

# SafeNet Authentication Service Integration Guide

Using RADIUS Protocol for CryptoAuditor

All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2017 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

**Document Part Number:** 007-013796-001, Rev. A

**Release Date:** August 2017

# Contents

|   |    |
|---|----|
| Third-Party Software Acknowledgement .....  | 4  |
| Description .....   | 4  |
| Applicability .....   | 4  |
| Environment .....   | 5  |
| Audience .....  | 5  |
| RADIUS-based Authentication using SafeNet Authentication Service Cloud .....                                      | 5  |
| RADIUS-based Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE ..... | 6  |
| RADIUS Authentication Flow using SafeNet Authentication Service .....   | 6  |
| RADIUS Prerequisites .....  | 7  |
| Configuring SafeNet Authentication Service .....  | 7  |
| Creating Users Stores in SafeNet Authentication Service .....   | 7  |
| Assigning an Authenticator in SafeNet Authentication Service .....  | 8  |
| Adding CryptoAuditor as an Authentication Node in SafeNet Authentication Service .....                            | 9  |
| Configuring CryptoAuditor .....   | 11 |
| Configuring External RADIUS Authentication Server .....   | 11 |
| Creating a Rule to Connect the Destination Server with SSH .....  | 13 |
| Creating a Rule to Connect the Destination Server with RDP .....  | 19 |
| Running the Solution .....  | 24 |
| Authentication for SSH Session .....  | 24 |
| Authentication for RDP Session .....  | 25 |
| Support Contacts .....  | 27 |

# Third-Party Software Acknowledgement

---

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

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

## Description

---

SafeNet Authentication Service (SAS) 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.

CryptoAuditor from SSH Communications Security Corporation reduces the security risks when organizations use SSH or RDP for remote system access.

CryptoAuditor monitors, controls, and audits encrypted administrator sessions, 3rd party access, and file transfers.

CryptoAuditor allows you to see, control, and record what happens inside encrypted privileged sessions to your corporate resources. CryptoAuditor monitors and controls encrypted secure connections, and enforces your corporate security policy also on privileged users.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in CryptoAuditor using SafeNet one-time password (OTP) authenticators managed by SafeNet Authentication Service.
- Configure CryptoAuditor to work with SafeNet Authentication Service in the RADIUS mode.

It is assumed that the CryptoAuditor environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

CryptoAuditor 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 – Private Cloud Edition (SAS-PCE)**
- **CryptoAuditor**—Version 2.2.1.25

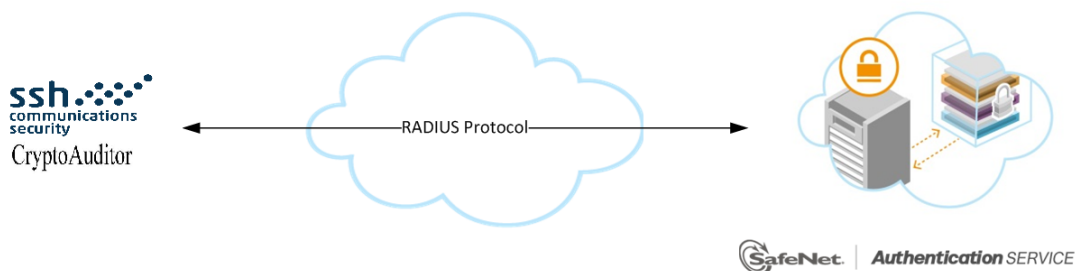
## Audience

This document is targeted to system administrators who are familiar with CryptoAuditor, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service (SAS).

## RADIUS-based Authentication using SafeNet Authentication Service Cloud

SafeNet Authentication Service (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.



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

For more information on how to install and configure SAS Agent for IAS/NPS, refer to:

[http://www2.gemalto.com/sas-downloads/docs/007-012390-002\\_SAS\\_Agent\\_for\\_NPS\\_1.30\\_ConfigurationGuide\\_RevD.pdf](http://www2.gemalto.com/sas-downloads/docs/007-012390-002_SAS_Agent_for_NPS_1.30_ConfigurationGuide_RevD.pdf)

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

# RADIUS-based Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE

For both on-premises versions, SafeNet Authentication Service (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.gemalto.com/sas-downloads/docs/007-012390-002\\_SAS\\_Agent\\_for\\_NPS\\_1.30\\_ConfigurationGuide\\_RevD.pdf](http://www2.gemalto.com/sas-downloads/docs/007-012390-002_SAS_Agent_for_NPS_1.30_ConfigurationGuide_RevD.pdf)

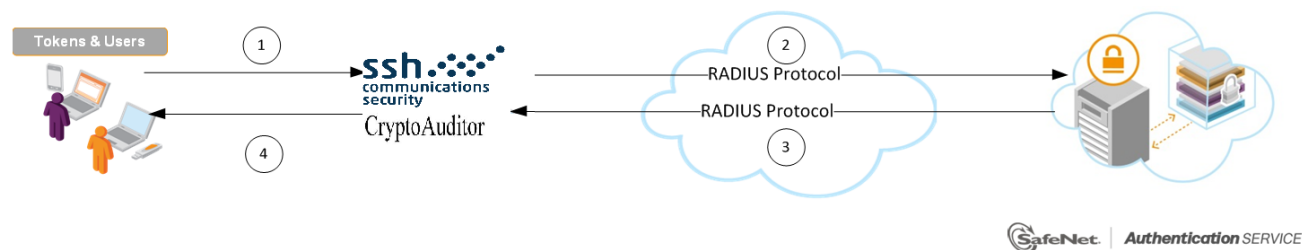
- **FreeRADIUS**—The SAS FreeRADIUS Agent is a strong authentication agent that is able to communicate with SAS through the RADIUS protocol.

For more information on how to install and configure the SAS FreeRADIUS Agent, refer to the [Gemalto Support Portal](#).

## RADIUS Authentication Flow using SafeNet Authentication Service

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

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



1. A user attempts to log on to CryptoAuditor using an OTP authenticator.
2. CryptoAuditor sends a RADIUS request with the user's credentials to SafeNet Authentication Service (SAS) for validation.
3. The SAS authentication reply is sent back to CryptoAuditor.
4. The user is granted or denied access to CryptoAuditor based on the OTP value calculation results from SAS.

