal.

RADIUS Authentication Flow using SAS

SafeNet Authentication Service 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 authenticator.
2. Tectia SSH sends a RADIUS request with the user's credentials to SafeNet Authentication Service for validation.
3. The SAS 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 SAS.

RADIUS Prerequisites

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

- End users can authenticate through 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 Service

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

- Synchronizing user stores to SAS
- Authenticator assignment in SAS
- Adding Tectia SSH as an Authentication Node in SAS
- Checking the SAS RADIUS IP address

Synchronizing User Stores to SafeNet Authentication Service

Before SAS can authenticate any user in your organization, you must create a user store in SAS that reflects the users that would need to use multi-factor authentication. User records are created in the SAS user store using one of the following methods:

- Manually, one user at a time using the **Create User** shortcut
- Manually, by importing one or more user records via a flat file
- Automatically, by synchronizing with your Active Directory/LDAP server using the SAS Synchronization Agent

For further details on importing users to SafeNet Authentication Service, refer to the section on “creating users” in the *SafeNet Authentication Service Subscriber Account Operator Guide*.

http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-SPE-SubscriberAccountOperatorGuide.pdf

All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.

Authenticator Assignment in SAS

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

The following authenticators are supported:

- eToken PASS
- SMS tokens
- MP-1 software token
- MobilePASS

Authenticators can be assigned to users in two ways:

- **Manual provisioning** – Assign an authenticator to users one by one.
- **Provisioning rules** – The administrator can set provisioning rules in SAS so that the rules will be triggered when group memberships and other user attributes change; an authenticator will be assigned automatically to the user.

Refer to “provisioning rules” in the *SafeNet Authentication Service - Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SAS user store.

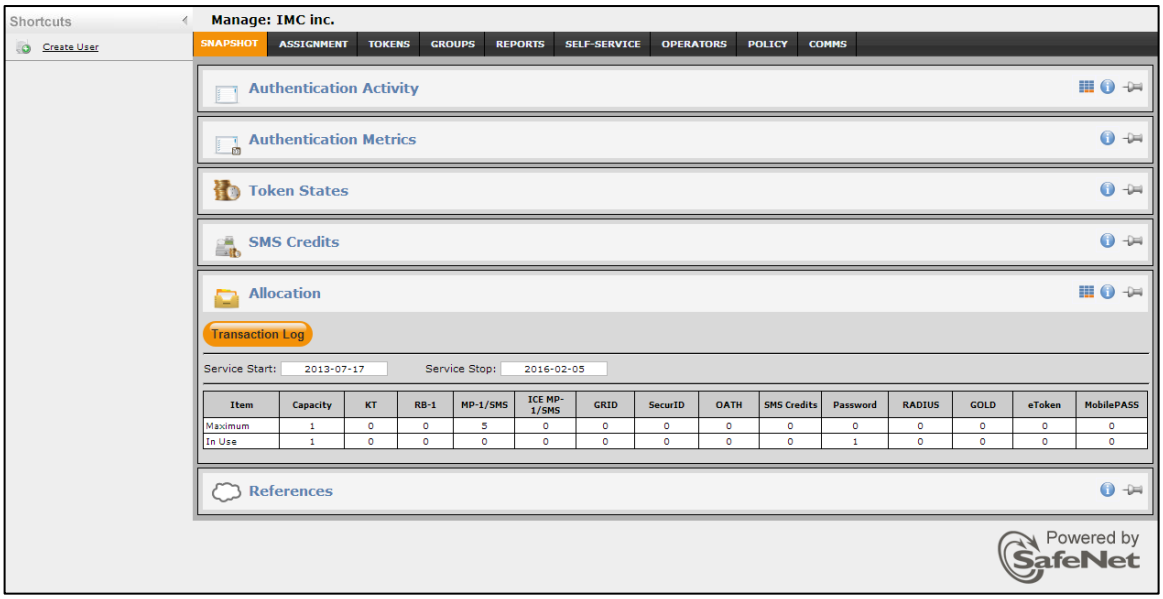
http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-SPE-SubscriberAccountOperatorGuide.pdf

