THALES

SafeNet Agent for Windows Logon 3.5.0

INSTALLATION AND CONFIGURATION GUIDE

Document Information

Product Version	3.5.0
Document Part Number	007-000282-002, Rev. L
Release Date	March 2022

Trademarks, Copyrights, and Third-Party Software

Disclaimer

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.

CONTENTS

PREFACE

This document describes how to install and configure the **SafeNet Agent for Windows Logon**.

Audience

This document is intended for personnel responsible for maintaining your organization's security infrastructure. This includes SafeNet Agent for Windows Logon 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 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.

Related Documents

The following documents contain related or additional information:

> *SafeNet Agent for Windows Logon: Customer Release Notes*

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 Group Customer Support.

Thales Group 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 Group 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 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 Thales Group 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.DIS@thalesgroup.com.

CHAPTER 1: Overview

The SafeNet Agent for Windows Logon is designed to help Microsoft enterprise 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 Windows environment is a critical step for information security.

System Requirements

Software Prerequisites	> Microsoft .NET 4.5 or later
Communication Protocols	> Hypertext Transfer Protocol (HTTP) > Hyper Text Transfer Protocol Secure (HTTPS): - Secure Sockets Layer (SSL) 2.0 and above - Transport Layer Security (TLS) 1.0 and above
Network	> TCP Port 80 (HTTP) or 443 (HTTPS)
Azure Support	> Azure AD* > Hybrid Azure AD
Supported Tokens	All tokens supported by SafeNet Trusted Access, except the following: 4.x legacy, 5.x legacy, 6.x legacy, UB, IronKey, SafeStick, Smart Cards, Microsoft Certificate-Based Authentication (CBA) Login, and FIDO.
Supported Tokens in Offline Authentication Mode	> Emergency Password > Static Password > Event-based tokens, for example, MobilePASS (in Quick Log mode) **NOTE:** Only last used event-based token is supported. When using MobilePASS+, the Push OTP feature does not work, but standard One Time Password (OTP) authentication works.
Supported SAS/STA Releases	> SAS PCE/SPE 3.9.1 (and later) > SafeNet Trusted Access (STA)

* Limitations for Azure AD joined machines

- The **Exempt Local/Domain Administrator strong authentication** does not work with pure Azure AD joined machines for domain admins. However, this feature works as expected for the local admins.
- The **Group Filter** feature does not work with pure **Azure AD** joined machines for domain groups. However, this feature works as expected for the local groups.
- Third-party federation services with Azure AD joined machines are not supported.

Supported Operating Systems

Operating System	Microsoft Credential Provider Tile Version 1	Microsoft Credential Provider Tile Version 2 (recommended)
Windows 8 (32-bit, 64-bit)	X	✓
Windows 8.1 (64-bit)	X	✓
Windows 10 (32-bit, 64-bit)	X	✓
Windows 11 (64-bit)	X	✓
Windows Server 2012 (64-bit)	✓	X
Windows Server 2012 R2 (64-bit)	X	✓
Windows Server 2016 (64-bit)	X	✓
Windows Server 2019 (64-bit)	X	✓

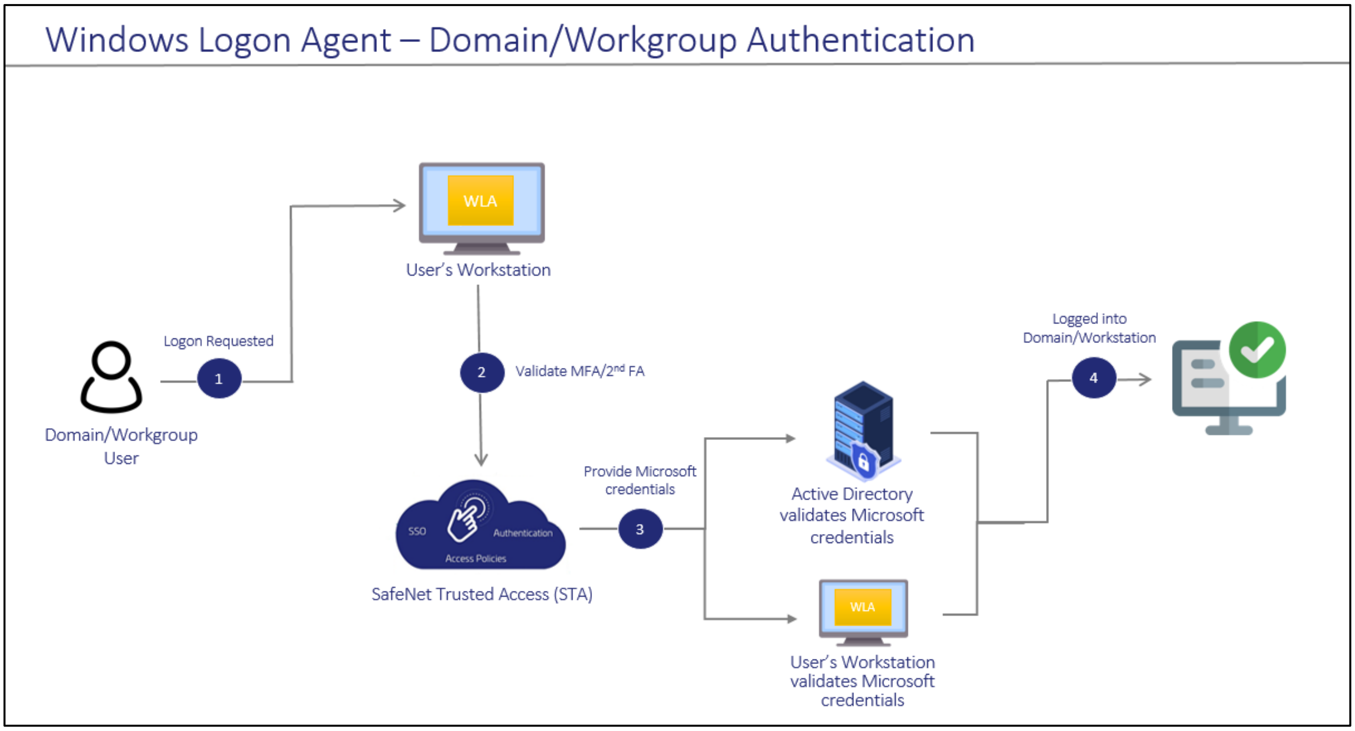
Windows Logon Agent – Authentication Methods

Authentication is a process to verify that the credentials presented are authentic. Windows Logon Agent offers following authentication methods:

- Domain/Workgroup Authentication
- Offline Authentication

Domain/Workgroup Authentication

Domain Authentication refers to the Multi-Factor Authentication of a domain user through the SafeNet server. **Workgroup Authentication** refers to the Multi-Factor Authentication of a local user through the SafeNet server. The following flow diagram describes the user authentication while accessing the domain or local workstation login:


Windows Logon Agent – Domain/Workgroup Authentication
WLA
User's Workstation
Logon Requested
1
Domain/Workgroup User
2
Validate MFA/2nd FA
SSO
Authentication
Access Policies
SafeNet Trusted Access (STA)
Provide Microsoft credentials
3
Active Directory validates Microsoft credentials
WLA
User's Workstation validates Microsoft credentials
Logged into Domain/Workstation
4

1. After invoking the workstation logon, the user is presented with the agent login screen.
2. If Multi-Factor Authentication is required, the user enters the credential of the supported second factor authentication, for example, OTP. The entered credentials are then sent to the SafeNet server for verification.
3. If the SafeNet credentials are valid, the user is prompted for Microsoft credentials.
   - If the user is part of the domain, the credentials are validated by the Active Directory (AD).
   - If the user is part of the local workstation, the credentials are validated by the user's workstation.
4. On successful validation of the Microsoft credentials, the user is logged on to the WLA installed machine.

Offline Authentication

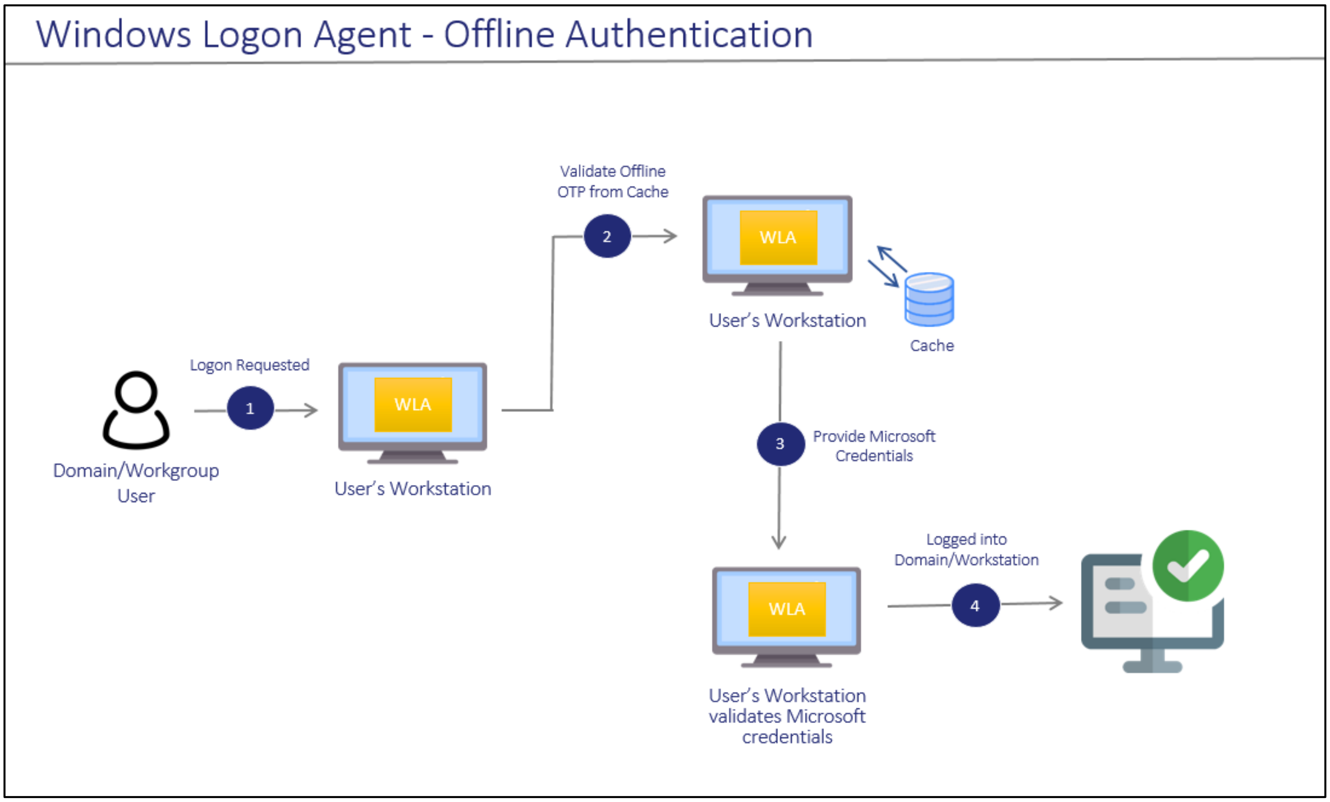
By default, SafeNet Agent for Windows Logon supports offline authentication, which enables users to log on using a SafeNet OTP when there is no connection to the SafeNet server. For details about disabling offline authentication, refer to the *SafeNet Authentication Service Administrator's Guide*.

The agent permits end-user workstations that may be offline periodically for the authentication. Under normal SafeNet Agent for Windows Logon authentication process, a user needs to furnish the OTP for transmission to the SafeNet server. When offline, there is no communication with the SafeNet server, only the local SafeNet Agent for Windows Logon. However, 2FA is preserved; the user must have the token and must know a PIN.

The token can be enabled (for example, using OTPs for logon) or disabled (for example, using a SafeNet static password for logon). However, offline authentication logon can only be done if the last logon before disconnecting from the network was done with an OTP. This is also applicable when the user is configured to use a SafeNet static password.

Refer to the System Requirements section to see the list of supported tokens in the Offline Authentication mode.

NOTE: Offline authentication is not supported in the Remote Desktop Public (RDP) mode.


Windows Logon Agent - Offline Authentication
Domain/Workgroup User
Logon Requested
1
WLA
User's Workstation
Validate Offline OTP from Cache
2
WLA
User's Workstation
Cache
3
Provide Microsoft Credentials
WLA
User's Workstation validates Microsoft credentials
Logged into Domain/Workstation
4

NOTE:
> To use offline authentication, the user must have had logged on online at least once.
> After successful online login, the offline tokens are replenished automatically.
> While online, the user (with admin rights) can also manually replenish the offline tokens through the Management console.

1. After invoking the workstation logon, the user is presented with the agent login screen.
2. If Multi-Factor Authentication is required, the user enters the credential of the supported second factor authentication, for example, OTP. The entered credentials are then verified by the offline authentication OTP stored on the local workstation. Otherwise, if the offline user is part of a local group authentication exception, the credentials are passed to the local workstation.
3. If the SafeNet credentials are valid, the user is prompted for Microsoft credentials.
4. On successful validation of the Microsoft credentials, the user is logged on to the WLA installed machine.

CHAPTER 2: Installing and Upgrading

This section outlines the following:

> Prerequisites

> Installing SafeNet Agent for Windows Logon

> Upgrading SafeNet Agent for Windows Logon

> Silent Installation and Upgrade

You can install and upgrade SafeNet Agent for Windows Logon using either the wizard or msi for silent install/upgrade.

Prerequisites

> TCP port 80 or 443 must be open between the SafeNet Agent for Windows Logon and the SafeNet server.

> Administrative rights for installing SafeNet Agent for Windows Logon on the Windows system.

> Microsoft .NET 4.5 or later must be installed on the machine.

IMPORTANT: Always work in **Run as administrator** mode when installing, upgrading, configuring, and uninstalling the agent.

Installing SafeNet Agent for Windows Logon

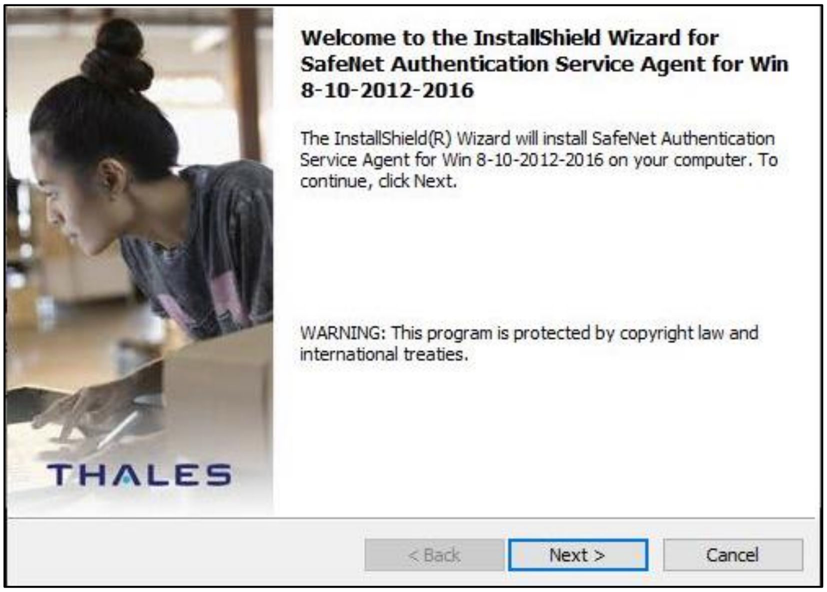
You can install the agent using either the wizard or perform the silent installation.

Installing with the wizard

Perform the following steps to install SafeNet Agent for Windows Logon:

1. Run one of the following installers from the downloaded package (as applicable):
   - *SafeNet Authentication Service Agent for Win 8-10-2012-2016 x86.exe (32-bit)*
   - *SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64.exe (64-bit)*

2. On the **Welcome to the InstallShield Wizard for SafeNet Authentication Service Agent for Win 8-10-2012-2016** window, click **Next**.

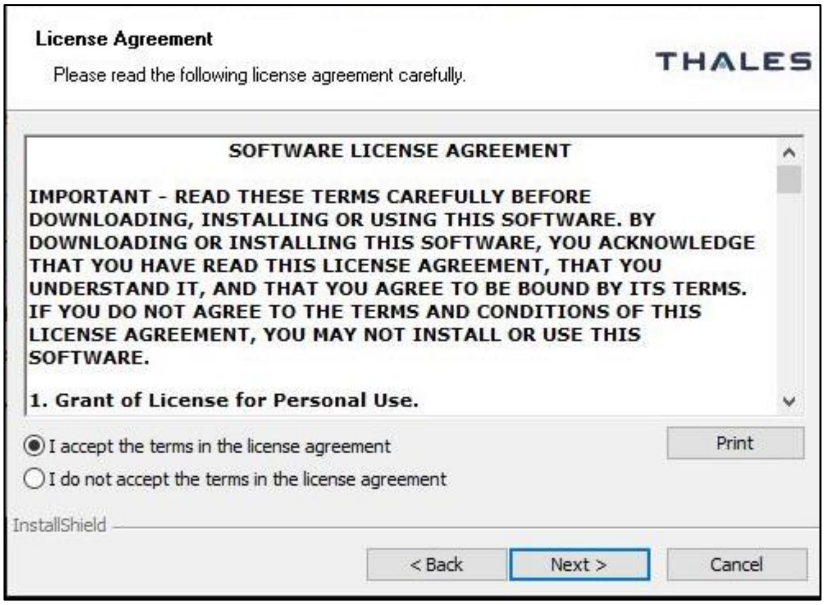


Welcome to the InstallShield Wizard for SafeNet Authentication Service Agent for Win 8-10-2012-2016

The InstallShield(R) Wizard will install SafeNet Authentication Service Agent for Win 8-10-2012-2016 on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

3. On the **License Agreement** window, read the software license agreement and to proceed, select the **I accept the terms in the license agreement** option, and click **Next**.



License Agreement

Please read the following license agreement carefully.

SOFTWARE LICENSE AGREEMENT

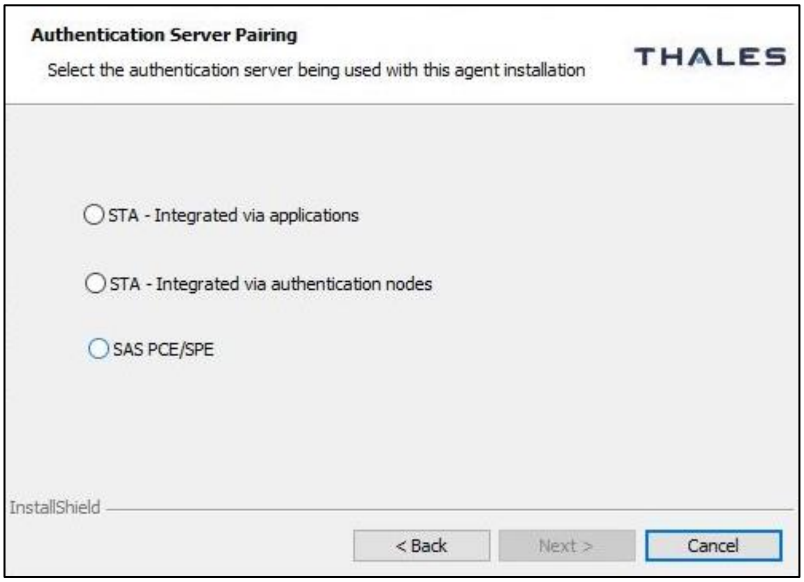
IMPORTANT - READ THESE TERMS CAREFULLY BEFORE DOWNLOADING, INSTALLING OR USING THIS SOFTWARE. BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT, YOU MAY NOT INSTALL OR USE THIS SOFTWARE.

1. Grant of License for Personal Use.

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

4. On the **Authentication Server Pairing** window, select **SAS PCE/SPE** authentication server type, and click **Next**.



Authentication Server Pairing

Select the authentication server being used with this agent installation

○ STA - Integrated via applications

○ STA - Integrated via authentication nodes

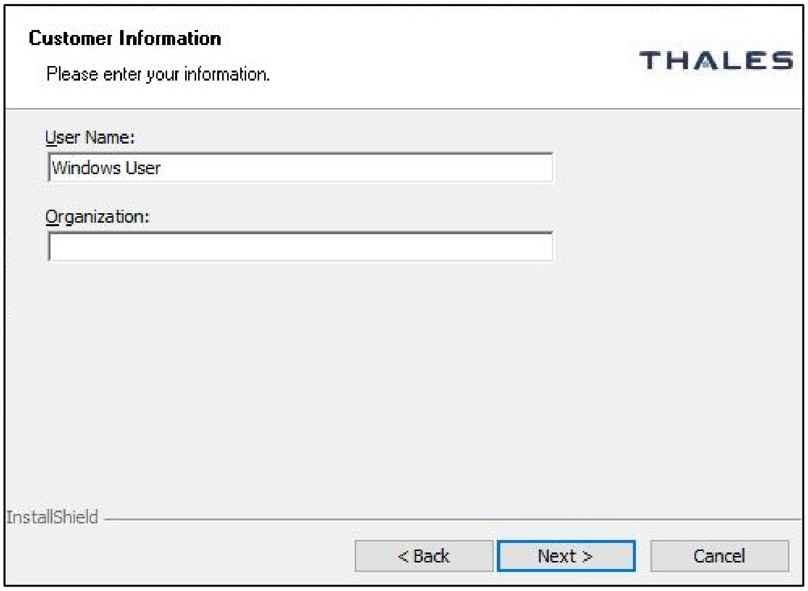
○ SAS PCE/SPE

5. On the **Customer Information** window, perform the following steps:

   a. In the **User Name** field, enter your user name.

   b. In the **Organization** field, enter the name of your organization.

   c. Click **Next**.



Customer Information

Please enter your information.

User Name: Windows User

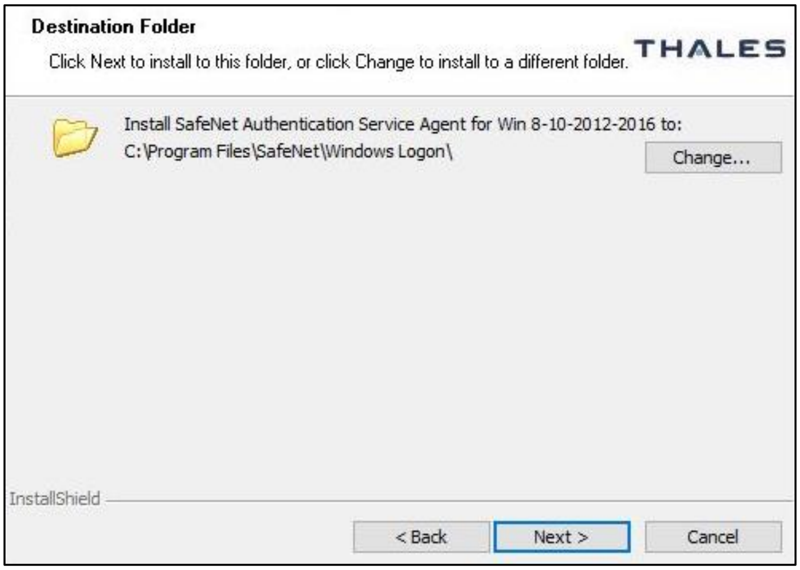
Organization:

6. On the **Destination Folder** window, perform one of the following steps:

   a. To accept the default installation destination folder, click **Next**.

   b. To change the installation folder, other than the default one, click **Change**, and then browse to locate and select the required folder.

   c. Click **Next**.



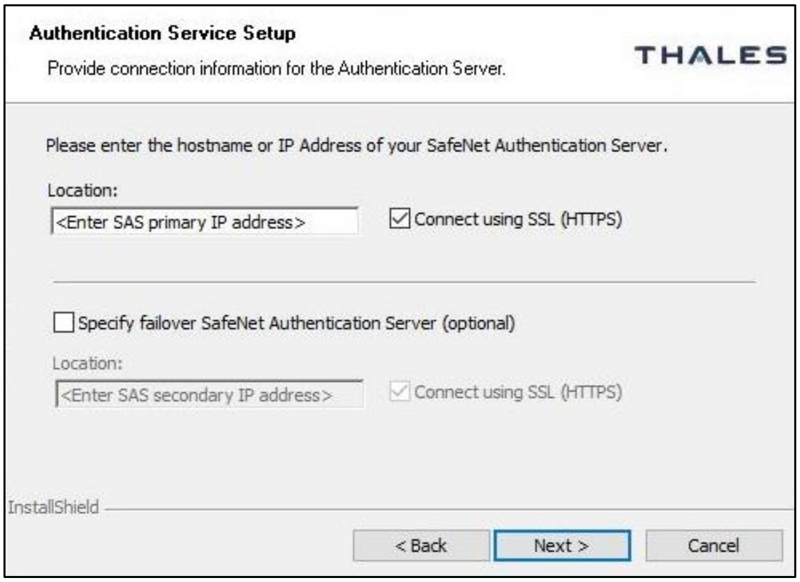
Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install SafeNet Authentication Service Agent for Win 8-10-2012-2016 to:
C:\Program Files\SafeNet\Windows Logon\

7. On the **Authentication Service Setup** window, provide the following information, and click **Next**.

Location	Enter the hostname or IP address of the primary SafeNet server. **NOTE:** Port number used for HTTPS is **443** and for HTTP is **80**.
Connect using SSL (HTTPS)	Select this option if SafeNet server is configured to accept the incoming SSL connections. **NOTE:** We strongly recommend using SSL.
Specify failover SafeNet Authentication Server	Select this check box if a failover SafeNet server is used. If selected, you must enter the **Location**.
Location	Enter the hostname or IP address of the failover SafeNet server.
Connect using SSL (HTTPS)	Select this option if the failover SafeNet server is configured to accept incoming SSL connections.



Authentication Service Setup

Provide connection information for the Authentication Server.

Please enter the hostname or IP Address of your SafeNet Authentication Server.

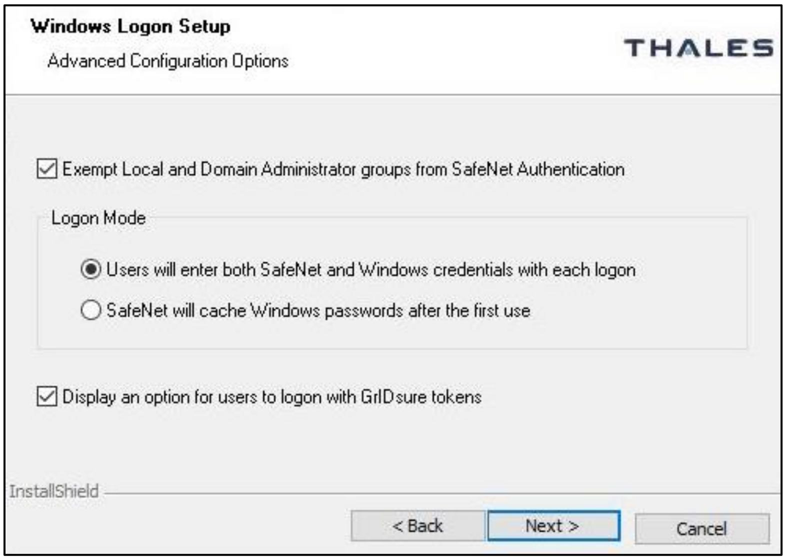
Location: <Enter SAS primary IP address> ☑ Connect using SSL (HTTPS)

□ Specify failover SafeNet Authentication Server (optional)

Location: <Enter SAS secondary IP address> ☑ Connect using SSL (HTTPS)

8. On the **Windows Logon Setup** window, provide the following information, and click **Next**.

Exempt Local and Domain Administrator groups from SafeNet Authentication	Select this check box to allow administrators to log on without providing SafeNet credentials.
Logon Mode	Select one of the following logon modes: • User will enter both SafeNet and Windows credentials with each logon. • SafeNet will cache Windows passwords after the first use.
Display an option for users to logon with GrIDsure tokens	If required, select this check box to logon using the GrIDsure tokens.



Windows Logon Setup

Advanced Configuration Options

☑ Exempt Local and Domain Administrator groups from SafeNet Authentication

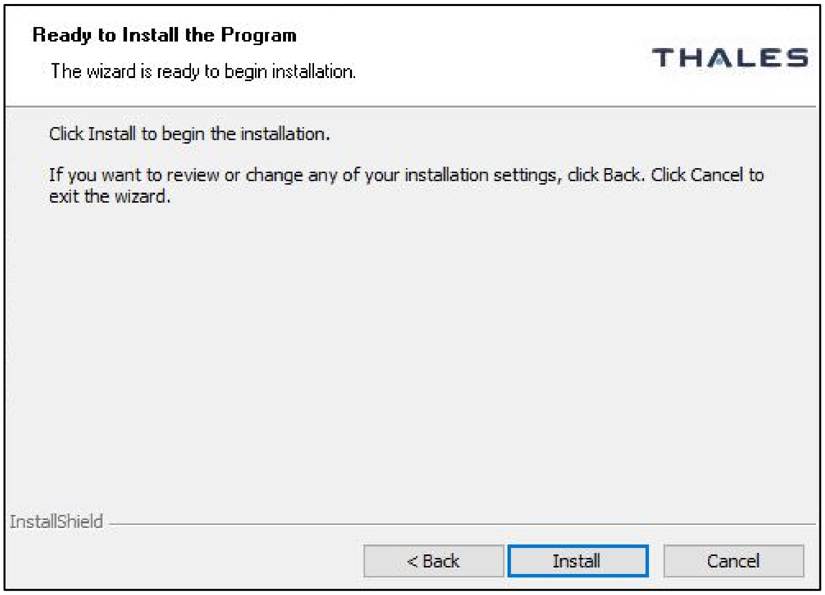
Logon Mode

● Users will enter both SafeNet and Windows credentials with each logon

○ SafeNet will cache Windows passwords after the first use

☑ Display an option for users to logon with GrIDsure tokens

9. On the **Ready to Install the Program** window, click **Install**.



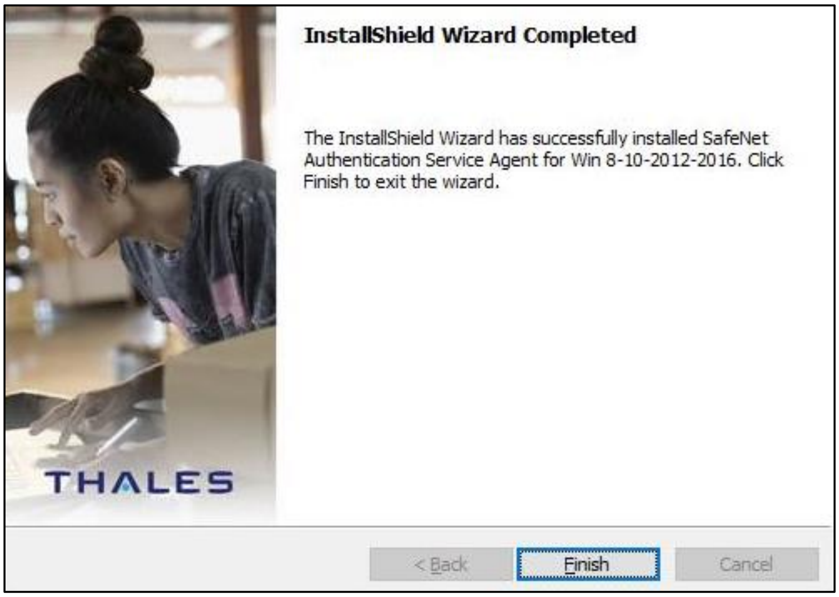
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

10. When the installation process completes, the **Installshield Wizard Completed** window is displayed.
11. Click **Finish**.



InstallShield Wizard Completed

The InstallShield Wizard has successfully installed SafeNet Authentication Service Agent for Win 8-10-2012-2016. Click Finish to exit the wizard.

Silent Installation

Another approach to install the agent is to run the installation silently with parameters. This allows to set the key configuration items for example, authentication server FQDN and logon mode.

A SafeNet Windows Logon **msi** installation package can be launched from the command line. The **msi** files have the same prefixes as the SafeNet installer **exe** files.

```
msiexec /i "SafeNet Authentication Service Agent for Win 8-10-2012-2016
x64.msi" /quiet
```

To set options, the property name is used in name value pairs with spaces in between each pair.

For example, to set the Primary SafeNet server to **192.168.10.200** with SSL and enabled Microsoft **Password Caching** mode, one must run the following command:

```
msiexec /i "SafeNet Authentication Service Agent for Win 8-10-2012-2016
x64.msi" /quiet TOKENVALIDATORLOCATION=192.168.10.200 USESSL=s LOGONMODE=1
```

NOTE: SSL will be enabled by default.

The following is a list of options (parameters) that can be specified. It outlines WLA specific properties with possible values as well as their explanation. If the option is not specified, it will be set to the default value, which is equivalent to clicking **Next** on all pages of the installer dialog.

NOTE: The below listed parameters can only be specified during fresh agent installations (cannot be specified during agent upgrades).