# RADIUS Prerequisites

---

To enable SafeNet Authentication Service (SAS) to receive RADIUS requests from CryptoAuditor, ensure the following:

- End users can authenticate from the CryptoAuditor environment with a static password before configuring the CryptoAuditor to use RADIUS authentication.
- Ports 1812/1813 are open to and from CryptoAuditor.
- A shared secret key has been selected. A shared secret key provides 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 RADIUS client for encryption, decryption, and digital signatures.

## Configuring SafeNet Authentication Service

---

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with CryptoAuditor using RADIUS protocol requires the following:

- Creating Users Stores in SafeNet Authentication Service, page 7
- Assigning an Authenticator in SafeNet Authentication Service, page 8
- Adding CryptoAuditor as an Authentication Node in SafeNet Authentication Service, page 8

## Creating Users Stores in SafeNet Authentication Service

Before SafeNet Authentication Service (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 additional details on importing users to SafeNet Authentication Service, refer to “Creating Users” in the *SafeNet Authentication Service Subscriber Account Operator Guide*:

[https://safenet.gemalto.com/resources/integration-guide/data-protection/Safenet\\_Authentication\\_Service/Safenet\\_Authentication\\_Service\\_\\_Subscriber\\_Account\\_Operator\\_Guide/](https://safenet.gemalto.com/resources/integration-guide/data-protection/Safenet_Authentication_Service/Safenet_Authentication_Service__Subscriber_Account_Operator_Guide/)

All SafeNet Authentication Service documentation can be found on the [SafeNet Knowledge Base](#) site.

## Assigning an Authenticator in SafeNet Authentication Service

SafeNet Authentication Service (SAS) supports a number of authentication methods that can be used as a second authentication factor for users who are authenticating through CryptoAuditor.

The following authenticators are supported:

- eToken PASS
- RB-1 Keypad Token
- KT-4 Token
- SafeNet Gold
- SMS Token
- MP-1 Software Token
- MobilePASS
- MobilePASS+

Authenticators can be assigned to users in two ways:

- **Manual provisioning**—Assign an authenticator to users one at a time.
- **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.

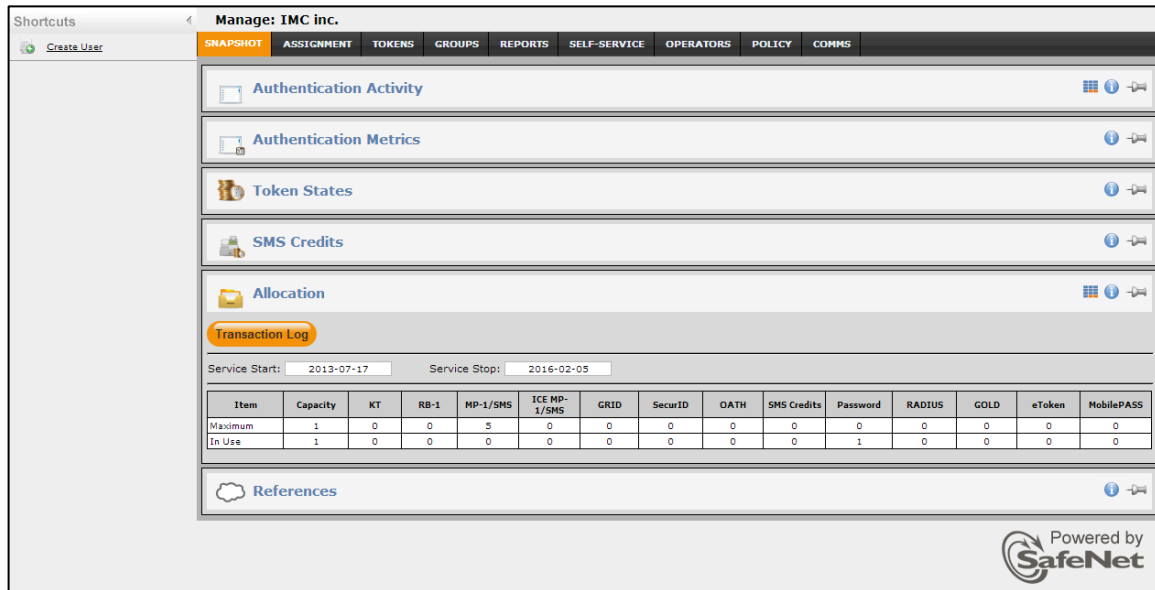
[https://safenet.gemalto.com/resources/integration-guide/data-protection/Safenet\\_Authentication\\_Service/Safenet\\_Authentication\\_Service\\_\\_Subscriber\\_Account\\_Operator\\_Guide/](https://safenet.gemalto.com/resources/integration-guide/data-protection/Safenet_Authentication_Service/Safenet_Authentication_Service__Subscriber_Account_Operator_Guide/)



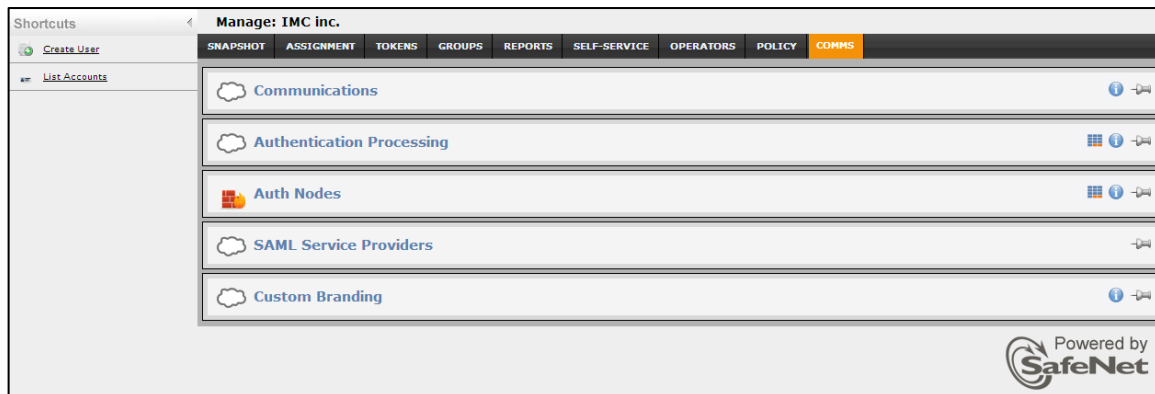
## Adding CryptoAuditor as an Authentication Node in SafeNet Authentication Service

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

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



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



- In the **Auth Nodes** module, click the **Auth Nodes** task.