Adding Tectia SSH as an Authentication Node in SAS

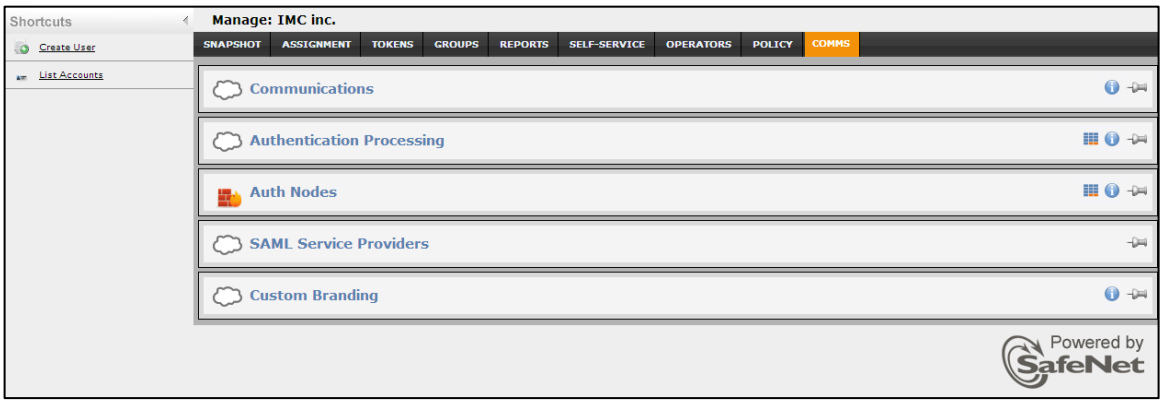
Add a RADIUS entry in the SAS **Authentication Nodes** module to prepare it to receive RADIUS authentication requests from Tectia SSH. You will need the IP address of Tectia SSH and the shared secret to be used by both SAS and Tectia SSH.

To add an Authentication Node in SAS:

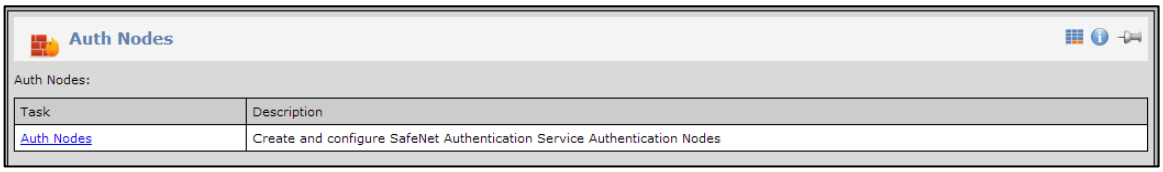
1. Log in to the SAS console with an Operator account.



2. Click the **COMMS** tab, and then select the **Auth Nodes** module.



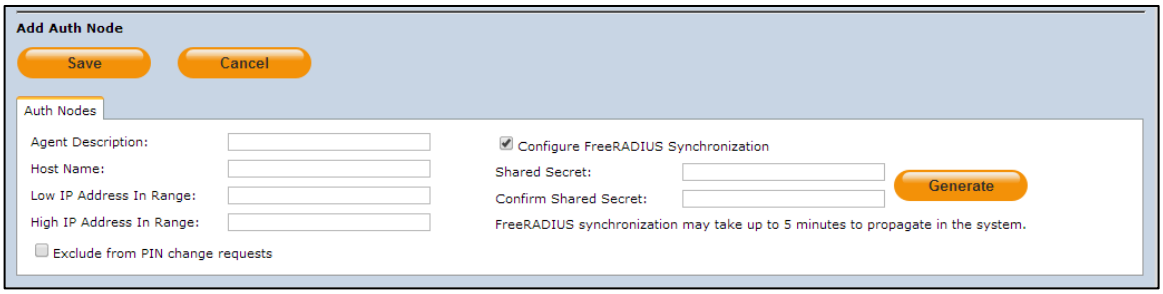
3. In the **Auth Nodes** module, click the **Auth Nodes** link.



