SafeNet Authentication Service

Integration Guide

SAS Using RADIUS Protocol with Amazon WorkSpaces

Document Information

Document Part Number	007-012822-001, Rev. A
Release Date	November 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 Amazon WorkSpaces.

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.

Amazon WorkSpaces is a fully managed desktop computing service in the cloud. Amazon WorkSpaces allows customers to easily provision cloud-based desktops that allow end users to access documents, applications, and resources they need with the device of their choice, including laptops, iPad, Kindle Fire, or Android tablets.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in Amazon WorkSpaces using SafeNet OTP authenticators managed by SafeNet Authentication Service.
- Configure Amazon WorkSpaces to work with SafeNet Authentication Service in RADIUS mode.

This document assumes that the Amazon WorkSpaces environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

Amazon WorkSpaces 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

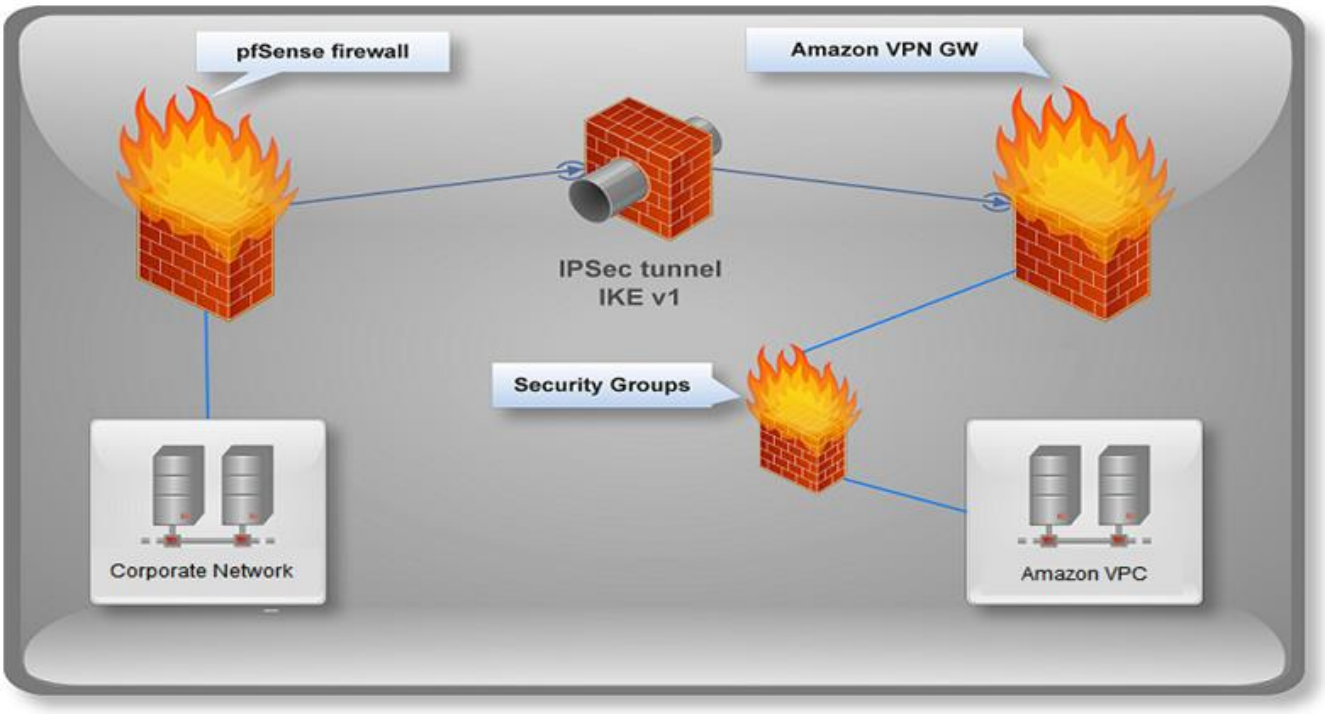
The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Service**—SafeNet's cloud-based authentication service
- **Amazon WorkSpaces**

Setting Up the Amazon Virtual Private Cloud

For using multi-factor authentication with Amazon WorkSpaces, the corporate network should be able to communicate with the Amazon Virtual Private Cloud (VPC). There are several methods through which this can be achieved. Some of the methods are:

- Deploying a VPN solution on the corporate network. For the list of supported VPN devices and other information, see Amazon documentation.
- Using the Amazon Direct Connect Service.
- Deploying Active Directory on a machine with a public IP (not recommended as it is not a secure connection).



In the above scenario, the pfSense firewall is deployed on the corporate network. The pfSense firewall is configured to communicate with the Amazon Virtual Private Network (VPN) through an IPsec tunnel.

On the Amazon Virtual Private Cloud (VPC), the Amazon VPN gateway is configured to communicate with the corporate network through the pfSense firewall.

