THALES

SafeNet Agent for Windows Logon 3.6.2

INSTALLATION AND CONFIGURATION GUIDE

Document Information

Product Version	3.6.2
Document Part Number	007-000282-002 Rev. T
Release Date	September 2023

Trademarks, Copyrights, and Third-Party Software

© 2023 THALES. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and affiliates and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Disclaimer

All information herein is either public information or is the property of and owned solely by Thales and/or its subsidiaries and 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 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 publicly accessible 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 7

Audience 7
Related Documents 7
Support Contacts 7
Customer Support Portal 7
Telephone Support 8
Email Support 8

CHAPTER 1: Overview 9

System Requirements 9
* Limitations for Azure AD joined machines 10
Windows Logon Agent – Authentication Methods 10
Domain/Workgroup Authentication 10
Offline Authentication 11
RDP Authentication 12

CHAPTER 2: Installing, Configuring, Upgrading, and Uninstalling the agent 14

Prerequisites 14
Installing the agent 14
Interactive Installation 14
Silent Installation 19
Configuring the Settings 20
Realm Stripping Settings 20
Configuring Transport Layer Security 20
Push Authentication 21
Configuration Management 21
Upgrading the agent 35
Silent Upgrade 35
Uninstalling the agent 35
Using the Windows Control Panel 35
Silent Uninstall 35

CHAPTER 3: Deploying the agent via Group Policy Object 36

Configuring the ADMX and ADML Settings 36
Deploying the agent 37
Creating a Distribution Point 38
Creating a Group Policy Object 38
Adding ADMX and ADML File to Group Policy Object Editor 39
Deploying the MSI 39
Registry Settings 40

CHAPTER 4: Deploying the agent via Intune 46

This section describes the steps to deploy the agent via **Intune**. 46
Prerequisites 46

Creating an IntuneWin package 46
Creating an IntuneWin package of WLA Installer 46
Creating an IntuneWin package for configuring the Settings 47
Deploying the IntuneWin package 48
Deploying the IntuneWin package of WLA Installer 48
Deploying the IntuneWin package for configuring the Settings 54
Deploying PowerShell Script to configure the Settings 57
Upgrading SafeNet Agent for Windows Logon 60

CHAPTER 5: Deploying the agent via Microsoft Endpoint Configuration Manager 66
Prerequisites 66
Installing the agent 66
Creating an Application in Microsoft Endpoint Configuration Manager 66
Distributing the content (Application) 68
Deploying the application into client machines 70
Pushing computer policy to the client machines 73
Configuring the Registry Settings 74
Copy the SCCM-Deployment folder from the downloaded agent package 75
Creating an Application in Microsoft Endpoint Configuration Manager 75
Distributing the content (Application) 80
Deploying the application into client machines 80
Pushing computer policy to the client machines 80
Uninstalling the agent 80
Deleting the deployment from Device Collection 80
Deploying the application into client machines for uninstallation 82
Pushing computer policy to the client machines 83
Upgrading the agent 83
Creating an application with new agent version in Microsoft Endpoint Configuration Manager 83
Creating Supersedence relationship 85
Update Detection method for the upgrade 86
Distributing the content (Application) 88
Deploying the application into client machines 88
Pushing computer policy to the client machines 88

CHAPTER 6: Troubleshooting and Advanced Configurations 89
Remote Users who Lost or Forgot Token 89
Refining Administrator Group Exclusions 90
Configuring Num Lock Settings 90

CHAPTER 7: Running the Solution 91

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 3.6.2: 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

SafeNet Agent for Windows Logon is a lightweight software that is installed on the Windows machines to augment logon security by invoking Multi-factor Authentication (MFA). It ensures that the valuable resources are accessible only by authorized users. The agent also protects desktop applications and processes which use CredUI.

The use of MFA in addition to AD authentication adds another layer of security. The agent provides a secured and consistent logon experience to the end users of Windows machines.

System Requirements

Software Prerequisites	> Microsoft .NET 4.5 or later
Communication Protocols	> HTTP > HTTPS • SSL 2.0 and above • TLS 1.0 and above
Network Port	> TCP Port 80 (HTTP) or 443 (HTTPS)
Azure Support	> Azure AD* > Hybrid Azure AD
Operating Systems	> Windows 10 > Windows 11 > Windows Server 2012 R2 > Windows Server 2016 > Windows Server 2019 > Windows Server 2022
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)

NOTE: The agent is compatible with the Microsoft native FDE tool, **BitLocker**.

* 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.

Windows Logon Agent – Authentication Methods

Authentication is a process to verify that the credentials presented are authentic. The agent offers following authentication methods:

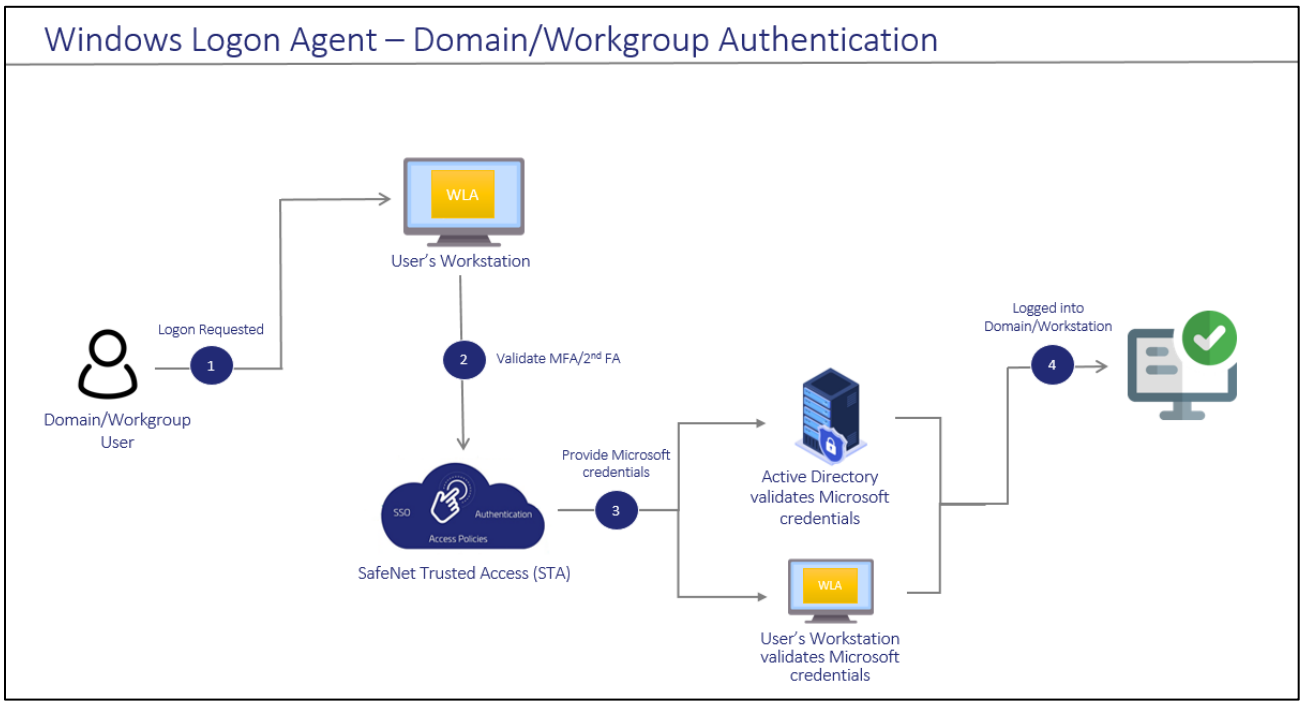
> Domain/Workgroup Authentication

> Offline Authentication

> RDP 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 illustrates the user authentication while accessing the domain or local workstation login:



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

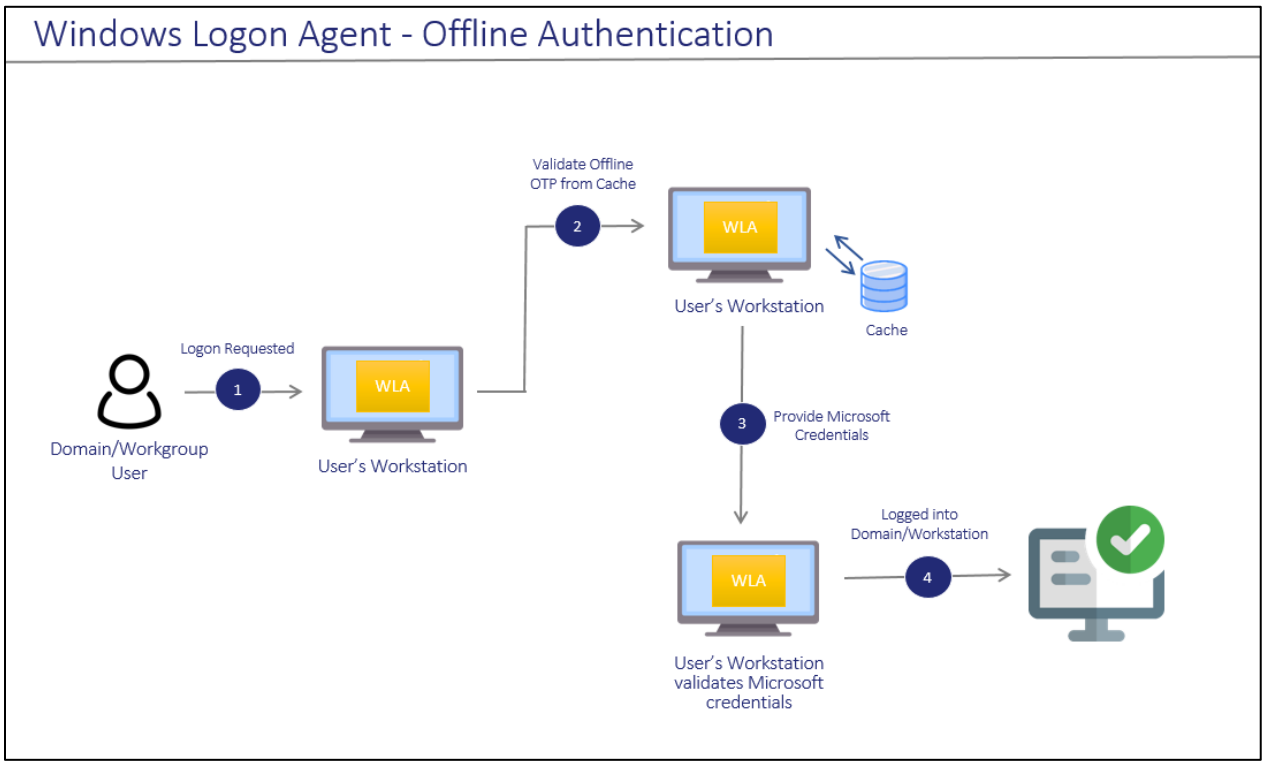
The SafeNet Agent for Windows Logon supports offline authentication, which enables users to log on to Windows machines securely using a SafeNet OTP when there is no connection to the SafeNet server.

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.

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

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

The following flow diagram illustrates the user authentication while accessing the workstation in offline mode:

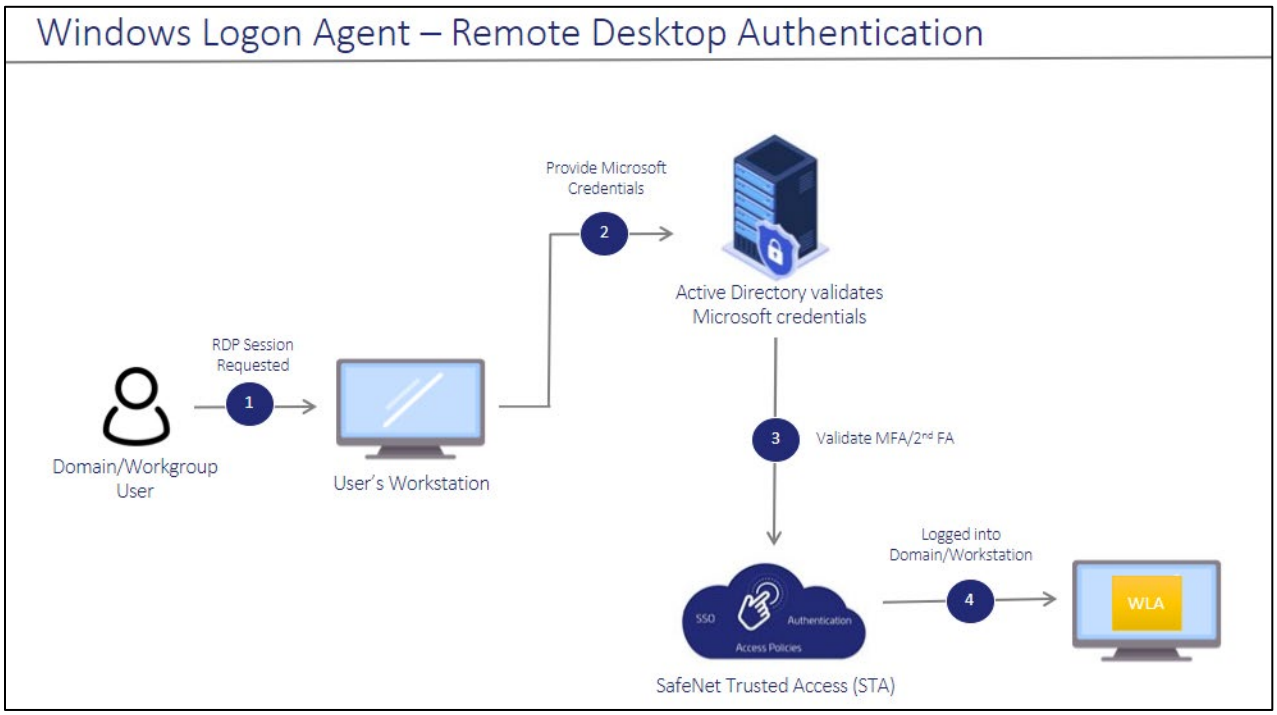


1. After invoking the workstation logon, the offline user is presented with the agent login screen.
2. If Multi-Factor Authentication is required, the user enters the credential of the supported second factor authentication, for example, OTP. The entered credentials are then verified by the offline authentication 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.

RDP Authentication

The following describes the RDP authentication flow for different scenarios when a user tries to access the remote machine:

Management Console Setting	**RDP Scenarios**		
Allow Outgoing RDP connection without OTP	Agent installed on remote machine but not on local machine	Agent installed on both local and remote machine	Agent installed on local machine but not on remote machine
Enabled	Microsoft credentials > SafeNet OTP	Microsoft credentials > SafeNet OTP	Microsoft credentials
Disabled	Microsoft credentials > SafeNet OTP	SafeNet OTP of local machine > Microsoft credentials of remote machine > SafeNet OTP of remote machine	SafeNet OTP of local machine > Microsoft credentials of remote machine



1. After invoking the RDP session, the user is presented with the RDP prompt.
2. The user enters the Microsoft password.
3. If the Microsoft credentials are valid, 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.
4. If the SafeNet credentials are valid, the user is logged on to the WLA installed machine.

CHAPTER 2: Installing, Configuring, Upgrading, and Uninstalling the agent

This section contains the instructions about the following:

> Installing the agent

> Configuring the Settings

> Upgrading the agent

> Uninstalling the agent

You can also deploy the agent on multiple machines using either GPO or Intune.

Prerequisites

> TCP port 80 or 443 must be open between the agent and the SafeNet server.

> Administrative rights for installing the agent on the Windows machine.

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

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

Installing the agent

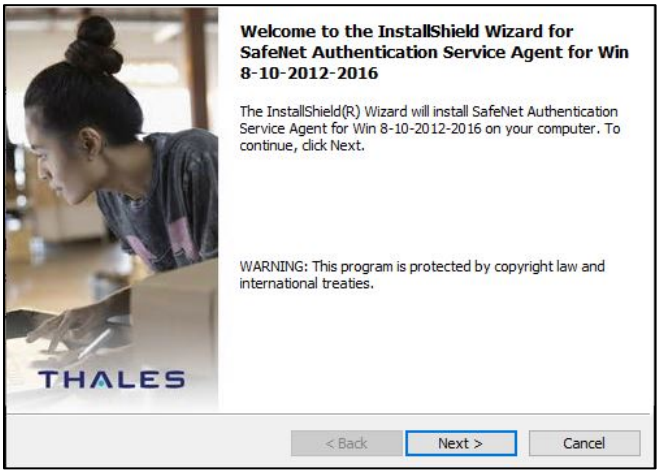
Following are the ways to install the agent:

Interactive Installation

Perform the following steps to install the agent on windows machine (with administrative privileges) using the **installer**:

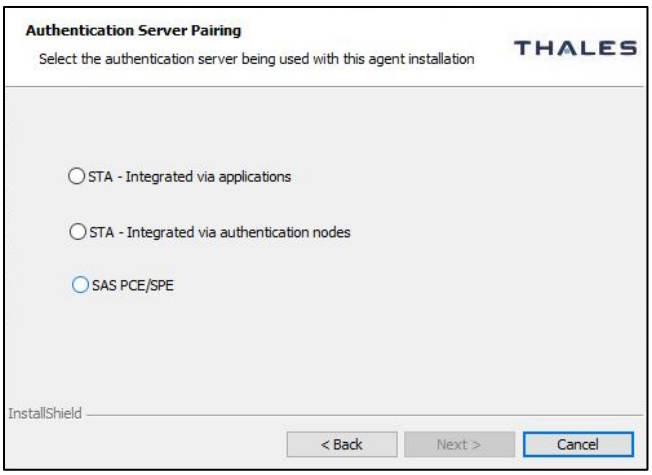
1. Run one of the following installers from the downloaded package (as applicable):
    - *SafeNet Authentication Service Agent for Win 8-10-2012-2016 x86.exe (32-bit)*
    - *SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64.exe (64-bit)*

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

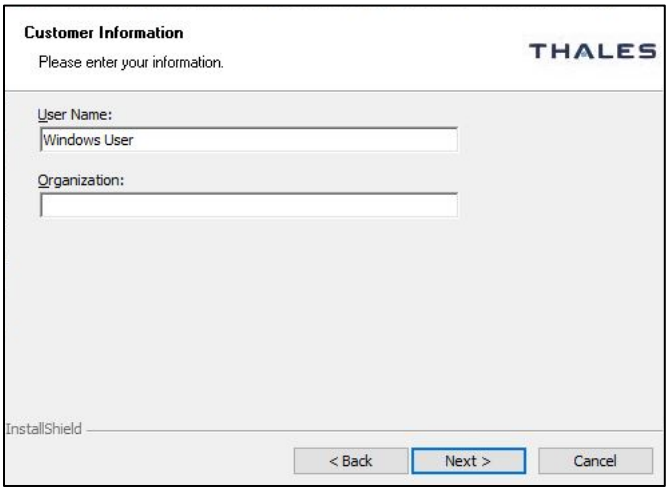


3. On the **License Agreement** window, read the software license agreement and to proceed, select **I accept the terms in the license agreement** option, and click **Next**.

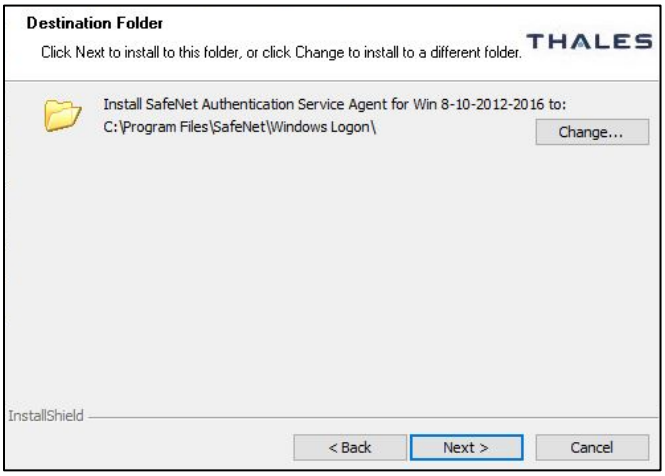
4. On the **Authentication Server Pairing** window, select **SAS PCE/SPE** authentication server type, and click **Next**.



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**.

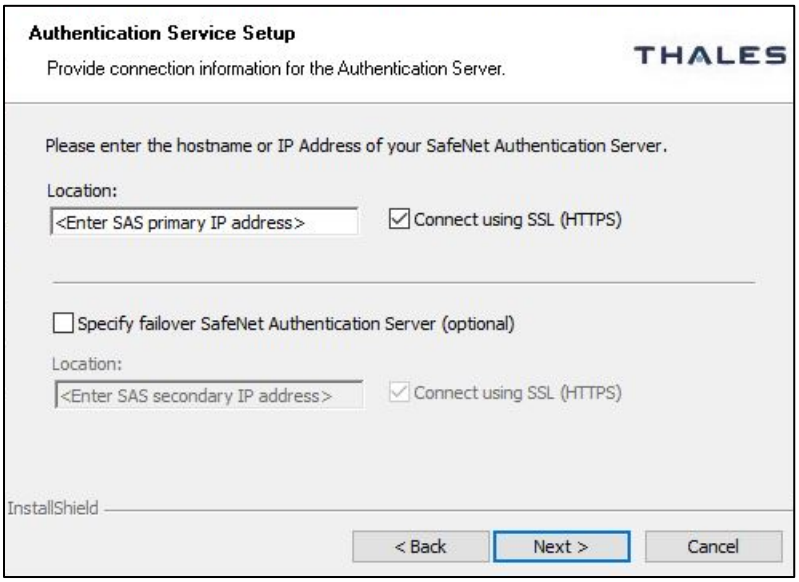


6. On the **Destination Folder** window, perform one of the following steps:
   a. To accept the default installation destination folder, click **Next**.
   b. To change the installation folder, other than the default one, click **Change**, and then browse to locate and select the required folder.
   c. Click **Next**.



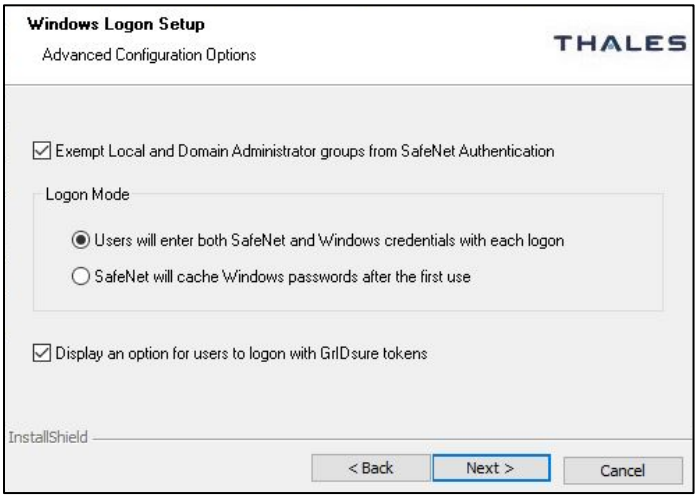
7. On the **Authentication Service Setup** window, provide the following information, and click **Next**.

Location	Enter the hostname or IP address of the primary SafeNet server. The port number for HTTPS and HTTP is **443** and **80** respectively.
Connect using SSL (HTTPS)	Select this check box if the SafeNet server is configured to accept the incoming SSL connections. **NOTE:** We strongly recommend to use 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 check box if the failover SafeNet server is configured to accept incoming SSL connections.

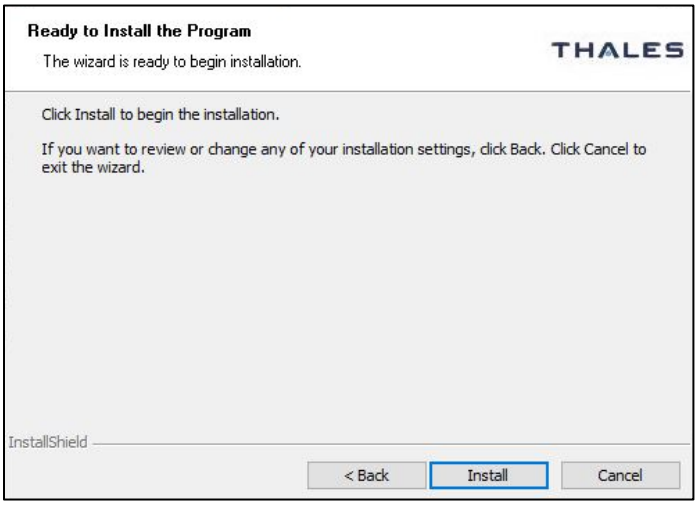


8. On the **Windows Logon Setup** window, provide the following information, and click **Next**.

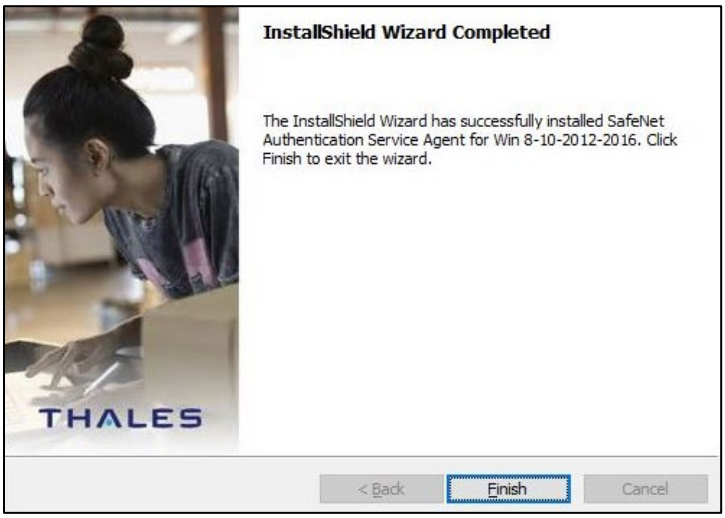
Exempt Local and Domain Administrator groups from SafeNet Authentication	Select this check box to allow administrators to log on without providing SafeNet credentials.
Logon Mode	Select one of the following logon modes: • User will enter both SafeNet and Windows credentials with each logon. • SafeNet 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 enable or disable the **Use a grid pattern** link on the login screen.