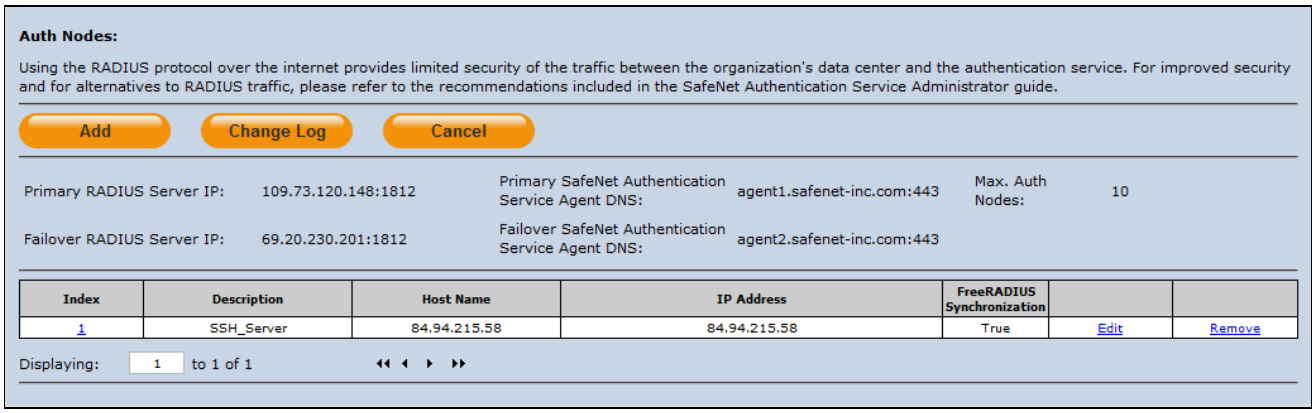
4. Click **Add**.

5. In the **Add Auth Nodes** section, complete the following fields, and then click **Save**:

Agent Description	Enter a host description.
Host Name	Enter the name of the host that will authenticate with SAS.
Low IP Address In Range	Enter the IP address of the host that will authenticate with SAS.
Configure FreeRADIUS Synchronization	Select this option.
Shared Secret	Enter the shared secret key.
Confirm Shared Secret	Re-enter the shared secret key to confirm it.



The Auth Node is added to the system.