**Auth Nodes**

Auth Nodes:

| Task                       | Description  |
|----------------------------|--|
| <a href="#">Auth Nodes</a> | Create and configure SafeNet Authentication Service Authentication Nodes |

**Auth Nodes:**

Using the RADIUS protocol over the internet provides limited security of the traffic between the organization's data center and the authentication service. For improved security and for alternatives to RADIUS traffic, please refer to the recommendations included in the SafeNet Authentication Service Administrator guide.

**Add** **Change Log** **Cancel**

|                            |                     |  |                            |                     |
|----------------------------|---------------------|--|----------------------------|---------------------|
| Primary RADIUS Server IP:  | 109.73.120.148:1812 | Primary SafeNet Authentication Service Agent DNS:  | agent1.safenet-inc.com:443 | Max. Auth Nodes: 10 |
| Failover RADIUS Server IP: | 69.20.230.201:1812  | Failover SafeNet Authentication Service Agent DNS: | agent2.safenet-inc.com:443 |                     |

No Records



**NOTE:** Before adding SafeNet Authentication Service (SAS) as a RADIUS server in CryptoAuditor, check its IP address ("Primary RADIUS Server IP"). The IP address will then be added to CryptoAuditor as a RADIUS server at a later stage.

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

|   |  |
|---|--|
| <b>Agent Description</b>                    | Enter a host description.  |
| <b>Host Name</b>                            | Enter the name of the host that will authenticate with SAS.  |
| <b>Low IP Address In Range</b>              | Enter the IP address of the host or the lowest IP address in a range of addresses that will authenticate with SAS (in this case, a range of IP addresses is being used). |
| <b>High IP Address In Range</b>             | Enter the highest IP address in a range of IP addresses that will authenticate with SAS (in this case, a range of IP addresses is being used).                           |
| <b>Configure FreeRADIUS Synchronization</b> | Select this option.  |
| <b>Shared Secret</b>                        | Enter the shared secret key.   |
| <b>Confirm Shared Secret</b>                | Re-enter the shared secret key.  |

**Add Auth Node**

**Save** **Cancel**

Auth Nodes

Agent Description:

Host Name:

Low IP Address In Range:

High IP Address In Range:

☐ Exclude from PIN change requests

☒ Configure FreeRADIUS Synchronization

Shared Secret:

Confirm Shared Secret:

**Generate**

FreeRADIUS synchronization may take up to 5 minutes to propagate in the system.

The authentication node is added to the system.

**Auth Nodes:**  
Using the RADIUS protocol over the Internet provides limited security of the traffic between the organization's data center and the authentication service. For improved security and for alternatives to RADIUS traffic, refer to the recommendations included in the SafeNet Authentication Service Administrator Guide.

AddChange LogCancel

Primary RADIUS Server IP:109.73.120.148:1812

Primary SafeNet Authentication Service Agent:agent1.safenet-inc.com:443

Max. Auth Nodes:10

Fallover RADIUS Server IP:69.20.230.201:1812

Fallover SafeNet Authentication Service Agent:agent2.safenet-inc.com:443

| Index | Auth Node Name | Host Name     | IP Address    | FreeRADIUS Synchronization |      |        |
|-------|----------------|---------------|---------------|----------------------------|------|--------|
| 1     | cryptoauditor  | 184.72.186.22 | 184.72.186.22 | True                       | Edit | Remove |

## Configuring CryptoAuditor

Configuring CryptoAuditor to use the RADIUS protocol as a secondary authentication method requires:

- Configuring External RADIUS Authentication Server, page 11
- Creating a Rule to Connect the Destination Server with SSH, page 13
- Creating a Rule to Connect the Destination Server with RDP, page 19

## Configuring External RADIUS Authentication Server

1. In a web browser, open the following URL:  
**https://<CryptoAuditor IP address>/accounts/login**
2. On the CryptoAuditor login window, enter your administrator **Username** and **Password**, and then click **LOGIN**.

ssh. CryptoAuditor™ 2.2.1.25

Username:

Password:

LOGIN

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

3. On the CryptoAuditor administrator dashboard, click the **Settings** tab.

ssh. CryptoAuditor™ 2.2.1.25

Home

Trails and Logs

Reports

Policy

Admins

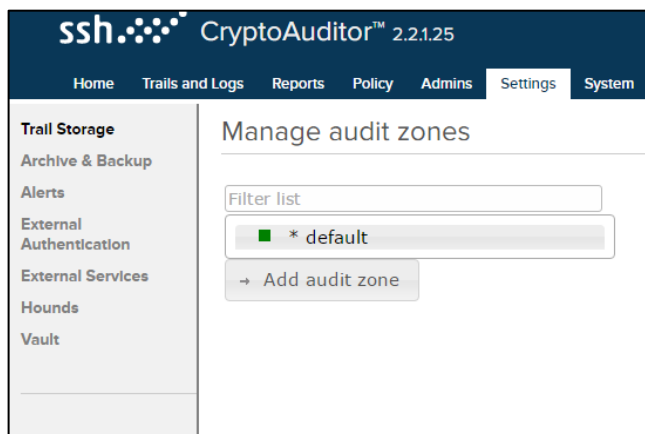
Settings

System

Pending changes

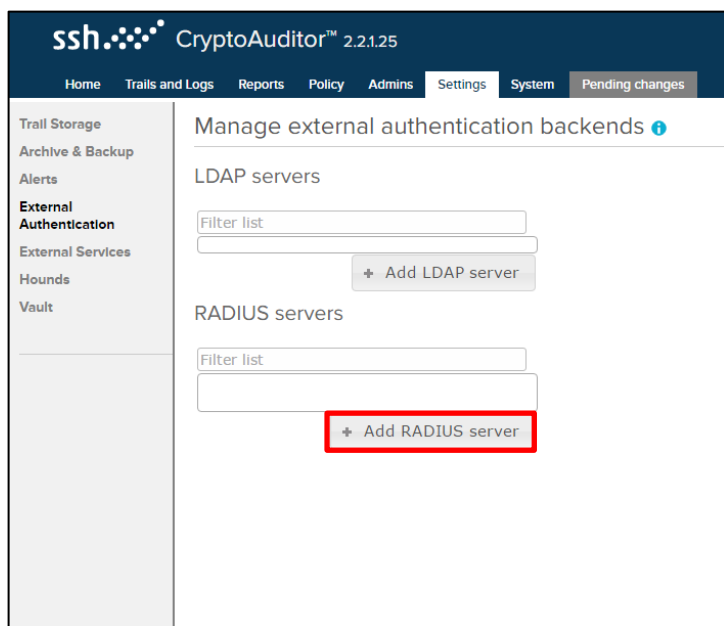
(The screen image above is from CryptoAuditor. Trademarks are the property of their respective owners.)

