

THALES

SafeNet Agent for macOS Logon 2.0.0

INSTALLATION AND CONFIGURATION GUIDE



All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and/or its subsidiaries or affiliates 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 Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as "Thales") 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, Thales 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, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Thales 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 Thales 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.

Thales 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 Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales 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.

Copyright © 2018-2022 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and affiliates and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the properties of their respective owners.

CONTENTS

Preface:	4
Audience	4
Support Contacts	4
Third Party Acknowledgment	5
Document Conventions	5
Command Syntax and Typeface Conventions	5
Notifications and Alerts	6
Chapter 1: Introduction	7
System Requirements	7
Default Configuration	7
SafeNet Agent for macOS Logon - Authentication Methods	8
Domain Authentication	8
Offline Authentication	8
Prerequisites	9
Chapter 2: Installing, Configuring and Uninstalling the agent using Jamf Pro	10
Prerequisites	10
Silent Installation	10
Silent Configuration	11
Silent Uninstallation	13
Chapter 3: Installing and Uninstalling the asgent using Installation file	14
Installing the Agent	14
Silent Installation	17
Uninstalling the Agent	18
Chapter 4: Configuring the macOS Logon Agent	19
Configuring Auth Node in SafeNet server	19
Configuring Settings within the Agent	22
Settings	22
Offline	27
Logs	29
Chapter 5: Testing the Solution	31
List of Users Option	31
Name and Password Option	33

PREFACE:

This document describes how to install and configure SafeNet Agent for macOS Logon 2.0.0.

Audience

This document is intended for personnel responsible for maintaining your organization's security infrastructure. This includes SafeNet Agent for macOS Logon users and security officers, 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 Thales Group 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.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or [Thales Customer Support](#).

Thales 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 Thales 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.thalesgroup.com>, is 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

The support portal also lists telephone numbers for voice contact ([Contact Us](#)).

Third Party Acknowledgment

This document is intended to help users of Thales products when working with third-party software. 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.

Document Conventions

This section describes the conventions used in this document.

Command Syntax and Typeface Conventions

This document uses the following conventions for command syntax descriptions, and to highlight elements of the user interface.

Format	Convention
bold	<p>The bold attribute is used to indicate the following:</p> <ul style="list-style-type: none"> > Command-line commands and options that you enter verbatim (Type dir /p.) > Button names (Click Save As.) > Check box and radio button names (Select the Print Duplex check box.) > Dialog box titles (On the Protect Document dialog box, click Yes.) > Field names (User Name: Enter the name of the user.) > Menu names (On the File menu, click Save.) (Click Menu > Go To > Folders.) > User input (In the Date box, type April 1.)
<i>italics</i>	In type, the italic attribute is used for emphasis or to indicate a related document. (See the <i>Installation Guide</i> for more information.)
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[optional] [<optional>]	Represent optional keywords or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.
{a b c} {<a> <c>}	Represent required alternate keywords or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.
[a b c] [<a> <c>]	Represent optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.

Notifications and Alerts

Notifications and alerts are used to highlight important information or alert you to the potential for data loss or personal injury.

Tips

Tips are used to highlight information that helps to complete a task more efficiently.

TIP This is some information that will allow you to complete your task more efficiently.

Notes

Notes are used to highlight important or helpful information.

NOTE Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss.

CAUTION! Exercise caution. Contains 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.

****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.

CHAPTER 1: Introduction

The SafeNet Agent for macOS Logon is designed to help macOS customers ensure that valuable resources are accessible only by authorized users. It delivers a simplified and consistent user login experience, virtually eliminates help desk calls related to password management, and helps organizations comply with regulatory requirements.

The use of Two-Factor Authentication (2FA) instead of just traditional static passwords to access a macOS environment is a critical step for information security.

NOTE The SafeNet Agent for macOS Logon is supported only on the new console logons, and not when unlocking the screen saver or when a user wakes the system from sleep.

System Requirements

Networking Environments	> AD Server
Communication Protocols	> Hyper Text Transfer Protocol Secure (HTTPS): <ul style="list-style-type: none">• Secure Sockets Layer (SSL) 2.0 and above• Transport Layer Security (TLS) 1.2 and above
Network	> TCP Port 443
Operating Systems	> Monterey v12.0 (and later) > Big Sur v11.0.1 (and later) > Catalina v10.15.2 (and later) NOTE Assuming the later OS versions are backward compatible.
Supported Authentication Tokens	> All authentication tokens currently supported by SafeNet server.
Unsupported Tokens in Offline Authentication Mode	> Challenge-response-enabled tokens, SMS, GrIDsure, and time-based tokens. > When using MobilePASS+ in this scenario, the Push OTP feature does not work, but standard One Time Password (OTP) authentication works.
SAS Releases	> SAS PCE/SPE 3.14 (and later)

Default Configuration

Mode	Description
PUSH authentication	> Time-out after 120 seconds

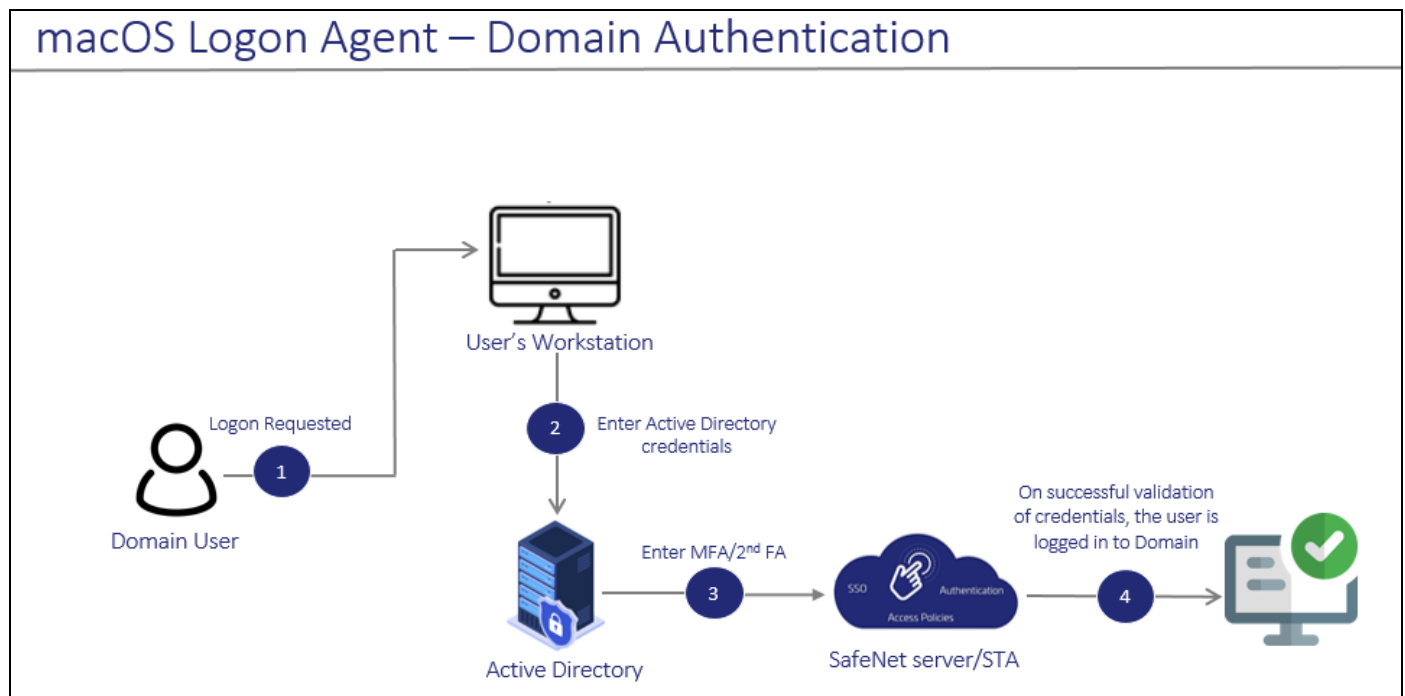
SafeNet Agent for macOS Logon - Authentication Methods

The macOS Logon Agent offers two types of authentication methods:

- > [Domain Authentication](#)
- > [Offline Authentication](#)

Domain Authentication

Domain Authentication refers to the online authentication when the machine is connected to AD. The following diagram describes the authentication flow for a user when machine is connected to domain.