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



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



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.

Launch the following SafeNet Windows Logon msi installation package from the command line:

```
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, 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.

If any of 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. **These parameters cannot be specified during agent upgrades**.

Option	Description	Value(s)
TOKENVALIDATORLOCATION	Defines the Primary SafeNet server	IP address or Hostname or FQDN. Default value: **localhost**
TOKENVALIDATORLOCATION2	Defines the Secondary SafeNet server	IP address or Hostname or FQDN. Default value: **Disabled**

Option	Description	Value(s)
USESSL	Enable SSL to Primary SafeNet server (requires certificate)	Set **USESSL=""** to disable the SSL. Default value: **Enabled**
EXEMPTADMINS	Logon mode of operation	**1**: exempts administrators from using MFA **0**: everybody must use MFA Default value: **Dual Logon (0)**
LOGONMODE	Logon mode of operation	**0**: both the Windows password and MFA is required **1**: for Microsoft password caching. Windows password is hidden (cached) Default value: **Dual Logon (0)**
AGENTSTATUS	To enable or disable the agent	**1**: Enable the agent **0**: Disable the agent Default Value: **0**

Configuring the Settings

This section describes configuration tasks related to the agent.

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.

Alternatively, this feature can also 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 on the agent, 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+.

> **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 above.

Configuration Management

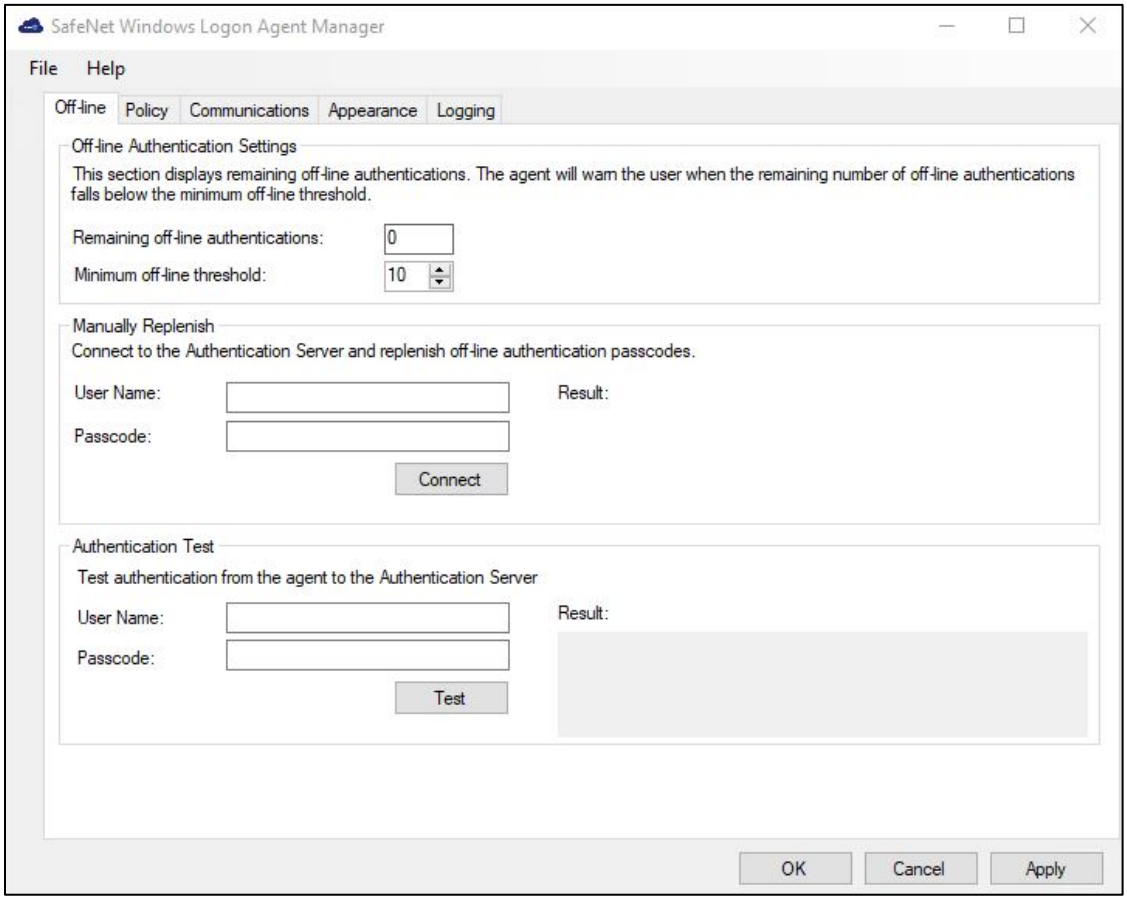
Use **SafeNet Windows Logon Agent Manager** to configure various options available within the agent.

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.

Off-line Tab

The **Off-line** tab deals with the following end-user offline authentication settings:

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



Off-line Authentication Settings

The agent allow users to log in to their workstations when the SafeNet server is not available.

Option	Description	Value
Remaining off-line authentications	The number of SafeNet authentication available before the user can authenticate against the SafeNet server or perform a manual replenish. To modify the default value of offline authentications, navigate to **Policy > Token Policies > Token Passcode Processing Policy** of the SafeNet server.	Default: **Configured value in SafeNet server** Range: **2 - 500**
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.	Default: **10** Range: **5 - 99**

Manually Replenish

The offline store is automatically replenished when a user returns and logs in to the corporate network.

If the offline store expires while the user is still at a remote location, the **Manually Replenish** option allows admin user to refill the user's offline authentication store. To replenish an offline authentication store manually, the administrator performs the following steps:

1. Establish a VPN connection to the corporate network.
2. Open the SafeNet Agent for Windows Logon Agent Manager.
3. Enter the user's SafeNet credentials into the **Passcode** field and click **Connect**.
4. The agent contacts the SafeNet server to verify the logon credentials. If the credentials are valid, the offline authentication is restored; otherwise, the user will receive a warning message to retry the authentication attempt.

Authentication Test

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

Policy Tab

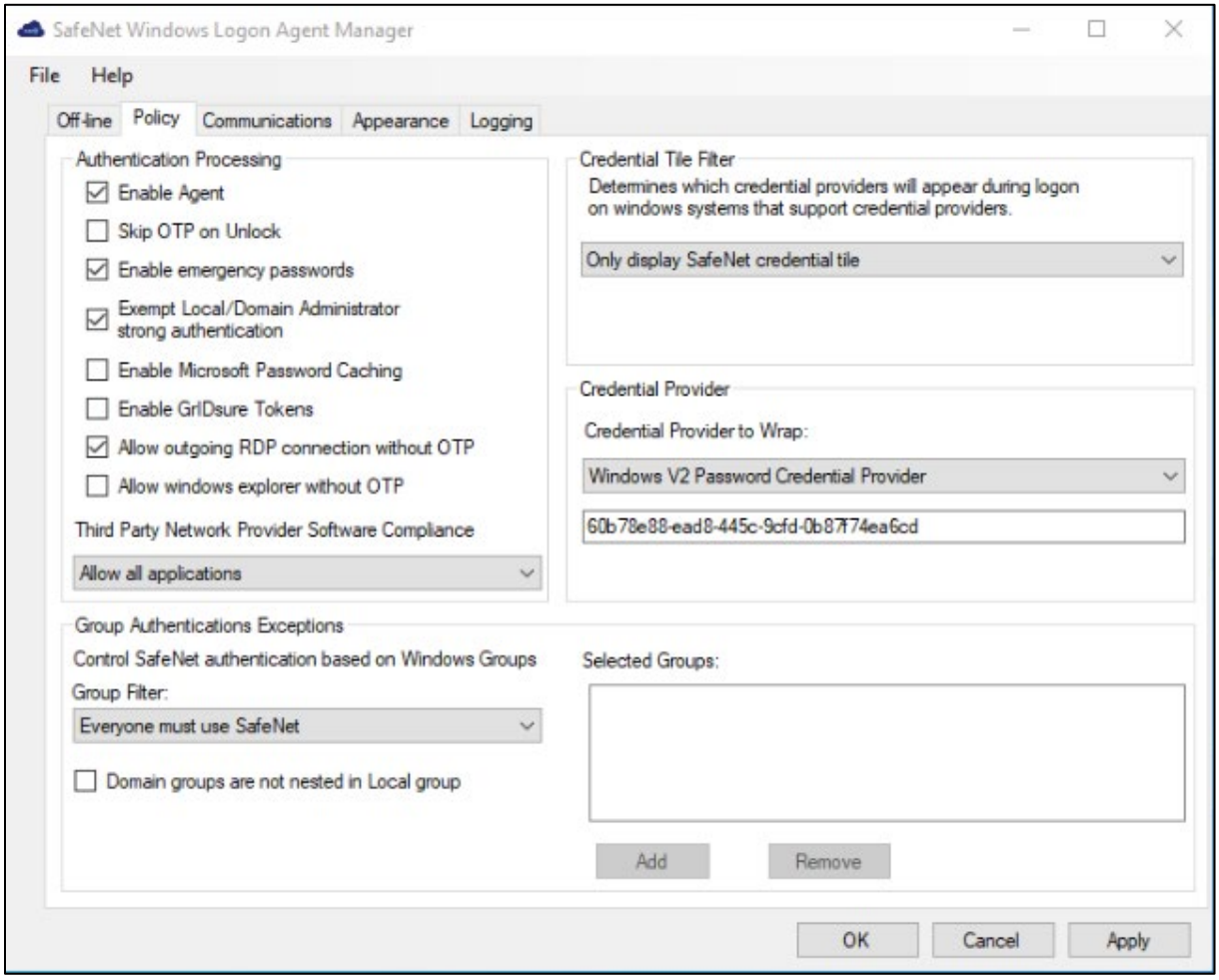
The **Policy** tab allows SafeNet authentication exclusions to be applied to the agent.

> Authentication Processing

> Credential Tile Filter

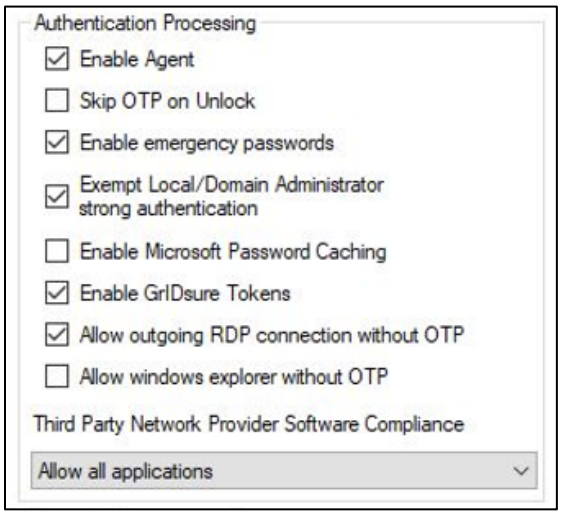
> Credential Provider

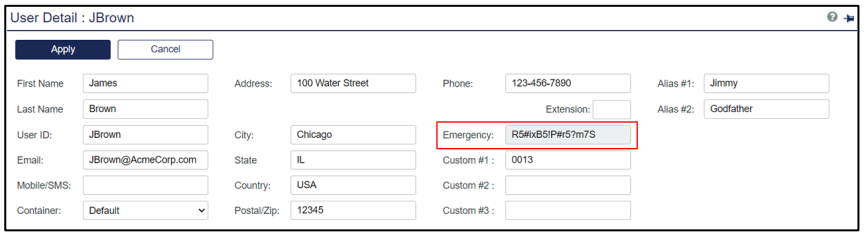
> Group Authentication Exceptions



Authentication Processing

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



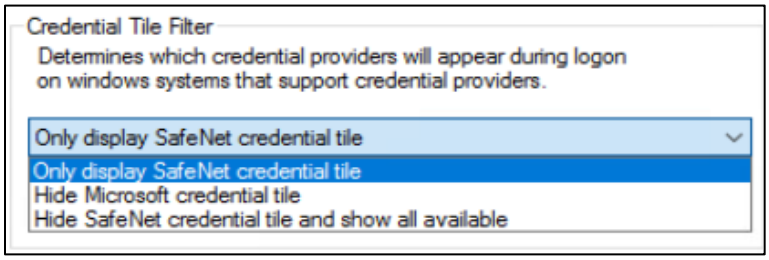
Option	Description	Default Setting
Enable Agent	Used to enable or disable the agent.	Enabled
Skip OTP on Unlock	Allows the administrators to enable or disable the SafeNet 2FA for last logged on user on system unlock. The functionality extends to sleep and hibernate modes, which means that if the **Skip OTP on Unlock** check box is selected, and the system enters sleep or hibernate mode, the agent does not prompt for an OTP, and instead logs in successfully using only the AD credentials.	Disabled
Enable emergency passwords	Allows a user to authenticate using an emergency password in offline mode, typically when off-line authentications are exhausted (**Remaining off-line authentications = 0**). This password can only be used until the workstation regains contact with the SafeNet server. Each user has a unique emergency password, which exists on the **Secured Users** tab of the SafeNet server. After each online authentication, its value gets changed. 	Enabled
Exempt Local/Domain Administrator strong authentication	Allows the **Local** and **Domain Administrator** groups to be exempt from SafeNet authentication during login. **NOTE:** This feature does not work with pure Azure AD joined machines for domain admins. However, this feature works as expected for the local admins.	Determined during agent installation
Enable Microsoft Password Caching	Used to enable or disable the **Microsoft Password Caching** mode. **Microsoft Password Caching mode**: For accessing a WLA protected machine, each user authenticates with OTP first, followed by the Microsoft password. In this mode, the user is prompted for their Microsoft password only once for their first log in. Subsequently, the agent caches the Microsoft password until its expiry or change.	

Option	Description	Default Setting
	NOTE: This feature does not work for the following: **>** Domain admin users **>** Users authenticating via the **Use a grid pattern** link. To use this feature for GrIDsure token, enter **"g" character** in the **Password** field.	
Enable GrIDsure Tokens	Used to enable or disable the **Use a grid pattern** link displayed on the login screen.	
Allow outgoing RDP connection without OTP	Enables SafeNet authentication to be bypassed while making an outgoing RDP connection. This feature is not effective if the Microsoft parameter, **`enablecredsspsupport:i:0`**, is set to null, which controls credentials usage on the Operating System level for RDP.	Enabled
Allow windows explorer without OTP	Allows Windows explorer to run without SafeNet Authentication (bypass SafeNet OTP). It is invoked when a network path is accessed or an application is run with other user credentials.	Disabled
Third Party Network Provider Software Compliance	Select one of the following options: > **Allow all applications** (Default): Allows 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 agent and the third-party network provider software. In this case, uninstall the third-party network provider software and remove its registry entry. Before executing this operation, 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**: Allows to reset the registry key under **[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order]** to **"ProviderOrder"=" RDPNP,LanmanWorkstation,webclient "**. After selecting this option, all the registry keys will be removed, except the following: • "ProviderOrder"=" RDPNP,LanmanWorkstation,webclient "	

Option	Description	Default Setting
	• 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.	

Credential Tile Filter

The **Credential Tile Filter** determines which credential providers are allowed to display the credential tiles on the login screen.



Option	Description
Only display SafeNet credential tile	SafeNet credential tile is displayed on the login screen with the authentication flow (OTP + Microsoft password). All other (third-party) credential tiles are hidden.
Hide Microsoft credential tile	SafeNet credential and third-party credential tiles are displayed on the login screen. The Microsoft credential tile is hidden.
Hide SafeNet credential tile and show all available	Third-party and Microsoft credential tiles are displayed on the login screen. The SafeNet credential tile is hidden.

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

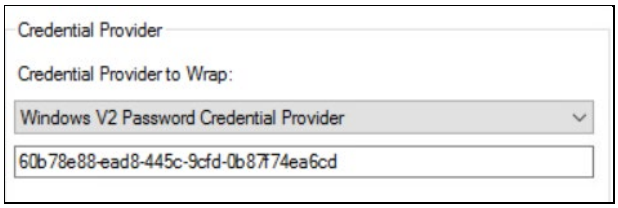
In such case, a warning will be displayed with two user-response options:

> **Yes**: removes the conflicting registry entry.

> **No**: disable the agent.

Credential Provider

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



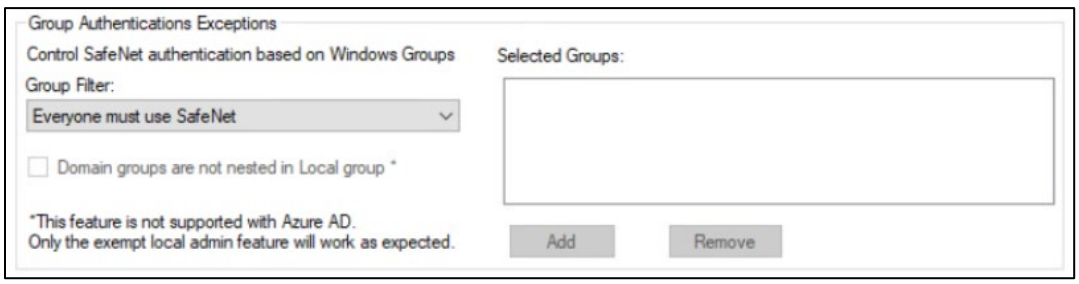
Option	Description
Credential Provider to Wrap	Allows the agent to dynamically wrap Microsoft or other third-party credential providers' GUID. > This option defaults to **Windows V2 Password Credential Provider**. The subsequent text field will auto-populate the relevant GUID. > To wrap another external (third-party) credential provider, select **Other Credential Provider** and enter its GUID in the subsequent text field. A popularly used external credential provider **ServiceNow Password Reset tool** is already configured to wrap. However, it will only be visible if ServiceNow is installed and running on the system. **NOTE**: Before uninstalling a third-party credential provider, unwrap it first.

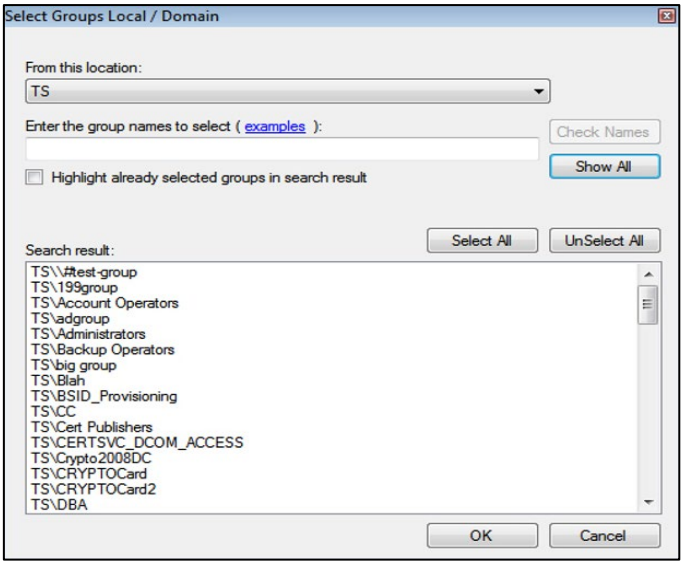
Group Authentication Exceptions

The **Group Authentication Exceptions** section allows to omit 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**

NOTE: MFA will not work (as configured) if Primary group is added in the Group Authentication Exception.

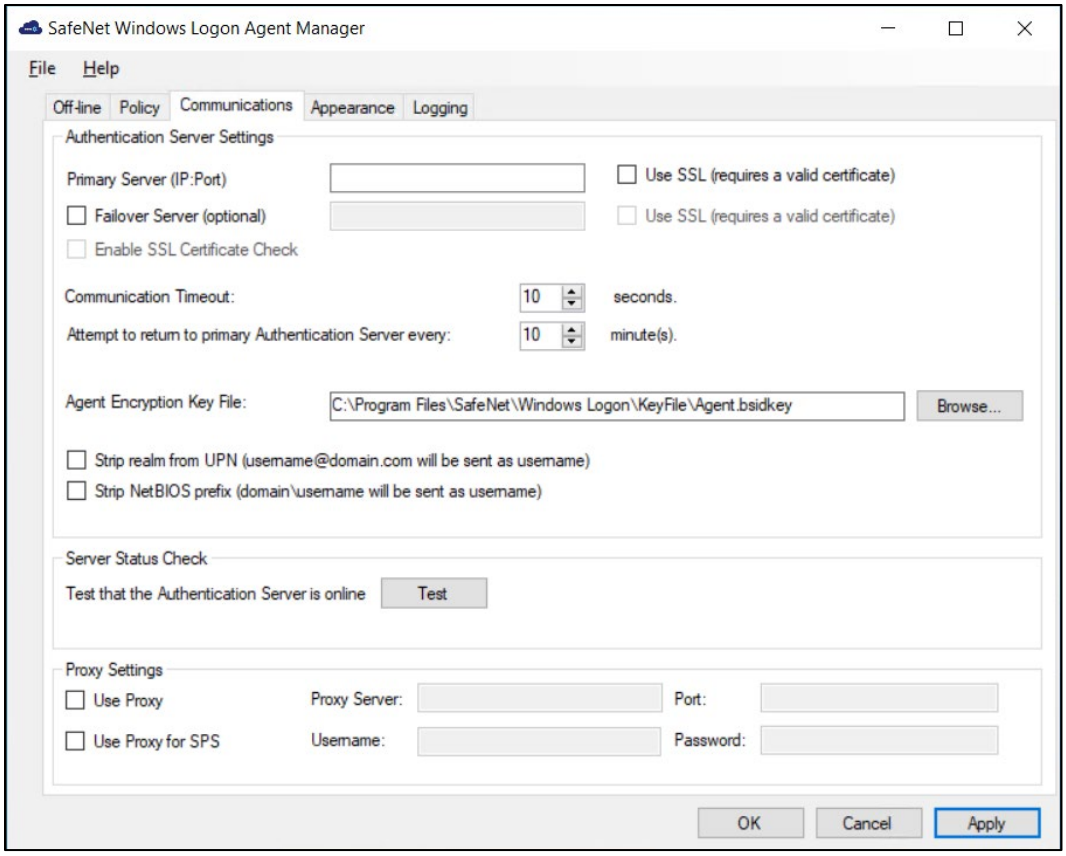


Option	Description
Group Filter	Select one of the following drop down option: > **Everyone must use SafeNet**: All users must perform SafeNet authentication. > **Only selected groups will bypass SafeNet**: All users are required to perform SafeNet authentication, except for the defined Microsoft group(s). > **Only selected groups must use SafeNet**: Users are not required to perform SafeNet authentication, except for the defined Microsoft group(s). **NOTE:** This feature does not work with pure Azure AD joined machines for domain groups. However, this feature works as expected for the local groups.
Selected Groups	Click **Add**. The **Select Groups Local / Domain** window will be displayed: > **From this location**: 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**: 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 is already configured in the exception, it will appear as a highlighted result. 

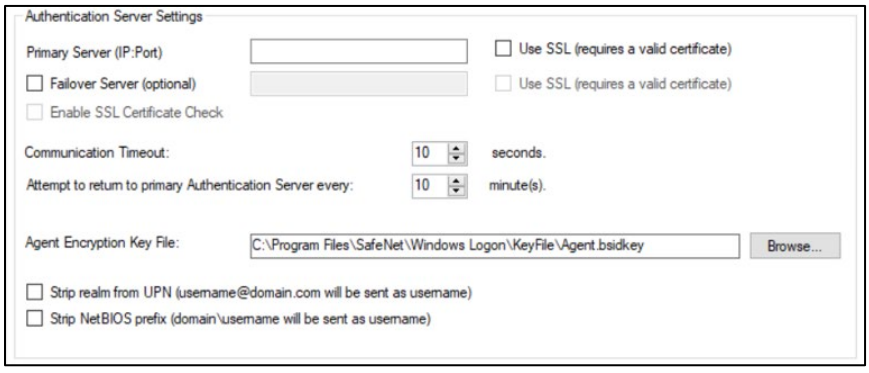
Option	Description
Domain groups are not nested in Local group	If selected, indicates that no Nested Groups (Domain groups are nested in the Local group) are present in the **Selected Groups** field. Domain lookup is skipped, which improves the login delay time.

Communications Tab

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



Authentication Server Settings



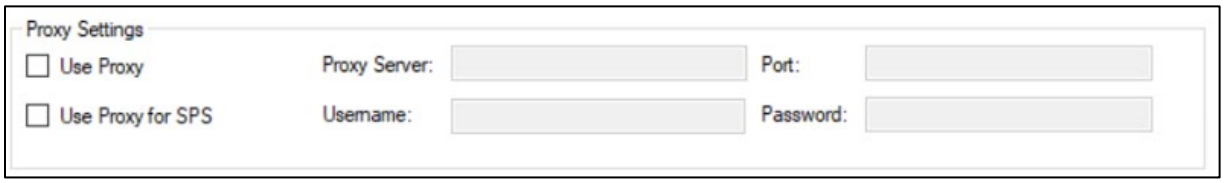
Option	Description
Primary Server (IP:Port)	Used to configure the IP address/hostname of the primary SafeNet server. Default port: **80** Alternatively, **Use SSL** check box option can also be selected. Default TCP Port for SSL Requests: **443** **NOTE**: To configure the SafeNet Agent for Windows Logon with TokenValidator Proxy (TVP), click here.
Failover Server (optional)	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:** For fresh installation, the Failover Server option is selected by default.
Enable SSL Certificate Check	If selected, the agent validates the certificate from the SafeNet server. The SSL certificate check is enabled by default. **NOTE:** We strongly recommend to enable the SSL certificate.
Communication Timeout	Specifies the maximum timeout value for authentication requests sent to the SafeNet server. Minimum value: **1 second**. Do not set a value below the minimum prescribed limit in the registry. Default value: **10** seconds. We highly recommend to use the default value.
Attempt to return to primary Authentication Server every	Specifies the primary authentication server retry interval. This setting only takes effect when the agent is using the Failover Server.
Agent Encryption Key File	Used to specify the location of the agent's Key File. To use the AES-GCM key standard, perform the following steps the to download a new *Agent.bsidkey* file from the SafeNet server: 1. Login to the SafeNet server as an administrator and navigate to **COMMS > Authentication Processing**. 2. Under **Task** list, click **Authentication Agent Settings** link and download the *Agent.bsidkey* file. 3. Click **Browse** to update the *Agent.bsidkey* file at **SafeNet Windows Logon Agent Manager > Communications > Agent Encryption Key File**.

Option	Description
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.

Proxy Settings



- **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.

  NOTE: The **Proxy Password** should be set only by using the **Configuration Management** tool, ensuring that it is stored encrypted.

Select the proxy settings, as follows:

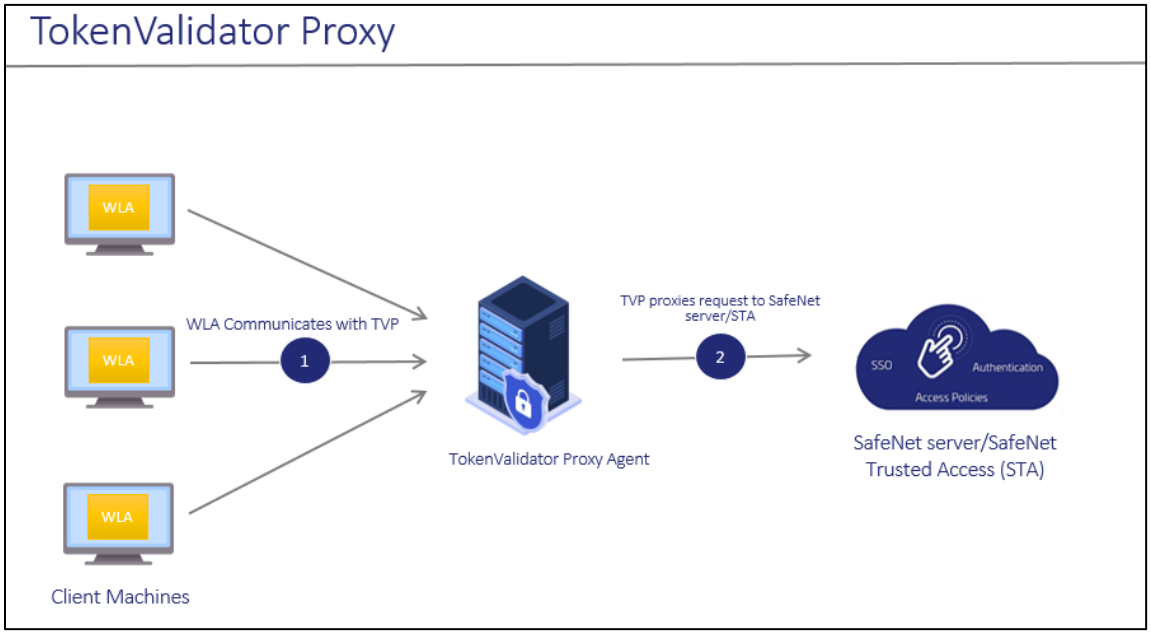
Configuration / Proxy Setting	Without Proxy	With Proxy (all calls)	With Proxy and TVP (non-push calls go to TVP, push calls go to proxy)	With Proxy for the SafeNet server (or TVP behind Proxy) and Proxy for SPS
Use Proxy	Not selected	Selected	Not selected	Selected
Use Proxy for SPS	Not selected	Not selected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

Configuring TokenValidator Proxy (TVP)

The function of the TokenValidator Proxy (TVP) Agent 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 need 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.



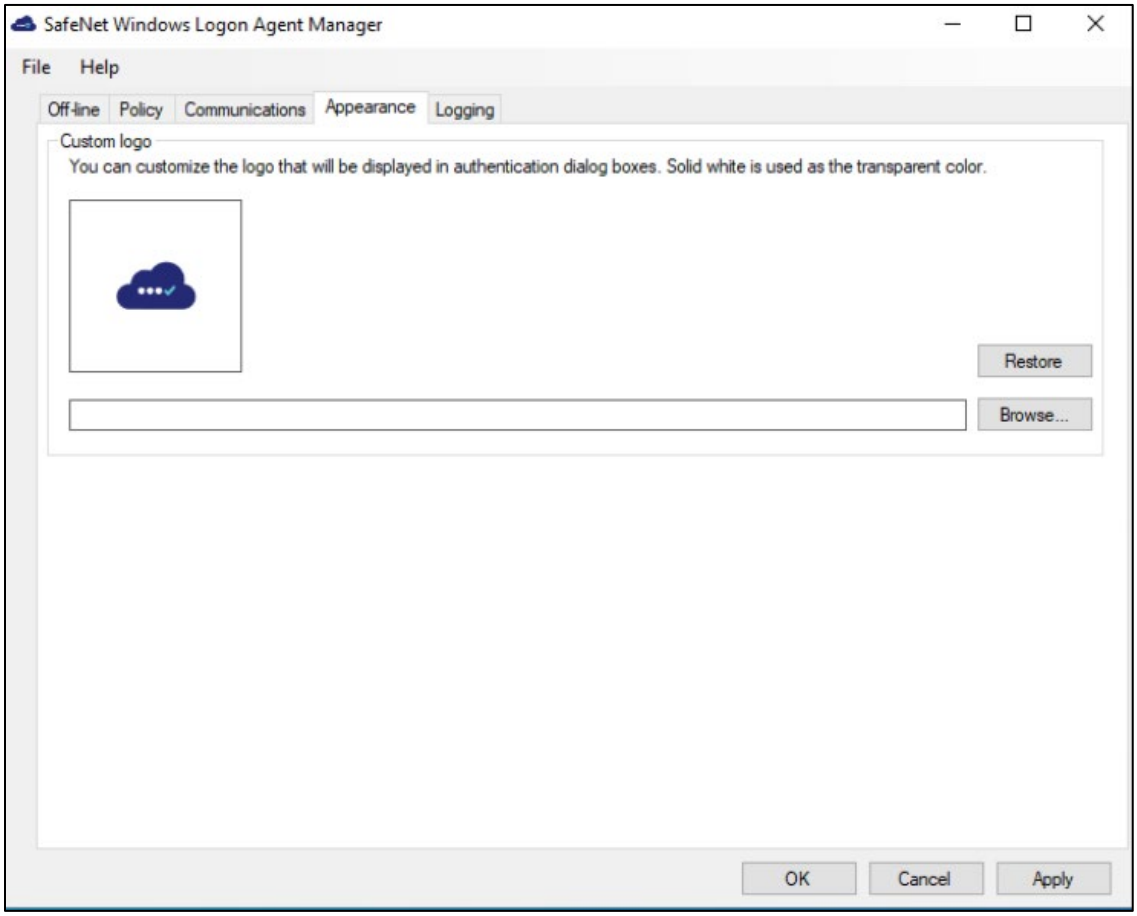
To configure TVP with the SafeNet Agent for Windows Logon, perform the following steps:

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.



Custom logo

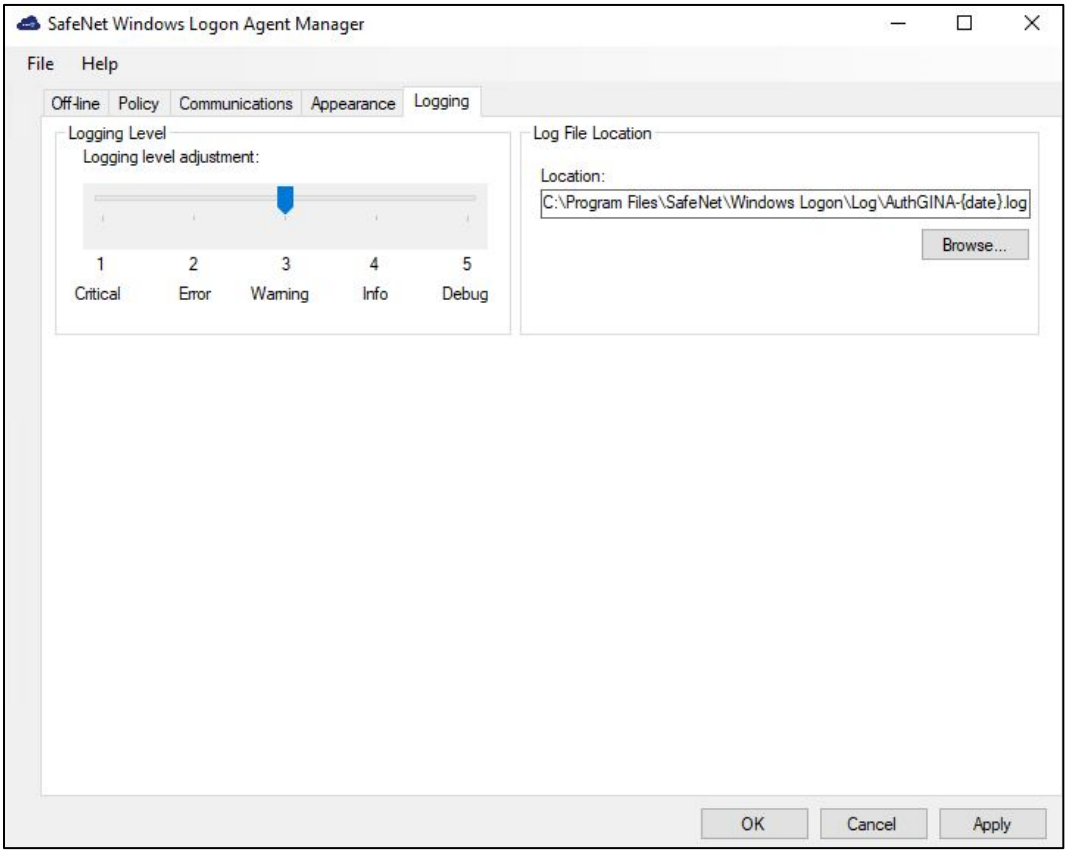
This configuration is used to customize the logo in authentication dialog box.

The logo file must be saved on the local computer. We recommend saving it in the agent installation folder.

1. The custom logo must be a bitmap of **110 x 110** pixels. Solid white is 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

This tab depicts the logging level and specifies the log file location.



Logging Level

This setting is used to adjust the logging level. 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**)

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

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

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

To enhance the overall security, additional log directory has been created in the default location with name **LogonUI** specifically for privileged process LogonUI**.**

Additional location for LogonUI process: **Default location\LogonUI**LogonUI--**{date}.log**

Upgrading the agent

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

The SafeNet Agent for Windows Logon 3.6.2 supports upgrade from 2.2.1 (or later versions).

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

Silent Upgrade

To run silent upgrade, run the following command on the command line:

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