4. In the left pane, click **External Authentication**.



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

5. In the right pane, under **Manage external authentication backends**, click **+Add RADIUS server**.



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

- Complete the following fields, and then click **SAVE**.

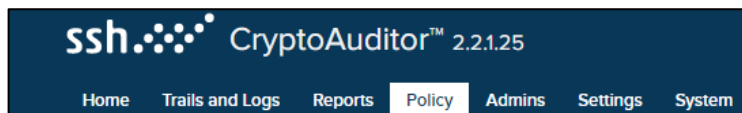
|                                   |  |
|-----------------------------------|--|
| <b>Address</b>                    | Enter the <b>Primary RADIUS Server IP</b> address that is available in the <b>Auth Nodes</b> module of your SAS server. Refer to step 3 of “Adding CryptoAuditor as an Authentication Node in SafeNet Authentication Service” on page 9. |
| <b>Shared secret</b>              | Enter the <b>Shared Secret</b> that you entered earlier in step 5 of “Adding CryptoAuditor as an Authentication Node in SafeNet Authentication Service” on page 9.   |
| <b>Shared secret confirmation</b> | Re-enter the shared secret.  |

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

## Creating a Rule to Connect the Destination Server with SSH

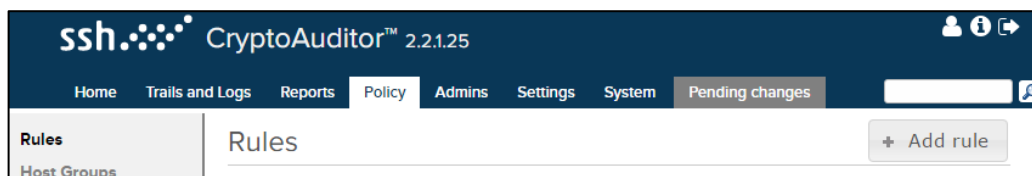
Perform the following steps to create a rule to connect the destination server with SSH:

- On the CryptoAuditor administrator dashboard, click the **Policy** tab.



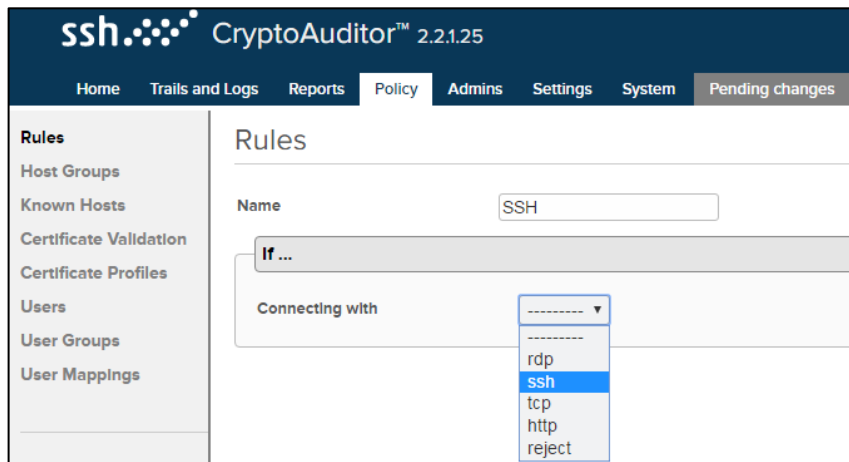
(The screen image above is from CryptoAuditor. Trademarks are the property of their respective owners.)

- In the right pane, under **Rules**, click **+Add rule**.



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

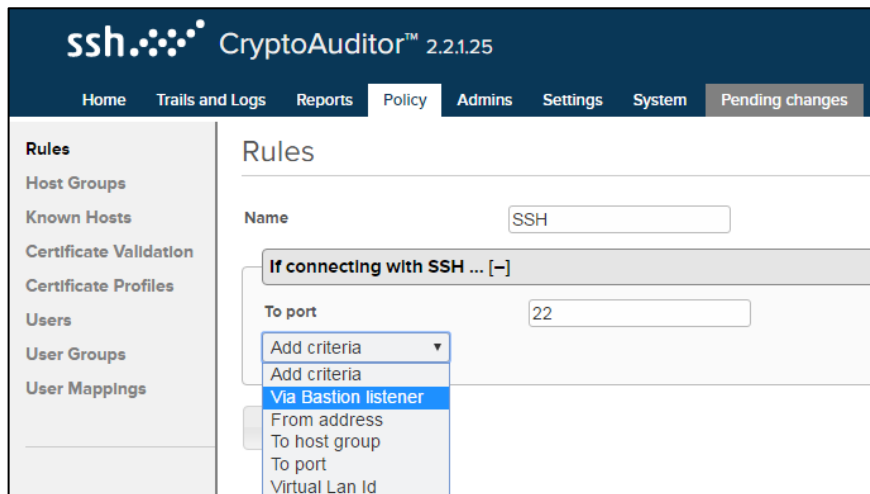
3. In the **Name** field, enter a name for the rule (for example, **SSH**).
4. In the **Connecting with** field, select **ssh**.



The screenshot shows the 'Rules' configuration page in the CryptoAuditor 2.2.1.25 web interface. The 'Name' field contains 'SSH'. The 'Connecting with' dropdown menu is open, displaying a list of protocols: rdp, ssh (highlighted in blue), tcp, http, and reject.