All communications between the corporate network and Amazon VPC occur through the secured IPsec tunnels.

NOTE: The above setup can be configured using the steps provided:
http://www.heitorlessa.com/site-to-site-vpn-pfsense-and-amazon-vpc/

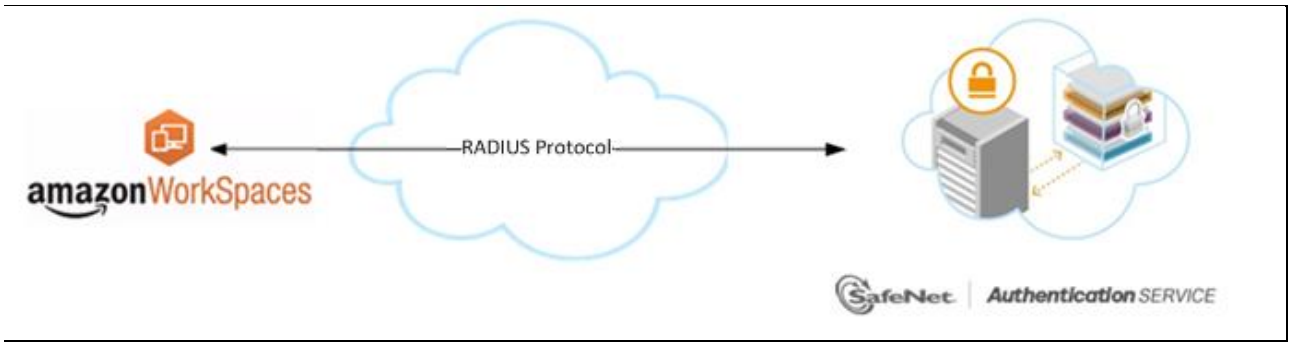
Audience

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

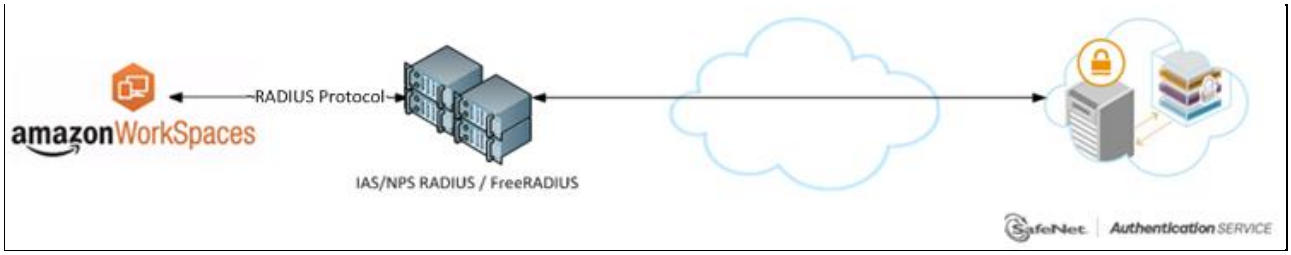
RADIUS-based Authentication using SAS Cloud

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 local RADIUS hosted on-premises.

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.

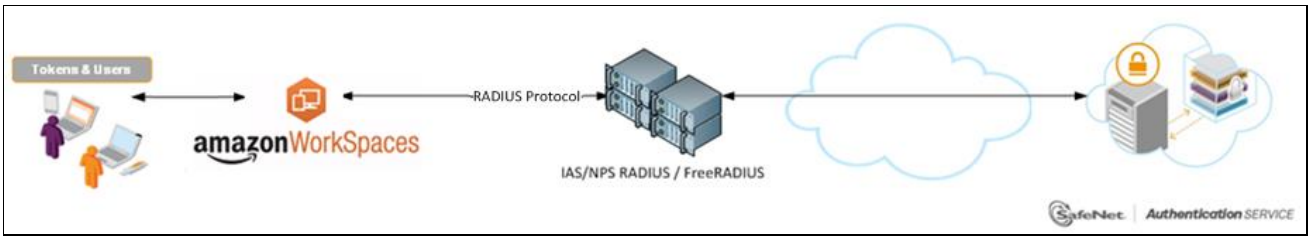
  For more information on how to install and configure the SAS FreeRADIUS Agent, refer to the SafeNet Support Portal.

RADIUS Authentication Flow using SAS

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

Amazon WorkSpaces does not directly support RADIUS server in the cloud. To overcome this, an intermediate RADIUS server is used, which can connect to both Amazon WorkSpaces and SAS Cloud.

The image below describes the data flow of a multi-factor authentication transaction for Amazon WorkSpaces.



1. A user attempts to log on to Amazon WorkSpaces using an OTP authenticator.
2. User enters the AD username and password, and then log in.
3. User enters the OTP and log in.
4. Amazon Workspace checks the AD credentials. If the credentials are correct, it forwards a RADIUS request with the username and OTP to the intermediate RADIUS server.
5. The intermediate RADIUS server forwards the request to SAS Cloud for validation.