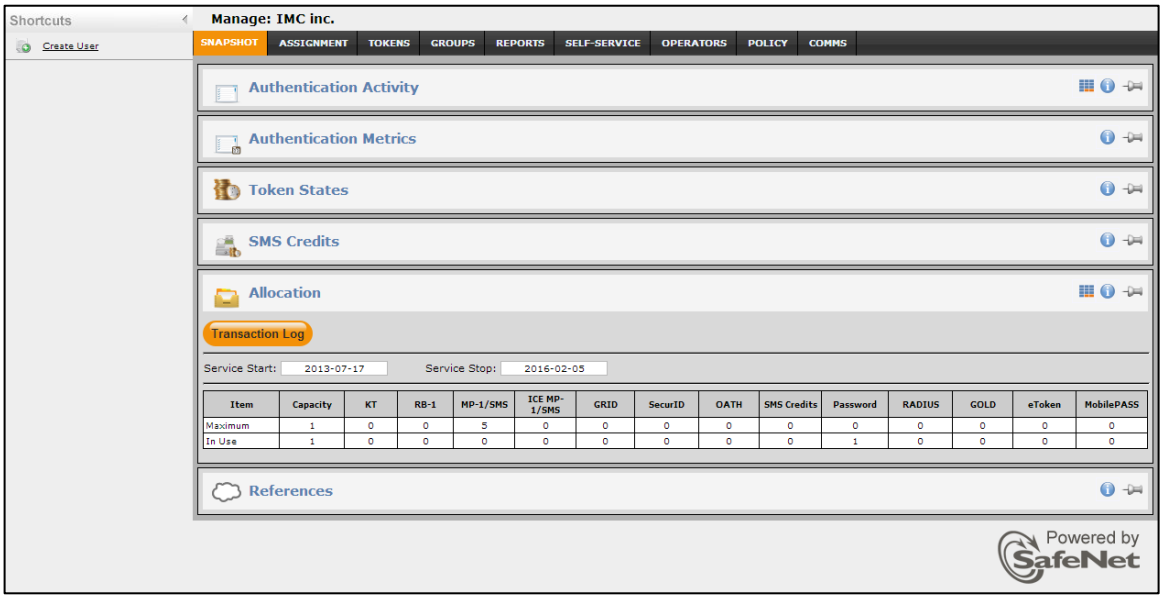


Checking the SAS RADIUS Address

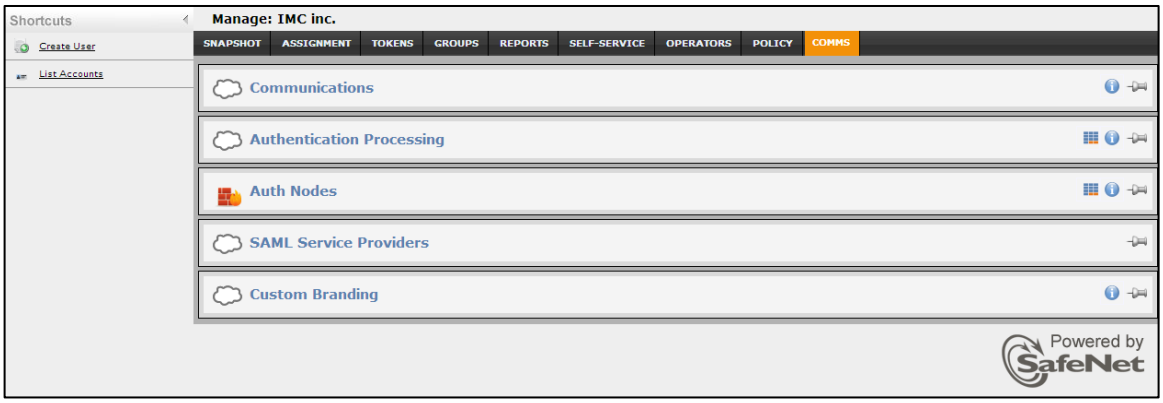
Before adding SafeNet Authentication Service as a RADIUS server in Tectia SSH, check the IP address of the SAS RADIUS server. The IP address will then be added to Tectia SSH as a RADIUS server at a later stage.

To check the IP address of the SAS RADIUS server:

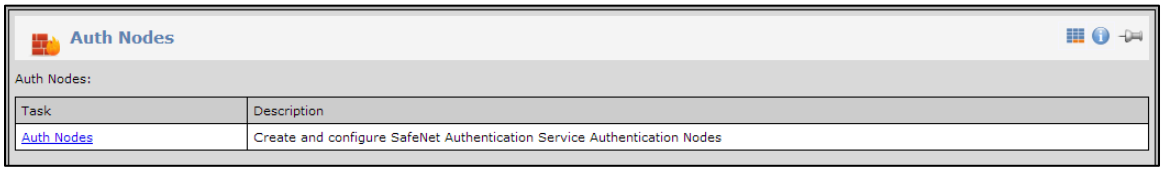
1. Log in to the SAS console with an Operator account.



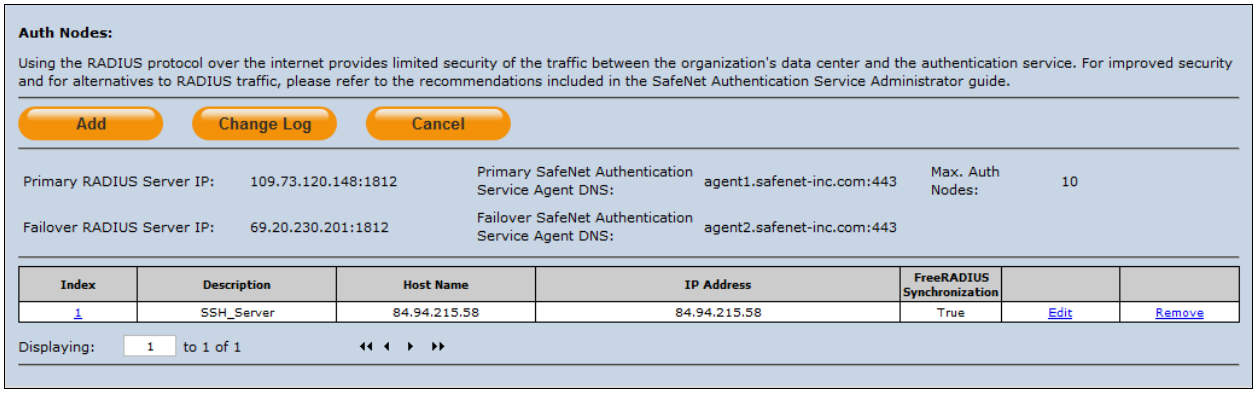
2. Click the **COMMS** tab, and then select the **Auth Nodes** module.