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

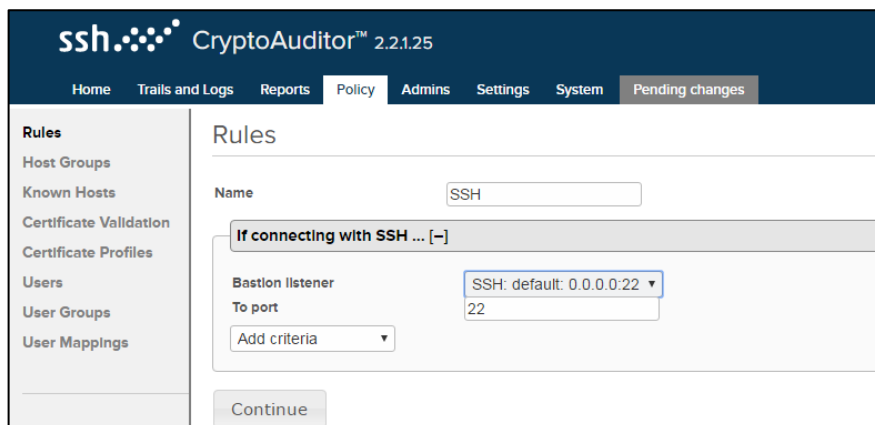
5. In the **To port** field, select **Via Bastion listener**.



The screenshot shows the 'Rules' configuration page in the CryptoAuditor 2.2.1.25 web interface. The 'Name' field contains 'SSH'. The condition 'If connecting with SSH ... [-]' is selected. The 'To port' field contains '22'. The 'Add criteria' dropdown menu is open, displaying a list of criteria: Add criteria, Via Bastion listener (highlighted in blue), From address, To host group, To port, and Virtual Lan Id.

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

6. In the **Bastion listener** field, select **SSH: default: 0.0.0.0:22**, and then click **Continue**.



The screenshot shows the 'Rules' configuration page in the CryptoAuditor 2.2.1.25 web interface. The 'Name' field contains 'SSH'. The condition 'If connecting with SSH ... [-]' is selected. The 'Bastion listener' dropdown menu is open, displaying a list of listeners: SSH: default: 0.0.0.0:22 (highlighted in blue). The 'To port' field contains '22'. The 'Continue' button is visible at the bottom.

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

7. Under **Authentication**, complete the following fields:

|                                       |  |
|---------------------------------------|--|
| <b>Client-to-Hound authentication</b> | Select <b>Authenticate against a RADIUS server</b> .   |
| <b>Radius server</b>                  | Select the RADIUS server IP address (given along with the port number) that you added in step 6 of “Configuring External RADIUS Authentication Server” on page 11. |
| <b>Hound-to-target authentication</b> | Select <b>Mapped user credentials</b> .  |

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

8. Under **Destination**, complete the following fields, and then click **Continue**.

|                                  |  |
|----------------------------------|--|
| <b>Destination selection</b>     | Select <b>Fixed address</b> .                            |
| <b>Fixed destination address</b> | Enter the IP address of the destination server for SSH.  |
| <b>Fixed destination port</b>    | Enter the port number of the destination server for SSH. |

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

9. Click **Save**.

... then [-]

Auditing actions

Members of the group: All users (no selection) ▼

+ Add user group matching

| Auditing Actions | Index                              | Content Inspection                  | IDS |
|------------------|------------------------------------|-------------------------------------|-----|
|                  | Real Time                          | Post-Process                        |     |
| Shell            | Store output ▼                     | <input checked="" type="checkbox"/> |     |
| Exec             | Store full session ▼               | <input checked="" type="checkbox"/> |     |
| SFTP             | Store filenames and control data ▼ | <input checked="" type="checkbox"/> |     |
| SCP              | Store metadata only ▼              | <input type="checkbox"/>            |     |
| Local Tunnels    | Deny channel ▼                     | <input type="checkbox"/>            |     |
| Remote Tunnels   | Deny channel ▼                     | <input type="checkbox"/>            |     |
| X11              | Deny channel ▼                     | <input type="checkbox"/>            |     |
| Other            | Deny channel ▼                     | <input type="checkbox"/>            |     |

Add auditing group

Auditing actions

All other connections matching this rule will be rejected.

Save Cancel

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

10. In the left pane, click **User Mappings**.

ssh. CryptoAuditor™ 2.2.1.25

Home Trails and Logs Reports Policy Admins Settings System Pending changes

Rules

- Host Groups
- Known Hosts
- Certificate Validation
- Certificate Profiles
- Users
- User Groups
- User Mappings

Rules

SSH RDP TCP HTTP

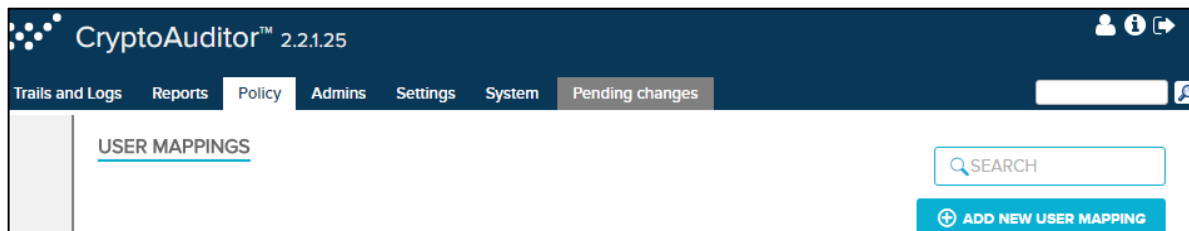
SSH ssh apm

via listener SSH: default: 0.0.0.0:22 to port 22  
authentication in: radius, out: mapped  
fixed destination 54.178.156.198:22