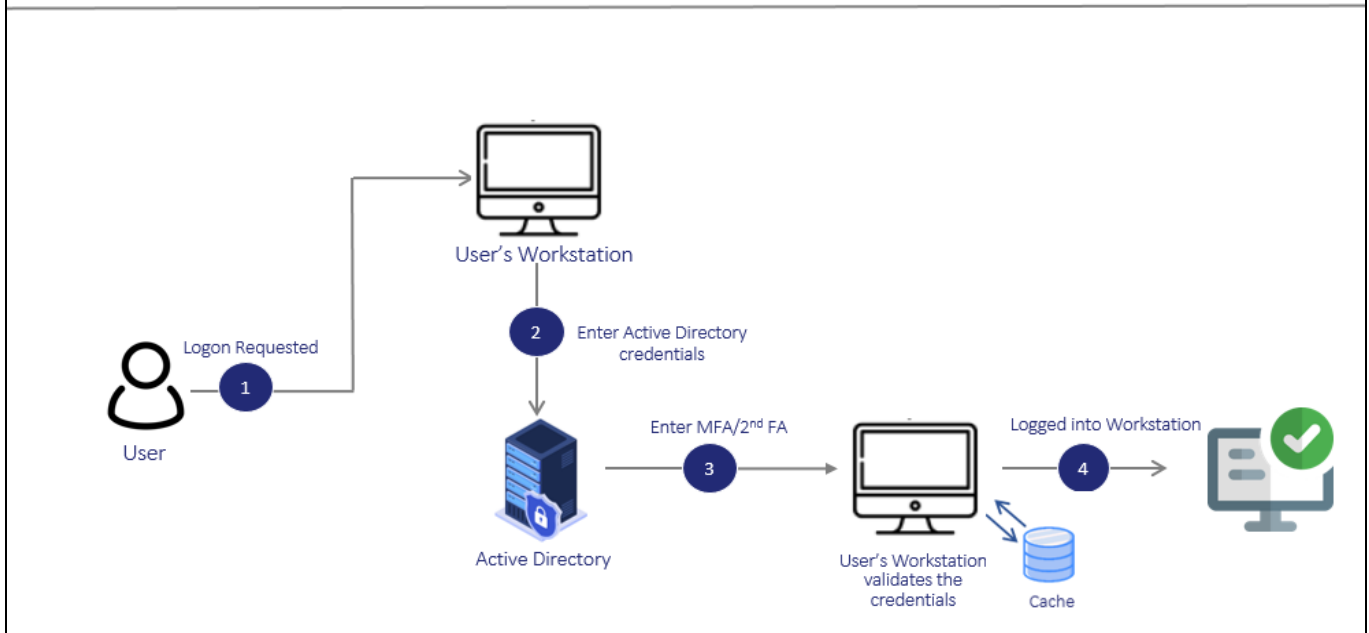
1. After invoking the workstation logon, the user is presented with the macOS Native Logon prompt.
2. On the macOS Native Logon prompt, the user enters user name (if applicable, the logon domain) and Active Directory (AD) password.
3. Then the user is prompted for the second factor authentication, for example, OTP. The user enters the OTP. The entered credentials are then sent to the SafeNet server for verification.
4. On successful validation of both the Active Directory (AD) and SafeNet credentials, the user is logged on to the workstation.

Offline Authentication

By default, SafeNet Agent for macOS Logon supports offline authentication, which enables users to log on using a SafeNet OTP when there is no connection to the SafeNet server.

NOTE To use offline authentication, the user must have completed one successful online authentication. Also, for Active Directory users, the mobile account needs to be enabled within the system preferences of Mac.

macOS Logon Agent – Offline Authentication



1. After invoking the workstation logon, the offline user is presented with the macOS Logon prompt.
2. The user enters the user name and Active Directory (AD) password.
3. Then the user is prompted for the second factor authentication, for example, OTP. The user enters the OTP. The entered credentials are then verified by the offline authentication OTP stored on the local workstation.
4. On successful validation of both the Active Directory (AD) and SafeNet credentials, the user is logged on to the workstation.

Prerequisites

- > Ensure that TCP port 443 is open between the SafeNet Agent for macOS Logon and SafeNet server.
- > Administrative rights to the macOS machine are required during installation of the SafeNet Agent for macOS Logon.
- > If the user connects via AD, they need to bind their Microsoft Active Directory account to the macOS machine.
- > Ensure that an [Auth Node](#) is configured in the SafeNet server.

CHAPTER 2: Installing, Configuring and Uninstalling the agent using Jamf Pro


This section describes the steps to perform the [installation](#), [configuration](#) and [uninstallation](#) of the agent using Jamf Pro. This process is used to deploy the Mac Logon Agent on multiple machines.

Prerequisites

- > A valid Jamf Pro license purchased from Jamf
- > Jamf Pro setup on the targeted machine

Silent Installation

Perform the following steps to add and run the policies on a targeted machine:

1. Log in to **Jamf Pro**.
2. Click the **Settings** icon  on the top right-hand side corner.
3. Select **Computer Management**, and then click **Packages**.
4. Click **New** to add a new package.
5. In the **General** tab, enter a **Display Name** for the package, and then click **Choose File** to upload **SafeNet_Agent_For_macOS_Installer.pkg**.
Click **Save** at the bottom right-hand side corner.
6. To add a policy, click **Computers > Policies** in the left pane, and then click **New**.
7. In the **Options** tab,
 - a. Under **General**,
 - i. Enter a **Display Name** for the policy.
 - ii. Select the **Enabled** check box.
 - iii. Select the options to **Trigger Event(s)** (to use to initiate the policy) as per your requirement.
 - iv. Select the **Execution Frequency** (frequency at which to run the policy).
 - b. Click **Packages**, and then click **Configure**.
 - i. Click **Add** (next to the package name) to select the above added .pkg file.
 - ii. Select **Cloud distribution point** from the **Distribution Point** drop down.
8. Select the **Scope** tab, and then add the target computers and target users to run the Jamf policies. You can click **Add**, displayed next to **Selected Deployment Targets** to add a specific target.
Click **Save**.

9. Execution of the policy to install the Mac Logon Agent by using Jamf Pro policies on the targeted machine will be done automatically (based on the configured trigger event).

Silent Configuration

Perform the following steps to configure the agent on a targeted machine:

1. Add the following parameters in the **sampleConfig.agent** file (available in the package):

```
{
  "Data": {
    "Communication": {
      "PrimaryTokenValidatorUrl": "",
      "SecondaryTokenValidatorUrl": "",
      "agentStatus": "0",
      "emergencyPassword": "1",
      "logLevel": "3",
      "defaultAuthenticator": "1"
      "sslCertificate": "1",
      "usernameFormat": "0",
      "bsidkeyPath": "/usr/local/tales/MLA/",
      "byPassAdmin": "1",
    }
  }
}
```


Parameter	Functionality	Values
PrimaryTokenValidatorUrl [Mandatory]	Primary Server URL	
agentStatus [Mandatory]	To turn on/off the macOS Logon Agent	0 - Off, 1 - On Default: Off
bsidkeyPath [Mandatory]	Downloaded .bsidkey file path location	
sslCertificate [Optional]	To enable/disable SSL Certificate check	1 - enable, 0 - disable Default: enable
SecondaryTokenValidatorUrl [Optional]	Secondary Server URL	
byPassAdmin [Optional]	To bypass strong authentication for domain administrators	0 - No, 1 -Yes Default: Yes
emergencyPassword [Optional]	To allow use of emergency passwords	0 - No, 1 -Yes Default: Yes

Parameter	Functionality	Values
usernameFormat [Optional]	To set the username format	0 - username, 1 - domain\username, 2 - user@domain.com Default: username
logLevel [Optional]	To set the minimum Log level	0 - Critical, 1 - Error, 2 - Warning, 3 - Info, 4 - Debug Default: Info
defaultAuthenticator [Optional]	Automatically use the default authenticator that is set for each user	0 - No, 1 - Yes Default : Yes

2. Copy the content of the updated sampleConfig.agent file.
3. Open **Configure_macLogon** script file and paste the content (that you copied in the previous step) in **line 3** between ' and ':


```
echo 'copied_content' > /usr/local/tales/MLA.agent
```

```
1 #!/bin/bash
2
3 echo ' ' > /usr/local/tales/MLA.agent
```

4. In **Jamf Pro**, click the **Settings** icon  on the top right-hand side corner.
5. Select **Computer Management**, and then click **Scripts**.
6. Click **New** on top right-hand side corner to add a new script.
 - a. In the **General** tab, enter a **Display Name** for the script.
 - b. In the **Script** tab, copy and paste the updated **Configure_macLogon.sh** script.
 - c. Click **Save**.
7. To add a policy,
 - a. Perform [Step 6](#) and [Step 7 > Point A](#) of the above section.
 - b. Click **Script**, and then click **Configure**. Now, click **Add** (next to the script name) to select the above added script.
 - c. Select the **Scope** tab, and then add the target computers and target users to run the Jamf policies. You can click **Add**, displayed next to **Selected Deployment Targets** to add a specific target.
 - d. Click **Save**.
8. Execution of the policy to configure the Mac Logon Agent by using Jamf Pro policies on the targeted machine will be done automatically (based on the configured trigger event).