3. Click the **Auth Nodes** link.



The SAS RADIUS server details are displayed.



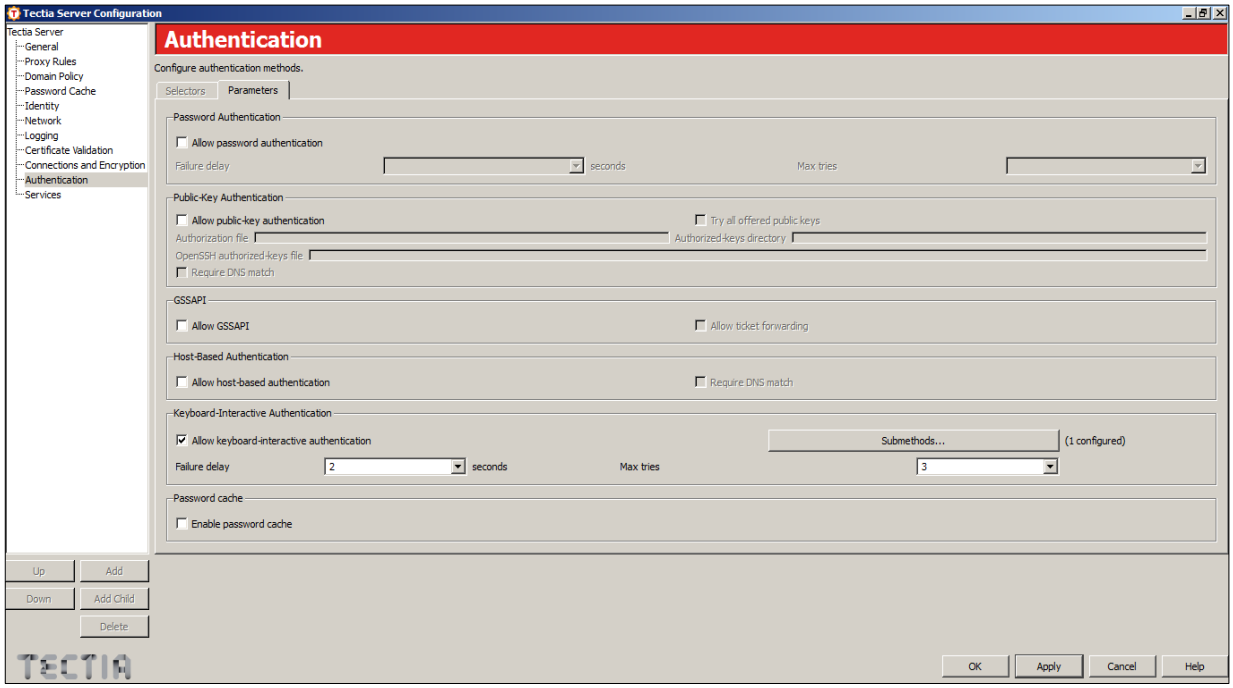
Configuring Tectia SSH

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 Service 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.