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



11. In the right pane, under **USER MAPPINGS**, click **ADD NEW USER MAPPING**.



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

12. Under **GATEWAY USER**, complete the following fields:

|                      |  |
|----------------------|--|
| <b>USER NAME</b>     | Enter the SAS username (for example, <b>alice</b> ).   |
| <b>USER PROVIDER</b> | Select the RADIUS server IP address (given along with the port number) that you added in step 6 of “Configuring External RADIUS Authentication Server” on page 11. |

| GATEWAY USER   |   |  |
|--|---|--|
| <b>USER NAME</b><br><input type="text" value="alice"/><br><small>Enter a user name for gateway authentication.</small> | <b>USER GROUP</b><br><input type="text" value="....."/><br><small>Select a pre-defined user group in a user database.</small> | <b>USER PROVIDER</b><br><input type="text" value="radius:109.73.120.148:1812"/><br><small>Select a fixed user database for the gateway authentication.</small> |

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

13. Under **TARGET**, complete the following fields:

|                 |  |
|-----------------|--|
| <b>ADDRESS</b>  | Enter the IP address of the destination server.      |
| <b>PORT</b>     | Enter the SSH port number (for example, <b>22</b> ). |
| <b>PROTOCOL</b> | Select <b>SSH</b> .                                  |

| TARGET  |   |  |  |
|---|---|--|--|
| <b>HOST GROUP</b><br><input type="text" value="....."/><br><small>If selected, the user is mapped at any target server that is defined in the host group.</small> | <b>ADDRESS</b><br><input type="text" value="52.195.205.49"/><br><small>Enter host address if you want to make a host-specific user mapping.</small> | <b>PORT</b><br><input type="text" value="22"/> | <b>PROTOCOL</b><br><input type="text" value="SSH"/><br><small>Specify the user mapping to be applied for SSH or RDP only. Leave empty to apply both.</small> |

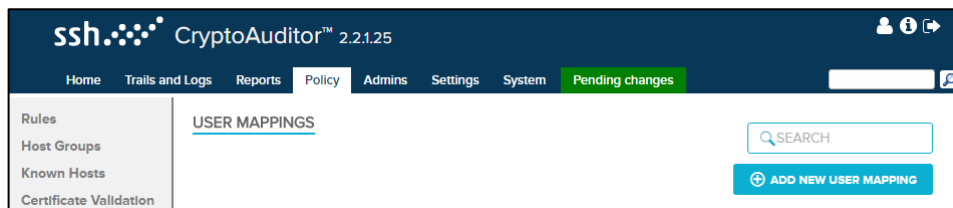
(The screen image above is from CryptoAuditor. Trademarks are the property of their respective owners.)

14. Under **AUTHENTICATION**, complete the following fields, and then click **SAVE**.

|                        |   |
|------------------------|---|
| <b>USER NAME</b>       | Enter the username of the destination server (for example, <b>nsroot</b> ). |
| <b>PASSWORD</b>        | Enter the password of the destination server.                               |
| <b>VERIFY PASSWORD</b> | Re-enter the password of the destination server.                            |

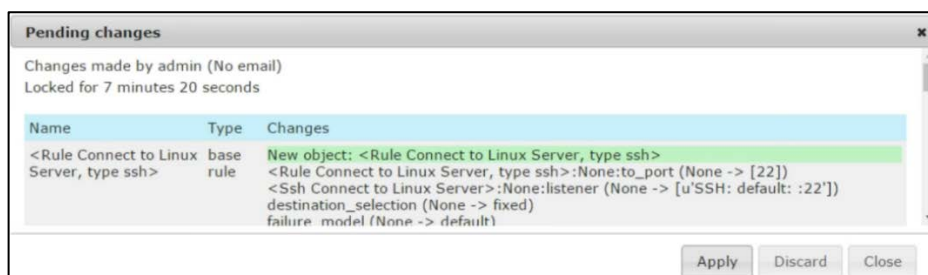
(The screen image above is from CryptoAuditor. Trademarks are the property of their respective owners.)

15. Click the **Pending changes** tab.



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

16. On the **Pending changes** window, click **Apply**.



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

## Creating a Rule to Connect the Destination Server with RDP

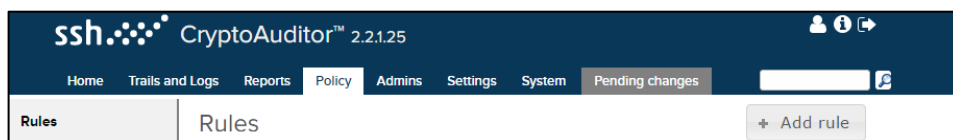
Perform the following steps to create a rule to connect the destination server with RDP:

1. On the CryptoAuditor administrator dashboard, in the left pane, click **Rules**.



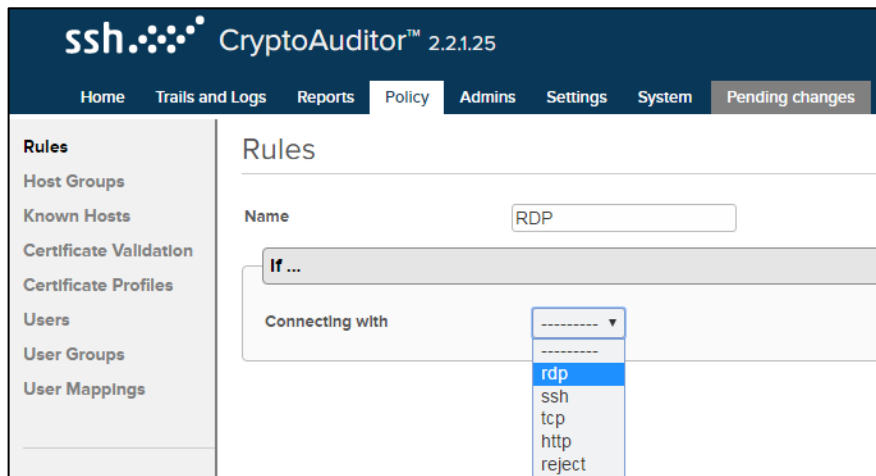
(The screen image above is from CryptoAuditor. Trademarks are the property of their respective owners.)

2. In the right pane, under **Rules**, click **+Add rule**.



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

3. In the **Name** field, enter a name for the rule (for example, **RDP**).
4. In the **Connecting with** field, select **rdp**.



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

- In the **To port** field, select **Via Bastion listener**.

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

- In the **Bastion listener** field, select **RDP: default: 0.0.0.0:3389**, and then click **Continue**.