Silent Uninstallation

Perform the following steps to uninstall the agent on the targeted machine:

1. In **JamfPro**, click the **Settings** icon  on the top right-hand side corner.
2. Select **Computer Management**, and then click **Scripts**.
3. Click **New** on top right-hand side corner to add a new script.
4. In the **General** tab, enter a **Display Name** for the script.
5. In the **Script** tab, copy and paste **SafeNet_Agent_For_macOS_UnInstaller.sh** script.
6. Click **Save**.
7. To add a policy, perform [Step 8](#) of the above section.
8. Execution of the policy to uninstall the Mac Logon Agent by using Jamf Pro policies on the targeted machine will be done automatically (based on the configured trigger event).

CHAPTER 3: Installing and Uninstalling the asgent using Installation file

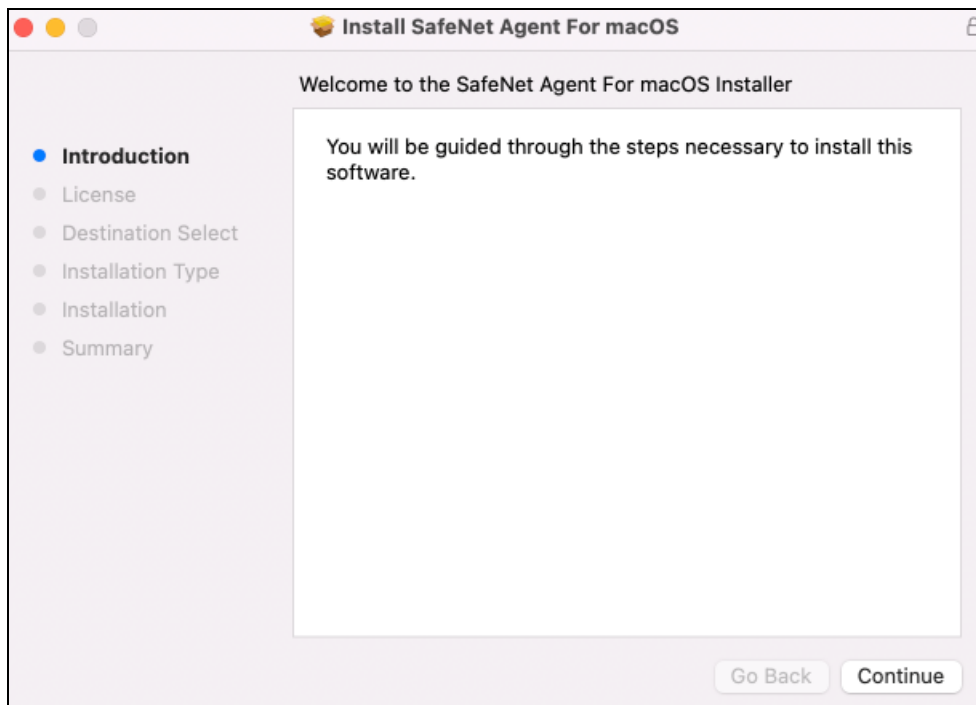
You can install the SafeNet Agent for macOS Logon using either the [wizard](#) or install it [silently](#). This section also describes the [uninstallation](#) process.

NOTE Administrative rights to the macOS system are required for installing, configuring, and uninstalling the SafeNet Agent for macOS Logon.

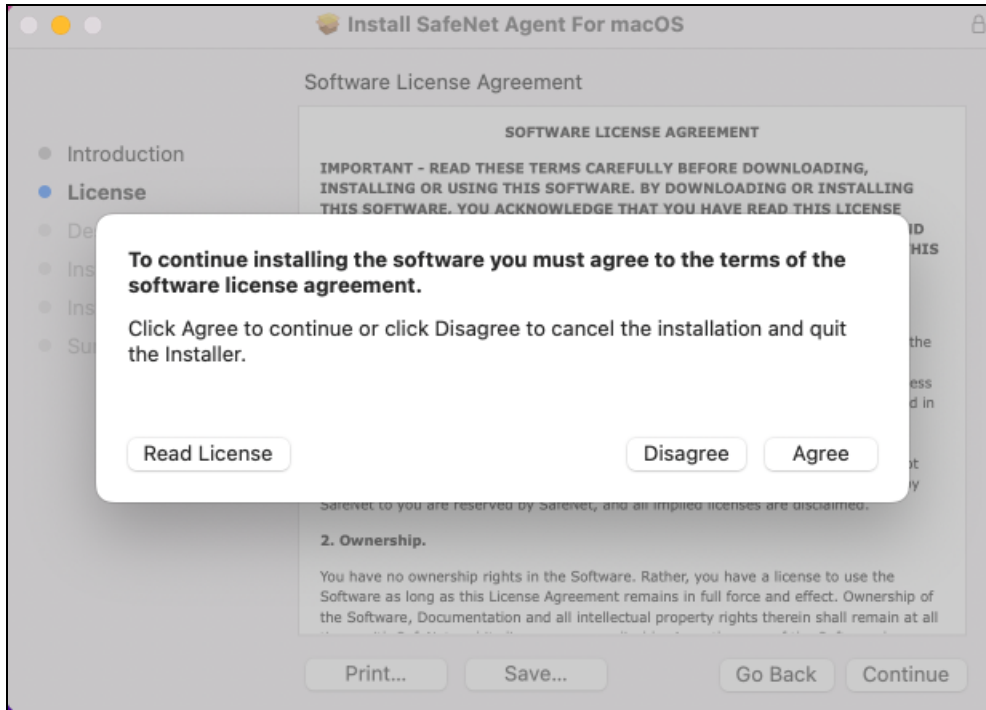
Installing the Agent

Perform the following steps to install the agent:

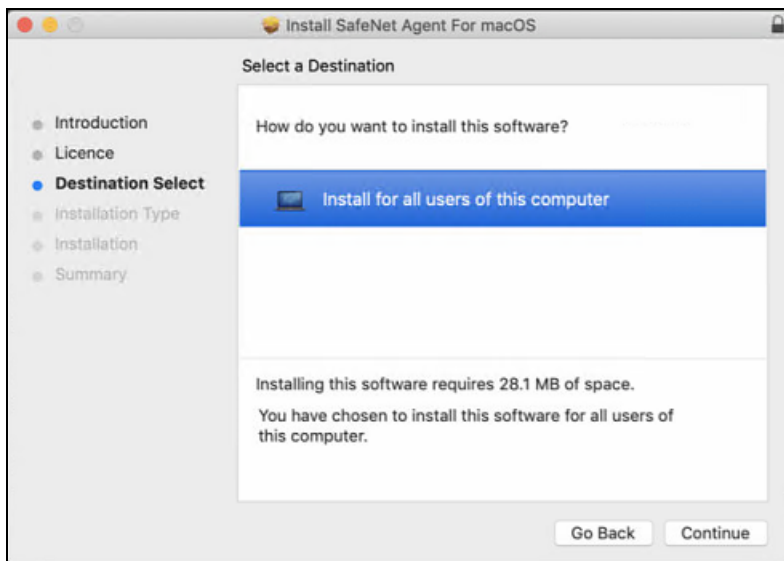
1. Locate the installation file and run the following installer:
`SafeNet_Agent_For_macOS_Installer.pkg`
2. Perform the following steps in the **Installation** wizard:
 - a. On the **Introduction** page, click **Continue**.



