

# SafeNet Agent for Pluggable Authentication Module 1.0.2

## INSTALLATION AND CONFIGURATION GUIDE



## Document Information

<b>Product Version</b>	1.0.2
<b>Document Part Number</b>	007-000343-001, Rev. C
<b>Release Date</b>	November 2019

## Trademarks, Copyrights, and Third-Party Software

© 2019 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. 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.

## Disclaimer

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.

# CONTENTS

<b>PREFACE .....</b>	<b>6</b>
Customer Release Notes .....	6
Audience .....	6
Document Conventions.....	6
Notifications .....	6
Command Syntax and Typeface Conventions .....	7
Related Documents .....	7
Support Contacts .....	8
Customer Support Portal .....	8
Telephone Support .....	8
Email Support .....	8
<b>CHAPTER 1: Overview .....</b>	<b>9</b>
Introduction .....	9
Solution Flow.....	9
Prerequisites .....	9
Exception .....	10
Environment.....	10
Upgrading the Agent .....	11
<b>CHAPTER 2: Installing the Agent.....</b>	<b>12</b>
<b>CHAPTER 3: Configuring the Agent.....</b>	<b>13</b>
<b>CHAPTER 4: Applying Multi-Factor Authentication .....</b>	<b>14</b>
RedHat Linux and CentOS .....	14
Ubuntu.....	17
<b>CHAPTER 5: Running the Agent.....</b>	<b>21</b>
Login Console .....	21
Character Support for Push SMS Grid Tokens .....	22
Secure Shell Connections.....	22

# PREFACE

This document is intended for personnel responsible for maintaining your organization's security infrastructure. All products manufactured and distributed by Gemalto are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

## Customer Release Notes

The Customer Release Notes (CRN) document provides important information about this release that is not included in other customer documentation. It is strongly recommended that you read the CRN to fully understand the capabilities, limitations, and known issues for this release.

## Audience

This document is intended for personnel responsible for maintaining your organization's security infrastructure. This includes SafeNet Agent for Pluggable Authentication Module (PAM) users and security officers, the key manager administrators, and network administrators. It is assumed that the users of this document are proficient with security concepts.

All products manufactured and distributed by Gemalto are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

## Document Conventions

This section provides information on the conventions used in this document.

### Notifications

This document uses notes, cautions, and warnings to alert you to important information that may help you to complete your task, or prevent personal injury, damage to the equipment, or data loss.

### Notes

Notes are used to alert you to important or helpful information. These elements use the following format:

**NOTE:** Take note. Notes contain important or helpful information.

## Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:

**CAUTION!** Exercise caution. Caution alerts contain important information that may help prevent unexpected results or data loss.

## Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. These elements use the following format:

**\*\*WARNING\*\*** Be extremely careful and obey all safety and security measures. In this situation, you might do something that could result in catastrophic data loss or personal injury.

## Command Syntax and Typeface Conventions

Convention	Description
<b>bold</b>	The bold attribute is used to indicate the following: <ul style="list-style-type: none"> <li>&gt; Command-line commands and options (Type <b>dir /p</b>.)</li> <li>&gt; Button names (Click <b>Save As</b>.)</li> <li>&gt; Check box and radio button names (Select the <b>Print Duplex</b> check box.)</li> <li>&gt; Window titles (On the <b>Protect Document</b> window, click <b>Yes</b>.)</li> <li>&gt; Field names (<b>User Name:</b> Enter the name of the user.)</li> <li>&gt; Menu names (On the <b>File</b> menu, click <b>Save</b>.) (Click <b>Menu &gt; Go To &gt; Folders</b>.)</li> <li>&gt; User input (In the <b>Date</b> box, type <b>April 1</b>.)</li> </ul>
<i>italic</i>	The italic attribute is used for emphasis or to indicate a related document. (See the <i>Installation Guide</i> for more information.)
Double quote marks	Double quote marks enclose references to other sections within the document.
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.