> **NOTE:** When upgrading in silent mode, the Off-line authentication parameter is not transferred.

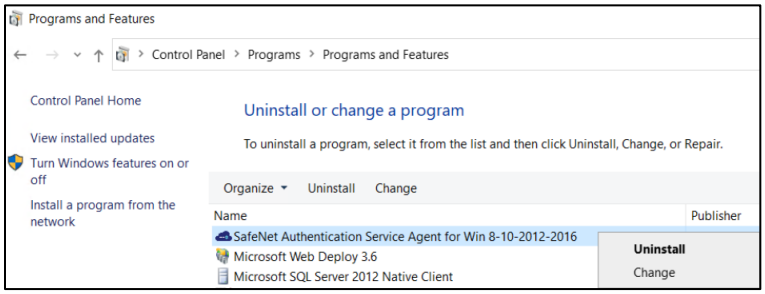
Uninstalling the agent

You can uninstall the agent either from *Control Panel* or perform silent uninstallation.

Using the Windows Control Panel

To uninstall the agent, 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**.



Silent Uninstall

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

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

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

CHAPTER 3: Deploying 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 agent 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.

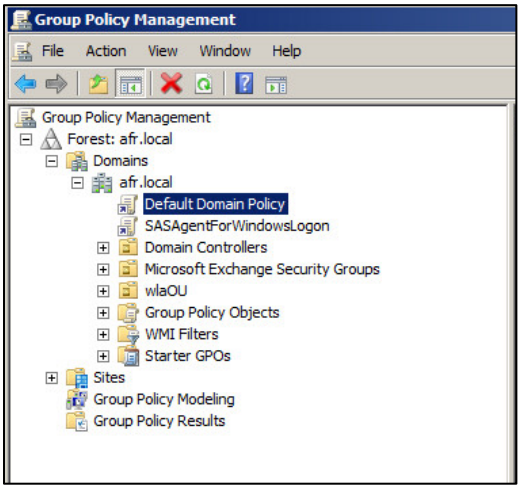
For more details about the Group Policy and Group Policy Objects, see Group Policy Overview.

Configuring the 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.

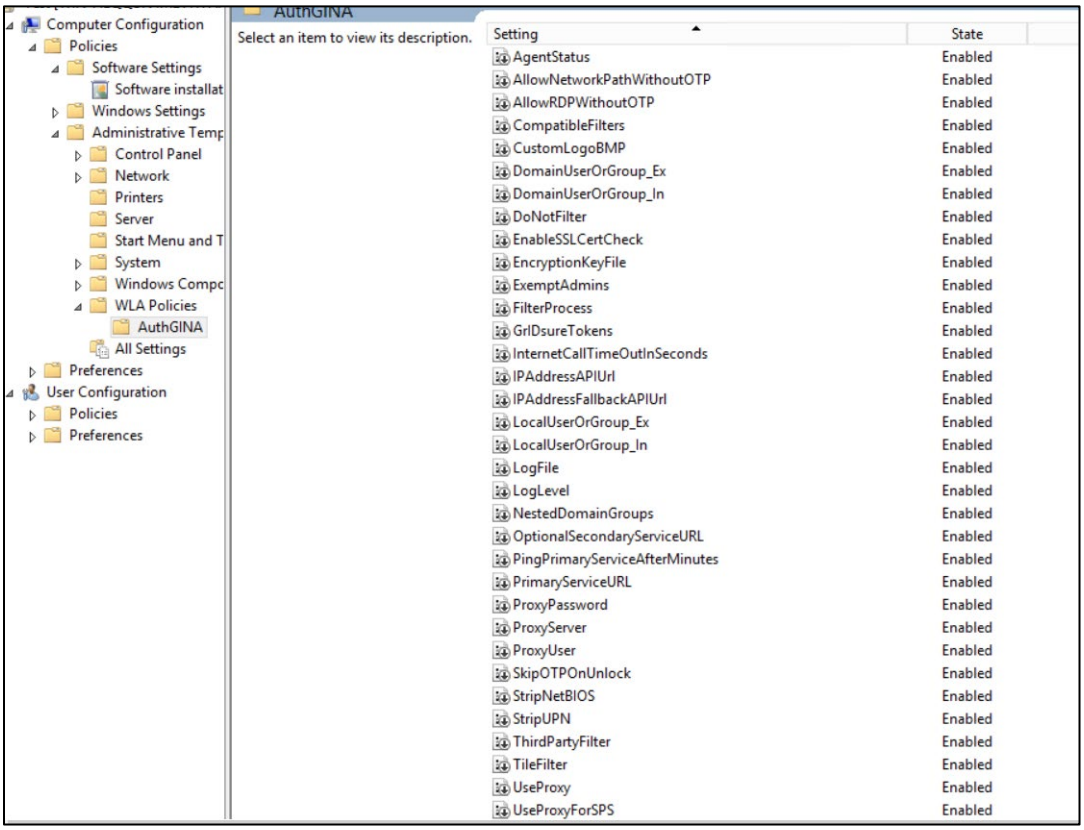
Open the administrative template and perform the following steps to configure the settings:

1. From the Windows taskbar, select **Start** > **All Programs** > **Accessories** > **Run**.
2. 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, go to the **Domain Controllers** node and right-click **Default Domain Controllers Policy**.

4. From the drop down 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.



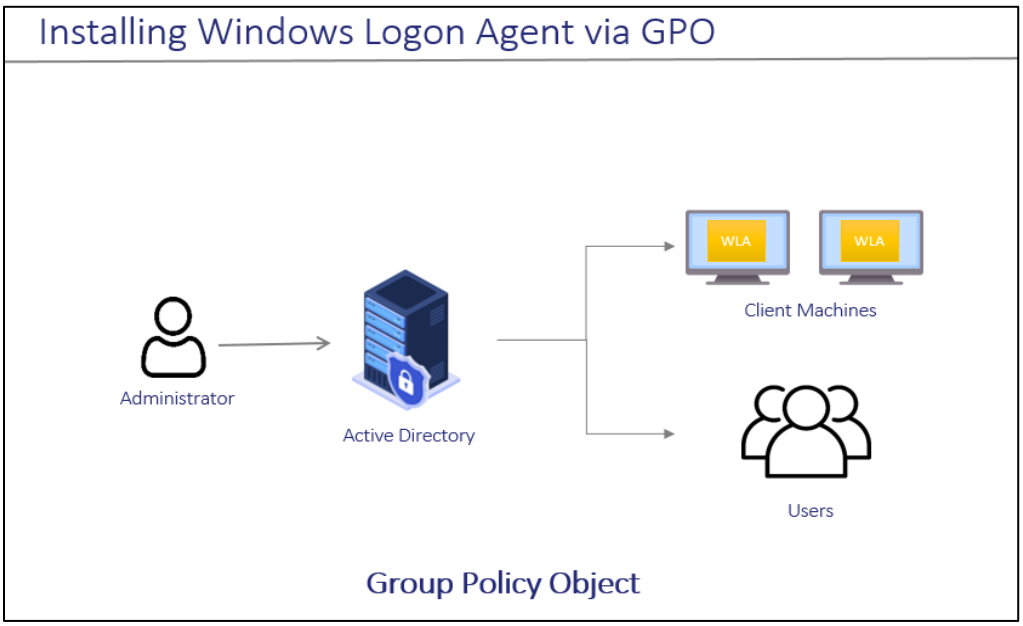
6. Enable all the setting as per your requirement, if not already enabled, with *default value* or *user-defined value*.

Click here to see the description of the registry settings available with the agent.

Deploying the agent

Deploying SafeNet Agent for Windows Logon via GPO requires:

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 and paste 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 and enforce a new GPO, perform the following steps:

1. From the Windows taskbar, select **Start > All Programs > Accessories > Run**.
2. 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**. The GPO will be linked 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*) from the package and paste it to the following location:

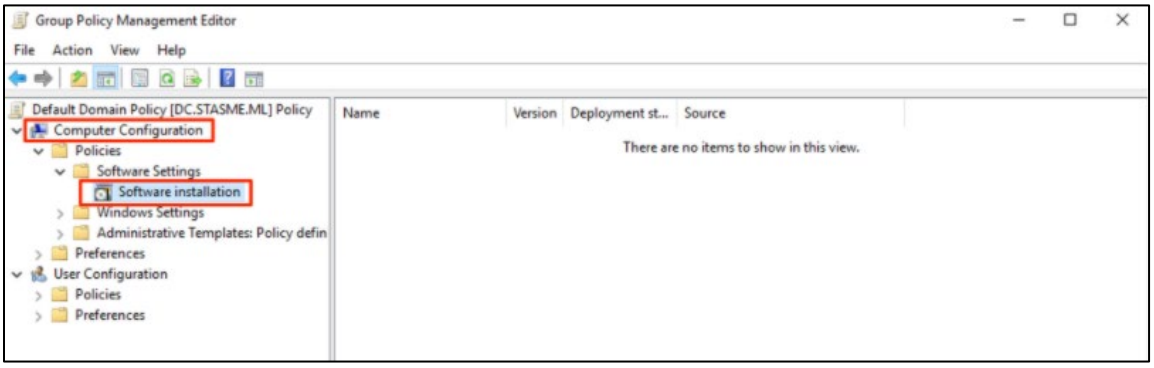
   `C:\Windows\SYSVOL\sysvol\<domain_name>\Policies\PolicyDefinitions`
3. Copy the appropriate *ADML* language file (*SafeNetAgentForWindowsLogon.adml*) to a language folder under the `\PolicyDefinitions`.

   For example, in Windows Server 2019, 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**.

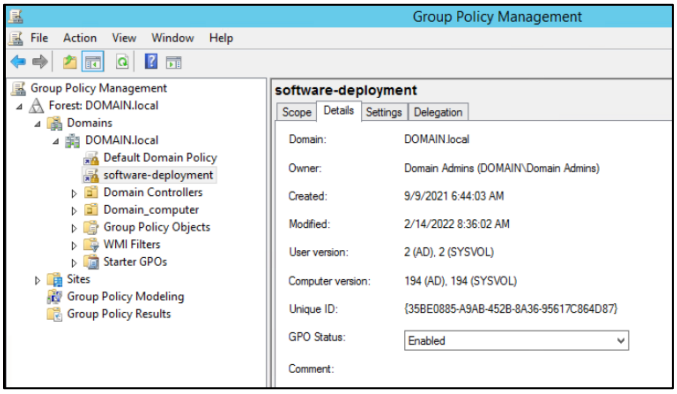


3. Right-click the **Software Installation**, and select **New > Package**.
4. Select the SafeNet Agent for Windows Logon MSI file (*SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64.msi*) from the previously created shared folder.
5. Select the **deployment Method – Assigned** and click **OK**.
6. Double-click **MSI** and under **Deployment** tab, click **Advanced**. 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

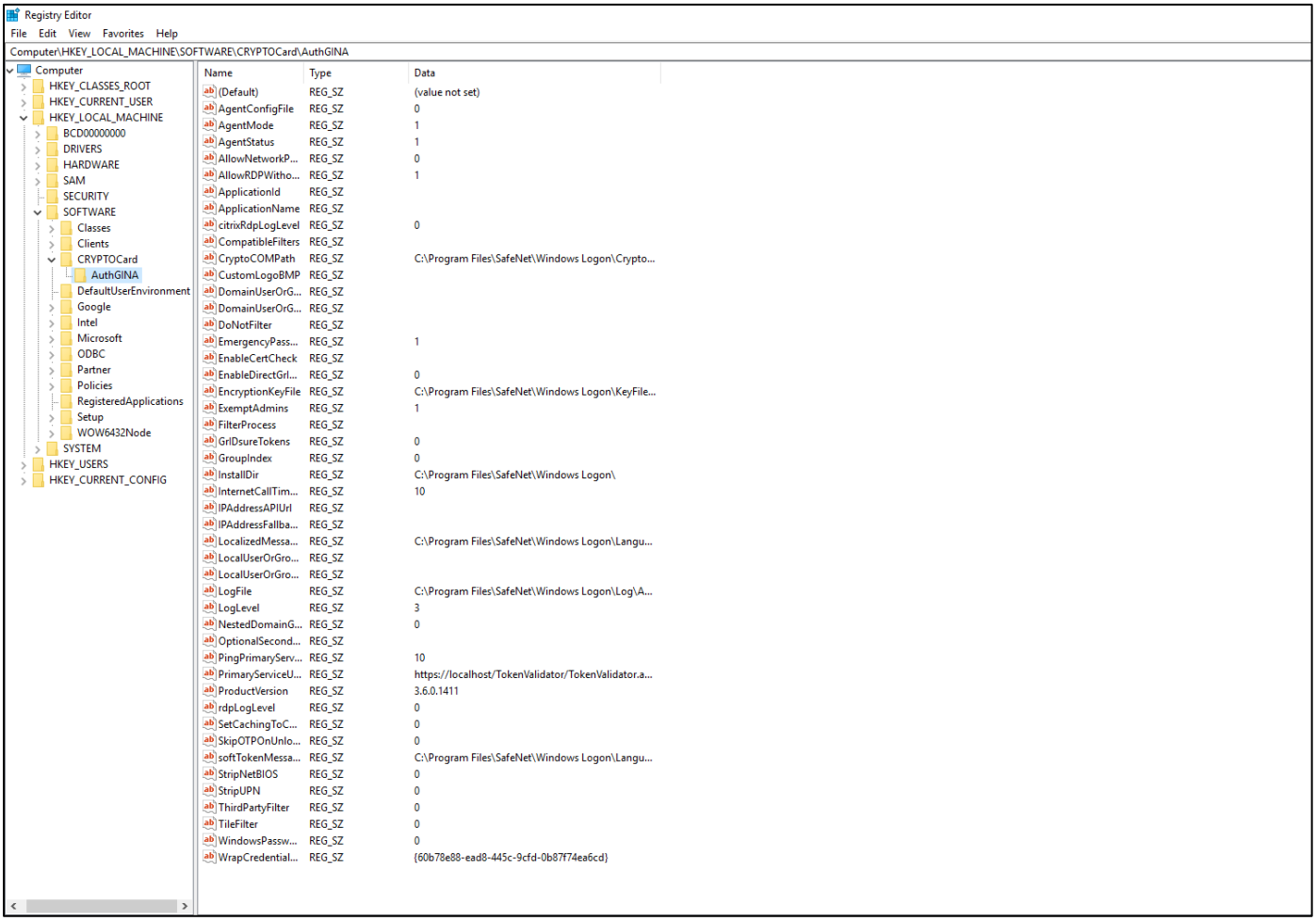
> **NOTE:** Restart might be required after executing the above command.

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



Registry Settings

The management console configurations exists as registry setting at **HKEY_LOCAL_MACHINE\SOFTWARE\CRYPTOCard\AuthGINA**. However, there are some settings which are not exposed on the management console due to some security reasons. Following are the registry settings that are not available on the management console:



Setting	Description	Accepted Values
UseProxy	Used to configure the proxy server to connect with SafeNet server via proxy. For example, Token Validation Proxy. **Note:** If you enable this setting, you must configure **Proxy Server**.	**1**: Enable the proxy server **0** (Default): Proxy server is not used
StripNetBIOS	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).	**1**: Strips the DOMAIN\ portion from the username when authenticating with SafeNet server **0** (Default): The agent will not sanitize the username
EnableSSLCertCheck	Used to validate the SafeNet server certificate or Proxy server certificate (if used).	**1** (Default): The agent will validate the server certificate **0**: The agent will not validate the server certificate
ProxyServer	Used to configure the proxy server IP address or FQDN and its port number. **Note:** Must be used with setting 'UseProxy' or 'UseProxyForSPS'.	'1.2.3.4:567' or 'host.domain.name:port'
ExemptAdmins	Used to exclude the local and domain administrators from strong authentication (OTP).	**1** (Default): Local and Domain Administrators are exempted from strong authentication **0**: All users musts use strong authentication
ProxyPassword	Used to configure the proxy server password. **WARNING:** The agent 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, configure this setting in the client machine using the management console, and then retrieve its value from the registry.	
LocalUserOrGroup_Ex	Used to exclude the Local Groups from the SafeNet authentication. When any group is added to this setting through GPO, **DomainUserOrGroup_In** needs to be set to "*".	**COMPUTERNAME\groupname, COMPUTERNAME\group2**: multiple values are separated by comma (,) **%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. **[ ]**: Default

Setting	Description	Accepted Values
PrimaryService URL	Used to configure the Primary SafeNet server (or the Token Validation Proxy).	**>** Protocol followed by IP address and port, for example, http://1.2.3.4:8080 **>** Protocol followed by FQDN and port, for example, https://server.domain.com
WindowsPasswordCaching	If enabled, WLA will cache the Microsoft password on first successful user authentication until password expiration or change. **Note:** This configuration is not applicable for domain administrators.	**1**: Users are prompted for OTP only **0** (Default): Users are prompted for OTP, then domain password
EncryptionKeyFile	It is used to set the key file location.	**Default**: C:\Program Files\SafeNet\Windows Logon\KeyFile\Agent.bsidkey
GrIDsureTokens	Used to enable the GrIDsure authentication link in the logon screen.	**1** (Default): Display the GrIDsure authentication link **0**: Hide the GrIDsure authentication link
WrapCredential Provider	Specify the GUID of the credential provider that the agent will use to wrap for the two-factor authentication.	**{GUID}**: Its default value is {60b78e88-ead8-445c-9cfd-0b87f74ea6cd} for V2 Credential provider
LogLevel	Used to configure the client side log level.	**1**: Critical **2**: Error **3**: Warning (default) **4**: Info **5**: Debug
PingPrimaryServiceAfterMinutes	Used to configure the time (in minutes) after which the agent will attempt to return to its Primary SafeNet server.	**Default**: 10 minutes
AllowRDPWithoutOTP	Used to exclude the outgoing RDP (remote desktop) from SafeNet authentication.	**1** (Default): SafeNet authentication is not enforced for outgoing RDP **0**: SafeNet authentication is required for outgoing RDP
DomainUserOrGroup_In	Used to include the Domain Groups for the SafeNet authentication. **Note:** If you define a group or multiple groups in this setting you must also set DomainUserOrGroup_Ex and LocalUserOrGroup_Ex with a value of '*'.	**[ ]**: Not configured **DomainName.com\Group Name**: Only the provided group must use strong authentication *: All users must use strong authentication
AllowNetworkPathWithoutOTP	Used to exclude the SafeNet authentication while accessing network resources over Windows Explorer.	**1**: SafeNet authentication is not enforced while accessing the network resource **0** (Default): SafeNet authentication is required while accessing the network

Setting	Description	Accepted Values
		resource for outgoing Windows Explorer
TileFilter	Used to configure the appearance of credential provider tiles during Windows Logon.	**0** (Default): All credential tiles presented to the user will enforce SafeNet authentication. **1**: Authentication can be performed using SafeNet or third-party credentials, but the Microsoft credential tile is hidden. **2**: Authentication can be performed with third-party or Microsoft credentials, but the SafeNet credential tile is hidden.
LocalUserOrGroup_In	Used to include the local users to use strong authentication (OTP). **Note:** If you define a group or multiple groups in this setting, you must also set DomainUserOrGroup_Ex with a value of '*'.	**[ ]**: Not configured **ComputerName\Group Name**: Only the provided group must use strong authentication **%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
ThirdPartyFilter	Some third-party credential provider software may conflict with the working of the agent. So, you can restrict their access with this registry key and only allow certain supported software to work with the agent.	**0** (Default): Allow all applications **1**: Allow SafeNet compliant applications
InternetCallTimeOutInSeconds	Specifies the maximum timeout value for authentication requests sent to the SafeNet server.	**Default**: 10 seconds
UseProxyForSPS	Used to connect to the Service Provider Server via proxy server.	
NestedDomainGroups	Enable it to improve logon performance if domain groups are not nested inside local groups.	**1**: Improves the agent performance when domain groups are not nested in local groups **0** (Default): Used when domain groups are nested in local groups
OptionalSecondaryServiceURL	Used to configure the secondary (failover) SafeNet server (or the Token Validation Proxy).	**>** Protocol followed by IP address and port, for example, http://1.2.3.4:8080 **>** Protocol followed by FQDN and port, for example, https://server.domain.com
LogFile	Used to configure the client log file path.	**Default:** C:\Program Files\SafeNet\Windows Logon\Log\AuthGINA-{date}.log

Setting	Description	Accepted Values
DomainUserOrGroup_Ex	Used to exclude the Domain Groups from the SafeNet authentication. **Note:** When any group is added to this setting, then the DomainUserOrGroup_In entry remains empty. You need to set LocalUserOrGroup_In to "*".	**[ ]**: Not configured **DomainName.com\Group Name**: Only the provided group is excluded from strong authentication
ProxyUser	Used to configure the proxy server username that is used to authenticate the defined proxy server. **Note:** Setting 'ProxyUser' assumes setting 'ProxyServer' and 'Password', and may also require setting 'UseProxyForSPS' (if applicable).	
StripUPN	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).	**1**: Strips the @domain.com portion from the UPN when authenticating with the SafeNet server **0** (Default): The agent will not sanitize the username
CustomLogoBMP	Allows to set a custom image in the logon screen for compatible credential providers. The customization is not compatible with the Windows V2 credential provider. **Note:** The custom logo must be a bitmap (.bmp) of 110 x 110 pixels and must be available locally on the client.	**Example syntax**: C:\Program Files\SafeNet\Windows Logon\customLogo.bmp
AgentStatus	Used to enable or disable the agent.	**1** (Default): The agent will be enabled and displayed at logon **0**: The agent will be disabled (remains installed and configured but is not used)
EmergencyPassword	Used to enable or disable the emergency password feature. This is applicable when the Windows machine is unable to communicate with the SafeNet server at the time of authentication.	**1** (Default): Emergency Password can be used for authentication **0**: Emergency Password cannot be used
SkipOTPOnUnlock	Used to exclude the SafeNet authentication for last logged on user on system unlock. The functionality extends to sleep and hibernate mode, which means the agent will not prompt for an OTP, and instead logs in successfully using only the AD credentials.	**1**: SafeNet authentication is skipped during unlock **0** (Default): SafeNet authentication is required during unlock

Following are some of the registry settings that are not configurable using Windows Logon Agent Manager. You need to create it manually in the registry at the following location:

`HKEY_LOCAL_ MACHINE\SOFTWARE\Cryptocard\AuthGINA`

Setting	Description	Accepted Values
DoNotFilter	Allows a view where third-party credential providers can also be displayed. By default, the agent filters out (do not display) other credential provider.	{GUID},{GUID},{GUID}
CompatibleFilters	Prevents the management console from displaying an Incompatible Filter message. This setting can only be added if a third-party credential provider is compatible with the agent and can be wrapped successfully. For example, if *SpecOps* credential provider is installed on a client machine along with the agent, then the management console 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}
FilterProcess	Allows to exclude applications from applying the SafeNet authentication. This setting can only be added when the agent is installed with default options. To exclude: > *Outlook* from using OTP to authenticate, add its executable (outlook.exe) to the *FilterProcess* list. > All the applications from SafeNet authentication, add an asterisk (*) in the *FilterProcess* list.	
SetCachingToCurrentUser	Augments the secured storage of a user's cached Microsoft password. This is mostly relevant for shared machine scenarios and is effective only when **Enable Microsoft Password Caching** is selected in the **SafeNet Windows Logon Agent Manager > Policy** tab. If **SetCachingToCurrentUser** is set to **1**, the password caching will not work in the following scenarios: > Access to a network path/resource > Outgoing RDP connections from a WLA protected machine > Run as a different user to access applications, such as command prompt For such cases, Microsoft password must be provided by the user. All other use cases supported for Microsoft password caching will function as expected. This setting will be applicable on next logon.	0 (Default) 1

CHAPTER 4: Deploying the agent via Intune

This section describes the steps to deploy the agent 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 **Setup enrollment for Windows devices** in the Microsoft documentation.

Deploying the agent 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 the agent 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:
   a. **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.

b. **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.

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

d. **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]
"EmergencyPassword"="1"
"LogLevel"="3"
"PingPrimaryServiceAfterMinutes"="10"
"LocalUserOrGroup_Ex"=""
"DomainUserOrGroup_In"=""
"rdpLogLevel"="0"
"DomainUserOrGroup_Ex"=""
"AgentStatus"="1"
"InternetCallTimeOutInSeconds"="10"
"WindowsPasswordCaching"="0"
"StripUPN"="0"
"StripNetBIOS"="0"
"DoNotFilter"=""
"AllowNetworkPathWithoutOTP"="0"
"GroupIndex"="0"
"WrapCredentialProvider"="{60b78e88-ead8-445c-9cfd-0b87f74ea6cd}"
"TileFilter"="0"
"WLAasV1Provider"="0"
"ExemptAdmins"="1"
"GrIDsureTokens"="0"
"AllowRDPWithoutOTP"="1"
"EnableCertCheck"=""
"ThirdPartyFilter"="0"
"LogFile"="C:\\Program Files\\SafeNet\\Windows Logon\\Log\\AuthGINA-{date}.log"
"FilterProcess"=""
"NestedDomainGroups"="0"
"AgentMode"="1"
"CompatibleFilters"=""
"SkipOTPOnUnlock"="0"
"AgentConfigFile"=""
"IPAddressAPIUrl"=""
"IPAddressFallbackAPIUrl"=""
"citrixRdpLogLevel"="0"
"LocalUserOrGroup_In"=""
"CustomLogoBMP"=""
```