Option	Description	Value
TOKENVALIDATORLOCATION	Defines the Primary SafeNet Authentication Server	IP address or Hostname or FQDN. Default Value: **localhost**
TOKENVALIDATORLOCATION2	Defines the Secondary SafeNet Authentication Server	IP address or Hostname or FQDN. Default Value: **Disabled**
USESSL	Enable SSL to Primary SafeNet Authentication Server (requires certificate)	S otherwise omit USESSL. Default Value: **Disabled**
EXEMPTADMINS	Logon Mode of Operation	**1** for yes, exempts administrators from using MFA **0** for no Default Value: **Dual Logon (0)**
LOGONMODE	Logon Mode of Operation	**0** for “users will supply both passwords each time”. Windows password and MFA is required **1** for “Microsoft password caching”. Windows password is hidden (cached) Default Value: **Dual Logon (0)**

Upgrading SafeNet Agent for Windows Logon

Upgrading with the wizard

The SafeNet Agent for Windows Logon 3.5.0 supports upgrade from 2.2.1 (or later versions).

To upgrade, run the installation wizard and select appropriate options when prompted.

> **NOTE:** For consistent behavior, we highly recommend you to upgrade the agent in online mode or when SafeNet server is available.

Silent Upgrade

To run silent upgrade, run the following command:

```
msiexec /i "SafeNet Authentication Service Agent for Win 8-10-2012-2016
x64.msi" /quiet REINSTALLMODE=vomus REINSTALL=ALL
```

> **NOTE:** The SafeNet Agent for Windows Logon 3.5.0 supports upgrade from 2.2.1 (or later versions). When upgrading in silent mode, the Off-line authentication parameter is not transferred.

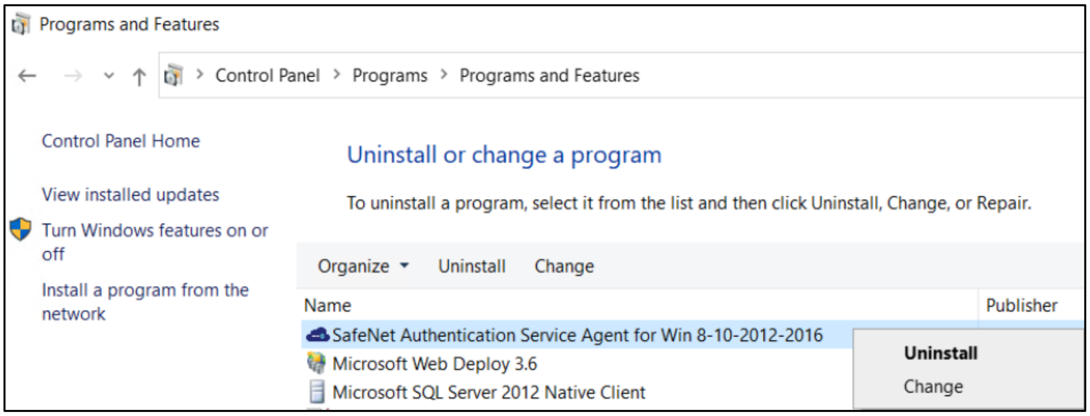
Uninstalling the SafeNet Agent for Windows Logon

You can uninstall the agent either from *Control Panel* or by running the *msi* for silent uninstallation.

Uninstalling using the Windows Control Panel

To uninstall the SafeNet Agent for Windows Logon, perform the following steps:

1. Navigate to **Start** > **Control Panel** > **Programs** > **Programs and Features**.
2. Select the **SafeNet Authentication Service Agent for Win 8-10-2012-2016** program.
3. Click **Uninstall**.


Programs and Features
Control Panel > Programs > Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Install a program from the network
Uninstall or change a program
Organize
Uninstall
Change
Uninstall
Change

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher
SafeNet Authentication Service Agent for Win 8-10-2012-2016	
Microsoft Web Deploy 3.6	
Microsoft SQL Server 2012 Native Client	

Silent Uninstall

To uninstall the agent silently, run the following command on the command line:

```
msiexec /x <installerName>.msi
```

> **NOTE**: If you have installed the agent using the provided .exe, then you cannot uninstall it using .msi and vice-versa.

CHAPTER 3: Configuration

This section describes deployment and configuration tasks related to the SafeNet Agent for Windows Logon.

Realm Stripping Settings

To work with a short SafeNet server username format (for example, *bill* instead of *Domain\bill* or bill@domain.com), after installation, activate the strip function in the **SafeNet Windows Logon Agent Manager > Communications** tab.

For more information, refer to the Communications Tab section.

> **NOTE:** Alternatively, the realm-stripping feature can be configured using the **SafeNet Authentication Service**, **Auth Node Module**. For more information, refer to the *SAS Service Provider Administrator Guide*.

Configuring Transport Layer Security

To configure TLS 1.1/1.2 support on the SafeNet Agent for Windows Logon, set the registry settings as given below:

> `HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client DisabledByDefault => 0x0`

> `HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client DisabledByDefault => 0x0`

> **NOTE:** The agent will always connect with the highest enabled protocol.

Push Authentication

The SafeNet Agent for Windows Logon supports Push OTP when working with MobilePASS+.

If the SafeNet server is configured to support Push OTP, the feature is supported by the SafeNet Agent for Windows Logon. No additional configuration is required in the agent.

> **NOTE:** Push Authentication is supported when working with STA Edition. For SAS PCE/SPE, Push Authentication is only supported with version 3.9.1 (and onwards).

For more details, refer to the SAS-PCE or STA documentation.

Configuration Management

Use the **SafeNet Windows Logon Agent Manager** to configure various options available within the agent.

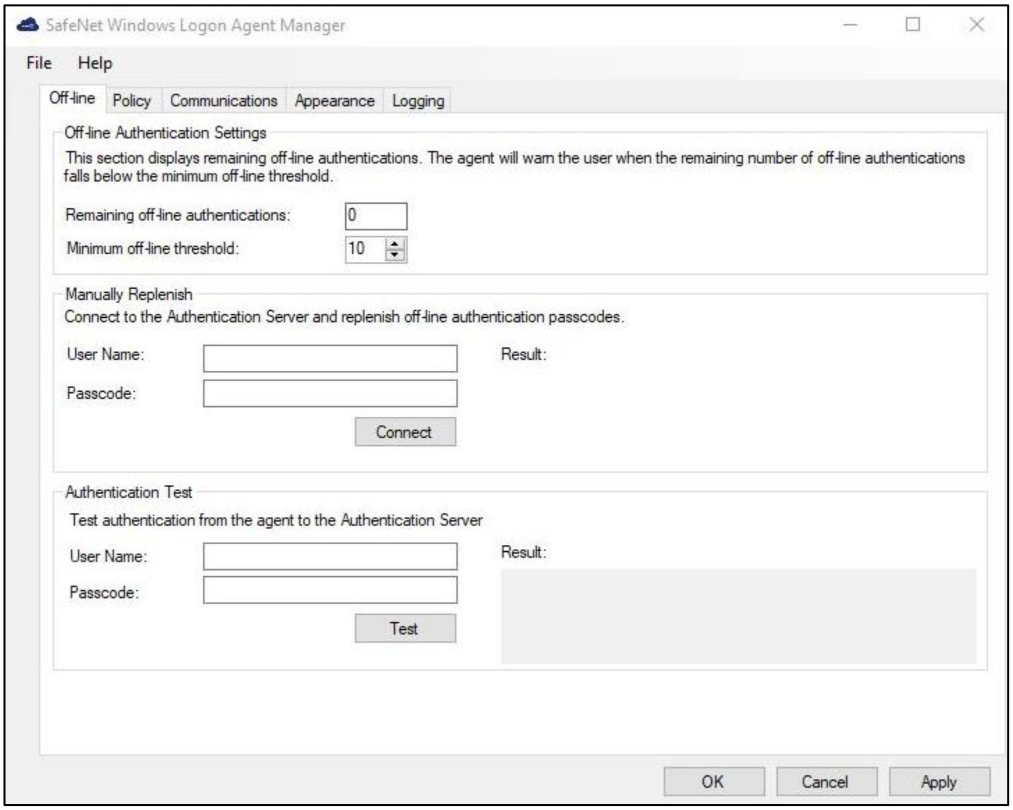
The **Off-line**, **Policy**, **Communications**, **Appearance**, and **Logging** tabs are available only to users who are part of the **Local Administrators** and **Domain Administrators** groups. All other groups will only see the Offline Authentication Settings in the **Off-line** tab.

> **NOTES:**
> **>** To use all features of the Windows Logon Agent Manager, you must work in **Run as Administrator** mode.
> **>** When working in **User** mode, the user can access the **Off-line** tab only.
> **>** The SafeNet Windows Logon Agent Manager cannot be accessed by a domain administrator from a trusted domain using administrator rights.

Off-line Tab

The **Off-line** tab deals with end-user offline authentication settings. It displays the current number of off-line authentication attempts, allows customization of the minimum off-line threshold, provides the ability to manually replenish the off-line OTP store, and to test authentication requests to the SafeNet server. This tab allows to configure the following parameters:

- Off-line Authentication Settings
- Manually Replenish
- Authentication Test



This section displays remaining off-line authentications. The agent will warn the user when the remaining number of off-line authentications falls below the minimum off-line threshold.

Remaining off-line authentications: 0

Minimum off-line threshold: 10

Connect to the Authentication Server and replenish off-line authentication passcodes.

User Name:

Passcode:

Result:

Test authentication from the agent to the Authentication Server

User Name:

Passcode:

Result:

Off-line Authentication Settings

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

The following is a list of options (parameters) that can be specified. If the option is not specified, it will be set to the default value.

Option	Description	Value
Remaining off-line authentications	The number of SafeNet authentication available before the user must authenticate against SafeNet server or perform a manual replenish. The offline authentications value is a global configuration setting configured within the **Policy Admin, Authentication Policy** section of the SafeNet server Manager.	Default Value: **100**
Minimum off-line 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 users return and log in to the corporate network, if the offline store expires while the users are still at a remote location, the **Manually Replenish** option allows admin users 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 Windows Logon Agent Manager as an administrator.
3. Enter the user’s SafeNet credentials into the **Passcode** field, and click **Connect**.
4. The SafeNet Agent for Windows Logon contacts 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.

Authentication Test

This allow 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.

Policy Tab

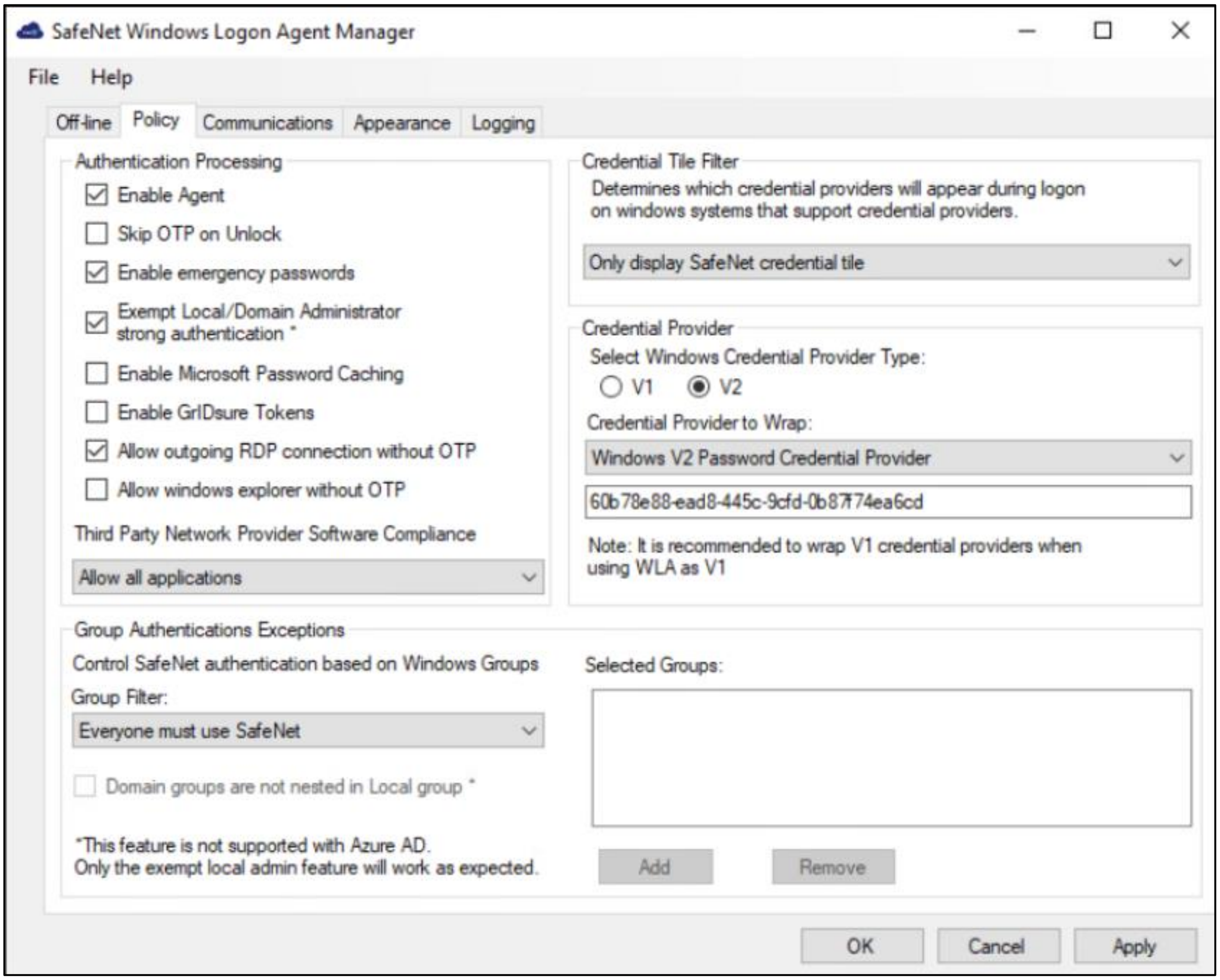
The **Policy** tab allows SafeNet authentication exclusions to be applied to the SafeNet Agent for Windows Logon. This tab allows to configure the following parameters:

> Authentication Processing

> Credential Tile Filter

> Credential Provider

> Group Authentication Exceptions



Authentication Processing

☑ Enable Agent

□ Skip OTP on Unlock

☑ Enable emergency passwords

☑ Exempt Local/Domain Administrator strong authentication *

□ Enable Microsoft Password Caching

□ Enable GrIDsure Tokens

☑ Allow outgoing RDP connection without OTP

□ Allow windows explorer without OTP

Third Party Network Provider Software Compliance: Allow all applications

Credential Tile Filter

Determines which credential providers will appear during logon on windows systems that support credential providers.

Only display SafeNet credential tile

Credential Provider

Select Windows Credential Provider Type: ○ V1 ● V2

Credential Provider to Wrap: Windows V2 Password Credential Provider

60b78e88-ead8-445c-9cfd-0b87f74ea6cd

Note: It is recommended to wrap V1 credential providers when using WLA as V1

Group Authentications Exceptions

Control SafeNet authentication based on Windows Groups

Group Filter: Everyone must use SafeNet

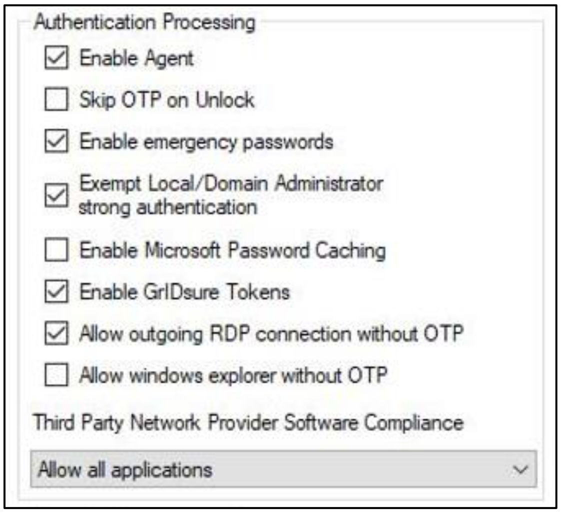
□ Domain groups are not nested in Local group *

*This feature is not supported with Azure AD. Only the exempt local admin feature will work as expected.

Selected Groups:

Authentication Processing

Authentication Processing section specifies the options to be enabled or disabled while processing the authentication.



Authentication Processing

☑ Enable Agent

□ Skip OTP on Unlock

☑ Enable emergency passwords

☑ Exempt Local/Domain Administrator strong authentication

□ Enable Microsoft Password Caching

☑ Enable GrIDsure Tokens

☑ Allow outgoing RDP connection without OTP

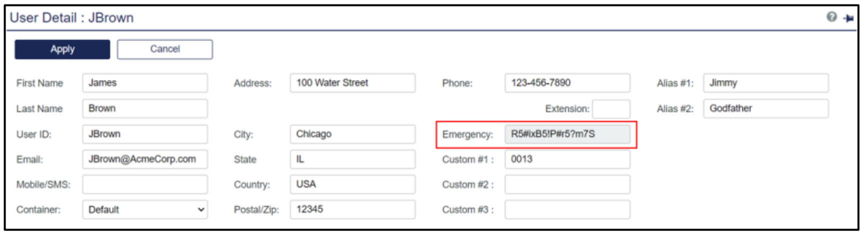
□ Allow windows explorer without OTP

Third Party Network Provider Software Compliance

Allow all applications

The following is a list of options (parameters) that can be specified. If the option is not specified, it will be set to the default setting.

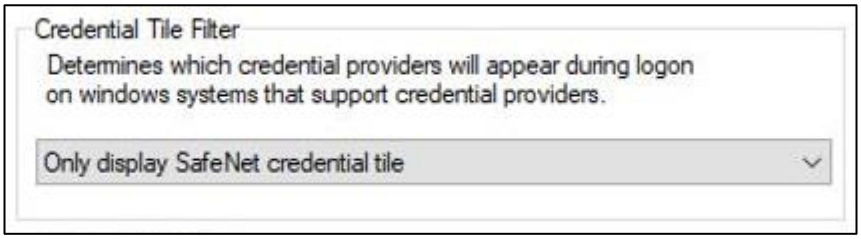
Option	Description	Default Setting
Enable Agent	This option turns the SafeNet Agent for Windows Logon On or Off.	Enabled
Skip OTP on Unlock	This option allows the administrators to enable/disable the SafeNet 2FA for last logged on user on system unlock. Selecting the option ensures that the SafeNet Agent for Windows Logon does not prompt for an OTP, reducing friction every time a user unlocks a machine. The functionality extends to sleep and hibernate modes, which means that if the Skip OTP on Unlock check box is selected, and the system enters sleep or hibernate mode, the SafeNet Agent for Windows Logon does not prompt for an OTP, and instead logs in successfully using only AD credentials.	Disabled
Enable emergency passwords	This option turns the emergency password feature On or Off. This feature is an authentication method that allows a user to authenticate using an Emergency password when the SafeNet server is not available. Each user will have a unique emergency password, which exists on the **Secured Users** tab of the SafeNet server Manager. The emergency password can be used until the workstation regains contact with the SafeNet server, at which point it will be randomized. **NOTE**: This is applicable only in the case of offline mode.	Enabled

Option	Description	Default Setting
	 User Detail : JBrown First Name: James Last Name: Brown User ID: JBrown Email: JBrown@AcmeCorp.com Mobile/SMS: Container: Default Address: 100 Water Street City: Chicago State: IL Country: USA Postal/Zip: 12345 Phone: 123-456-7890 Extension: Emergency: R5#ixB5!P#r5?m7S Custom #1 : 0013 Custom #2 : Custom #3 : Alias #1: Jimmy Alias #2: Godfather	
Exempt Local/Domain Administrator strong authentication	This option allows the **Local** and **Domain Administrator** groups to be exempt from SafeNet authentication during login. **NOTE:** This feature will not work for pure Azure AD joined machines.	Determined during agent installation
Enable Microsoft Password Caching	This option enables or disables **Microsoft Password Caching** mode. **Microsoft Password Caching mode**: For accessing a WLA protected machine, each user authenticates with OTP first, followed by their Microsoft password. In this mode, the user is prompted for their Microsoft password only once for their first log in. Subsequently, the SafeNet Agent for Windows Logon caches the Microsoft password until its expiry or change, furnishing it as required. Passwords are not cached for domain administrators and this mode does not apply for domain admin users.	
Enable GrIDsure Tokens	This option enables or disables the **Use GrIDsure Token** option displayed in the **Windows Logon** dialog prompt. This is required if users have been assigned GrIDsure tokens.	
Allow outgoing RDP connection without OTP	This option enables SafeNet authentication to be bypassed when making an outgoing RDP connection. The **Allow outgoing RDP connection without OTP** feature is not effective if the Microsoft parameter, **`enablecredsspsupport:i:0`**, is set to null. This Microsoft parameter controls credentials usage on the Operating System level for RDP.	Enabled
Allow windows explorer without OTP	Enabling this option allows Windows explorer to run without SafeNet Authentication (bypass SafeNet OTP option). The option is invoked when a network path is accessed or an application is run with other user credentials.	Disabled

Option	Description	Default Setting
Third Party Network Provider Software Compliance	Select one of the following options: > **Allow all applications**: This option is selected by default when the Management console is opened for the first time. This option allows you to install the agent without updating the registry keys under [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order]. **NOTE:** Sometimes, selecting this option creates a conflict between the SafeNet Agent for Windows Logon and the third-party network provider software. In this case, you need to uninstall the third-party network provider software and remove its registry entry. Before executing this operation, you need to perform the following steps: **1.** Ensure that the **Allow all applications** option is selected. **2.** Click **Apply** and close the Management console. > **Allow only SafeNet compliant applications**: This option allows you to reset the registry key under **[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order]** to **“ProviderOrder"=" RDPNP,LanmanWorkstation,webclient "**. When you select this option, all the registry keys will be removed, except the following: • "ProviderOrder"=" RDPNP,LanmanWorkstation,webclient " • SafeNet compliant keys, such as **“PICAClientNetwork”** If you change the option from **Allow only SafeNet compliant applications** to **Allow all applications** and apply the changes, the registry state under **[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order]** will be restored to the previous state. This option increases the security via the agent, where it restricts certain third-party network providers from allowing the user to bypass the SafeNet Agent for Windows Logon authentication. However, some third-party credential provider software may conflict with the working of the SafeNet Agent for Windows Logon. So, you can restrict their access with this registry key and only allow certain supported software to work with the agent.	

Credential Tile Filter

The **Credential Tile Filter** determines which credential providers are allowed to provide credential tiles.



Credential Tile Filter

Determines which credential providers will appear during logon on windows systems that support credential providers.

Only display SafeNet credential tile

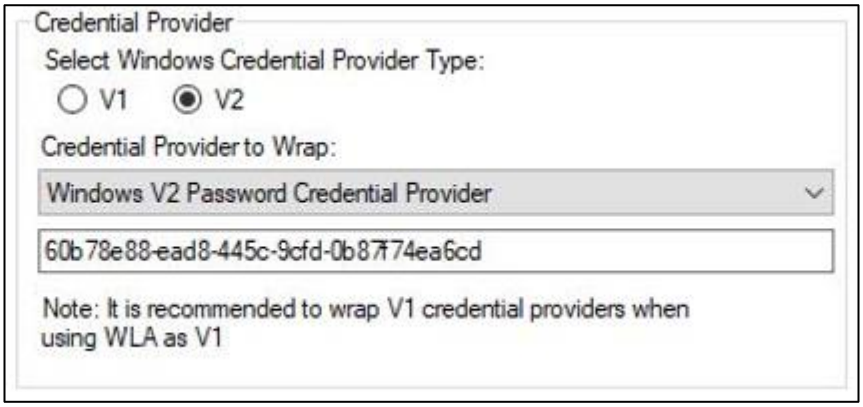
The following is a list of options (parameters) that can be selected.

Option	Description
Only display SafeNet credential tile	All credential tiles presented to the user will enforce SafeNet authentication.
Hide Microsoft credential tile	Authentication can be performed using SafeNet or third-party credentials. Only the SafeNet credential tiles and third-party credential tiles are displayed. The Microsoft credential tile is hidden from the user.
Hide SafeNet credential tile and show all available	Authentication can be performed with third-party or Microsoft credentials. Only third-party or Microsoft credential tiles are displayed. The SafeNet credential tile is not displayed.

> **NOTE:** An '*Incompatible Filter*' warning may be displayed if a conflicting credential provider filter entry is listed at the following path:
>
> `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters`
>
> In such a case, the warning will be displayed with two user-response options:
>
> 1. If you click **Yes**, the conflicting registry entry will be removed.
> 2. If you click **No**, the SafeNet Agent for Windows Logon will be disabled.

Credential Provider

The **Credential Provider** determines which version of a credential provider is to be created and dynamically wrapped.



Credential Provider

Select Windows Credential Provider Type:

○ V1 ● V2

Credential Provider to Wrap:

Windows V2 Password Credential Provider

60b78e88-ead8-445c-9cfd-0b87f74ea6cd

Note: It is recommended to wrap V1 credential providers when using WLA as V1

The following is a list of options (parameters) that can be specified.

Option	Description
Select Windows Credential Provider Type	This option allows the agent to create a specific version of a credential provider (V1 or V2). > For Windows 8 and above, both **V1** and **V2** radio buttons are enabled. > For Windows 8.1 and above, the **V2** option will be selected by default.
Credential Provider to Wrap	This option allows the agent to dynamically wrap Microsoft or other external third-party Credential Providers' GUID. > If **V1** is selected in the **Select Windows Credential Provider Type** field, this option defaults to **Windows V1 Password Credential Provider**. The text field will auto-populate the relevant GUID. > If **V2** is selected in the **Select Windows Credential Provider Type** field, this option defaults to **Windows V2 Password Credential Provider**. The text field will auto-populate the relevant GUID. > To wrap another external (third-party) credential provider, select **Other Credential Provider** dropdown option, and enter its GUID in the text field.

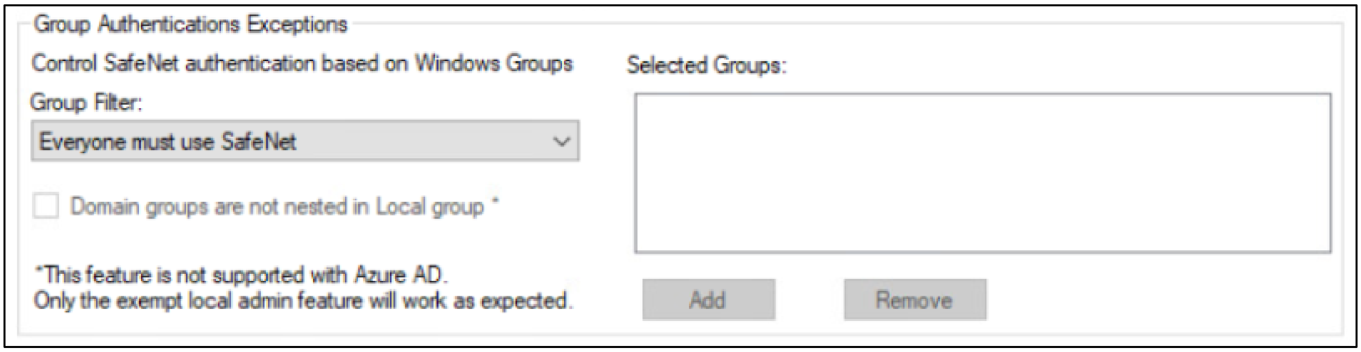
NOTE:

1. A popularly used external credential provider **ServiceNow Password Reset tool** is already configured. To wrap the **ServiceNow Password Reset tool**, select the option in the **Credential Provider to Wrap** field, and the text field will auto-populate the relevant GUID. The **ServiceNow Password Reset tool** option will only be visible if you have ServiceNow installed and running on the system.
2. Before uninstalling a third-party credential provider, unwrap it first.

Group Authentication Exceptions

The **Group Authentication Exceptions** section omits single or multiple local or domain groups from performing SafeNet authentication. Only one group filter option is valid at any given time, and it cannot overlap with another group authentication exception.

Default Setting: **Everyone must use SafeNet**



Group Authentications Exceptions

Control SafeNet authentication based on Windows Groups

Group Filter: Everyone must use SafeNet

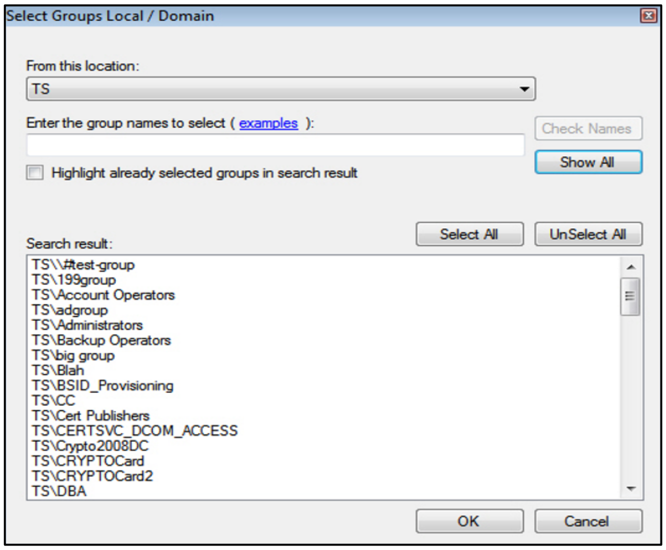
□ Domain groups are not nested in Local group *

*This feature is not supported with Azure AD.
Only the exempt local admin feature will work as expected.

Selected Groups:

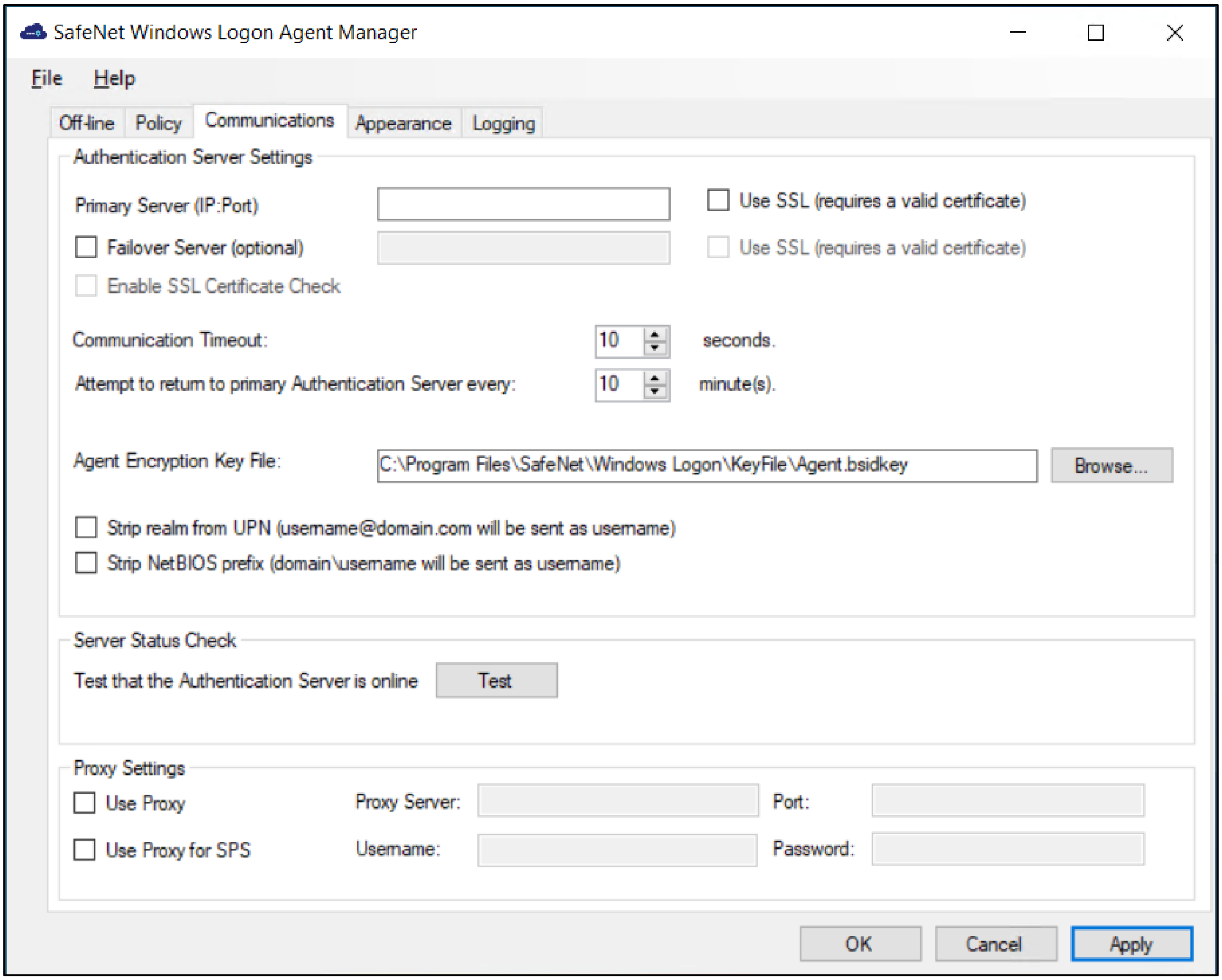
The following is a list of options (parameters) that can be specified.