## Related Documents

The following document(s) contain related or additional information:

- > SafeNet Agent for PAM: Customer Release Notes

---

## Support Contacts

---

If you encounter a problem while installing, registering, or operating this product, refer to 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.

### Customer Support Portal

The Customer Support Portal, at <https://supportportal.gemalto.com>, is a where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

**NOTE:** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

### Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Gemalto Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

### Email Support

You can also contact technical support by email at [technical.support@gemalto.com](mailto:technical.support@gemalto.com).

# CHAPTER 1: Overview

## Introduction

Pluggable Authentication Module (PAM) is a program (or a set of programs) that aims to identify a user before granting system access. The PAM provides open-source, customizable libraries that enables:

- Developers to focus on creating programs, without having to worry about creating authentication schemes. In other words, the PAM renders a common authentication scheme that can be used with a number of applications.
- System administrators and developers to exercise better control and flexibility over the authentication.

The SafeNet Agent for Pluggable Authentication Module (PAM) is a Two-Factor Authentication (2FA) solution to authenticate Linux users before granting system access. The SafeNet Agent for PAM can be easily configured for any number of Linux systems to provide a secure mechanism of protecting PAM aware applications like login console or remote (SSH) sessions.

By taking advantage of our industry-leading authentication solution, coupled with the flexibility of PAM, organizations can prevent their Linux systems from unauthorized access. Requiring a second factor of authentication, in addition to a valid username and password, is a critical measure for information security.

## Solution Flow

The SafeNet Agent for PAM is installed on a Linux machine, and acts as an intermediary between users and the SafeNet Authentication Service (SAS). The following are the steps that will help illustrate the solution flow for the users:

1. A user attempts to access a Linux machine protected by the SafeNet agent, either via login console, or remotely with SSH.
2. After providing valid username and password, the user is prompted to provide SafeNet credentials, which are then send over to the SAS.
3. The SAS provides the agent with authentication methods configured for the user. The agent prompts the user to authenticate. The user chooses the available authentication method and authenticates.
  - If the SAS approves the request, the information is sent to the PAM, which then denies or grants the system access.

## Prerequisites

- The user must already be created and available in the SAS.
- The user must also exist locally on the machine on which the PAM agent is proposed for installation.
- Root permissions must be obtained on the machine on which the PAM agent is proposed for installation.



- SAS server should be available and reachable from the Linux machine.
- Ensure that the agent's public key, `gpg_verfiy.key`, is imported, before beginning the installation. To import, execute the following command:
  - `rpm --import /path/to/gpg_verfiy.key` (RedHat Linux and CentOS)
  - `gpg --import /path/to/gpg_verfiy.key` (Ubuntu)
- An **Auth Node** must be created for the agent to allow authentication requests to the SAS. To define Auth Nodes in the SAS, follow the steps:
  - a. On the **Virtual Servers** tab, select **Comms > Auth Nodes**, and click **Add**.
  - b. Complete the following fields, and click **Save**.

Field	Description
<b>Agent Description</b>	Enter a description for the agent.
<b>Hostname</b>	Enter the hostname of the server.
<b>Low IP Address In Range</b>	Enter the lowest IP address in the range.
<b>High IP Address In Range</b>	Enter the highest IP address in the range.

#### NOTES:

- If you are specifying a single IP address, enter the IP address in the **Low IP Address**. The **High IP Address** can be left empty.
- If more than one IP address is required, expand the **Services** module and then modify the value in **Auth Nodes: Max. Auth Nodes** field.

## Exception

If **AutoLogin** feature is enabled on a Linux system for a user, the SafeNet OTP functionality will not be invoked.