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"
```

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:
   a. **source folder** - Enter the path of the folder where the .reg and setup file is present. For example, C:\Intune-Deployment\Configuration.
   b. **setup file** - Enter the path of **ConfigurationSetup.cmd**. For example, C:\Intune-Deployment\Configuration\ConfigurationSetup.cmd.
   c. **output folder** - Enter the path of the **ConfigurationOutput** folder to save the .IntuneWin package. For example, C:\Intune-Deployment\ConfigurationOutput.
   d. **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
```

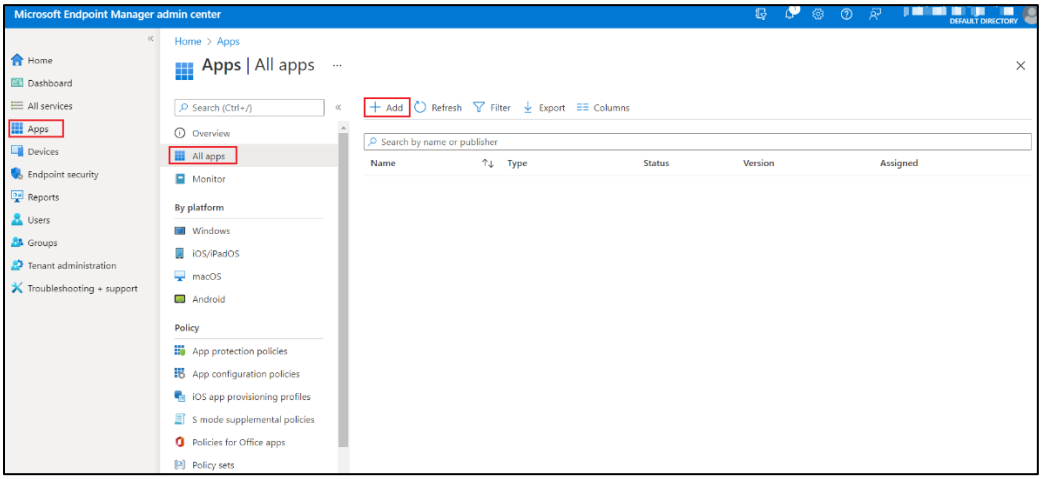
Now, a .IntuneWin package (ConfigurationSetup.intunewin) is ready for deployment under **Intune-Deployment\ConfigurationOutput** as a Win32 application in Intune.

Deploying the IntuneWin package

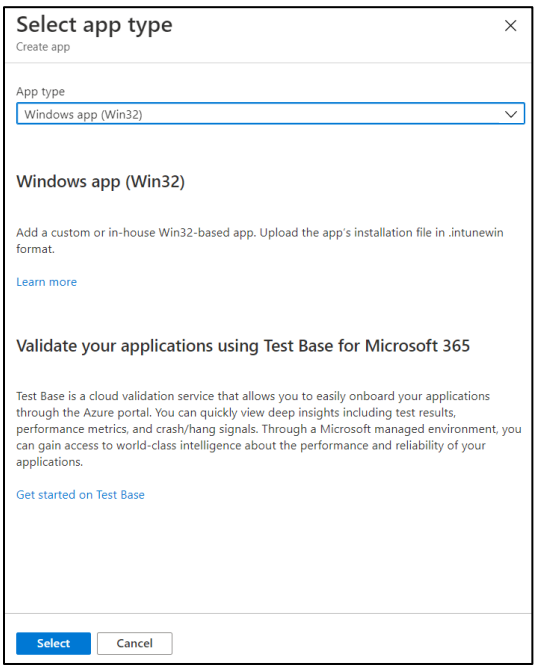
Perform the following steps to deploy the agent via Intune:

Deploying the IntuneWin package of WLA Installer

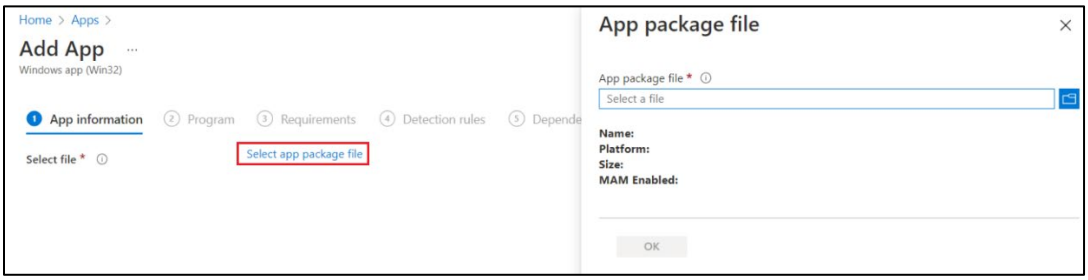
1. Login to the Microsoft Endpoint Manager admin center using https://endpoint.microsoft.com.
2. In the left pane, select **Apps > All apps > Add**.



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



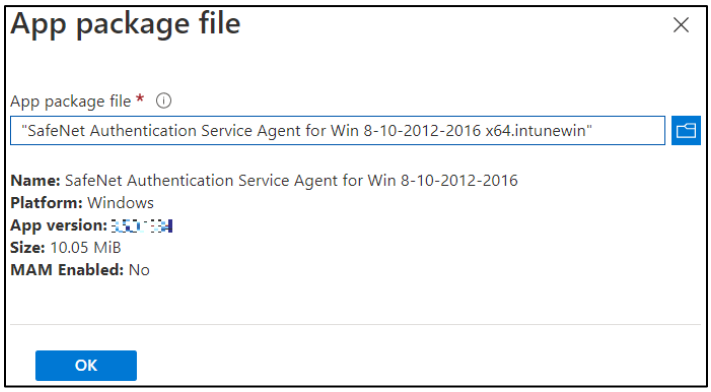
4. Click **Select app package** file. The **App package file** window appears.



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

   a. 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.

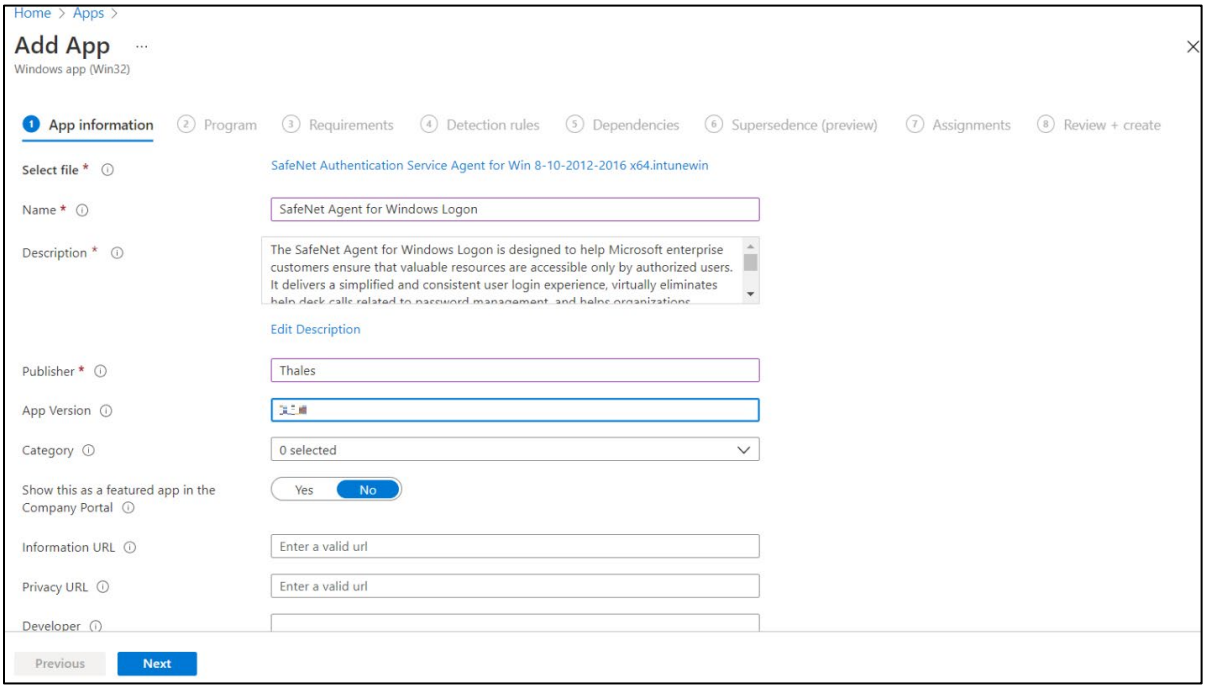
   b. Click **OK**.



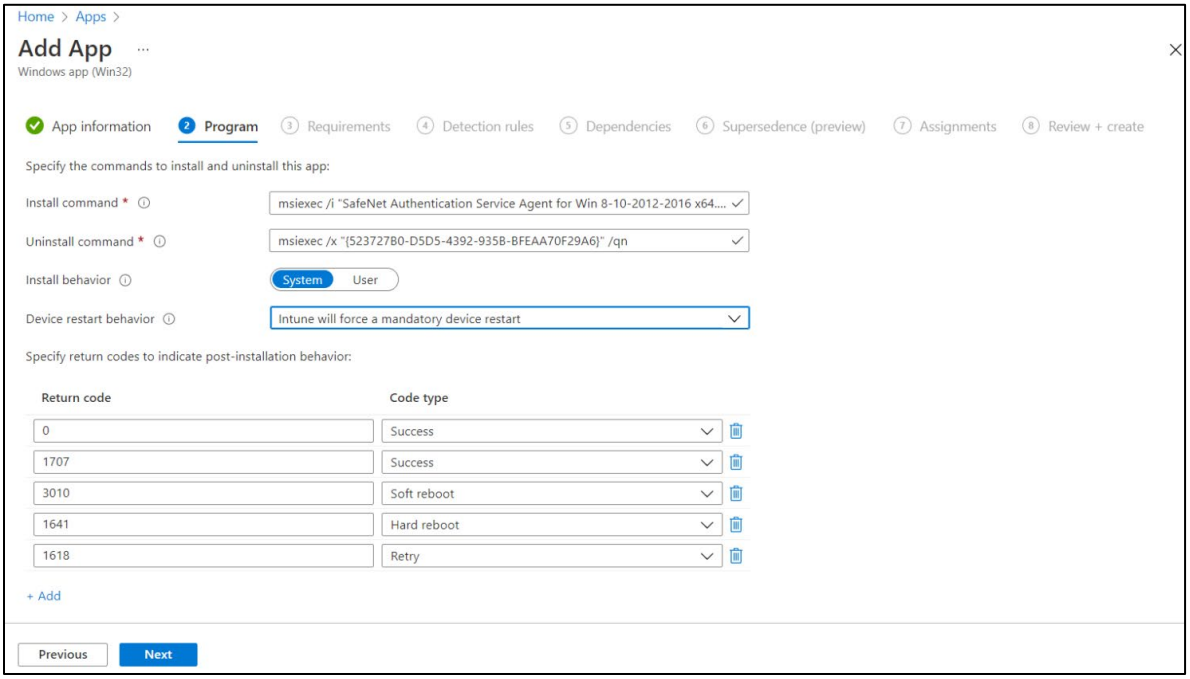
6. In the **Add App** window, under the **App information** tab, enter the following details for your app:
   a. **Name**: Enter name of the app. Ensure the app names that you use are unique. For example, SafeNet Agent for Windows Logon.
   b. **Description**: Click **Edit Description** to enter a small description of the app and then click **OK**.
   c. **Publisher**: Enter the name of the publisher of the app. For example, Thales.
   d. **App Version**: Depicts the app version. For example, 3.5.0.