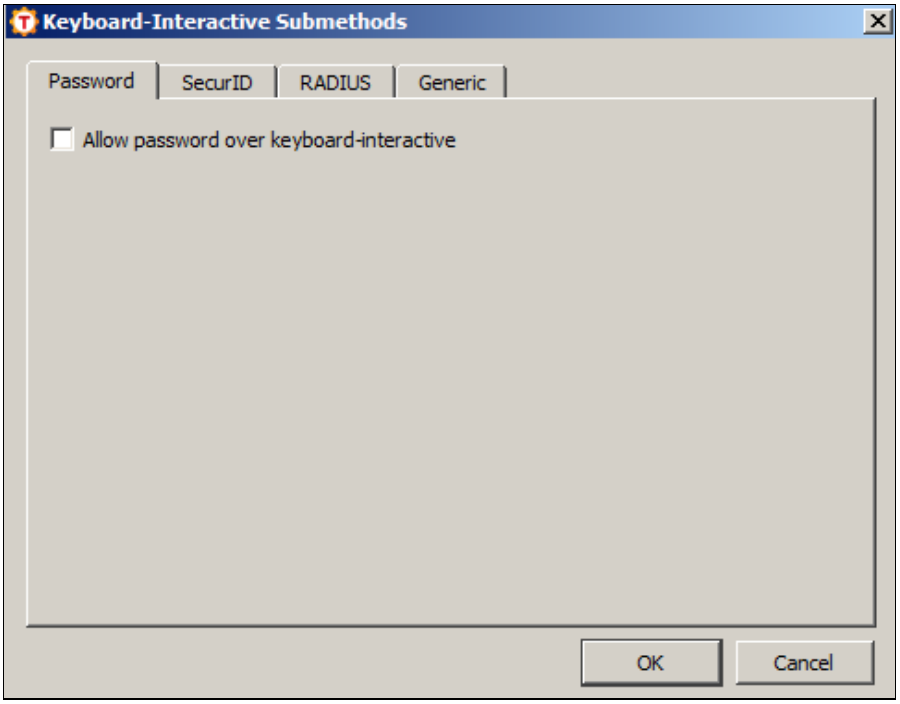
1. Create a text file (for example, **secret.txt**) on the local computer containing the RADIUS server shared secret, and then save the file.
2. Launch the **Tectia Server Configuration** tool from **Start > Programs > SSH Tectia Server > SSH Tectia Server Configuration**.
3. On the **Tectia Server Configuration**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



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

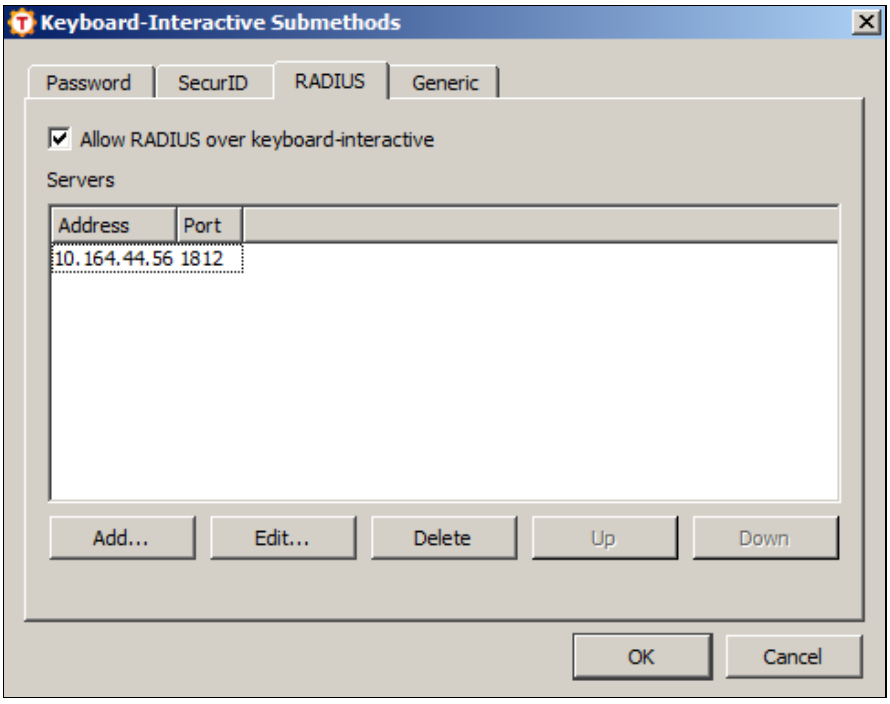
4. In the right pane, click the **Parameters** tab.
5. On the **Parameters** tab, under **Keyboard-Interactive Authentication**, perform the following steps:
   a. Ensure that **Allow keyboard-interactive authentication** is selected (the default mode), and that other authentication methods are not selected.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

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



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

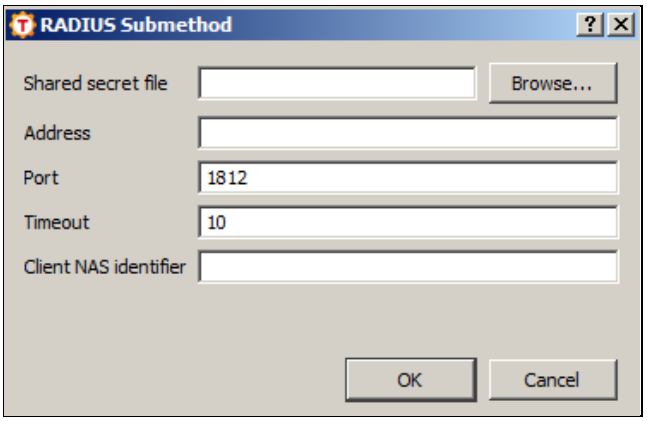
d. On the **Keyboard-Interactive Submethods** window, click the **RADIUS** tab. Select **Allow RADIUS over keyboard-interactive**, and then click **Add**.