6. The SAS authentication reply is sent back to Amazon Workspaces via the on-premises RADIUS server.
7. The user is granted or denied access to the Amazon WorkSpaces based on the OTP value calculation results from SAS.

RADIUS Prerequisites

To enable SafeNet Authentication Service to receive RADIUS requests from Amazon WorkSpaces, ensure the following:

- End users can authenticate through the Amazon WorkSpaces environment with a static password before configuring the Amazon WorkSpaces to use RADIUS authentication.
- Ports 1812/1813 are open to and from Amazon WorkSpaces.
- An on-premises FreeRADIUS server that has connectivity to both Amazon Workspace and SAS Cloud. The FreeRADIUS Agent and Updater are already installed on the RADIUS server.
- 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.

NOTE: Currently, multi-factor authentication is only supported with Amazon Connect Directory. It does not work with Amazon Cloud Directory.

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SAS with Amazon WorkSpaces using the RADIUS protocol requires the following:

- Synchronizing Users Stores to SAS
- Authenticator Assignment in SAS
- Adding Amazon WorkSpaces as an Authentication Node in SAS
- Checking the SAS RADIUS IP address

Synchronizing Users Stores to SafeNet Authentication Service

Before SAS can authenticate any user in your organization, you need to 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 *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 Amazon WorkSpaces.

The following authenticators are supported:

- eToken PASS
- RB-1 Keypad Token
- KT-4 Token
- SafeNet GOLD
- SMS Tokens
- MP-1 Software Token
- GrIDsure Authentication
- 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 SafeNet Authentication Service user store.

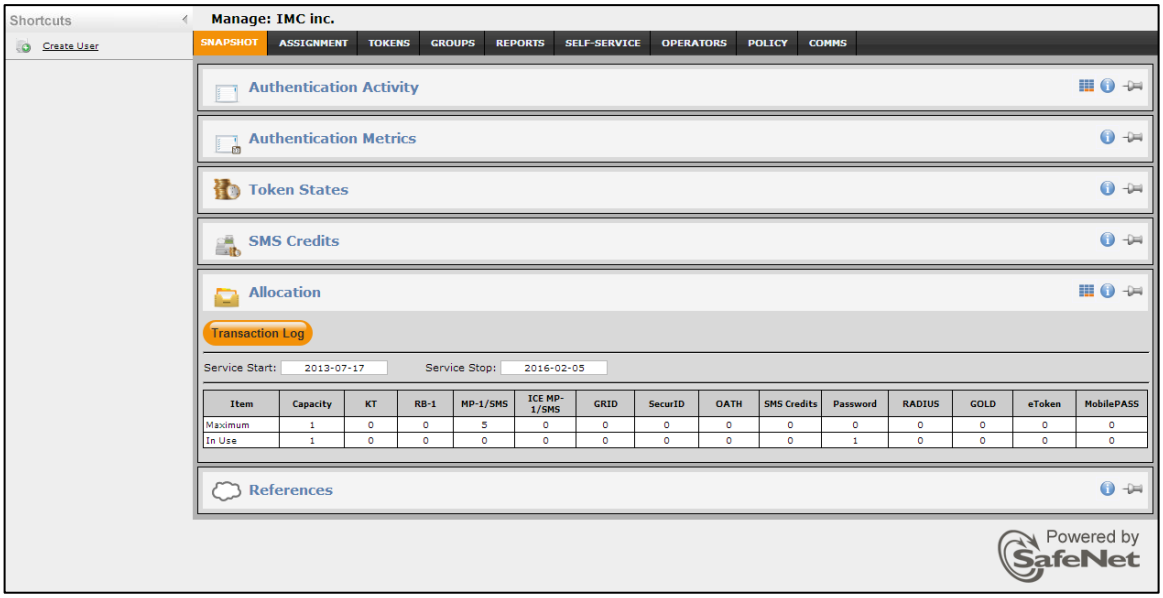
http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-SPE-SubscriberAccountOperatorGuide.pdf