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

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



7. Under the **Program** tab, enter the following details to configure the app installation and removal commands for the app:
   a. **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.
   b. **Uninstall command**: Enter **msiexec /x "{523727B0-D5D5-4392-935B-BFEAA70F29A6}" /qn** as the command to uninstall the app.
   c. **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.
   d. Click **Next** to display the **Requirements** page.

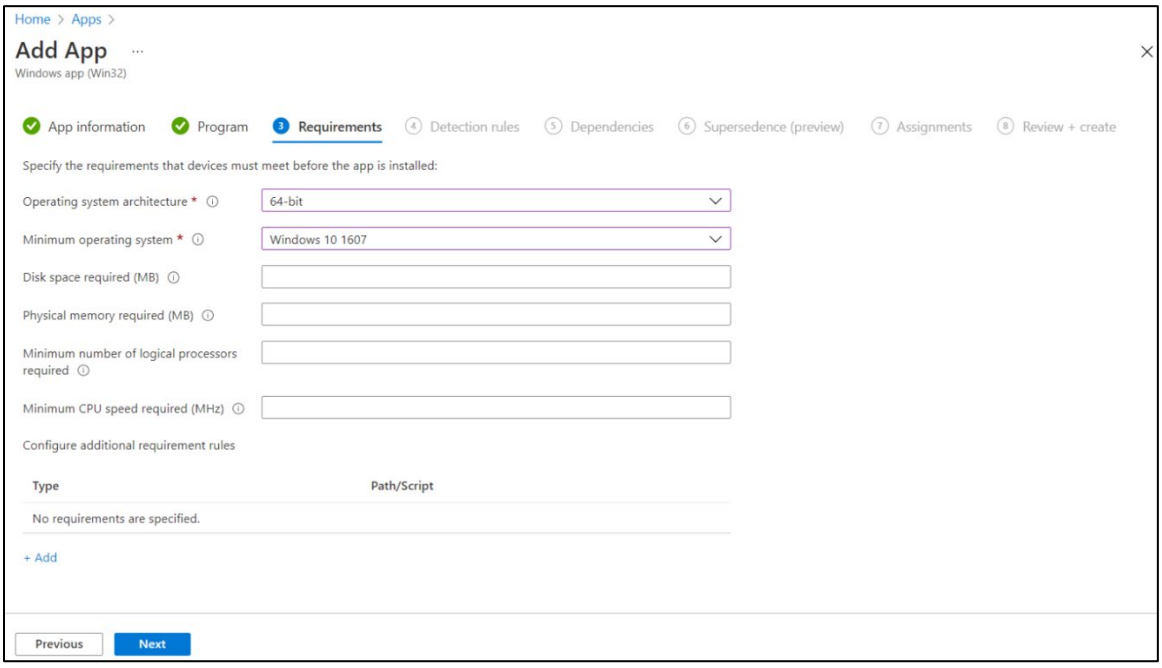


8. Under the **Requirements** tab, specify the following requirements that the device must meet before the app is installed:

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

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

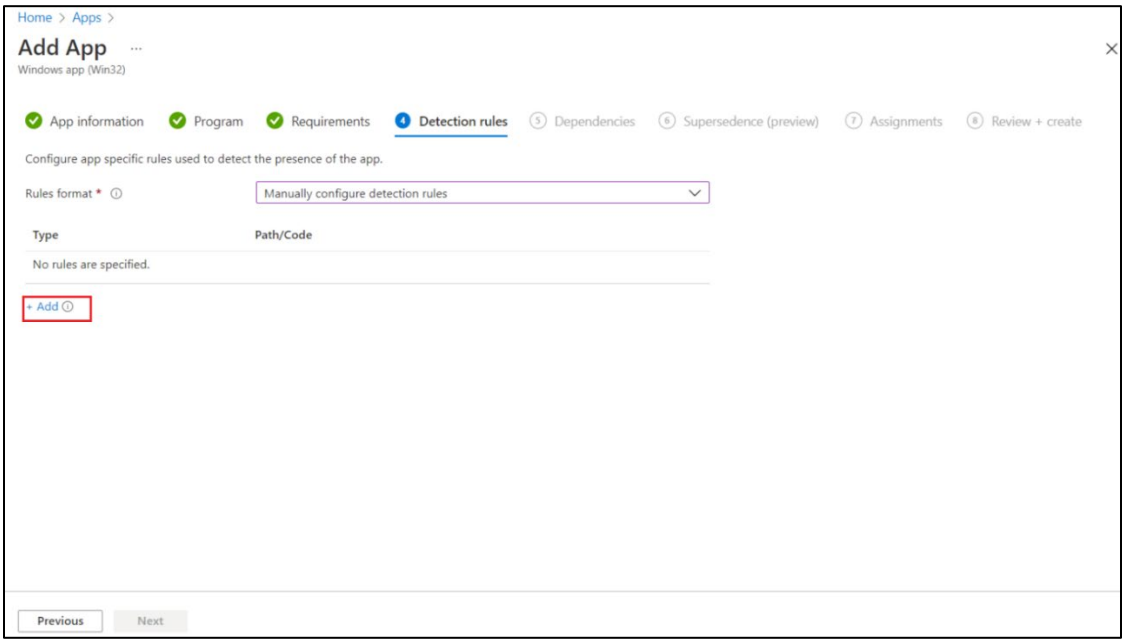
   c. Click **Next** to display the **Detection rules** page.



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

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

b. Click **Add**.



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

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

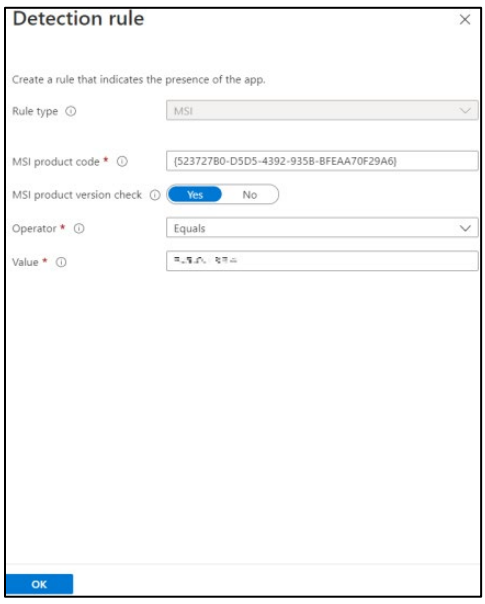
b. **MSI product code**: Enter **{523727B0-D5D5-4392-935B-BFEAA70F29A6}** as the MSI product code.

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

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

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

f. Click **OK**.

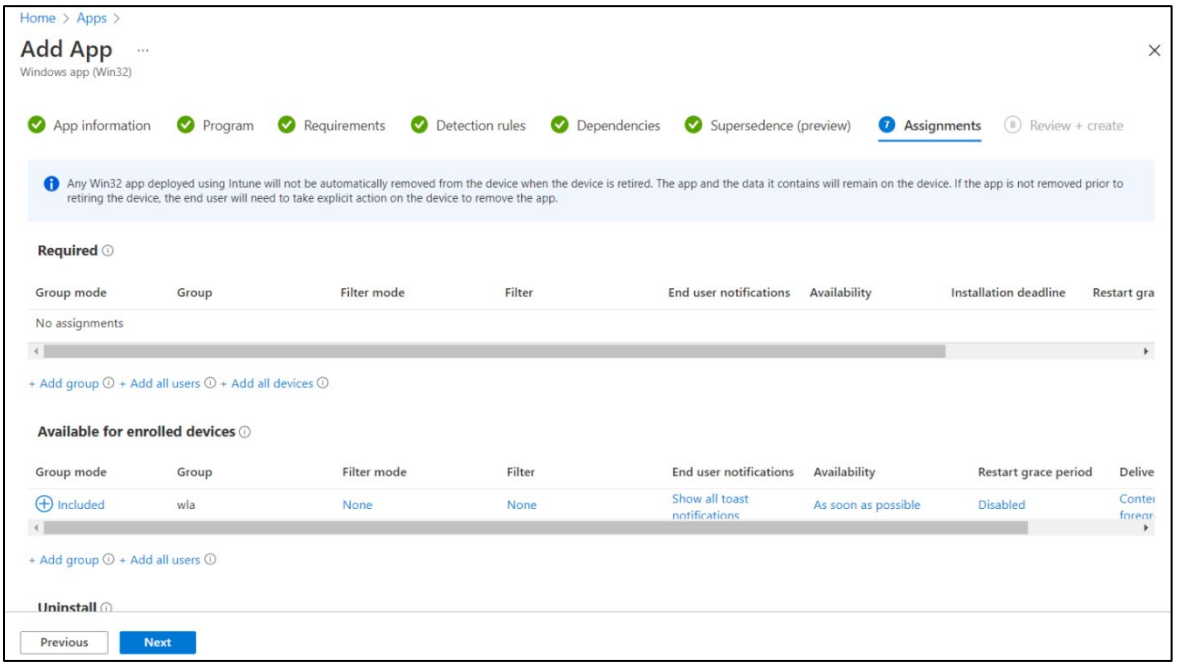


After adding your rules, click **Next** to display the **Dependencies** page.

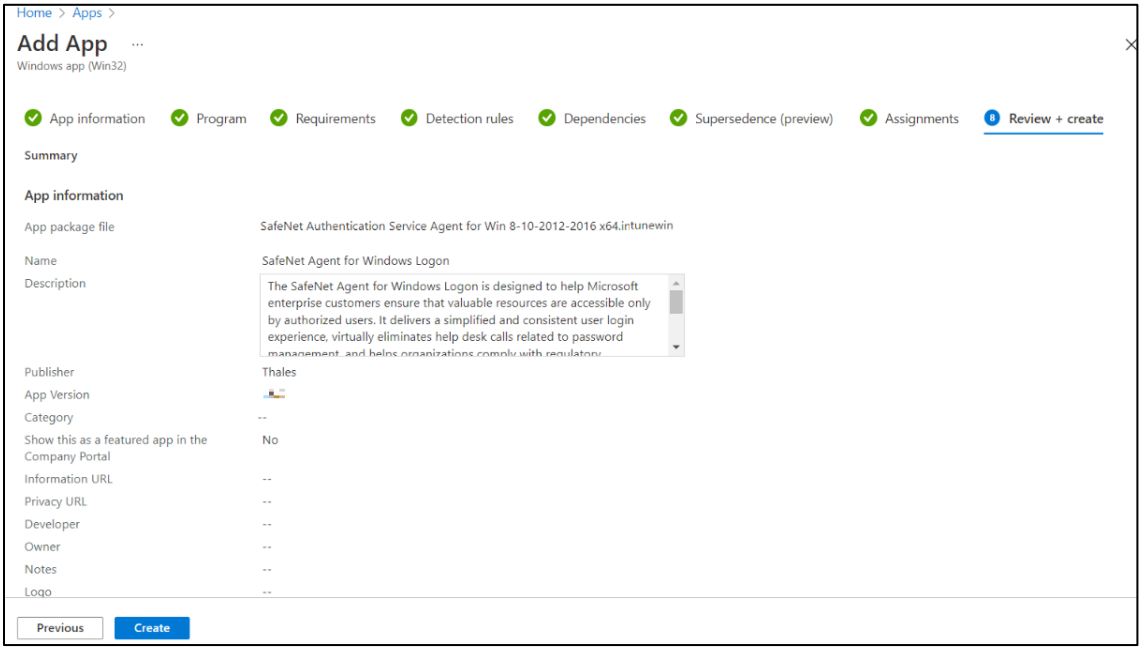
10. In the **Dependencies** tab, click **Next**.
11. In the **Supersedence (preview)** tab, click **Next**.
12. Under the **Assignments** tab, you can select the **Required**, **Available for enrolled devices**, or **Uninstall** group assignments for the app.
    a. Select an assignment type for the 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.

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



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

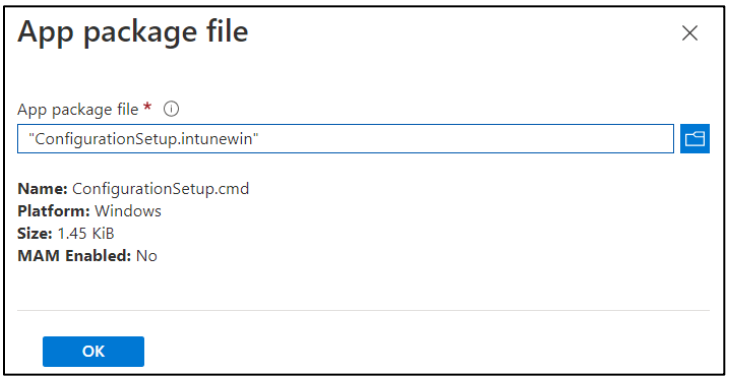


After completing the above steps, the **SafeNet Agent for Windows Logon** app will be deployed successfully.

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:
   a. 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.
   b. Click **OK**.



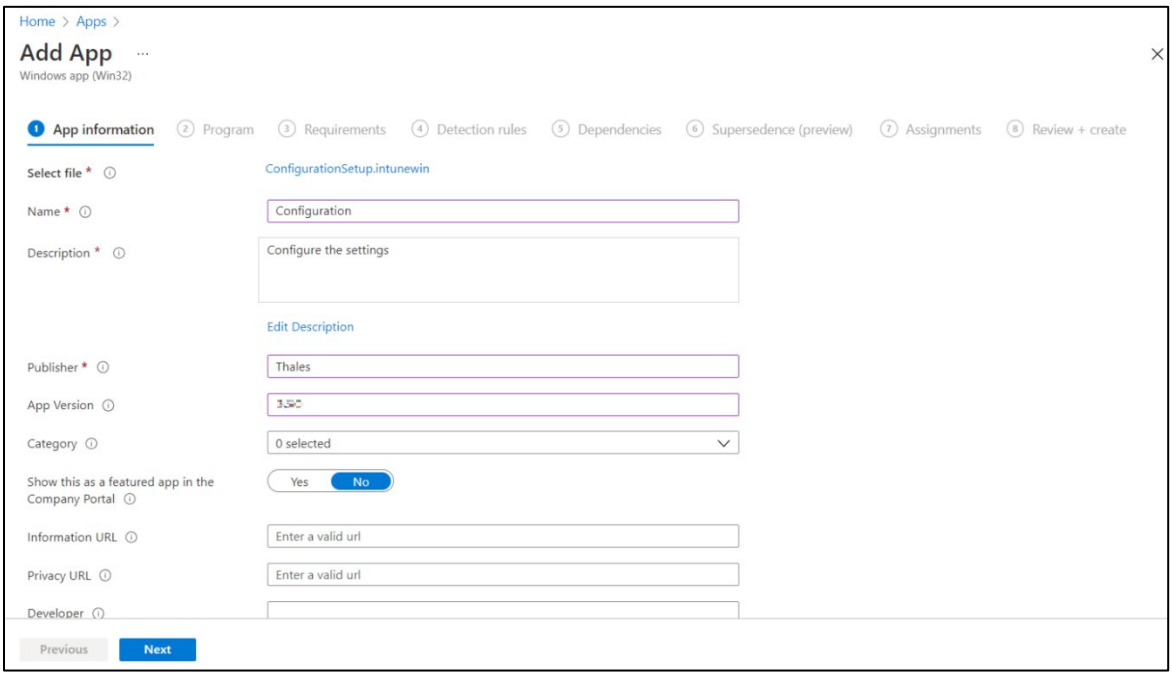
3. In the **Add App** window, under **App information** tab, enter the following details for your app:
   a. **Name**: Enter name of the app. Ensure the app names that you use are unique. For example, Configuration.
   b. **Description**: Click **Edit Description** to enter a small description of the app and then click **OK**.

c. **Publisher**: Enter the name of the publisher of the app as **Thales**.

d. **App Version**: Depicts the app's version as **3.6.0**.

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

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



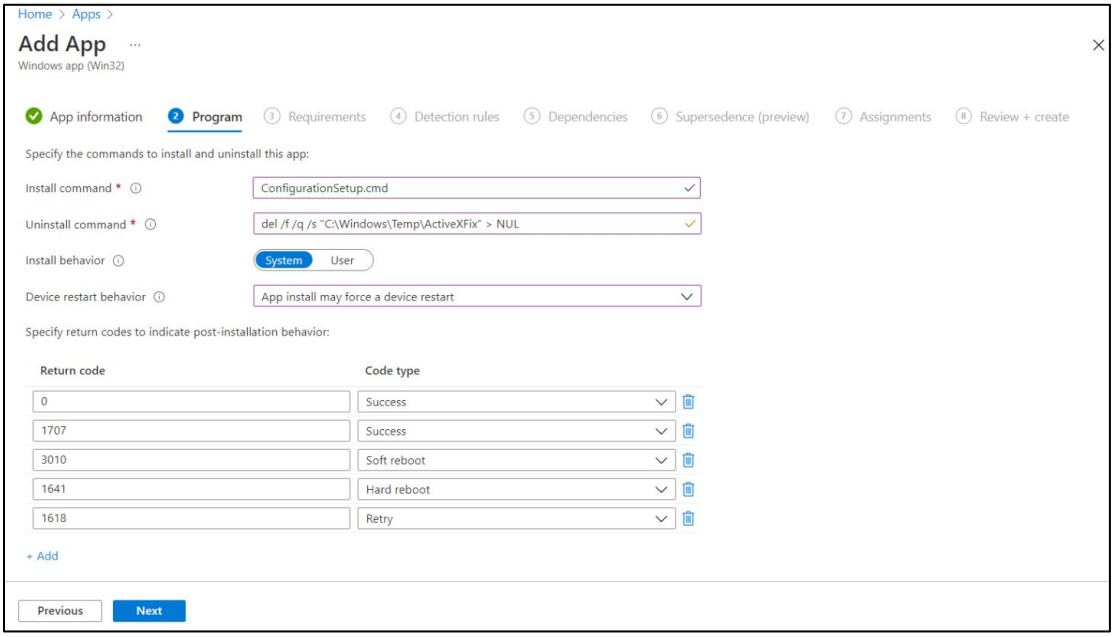
4. Under the **Program** tab, enter the following details to configure the app installation and removal commands for the app:

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

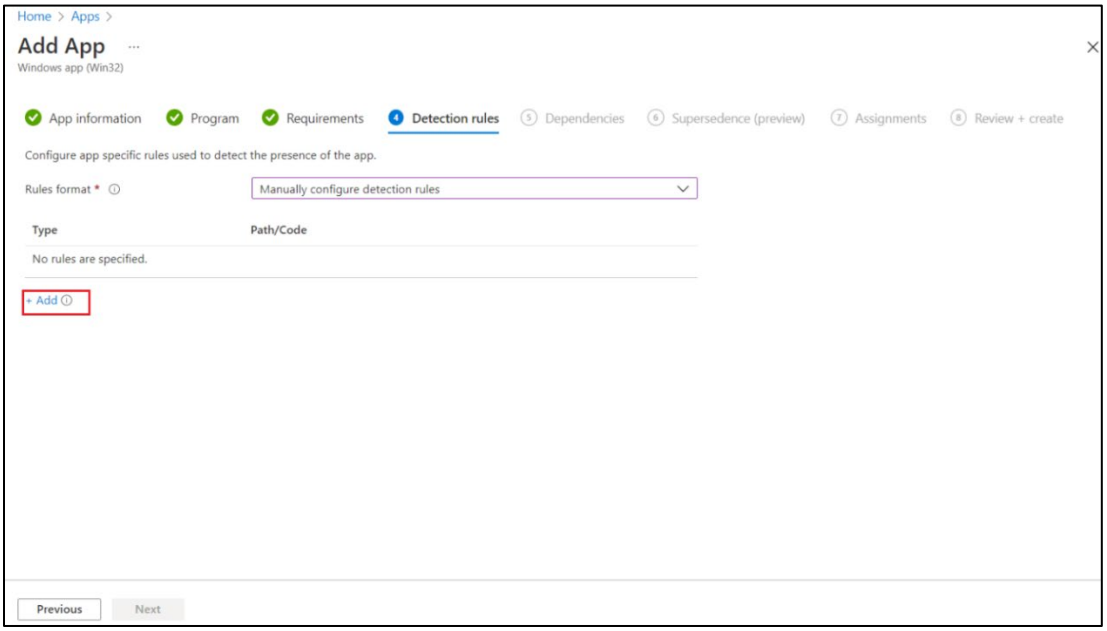
b. **Uninstall command**: Enter **del /f /q /s "C:\Windows\Temp\ActiveFix" > NUL** as the command to uninstall the app.

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

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



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

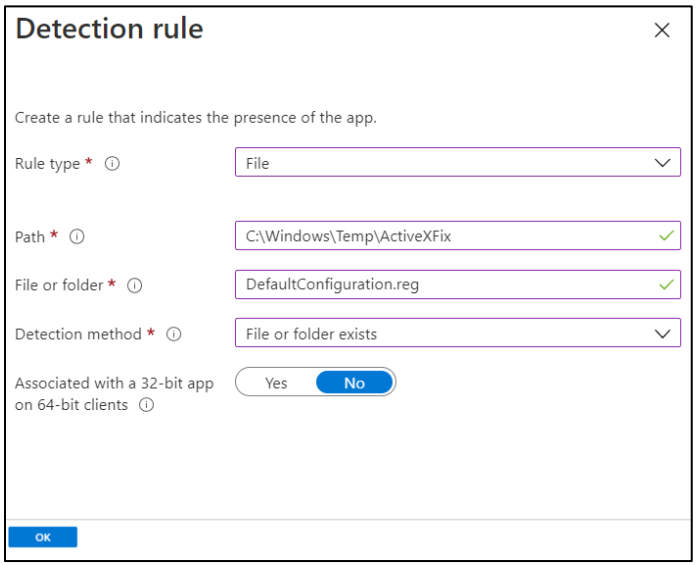


Detection rule window appears. Enter the following details to create a detection rule:

   a. **Rule type**: Select **File** from the drop-down.
   b. **Key path**: Enter **C:\Windows\Temp\ActiveXFix** as the full path of the file that contains the value to detect.
   c. **Value name**: Enter **DefaultConfiguration.reg** as the name of the file value to detect.

d. **Detection method**: Select **File or Folder Exists** from the drop-down to validate the presence of the app.

e. Click **OK**.



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

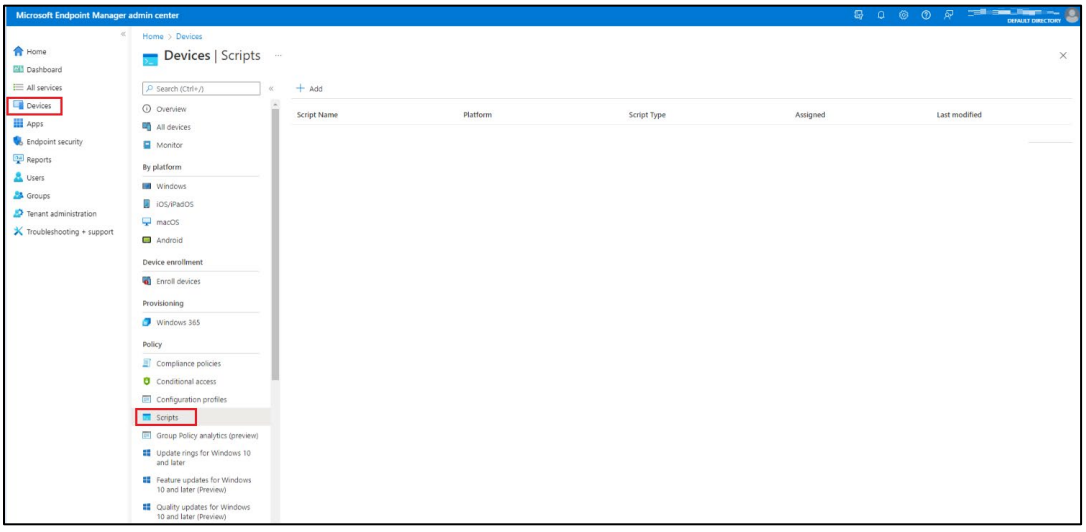
7. Repeat the steps Step 10 to Step 13 in the above section.

After completing the above steps, the **SafeNet Agent for Windows Logon** app will be deployed successfully. The **DefaultConfiguration.reg** file will be copied in the client system.