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

- Under **Authentication**, complete the following fields:

|                                       |  |
|---------------------------------------|--|
| <b>Client-to-Hound authentication</b> | Select <b>Authenticate against a RADIUS server</b> .   |
| <b>Radius server</b>                  | Select the RADIUS server IP address (given along with the port number) that you added in step 6 of “Configuring External RADIUS Authentication Server” on page 11. |
| <b>Hound-to-target authentication</b> | Select <b>Mapped user credentials</b> .  |

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

8. Under **Destination**, complete the following fields, and then click **Continue**.

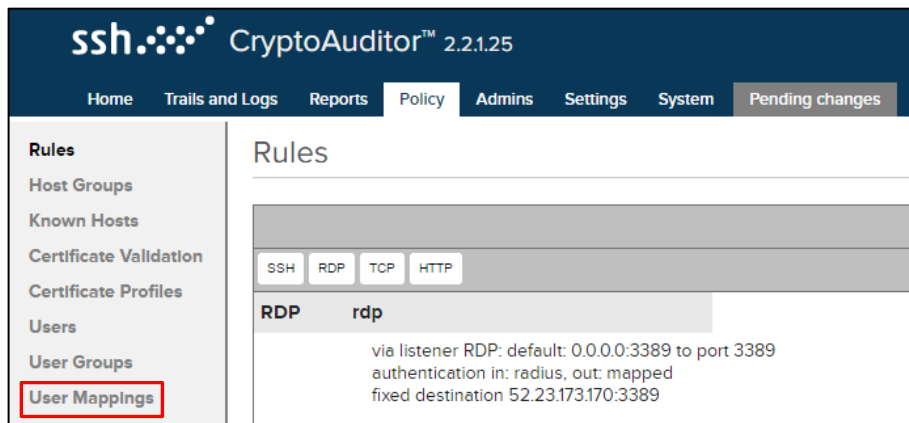
|                                  |  |
|----------------------------------|--|
| <b>Destination selection</b>     | Select <b>Fixed address</b> .                            |
| <b>Fixed destination address</b> | Enter the IP address of the destination server for RDP.  |
| <b>Fixed destination port</b>    | Enter the port number of the destination server for RDP. |

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

9. Click **Save**.

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

10. In the left pane, click **User Mappings**.



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

11. In the right pane, click **ADD NEW USER MAPPING**.



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

12. Under **GATEWAY USER**, complete the following fields:

|                      |  |
|----------------------|--|
| <b>USER NAME</b>     | Enter the SAS username (for example, <b>alice</b> ).   |
| <b>USER PROVIDER</b> | Select the RADIUS server IP address (given along with the port number) that you added in step 6 of “Configuring External RADIUS Authentication Server” on page 11. |

| GATEWAY USER   |   |  |
|--|---|--|
| <b>USER NAME</b><br><input type="text" value="alice"/><br><small>Enter a user name for gateway authentication.</small> | <b>USER GROUP</b><br><input type="text" value="....."/><br><small>Select a pre-defined user group in a user database.</small> | <b>USER PROVIDER</b><br><input type="text" value="radius:109.73.120.148:1812"/><br><small>Select a fixed user database for the gateway authentication.</small> |

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

13. Under **TARGET**, complete the following fields:

|                 |  |
|-----------------|--|
| <b>ADDRESS</b>  | Enter the IP address of the destination server.        |
| <b>PORT</b>     | Enter the RDP port number (for example, <b>3389</b> ). |
| <b>PROTOCOL</b> | Select <b>RDP</b> .                                    |

| TARGET  |   |  |  |
|---|---|--|--|
| <b>HOST GROUP</b><br><input type="text" value="....."/><br><small>If selected, the user is mapped at any target server that is defined in the host group.</small> | <b>ADDRESS</b><br><input type="text" value="13.113.37.214"/><br><small>Enter host address if you want to make a host-specific user mapping.</small> | <b>PORT</b><br><input type="text" value="3389"/> | <b>PROTOCOL</b><br><input type="text" value="RDP"/><br><small>Specify the user mapping to be applied for SSH or RDP only. Leave empty to apply both.</small> |

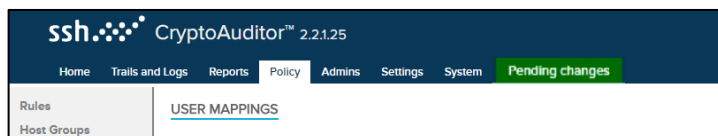
(The screen image above is from CryptoAuditor. Trademarks are the property of their respective owners.)

14. Under **AUTHENTICATION**, complete the following fields, and then click **SAVE**.

|                        |  |
|------------------------|--|
| <b>USER NAME</b>       | Enter the username of the destination server (for example, <b>Administrator</b> ). |
| <b>PASSWORD</b>        | Enter the password of the destination server.                                      |
| <b>VERIFY PASSWORD</b> | Re-enter the password of the destination server.                                   |

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

15. Click the **Pending changes** tab.



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

16. On the **Pending changes** window, click **Apply**.

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

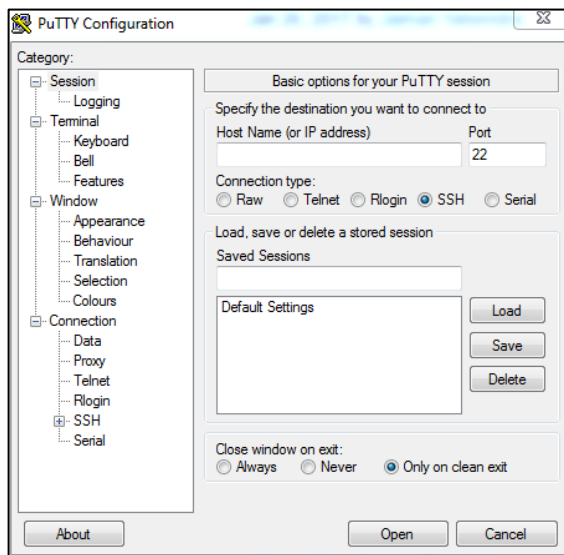
# Running the Solution

For this integration, PASSWORD token is configured for authentication with the SAS solution.