Adding Amazon WorkSpaces as an Authentication Node in SAS

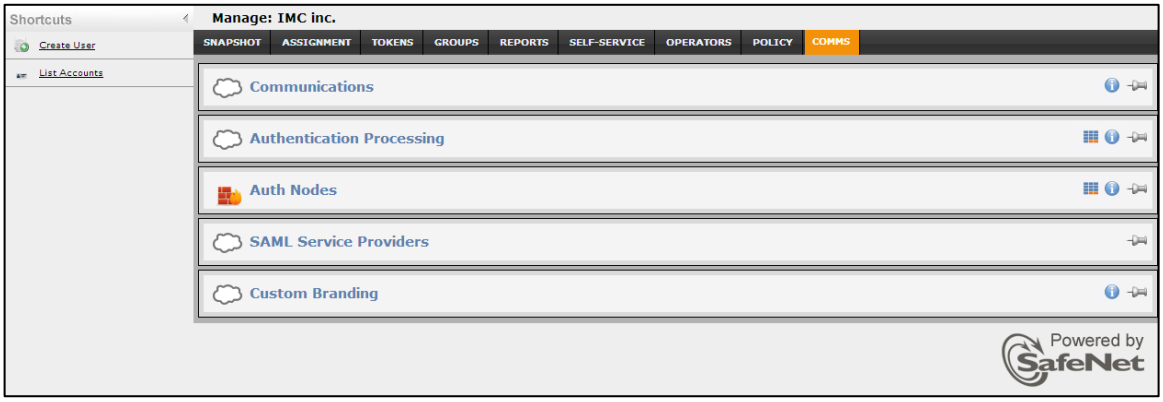
Add a RADIUS entry in the SAS **Authentication Nodes** module to prepare it to receive RADIUS authentication requests from Amazon WorkSpaces. You will need the public IP address of the FreeRADIUS server and the shared secret to be used by both SAS and Amazon WorkSpaces.

To add an Authentication Node in SAS:

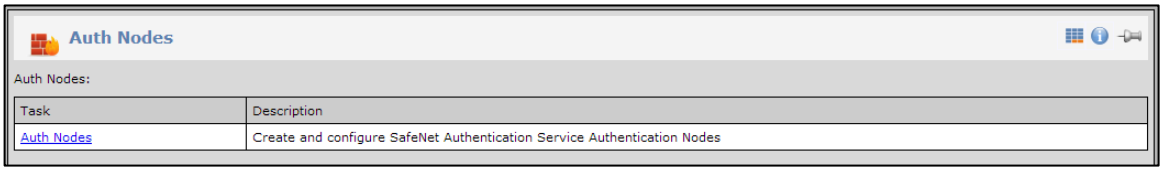
1. Log in to the SAS console with an Operator account.



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



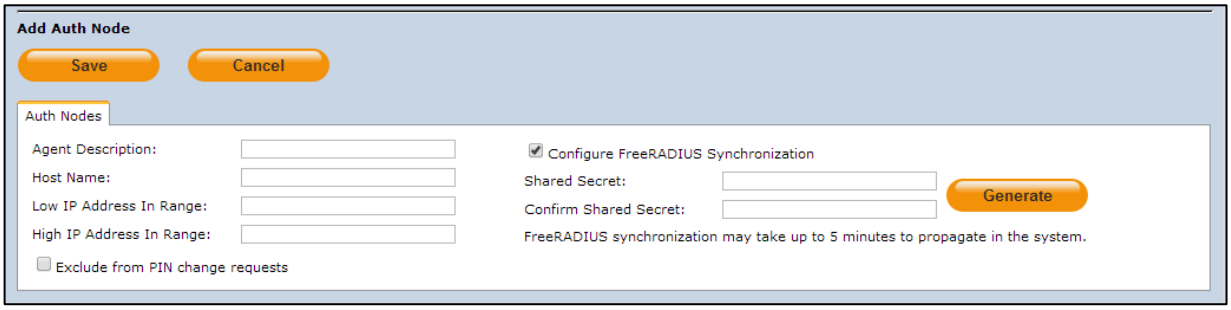
3. In the **Auth Nodes** module, click the **Auth Nodes** link.



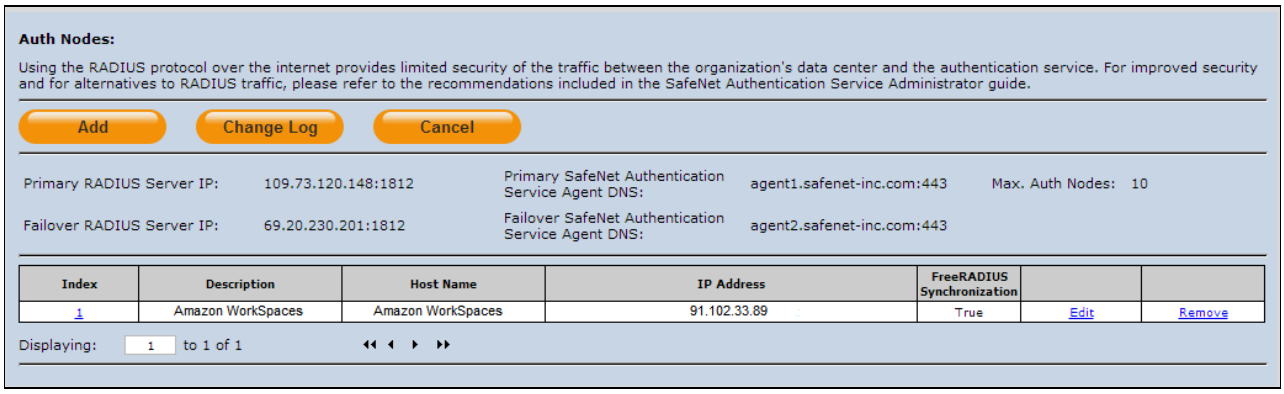
4. Click **Add**.