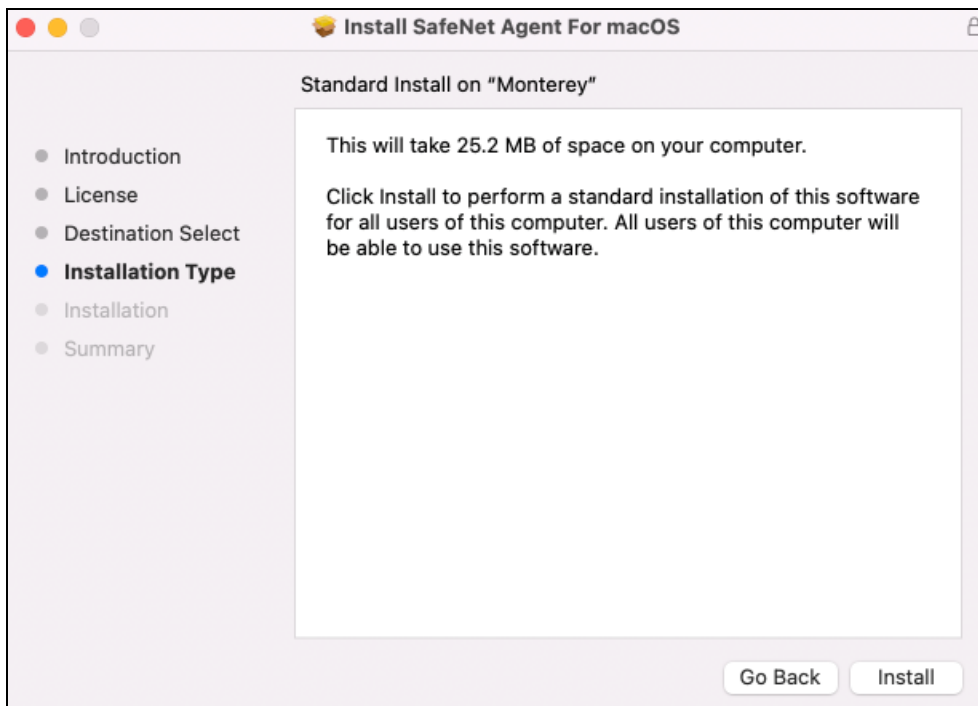
- b. On the **License Agreement** page, read the software license agreement, click **Continue** and to proceed, and click **Agree** to accept the license agreement.



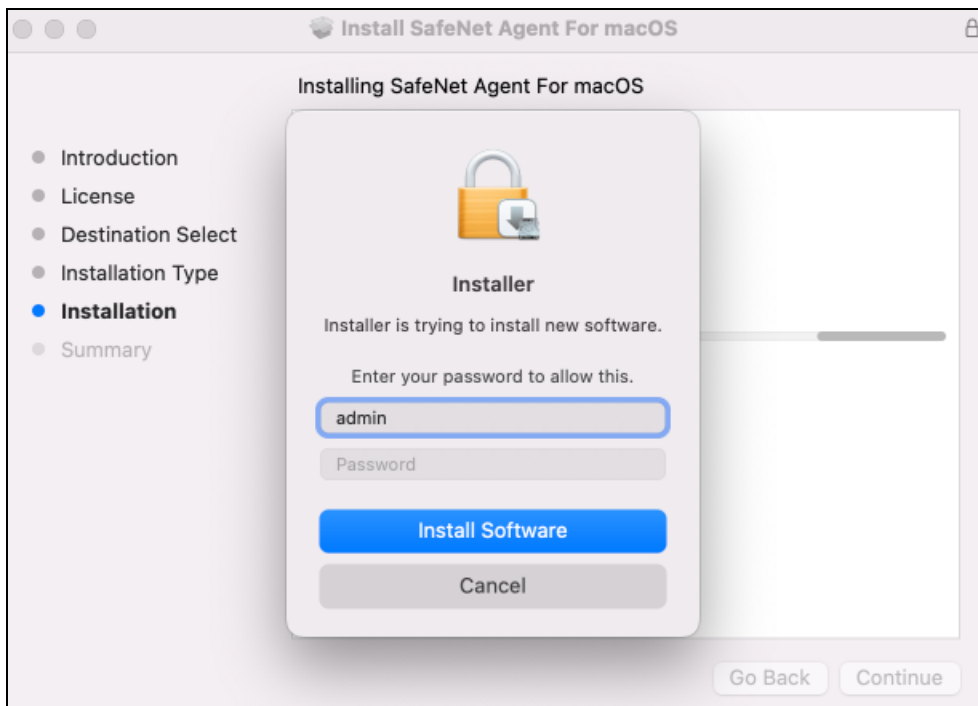
- c. On the **Destination Select** page, click **Continue**.



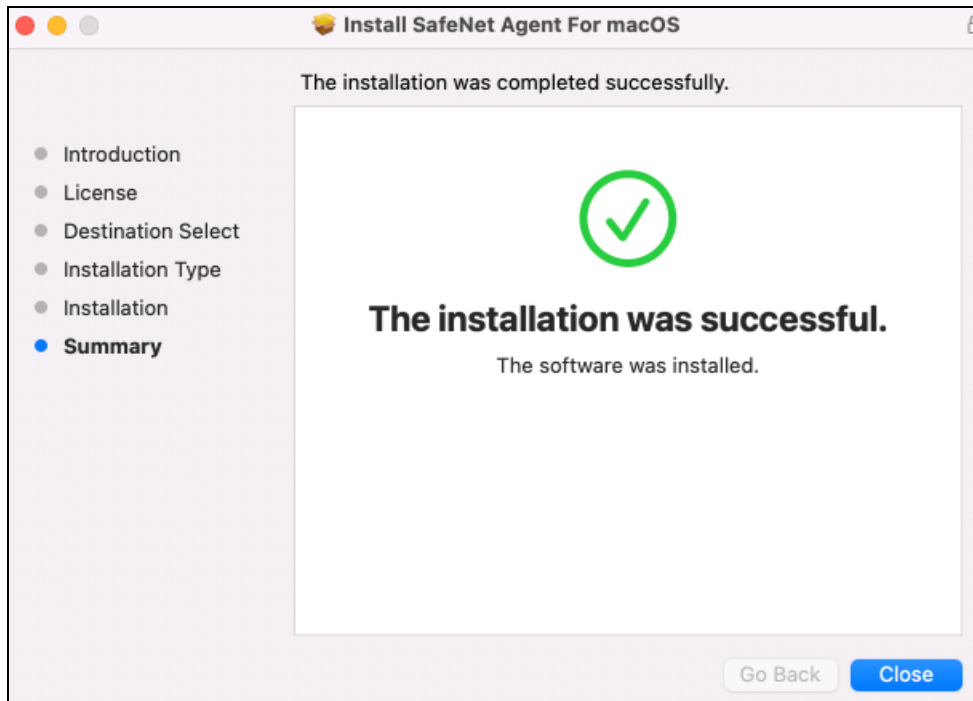
- d. On the **Installation Type** page, click **Install**.



- e. Enter the administrator's **Username** and **Password**, and click **Install Software**.



After successful authentication, the agent gets installed, and a successful installation message is displayed.



NOTE The agent files are installed at a fixed location.

Silent Installation

To install the SafeNet Agent for macOS Logon in silent mode, perform the following steps:

1. Open the terminal and navigate to the folder that contains the installer.
2. Run the following command from the command line:


```
sudo installer -store -pkg SafeNet_Agent_For_macOS_Installer.pkg -target /
```
3. To configure the agent in SAS PCE:

- a. Update the **sampleConfig.agent** (available in the downloaded package) as per your requirement.
- b. Copy the content of the updated sampleConfig.agent file.
- c. Open **Configure_macLogon.sh** script file and paste the value (that you have copied in the previous step) in **line 3** between ' and '.

```
echo 'copied_content' > /usr/local/thales/MLA.agent
```

```
1 #!/bin/bash
2
3 echo '' > /usr/local/thales/MLA.agent
```

- d. Run Configure_macLogon using the following command:

```
sh Configure_macLogon
```

Uninstalling the Agent

You can uninstall the SafeNet Agent for macOS Logon in two ways:

Perform the following steps to uninstall the agent:

1. Run **SafeNet_Agent_For_macOS_UnInstaller**, provided with the installer package.
2. Enter your local administrator **password**.