## Environment

Environment	Description
<b>Tokens</b>	All tokens supported by SafeNet Authentication Service.
<b>SAS Releases</b>	<ul style="list-style-type: none"> <li>&gt; SAS PCE/ SPE 3.5 (and later)</li> <li>&gt; SAS Cloud Edition</li> </ul>

Environment	Description
<b>Operating Systems</b>	<ul style="list-style-type: none"><li>&gt; RHEL 7.5</li><li>&gt; CentOS 7.6</li><li>&gt; Ubuntu 18.04</li></ul>
<b>OpenSSL Version</b>	<ul style="list-style-type: none"><li>&gt; RHEL-7.5 /CentOS-7.6: OpenSSL-1.0.2k</li><li>&gt; Ubuntu-18.04 OS: OpenSSL-1.1.1</li></ul>

## Upgrading the Agent

The upgrade from any earlier release is not supported officially in this release. To use the latest version, please uninstall the old agent and install the new one.

# CHAPTER 2: Installing the Agent

Install the SafeNet Agent:

1. Run the following command:

- RedHat Linux and CentOS:  
`rpm -i SafeNet_Agent_for_PAM_Linux-[your installation build no].rpm`
- Ubuntu:  
`dpkg -i SafeNet_Agent_for_PAM_Linux-[your installation build no]_amd64.deb`

2. By default, the installation package will be installed at the following location:

`/usr/local/gemalto/pam/`

3. Navigate to the installed directory (`/usr/local/gemalto/pam/`):

`cd /usr/local/gemalto/pam/`

4. Copy the **SAS\_PAMConf.ini** file from the Config folder to `/usr/local/` using the following command:

`cp config/SAS_PAMConf.ini /usr/local/`

5. For the following options available in the **sshd\_config** file (at `/etc/ssh`), perform the actions:

- Enable **PasswordAuthentication** option, by setting it to **yes**.
- Enable **ChallengeResponseAuthentication** option, by setting it to **yes**.

```
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication yes
```

6. Restart the **sshd** service using the following command:

`service sshd restart`

7. Edit **config** file available at, `/etc/selinux`

- Open the file using the following command:  
`vi /etc/selinux/config`
- Change **SELINUX=enforcing** to **SELINUX=disabled**
- Save the **config** file, and restart the system.

**NOTE:** By default, `selinux` is not available for Ubuntu, so the above edit is not required. If it exists in the system, ensure that **SELINUX** is disabled.

# CHAPTER 3: Configuring the Agent

The initialization (.ini) file is used to configure parameters for operating systems and programs. Edit the **SAS\_PAMConf.ini** file, available at `/usr/local/`.

The following options can be configured:

1. **Encryption key file path:** The agent encryption key file is used to encrypt/ decrypt the data. Provide the path of the agent BSID key below:

```
EncryptionKeyFile=/usr/local/gemalto/pam/bsidkey/Agent.bsidkey
```

**NOTE:** If you are moving from one SAS version to another, the key file needs be downloaded (and updated above) by following the steps:

1. Login to SAS account, and navigate to **COMMS > Authentication Processing** section.
2. Under the **Task** list, click **Authentication Agent Settings** link and download the key.

The key file must be kept at a location accessible by all the authorized users.

2. **Primary BSID Server URL:** Provide the IP address of the primary authentication server.

```
PrimaryServiceURL=<IP>
```

3. **Secondary BSID Server URL** (not mandatory): Provide the IP address of the secondary authentication server, if applicable.

```
SecondaryServiceURL=<IP>
```

4. **Log file full path** and **Log level:** Specify the location where the log files will be saved. In addition, adjust the logging level as per the following definitions:

1 – Error, 2 – Info (Default), 3 – Debug

```
LogFile=/usr/local/gemalto/pam/logs/SAS_PAM_Logs-{date}.log
```

```
LogLevel=2
```

5. **Enable/Disable SSL:** This option allows to enable/ disable SSL requests to the TokenValidator. The SSL option is enabled by default. To disable, change the value to **0**.

```
EnableSSL=1
```

6. **TokenValidator path:** This setting is used for SAS internal purposes. We recommend not to edit this setting.

```
TokenValidatorURL=/TokenValidator/TokenValidator.asmx
```

7. **AutoPush:** If AutoPUSH is enabled (value set to **1**), a PUSH request will be sent to the user's mobile device automatically. Enable this option only if all user accounts on the server have SAS Push tokens assigned.