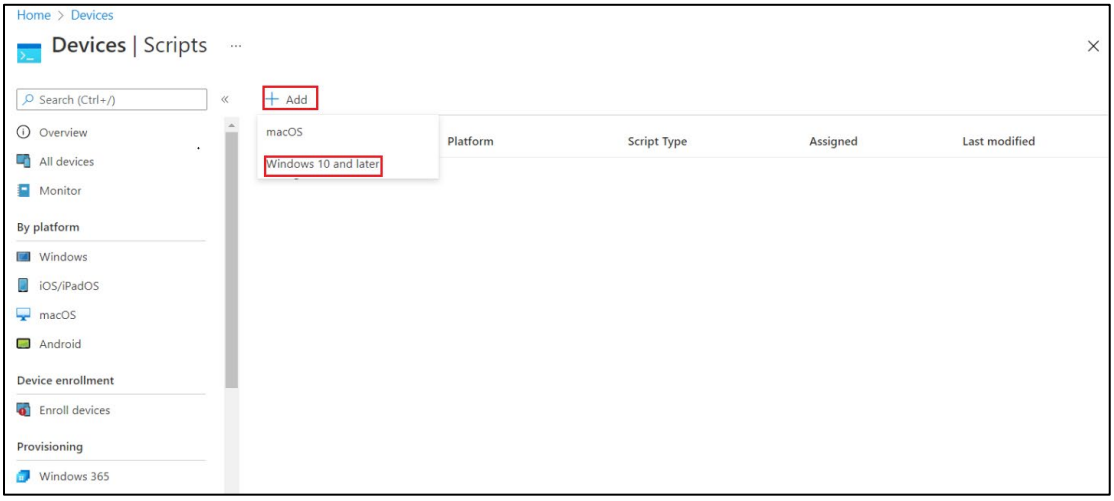
Deploying PowerShell Script to configure the Settings

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

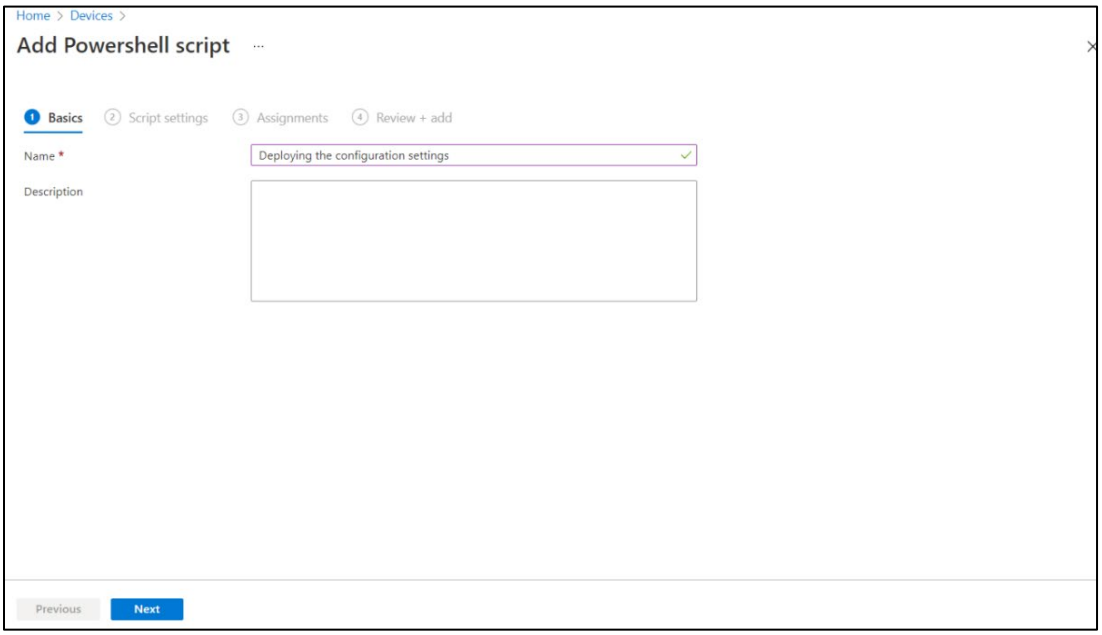
1. In the left pane of the Microsoft Endpoint Manager admin center, select **Devices > Scripts**.



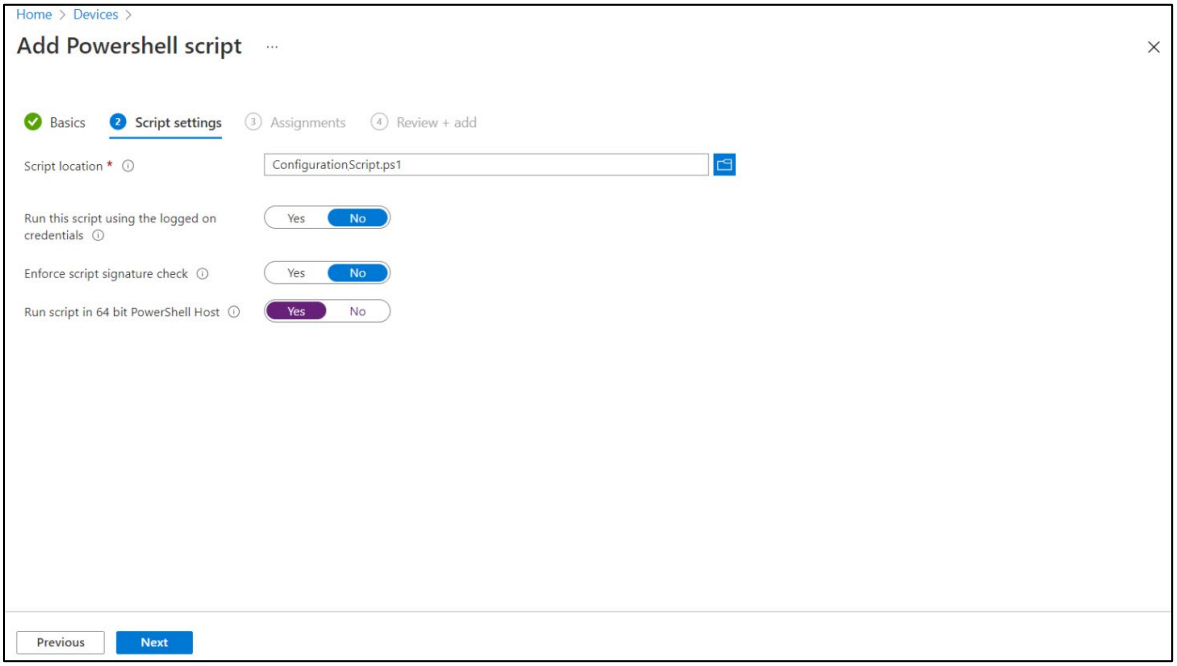
2. Click **Add** to add a new PowerShell script, and then select **Windows 10 and later** to deploy it to Windows 10 (and later) devices.



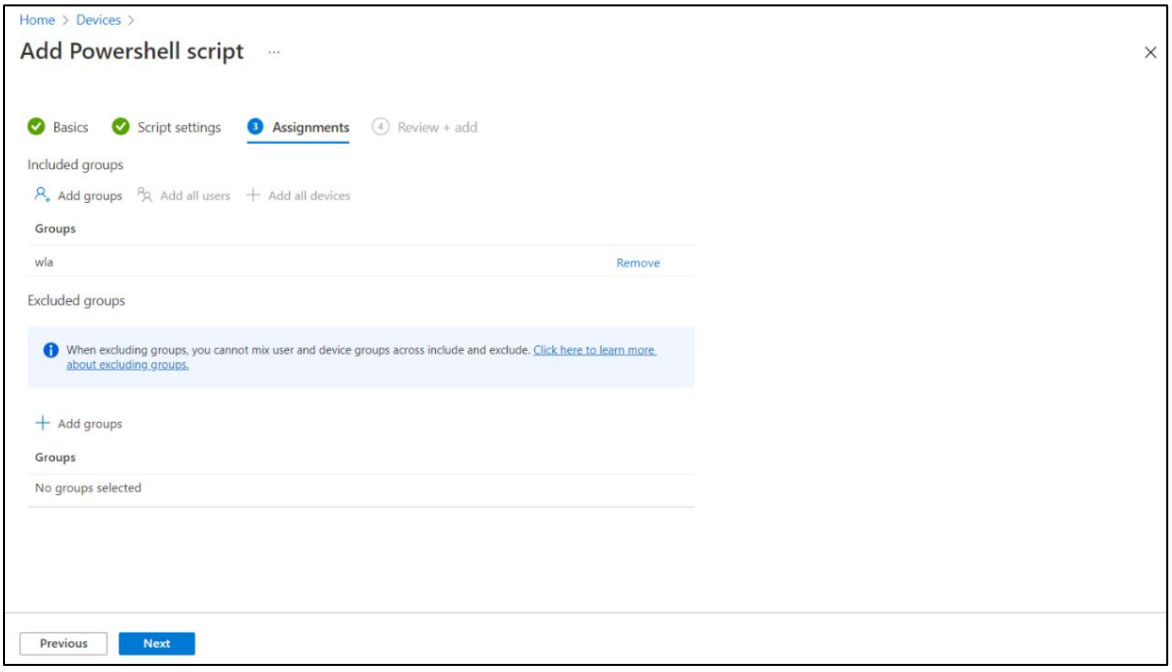
3. In the **Add Powershell script** window, under the **Basics** tab, enter the following properties:
   a. **Name**: Enter a name for the PowerShell script. For example, Deploying the configuration settings.
   b. **Description**: [Optional] Enter a description for the PowerShell script.
   c. Click **Next**.



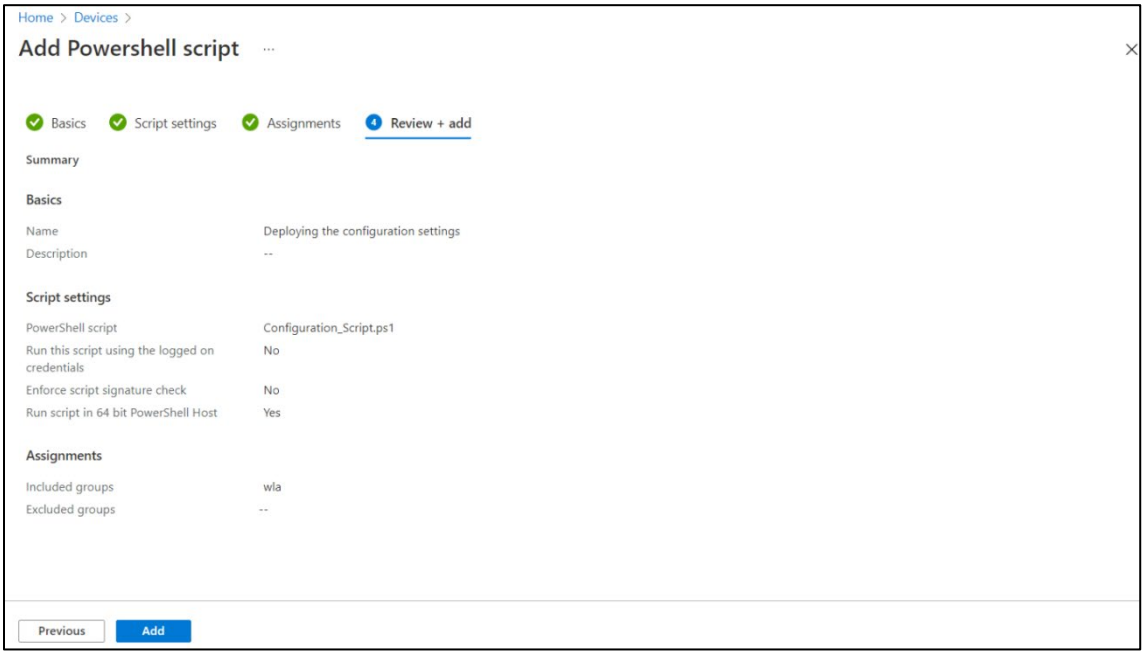
4. Under the **Script settings** tab, enter the following properties:
   a. **Script location**: Browse to the PowerShell script (ConfigurationScript.ps1) that is present in the Intune-Deployment folder. For example, C:\Intune-Deployment\ConfigurationScript.ps1
   b. **Run script in 64-bit PowerShell 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.
   c. Click **Next**.



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



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

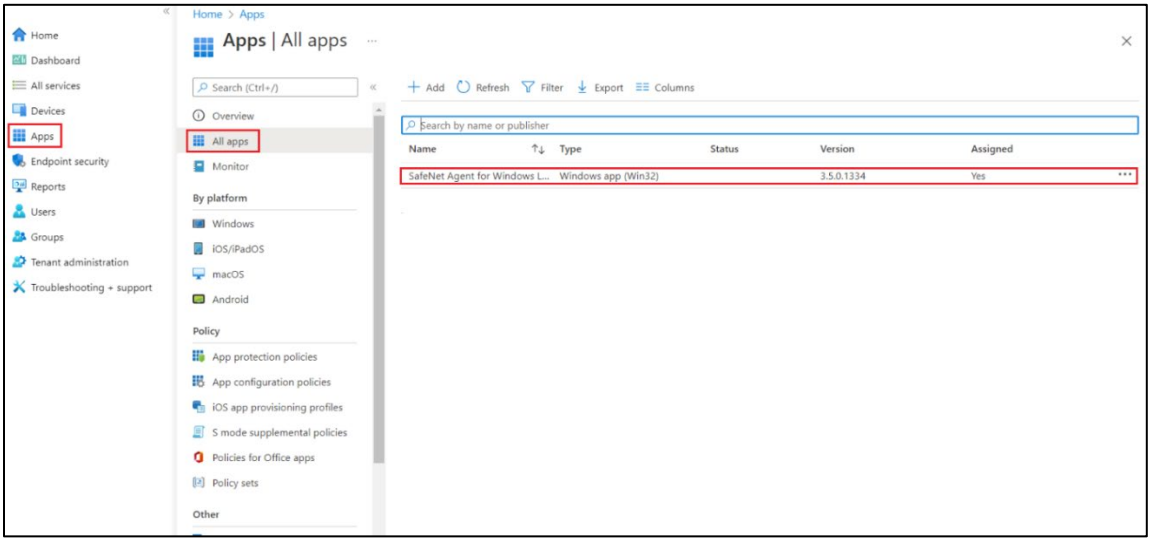


After selecting **Add**, the policy is deployed to the groups you chose.

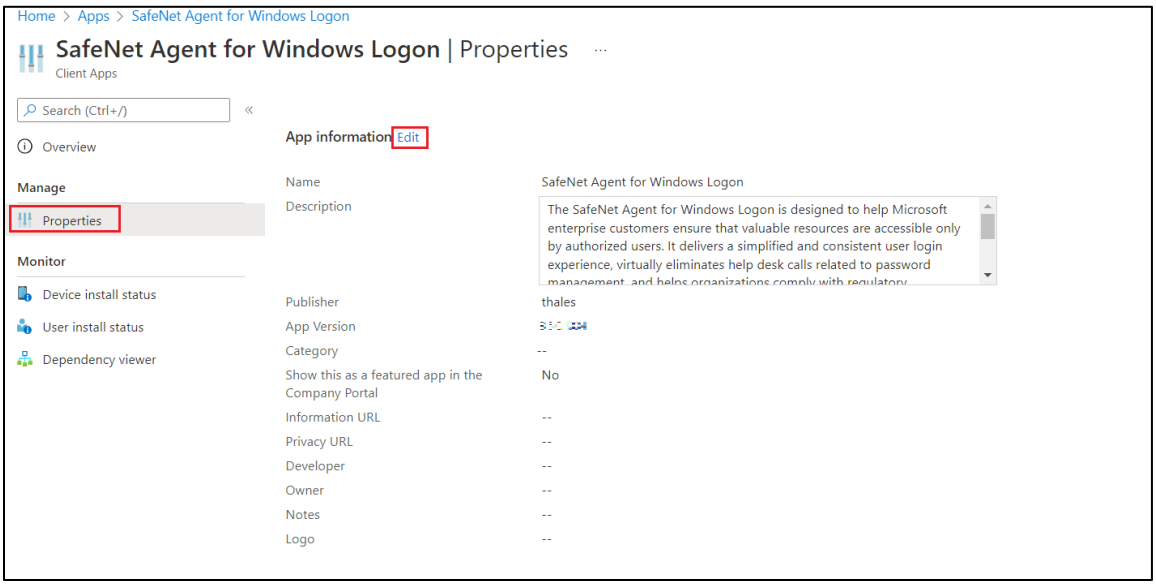
Upgrading SafeNet Agent for Windows Logon

To upgrade the agent with the latest version, perform the following steps:

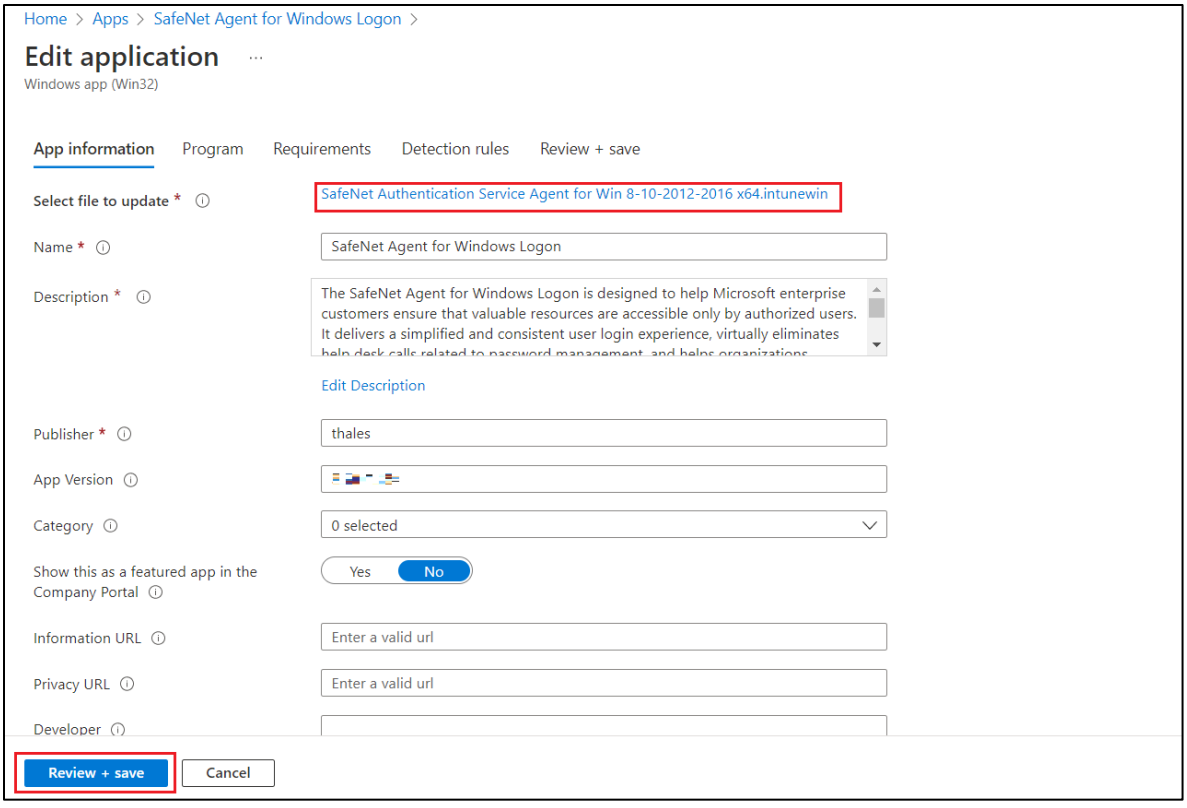
1. Perform all the steps in Creating an IntuneWin package.
2. Login to the Microsoft Endpoint Manager admin center using https://endpoint.microsoft.com.
3. In the left pane, select **Apps > All apps**. Select the previously created app.



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



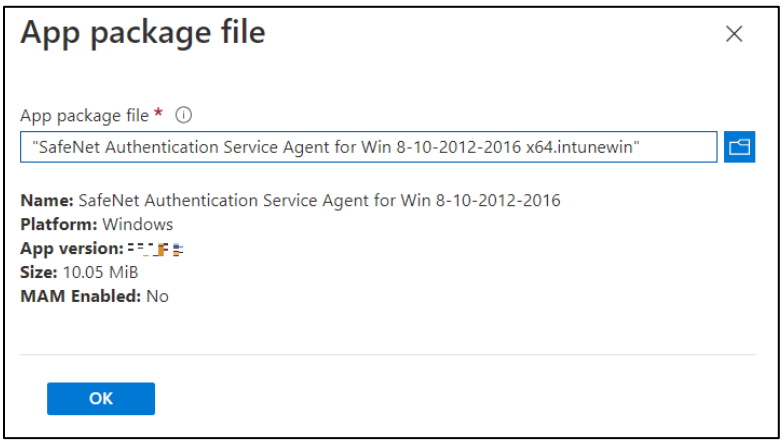
5. Under the **App information** tab, click the previously created app from the **Select file to update** field.



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

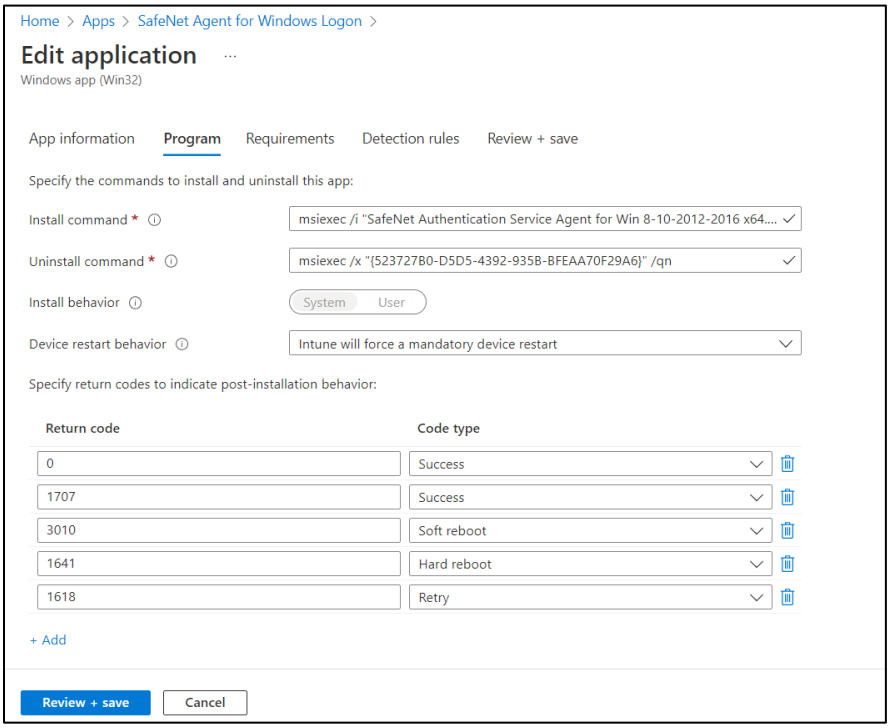
a. Click to select the newly created App package file, that is, *SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64.intunewin*, which you have previously created in **Step 1**.

b. Click **OK**.



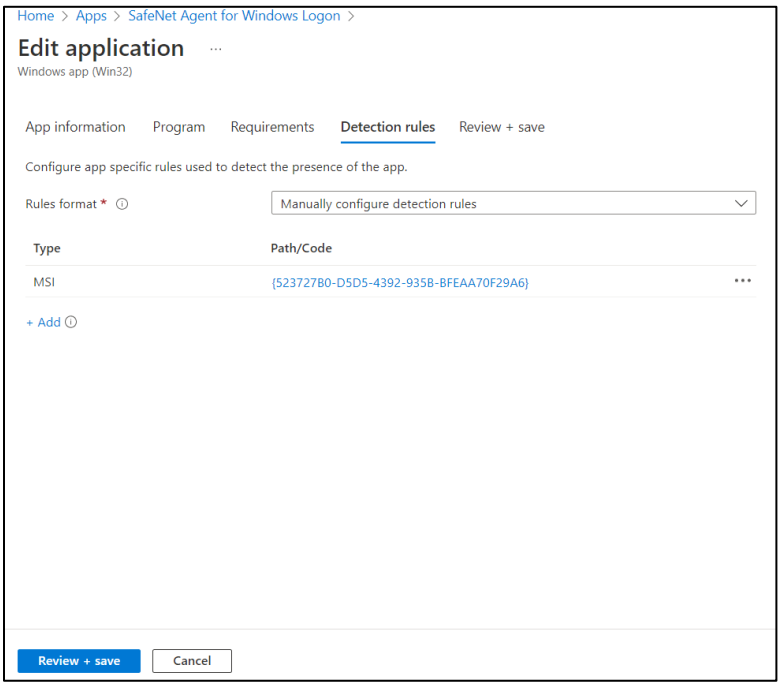
Click **Review + save** on the **App information** page to display the **Program** page.

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.