Or,

Perform the following steps using the **terminal**:

1. Navigate to the directory where the package is downloaded.
2. Run the following command:
`sh SafeNet_Agent_For_macOS_UnInstaller`
3. Enter the administrator password.

All the installed files of macOS Logon Agent will be uninstalled.

CHAPTER 4: Configuring the macOS Logon Agent

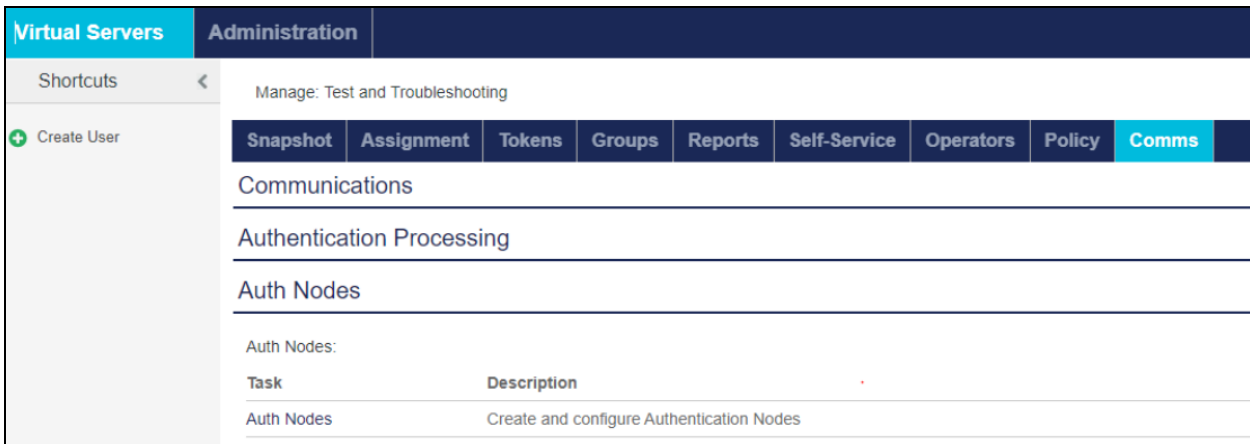
This section describes the steps to configure an Auth Node in the SafeNet server and explains the management console settings to configure various options available within the agent.

- > [Configuring Auth Node in SafeNet server](#)
- > [Configuring Settings within the Agent](#)

Configuring Auth Node in SafeNet server

An **Auth Node** enables you to configure the macOS Logon agent so that it can send authentication requests to your Virtual Server in the SafeNet server. To add an Auth Node, perform the following steps:

1. Click **Virtual Servers > Comms > Auth Nodes (Module) > Auth Nodes (Task)**.



2. Click **Add** to add an Auth Node.

Auth Nodes

Auth Nodes:

Task	Description
Auth Nodes	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, refer to the recommendations included in the SafeNet Authentication Service Administrator Guide.

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

Primary RADIUS Server IP: nnn.nn.nn:nnnn Primary Agent: domain.com:nnn Max. Auth Nodes:10

Failover RADIUS Server IP: nnn.nn.nn:nnnn Failover Agent: domain.com:nnn

No Records

You can click **Change Log** to view the last five changes to Auth Nodes.

NOTE The number of Auth Nodes that can be added is limited to the **Max. Auth Nodes** value entered in On-Boarding > Services. For more information, refer to the *SAS Service Provider Administrator Guide*. To increase this value, contact your Service Provider.

- The **Add Auth Node** section displays. Complete the fields provided to accurately describe the Auth Node, as follows:

Add Auth Node

Save **Cancel**

Auth Nodes

Auth Node Name: Exclude from PIN change requests

Resource Name: Configure FreeRADIUS Synchronization

Host Name: Shared Secret: **Generate**

Low IP Address In Range: Confirm Shared Secret:

High IP Address In Range: FreeRADIUS synchronization may take up to 5 minutes to propagate in the system.

- Auth Node Name** — Enter a descriptive name of the device that can be used to indicate the vendor and model of the Auth Node product.
- Resource Name** — Identifies in a push notification which authentication node it relates to, so the user can be sure they are authenticating a valid node. By default, this is the **Auth Node Name**. Unlike **Auth Node Name**, the **Resource Name** does not have to be unique.

NOTE If authentication nodes are shared, the **Resource Name** is inherited from the parent account. If authentication nodes are shared with child accounts, make sure that the **Resource Name** is also meaningful to users of these child accounts.

- Host Name** — Indicates the FQDN (Fully Qualified Domain Name) of the Auth Node. This entry is optional.

- **IP Address** — Indicates the external IP address of the agent (that is, the address from which the Accounts virtual server will receive authentication requests). This field must conform to IPv4 or IPv6 address standards.

4. Click **Save** to save your changes or click **Cancel** to discard your changes.

The **Auth Nodes** section lists the configured auth nodes. Click **Edit** to edit and **Remove** to remove the corresponding Auth Node configuration.

Configuring Settings within the Agent

Use the **SafeNet Logon Configuration** to configure various options available within the agent. To configure settings, the following tabs are available:

- > [Settings](#)
- > [Offline](#)
- > [Logs](#)

Settings

This tab deals with the connection options for the SafeNet server.

The screenshot shows the 'SafeNet Logon Configuration' window with the 'Settings' tab selected. The window is divided into four main sections:

- 1. Choose Authentication Options**
 - Turn on agent
 - Bypass strong authentication for domain administrators
 - Allow use of emergency passwords
 - Automatically trigger MobilePASS+ Push, Gridsure or SMS/Email authentication
 - Submit the username in the following format:
 - username
 - domain\username (NetBIOS format)
 - username@domain.com (UPN format)
- 2. Load your Configuration File**
 - STA configuration
 - Configuration file:
 - SAS PCE configuration
 - Primary Server:
 - Secondary Server:
 - Check SSL certificate
 - Agent BSID key:
- 3. Check Connectivity**
 - Test Connectivity with authentication servers
- 4. Test Authentication**
 - Ensure that you can authenticate successfully before you turn on the agent. Use your local username, as defined in the macOS System Preferences > Users & Groups.
 - Username: Result:
 - Passcode:
 -

At the bottom of the window are three buttons: (highlighted in blue), , and .

Choose Authentication Options

Authentication options are used in the process of authenticating information received from authentication sources.

- > **Turn on agent:** This option turns the SafeNet Agent for macOS Logon On or Off.
- > **Bypass strong authentication for domain administrators:** This option allows the following user groups to be exempt from SafeNet authentication during login:
 - Domain Admins
 - Administrators
 - Enterprise Admins
 - Schema Admins
 - DNS Admins

Default Setting: **Enabled**

NOTE

- > Nested groups are not supported.
- > Local Admins cannot be exempted from OTP.

- > **Allow use of emergency passwords:** This allows the use of emergency passwords in the offline mode.
- > **Automatically trigger MobilePASS+ Push, Gridsure or SMS/Email authentication:** Select this option to trigger the automatic challenge. If this option is not selected, the user must submit an empty passcode manually for using MobilePASS+ Push , Gridsure or SMS/Email authentication.

Default Setting: **Enabled**

Submit the username in the following format:

Select any of the following format, based on the user synchronization between AD and STA:

- > **username:** Selecting this option validates the username that is synced in the SafeNet server.
Default Setting: **Enabled**
- > **domain\username(NetBIOS format):** Select if the username exists in the SafeNet server with the prefix **domain**.
Default Setting: **Disabled**
- > **username@domain.com (UPN format):** Select if the username exists in the SafeNet server with the suffix **@domain**.
Default Setting: **Disabled**

Load Your Configuration File

- > **STA configuration: [Default]** This option enables the configuration of macOS Logon agent using STA. It requires a unique agent configuration file. After configuring the agent using this option, the [SAS PCE configuration](#) option will be disabled.

- **Configuration file:** Use this setting to select the agent configuration file, which you have previously downloaded from the **Download and Deploy** section in STA. Click **Browse** to specify the location of the agent's configuration file.

NOTE For more information, refer to *SafeNet Agent for macOS Logon STA* documentation.