Option	Description
Group Filter	Select one of the following dropdown option: > **Everyone must use SafeNet**: All users must perform SafeNet authentication. > **Only selected groups will bypass SafeNet**: All users are required to perform SafeNet authentication, except for the defined Microsoft group(s). > **Only selected groups must use SafeNet**: Users are not required to perform SafeNet authentication, except for the defined Microsoft group(s). **NOTE:** This feature will not work for pure Azure AD joined machines.
Selected Groups	Click **Add**. The **Select Groups Local / Domain** window will be displayed: > **From this location**: This option displays local or domain search results. The search results will not be visible in case of pure Azure AD joined machines. > **Enter the group names to select**: This option is used in conjunction with **Check Names** or **Show All**, and allows searches for Microsoft groups. > **Highlight already selected groups in search result**: If a Microsoft group has already been configured in the exception, it will appear as a highlighted result.

Option	Description
	 Select Groups Local / Domain From this location: TS Enter the group names to select (examples): ☐ Highlight already selected groups in search result Search result: TS\\#test-group TS\199group TS\Account Operators TS\adgroup TS\Administrators TS\Backup Operators TS\big group TS\Blah TS\BSID_Provisioning TS\CC TS\Cert Publishers TS\CERTSVC_DCOM_ACCESS TS\Crypto2008DC TS\CRYPTOCard TS\CRYPTOCard2 TS\DBA Check Names Show All Select All UnSelect All OK Cancel
Domain groups are not nested in Local group	The option, if selected, indicates that no Nested Groups (Domain groups are nested in the Local group) are present inside the **Selected Groups** field. Domain lookup is skipped in such a case, helping improve the login delay time.

Communications Tab

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



Authentication Server Settings

Primary Server (IP:Port)
□ Use SSL (requires a valid certificate)

□ Failover Server (optional)
□ Use SSL (requires a valid certificate)

□ Enable SSL Certificate Check

Communication Timeout: 10 seconds.

Attempt to return to primary Authentication Server every: 10 minute(s).

Agent Encryption Key File: C:\Program Files\SafeNet\Windows Logon\KeyFile\Agent.bsidkey

□ Strip realm from UPN (username@domain.com will be sent as username)

□ Strip NetBIOS prefix (domain\username will be sent as username)

Server Status Check

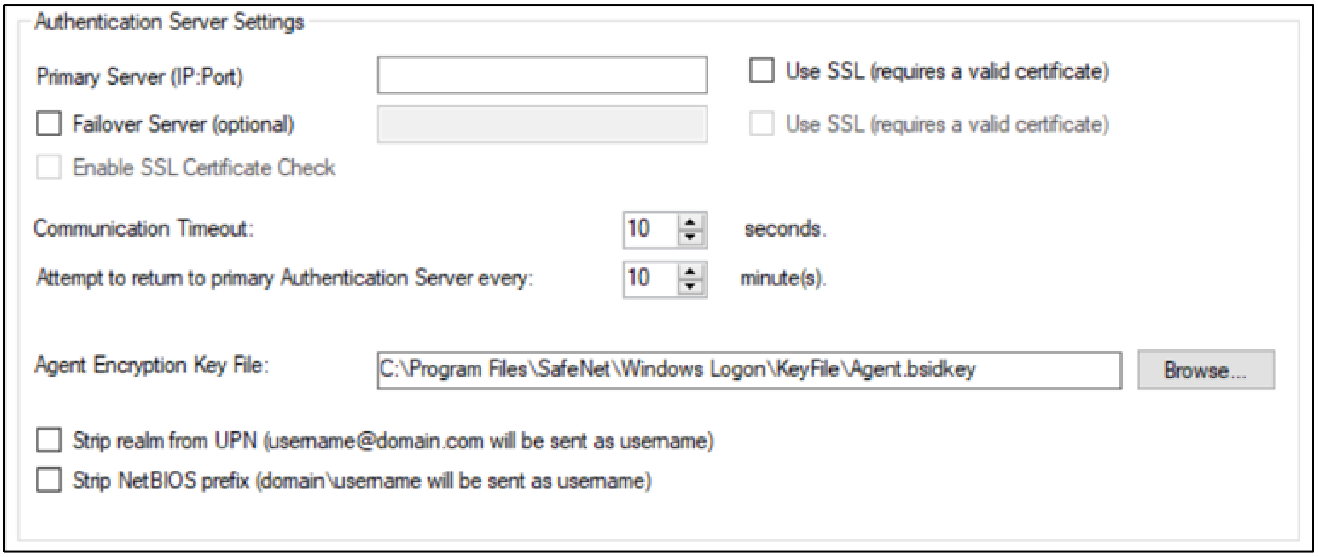
Test that the Authentication Server is online

Proxy Settings

□ Use Proxy Proxy Server: Port:

□ Use Proxy for SPS Username: Password:

Authentication Server Settings



Authentication Server Settings

Primary Server (IP:Port) □ Use SSL (requires a valid certificate)

□ Failover Server (optional) □ Use SSL (requires a valid certificate)

□ Enable SSL Certificate Check

Communication Timeout: 10 seconds.

Attempt to return to primary Authentication Server every: 10 minute(s).

Agent Encryption Key File: C:\Program Files\SafeNet\Windows Logon\KeyFile\Agent.bsidkey

□ Strip realm from UPN (username@domain.com will be sent as username)

□ Strip NetBIOS prefix (domain\username will be sent as username)

The following is a list of options (parameters) that can be specified.

Option	Description
Primary Server (IP:Port)	This setting is used to configure the IP address/hostname of the primary SafeNet server. Default Port: **80** Alternatively, **Use SSL** check box option can also be selected. Default TCP Port for SSL Requests: **443** **NOTE**: To configure the SafeNet Agent for Windows Logon with TokenValidator Proxy (TVP), click here.
Failover Server (optional)	This setting is used to configure the IP address/hostname of the failover SafeNet server. Default Port: **80** Alternatively, **Use SSL** check box option can also be selected. Default TCP Port for SSL Requests: **443** **NOTE:** In a new installation, the Failover Server option is selected by default.
Enable SSL Certificate Check	Clear to disable the SSL server certificate error check. If selected, the agent validates the certificate from the SafeNet server. The SSL certificate check is enabled by default. This supports backward compatibility for customers using the on-premises deployment of the SafeNet server.

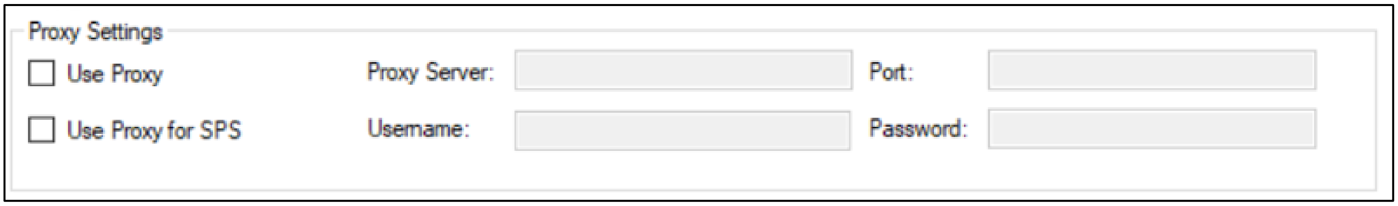
Option	Description
	NOTE: We strongly recommend to use the SSL certificate.
Communication Timeout	This setting specifies the maximum timeout value for authentication requests sent to the SafeNet server. **NOTE:** The minimum value for **the Communication Timeout** field is **1** second. Do not set a value below the minimum prescribed limit in the Registry. The default value of the field is **10** seconds. We highly recommend using the default value.
Attempt to return to primary Authentication Server every	This setting specifies the primary authentication server retry interval. This setting only takes effect when the agent is using the Failover Server.
Agent Encryption Key File	This setting is used to specify the location of the agent's Key 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 Windows Logon Agent Manager > Communications > Agent Encryption Key File**.
Strip realm from UPN (username@domain.com will be sent as username)	Select if the SafeNet server username is required without the suffix **@domain**.
Strip NetBIOS prefix (domain\username will be sent as username)	Select if the SafeNet server username is required without the prefix **domain\**. **NOTE:** The realm-stripping feature applies to SafeNet server usernames only. AD usernames are not affected.

Server Status Check

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

Server Status Check
Test that the Authentication Server is online
Test

Proxy Settings



Proxy Settings

□ Use Proxy

□ Use Proxy for SPS

Proxy Server:

Port:

Username:

Password:

- **Use Proxy**: Select to connect to the the SafeNet server via proxy server.
- **Use Proxy for SPS**: Select to connect to the Service Provider Server via proxy server.
- **Proxy Server**: Enter IP address of the proxy server.
- **Port**: Enter proxy server port.

> **NOTE**: Ensure that the port is open in Windows network**.**

- **Username**: Enter proxy server user name.
- **Password**: Enter proxy server password.

Select the proxy settings, as follows:

Configuration / Proxy Setting	Without Proxy	With Proxy (all calls)	With Proxy and TVP (non-push calls go to TVP, push calls go to proxy)	With Proxy for the SafeNet server (or TVP behind Proxy) and Proxy for SPS
Use Proxy	Not selected	Selected	Not selected	Selected
Use Proxy for SPS	Not selected	Not selected	Selected	Selected

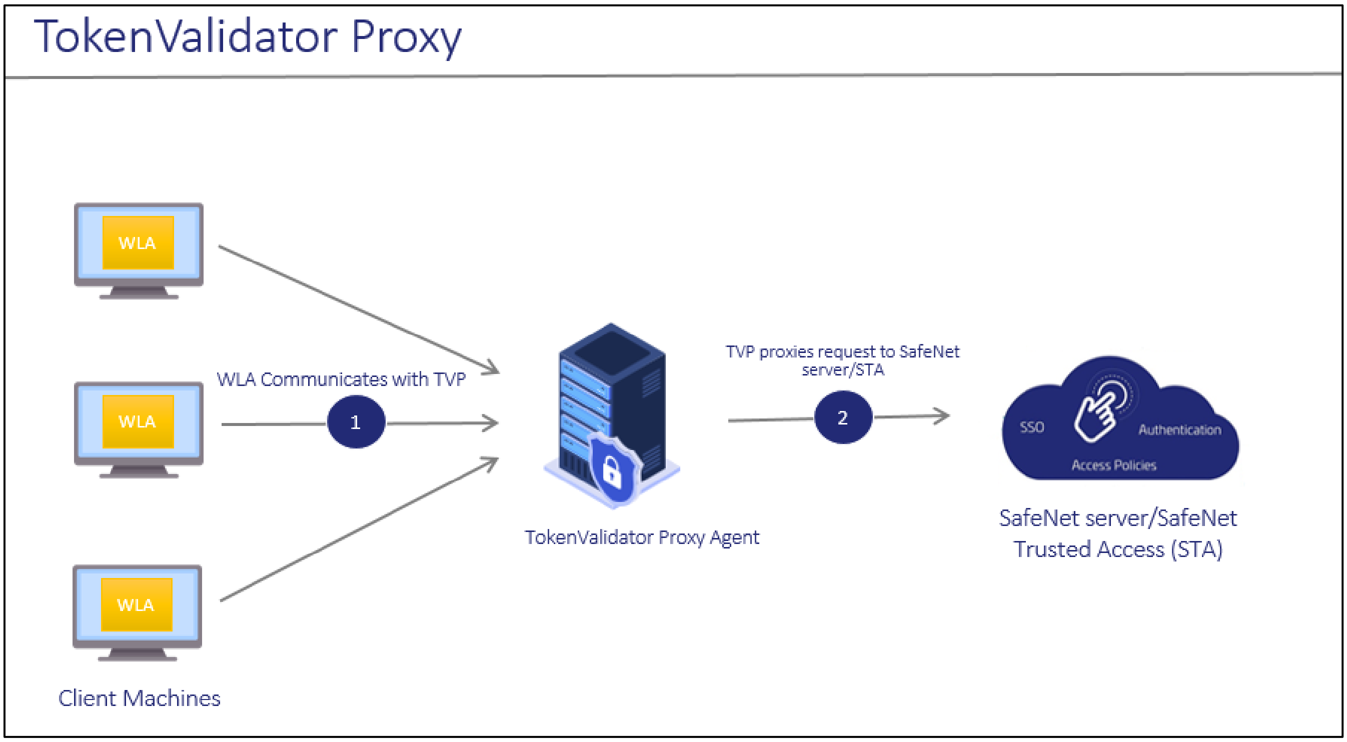
> **NOTE:** The **Proxy Password** should always be set using the Configuration Management tool, ensuring that it is stored encrypted. The key ***ProxyPassword*** should never be set instead using the Registry/ADMX file.

Configuring TokenValidator Proxy (TVP)

The function of the SafeNet Agent for TokenValidator Proxy (TVP) is to implement proxy authentication requests from other agents to the SafeNet server.

When working with SafeNet Agent for Windows Logon, without SafeNet Agent for TVP, you will be required to add an **Auth Node** for each workstation to the SafeNet server and have each workstation communicate directly with the SafeNet server.

When the SafeNet Agent for Windows Logon is configured with TVP, each Windows Logon agent can be pointed at the TVP Agent, and only the TVP IP address needs to be added as an Auth Node to the SafeNet server.

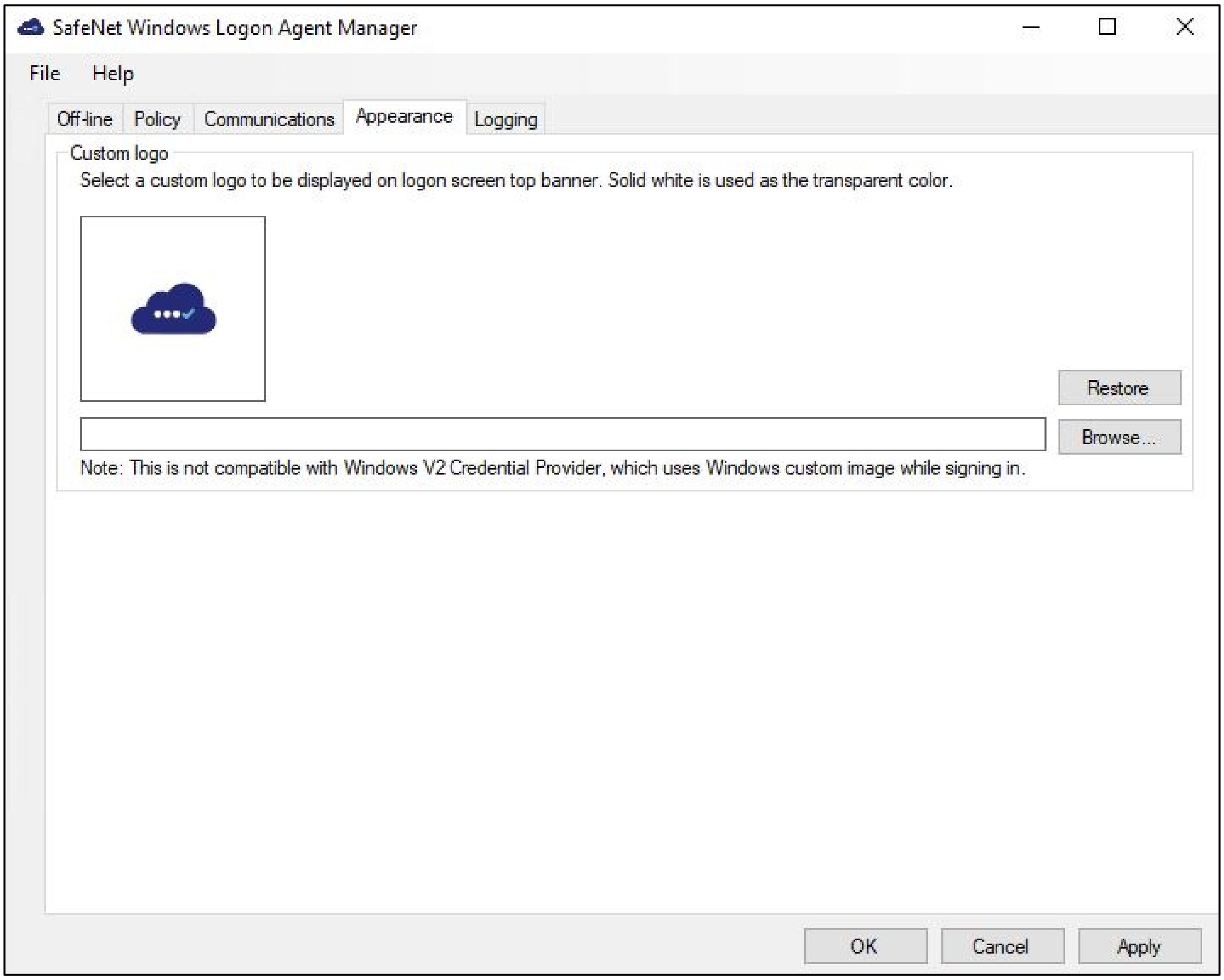

TokenValidator Proxy
WLA
WLA
WLA
Client Machines
WLA Communicates with TVP
1
TokenValidator Proxy Agent
TVP proxies request to SafeNet server/STA
2
SSO
Authentication
Access Policies
SafeNet server/SafeNet Trusted Access (STA)

To configure TVP with the SafeNet Agent for Windows Logon, perform the following steps:

1. Configure TVP IP address as the Primary Server or the Failover Server in the Windows Logon Management console.
2. Configure the SafeNet server IP or FQDN in TVP. For more information, see *SafeNet Agent for TokenValidator Proxy: Installation and Configuration Guide*.

Appearance Tab

This tab allows to customize the logo displayed during authentication.



Select a custom logo to be displayed on logon screen top banner. Solid white is used as the transparent color.

Note: This is not compatible with Windows V2 Credential Provider, which uses Windows custom image while signing in.

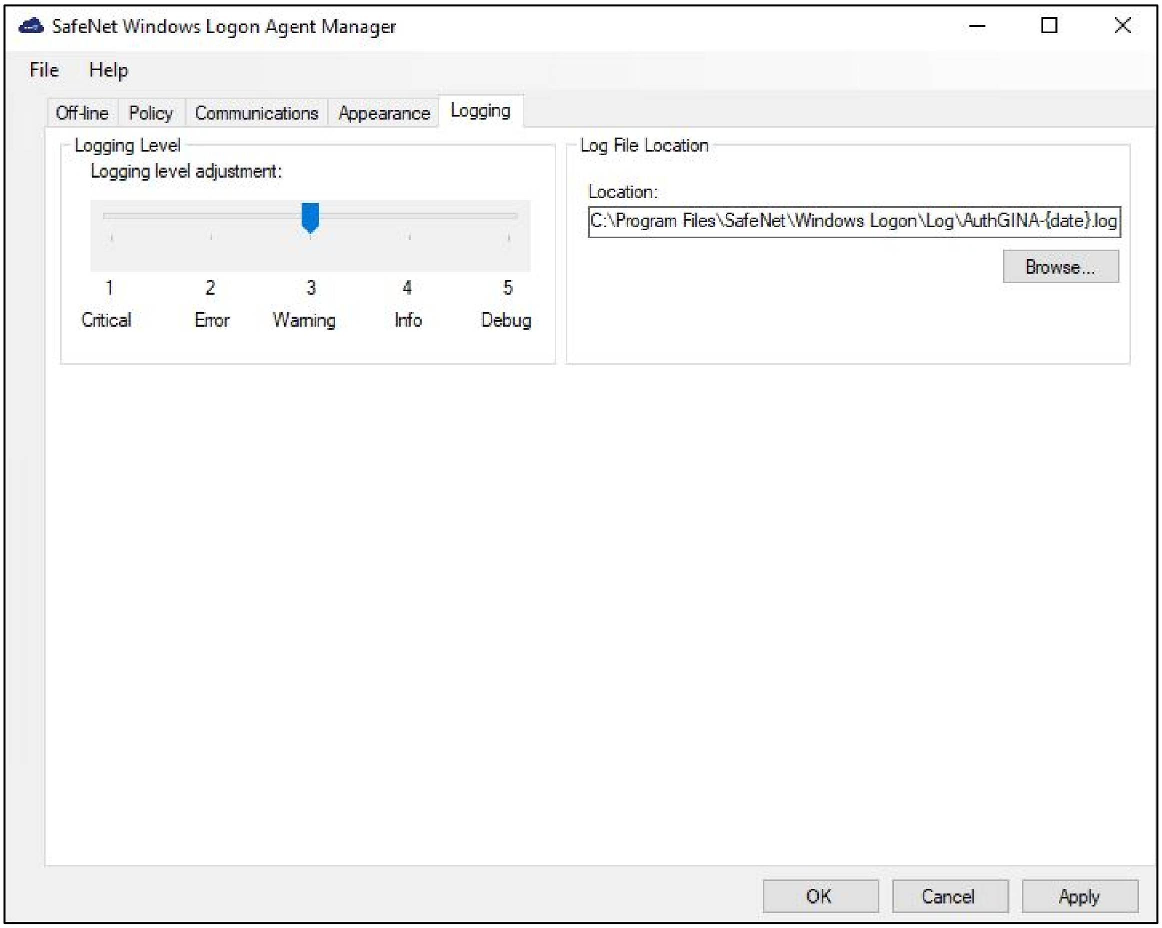
Custom logo

The logo file must be saved on the local computer. We recommend saving it in the SafeNet Agent for Windows Logon installation folder or any other protected location.

A V2 credential provider is represented by an icon displayed below the **Sign-in options** link. If SafeNet Agent for Windows Logon is set as a V2 credential provider, the **Custom logo** set on this page will be assigned to the credential provider listed under **Sign-in options**. The User Profile picture (User Tile image) will be the image set in Windows Account Picture settings.

1. The custom logo must be a bitmap of **110 x 110** pixels. Solid white will be used as the transparent color if the image is smaller than 110 x 110 pixels.
2. The **Restore** option will revert to the default SafeNet logo.

Logging Tab



Location: C:\Program Files\SafeNet\Windows Logon\Log\AuthGINA-{date}.log

Logging Level

This setting adjusts the logging level. 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**: Very severe error events that might cause the application to terminate.
- **2 – Error**: Error events that prevent normal program execution, but might still allow the application to continue running.
- **3 – Warning**: Potentially harmful error events. (**Default Option**)
- **4 – Info**: Informational error events that highlight the progress of the application.
- **5 – Debug**: Detailed tracing error events that are useful to debug an application. (**Recommended**)

Log File Location

This setting specifies the location where the log files are saved. The log files are rotated on a daily basis.

For **Windows 8 and later**, the default location is **C:\Program Files\SafeNet\Windows Logon\AuthGINA-{date}.log**

CHAPTER 4: Configuring and Installing the agent via Group Policy Object

The use of Microsoft Group Policy or Group Policy Objects (GPO) enables the SafeNet administrator to centrally manage the Windows Logon Agent (WLA) configuration for users and computers in an Active Directory environment. It allows to configure many important policy settings to provide flexibility and support extensive configuration information.

> **NOTE:** For more details about the Group Policy and Group Policy Objects, see Group Policy Overview.

Configuration of SafeNet Agent for Windows Logon via Group Policy Object (GPO)

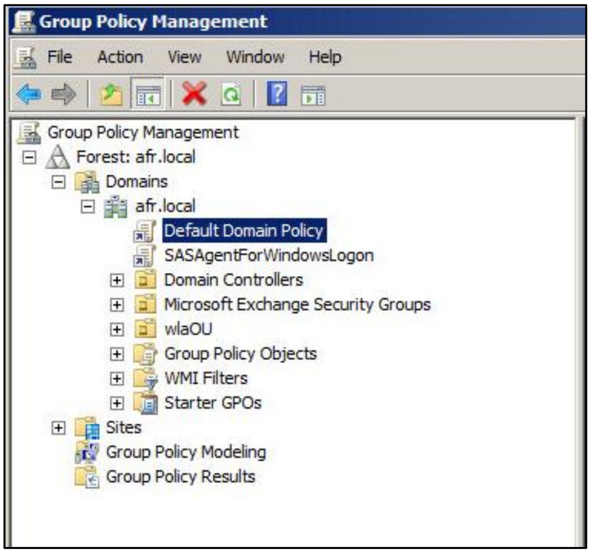
Configuring ADMX and ADML Settings

The SafeNet Agent for Windows Logon policy settings are stored in a **Windows Administrative Template (ADMX)** file. The settings can be edited using the Windows tools. It can be propagated to the entire domain, or be applied to the local computer and domain controllers only.

After the Administrative Template is added, open the template to configure the settings.

To open the SafeNet Network Logon settings, perform the following steps:

1. From the Windows taskbar, select **Start** > **All Programs** > **Accessories** > **Run**.
2. In the **Run** window, enter *gpmc.msc*, and click **OK**. The **Group Policy Management** window is displayed.



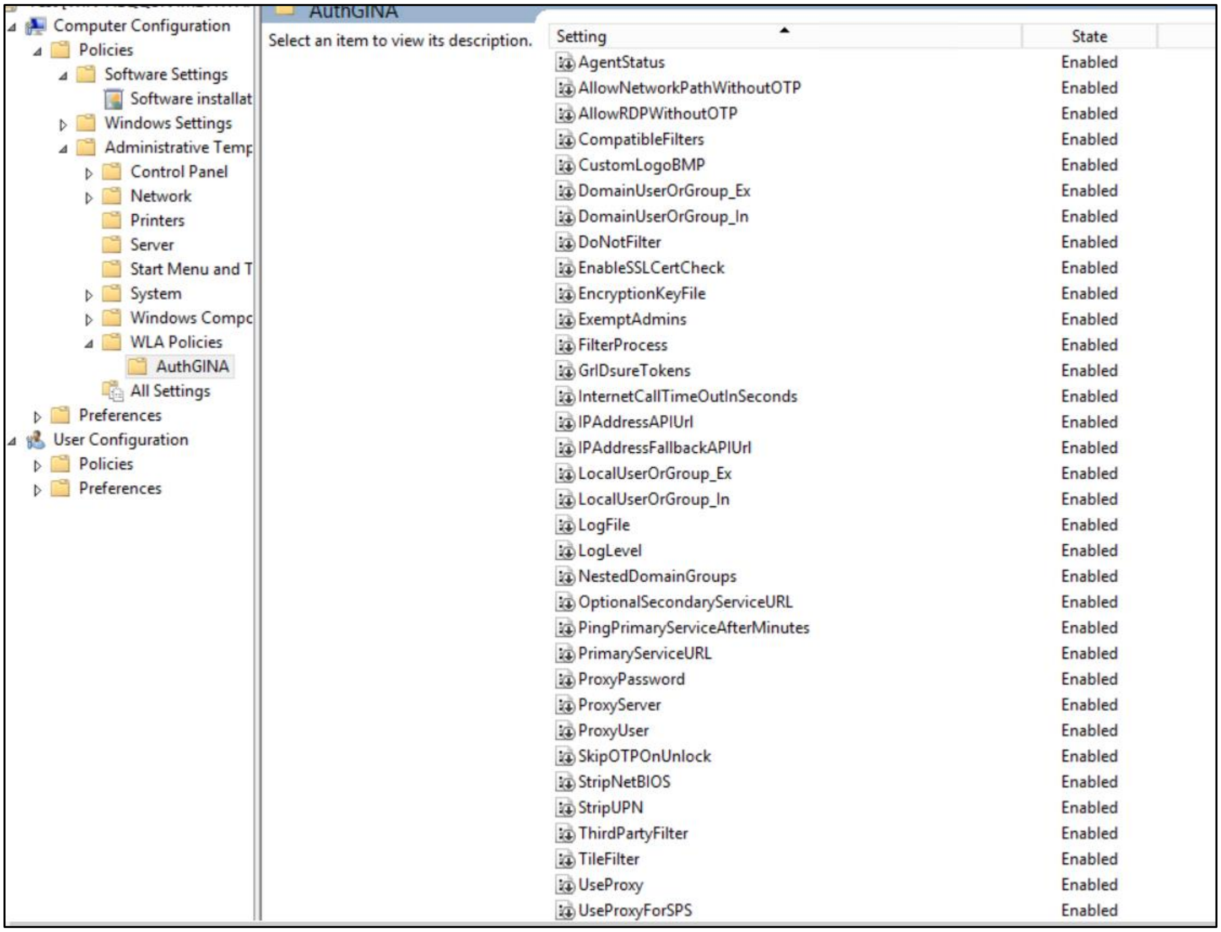
3. Perform one of the following actions:

   - To propagate the settings to all clients in the domain, right-click **Default Domain Policy** or **newly created GPO** under the domain node.

   - To apply the settings to the local machine and any other domain controllers in this domain, under the **Domain Controllers** node, right-click **Default Domain Controllers Policy**.

4. From the dropdown menu, select **Edit…**. The **Group Policy Management Editor** window is displayed.

5. In the left pane, navigate to **Computer Configuration** > **Policies** > **Administrative Templates** > **WLA Policies** > **AuthGINA**. The SafeNet Agent for Windows Logon settings are displayed in the right pane.



Setting	State
AgentStatus	Enabled
AllowNetworkPathWithoutOTP	Enabled
AllowRDPWithoutOTP	Enabled
CompatibleFilters	Enabled
CustomLogoBMP	Enabled
DomainUserOrGroup_Ex	Enabled
DomainUserOrGroup_In	Enabled
DoNotFilter	Enabled
EnableSSLCertCheck	Enabled
EncryptionKeyFile	Enabled
ExemptAdmins	Enabled
FilterProcess	Enabled
GrIDsureTokens	Enabled
InternetCallTimeOutInSeconds	Enabled
IPAddressAPIUrl	Enabled
IPAddressFallbackAPIUrl	Enabled
LocalUserOrGroup_Ex	Enabled
LocalUserOrGroup_In	Enabled
LogFile	Enabled
LogLevel	Enabled
NestedDomainGroups	Enabled
OptionalSecondaryServiceURL	Enabled
PingPrimaryServiceAfterMinutes	Enabled
PrimaryServiceURL	Enabled
ProxyPassword	Enabled
ProxyServer	Enabled
ProxyUser	Enabled
SkipOTPOnUnlock	Enabled
StripNetBIOS	Enabled
StripUPN	Enabled
ThirdPartyFilter	Enabled
TileFilter	Enabled
UseProxy	Enabled
UseProxyForSPS	Enabled

6. Enable all the setting, if not already enabled, with *default value* or *user-defined value*.

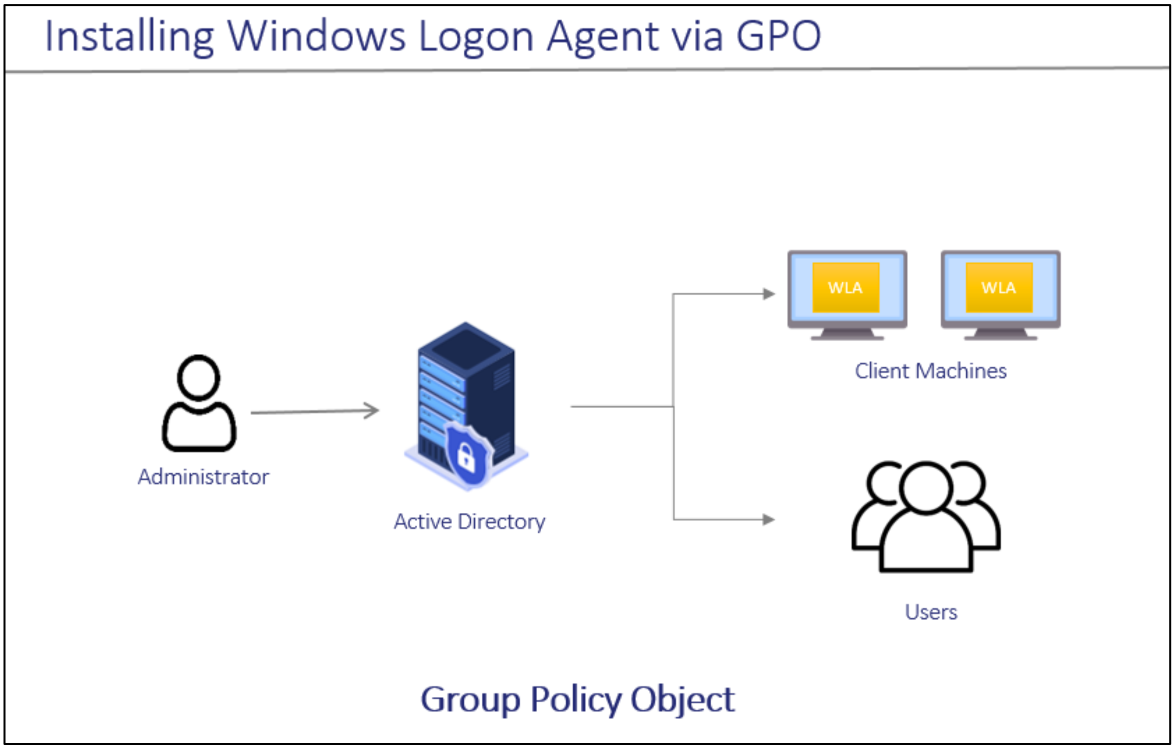
   NOTE: For **LocalUserOrGroup_Ex** and **LocalUserOrGroup_In** settings, in the **Value** field, you can enter **%COMPUTERNAME%\groupname.** In this case, when the GPO settings are pushed to the client machines, the variable (**%COMPUTERNAME%**) will be automatically set to the computer name of the respective client machine**.**

ADMX and ADML Settings

Click here to see the description of the GPO Settings available with the SafeNet Agent for Windows Logon.