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 or the lowest IP address in a range of addresses that will authenticate with SAS.
High IP Address In Range	Enter the highest IP address in a range of IP addresses 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 entered above to confirm it.



The Auth Node is added to the system.

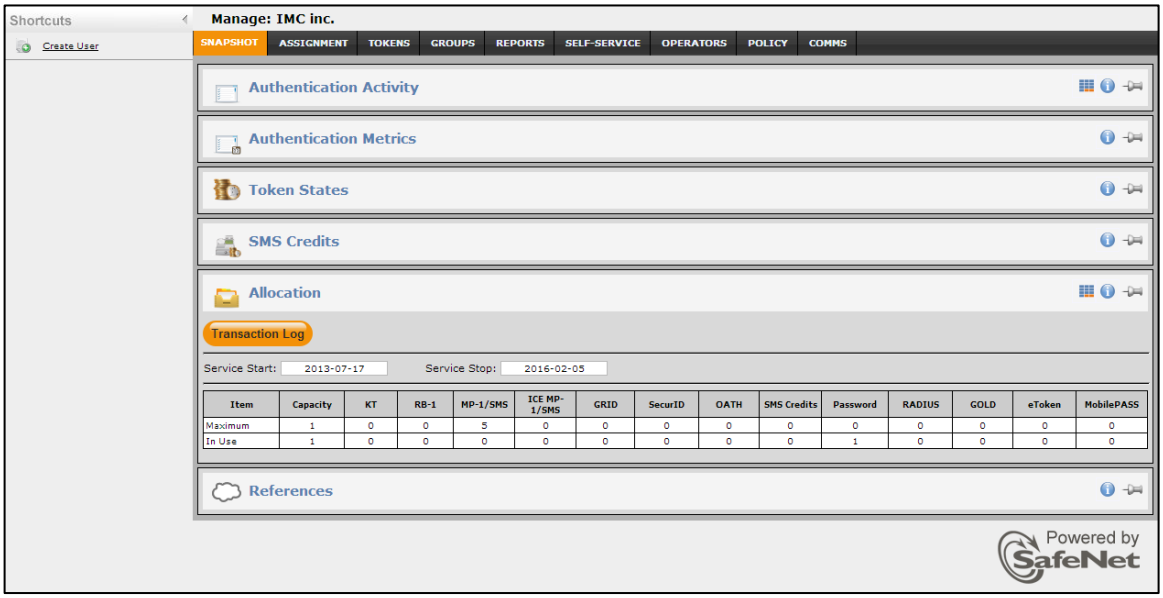


Checking the SAS RADIUS Address

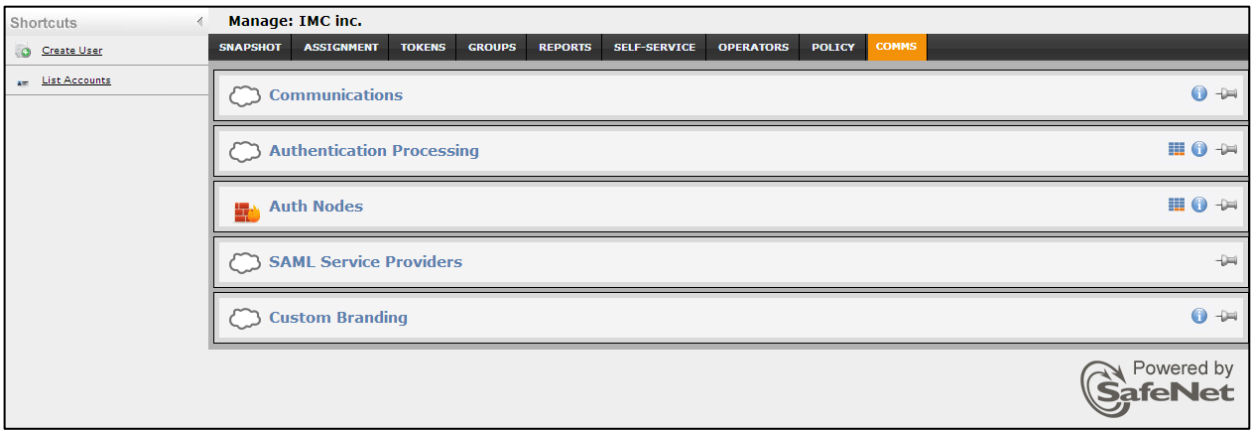
Before adding SafeNet Authentication Service as a RADIUS server in Amazon WorkSpaces, check the IP address of the SAS RADIUS server. The IP address will then be added to Amazon WorkSpaces as a RADIUS server at a later stage.