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

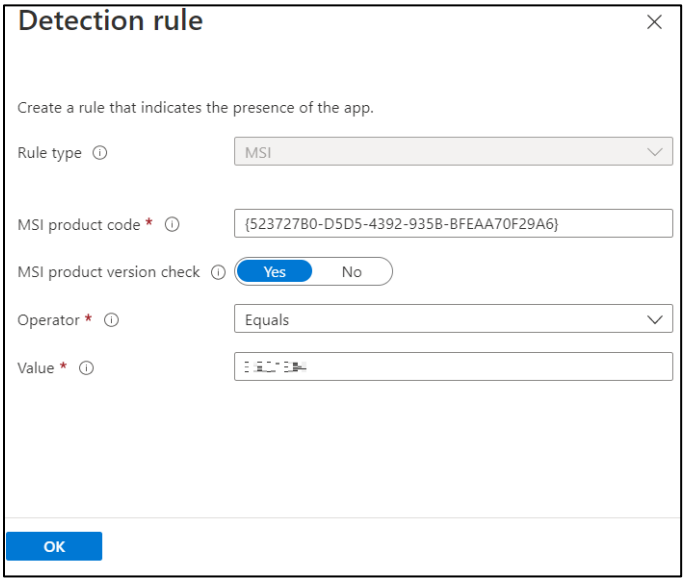
7. Under the **Requirements** tab, click **Review + save** to display the **Detection rules** page.
8. Under the **Detection rules** tab, select the value of **Path/Code** of the previously created detection rule.



Detection rule window appears. Perform the following steps:

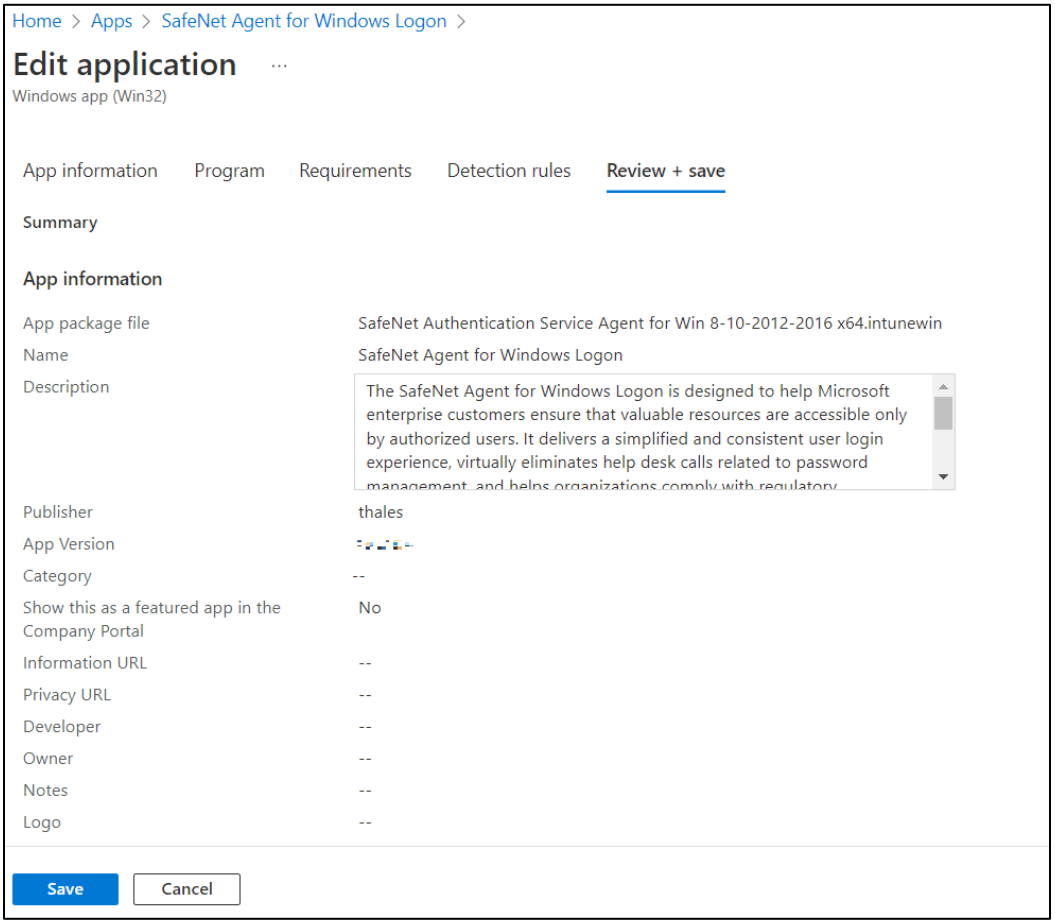
a. In the **Value** field, enter the **latest Build number** as mentioned in the CRN.

b. Click **OK**.



Click Review + save.

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

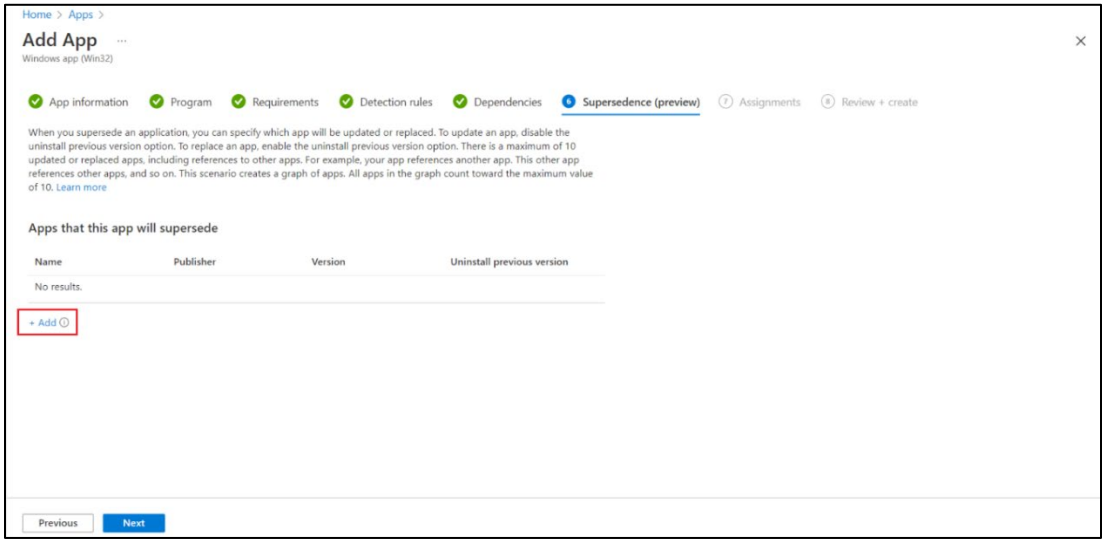


After performing the above steps, SafeNet Agent for Windows Logon will be upgraded to its latest version. **WLA will not be installed on the newly added devices through the upgrade process**.

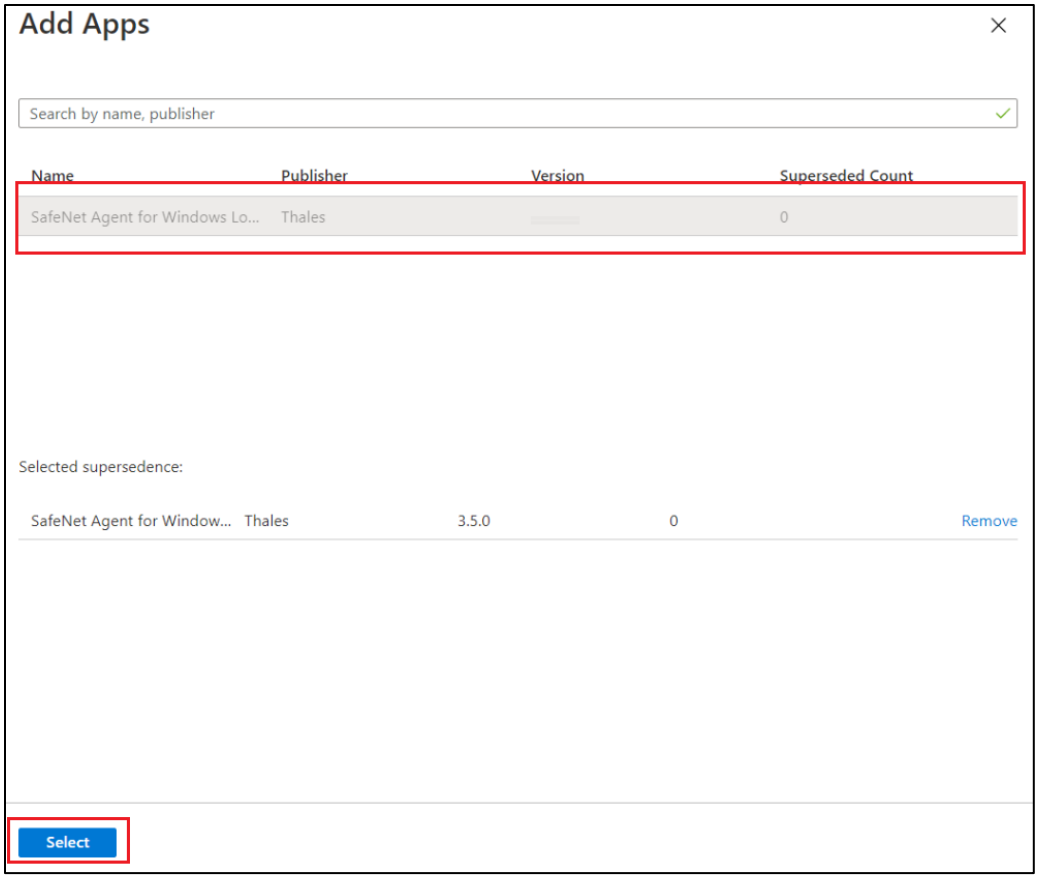
> **IMPORTANT:** For an ongoing upgrade, you must wait until all the devices are successfully upgraded before installing the agent on the newly added devices.

To install the agent 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.
   a. In the **Supersedence (preview)** tab, perform the following steps:
   i. Click **Add**.



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



ii. Click **Next**.

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

CHAPTER 5: Deploying the agent via Microsoft Endpoint Configuration Manager

This section describes the steps to deploy the agent via **Microsoft Endpoint Configuration Manager**, formerly known as, **Microsoft System Center Configuration Manager** (SCCM).

> The agent deployment is tested with Microsoft Endpoint Configuration Manager version **2203**.

Prerequisites

As a prerequisite,

- Microsoft Endpoint Configuration Manager must be installed on the admin machine from which the agent will be deployed on the client machines.
- Configuration Manager client must be installed on all the machines in which the agent needs to be deployed.

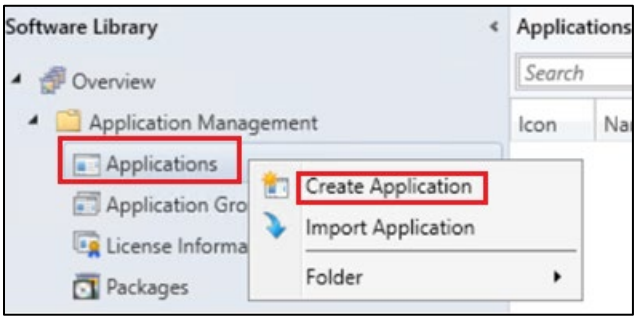
Installing the agent

Installing the agent involves the following steps:

1. Creating an Application in Microsoft Endpoint Configuration Manager
2. Distributing the content (Application)
3. Deploying the application into client machines
4. Pushing computer policy to the client machines

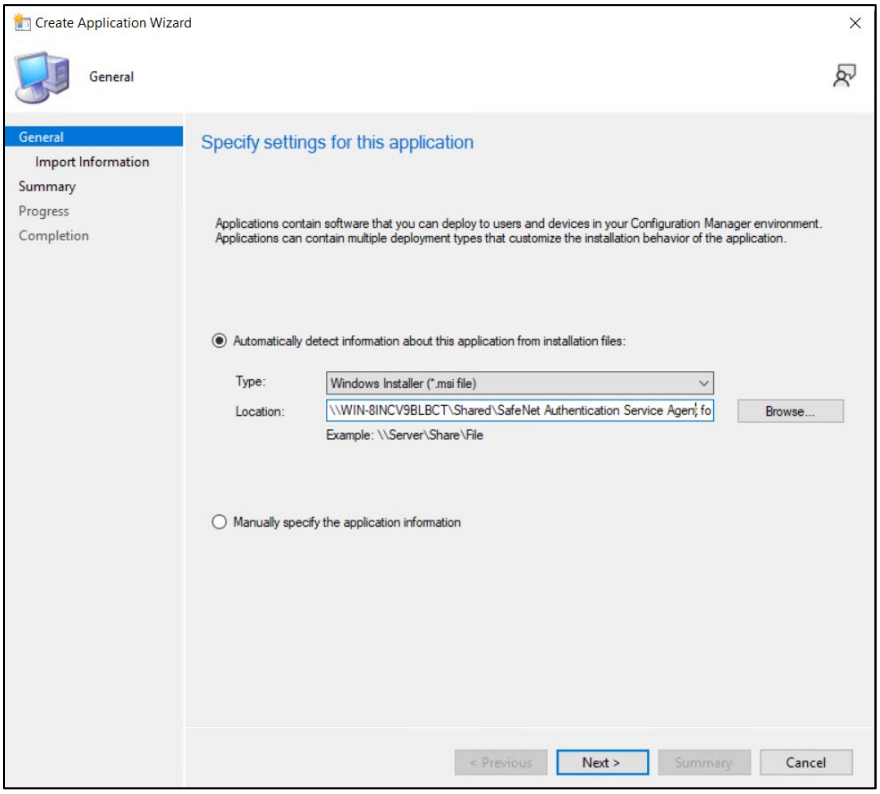
Creating an Application in Microsoft Endpoint Configuration Manager

1. Open the Configuration Manager console. On the left pane, click **Software Library** > **Application Management** > **Applications** > **Create Application**.



2. On the **Create Application Wizard** window, under **General**, in the **Location** field, enter the file path where the SafeNet Agent for Windows Logon MSI is present in UNC format.
For example, \\WIN-8INCV9BLBCT\Shared\SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64.MSI

   NOTE: Use the default MSI name as provided in the downloaded agent package.

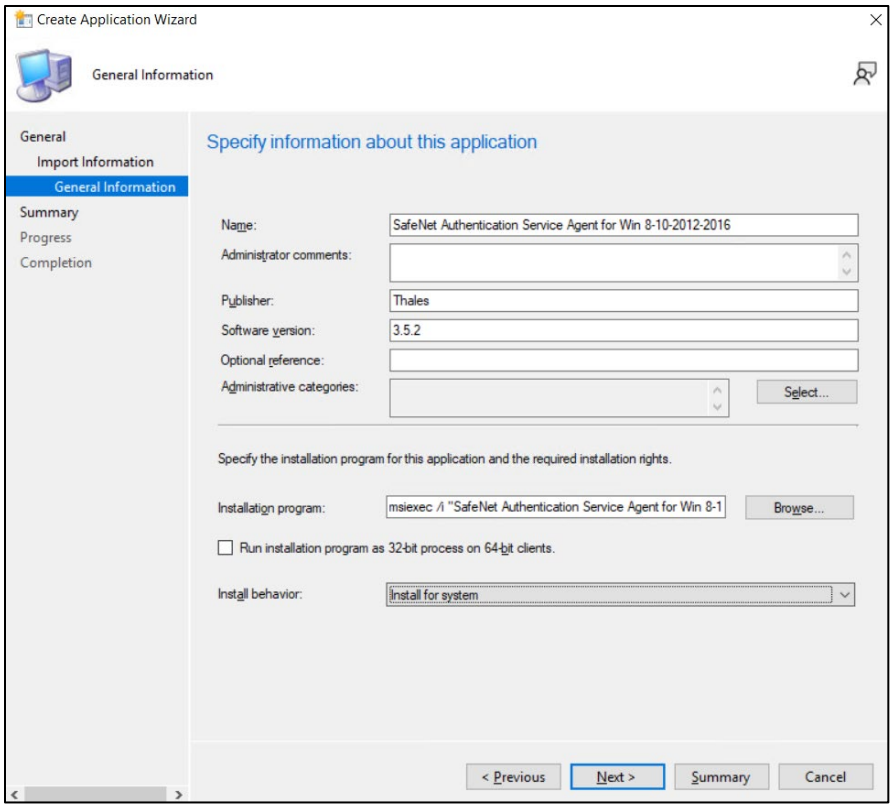


3. Click **Next**.
4. On the **Import Information** window, click **Next**.
5. On the **General Information** window, perform the following steps:
   a. In the **Name** field, enter the application name of your choice or proceed with the default name, that is, SafeNet Authentication Service Agent for Win 8-10-2012-2016.
   b. In the **Publisher** field, enter the company name. For example, Thales.
   c. In the **Software version** field, enter the version of the agent. For example, 3.5.2.
   d. In the **Installation program** field, enter the following command:
   `msiexec /i "SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64.MSI" /quiet TOKENVALIDATORLOCATION=<Primary SafeNet Server IP address or hostname or FQDN>`

      NOTE: With the above command, after the agent installation, hard restart will be triggered on the client device. To avoid this, append **/norestart** parameter in the above command and ensure that you restart the client device later (for the agent to work properly).

   e. In the **Install behavior** drop-down, ensure **Install for system** is selected.

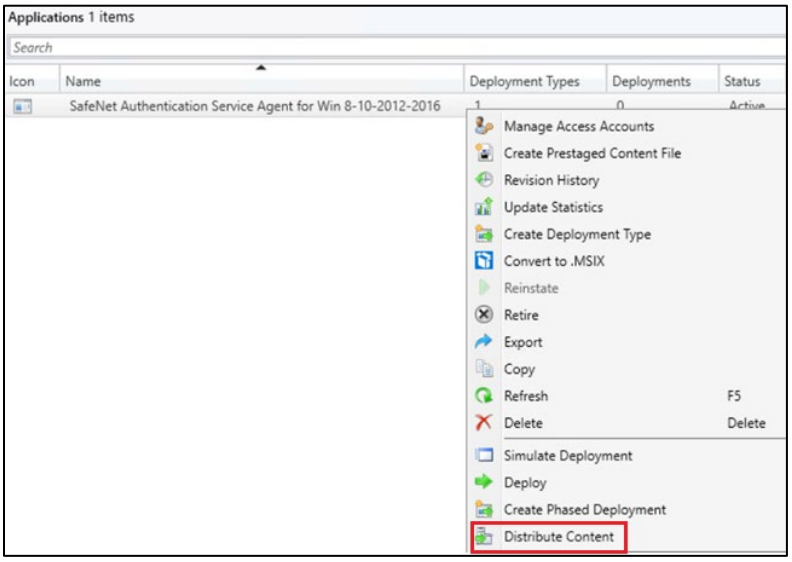
f. Click **Next**.



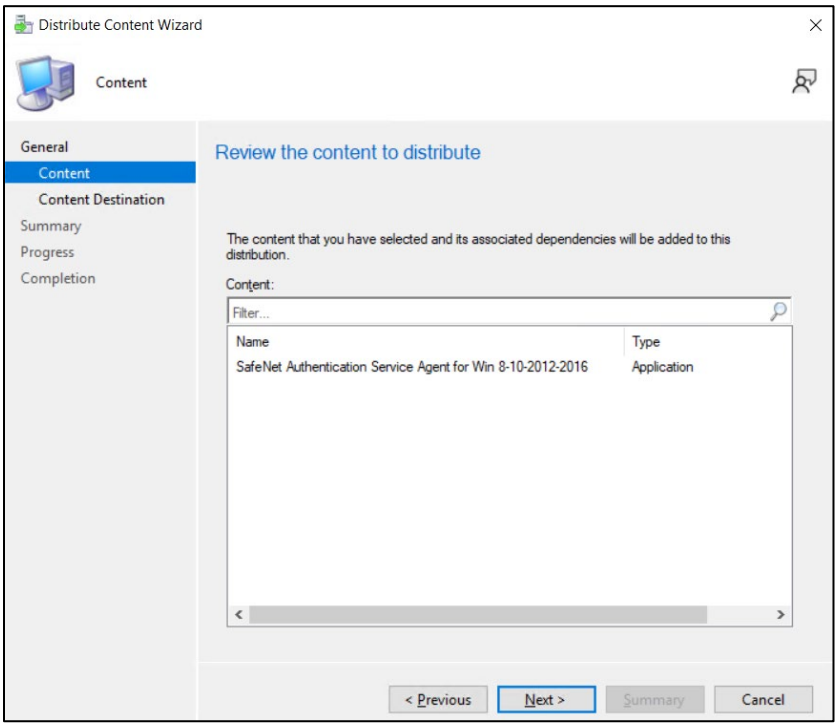
6. On the **Summary** window, click **Next**.
7. On the **Completion** window, click **Close**.

Distributing the content (Application)

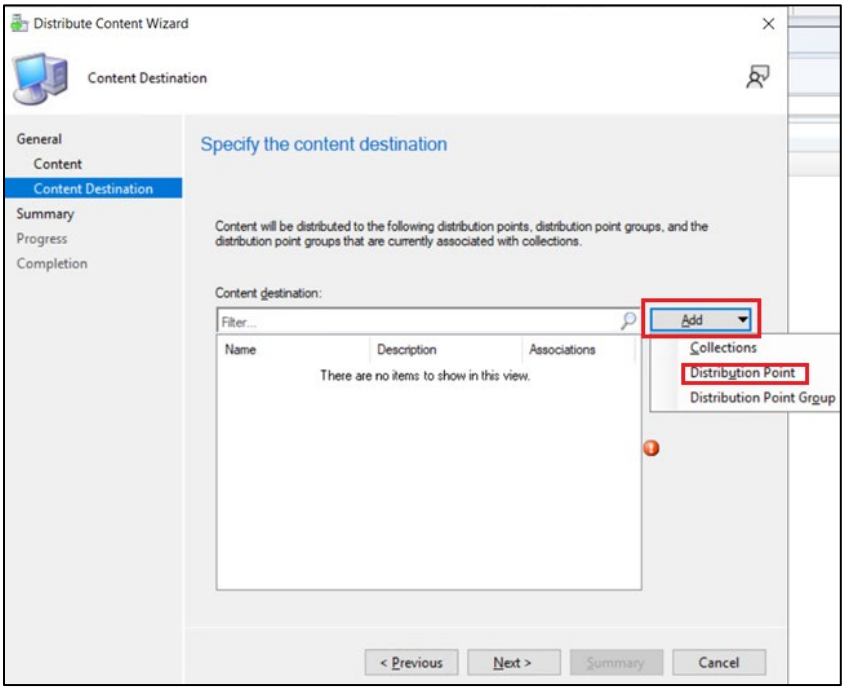
1. On the Configuration Manager console, on the right pane, under **Applications**, right-click on the application that you have created in the above step, and then click **Distribute Content**.



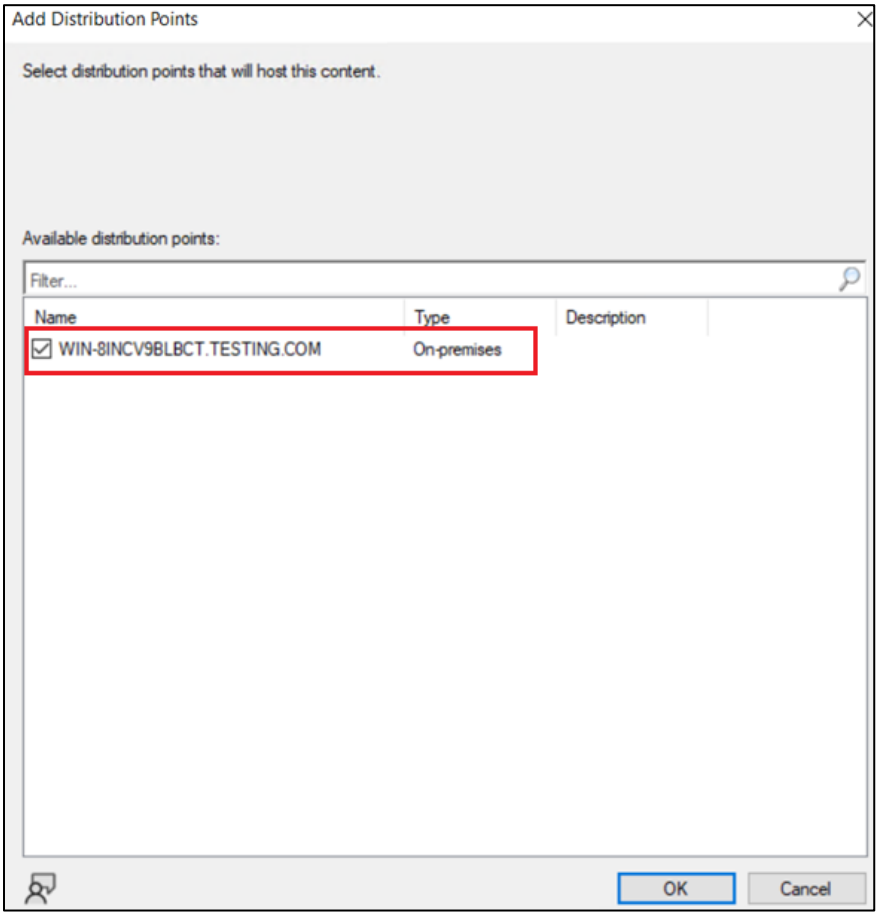
2. On the **Distribute Content Wizard**, under **General**, click **Next**.
3. On the **Content** window, ensure that your application name is listed and then click **Next**.