Installation of SafeNet Agent for Windows Logon via Group Policy Object (GPO)

The use of Microsoft Group Policy or Group Policy Object (GPO) enables the SafeNet administrator to centrally manage the Windows Logon Agent (WLA) configuration for users and computers in an Active Directory environment.



To install the SafeNet Agent for Windows Logon via GPO, perform the following steps:

1. Creating a Distribution Point
2. Creating a Group Policy Object
3. Adding ADMX and ADML File to Group Policy Object Editor
4. Deploying the MSI

Creating a Distribution Point

To deploy an MSI through GPO, perform the following steps to create a distribution point on the **Publishing Server**:

1. Log in to the server as an administrator.
2. Create a shared network folder.

> **NOTE:** The shared network folder contains the MSI package and Agent file.

3. Set permissions on this folder to allow access to the distribution package.
4. Copy the SafeNet Agent for Windows Logon MSI file (*SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64.msi*) and Agent file in the previously created shared network folder.

Creating a Group Policy Object

An MSI package is deployed/distributed through GPO. To create an object, perform the following steps:

1. From the Windows taskbar, select **Start > All Programs > Accessories> Run**.
2. In the **Run** window enter *gpmc.msc* and click **OK**. The **Group Policy Management** window is displayed.
3. Expand **Forest** (your forest) > **Domains** (your domain).
4. Right-click the **Group Policy Objects** and select **New**.
5. Enter a name for your policy and leave **Source Starter GPO** as *none*.
6. Right-click the **domain name** and select **Link an Existing GPO…**.
7. In **Select GPO** pop-up window, select *newly created GPO* and click **OK**.
8. Click the newly created GPO. In the right pane, right-click the linked domain name and select **enforce**.

Performing the above steps will create and enforce a new GPO, and will link it with the domain.

Adding ADMX and ADML File to Group Policy Object Editor

To add the SafeNet Agent for Windows Logon ADMX and ADML file to the GPO Editor, perform the following steps:

1. Copy the Local Group Policy definition (*C:\Windows\PolicyDefinitions*) to Domain Group Policy (*C:\Windows\SYSVOL\sysvol\<domain_name>\Policies*).
2. Copy the *ADMX* file (*SafeNetAgentForWindowsLogon.admx*) included in the agent software package to the following location:

   `C:\Windows\SYSVOL\sysvol\<domain_name>\Policies\PolicyDefinitions`

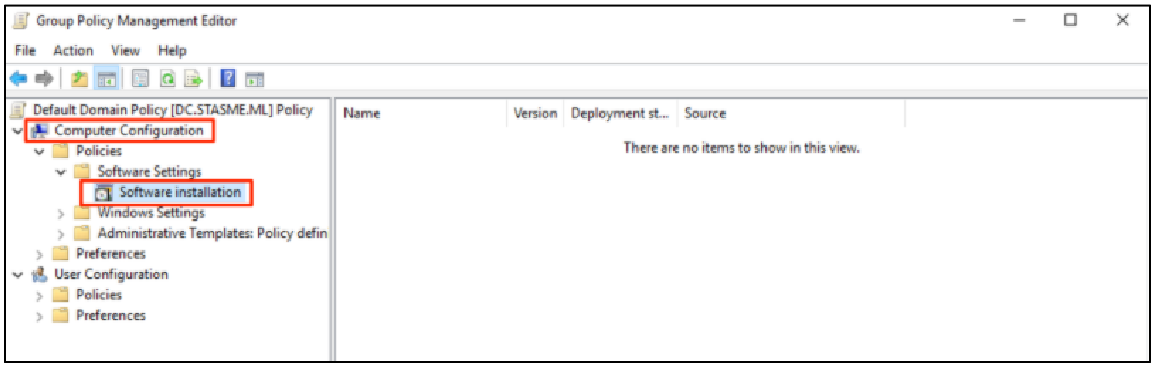
3. Copy the appropriate *ADML* language file (*SafeNetAgentForWindowsLogon.adml*) to a language folder under the `\PolicyDefinitions` folders.

   For example, in Windows Server 2016 R2, the English language file provided should be written to: `C:\Windows\SYSVOL\sysvol\<domain_name>\Policies\PolicyDefinitions\en-US`

Deploying the MSI

To deploy the WLA MSI to the client machines, perform the following steps:

1. Right-click the **GPO** and select **Edit…**.
2. In the Group Policy Management Editor, navigate to **Computer Configuration > Policies > Software Settings > Software Installation**.



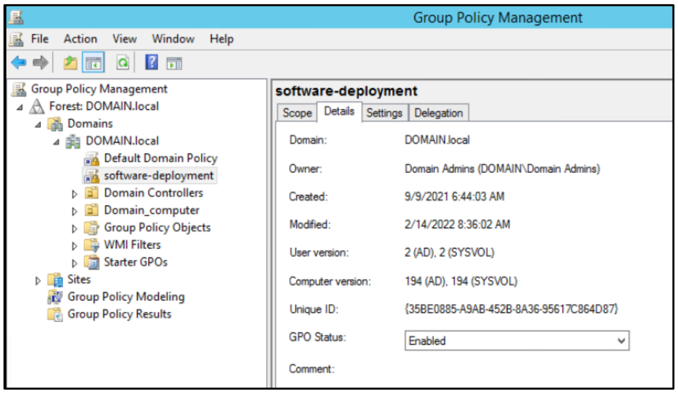
There are no items to show in this view.

3. Right-click the **Software Installation**, and select **New > Package….**
4. Select the SafeNet Agent for Windows Logon MSI file (*SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64.msi*) from the previously created shared folder.
5. Select the **deployment Method – Assigned** and click **OK**.
6. Double-click **MSI** and under **Deployment** tab, click **Advance**. Select **Ignore language** checkbox.
7. On **Security** tab, select the client machine, give the required permission and click **OK**.

Now, the GPO will have the MSI Installation package. Next time, if the GPO is updated on the client computer, it will silently install the MSI. To apply the changes instantly, use the following command:
gpupdate/force

> **NOTE:** Restart might be required after executing the above command.

Under **Details** tab, **Enabled** status displays for the created GPO.



software-deployment

Domain: DOMAIN.local
Owner: Domain Admins (DOMAIN\Domain Admins)
Created: 9/9/2021 6:44:03 AM
Modified: 2/14/2022 8:36:02 AM
User version: 2 (AD), 2 (SYSVOL)
Computer version: 194 (AD), 194 (SYSVOL)
Unique ID: {35BE0885-A9AB-452B-8A36-95617C864D87}
GPO Status: Enabled
Comment:

Using Registry to Hide Configuration Management Features

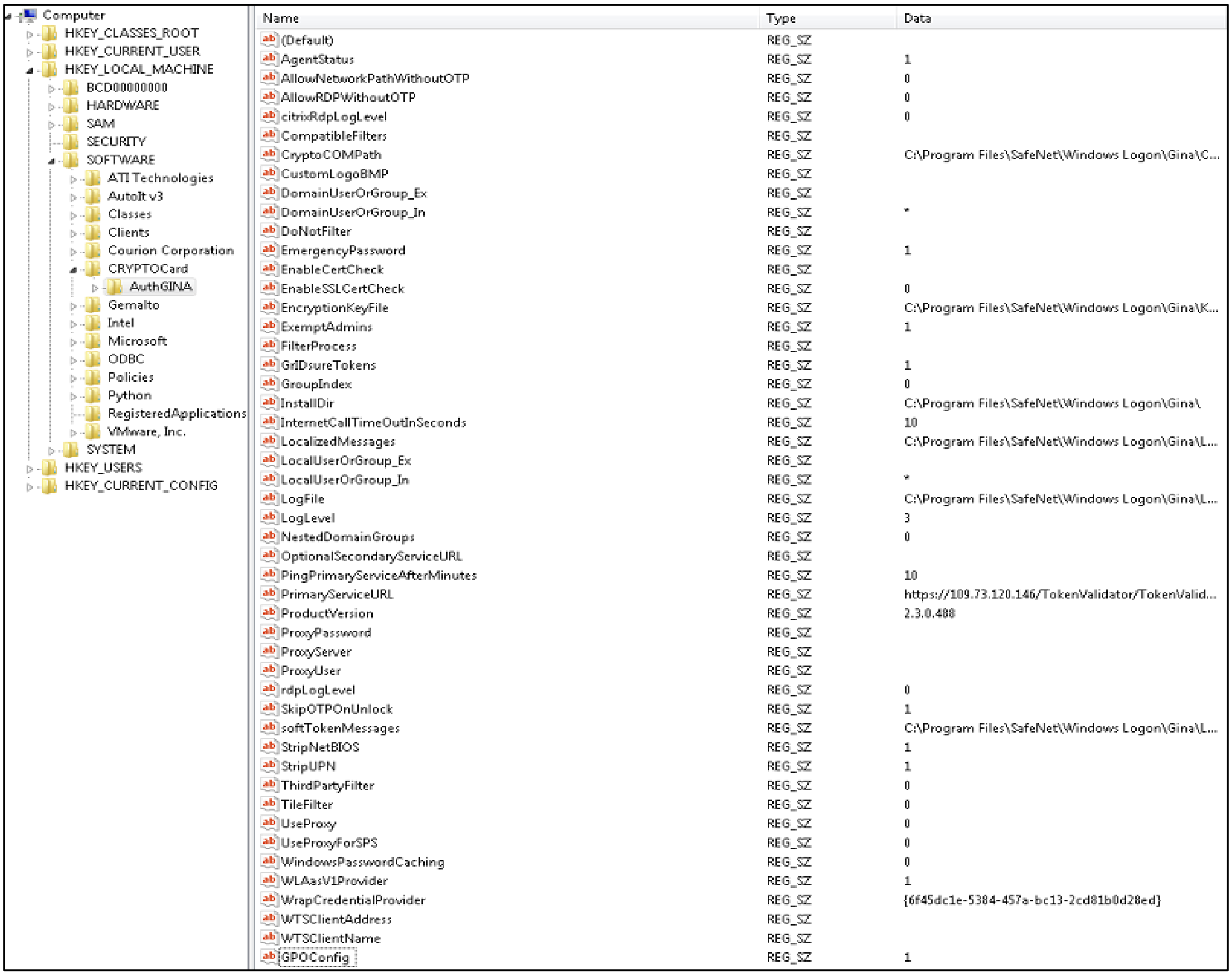
If working with GPO, you can create a registry key to limit user access to Configuration Management features by displaying only the **Off-line** tab.

To display only the Off-line tab in the SafeNet Windows Logon Agent Manager window, perform the following steps:

1. Add **GPOConfig** to the registry manually at the following location:

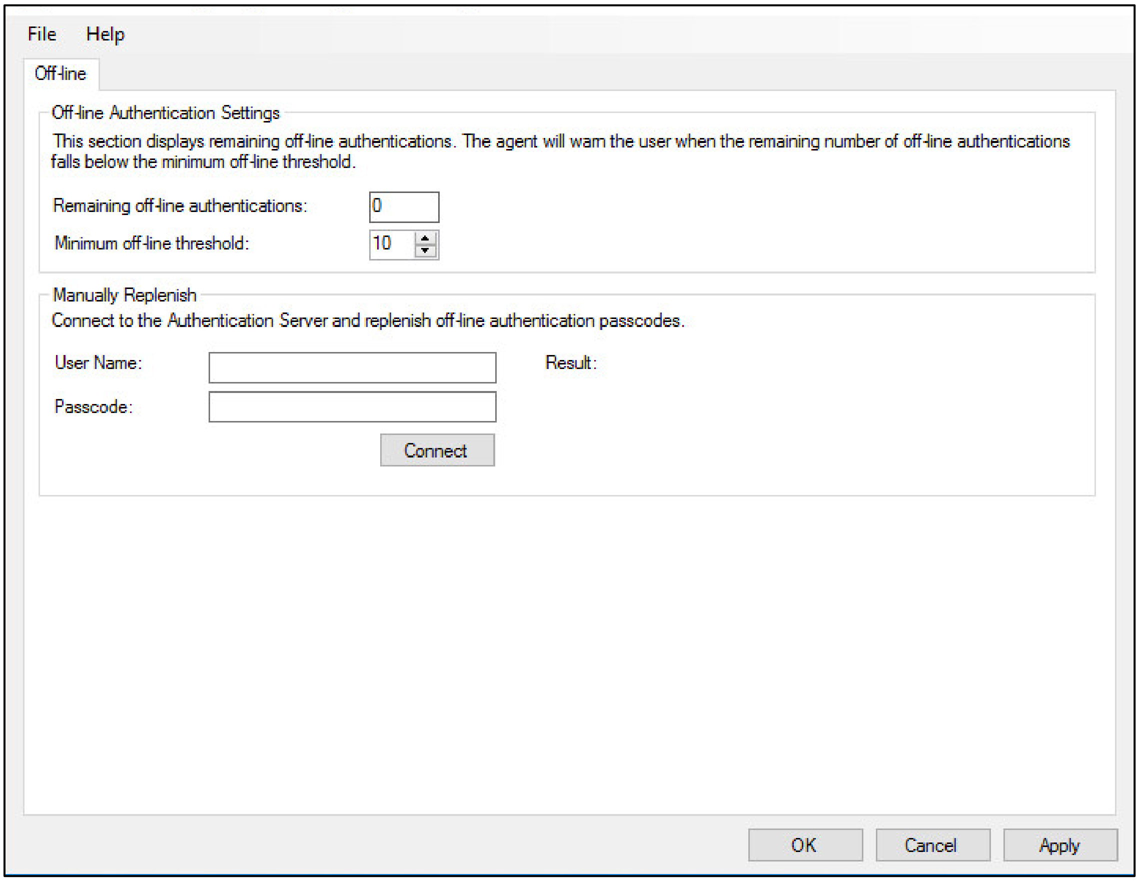
```
HKEY_LOCAL_ MACHINE\SOFTWARE\Cryptocard\AuthGINA
```

2. Set the value of **GPOConfig** to 1.



Name	Type	Data
(Default)	REG_SZ	
AgentStatus	REG_SZ	1
AllowNetworkPathWithoutOTP	REG_SZ	0
AllowRDPWithoutOTP	REG_SZ	0
citrixRdpLogLevel	REG_SZ	0
CompatibleFilters	REG_SZ	
CryptoCOMPath	REG_SZ	C:\Program Files\SafeNet\Windows Logon\Gina\C...
CustomLogoBMP	REG_SZ	
DomainUserOrGroup_Ex	REG_SZ	
DomainUserOrGroup_In	REG_SZ	*
DoNotFilter	REG_SZ	
EmergencyPassword	REG_SZ	1
EnableCertCheck	REG_SZ	
EnableSSLCertCheck	REG_SZ	0
EncryptionKeyFile	REG_SZ	C:\Program Files\SafeNet\Windows Logon\Gina\K...
ExemptAdmins	REG_SZ	1
FilterProcess	REG_SZ	
GrIDsureTokens	REG_SZ	1
GroupIndex	REG_SZ	0
InstallDir	REG_SZ	C:\Program Files\SafeNet\Windows Logon\Gina\
InternetCallTimeOutInSeconds	REG_SZ	10
LocalizedMessages	REG_SZ	C:\Program Files\SafeNet\Windows Logon\Gina\L...
LocalUserOrGroup_Ex	REG_SZ	
LocalUserOrGroup_In	REG_SZ	*
LogFile	REG_SZ	C:\Program Files\SafeNet\Windows Logon\Gina\L...
LogLevel	REG_SZ	3
NestedDomainGroups	REG_SZ	0
OptionalSecondaryServiceURL	REG_SZ	
PingPrimaryServiceAfterMinutes	REG_SZ	10
PrimaryServiceURL	REG_SZ	https://109.73.120.146/TokenValidator/TokenValid...
ProductVersion	REG_SZ	2.3.0.488
ProxyPassword	REG_SZ	
ProxyServer	REG_SZ	
ProxyUser	REG_SZ	
rdpLogLevel	REG_SZ	0
SkipOTPOnUnlock	REG_SZ	1
softTokenMessages	REG_SZ	C:\Program Files\SafeNet\Windows Logon\Gina\L...
StripNetBIOS	REG_SZ	1
StripUPN	REG_SZ	1
ThirdPartyFilter	REG_SZ	0
TileFilter	REG_SZ	0
UseProxy	REG_SZ	0
UseProxyForSPS	REG_SZ	0
WindowsPasswordCaching	REG_SZ	0
WLAasV1Provider	REG_SZ	1
WrapCredentialProvider	REG_SZ	{6f45dc1e-5384-457a-bc13-2cd81b0d28ed}
WTSClientAddress	REG_SZ	
WTSClientName	REG_SZ	
GPOConfig	REG_SZ	1

The Off-line tab, displayed after setting the **GPOConfig** registry key to 1, includes the **Off-line Authentication Settings** and **Manual Replenish** sections. However, it does not include the **Authentication Test** section that would normally be displayed if the user’s access to the SafeNet Windows Logon Agent Manager window had not been restricted.



Off-line Authentication Settings

This section displays remaining off-line authentications. The agent will warn the user when the remaining number of off-line authentications falls below the minimum off-line threshold.

Remaining off-line authentications: 0

Minimum off-line threshold: 10

Manually Replenish

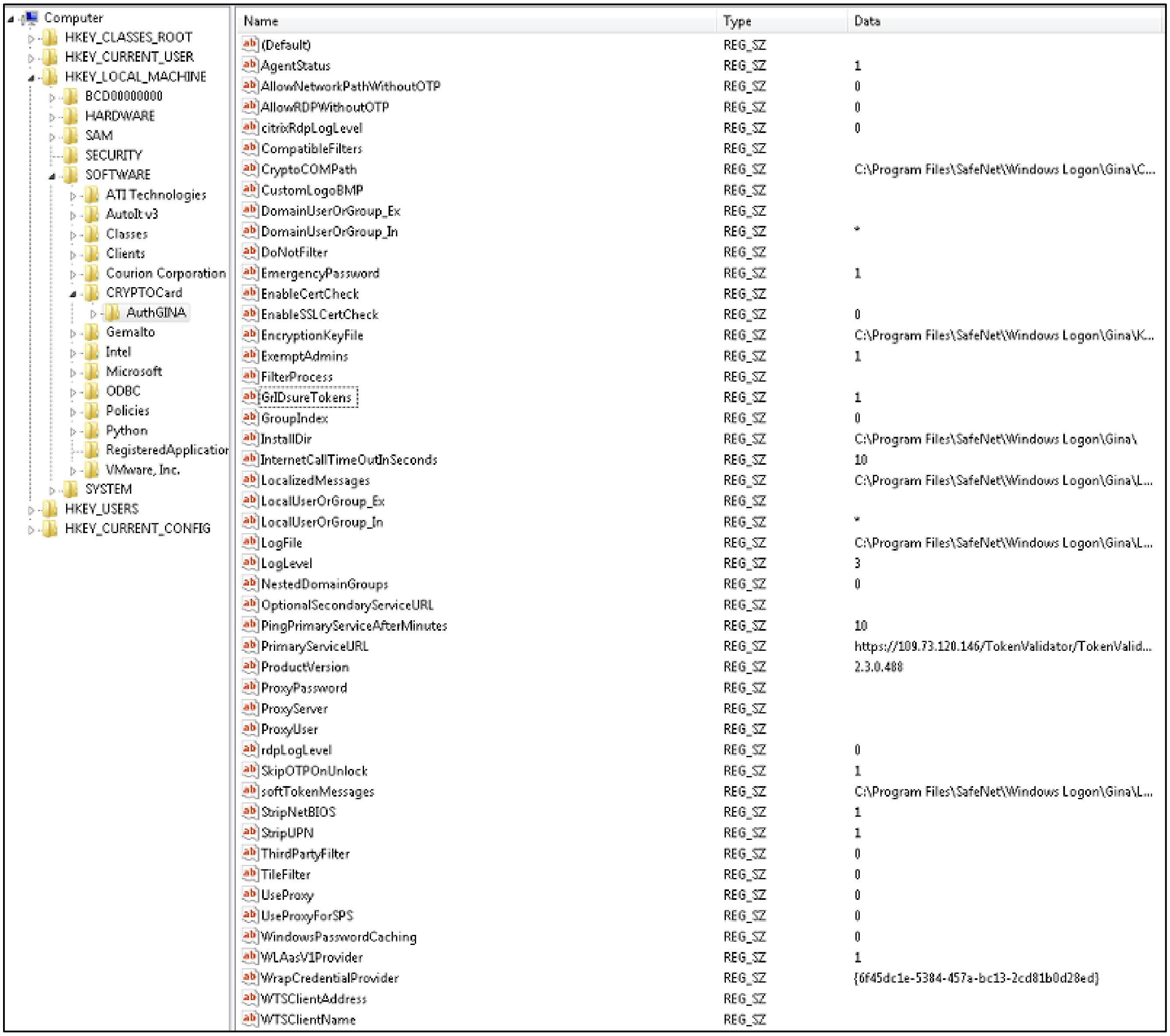
Connect to the Authentication Server and replenish off-line authentication passcodes.

User Name:

Passcode:

Result:

Registry Settings



Name	Type	Data
(Default)	REG_SZ	
AgentStatus	REG_SZ	1
AllowNetworkPathWithoutOTP	REG_SZ	0
AllowRDPWithoutOTP	REG_SZ	0
citrixRdpLogLevel	REG_SZ	0
CompatibleFilters	REG_SZ	
CryptoCOMPath	REG_SZ	C:\Program Files\SafeNet\Windows Logon\Gina\C...
CustomLogoBMP	REG_SZ	
DomainUserOrGroup_Ex	REG_SZ	
DomainUserOrGroup_In	REG_SZ	*
DoNotFilter	REG_SZ	
EmergencyPassword	REG_SZ	1
EnableCertCheck	REG_SZ	
EnableSSLCertCheck	REG_SZ	0
EncryptionKeyFile	REG_SZ	C:\Program Files\SafeNet\Windows Logon\Gina\K...
ExemptAdmins	REG_SZ	1
FilterProcess	REG_SZ	
GrIDsureTokens	REG_SZ	1
GroupIndex	REG_SZ	0
InstallDir	REG_SZ	C:\Program Files\SafeNet\Windows Logon\Gina\
InternetCallTimeOutInSeconds	REG_SZ	10
LocalizedMessages	REG_SZ	C:\Program Files\SafeNet\Windows Logon\Gina\L...
LocalUserOrGroup_Ex	REG_SZ	
LocalUserOrGroup_In	REG_SZ	*
LogFile	REG_SZ	C:\Program Files\SafeNet\Windows Logon\Gina\L...
LogLevel	REG_SZ	3
NestedDomainGroups	REG_SZ	0
OptionalSecondaryServiceURL	REG_SZ	
PingPrimaryServiceAfterMinutes	REG_SZ	10
PrimaryServiceURL	REG_SZ	https://109.73.120.146/TokenValidator/TokenValid...
ProductVersion	REG_SZ	2.3.0.488
ProxyPassword	REG_SZ	
ProxyServer	REG_SZ	
ProxyUser	REG_SZ	
rdpLogLevel	REG_SZ	0
SkipOTPOnUnlock	REG_SZ	1
softTokenMessages	REG_SZ	C:\Program Files\SafeNet\Windows Logon\Gina\L...
StripNetBIOS	REG_SZ	1
StripUPN	REG_SZ	1
ThirdPartyFilter	REG_SZ	0
TileFilter	REG_SZ	0
UseProxy	REG_SZ	0
UseProxyForSPS	REG_SZ	0
WindowsPasswordCaching	REG_SZ	0
WLAasV1Provider	REG_SZ	1
WrapCredentialProvider	REG_SZ	{6f45dc1e-5384-457a-bc13-2cd81b0d28ed}
WTSClientAddress	REG_SZ	
WTSClientName	REG_SZ	

Setting	Description and Usage
UseProxy	This policy setting configures the use of a proxy server for connecting with the token validation service. For example, SafeNet server or a Token Validation Proxy. The setting corresponds to the UI option (Communications tab) called **Use Proxy**. [1] Enables the use of a proxy server [0] Proxy server is not used (default value)

Setting	Description and Usage
	Note: If you enable this setting, you must also enable 'Proxy Server'.
DoNotFilter	This policy setting allows a view where other third-party credential providers can also be displayed. By default, WLA filters out (do not display) any other credential provider. The correct syntax is: **{GUID},{GUID},{GUID}**
Strip NETBIOS prefix (domain\username will be sent as username)	This policy setting determines if a NETBIOS name (DOMAIN\USERNAME) is sent to the authentication server as-is, or if the portion prefixing the username is removed (stripped). The setting corresponds to the UI option (Communications tab) called **Strip NETBIOS prefix** (domain\username will be sent as username) [1] Strips the DOMAIN\ portion from the username when authenticating with SafeNet server [0] WLA will not sanitize the username (default value) **Note:** This is useful when users log in with NETBIOS sometimes and SafeNet server username at other times and you need to sanitize what is being sent from different protected resources so that SafeNet server can still authenticate the user(s) consistently.
WLAasV1Provider	WLAasV1Provider is used to select the Credential Provider Type and specify whether Credential Provider Type is set to V1 or not. • Windows Credential Provider Type selected as V2: WLAasV1Provider=0 • Windows Credential Provider Type selected as V1: WLAasV1Provider=1 In Windows 8, 10, 2012, 2016, 2019, it is recommended to keep the value 0 that is, using V2 credential provider.
EnableSSLCertCheck	This policy setting enable or disable the validation of the SafeNet server or Token Validation Proxy (if used) server certificate. The setting corresponds with the UI option called **Enable SSL Certificate Check**. [1] WLA will validate the server certificate (default value) [0] Does not validate server certificate **Note:** Disabling the certificate check can be useful in troubleshooting or when testing using a self-signed untrusted certificate.
ProxyServer	This policy setting configures the proxy server IP address or FQDN and its port number for use when connecting with the token validation service (For example, SafeNet server or a Token Validation Proxy). The values set corresponds to UI options (Communications tab) called 'Proxy Server:' and 'Port:' The correct syntax is: '1.2.3.4:567' or 'host.domain.name:port'. **Note:** Must be used with setting 'Use Proxy' and/or 'Use Proxy for SPS'.

Setting	Description and Usage
Exempt Local/Domain Administrator strong authentication	This policy setting configures the exclusion of local and domain administrators from using strong authentication (OTP). When set, administrators can authenticate with fixed passwords instead of dynamic passwords. When disabled [0] all users must use OTP for Windows Logon (assuming no other exemptions are configured). The setting corresponds to UI option: 'Exempt Local/Domain Administrator strong authentication' (Policy tab). [1] Local & Domain Administrators are exempt from strong authentication (default value) [0] All users musts use strong authentication
ProxyPassword	This policy setting configures the proxy server password as used when authenticating to the defined proxy server (if required), in order to connect with the token validation service (For example, SafeNet server or a Token Validator Proxy host). The setting corresponds to the UI option called: 'Password'. Note that setting 'Password' also assumes setting ‘Proxy Server’ and ‘Username’, and may also require setting 'Use Proxy for SPS' (if applicable). **WARNING:** Windows Logon Agent (WLA) uses the SafeNet server key file to encrypt and decrypt the proxy password during operation and thus assumes the password is propagated from the GPO in encrypted form (!). To set the password with the GPO it is therefore best to retrieve it from the registry of a client already installed.
LocalUserOrGroup_Ex	Local Groups which are excluded from SafeNet Authentication. **NOTE:** When any group is added to this setting through GPO, **DomainUserOrGroup_In** needs to be set to “*”.
PrimaryServerURL (IP:Port)	This policy setting configures the primary SafeNet server authentication server (or the Token Validation Proxy). Syntax is either protocol followed by IP address and port (if non-standard) or protocol followed by FQDN and port (if non-standard), that is, 'http://1.2.3.4:8080' or 'https://server.domain.com'. The setting corresponds to UI options (Communications tab): 'Primary Server (IP:Port)' and when the default value is used (or when a custom value is used with https): 'Use SSL'.
WindowsPasswordCaching	If enabled, WLA will cache the Microsoft password on first successful user authentication until password expiration or change. The setting corresponds to the UI option called: ‘Enable Microsoft Password Caching’. [1] Users are prompted for OTP only [0] Users are prompted for OTP, then domain password (default) **Note:** • Enabling this setting improves usability (user convenience) of the solution. • This configuration is not applicable for domain administrators as WLA does not store password of domain administrators.
EncryptionKeyFile	This policy setting sets the key file location. Refer to default value below for example syntax. The setting corresponds to the UI option called: 'Agent Encryption Key File:' (Communications tab).

Setting	Description and Usage
	Default value: [C:\Program Files\SafeNet\Windows Logon\KeyFile\Agent.bsidkey] **Note:** A customer may use the default (bundled with the agent) key file or set their own virtual server specific key file.
GrIDsureTokens	This policy setting configures the appearance and use of GrIDsure authentication in WLA during Windows Logon. The setting corresponds to the UI option (Policy tab) called: 'Enable GrIDsure tokens'. [1] Enables GrIDsure authentication in WLA (default value) [0] Disables the use of GrIDsure authentication **Note:** Only leave this setting enabled if you need to support GrIDsure.
WrapCredentialProvider	This entry specifies the GUID of the credential provider the agent is wrapping to provide two-factor authentication. This setting corresponds to the UI option under Credential Provider (Policy Tab). It could be set to either Windows v1 Password Credential Provider- {6f45dc1e-5384-457a-bc13-2cd81b0d28ed} or Windows v2 Password Credential Provider- {60b78e88-ead8-445c-9cfd-0b87f74ea6cd **Note:** It can be set to wrap some other 3rd party credential provider by selecting "Other credential Provider" and specifying its GUID. The correct syntax is **{GUID}**.
LogLevel	This policy setting configures client side log level. The setting corresponds to the UI option called: 'Logging Level' (Logging tab). [1] Critical [2] Error [3] Warning (default value) [4] Info [5] Debug
PingPrimaryServiceAfterMinutes	This policy setting configures the time, in minutes, after which the WLA client will attempt to return to its primary authentication server following a failover to a defined secondary server. The setting corresponds to the UI option called: 'Attempt to return to primary Authentication Server every [ ] minute(s)' (Communications tab). The default value for this setting is 10 minutes. **Note:** This setting is only applicable if a failover server has been defined using setting 'Failover Server (optional)'.
AllowRDPWithoutOTP	This policy setting configures if WLA should be used for outgoing RDP (remote desktop). The setting corresponds to the UI option called: 'Allow outgoing RDP connection without OTP'. [1] WLA is not enforced for outgoing RDP (default value)

Setting	Description and Usage
	[0] Outgoing RDP is subject to the use of OTP
DomainUserOrGroup_In	This policy setting configures what users are subject to using strong authentication (OTP). When a group is added to DomainUserOrGroup_In (Only selected group must use SafeNet), then the LocalUserOrGroup_Ex is set to "*". If pushing through GPO, the user needs to set the registry entry to "*". [ ] Not configured [DomainName.com\Group Name] Only the provided group must use strong authentication [*] All users must use strong authentication (sets UI option: 'Everyone must use SafeNet') **Note:** If you define a group or multiple groups in this setting you must also set DomainUserOrGroup_Ex with a value of '*', meaning all but the defined groups of users are excluded from strong authentication.
AllowNetworkPathWithoutOTP	This policy setting configures if WLA should be used for accessing network resources over Windows Explorer. The setting corresponds to the UI option called: 'Allow windows explorer without OTP' (Policy tab). [1] WLA is not enforced for outgoing Windows Explorer [0] Outgoing Windows Explorer is subject to OTP (default value)
TileFilter	This policy setting configures the appearance of credential provider tiles during Windows Logon. [0] All credential tiles presented to the user will enforce SafeNet authentication. Corresponds to the UI setting (Policy tab) called: 'Only display SafeNet credential tile' This is the default value. [1] Authentication can be performed using SafeNet or third-party credentials, but the Microsoft credential tile is hidden. Corresponds to the UI setting (Policy tab) called: 'Hide Microsoft credential tile' [2] Authentication can be performed with third-party or Microsoft credentials and ONLY third-party or Microsoft credential tiles are displayed. Corresponds to the UI setting (Policy tab) called: 'Hide SafeNet credential tile and show all available'.
LocalUserOrGroup_In	This policy setting configures what local users are subject to using strong authentication (OTP). [ ] Not configured [ComputerName\Group Name] Only the provided group must use strong authentication **Note:** If you define a group or multiple groups in this setting, you must also set DomainUserOrGroup_Ex with a value of '*', meaning all but the defined local groups of users are excluded from strong authentication.