To check the IP address of the SAS RADIUS server:

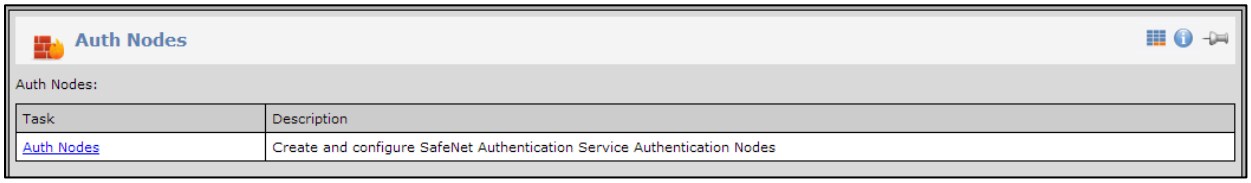
1. Log in to the SAS console with an Operator account.



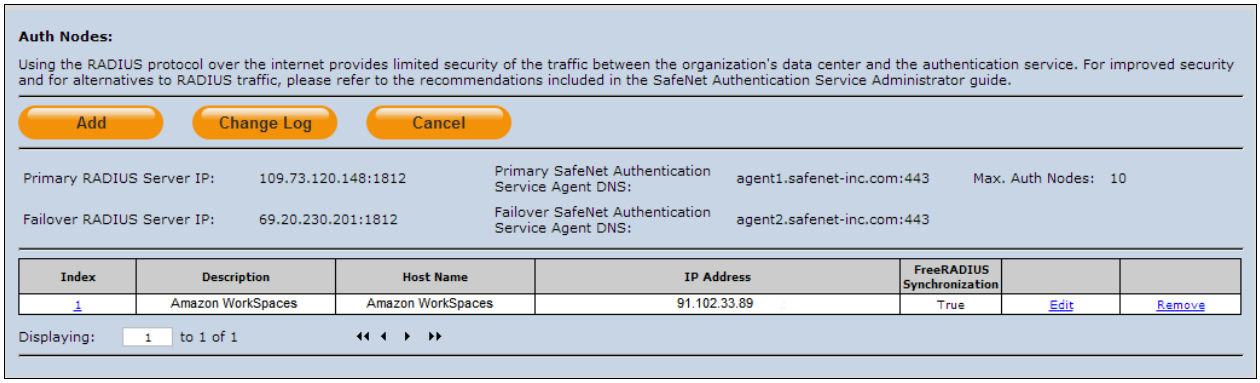
2. Click the **COMMS** tab, and then select the **Auth Nodes** module.



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



The SAS RADIUS server details are displayed.



Configuring the On-Premises FreeRADIUS Server

Configure the on-premises FreeRADIUS server so that it can communicate with both Amazon WorkSpaces and SAS Cloud.

Add Amazon WorkSpaces as a RADIUS Client in FreeRADIUS

1. Go to the following directory: **/opt/freeradius/freeradius-server-2.2.0/etc/raddb/**
2. Open the **clients.conf** file.
3. At the end of the **clients.conf** file, add the Amazon WorkSpaces Connected Directory as a RADIUS client. The Connected Directory has two IP addresses (one for each subnet). Both of the subnet IPs should be added as a separate client with the same shared secret. The IP addresses can be found in the Directory details on the Amazon WorkSpaces console.

   client "Client Name " {
   ipaddr = 10.10.11.3
   secret = '1111'
   }
4. Save the file.

Edit the FreeRADIUS Agent Configuration File

1. Go to the following directory: **/usr/local/cryptocard/freeradius/**
2. Open the **CryptocardFreeRadiusConfig** file.
3. Make the following changes to the file:
   a. Under Section 7, change the default value from 0 to 1.

      The RADIUS authentication request will pass with the original IP of the client. It enables the FreeRADIUS server to accept requests from clients on different SAS accounts.

      The value 0 indicates that IP address passing is OFF.

      The value 1 indicates that IP address passing is ON.

   b. Under Section 16, enter the **Primary SAS Agent DNS**. To get the **Primary SAS Agent DNS**, refer to “Checking the SAS RADIUS Address” on page 12.

   c. Under Section 17, enter **port 443**.

   d. Under Section 18, change the value to **30000**.

   e. Under Section 20, change the value to 1, as SAS cloud validates on HTTPS.

The sample content of the **CryptocardFreeRadiusConfig** file is shown below.

```
#######  Primary Token Validator START
#
###### Section 16: Primary TokenValidator IP Address
agent1.safenet-inc.com
######
#
###### Section 17: Primary TokenValidator Port
443
######
#
###### Section 18: Primary TokenValidator Timeout in milli seconds
30000
######
#
###### Section 19: Path to Primary TokenValidator
/TokenValidator/TokenValidator.asmx
######
#
###### Section 20: Primary TokenValidator connection is HTTPS or HTTP
#                   1 - HTTPS
#                   0 - HTTP
1
######
```

4. Save the file and exit the editor.
5. Restart the FreeRADIUS server.

Configuring Amazon WorkSpaces

Enable multi-factor authentication for Amazon WorkSpaces by configuring the RADIUS server. In addition, add the details of the intermediate RADIUS server in Amazon Directory.