(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 SAS server.
Port	Enter **1812**.



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

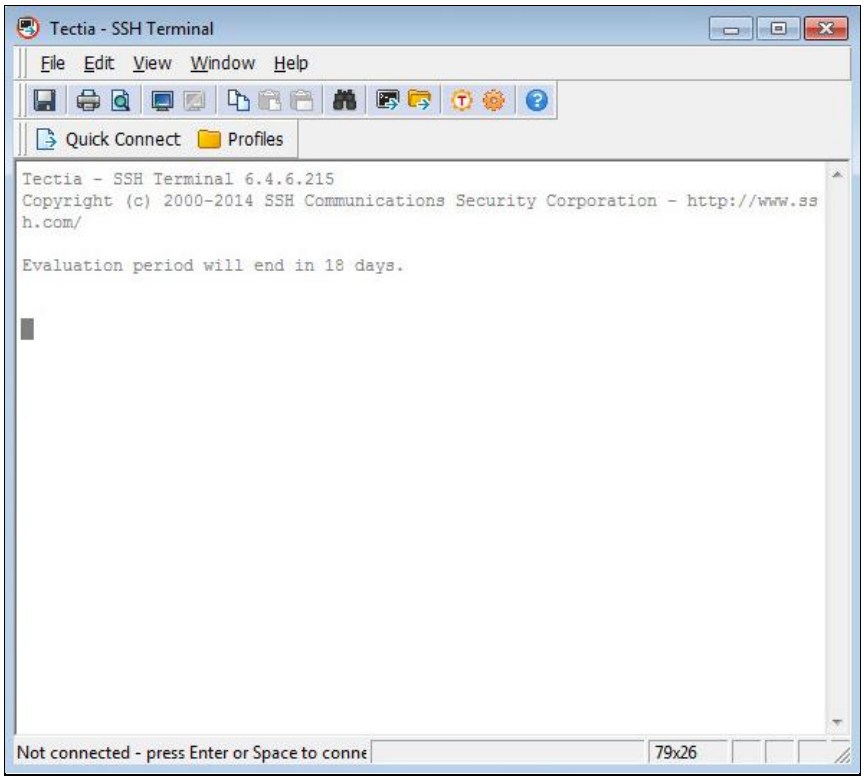
f. Click **OK** twice to return to the **Parameters** tab on the **Tectia Server Configuration** window.

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 SAS.

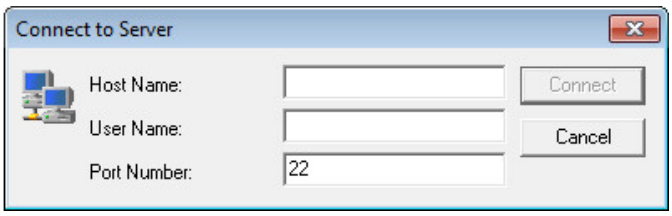
1. Start the **Tectia SSH ConnectSecure Client** or the **Tectia SSH Client** application from **Start > Programs > Tectia ConnectSecure > Tectia SSH Terminal**.
2. On the **Tectia SSH Terminal** window, click **Quick Connect**.



(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**:

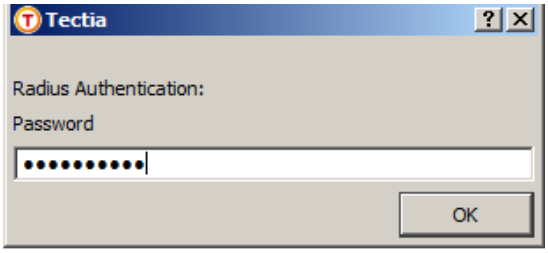
Host Name	Enter the IP address of the Tectia SSH server.
User Name	Enter the user name.



(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.	