To disable, set the value to **0**.

```
AutoPush=0
```

# CHAPTER 4: Applying Multi-Factor Authentication

## RedHat Linux and CentOS

To apply the SafeNet 2FA to different login types, follow one of the following three instruction sets:

- For **login console** and **ssh** access formats, change the parameter of the **pam\_unix.so** module from **sufficient** to **required** in the **/etc/pam.d/password-auth-ac** file.

Also, add the following content after the **pam\_unix.so** module row:

```
auth sufficient /usr/local/gemalto/pam/bin/SASAuth.so
```

### **Before** (RedHat Linux Example)

```

#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth      required      pam_env.so
auth      required      pam_faildelay.so delay=2000000
auth      sufficient    pam_unix.so nullok try_first_pass
auth      requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth      required      pam_deny.so

account   required      pam_unix.so
account   sufficient    pam_localuser.so
account   sufficient    pam_succeed_if.so uid < 1000 quiet
account   required      pam_permit.so

password  requisite     pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=
password  sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok

password  required      pam_deny.so

session   optional     pam_keyinit.so revoke
session   required    pam_limits.so
-session  optional     pam_systemd.so
session   [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session   required     pam_unix.so

```

**After** (RedHat Linux Example)

```

#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth      required      pam_env.so
auth      required      pam_faildelay.so delay=2000000
#auth     sufficient    pam_unix.so nullok try_first_pass
auth      required      pam_unix.so nullok try_first_pass
auth      sufficient    /usr/local/gemalto/pam/bin/SASAuth.so

auth      requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth      required      pam_deny.so

account   required      pam_unix.so
account   sufficient     pam_localuser.so
account   sufficient     pam_succeed_if.so uid < 1000 quiet
account   required      pam_permit.so

password  requisite     pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=
password  sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok

password  required      pam_deny.so

session   optional      pam_keyinit.so revoke
session   required     pam_limits.so
#session  optional     pam_systemd.so
session   [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session   required     pam_unix.so

```

**NOTES:**

- To disable the agent, revert the above changes.
- To enable only OTP-based login sessions, comment the **pam\_unix.so** module row:

```
#auth      required      pam_unix.so nullok
try_first_pass
```

This action ensures that the user need not provide the system password, and will be granted system access, based on a combination of system username and SafeNet Credentials.

- Only for SSH connections, add the following content to the **/etc/pam.d/ssh** file (at the end):  

```
auth      required      /usr/local/gemalto/pam/bin/SASAuth.so
```
- Only when the user is switched, add the following content to the **/etc/pam.d/su** file (at the end):  

```
auth      required      /usr/local/gemalto/pam/bin/SASAuth.so
```

**Before** (RedHat Linux Example)

```
#%PAM-1.0
auth          sufficient      pam_rootok.so
# Uncomment the following line to implicitly trust users in the "wheel" group.
#auth         sufficient      pam_wheel.so trust use_uid
# Uncomment the following line to require a user to be in the "wheel" group.
#auth         required        pam_wheel.so use_uid
auth          substack        system-auth
auth          include         postlogin
account       sufficient      pam_succeed_if.so uid = 0 use_uid quiet
account       include         system-auth
password      include         system-auth
session       include         system-auth
session       include         postlogin
session       optional        pam_xauth.so
```