1. Log in to the **Amazon WorkSpaces Management Console**.
2. In the left pane, click **Directories**.

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

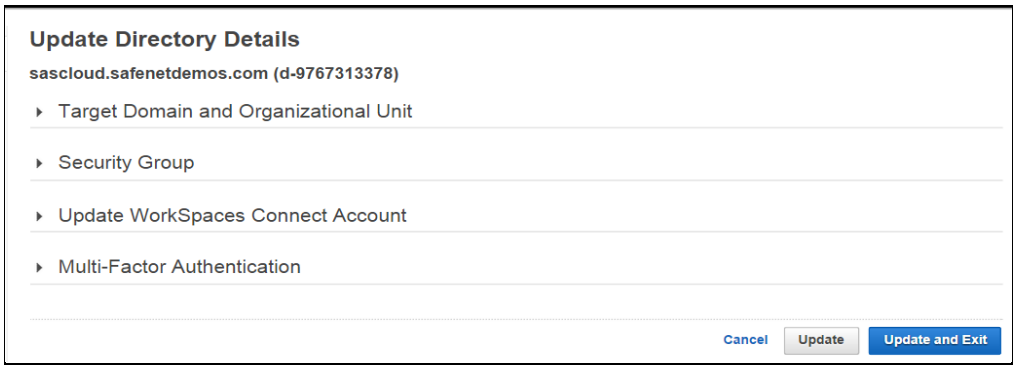
3. To enable MFA for the users under a directory, select the check box for that directory.

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

4. Click **Actions > Update Details**.

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

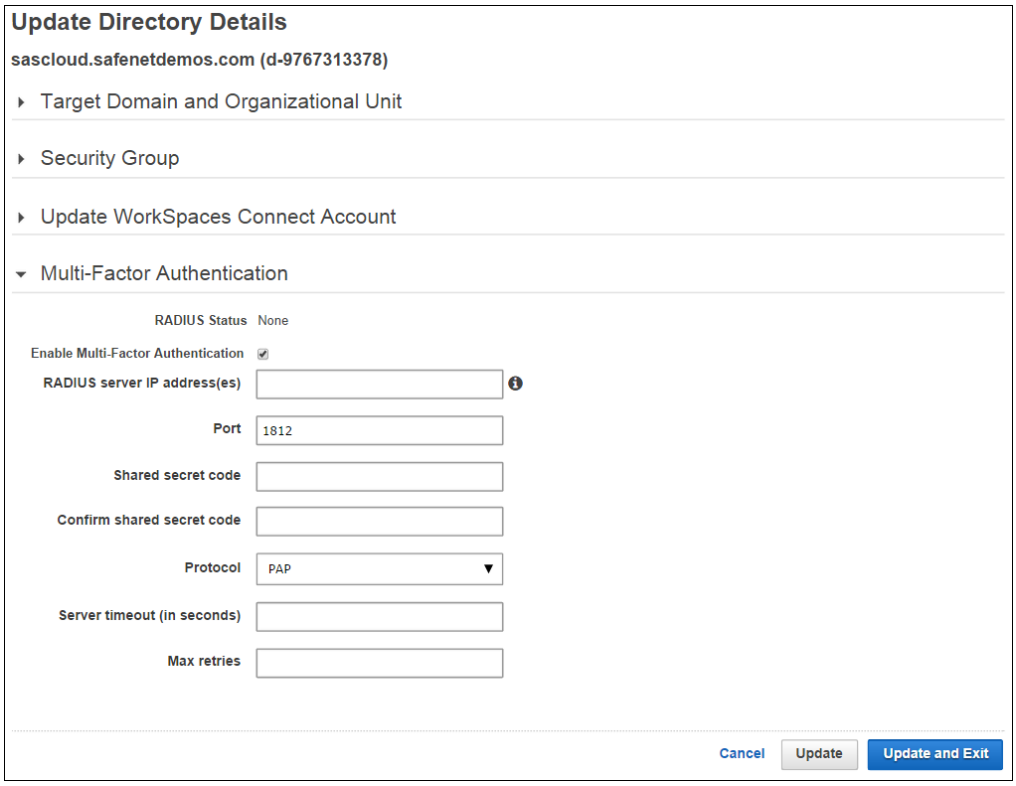
5. In the **Update Directory Details** window, click **Multi-Factor Authentication**.