- > **SAS PCE configuration:** Select this option to configure the agent using SAS PCE. It requires a unique **BSID key** file.
 - **Primary Server:** Enter the Primary Server Hostname of the SafeNet server.
 - **Secondary Server:** Enter the Secondary Server Hostname of the SafeNet server.
 - **Check SSL certificate:** If selected, the agent validates the certificate from the SafeNet server. The SSL certificate check is enabled by default.
 - **Agent BSID key:** This setting is used to specify the location of the Agent's BSID key File. Click **Load from file** to select the file.

To use the AES-GCM key standard, the administrator needs to download a new *Agent.bsidkey* file from the SafeNet server. Perform the following steps:

1. Login to your SafeNet server account, and navigate to **COMMS > Authentication Processing**.
2. Under **Task** list, click **Authentication Agent Settings** link and download the *Agent.bsidkey* file.
3. Now, click **Browse** to update the *Agent.bsidkey* file at **SafeNet Agent Configuration > Settings > Agent BSID key**.

NOTE

- > If you want to upgrade, you can select **STA configuration** later. There is no need to uninstall the agent explicitly.
- > If you select STA configuration, agent cannot be configured for SAS PCE.

Check Connectivity

Under this section, click **Test** to run a communication test to verify the connection to the SafeNet server.

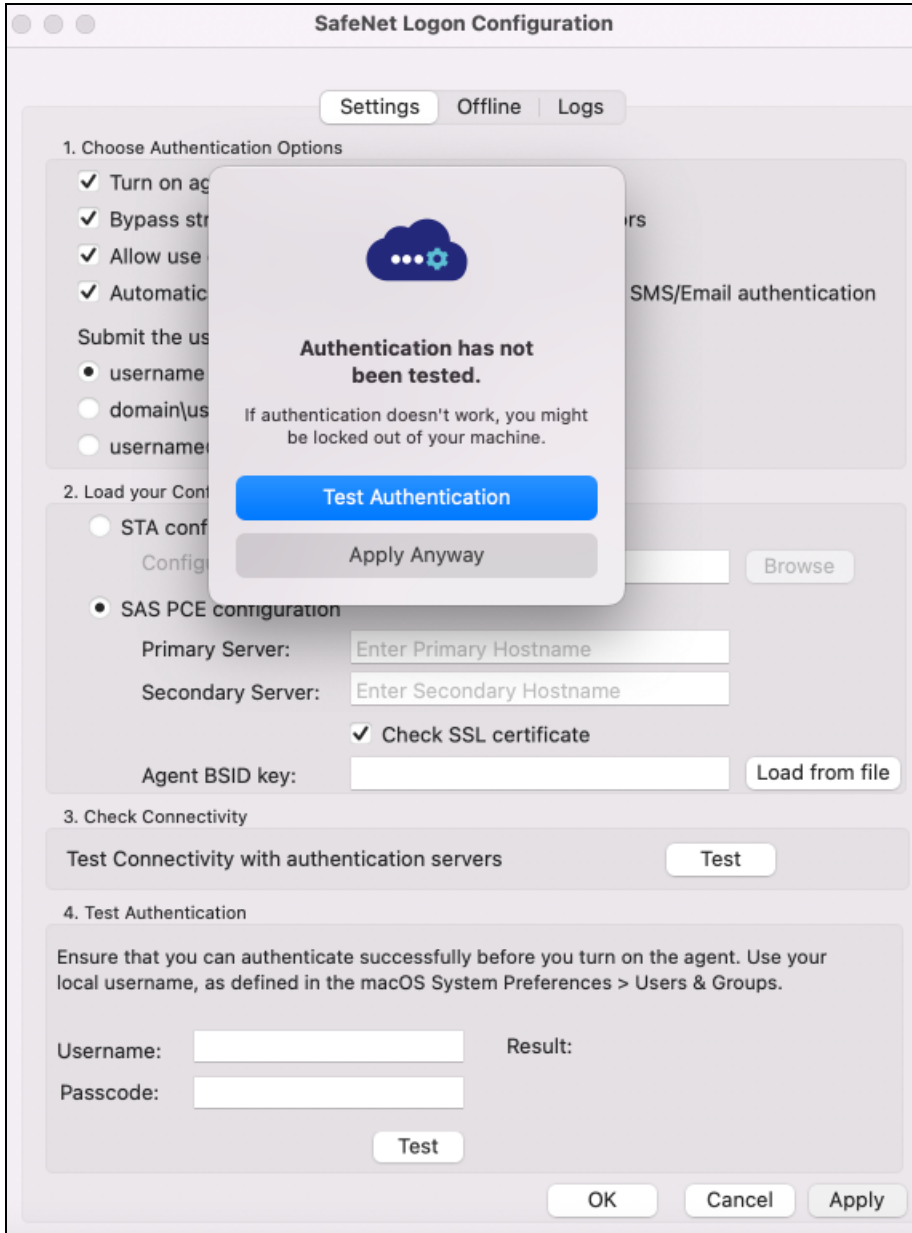
Test Authentication

This allows administrators to test authentication between the agent and the SafeNet server.

NOTE The User Name format needs to be the same as defined for use in the SafeNet server.

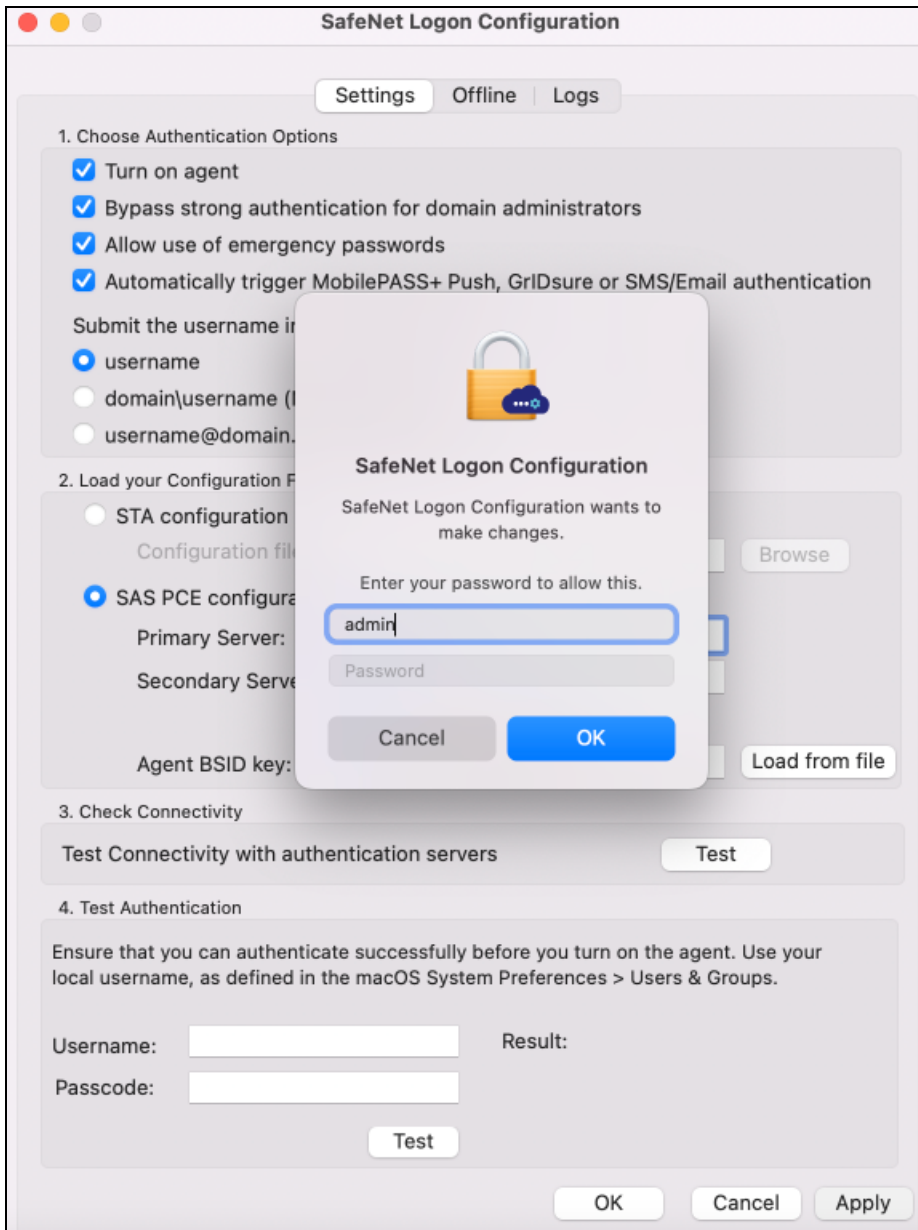
Apply Agent Settings

Click **Apply/Ok** for saving the agent settings. If it is the first time testing the authentication, a confirmation dialog will be displayed. If the authentication is not tested previously, the below pop-up is displayed:



If you click **Apply anyway**, a dialog box prompting administrator password will be displayed.