**After** (RedHat Linux Example)

```
#%PAM-1.0
auth          sufficient      pam_rootok.so
# Uncomment the following line to implicitly trust users in the "wheel" group.
#auth         sufficient      pam_wheel.so trust use_uid
# Uncomment the following line to require a user to be in the "wheel" group.
#auth         required        pam_wheel.so use_uid
auth          substack        system-auth
auth          include         postlogin
account       sufficient      pam_succeed_if.so uid = 0 use_uid quiet
account       include         system-auth
password      include         system-auth
session       include         system-auth
session       include         postlogin
session       optional        pam_xauth.so
auth          required        /usr/local/gemalto/pam/bin/SASAuth.so
```

**NOTE:** To disable the agent, comment the following content (as added above):

```
#auth         required        /usr/local/gemalto/pam/bin/SASAuth.so
```



## Ubuntu

To apply the SafeNet 2FA to different login types, follow one of the following three instruction sets:

- For all the access formats (**login console**, **su**, and **ssh**), change the parameter of the **pam\_unix.so** module from **sufficient** to **required** in the **/etc/pam.d/common-auth** file.

Also, add the following content after the **pam\_unix.so** module row:

```
auth sufficient /usr/local/gemalto/pam/bin/SASAuth.so
```

### Before

```
# /etc/pam.d/common-auth - authentication settings common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.). The default is to use the
# traditional Unix authentication mechanisms.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.
#
# here are the per-package modules (the "Primary" block)
auth [success=1 default=ignore] pam_unix.so nullok_secure

# here's the fallback if no module succeeds
auth requisite pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth required pam_permit.so
# and here are more per-package modules (the "Additional" block)
auth optional pam_cap.so
## end of pam-auth-update config
"/etc/pam.d/common-auth" 28L, 1395C          28,1          Bot
```



**After**

```

# /etc/pam.d/common-auth - authentication settings common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.). The default is to use the
# traditional Unix authentication mechanisms.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
#auth [success=1 default=ignore] pam_unix.so nullok_secure

auth required pam_unix.so nullok_secure
auth sufficient /usr/local/gemalto/pam/bin/SASAuth.so
# here's the fallback if no module succeeds
auth requisite pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth required pam_permit.so
# and here are more per-package modules (the "Additional" block)

```

1,1 Top

**NOTES:**

- To disable the agent, revert the above changes.
- To enable only OTP-based login sessions, comment the **pam\_unix.so** module row:

```
#auth required pam_unix.so nullok_secure
```

This action ensures that the user need not provide the system password, and will be granted system access, based on a combination of system username and SafeNet Credentials.

- Only for SSH connections, add the following content to the **/etc/pam.d/sshd** file:

```
auth required /usr/local/gemalto/pam/bin/SASAuth.so
```
- Only when the user is switched, add the following content to the **/etc/pam.d/su** file:

```
auth required /usr/local/gemalto/pam/bin/SASAuth.so
```

**Before**

```
# parsing /etc/environment needs "readenv=1"
session      required    pam_env.so readenv=1
# locale variables are also kept into /etc/default/locale in etch
# reading this file *in addition to /etc/environment* does not hurt
session      required    pam_env.so readenv=1 envfile=/etc/default/locale

# Defines the MAIL environment variable
# However, userdel also needs MAIL_DIR and MAIL_FILE variables
# in /etc/login.defs to make sure that removing a user
# also removes the user's mail spool file.
# See comments in /etc/login.defs
#
# "nopen" stands to avoid reporting new mail when su'ing to another user
session      optional    pam_mail.so nopen

# Sets up user limits according to /etc/security/limits.conf
# (Replaces the use of /etc/limits in old login)
session      required    pam_limits.so

# The standard Unix authentication modules, used with
# NIS (man nsswitch) as well as normal /etc/passwd and
# /etc/shadow entries.
@include common-auth
@include common-account
@include common-session

"/etc/pam.d/su" 61L, 2322C                                     61,0-1 Bot
```