Setting	Description and Usage
ThirdPartyFilter	This can be set to **0** for “Allow all applications” or **1** for “Allow SafeNet compliant applications”. Some third-party credential provider software may conflict with the working of the SafeNet Agent for Windows Logon. So, you can restrict their access with this registry key and only allow certain supported software to work with the agent.
InternetCallTimeOutInSeconds	This policy setting specifies the maximum timeout value for authentication requests sent to SafeNet server. The setting corresponds to UI option: 'Communication Timeout: [ ] seconds' (Communications tab). The default value is **120 seconds**.
UseProxyForSPS	Select to connect to the Service Provider Server via proxy server. This setting is used to connect to the Service Provider Server via proxy server.
NestedDomainGroups	This policy setting can be enabled to improve logon performance if (and only if) domain groups are not nested inside local groups. The setting corresponds to UI option called: ‘Domain groups are not nested in Local group’ (Policy tab). [1] Improves WLA client performance when domain groups are not nested in local groups [0] Used when domain groups are not nested in local groups (default value)
OptionalSecondaryServiceURL	This policy setting configures the secondary (failover) SafeNet server authentication server (or the Token Validation Proxy). Syntax is either protocol followed by IP address and port (if non-standard) or protocol followed by FQDN and port (if non-standard), that is, 'http://1.2.3.4:8080' or 'https://server.domain.com'. The setting corresponds to UI options (Communications tab): 'Failover Server (optional)' and when the default value is used (or when a custom value is used with https): 'Use SSL (requires a valid certificate)'.
LogFile	This policy settings configures the client log file path and its naming. The setting corresponds to the UI option called: 'Log File Location' (Logging tab). Refer to default value below for example syntax. **Default value:** [C:\Program Files\SafeNet\Windows Logon\Log\AuthGINA-{date}.log]
DomainUserOrGroup_Ex	When any group is added to this setting, then the DomainUserOrGroup_In entry remains empty. You need to set LocalUserOrGroup_In to “*”.
ProxyUser	This policy setting configures the proxy server username as used when authenticating to the defined proxy server (if required), in order to connect with the token validation service (For example, SafeNet server or a Token Validation Proxy). The setting corresponds to the UI option called: 'Username'. Correct syntax is: 'username'. **Note:** Setting 'Username' also assumes setting ‘Proxy Server’ and ‘Password’, and may also require setting 'Use Proxy for SPS' (if applicable).
Strip realm from UPN (username@domain.com will be sent as username)	This policy setting determines if a UPN (username@domain.com) is sent to the authentication server as-is, or if the portion following the username is removed (stripped).

Setting	Description and Usage
	The setting corresponds to the UI option (Communications tab) called: ‘Strip realm from UPN (username@domain.com will be sent as username)’ [1] Strips the @domain.com portion from the UPN when authenticating with SafeNet server [0] WLA will not sanitize the username (default value) **Note:** This is useful when the user logs in with UPN sometimes and SafeNet server username at other times and you need to sanitize what is being sent from different protected resources so that SafeNet server can still authenticate the user(s) consistently.
CustomLogoBMP	This policy settings allows you to set a custom image in the logon screen for compatible credential providers (customization is not compatible with the Windows V2 provider). The setting corresponds to the UI option: 'Custom Logo' (Appearance tab). Example syntax is: 'C:\Program Files\SafeNet\Windows Logon\customLogo.bmp'. **Note:** The custom logo must be a bitmap (.bmp) of 110 x 110 pixels and must be available locally on the client.
AgentStatus	This policy setting configures the Windows Logon Agent (WLA) as enabled or disabled. The setting corresponds to the UI option called: ‘Enable Agent’ (Policy tab). When enabled, WLA will be displayed at logon. [1] WLA will be enabled and displayed at logon (default value) [0] WLA will be disabled (remains installed and configured but is not used)
FilterProcess	This policy setting can be configured to exclude applications from SafeNet server authentication. For example, Outlook may prompt for authentication using OTP when WLA is installed with default options. To exclude Outlook from using OTP, simply add the executable name (outlook.exe) to the FilterProcess list of values. To exclude multiple applications for using OTP, use ‘,’ for separation. For example, “outlook.exe,consent.exe”. **Note:** The FilterProcess setting does not have an equivalent UI setting in WinLogonManager, and can only be set directly in client registry or using Group Policy.
EmergencyPassword	This option turns the emergency password feature *on* or *off*. The setting corresponds to the UI option called: ‘Enable emergency passwords’ (Policy tab). This feature is an authentication method that allows an administrator to authenticate to a user’s computer as the user without entering a SafeNet OTP. This applies when the emergency password is enabled and the Windows system is unable to communicate with the SafeNet server at the time of authentication. Default Setting: **Enabled**
SkipOTPOnUnlock	This option allows the administrators to enable/disable the SafeNet 2FA for last logged on user on system unlock. Selecting the option ensures that the SafeNet Agent for Windows Logon does not prompt for an OTP, reducing friction every time a user unlocks a machine. The functionality extends to sleep and hibernate modes, which means that if the **Skip OTP on Unlock** check box is selected, and the system enters sleep or

Setting	Description and Usage
	hibernate mode, the SafeNet Agent for Windows Logon does not prompt for an OTP, and instead logs in successfully using only AD credentials. Default Setting: **Disabled**

DoNotFilter

A new registry entry is created (as part of the installation) to ensure that external (third-party) credential providers work with enhanced flexibility (and functionality), while the SafeNet Agent for Windows Logon is enabled and working.

The entry must be created manually in the registry at the following location:
`HKEY_LOCAL_ MACHINE\SOFTWARE\Cryptocard\AuthGINA`

Registry Entry	Functionality	Format / Accepted Registry Values
DoNotFilter	Allows a view where other third-party credential providers can also be displayed. By default, filters out (do not display) any other credential provider.	**{GUID},{GUID},{GUID}**

CompatibleFilters

A new registry entry is created to prevent **SafeNet Windows Logon Agent Manager** from displaying an *Incompatible Filter* message. *CompatibleFilters* setting can only be added if a third-party credential provider is compatible with the agent and can be wrapped successfully.

The entry must be created manually in the Registry at the following location:

`HKEY_LOCAL_ MACHINE\SOFTWARE\Cryptocard\AuthGINA`

Registry Entry	Functionality	Format / Accepted Registry Values
CompatibleFilters	Allows to exclude Credential Filters from being filtered. For example, if *SpecOps* credential provider is installed on a client machine along with the agent, then the **SafeNet Windows Logon Agent Manager** may display *Incompatible Filter* message. To exclude *SpecOps* Credential Filter, add its GUID to the *CompatibleFilters* list. To add multiple filters, use comma (**,**) for separation.	**{GUID},{GUID},{GUID}**

NOTE: The *CompatibleFilters* setting does not have an equivalent UI setting, and thus can only be set directly in the client Registry or using the Group Policy.

FilterProcess

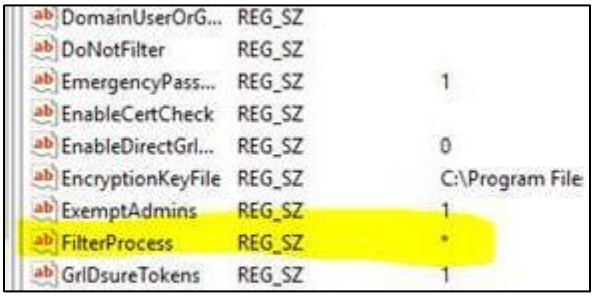
A new registry entry is created to prevent applications from applying the SafeNet authentication. *FilterProcess* setting can only be added when the agent is installed with default options.

Registry values must be entered manually at the following location:
`HKEY_LOCAL_ MACHINE\SOFTWARE\Cryptocard\AuthGINA`

Registry Entry	Functionality	Format / Accepted Registry Values
FilterProcess	Allows to exclude applications from SafeNet authentication. For example, the *Outlook* application may prompt for authentication using OTP. To exclude *Outlook* from using OTP to authenticate, add its executable (*outlook.exe*) to the *FilterProcess* list. To exclude multiple applications, use comma (**,**) for separation.	**{GUID},{GUID},{GUID}**

Bypassing SafeNet Authentication for All Applications

If an administrator does not explicitly want to add all the applications that must be excluded from the SafeNet OTP authentication, the administrator can instead add a wildcard, an asterisk (*****) in the FilterProcess Registry flag to exclude all applications. Adding an asterisk (*****) bypasses OTP authentication for all the applications except Windows logon events, ensuring that the user will be prompted to enter an OTP only on the Windows logon screens.



DomainUserOrG...	REG_SZ	
DoNotFilter	REG_SZ	
EmergencyPass...	REG_SZ	1
EnableCertCheck	REG_SZ	
EnableDirectGrI...	REG_SZ	0
EncryptionKeyFile	REG_SZ	C:\Program File
ExemptAdmins	REG_SZ	1
FilterProcess	REG_SZ	*
GrIDsureTokens	REG_SZ	1

NOTE: The *FilterProcess* setting does not have an equivalent UI setting, and thus can only be set directly in the client Registry or using the Group Policy.

CHAPTER 5: Installing, Configuring and Upgrading Settings via Intune

This section describes the steps to deploy and configure the SafeNet Agent for Windows Logon via Intune.

Prerequisites

- The user must have an Azure account with an active Microsoft Intune license.
- Users and groups must be created and assigned to the Microsoft Intune license.
- MDM service must be enabled and assigned to the Groups. For detailed information, refer to the **Setup enrollment for Windows devices** in the Microsoft documentation.

Installing SafeNet Agent for Windows Logon via Intune involves the following steps:

- Creating an IntuneWin package
- Deploying the IntuneWin package
- Deploying PowerShell Script to configure the Settings
- Upgrading SafeNet Agent for Windows Logon

Creating an IntuneWin package

Deploying SafeNet Agent for Windows Logon via Intune (as a Win32 Application) requires a **.IntuneWin** package for WLA Installer and Settings Configuration.

1. Copy the **Intune-Deployment** folder from the package to a different location, for example, C:\.
2. Open the **Intune-Deployment** folder and create the following sub-folders:
   - Installer
   - InstallerOutput
   - ConfigurationOutput

Creating an IntuneWin package of WLA Installer

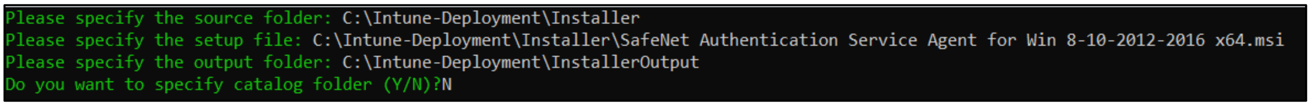
1. Copy the **.msi** file (SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64.msi) and paste it in the **Intune-Deployment\Installer** folder.
2. Download the Microsoft Win32 Content Prep Tool as a .zip package. Under **Intune-Deployment** folder, unzip the package and then launch **IntuneWinAppUtil.exe**. The tool converts application installation files into the *.intunewin* format.
3. In the command prompt, enter the following details:

i. **source folder** - Enter the path of the folder where the **.msi** file (SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64.msi) is present. For example, C:\Intune-Deployment\Installer.

ii. **setup file** - Enter the path of **.msi** file. For example, C:\Intune-Deployment\Installer\SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64.msi.

iii. **output folder** - Enter the path of the **InstallerOutput** folder to save the .IntuneWin package. For example, C:\Intune-Deployment\InstallerOutput.

iv. **catalog folder** - Enter **N**.



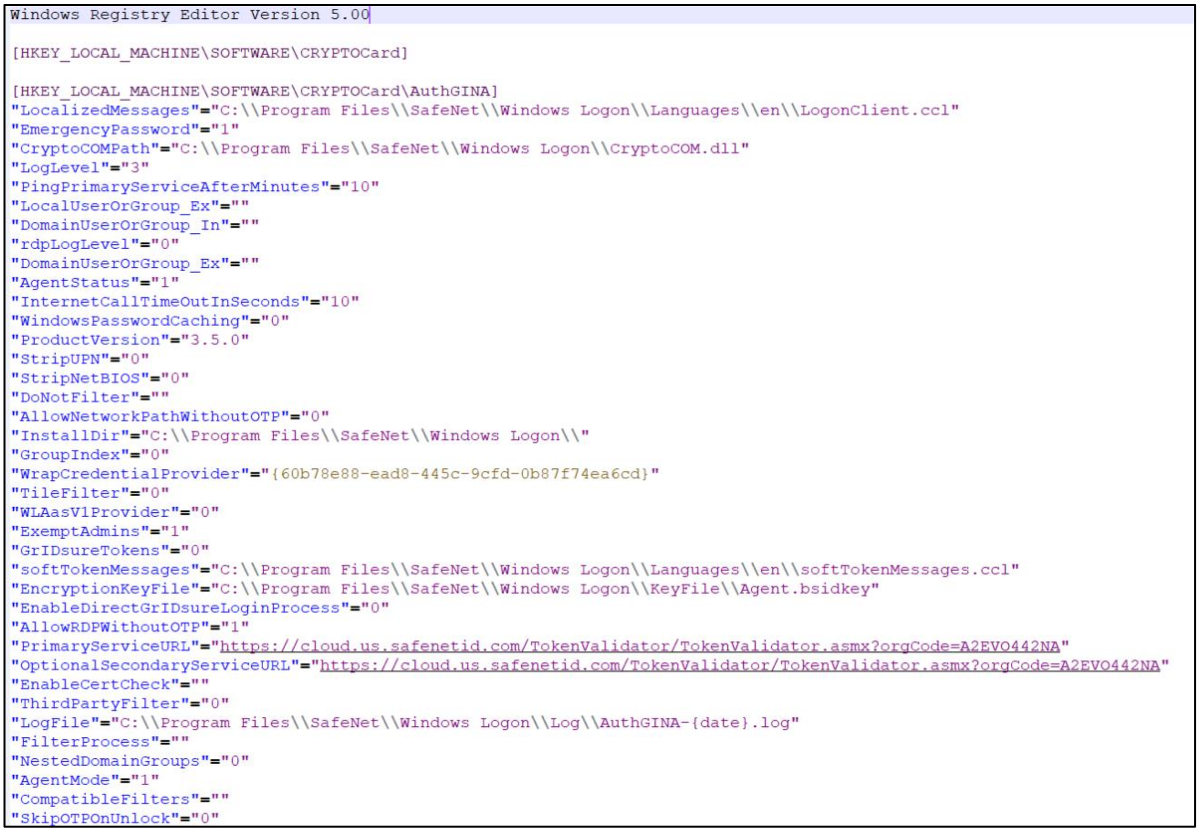
```
Please specify the source folder: C:\Intune-Deployment\Installer
Please specify the setup file: C:\Intune-Deployment\Installer\SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64.msi
Please specify the output folder: C:\Intune-Deployment\InstallerOutput
Do you want to specify catalog folder (Y/N)?N
```

Now, a .IntuneWin package (SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64.intunewin) is ready for deployment under **Intune-Deployment\InstallerOutput** as a Win32 application in Intune.

Creating an IntuneWin package for configuring the Settings

1. In the **Intune-Deployment** folder, navigate to **Configuration** and open **DefaultConfiguration.reg** in any text editor.
2. Update the required parameters and remove the parameters that are not needed. For more details about the Registry Settings, click here.

> **NOTE:** It is recommended to update the **PrimaryServiceURL** and **OptionalSecondaryServiceURL**.

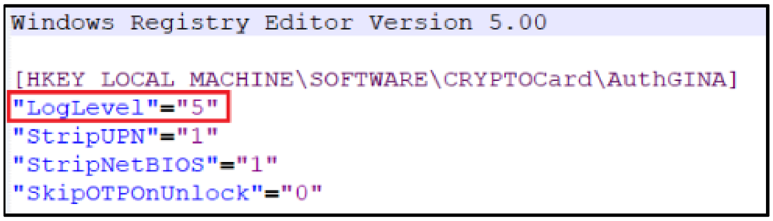


```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\CRYPTOCard]

[HKEY_LOCAL_MACHINE\SOFTWARE\CRYPTOCard\AuthGINA]
"LocalizedMessages"="C:\\Program Files\\SafeNet\\Windows Logon\\Languages\\en\\LogonClient.ccl"
"EmergencyPassword"="1"
"CryptoCOMPath"="C:\\Program Files\\SafeNet\\Windows Logon\\CryptoCOM.dll"
"LogLevel"="3"
"PingPrimaryServiceAfterMinutes"="10"
"LocalUserOrGroup_Ex"=""
"DomainUserOrGroup_In"=""
"rdpLogLevel"="0"
"DomainUserOrGroup_Ex"=""
"AgentStatus"="1"
"InternetCallTimeOutInSeconds"="10"
"WindowsPasswordCaching"="0"
"ProductVersion"="3.5.0"
"StripUPN"="0"
"StripNetBIOS"="0"
"DoNotFilter"=""
"AllowNetworkPathWithoutOTP"="0"
"InstallDir"="C:\\Program Files\\SafeNet\\Windows Logon\\"
"GroupIndex"="0"
"WrapCredentialProvider"="{60b78e88-ead8-445c-9cfd-0b87f74ea6cd}"
"TileFilter"="0"
"WLAasV1Provider"="0"
"ExemptAdmins"="1"
"GrIDsureTokens"="0"
"softTokenMessages"="C:\\Program Files\\SafeNet\\Windows Logon\\Languages\\en\\softTokenMessages.ccl"
"EncryptionKeyFile"="C:\\Program Files\\SafeNet\\Windows Logon\\KeyFile\\Agent.bsidkey"
"EnableDirectGrIDsureLoginProcess"="0"
"AllowRDPWithoutOTP"="1"
"PrimaryServiceURL"="https://cloud.us.safenetid.com/TokenValidator/TokenValidator.asmx?orgCode=A2EVO442NA"
"OptionalSecondaryServiceURL"="https://cloud.us.safenetid.com/TokenValidator/TokenValidator.asmx?orgCode=A2EVO442NA"
"EnableCertCheck"=""
"ThirdPartyFilter"="0"
"LogFile"="C:\\Program Files\\SafeNet\\Windows Logon\\Log\\AuthGINA-{date}.log"
"FilterProcess"=""
"NestedDomainGroups"="0"
"AgentMode"="1"
"CompatibleFilters"=""
"SkipOTPOnUnlock"="0"
```

For example, if you want to change the LogLevel to 5, you can edit the registry file (DefaultConfiguration.reg) using any text editor.



```
Windows Registry Editor Version 5.00

[HKEY LOCAL MACHINE\SOFTWARE\CRYPTOCard\AuthGINA]
"LogLevel"="5"
"StripUPN"="1"
"StripNetBIOS"="1"
"SkipOTPOnUnlock"="0"
```

3. Download the Microsoft Win32 Content Prep Tool as a .zip package. Under **Intune-Deployment** folder, unzip the package and then launch **IntuneWinAppUtil.exe**. The tool converts application installation files into the *.intunewin* format.

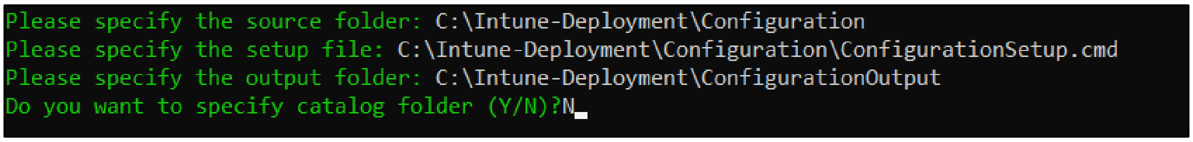
4. In the command prompt, enter the following details:

   i. **source folder** - Enter the path of the folder where the .reg and setup file is present. For example, C:\Intune-Deployment\Configuration.

   ii. **setup file** - Enter the path of **ConfigurationSetup.cmd**. For example, C:\Intune-Deployment\Configuration\ConfigurationSetup.cmd.

   iii. **output folder** - Enter the path of the **ConfigurationOutput** folder to save the .IntuneWin package. For example, C:\Intune-Deployment\ConfigurationOutput.

   iv. **catalog folder** - Enter **N**.



```
Please specify the source folder: C:\Intune-Deployment\Configuration
Please specify the setup file: C:\Intune-Deployment\Configuration\ConfigurationSetup.cmd
Please specify the output folder: C:\Intune-Deployment\ConfigurationOutput
Do you want to specify catalog folder (Y/N)?N
```

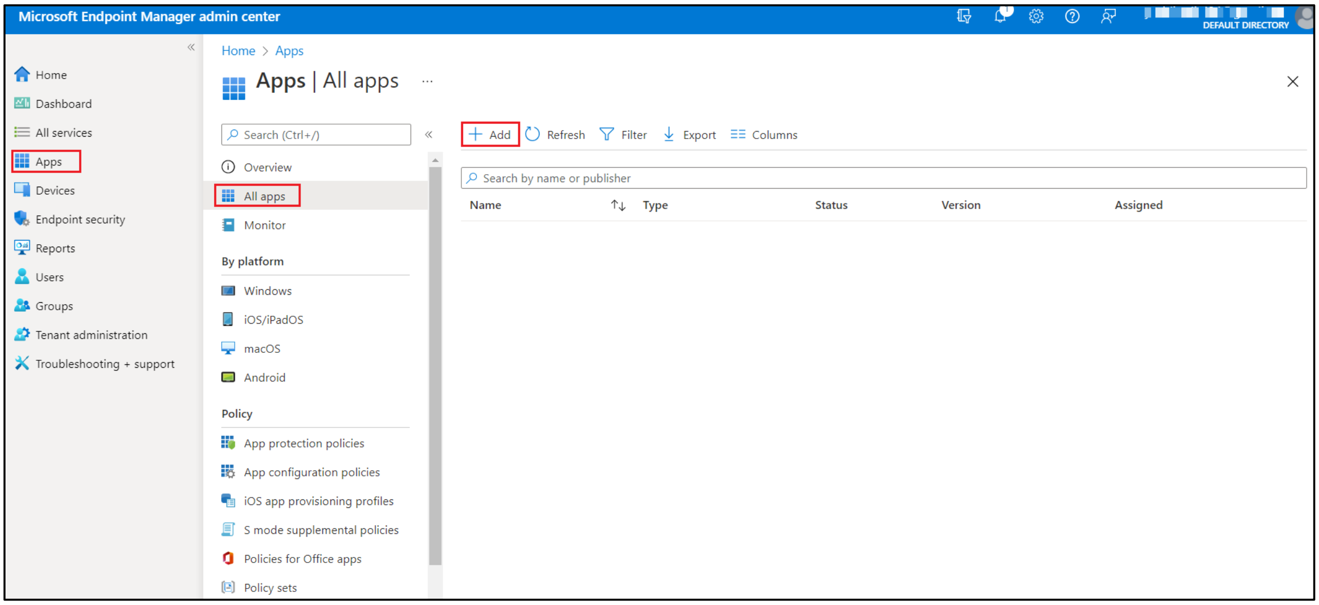
Now, a .IntuneWin package (ConfigurationSetup.intunewin) is ready for deployment under **Intune-Deployment\ConfigurationOutput** as a Win32 application in Intune.

Deploying the IntuneWin package

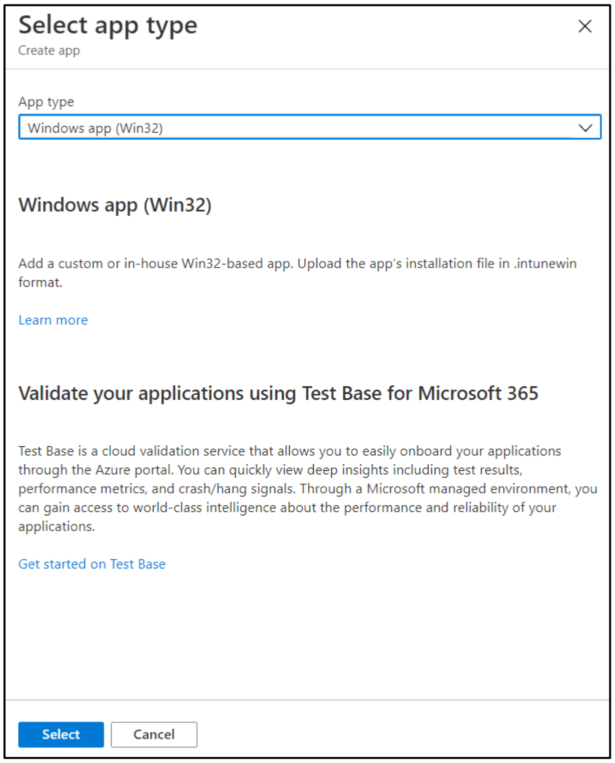
Perform the following steps to deploy SafeNet Agent for Windows Logon via Intune:

Deploying the IntuneWin package of WLA Installer

1. Login to the Microsoft Endpoint Manager admin center using https://endpoint.microsoft.com.
2. In the left pane, select **Apps > All apps > Add**.



3. In the **Select app type** window, under the **App type** drop-down, select **Windows app (Win32)**, and then click **Select**.



Select app type

Create app

App type: Windows app (Win32)

Windows app (Win32)

Add a custom or in-house Win32-based app. Upload the app's installation file in .intunewin format.

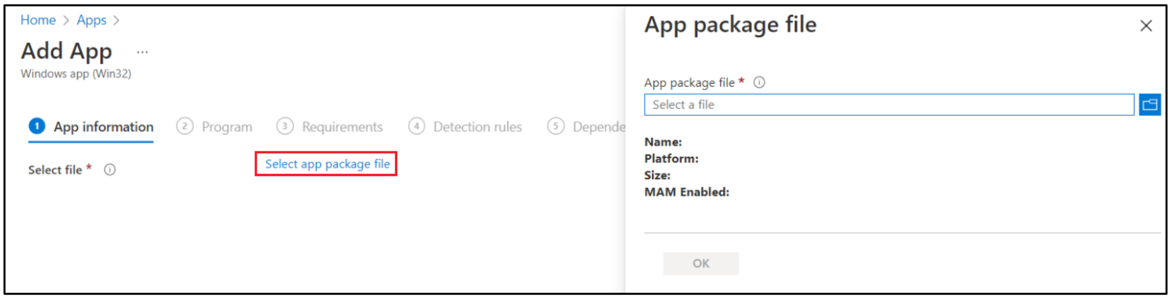
Learn more

Validate your applications using Test Base for Microsoft 365

Test Base is a cloud validation service that allows you to easily onboard your applications through the Azure portal. You can quickly view deep insights including test results, performance metrics, and crash/hang signals. Through a Microsoft managed environment, you can gain access to world-class intelligence about the performance and reliability of your applications.

Get started on Test Base

4. Click **Select app package** file. The **App package file** window appears.



Home > Apps >

Add App ...

Windows app (Win32)

Select file * ⓘ Select app package file

App package file

App package file * ⓘ

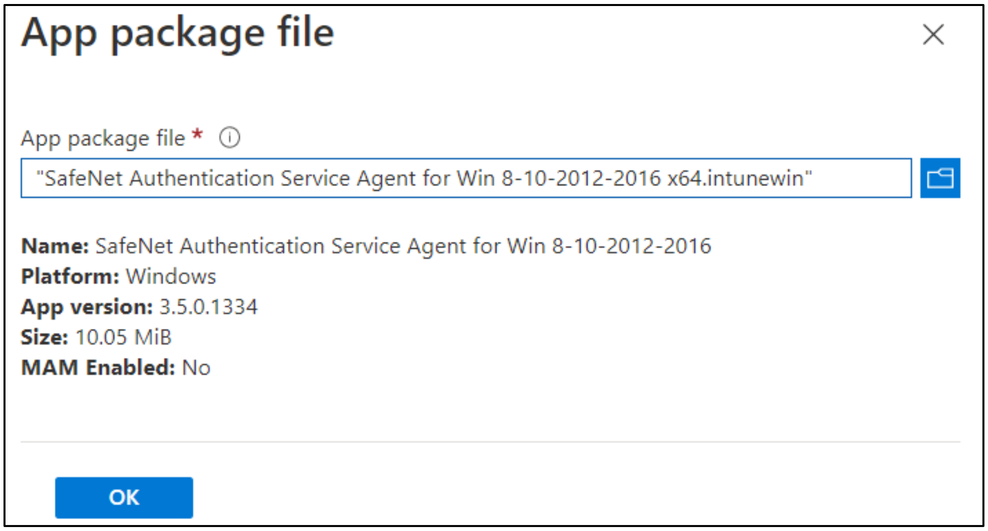
Select a file

Name:
Platform:
Size:
MAM Enabled:

5. In the **App package file** window, perform the following steps:

   i. Click 🗀 to select the **App package file**, that is, *SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64.intunewin*, which you have previously created in Creating an IntuneWin package of WLA Installer section.

   ii. Click **OK**.



App package file

App package file * ⓘ

"SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64.intunewin"

Name: SafeNet Authentication Service Agent for Win 8-10-2012-2016
Platform: Windows
App version: 3.5.0.1334
Size: 10.05 MiB
MAM Enabled: No

6. In the **Add App** window, under the **App information** tab, enter the following details for your app:

   i. **Name**: Enter name of the app. Ensure the app names that you use are unique. For example, SafeNet Agent for Windows Logon.

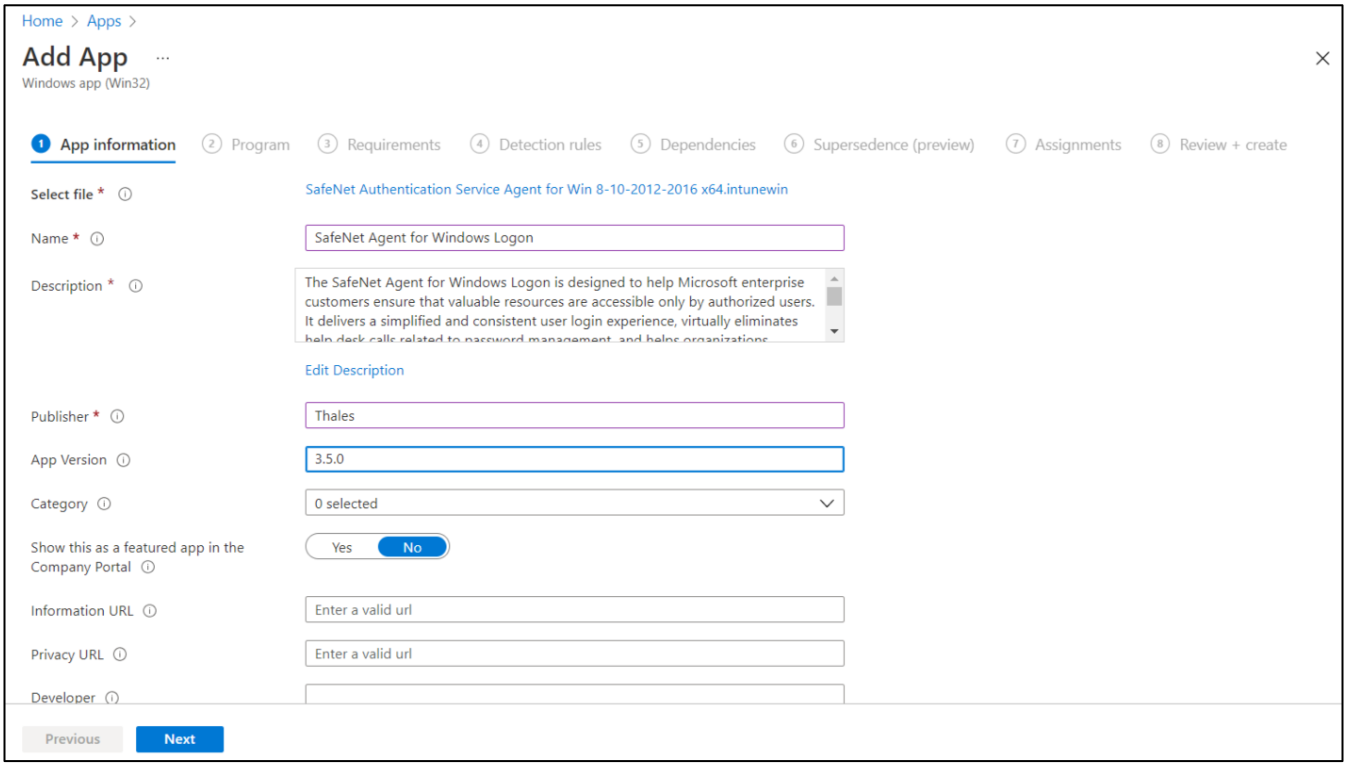
   ii. **Description**: Click **Edit Description** to enter a small description of the app and then click **OK**.

   iii. **Publisher**: Enter the name of the publisher of the app. For example, Thales.

   iv. **App Version**: Depicts the app version. For example, 3.5.0.

   You can also update the other fields as per your requirement.

   v. Click **Next** to display the **Program** page.