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

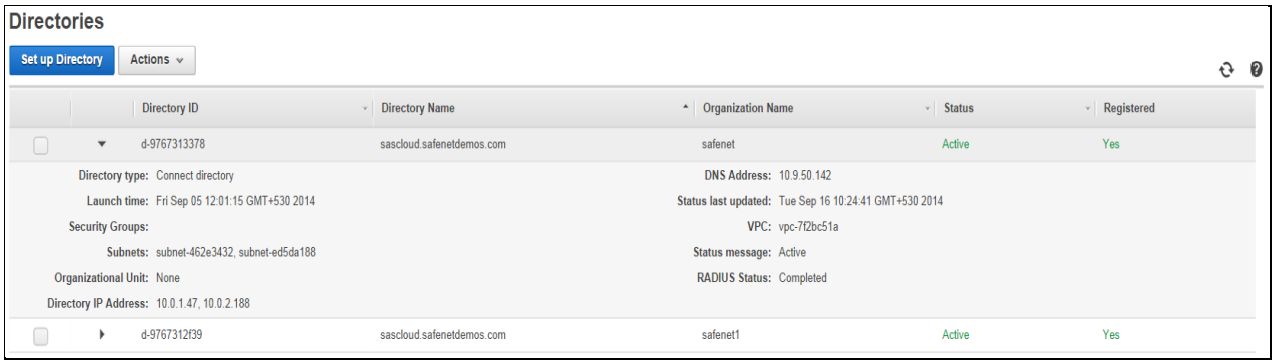
6. Select **Enable Multi-Factor Authentication**, and then complete the following fields. When finished, click **Update and Exit**.

RADIUS server IP address(es)	Enter the IP address of the on-premises RADIUS server.
Port	Enter the port number of the RADIUS server.
Shared secret code	Enter the shared secret key. It should be same as entered in FreeRADIUS server.
Confirm shared secret code	Re-enter the shared secret key.
Protocol	Select **PAP**.
Server timeout (in seconds)	Enter the timeout period for server.
Max retries	Enter the maximum number of retries.



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

7. Amazon takes few minutes to check connectivity with the RADIUS server. To check the RADIUS status of the directory, expand the Directory ID. The details are shown below the row. Verify that **Completed** is displayed for the **RADIUS Status**.

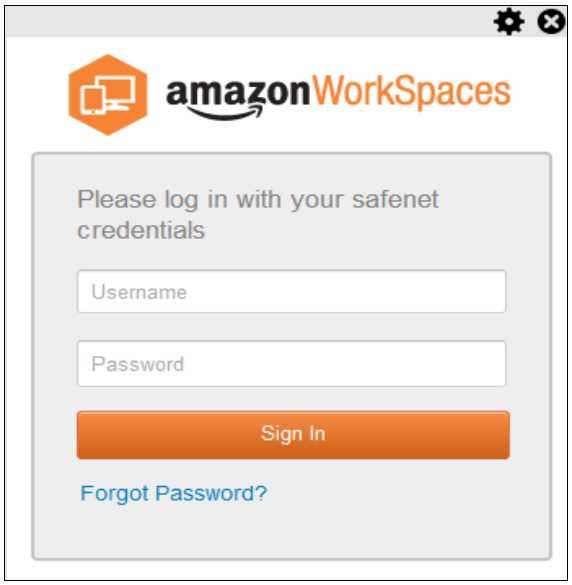


(The screen image above is from Amazon®. Trademarks are the property of their respective owners.)

Running the Solution

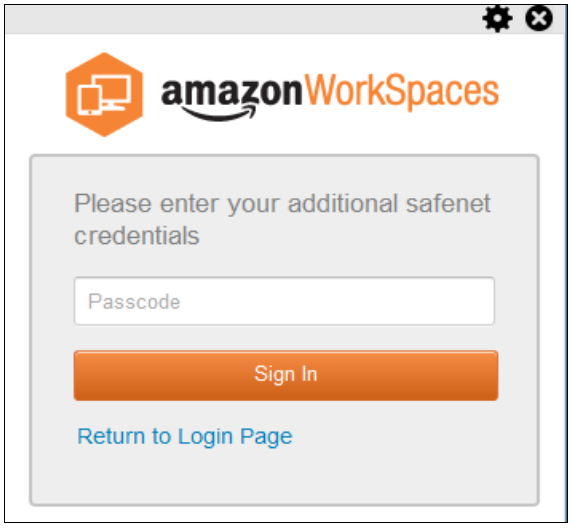
The Amazon WorkSpaces Client application is used to connect to Amazon Workspaces. The client should be installed on the machine from where the user wishes to access Amazon Workspaces.

1. Start the **Amazon Workspaces Client** application.
2. In the login window, enter your username and Active Directory password, and then click **Sign In**.



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

3. Enter the OTP in the **Passcode** field, and then click **Sign In**.



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

On successful authentication, the user will be logged in to Amazon WorkSpaces.

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

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.	