**After**

```

# parsing /etc/environment needs "readenv=1"
session      required    pam_env.so readenv=1
# locale variables are also kept into /etc/default/locale in etch
# reading this file *in addition to /etc/environment* does not hurt
session      required    pam_env.so readenv=1 envfile=/etc/default/locale

# Defines the MAIL environment variable
# However, userdel also needs MAIL_DIR and MAIL_FILE variables
# in /etc/login.defs to make sure that removing a user
# also removes the user's mail spool file.
# See comments in /etc/login.defs
#
# "nopen" stands to avoid reporting new mail when su'ing to another user
session      optional    pam_mail.so nopen

# Sets up user limits according to /etc/security/limits.conf
# (Replaces the use of /etc/limits in old login)
session      required    pam_limits.so

# The standard Unix authentication modules, used with
# NIS (man nsswitch) as well as normal /etc/passwd and
# /etc/shadow entries.
@include common-auth
@include common-account
@include common-session
auth         required    /usr/local/gemalto/pam/bin/SASAuth.so

"/etc/pam.d/su" 61L, 2322C                                     56,1          Bot

```

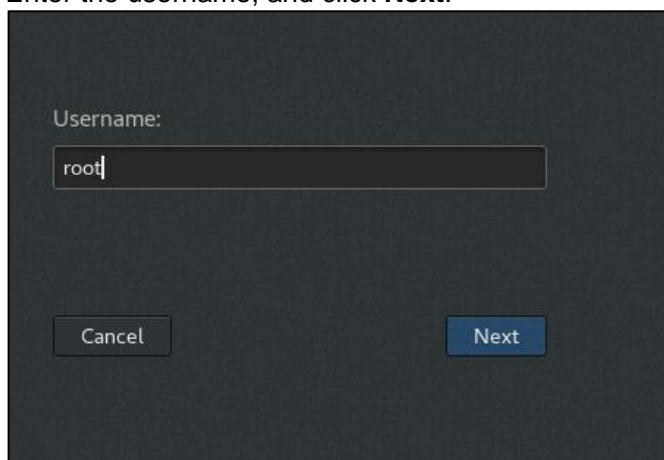
**NOTE:** To disable the agent, comment the following content (as added above):

```
#auth         required    /usr/local/gemalto/pam/bin/SASAuth.so
```

# CHAPTER 5: Running the Agent

## Login Console

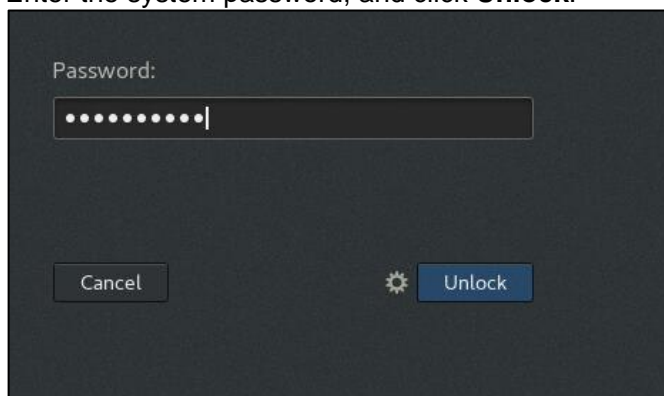
1. Enter the username, and click **Next**.




Username:

Cancel Next

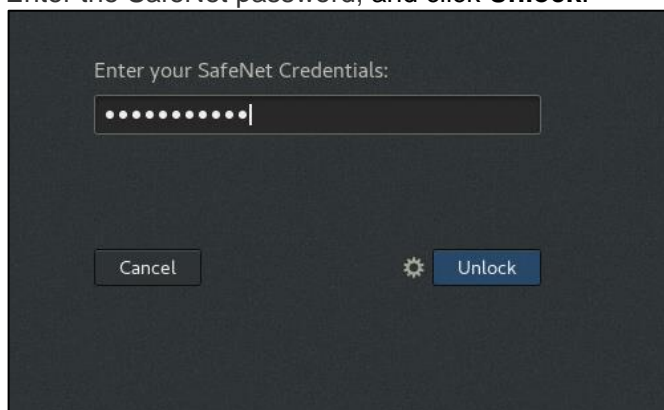
2. Enter the system password, and click **Unlock**.