Select file * : SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64.intunewin

Name * : SafeNet Agent for Windows Logon

Description * : The SafeNet Agent for Windows Logon is designed to help Microsoft enterprise 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

Edit Description

Publisher * : Thales

App Version : 3.5.0

Category : 0 selected

Show this as a featured app in the Company Portal : Yes [✓ No]

Information URL : Enter a valid url

Privacy URL : Enter a valid url

Developer :

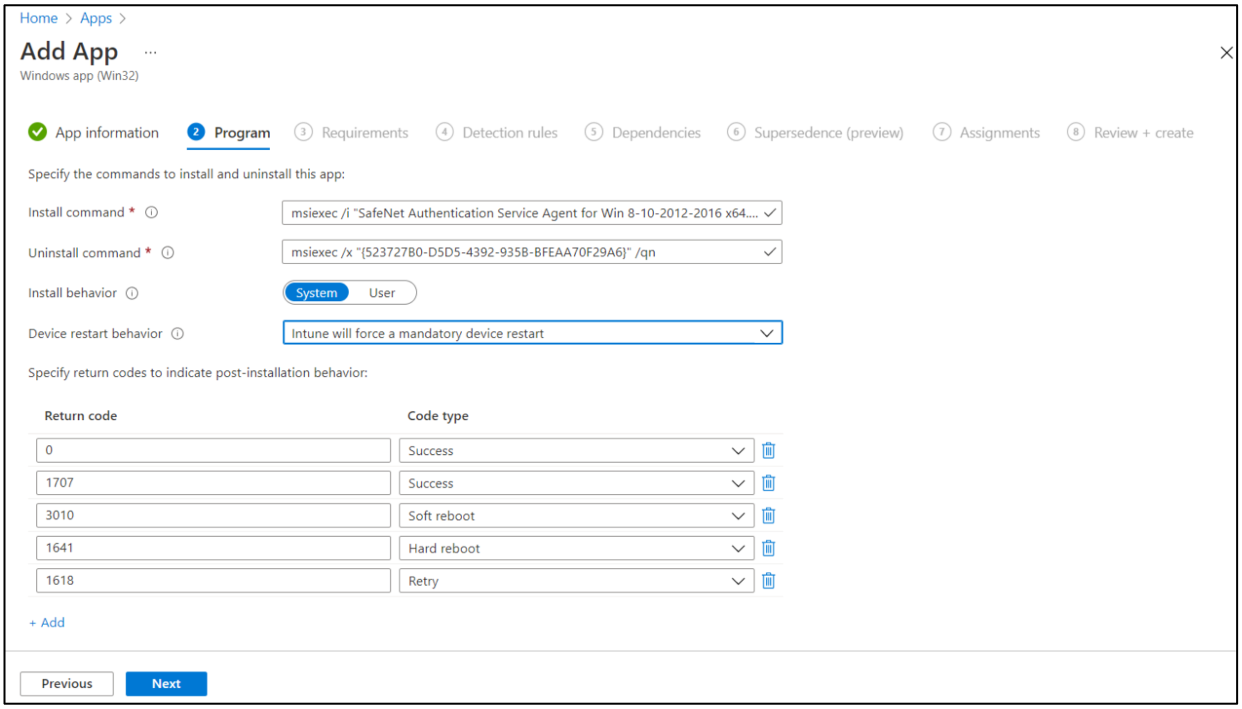
7. Under the **Program** tab, enter the following details to configure the app installation and removal commands for the app:

   i. **Install command**: Enter **msiexec /i "SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64.msi" /quiet** as the installation command to install the app.

   ii. **Uninstall command**: Enter **msiexec /x "{523727B0-D5D5-4392-935B-BFEAA70F29A6}" /qn** as the command to uninstall the app.

   iii. **Device restart behavior**: Select **Intune will force a mandatory restart** option from the drop-down to always restart the device after a successful app installation.

   iv. Click **Next** to display the **Requirements** page.



Specify the commands to install and uninstall this app:

Install command * ⓘ	msiexec /i "SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64....
Uninstall command * ⓘ	msiexec /x "{523727B0-D5D5-4392-935B-BFEAA70F29A6}" /qn
Install behavior ⓘ	[✓ System] User
Device restart behavior ⓘ	Intune will force a mandatory device restart

Specify return codes to indicate post-installation behavior:

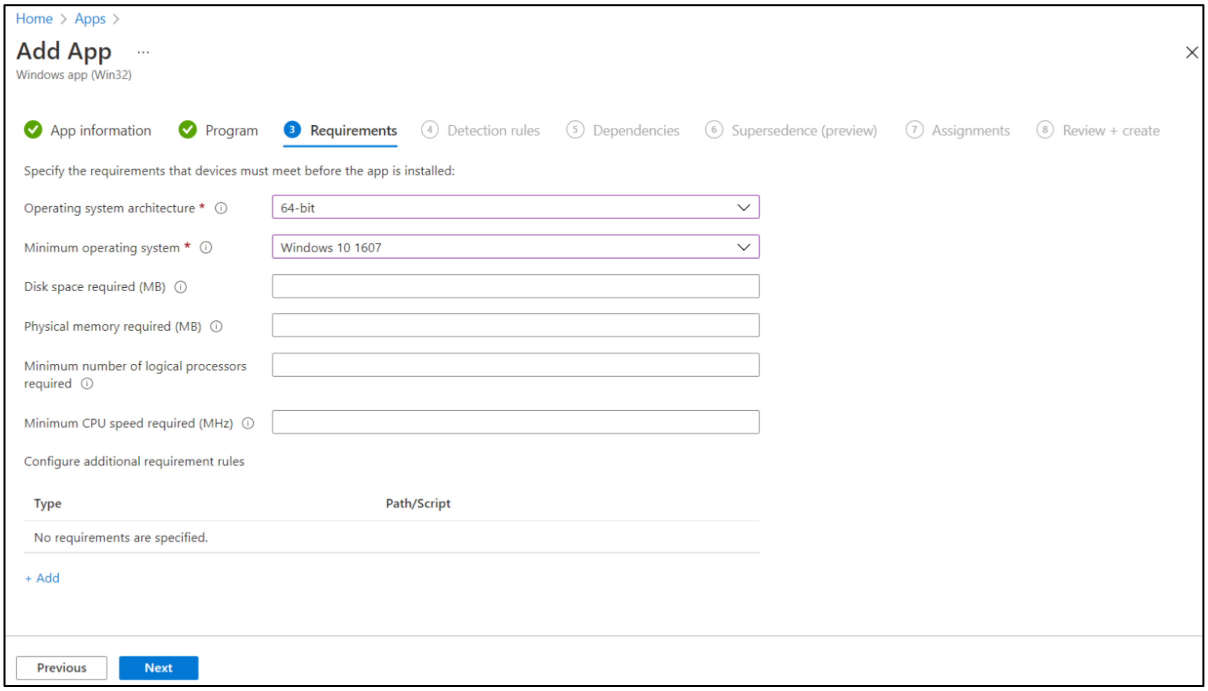
Return code	Code type
0	Success
1707	Success
3010	Soft reboot
1641	Hard reboot
1618	Retry

8. Under the **Requirements** tab, specify the following requirements that the device must meet before the app is installed:

   i. **Operating system architecture**: Select either **32-bit** or **64-bit** as the architecture needed to install the app.

   ii. **Minimum operating system**: Select the minimum operating system needed to install the app. For example, Windows 10 1607.

   iii. Click **Next** to display the **Detection rules** page.



Specify the requirements that devices must meet before the app is installed:

Operating system architecture * ⓘ	64-bit
Minimum operating system * ⓘ	Windows 10 1607
Disk space required (MB) ⓘ	
Physical memory required (MB) ⓘ	
Minimum number of logical processors required ⓘ	
Minimum CPU speed required (MHz) ⓘ	

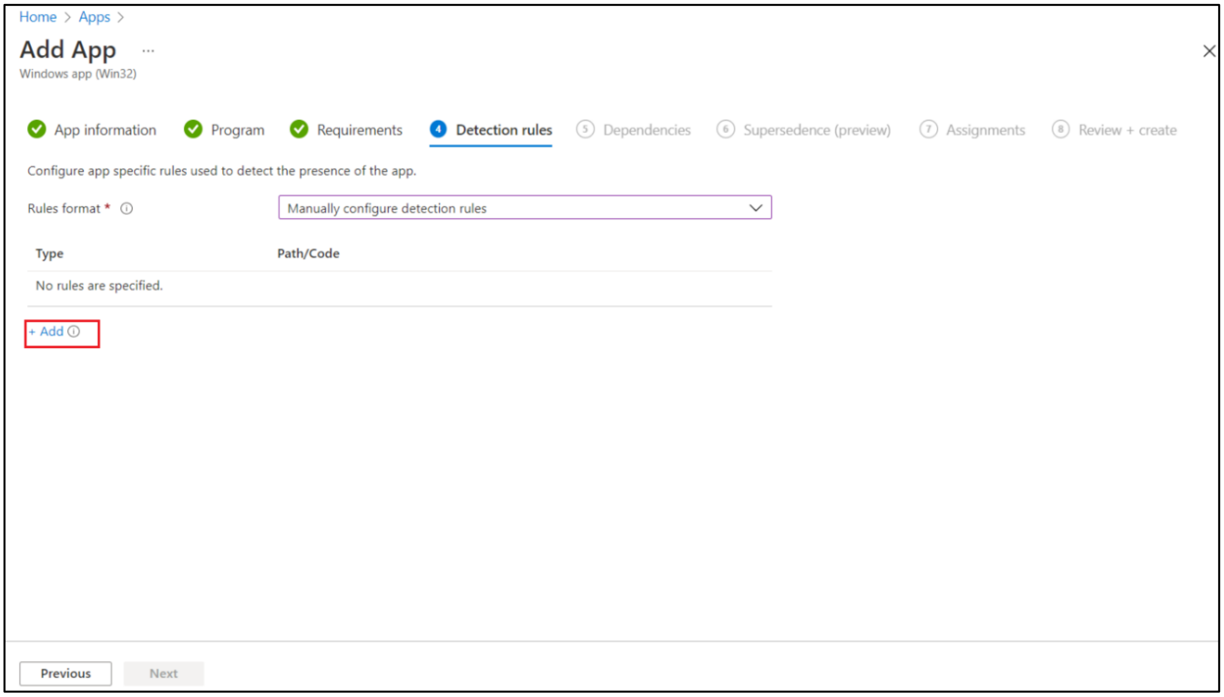
Configure additional requirement rules

Type	Path/Script
No requirements are specified.	

9. Under the **Detection rules** tab, specify the rues to detect the presence of the app:

   i. **Rules format**: Select **Manually configure detection rules** from the drop-down.

   ii. Click **Add**.



Configure app specific rules used to detect the presence of the app.

Rules format * ⓘ Manually configure detection rules

Type	Path/Code
No rules are specified.	

+ Add ⓘ

Detection rule window appears. Enter the following details to create a detection rule:

i. **Rule type**: Select **MSI** from the drop-down.

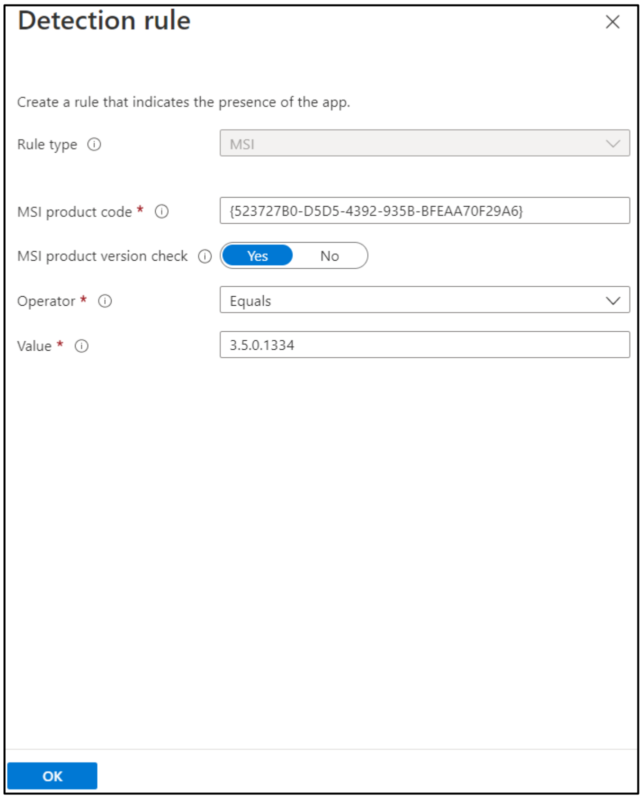
ii. **MSI product code**: Enter **{523727B0-D5D5-4392-935B-BFEAA70F29A6}** as the MSI product code.

iii. **MSI product version check**: Select **Yes**.

iv. **Operator**: Select **Equals** from the drop-down.

v. **Value**: Enter the **Build Number** mentioned in the CRN, associated with this release.

vi. Click **OK**.



Detection rule

Create a rule that indicates the presence of the app.

Rule type: MSI

MSI product code *: {523727B0-D5D5-4392-935B-BFEAA70F29A6}

MSI product version check: Yes

Operator *: Equals

Value *: 3.5.0.1334

After adding your rules, click **Next** to display the **Dependencies** page.

10. In the **Dependencies** tab, click **Next.**

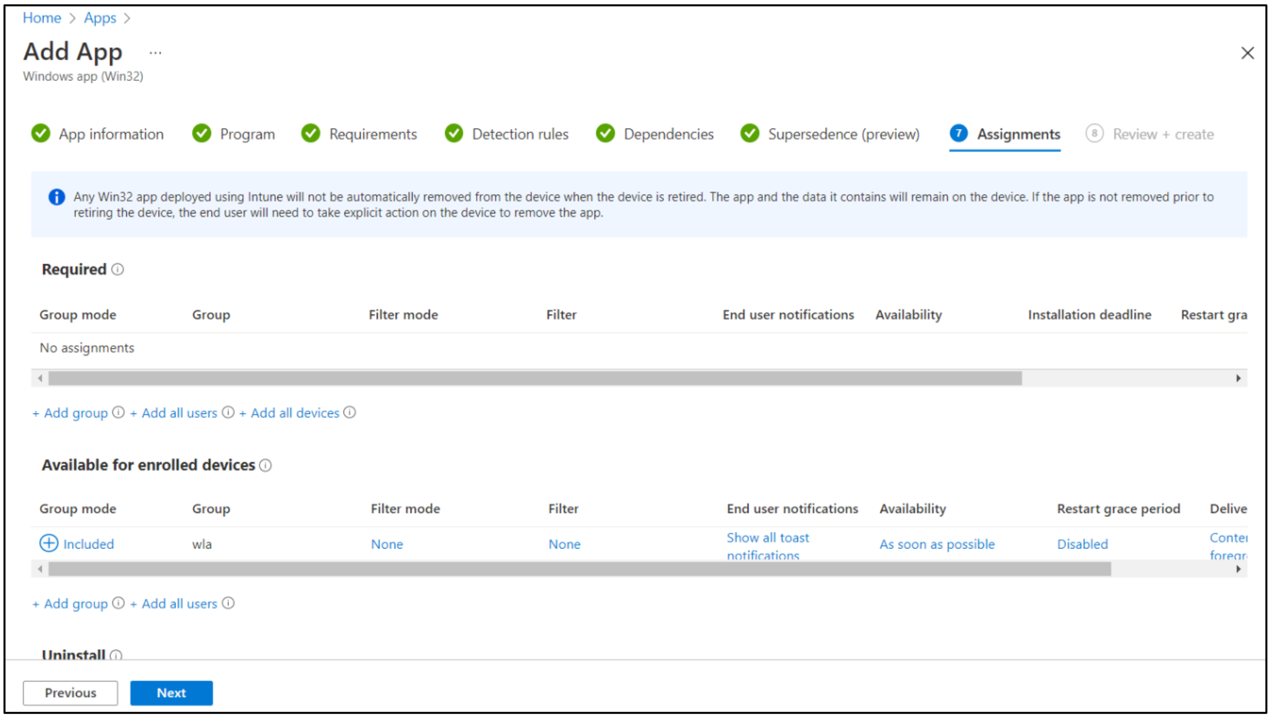
11. In the **Supersedence (preview)** tab, click **Next.**

12. Under the **Assignments** tab, you can select the **Required**, **Available for enrolled devices**, or **Uninstall** group assignments for the app.

    i. Select an assignment type for the app:

    - **Required**: The app is installed on devices in the selected groups. In this section,
        - Click **Add group** to assign the groups that will use the app.
        - Click **Add all users** to assign app access to all the users.
        - Click **Add all devices** to install the app in all Azure AD joined devices.
    - **Available for enrolled devices**: Users install the app from the company portal app or the company portal website. In this section,
        - Click **Add group** to assign the groups for which you want to make the app available.
        - Click **Add all users** to assign app access to all the users.
    - **Uninstall**: The app is uninstalled from devices in the selected groups.

    ii. Click **Next** to display the **Review + create** page.



Home > Apps >

Add App ...

Windows app (Win32)

Any Win32 app deployed using Intune will not be automatically removed from the device when the device is retired. The app and the data it contains will remain on the device. If the app is not removed prior to retiring the device, the end user will need to take explicit action on the device to remove the app.

Required ⓘ

Group mode	Group	Filter mode	Filter	End user notifications	Availability	Installation deadline	Restart gra
No assignments							

+ Add group ⓘ + Add all users ⓘ + Add all devices ⓘ

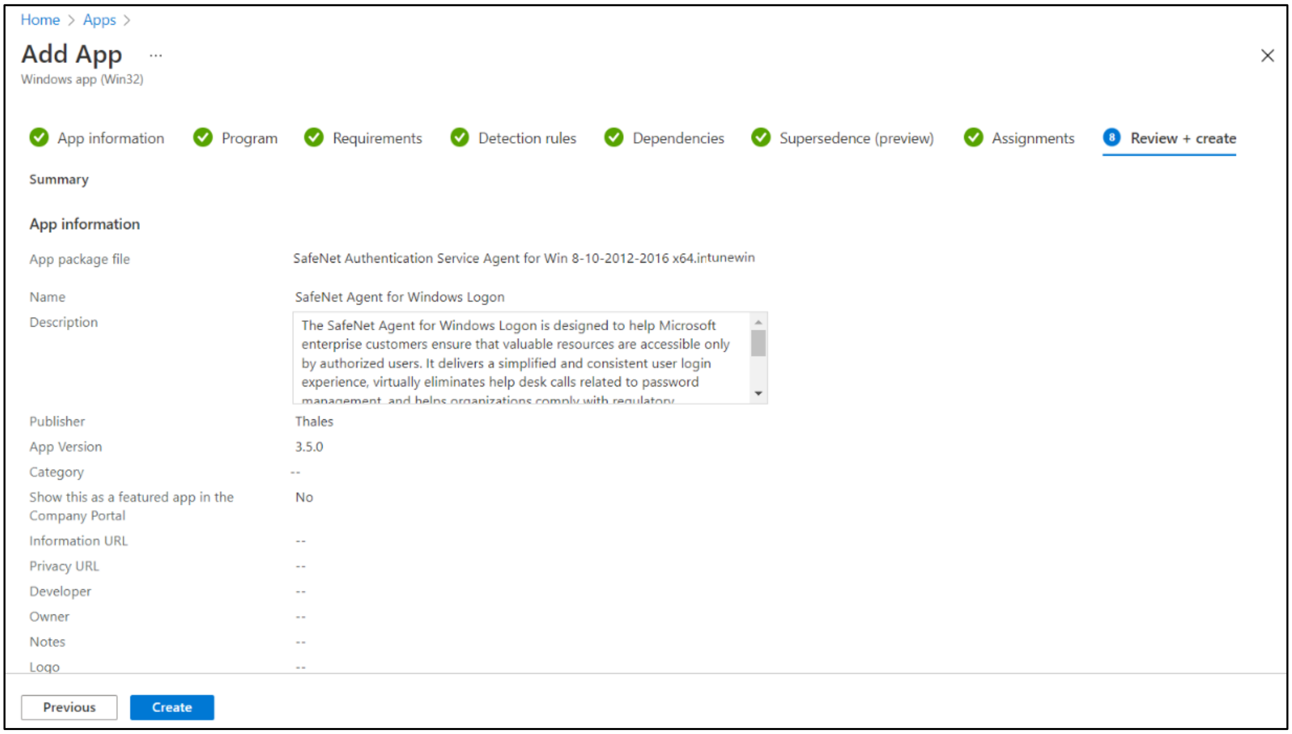
Available for enrolled devices ⓘ

Group mode	Group	Filter mode	Filter	End user notifications	Availability	Restart grace period	Delive
Included	wla	None	None	Show all toast notifications	As soon as possible	Disabled	Conter foregr

+ Add group ⓘ + Add all users ⓘ

Uninstall ⓘ

13. In the **Review + create** tab, review the values and settings that you entered for the app, and then click **Create**.



Home > Apps >

Add App ...

Windows app (Win32)

Summary

App information

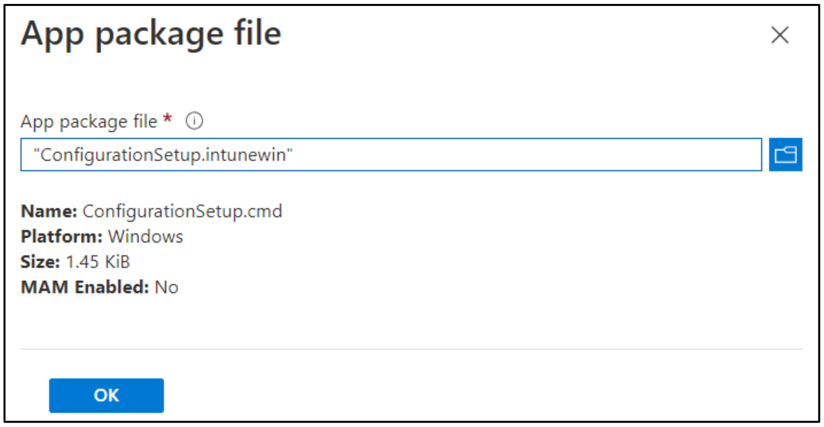
App package file	SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64.intunewin
Name	SafeNet Agent for Windows Logon
Description	The SafeNet Agent for Windows Logon is designed to help Microsoft enterprise customers ensure that valuable resources are accessible only by authorized users. It delivers a simplified and consistent user login experience, virtually eliminates help desk calls related to password management, and helps organizations comply with regulatory
Publisher	Thales
App Version	3.5.0
Category	--
Show this as a featured app in the Company Portal	No
Information URL	--
Privacy URL	--
Developer	--
Owner	--
Notes	--
Logo	--

After completing the above steps, the **SafeNet Agent for Windows Logon** app will be deployed successfully.

Deploying the IntuneWin package for configuring the Settings

Perform the following steps to deploy the IntuneWin package for configuring the Settings of WLA in Intune. After performing all the steps, the DefaultConfiguration.reg file will be copied in the client system.

1. Repeat the steps from Step 1 to Step 4 in the above section.
2. In the **App package file** window, perform the following steps:
   i. Click 🗀 to select the **App package file**, that is, *ConfigurationSetup.intunewin*, which you have previously created in Creating an IntuneWin package for configuring the Settings section.
   ii. Click **OK**.



App package file

App package file *

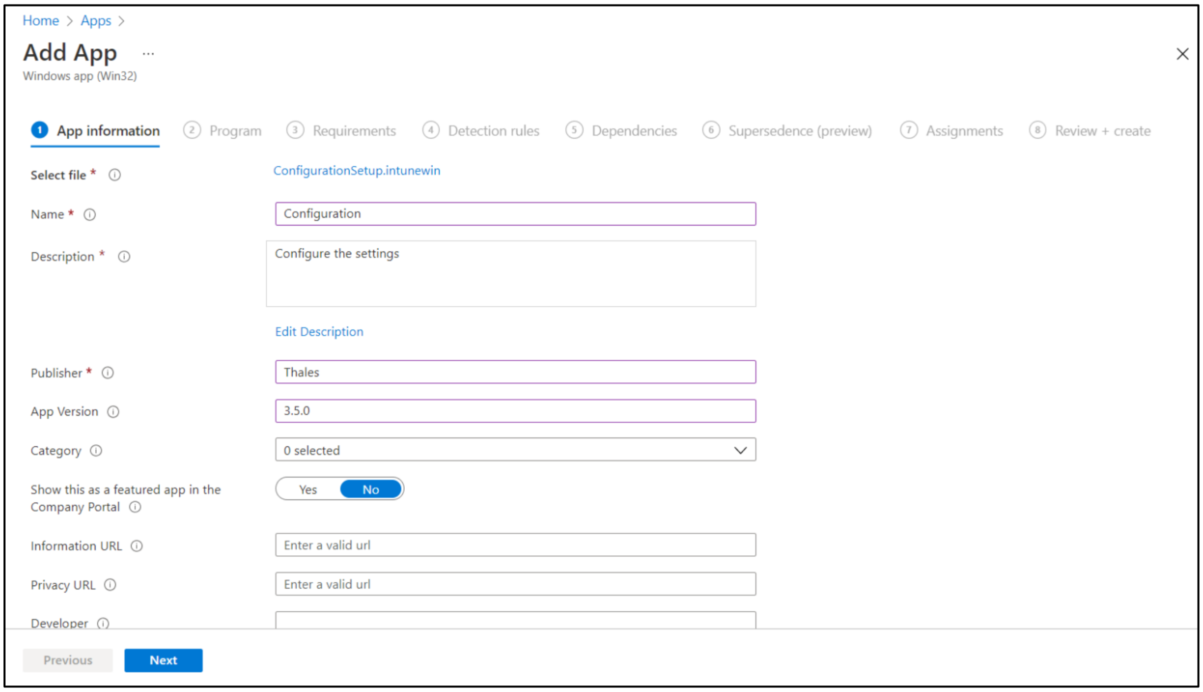
"ConfigurationSetup.intunewin"

Name: ConfigurationSetup.cmd
Platform: Windows
Size: 1.45 KiB
MAM Enabled: No

3. In the **Add App** window, under **App information** tab, enter the following details for your app:
   i. **Name**: Enter name of the app. Ensure the app names that you use are unique. For example, Configuration.
   ii. **Description**: Click **Edit Description** to enter a small description of the app and then click OK.
   iii. **Publisher**: Enter the name of the publisher of the app as **Thales**.
   iv. **App Version**: Depicts the app's version as **3.5.0**.

   You can also update the other fields as per your requirement.

   v. Click **Next** to display the **Program** page.



Select file * ⓘ	ConfigurationSetup.intunewin
Name * ⓘ	Configuration
Description * ⓘ	Configure the settings
Publisher * ⓘ	Thales
App Version ⓘ	3.5.0
Category ⓘ	0 selected
Show this as a featured app in the Company Portal ⓘ	Yes [✓ No]
Information URL ⓘ	Enter a valid url
Privacy URL ⓘ	Enter a valid url
Developer ⓘ	

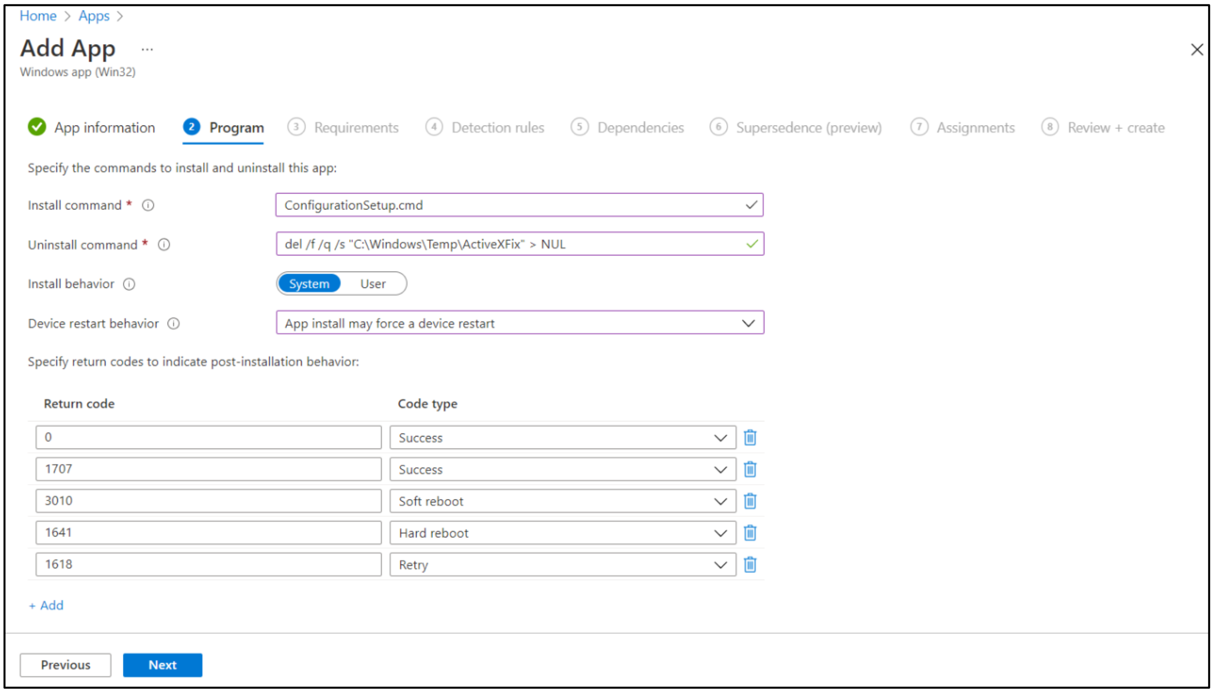
4. Under the **Program** tab, enter the following details to configure the app installation and removal commands for the app:

   i. **Install command**: Enter **ConfigurationSetup.cmd** as the installation command to install the app.

   ii. **Uninstall command**: Enter **del /f /q /s "C:\Windows\Temp\ActiveFix" > NUL** as the command to uninstall the app.

   iii. **Device restart behavior**: Select **App install may force a device restart** option from the drop-down.

   iv. Click **Next** to display the **Requirements** page.



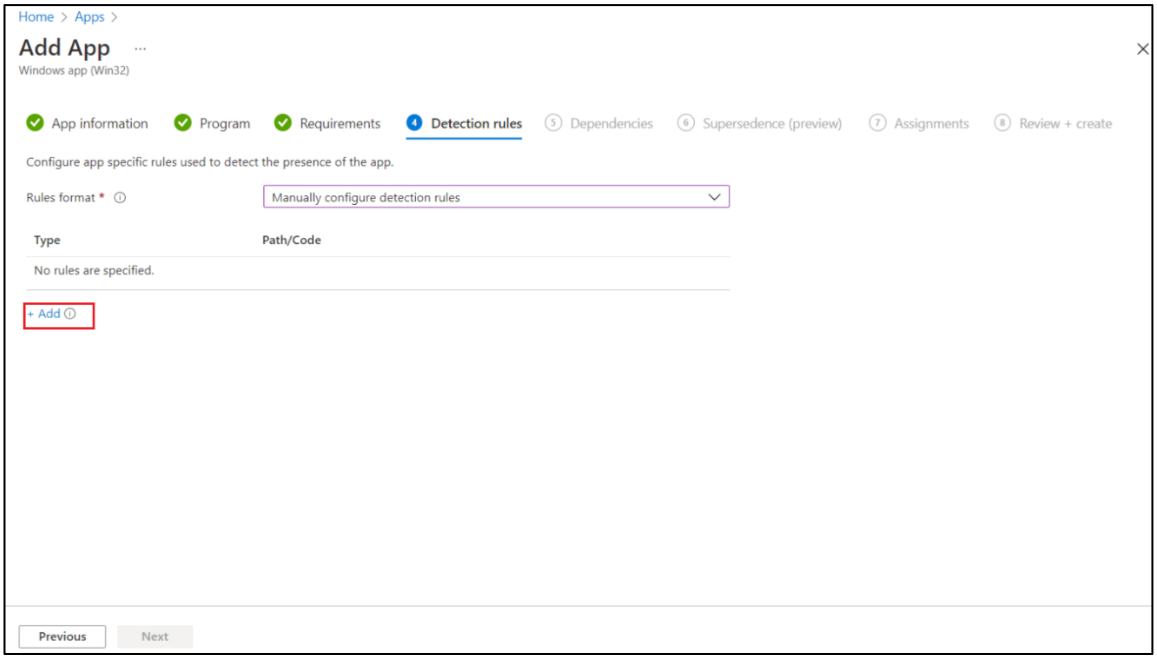
Specify the commands to install and uninstall this app:

Install command * ⓘ	ConfigurationSetup.cmd ✓
Uninstall command * ⓘ	del /f /q /s "C:\Windows\Temp\ActiveXFix" > NUL ✓
Install behavior ⓘ	[✓ System] User
Device restart behavior ⓘ	App install may force a device restart

Specify return codes to indicate post-installation behavior:

Return code	Code type
0	Success
1707	Success
3010	Soft reboot
1641	Hard reboot
1618	Retry

5. Repeat Step 8 in the above section.
6. Under the **Detection rules** tab, specify the rues to detect the presence of the app:
   i. **Rules format**: Select **Manually configure detection rules** from the drop-down.
   ii. Click **Add**.