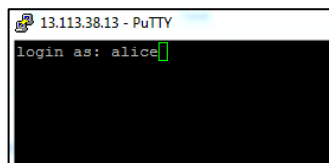
## Authentication for SSH Session

Perform the following steps to access the SSH destination server using the CryptoAuditor IP address:

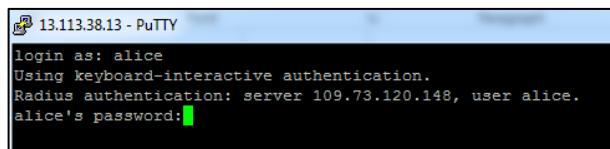
1. Open the Putty application.
2. On the **Putty Configuration** window, in the right pane, perform the following steps:
  - a. In the **Host Name (or IP address)** field, enter the IP address of the CryptoAuditor.
  - b. Under **Connection type**, select the **SSH** option.



3. On the SSH console, enter the SAS username (for example, **alice**), and then press the **Enter** key.

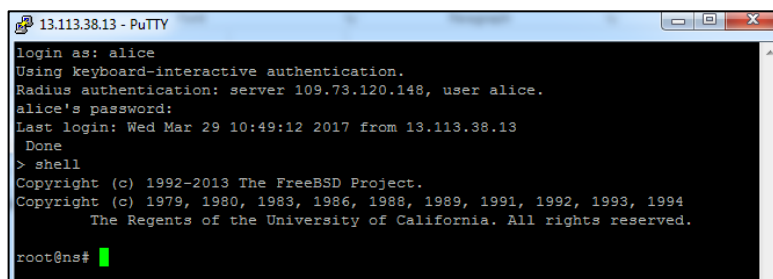


4. Enter the user password that is provisioned as the token code in SAS and then press the **Enter** key.






After successful authentication done by the RADIUS server, the SSH session of the destination server is opened.

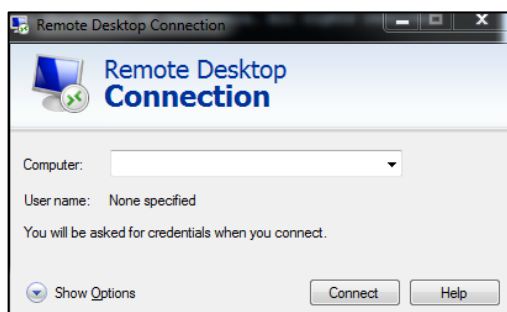


```
13.113.38.13 - PuTTY
login as: alice
Using keyboard-interactive authentication.
Radius authentication: server 109.73.120.148, user alice.
alice's password:
Last login: Wed Mar 29 10:49:12 2017 from 13.113.38.13
Done
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.
root@ns#
```

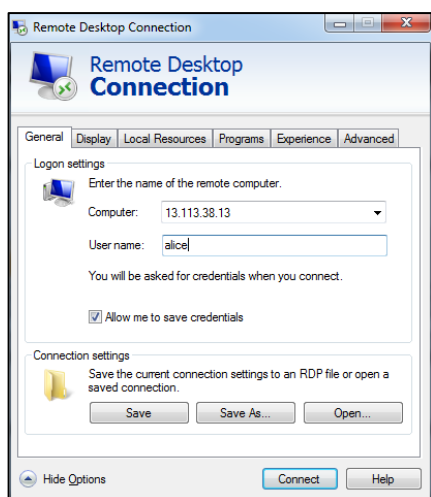
## Authentication for RDP Session

Perform the following steps to access the RDP destination server using the CryptoAuditor IP address:

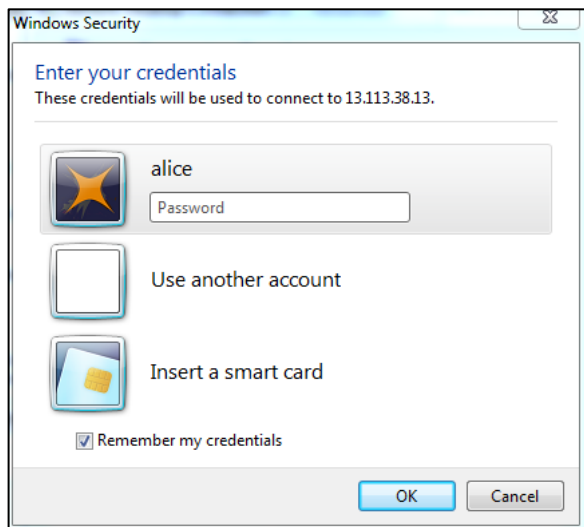
1. Open the **Remote Desktop Connection** application.
2. On the **Remote Desktop Connection** application console, in the **Computer** field, enter the IP address of CryptoAuditor, and then click the **Show Options** icon .



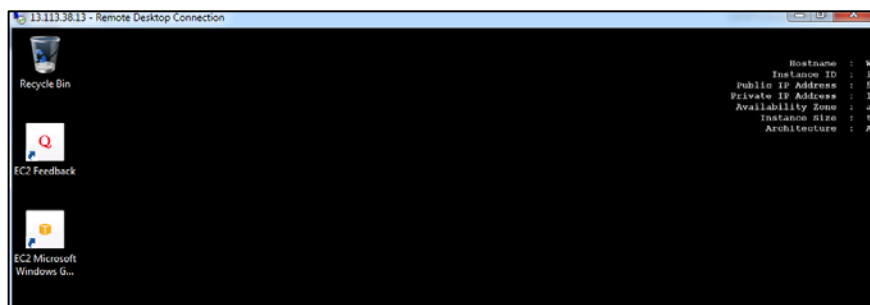
3. Perform the following steps:
  - a. In the **User name** field, enter the SAS username (for example, **alice**)
  - b. Select the **Allow me to save credentials** check box.
  - c. Click **Connect**.



4. On the **Windows Security** window, enter the user password that is provisioned as the token code in SAS, and then click **OK**.



After successful authentication done by the RADIUS server, the RDP session of the destination server is opened.



## 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 Gemalto Customer Support. Gemalto 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 Gemalto 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                           | Gemalto<br>4690 Millennium Drive<br>Belcamp, Maryland 21017 USA   |                |
| Phone                             | United States   | 1-800-545-6608 |
|                                   | International   | 1-410-931-7520 |
| Technical Support Customer Portal | <a href="https://supportportal.gemalto.com">https://supportportal.gemalto.com</a><br>Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base. |                |