NOTE After applying the changes, log off is mandatory for the SafeNet Agent for macOS Logon authentication.



Offline

The **Offline** tab deals with the end-user offline authentication settings. It displays the current amount of offline authentication attempts, allows for the customization of the minimum warning notification threshold, and the ability to replenish manually the offline OTP store.

The screenshot shows the 'SafeNet Logon Configuration' window with the 'Offline' tab selected. The window has three tabs: 'Settings', 'Offline', and 'Logs'. The 'Offline' tab is active and contains two main sections: 'Offline Authentication Settings' and 'Manually Replenish'.

Offline Authentication Settings: This section includes a descriptive paragraph: "Offline authentications allow you to log on when you are not connected to a network. When the minimum offline threshold is met, a message reminds you to authenticate online and renew the cache of offline passcodes." Below this are two input fields: 'Remaining offline authentication' with a value of '0' and 'Minimum offline threshold' with a value of '10' and a dropdown arrow.

Manually Replenish: This section includes a descriptive paragraph: "Authenticate with your account to manually replenish your passcode cache and log on to your machine even when you are not connected to a network." Below this are two input fields: 'Username:' and 'Passcode:'. To the right of the 'Username' field is a 'Result:' label. At the bottom of this section is an 'Authenticate' button.

At the bottom of the window are three buttons: 'OK' (highlighted in blue), 'Cancel', and 'Apply'.

Offline Authentication Settings

The SafeNet Agent for macOS Logon allows users to log in to their workstations when the SafeNet server is not available.

- > **Remaining offline authentication:** The number of SafeNet authentication available before the user must authenticate against the SafeNet server or perform a manual replenish. The offline authentication value is a global configuration setting configured within the **Policy Admin, Authentication Policy** section of the SafeNet Manager.

Default Value: **100**

- > **Minimum offline threshold:** The user will see a warning to authenticate against the SafeNet server or perform a manual replenish if this value is reached.

The value may range between **5** and **99**.

Default Value: **10**

Manually Replenish

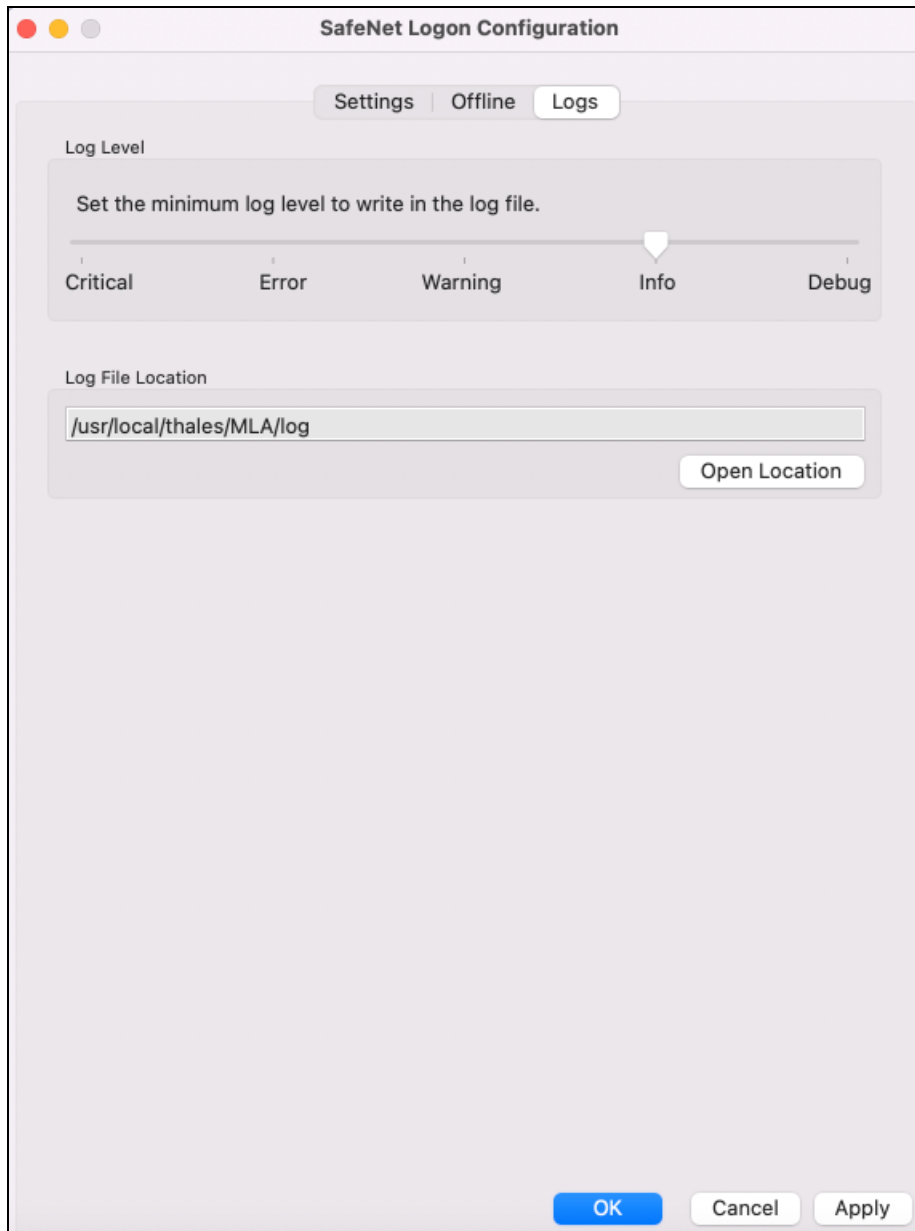
The offline store is automatically replenished when a user returns and logs in to the corporate network, but if the offline store expires while the user is still at a remote location, the **Manually Replenish** option allows the admin user to refill their offline authentication store remotely.

NOTE The User Name format needs to be the same as defined for use in the SafeNet server.

To replenish an offline authentication store manually, perform the following steps:

1. Establish a VPN connection to the corporate network.
2. Open the SafeNet Agent for macOS Logon Configuration tool as an administrator.
3. Enter user's SafeNet credentials in the **Passcode** field, and click **Test**.
4. The SafeNet Agent for macOS Logon contacts the SafeNet server to verify the logon credentials. If the credentials are valid, the offline authentication is restored, otherwise, the user will receive a warning message to retry the authentication attempt.

Logs



Log Level

This setting adjusts the logging level. Each log message has an associated LogLevel, which depicts the importance and urgency of the message. The logs are maintained according to the set LogLevel. For log levels 1, 2, and 3, only the initial connection between the agent and the server, and any failed connection attempts are logged.

Drag the pointer on the **Logging level adjustment** scale to the required level:

- > **1 – Critical:** [Only critical] Very severe error events that might cause the application to terminate.
- > **2 – Error:** [Critical and errors] Error events that prevent normal program execution, but might still allow the application to continue running.

- > **3 – Warning:** [Critical, errors, and warnings] Potentially harmful error events.
- > **4 – Info:** [Critical, errors, warnings, and information messages] Informational error events that highlight the progress of the application. (**Default Option**)
- > **5 – Debug:** [All available information] Detailed tracing error events that are useful to debug an application. (**Recommended**)

The Log files are stored at a fixed location (**/usr/local/thales/MLA/log**).