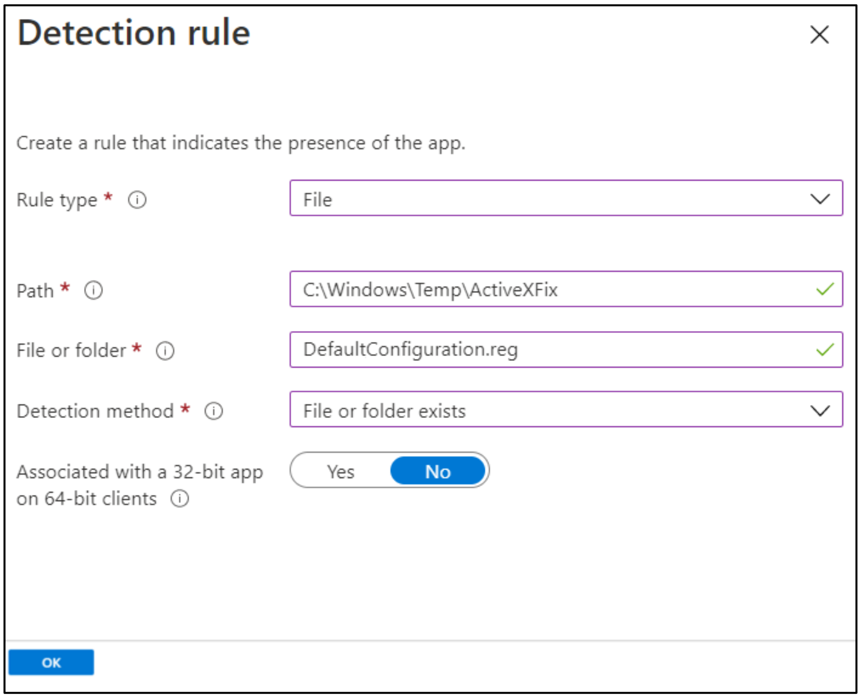
Configure app specific rules used to detect the presence of the app.

Rules format * ⓘ Manually configure detection rules

Type	Path/Code
No rules are specified.	

Detection rule window appears. Enter the following details to create a detection rule:

i. **Rule type**: Select **File** from the drop-down.
ii. **Key path**: Enter **C:\Windows\Temp\ActiveXFix** as the full path of the file that contains the value to detect.
iii. **Value name**: Enter **DefaultConfiguration.reg** as the name of the file value to detect.
iv. **Detection method**: Select **File or Folder Exists** from the drop-down to validate the presence of the app.
v. Click **OK**.



Detection rule

Create a rule that indicates the presence of the app.

Rule type * : File

Path * : C:\Windows\Temp\ActiveXFix

File or folder * : DefaultConfiguration.reg

Detection method * : File or folder exists

Associated with a 32-bit app on 64-bit clients: Yes [✓ No]

After adding your rules, click **Next** to display the **Dependencies** page.

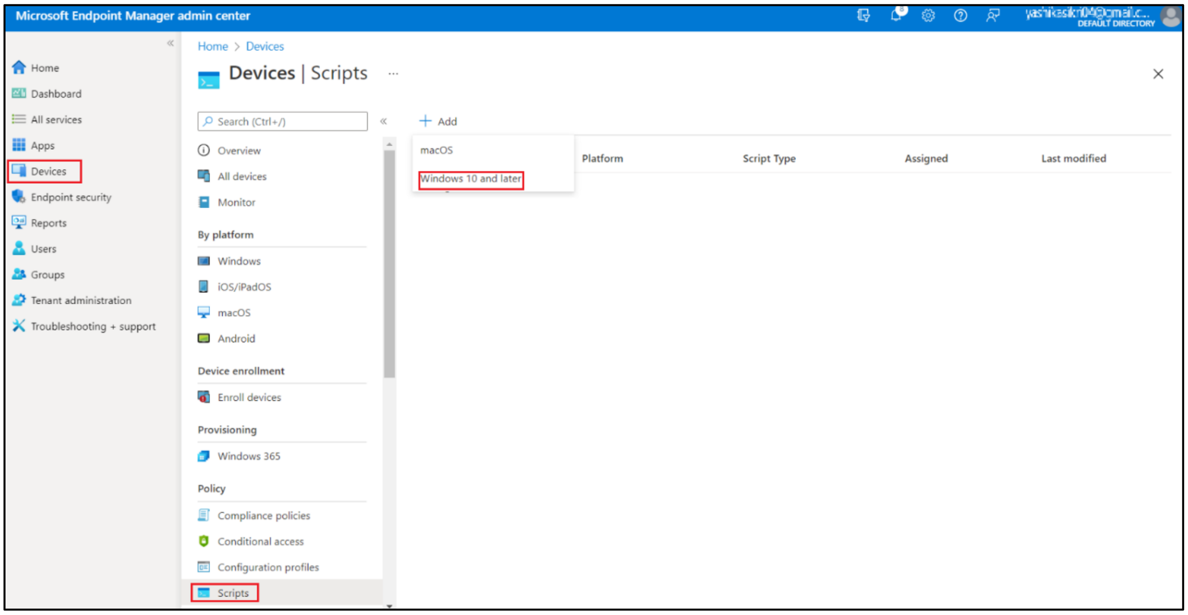
7. Repeat the steps Step 10 to Step 13 in the above section.

After completing the above steps, the **SafeNet Agent for Windows Logon** app will be deployed successfully.

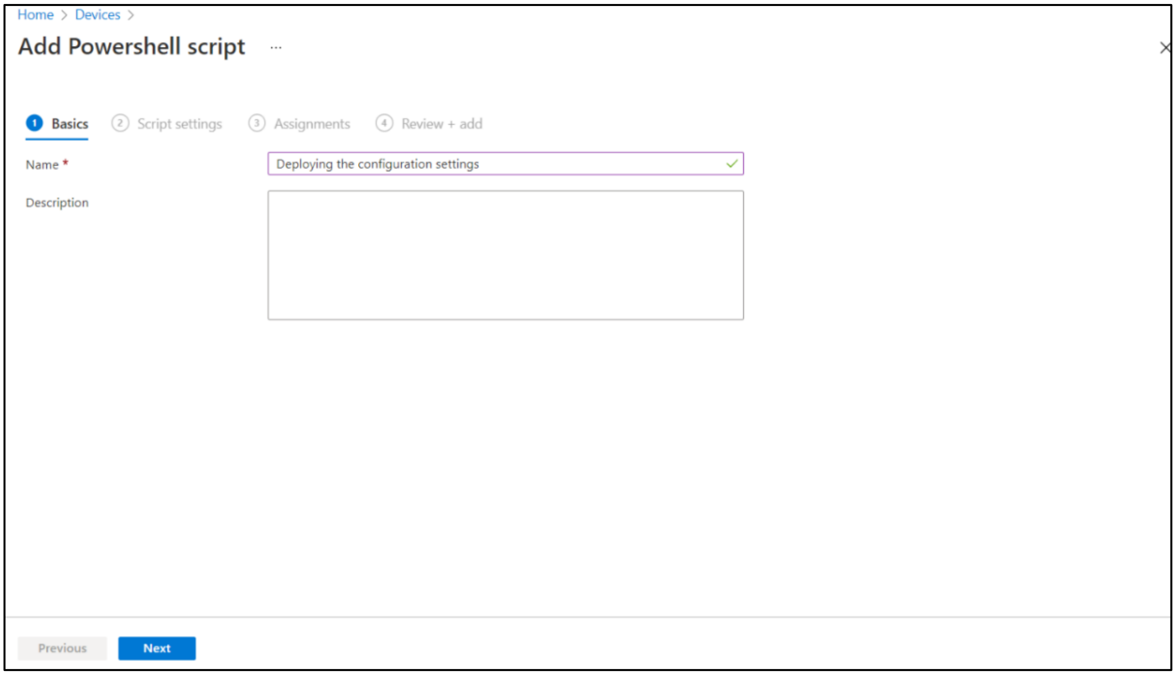
Deploying PowerShell Script to configure the Settings

Perform the following steps to deploy the PowerShell script using Intune:

1. In the left pane of the Microsoft Endpoint Manager admin center, select **Devices > Scripts**.



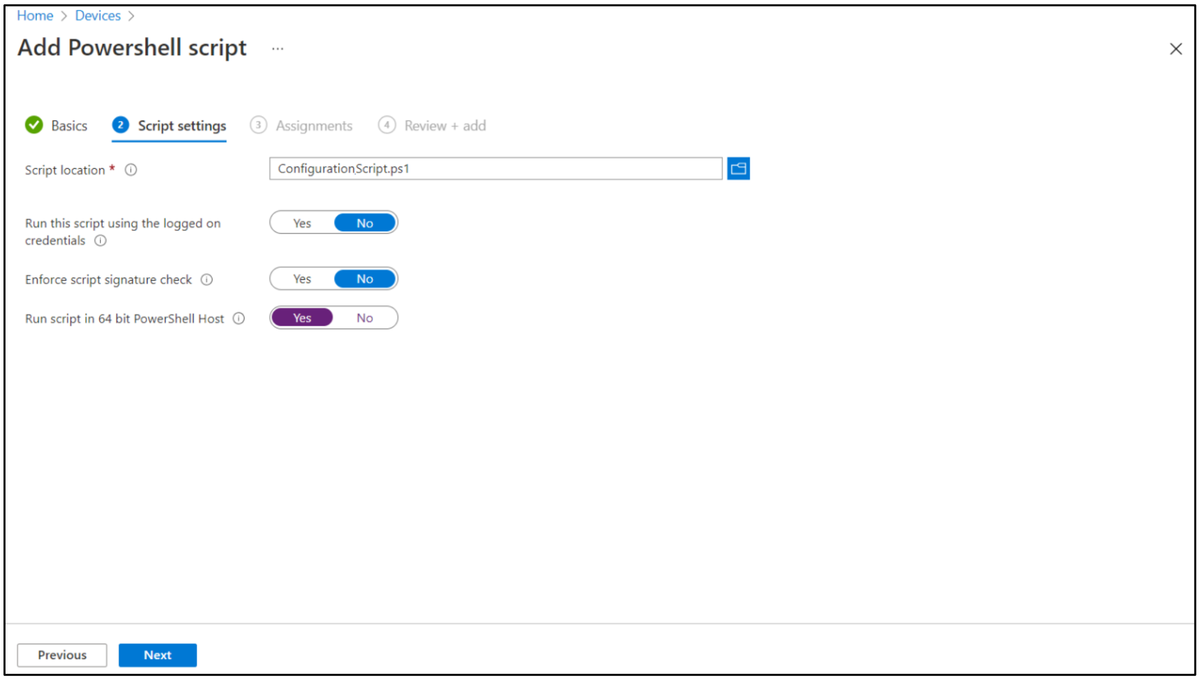
2. Click **Add** to add a new PowerShell script, and then select Windows 10 and later to deploy it to Windows 10 (and later) devices.
3. In the **Add Powershell script** window, under the **Basics** tab, enter the following properties:
   i. **Name**: Enter a name for the PowerShell script. For example, Deploying the configuration settings.
   ii. **Description**: [Optional] Enter a description for the PowerShell script.
   iii. Click **Next**.



Name * Deploying the configuration settings

Description

4. Under the **Script settings** tab, enter the following properties:
   i. **Script location**: Browse to the PowerShell script (ConfigurationScript.ps1) that is present in the Intune-Deployment folder. For example, C:\Intune-Deployment\ConfigurationScript.ps1
   ii. **Run script in 64-bit PowerShell host**: Select **Yes** to run the script in a 64-bit PowerShell host on a 64-bit client architecture. Selecting No (default) runs the script in a 32-bit PowerShell host.
   iii. Click **Next**.



Home > Devices >

Add Powershell script ...

✓ Basics 2 Script settings 3 Assignments 4 Review + add

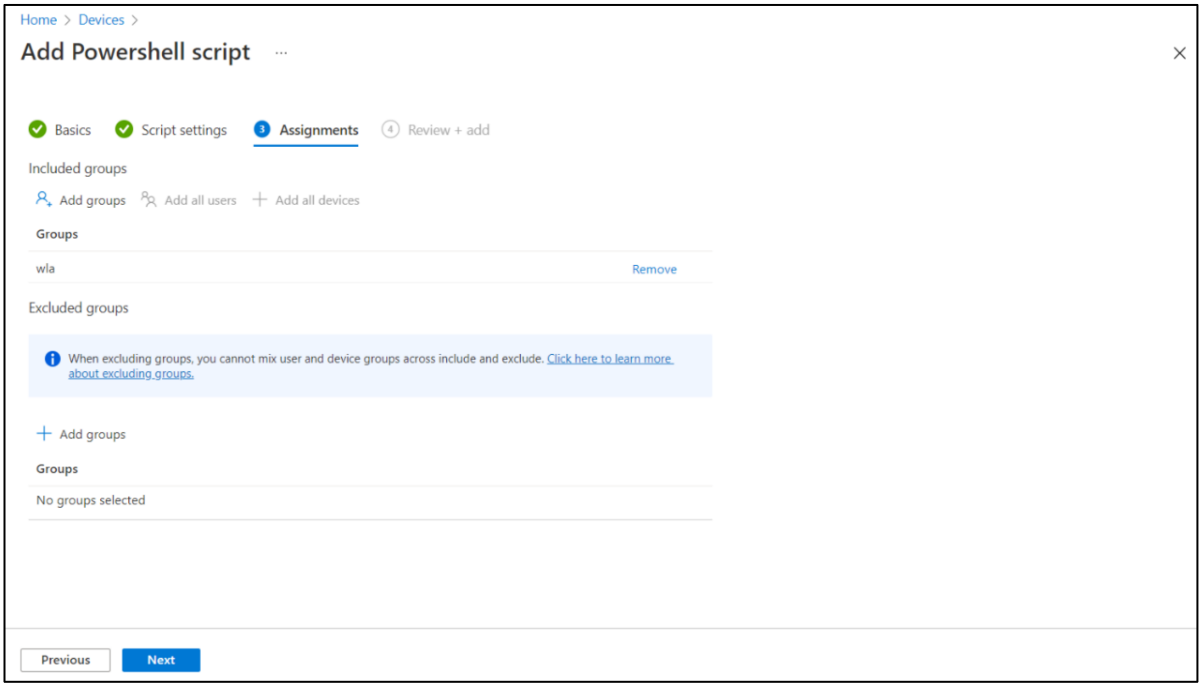
Script location * ⓘ: ConfigurationScript.ps1

Run this script using the logged on credentials ⓘ: Yes [✓ No]

Enforce script signature check ⓘ: Yes [✓ No]

Run script in 64 bit PowerShell Host ⓘ: [✓ Yes] No

5. Under the **Assignments** tab,
   i. Click **Add Group** to select groups to include the users whose devices receive the PowerShell script.
   ii. Click **Next**.



Home > Devices >

Add Powershell script ...

✓ Basics ✓ Script settings 3 Assignments 4 Review + add

Included groups

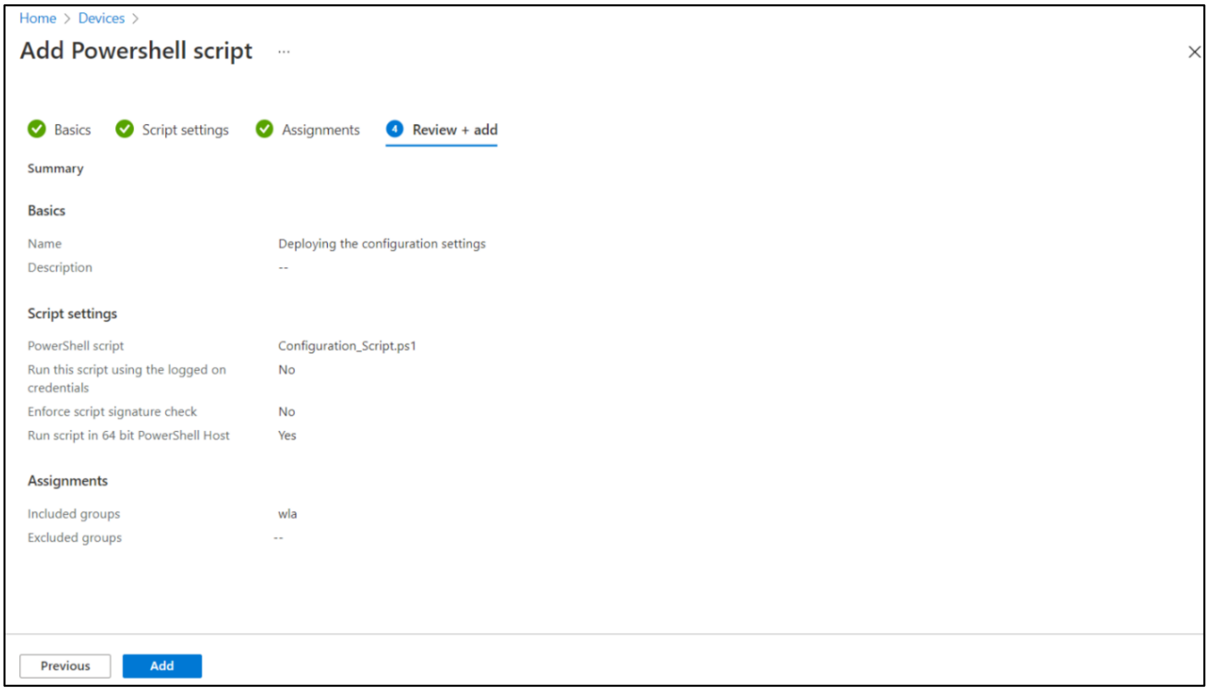
Groups	
wla	Remove

Excluded groups

When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more about excluding groups.

Groups
No groups selected

6. In the **Review + add** tab, a summary is shown of the settings that you have configured. Click **Add** to save the script.



Summary

Basics

Name	Deploying the configuration settings
Description	--

Script settings

PowerShell script	Configuration_Script.ps1
Run this script using the logged on credentials	No
Enforce script signature check	No
Run script in 64 bit PowerShell Host	Yes

Assignments

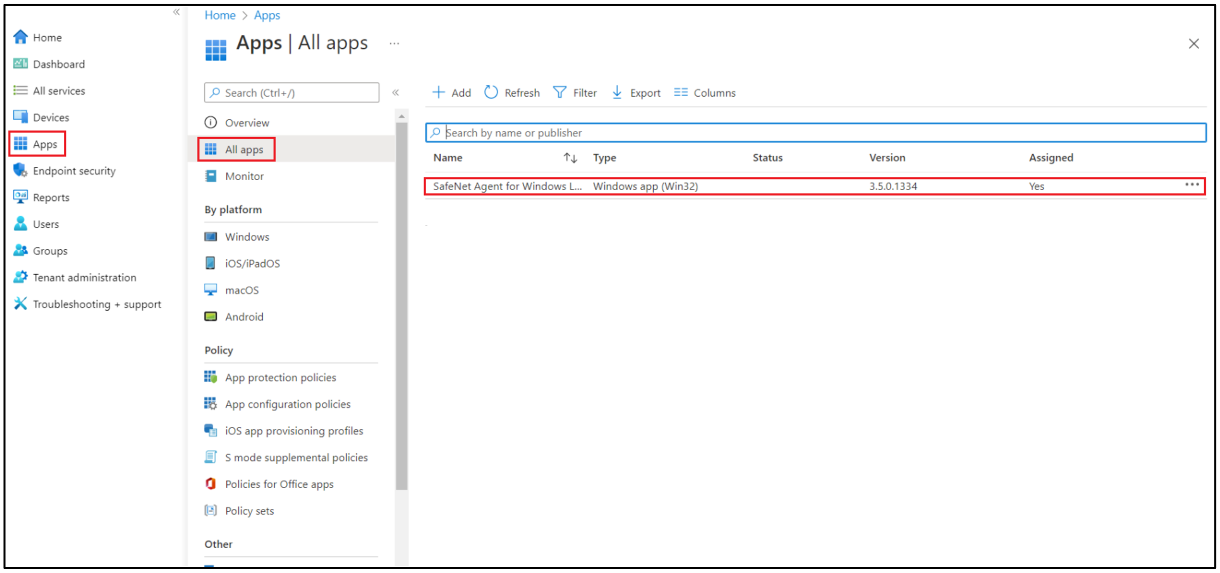
Included groups	wla
Excluded groups	--

After selecting **Add**, the policy is deployed to the groups you chose.

Upgrading SafeNet Agent for Windows Logon

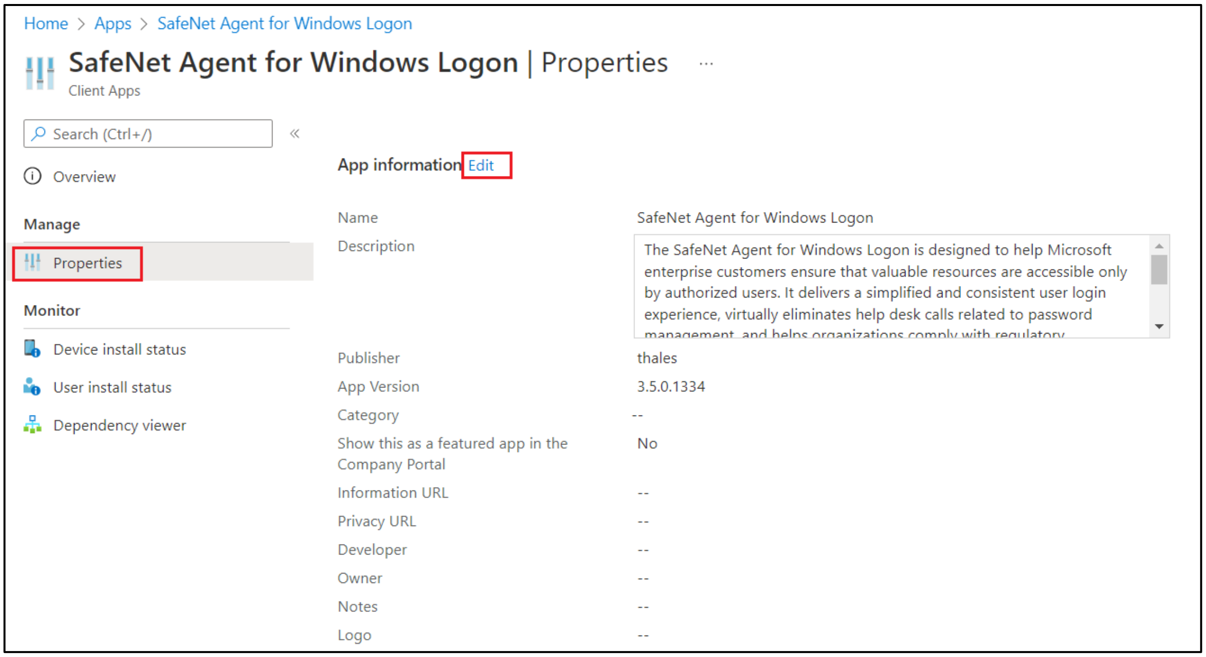
To upgrade the SafeNet Agent for Windows Logon with the latest version, perform the following steps:

1. Perform all the steps in Creating an IntuneWin package.
2. Login to the Microsoft Endpoint Manager admin center using https://endpoint.microsoft.com.
3. In the left pane, select **Apps > All apps**. Select the previously created app.



Name	Type	Status	Version	Assigned
SafeNet Agent for Windows L...	Windows app (Win32)		3.5.0.1334	Yes

4. In the right pane, under **Manage**, click **Properties** and then click **Edit** (next to **App information**).



Home > Apps > SafeNet Agent for Windows Logon

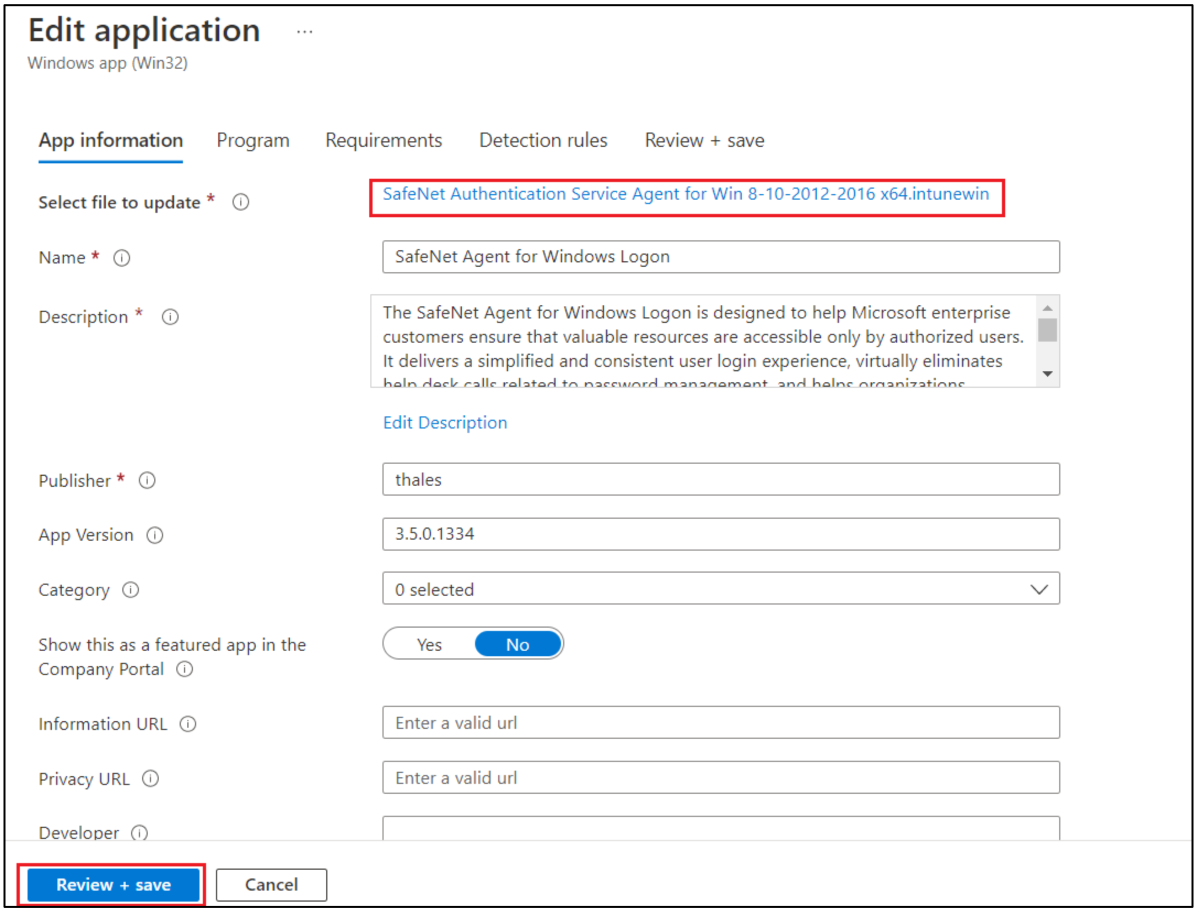
SafeNet Agent for Windows Logon | Properties ...

Client Apps

App information Edit

Name	SafeNet Agent for Windows Logon
Description	The SafeNet Agent for Windows Logon is designed to help Microsoft enterprise 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
Publisher	thales
App Version	3.5.0.1334
Category	--
Show this as a featured app in the Company Portal	No
Information URL	--
Privacy URL	--
Developer	--
Owner	--
Notes	--
Logo	--

5. Under the **App information** tab, click the previously created app from the **Select file to update** field.



Edit application ...

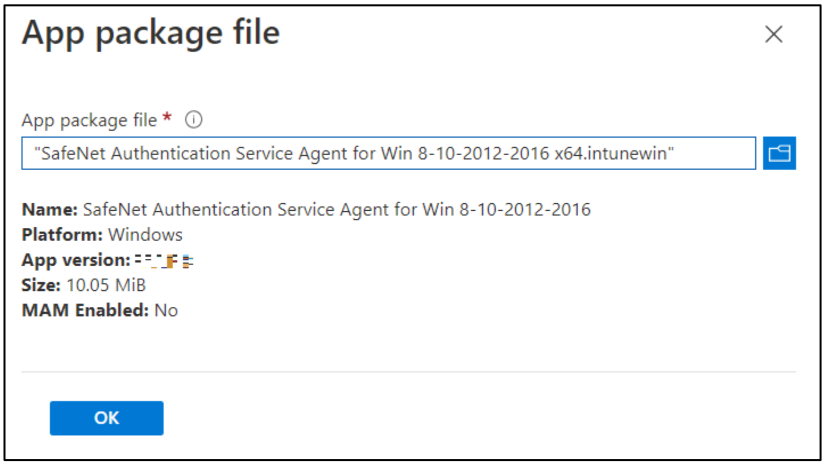
Windows app (Win32)

Select file to update *	SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64.intunewin
Name *	SafeNet Agent for Windows Logon
Description *	The SafeNet Agent for Windows Logon is designed to help Microsoft enterprise 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
	Edit Description
Publisher *	thales
App Version	3.5.0.1334
Category	0 selected
Show this as a featured app in the Company Portal	Yes [✓ No]
Information URL	Enter a valid url
Privacy URL	Enter a valid url
Developer	

The **App package file** window appears. Perform the following steps:

i. Click 🗀 to select the newly created App package file, that is, *SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64.intunewin*, which you have previously created in **Step 1**.

ii. Click **OK**.



App package file

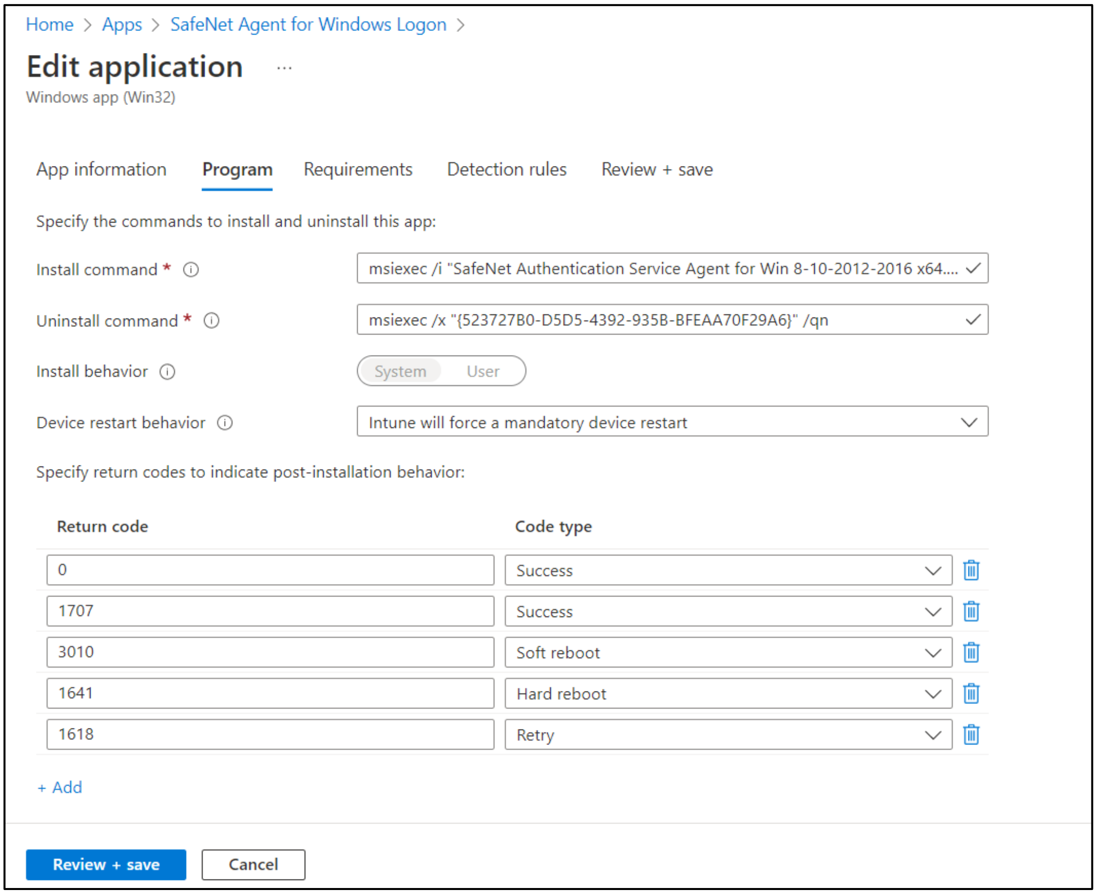
App package file * ⓘ

"SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64.intunewin"

Name: SafeNet Authentication Service Agent for Win 8-10-2012-2016
Platform: Windows
App version: [redacted]
Size: 10.05 MiB
MAM Enabled: No

Click **Review + save** on the **App information** page to display the **Program** page.

6. Under the **Program** tab, enter **msiexec /i "SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64.msi" /quiet REINSTALLMODE=vomus REINSTALL=ALL** as the **Install command** to upgrade the app to its latest version.



Edit application ...

Windows app (Win32)

Specify the commands to install and uninstall this app:

Install command * ⓘ: msiexec /i "SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64....