Password:

Cancel  Unlock

3. Enter the SafeNet password, and click **Unlock**.



Enter your SafeNet Credentials:

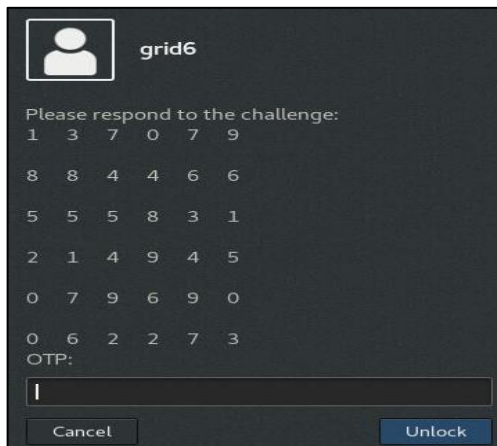
Cancel  Unlock



**NOTES:**

- To quickly select **PUSH**, **Grid** or **SMS (PGS)** token for authentication, **character support** is now provided.
- If **Auto Push is configured**, a PUSH request will be sent to the user's mobile device automatically.

- a. If Gridsure is configured or selected, enter **OTP**, derived from your grid pattern, and click **Unlock**.



- b. If PUSH is configured or selected, the user receives a push notification on their mobile's MobilePASS app to indicate there is a login request pending. The user taps on the notification to view the login request details, and can respond with a tap to approve or deny the request.
- c. If SMS is configured or selected, the user receives an SMS on their mobile. The user enters the SMS as the SafeNet password, and clicks on **Unlock**.

The (approval) response (with a passcode attached) is sent back to the SAS server, where it is validated, and when the authentication is complete, the access is granted to the user.

## Character Support for Push SMS Grid Tokens

To quickly select PUSH, Grid or SMS (PGS) token to use with the agent, character support is provided. The SafeNet Credentials field behaviour is decided by the character input; with **p** defaulting to trigger **PUSH**, **s** to **SMS** and **g** to **Gridsure**.

If blank is submitted, the SAS verifies, and provides the agent with the authentication token configured for the user, which is then prompted to the user for a response.

## Secure Shell Connections

1. Enter the system password, and press **Enter**.

```
login as: root
Using keyboard-interactive authentication.
Password: █
```

2. Enter the SafeNet password, and press **Enter**.

```
login as: root
Using keyboard-interactive authentication.
Password:
Using keyboard-interactive authentication.
Enter your SafeNet Credentials: █
```

#### NOTES:

- To quickly select **PUSH**, **Grid** or **SMS (PGS)** token for authentication, character support is now provided.
- If Auto Push is configured, a PUSH request will be sent to the user's mobile device automatically.

- a. If GrIDsure is configured or selected, enter **OTP**, derived from your grid pattern, and press **Enter**.

```
login as: grid6
Using keyboard-interactive authentication.
Password:
Using keyboard-interactive authentication.
Enter your SafeNet Credentials:
Using keyboard-interactive authentication.
Please respond to the challenge:
1   3   7   0   7   9
8   8   4   4   6   6
5   5   5   8   3   1
2   1   4   9   4   5
0   7   9   6   9   0
0   6   2   2   7   3
OTP: █
```

- b. If PUSH is configured or selected, the user receives a push notification on their mobile's MobilePASS app to indicate there is a login request pending. The user taps on the notification to view the login request details, and can respond with a tap to approve or deny the request.
- c. If SMS is configured or selected, the user receives an SMS on their mobile. The user enters the SMS as the SafeNet password, and press **Enter**.

The (approval) response (with a passcode attached) is sent back to the SAS server, where it is validated, and when the authentication is complete, the access is granted to the user.