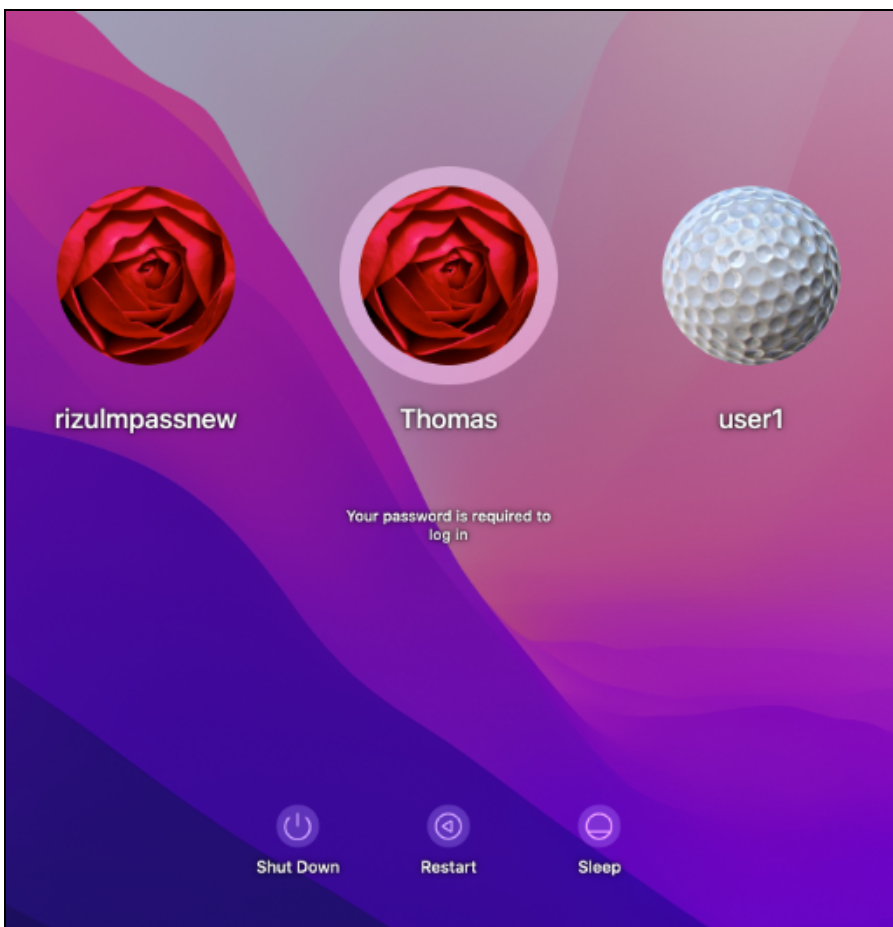
CHAPTER 5: Testing the Solution

You can test the macOS Logon agent using any of the following two options. Perform the following steps:

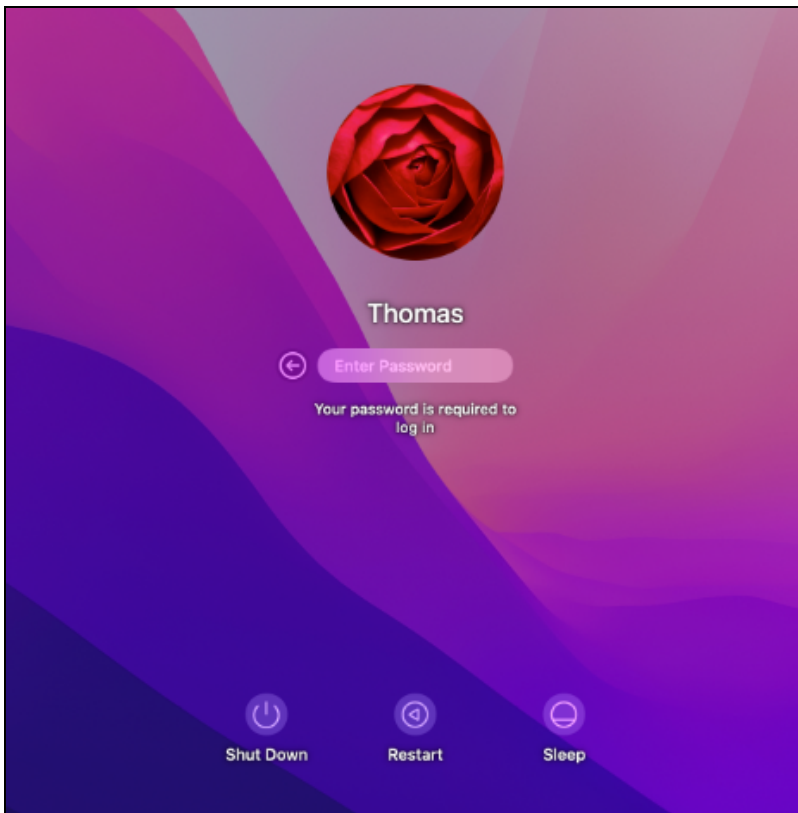
List of Users Option

The following displays the login screen for different user types:

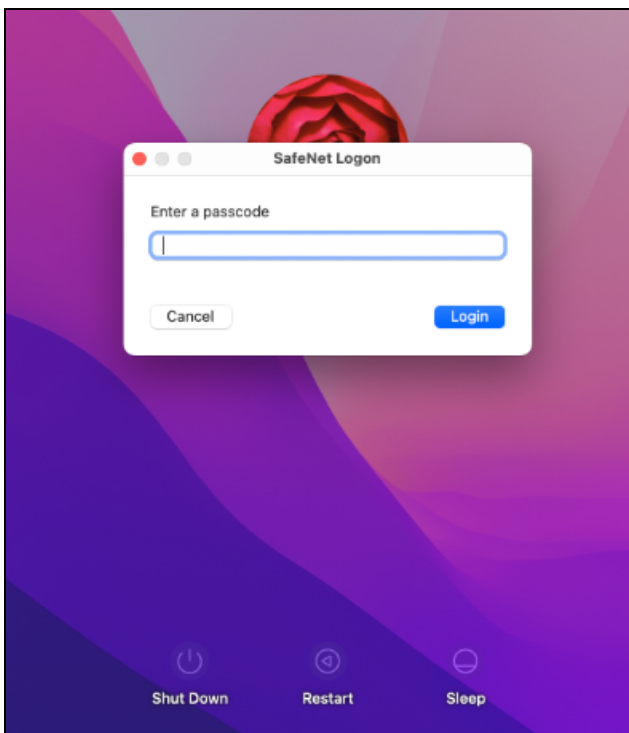
1. On the logon tile, click your **Username** to log in to the macOS Logon agent.



2. In the **Password** field, enter your password and click .

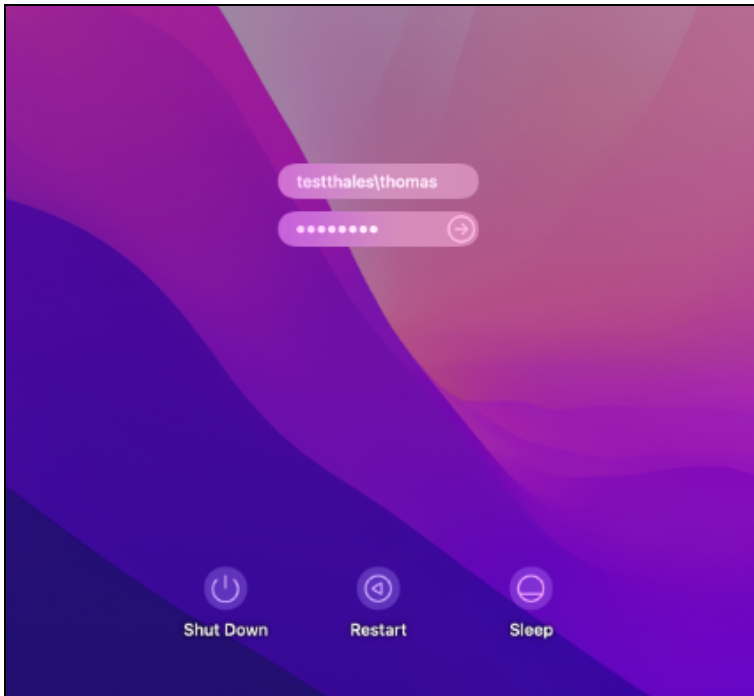


3. In the **Passcode** field, enter the SafeNet OTP and click  to complete the authentication.



Name and Password Option

1. Enter your **Username** and **Password**, and then click .



2. In the **Passcode** field, enter the SafeNet OTP and click  to complete the authentication.