Uninstall command * ⓘ: msiexec /x "{523727B0-D5D5-4392-935B-BFEAA70F29A6}" /qn

Install behavior ⓘ: System User

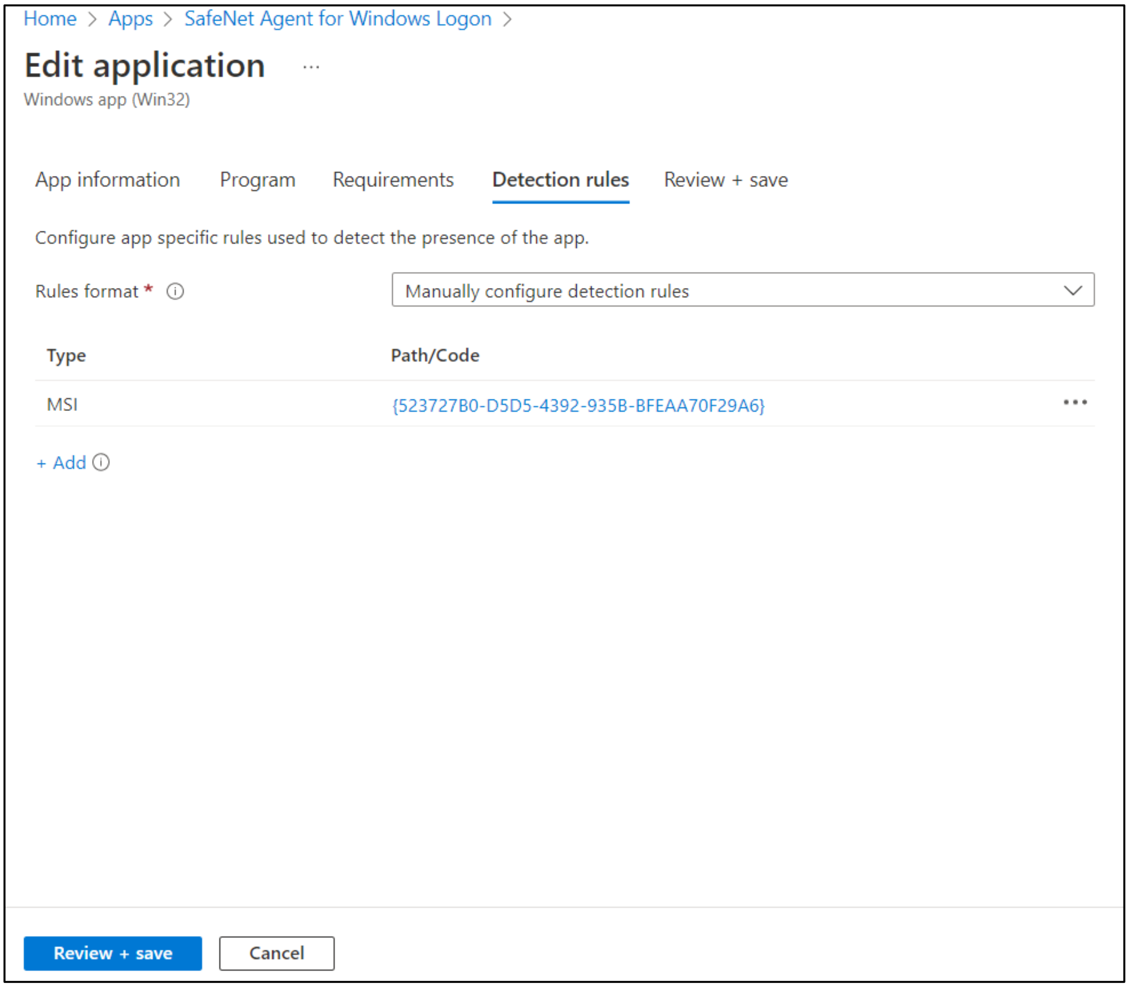
Device restart behavior ⓘ: Intune will force a mandatory device restart

Specify return codes to indicate post-installation behavior:

Return code	Code type
0	Success
1707	Success
3010	Soft reboot
1641	Hard reboot
1618	Retry

Click **Review + save** to display the **Requirements** page.

7. Under the **Requirements** tab, click **Review + save** to display the **Detection rules** page.
8. Under the **Detection rules** tab, select the value of **Path/Code** of the previously created detection rule.



Configure app specific rules used to detect the presence of the app.

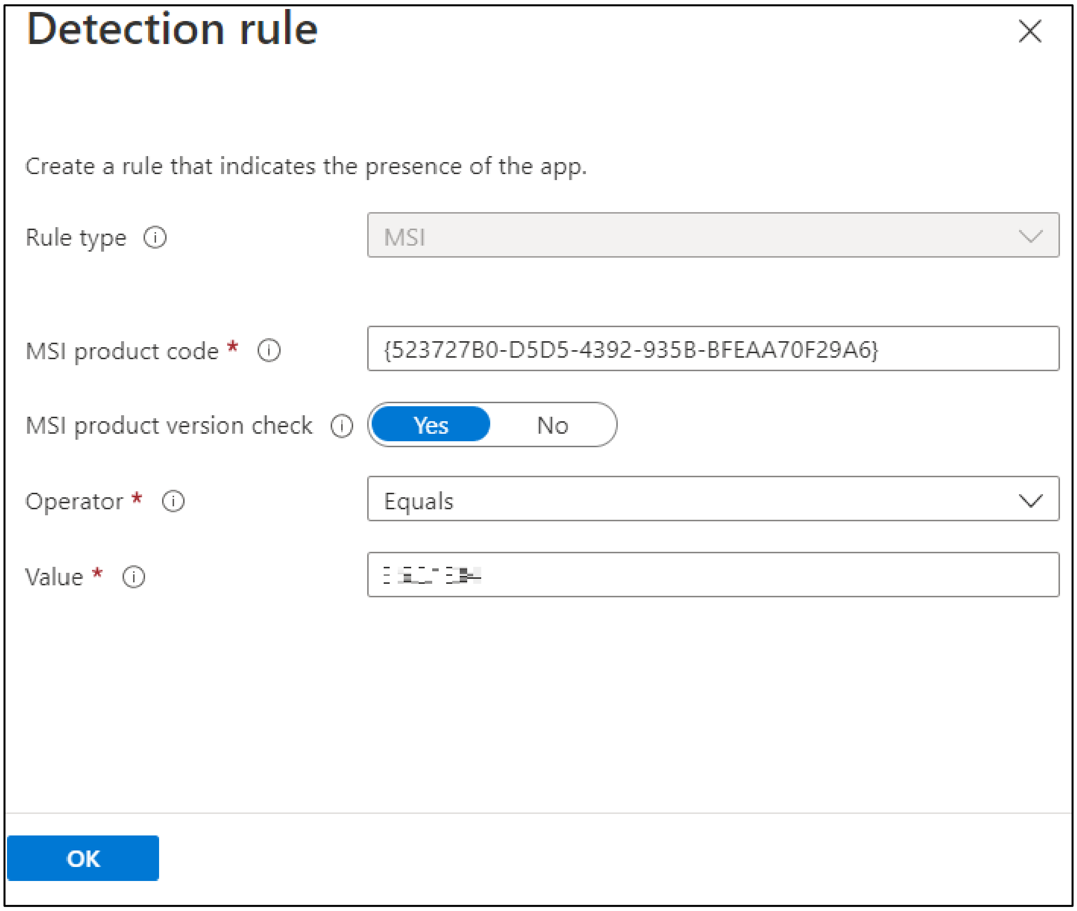
Rules format * ⓘ Manually configure detection rules

Type	Path/Code
MSI	{523727B0-D5D5-4392-935B-BFEAA70F29A6}

Detection rule window appears. Perform the following steps:

i. In the **Value** field, enter the **latest Build number** as mentioned in the CRN.

ii. Click **OK**.



Detection rule

Create a rule that indicates the presence of the app.

Rule type: MSI

MSI product code *: {523727B0-D5D5-4392-935B-BFEAA70F29A6}

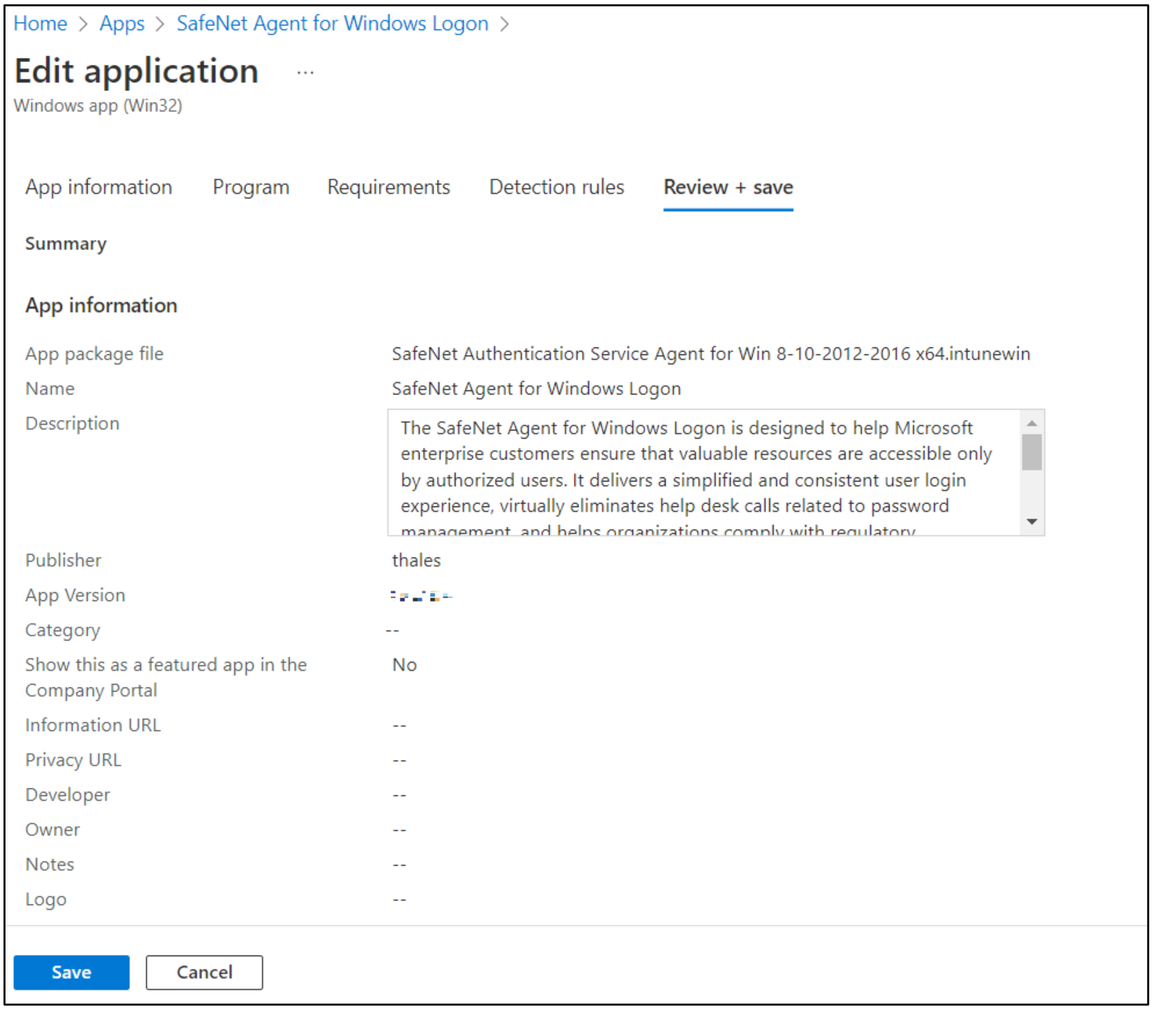
MSI product version check: Yes

Operator *: Equals

Value *: [illegible]

Click **Review + save**.

9. Under the **Review + save** tab, click **Save**.



Summary

App information

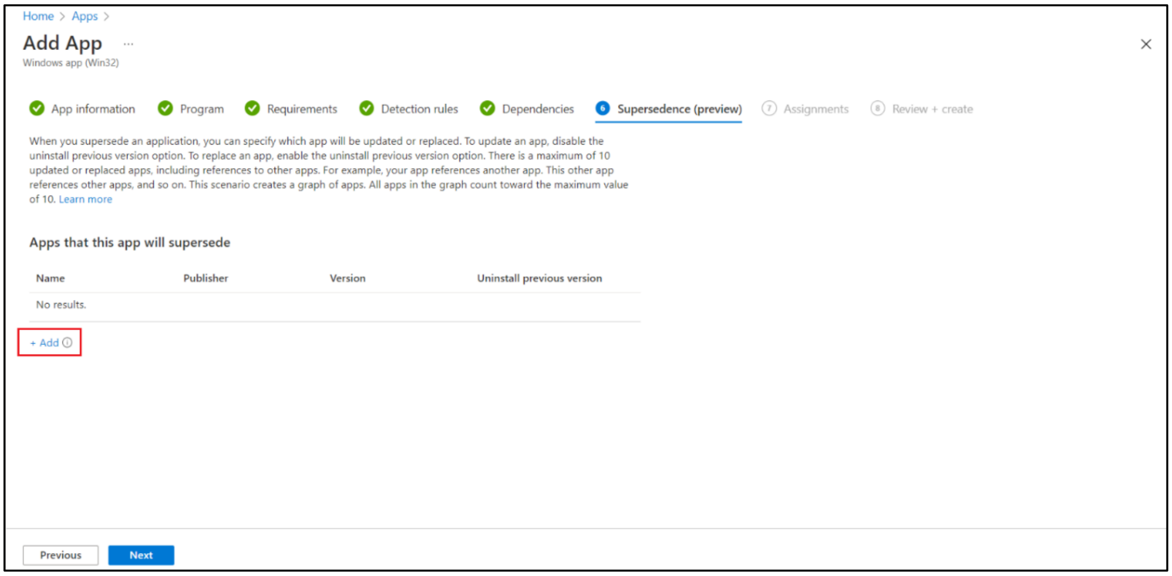
App package file	SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64.intunewin
Name	SafeNet Agent for Windows Logon
Description	The SafeNet Agent for Windows Logon is designed to help Microsoft enterprise customers ensure that valuable resources are accessible only by authorized users. It delivers a simplified and consistent user login experience, virtually eliminates help desk calls related to password management, and helps organizations comply with regulatory
Publisher	thales
App Version	[redacted]
Category	--
Show this as a featured app in the Company Portal	No
Information URL	--
Privacy URL	--
Developer	--
Owner	--
Notes	--
Logo	--

After performing the above steps, SafeNet Agent for Windows Logon will be upgraded to its latest version. **WLA will not be installed on the newly added devices through the upgrade process**.

> **IMPORTANT:** For an ongoing upgrade, you must wait until all the devices are successfully upgraded before installing the agent on the newly added devices.

To install the SafeNet Agent for Windows Logon on newly added devices, perform the following steps.

1. Perform all the steps in Creating an IntuneWin package.
2. Perform all the steps in Deploying the IntuneWin package, except Step 11.
   i. In the **Supersedence (preview)** tab, perform the following steps:
      – Click **Add**.

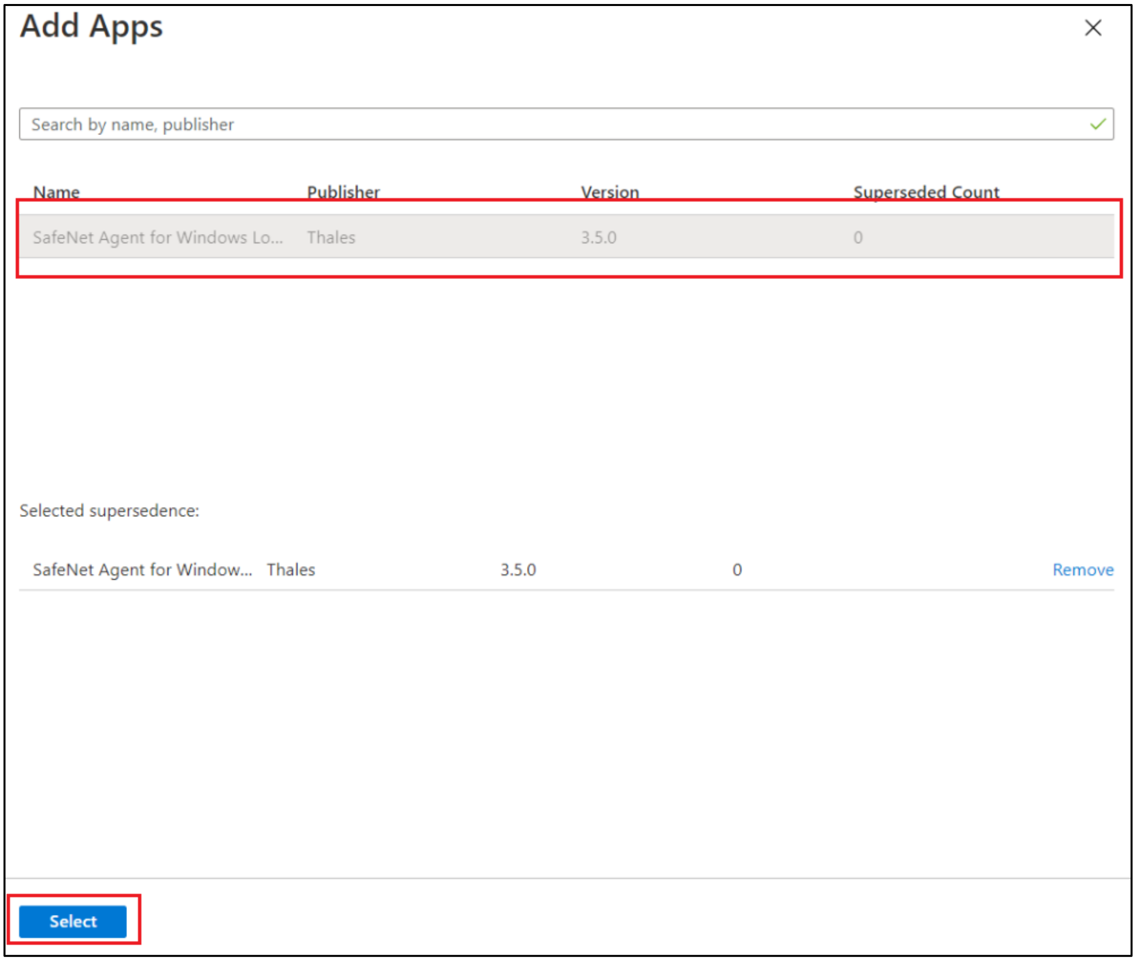


When you supersede an application, you can specify which app will be updated or replaced. To update an app, disable the uninstall previous version option. To replace an app, enable the uninstall previous version option. There is a maximum of 10 updated or replaced apps, including references to other apps. For example, your app references another app. This other app references other apps, and so on. This scenario creates a graph of apps. All apps in the graph count toward the maximum value of 10. Learn more

Apps that this app will supersede

Name	Publisher	Version	Uninstall previous version
No results.			

The **Add Apps** window appears. Select the app and then click **Select**.



Name	Publisher	Version	Superseded Count
SafeNet Agent for Windows Lo...	Thales	3.5.0	0

Selected supersedence:

SafeNet Agent for Window...	Thales	3.5.0	0	Remove

– Click **Next**.

The latest app will be successfully installed on the newly added devices.

CHAPTER 6: Troubleshooting and Advanced Configurations

In this chapter, you will learn to troubleshoot and resolve the following types of a problem quickly and effectively. First, you need to understand how to approach the issue by discovering the cause of the problem. Then, you will learn to fix the issue. For further assistance, contact Thales Customer Support.

Remote Users with Depleted Off-line Authentication Store

The following steps must be taken if the emergency password is enabled and the offline authentication store is empty, resulting in the user being unable to log in to their workstation:

1. The user contacts the SafeNet server Administrator/Operator.
2. The SafeNet server Administrator/Operator logs in to the SafeNet server Manager, finds the user on the **Secured Users** tab, and makes note of the emergency password.
3. The SafeNet server Administrator/Operator provides the user with the emergency password.
4. The user logs in to their workstation using the emergency password.
5. The user establishes a VPN connection to the network.
6. The user launches the SafeNet Windows Logon Agent Manager and performs a manual replenish with their SafeNet credentials to restore their offline authentication store. Do not attempt to replenish with the emergency password, as this will fail.
7. The user may now log in with their SafeNet credentials while being offline.

Remote Users Who Lost or Forgot Token

The following steps must be taken if the emergency password is enabled and the workstation is unable to communicate with the SafeNet server at the time of authentication:

1. The user contacts the SafeNet server Administrator/Operator.
2. The SafeNet server Administrator/Operator logs in to the SafeNet server Manager, finds the user on the **Secured Users** tab and makes note of the emergency password.
3. The SafeNet server Administrator/Operator provides the user with the emergency password.
4. The user logs in to their workstation using the emergency password.

5. The SafeNet server Administrator/Operator assigns the user a new token or enables a SafeNet server static password.
6. The user establishes a VPN connection to the network.
7. The user launches the SafeNet Windows Logon Agent Manager and performs a manual replenish with the new token or SafeNet static password.
8. The user may now log in with their SafeNet credentials while being offline.

Refining Administrator Group Exclusions

During the installation of the SafeNet Agent for Windows Logon, an option can be enabled to exempt the **Local** and **Domain Administrators** groups from performing SafeNet authentication. In certain cases, restrictions may only be needed for the **Local Administrators** group or the **Domain Administrators** group rather than all **Administrator** groups. The following steps can be completed to achieve the same:

1. During the installation of the SafeNet Agent for Windows Logon, clear the option **Exempt Local and Domain Administrator groups from SafeNet Authentication Service Authentication**.
2. Log in to the SafeNet Windows Logon protected workstation with SafeNet credentials and then with Microsoft credentials.
3. Right-click the SafeNet Windows Logon Agent Manager and select **Run as administrator**.
4. Click **Policy** tab. In the **Group Authentication Exceptions** section, select **Only selected groups will bypass SafeNet**. Add the administrator group(s) to be excluded from SafeNet authentication.
5. Log out and log in again.

Configuring Num Lock Settings

The **Num Lock** setting can be controlled from the registry. If required, perform the following steps:

1. Click **Start > Run**.
2. In the **Open** box, type *regedit*, and click **OK**.
3. In the registry, open one of the following:
    - For a single user: `HKEY_CURRENT_USER > Control Panel > Keyboard`
    - For all users: `KEY_USERS| .Default > Control Panel > Keyboard`
4. Edit the string value named *InitialKeyboardIndicators*, as follows:
    - Set to **0** to set NumLock **OFF**.
    - Set to **2** to set NumLock **ON**.

CHAPTER 7: Running the Solution

The login and authentication flow remains the same for both versions of the credential provider. The display of login tiles differ though; while V1 creates a new tile in the login screen, for V2, windows attaches credential provider to the same user account and does not create a separate tile.

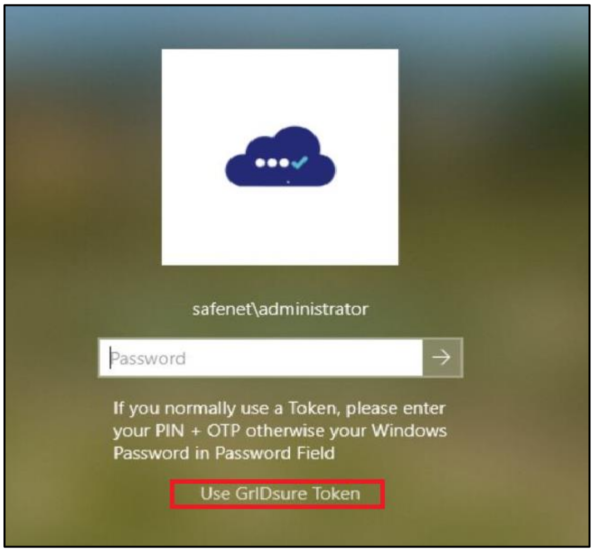
1. Microsoft Credential Provider Tile Version 1
2. Microsoft Credential Provider Tile Version 2

NOTE: To view the supported operating systems, click **here**.

Credential Provider Version 1

The following displays the login screen for different user types:

1. Admin Login Screen:



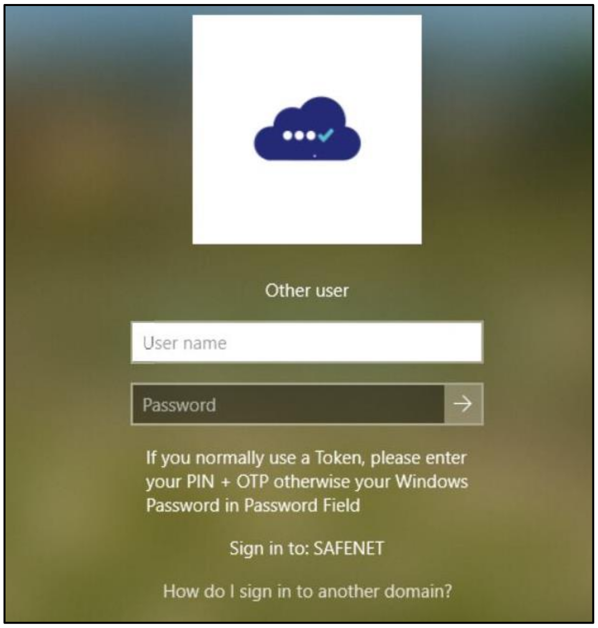
safenet\administrator

Password

If you normally use a Token, please enter your PIN + OTP otherwise your Windows Password in Password Field

Use GrIDsure Token

2. User Login Screen:



Other user

User name

Password

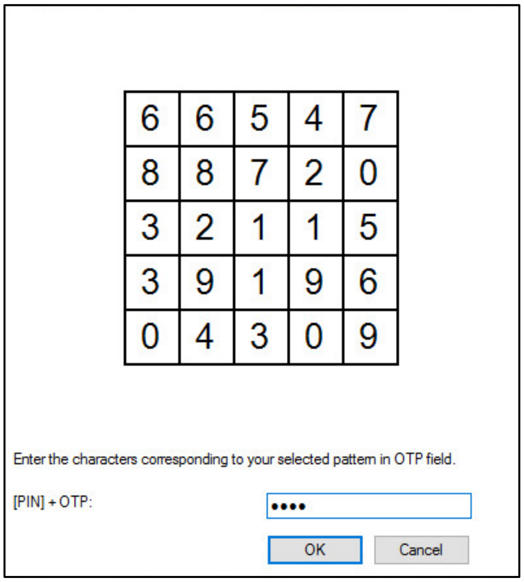
If you normally use a Token, please enter your PIN + OTP otherwise your Windows Password in Password Field

Sign in to: SAFENET

How do I sign in to another domain?

ii. Enter Username and SafeNet Password (only password, if you are an administrator) and press **Enter** (or click the forward arrow sign).

> **NOTE:** If the selected token type is *GrIDsure*, enter the **Username** (keeping the Password field blank), and click **Use GrIDsure Token** link. If the selected token type is *Challenge-Response*, enter the **Username** (keeping the Password field blank), and press **Enter** (or click the forward arrow sign). The following window will be displayed, that will help the user to complete the authentication by the selected token type.

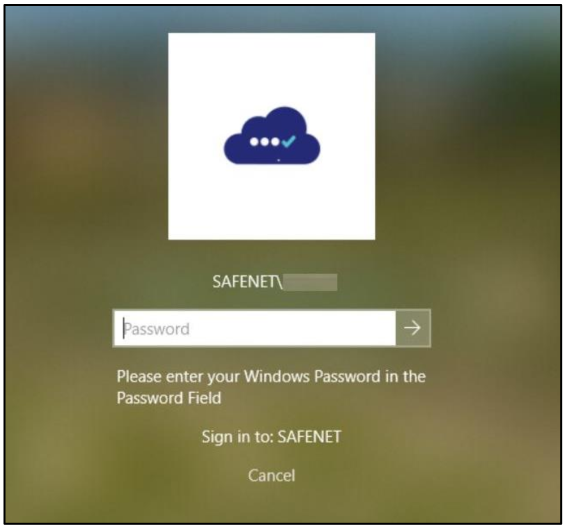


6	6	5	4	7
8	8	7	2	0
3	2	1	1	5
3	9	1	9	6
0	4	3	0	9

Enter the characters corresponding to your selected pattern in OTP field.

[PIN] + OTP: ••••

iii. Enter AD or LDAP password to login:



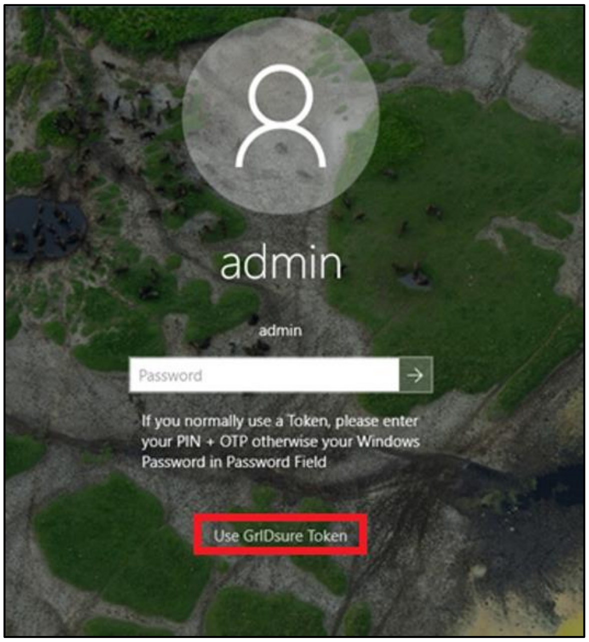
SAFENET\[redacted]

Please enter your Windows Password in the Password Field

Credential Provider Version 2

The following displays the login screen for different user types:

1. Admin Login Screen:

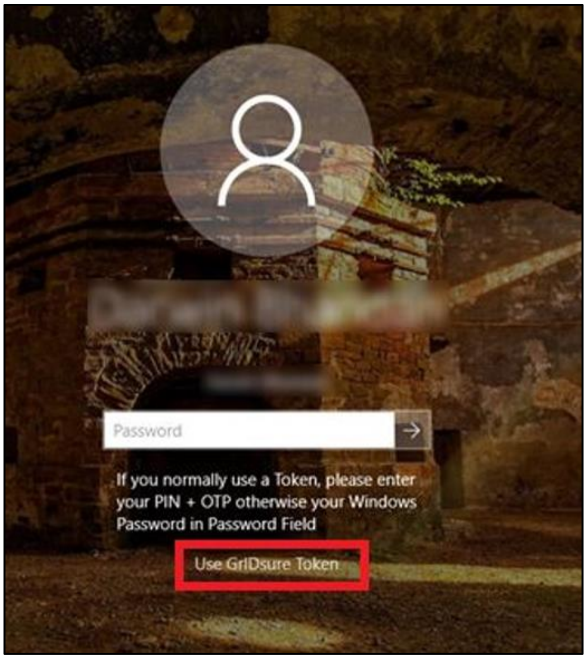


admin

admin

If you normally use a Token, please enter your PIN + OTP otherwise your Windows Password in Password Field

2. User Login Screen:



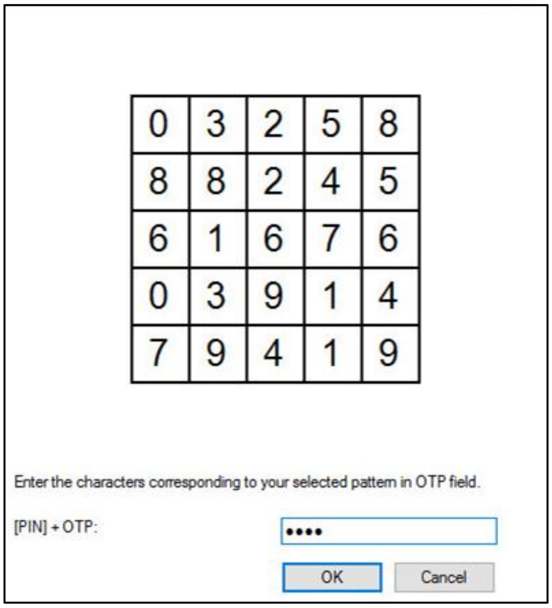
[redacted]

[redacted]

If you normally use a Token, please enter your PIN + OTP otherwise your Windows Password in Password Field

i. Enter the SafeNet Password, and press **Enter** (or click the forward arrow sign).

> **NOTE:** If the selected token type is *GrIDsure*, keep the Password field blank, and click **Use GrIDsure Token** link. If the selected token type is *Challenge-Response*, keep the Password field blank and press **Enter** (or click the forward arrow sign). The following window will be displayed, that will help the user to complete the authentication by the selected token type.

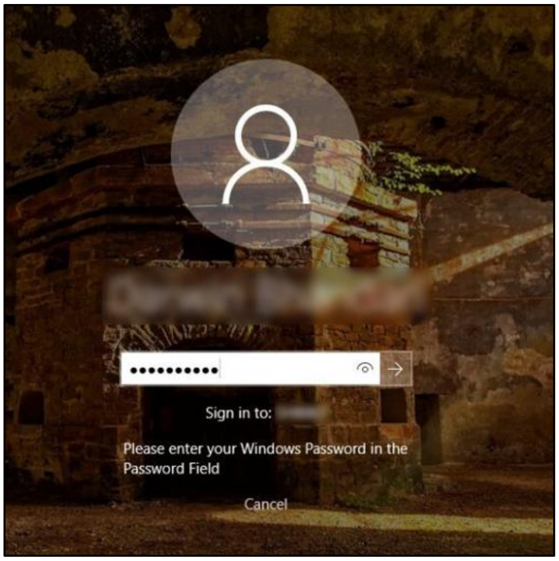


0	3	2	5	8
8	8	2	4	5
6	1	6	7	6
0	3	9	1	4
7	9	4	1	9

Enter the characters corresponding to your selected pattern in OTP field.

[PIN] + OTP: ••••

ii. Enter AD or LDAP password to login:



[redacted]

••••••••••••

Sign in to: [redacted]

Please enter your Windows Password in the Password Field