4. On the **Content Destination** window, click **Add** and then click **Distribution Point**.



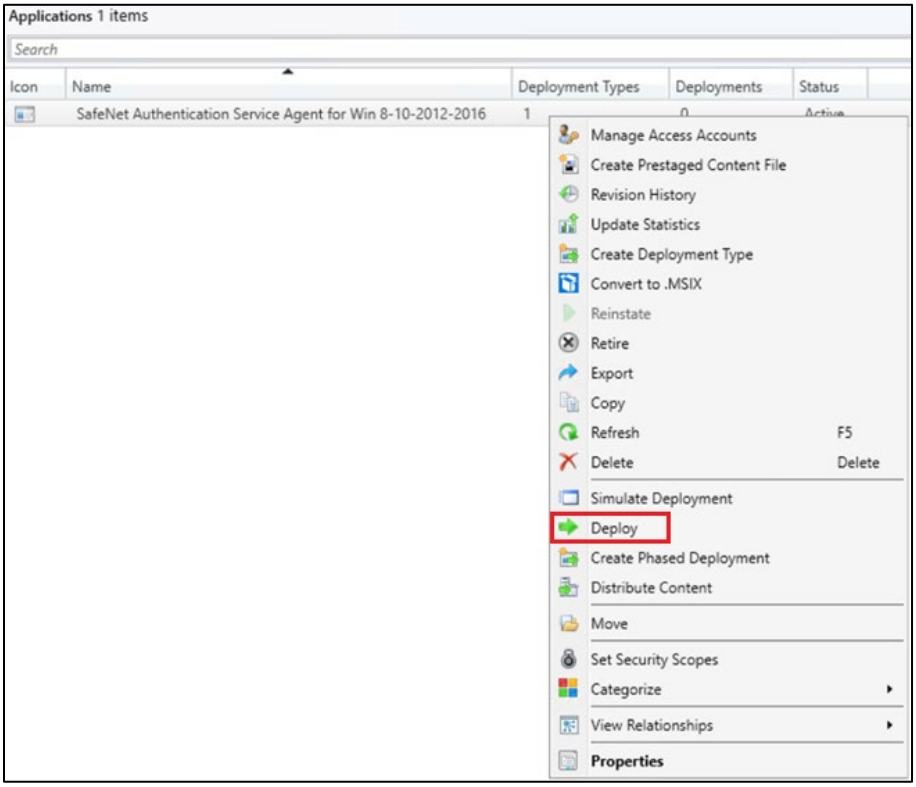
5. On the **Add Distribution Points** window, under **Available distribution points**, select the distribution point that will host the content.



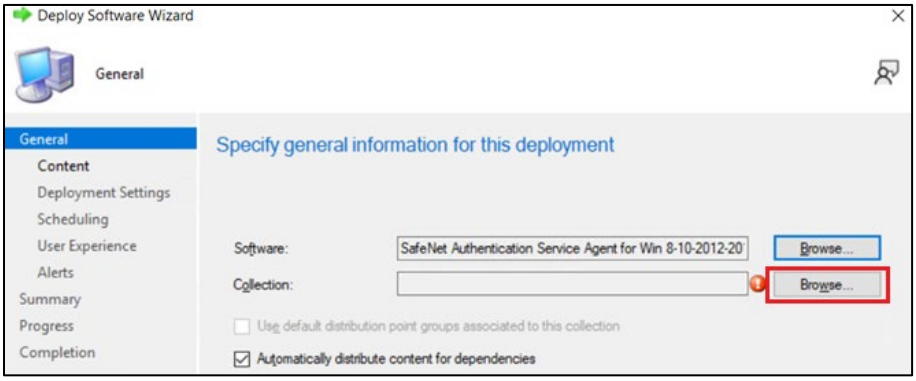
6. Click **OK**.
7. On the **Content Destination** window, click **Next**.
8. On the **Summary** window, click **Next**.
9. On the **Completion** window, click **Close**.

Deploying the application into client machines

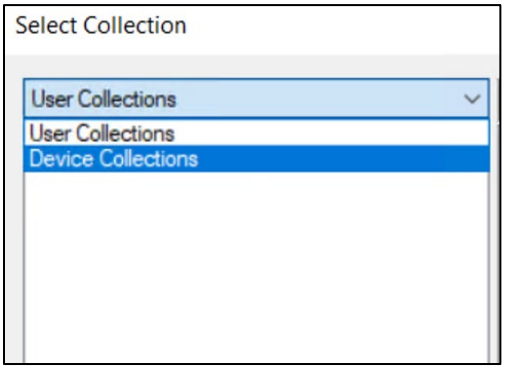
1. Under **Applications,** right-click the application that you have created in Creating an Application in Microsoft Endpoint Configuration Manager section and then click **Deploy**.



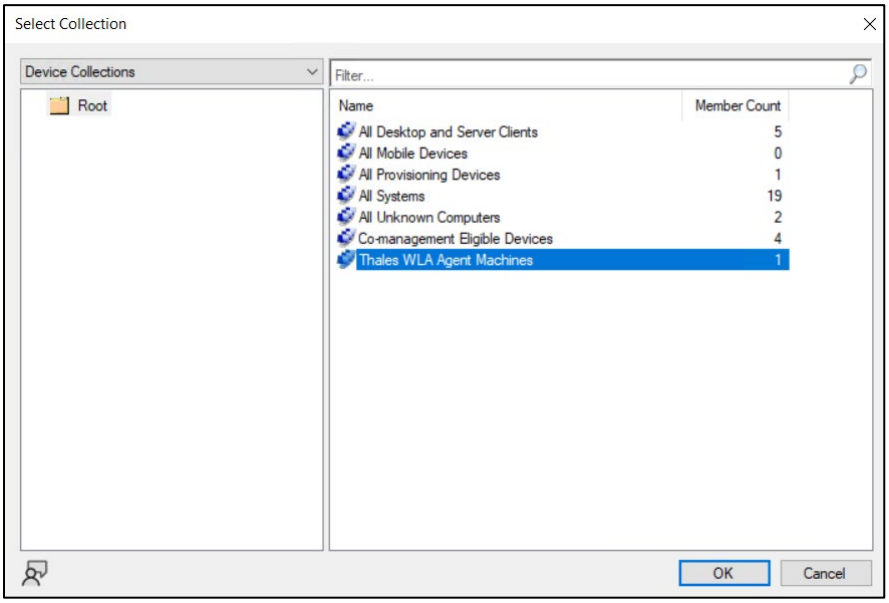
2. On the **Deploy Software Wizard**, under **General**, click **Browse** displayed against the **Collection** field.



Now, under **Select Collection** window, select **Device Collections** from the drop-down.

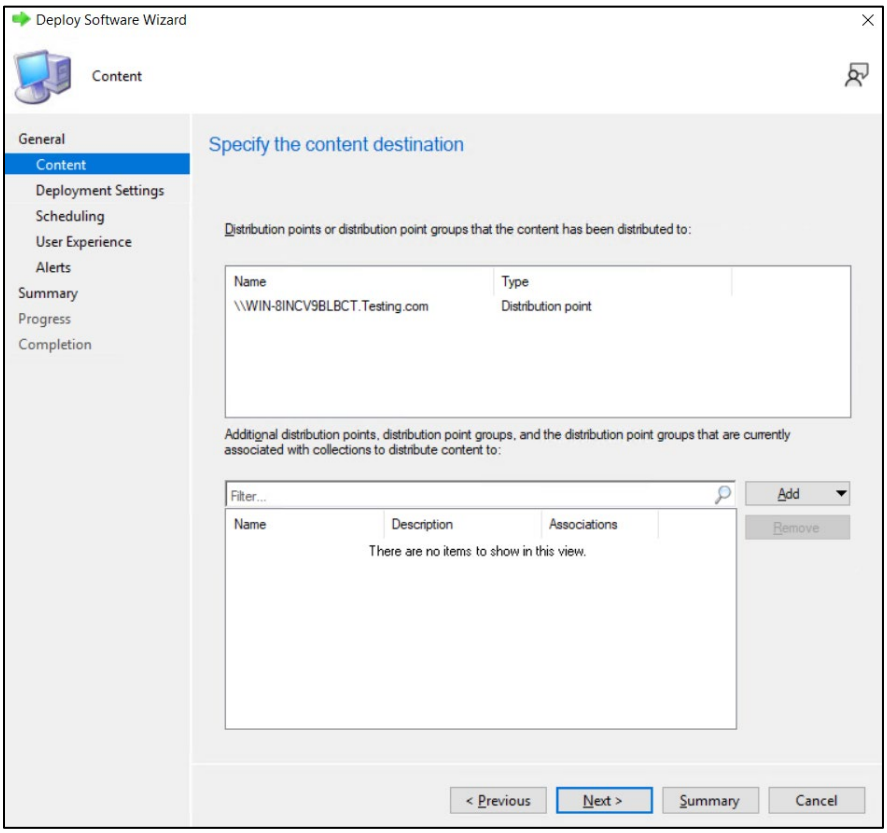


3. Under **Device Collections**, select the device collection where you want to deploy the agent and then click **OK**.

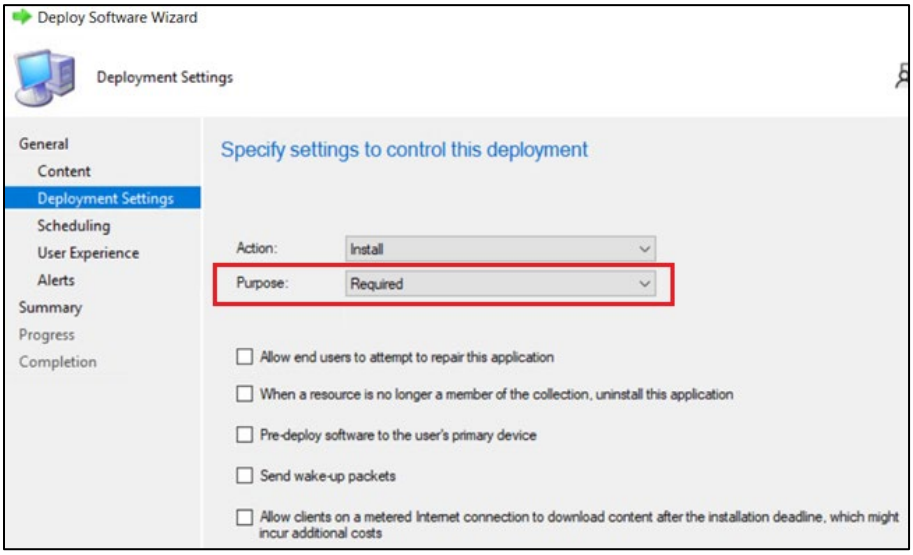


4. On the **General** window, click **Next**.

5. Under **General** > **Content**, ensure that the distribution point that you have selected in Distributing the content (Application) is listed and then click **Next**.



6. Under **General** > **Deployment Settings**, in **Purpose**, select **Required** from the drop-down and then click **Next**.

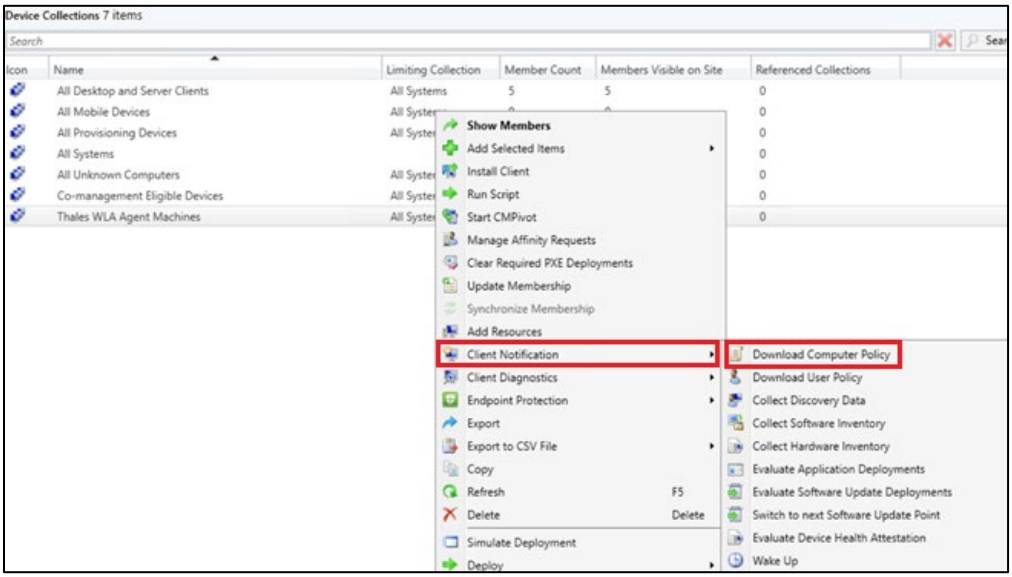


7. Under **General** > **Scheduling**, proceed with the default settings and click **Next**.
8. Under **General** > **User Experience**, proceed with the default settings and click **Next**.
9. Under **General** > **Alerts**, proceed with the default settings and click **Next**.
10. On the **Summary** window, click **Next**.
11. On the **Completion** window, click **Close**.

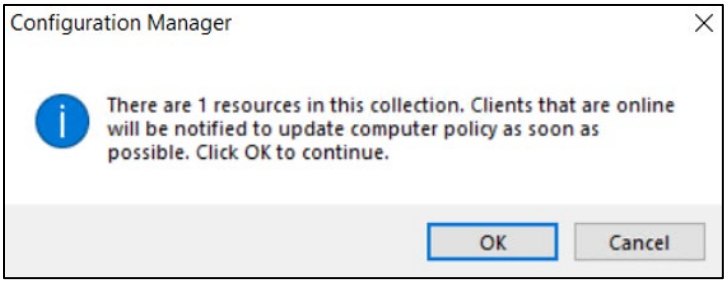
Pushing computer policy to the client machines

1. On the left pane, click **Assets and Compliance** > **Device Collections**.

2. Under **Device Collections**, on the right pane, right-click on the device collection which you have selected in Step 3 of Deploying the application into client machines section**.** Click **Client Notification** and then click **Download Computer Policy**.



3. On the **Configuration Manager** pop-up, click **OK**.



After following the above steps, the agent will be successfully deployed on the client machine.

> **NOTE**: Restart might be required after the installation.

Configuring the Registry Settings

This section involves the steps to configure the registry key values as per your requirement. After the configuration, the updated registry key values will be pushed to the client machines.

Perform the following steps to configure the registry settings:

1. Copy the SCCM-Deployment folder from the downloaded agent package
2. Creating an Application in Microsoft Endpoint Configuration Manager
3. Distributing the content (Application)
4. Deploying the application into client machines
5. Pushing computer policy to the client machines

Copy the SCCM-Deployment folder from the downloaded agent package

1. Copy the **SCCM-Deployment** folder from the downloaded agent package and paste it on your local machine. The files present in this folder will be used later.

   The **SCCM-Deployment** folder contains the following two files:

   - **ConfigurationSetup.cmd**
   - **RegistryConfiguration.reg**

   > **NOTE**: If you rename the registry file named **RegistryConfiguration**, then update the same in **ConfigurationSetup.cmd** file.

2. To update the registry file,
   a. Open the **RegistryConfiguration.reg** file in any text editor.
   b. Uncomment the specific registry entry that you want to change by removing semi-colon (;).
   c. Change the registry key's value as per your requirement. For example, change the **LogLevel** key value from **3** to **4**.

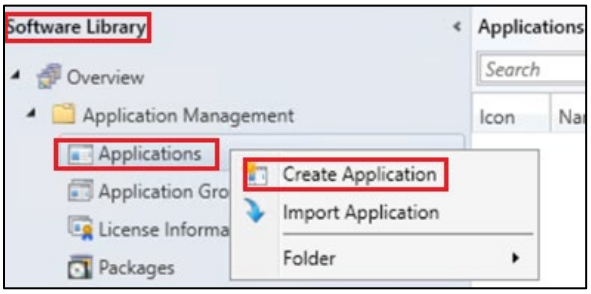
   For more details about the Registry Settings, click here.
3. Save the **RegistryConfiguration.reg** file after making the required changes.

It is recommended that you take a backup of the updated **RegistryConfiguration.reg** file for contigencies.

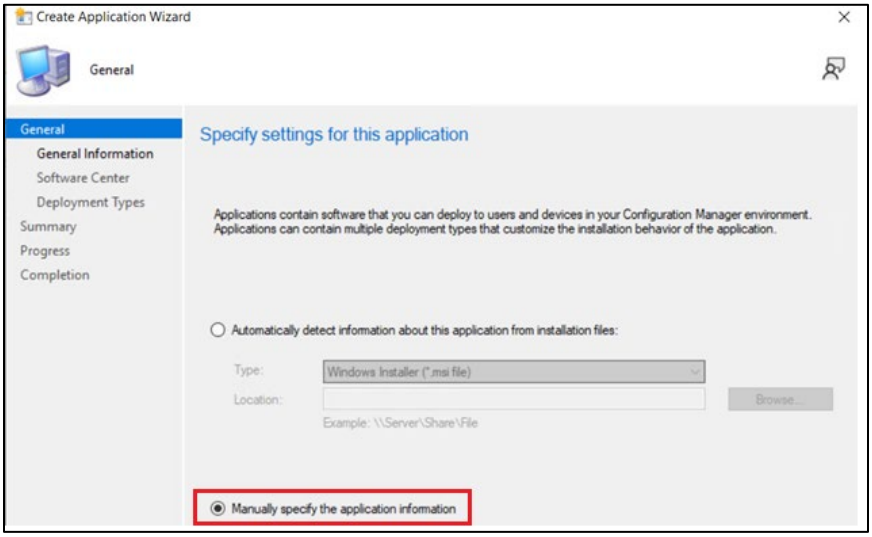
Creating an Application in Microsoft Endpoint Configuration Manager

To push the updated registry settings into the client machines, you need to create an application and deploy it.

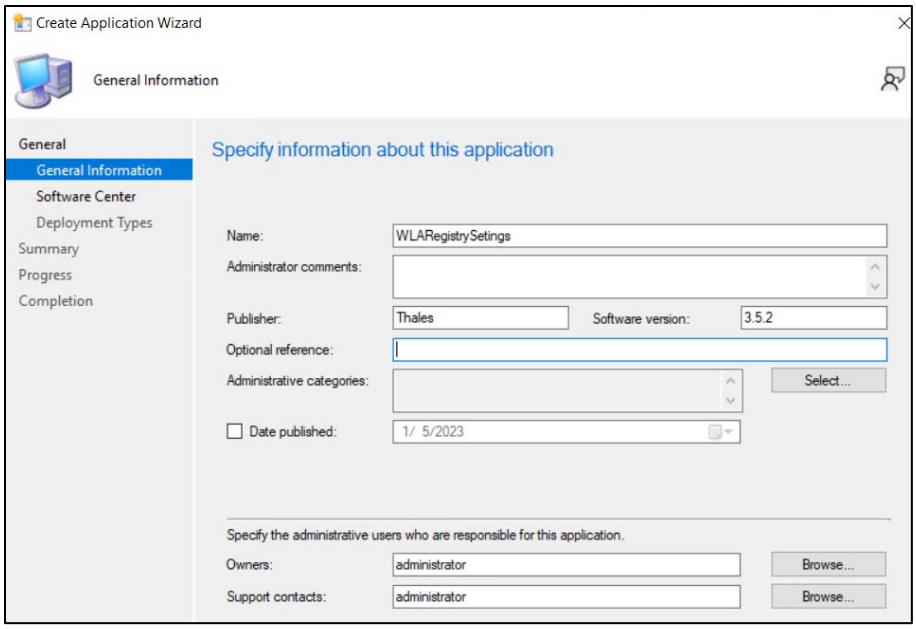
1. Open the Configuration Manager console. On the left pane, click **Software Library** > **Application Management** > **Applications** > **Create Application**.



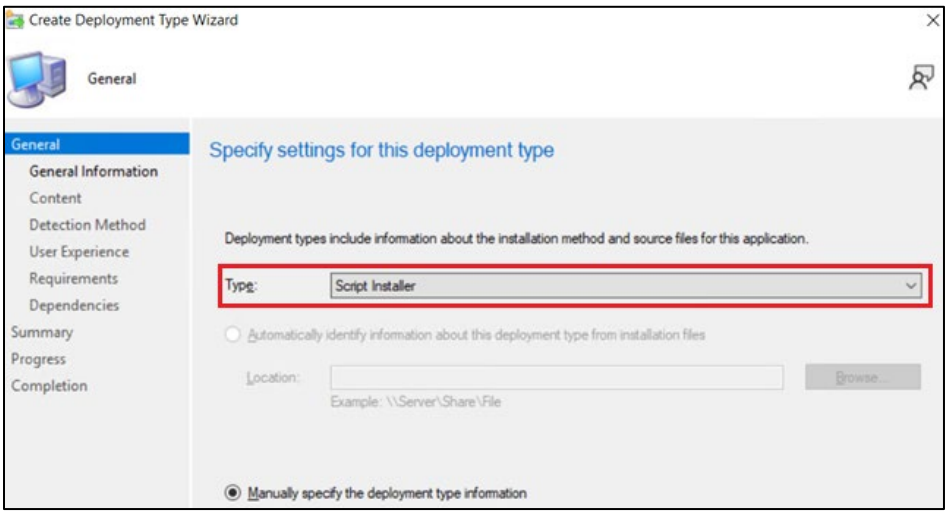
2. On the **Create Application Wizard**, under **General**, select **Manually specify the application information** radio button and then click **Next**.



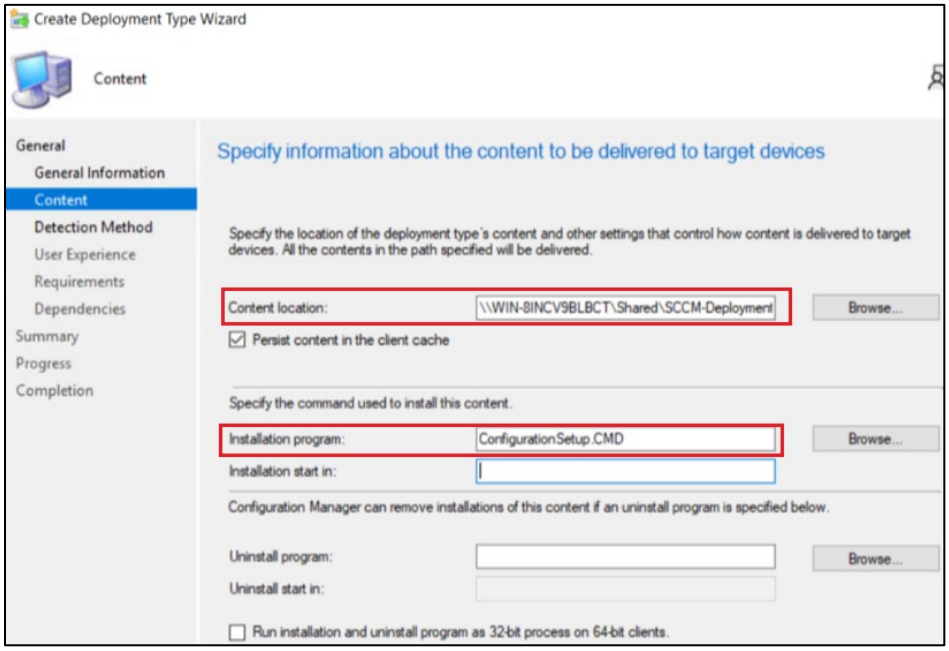
3. Under **General** > **General Information**, perform the following steps:
   a. In the **Name** field, enter the name of the application. For example, WLARegistrySettings.
   b. In the **Publisher** field, enter the company name. For example, Thales.
   c. In the **Software version** field, enter the version of the agent for these registry settings. For example, 3.5.2.
   d. Click **Next**.



4. Under **General** > **Software Center**, proceed with the default settings and click **Next**.
5. Under **General** > **Deployment Types**, click **Add**.
6. On the **Create Deployment Type Wizard**, under **General**, select **Script Installer** from the **Type** drop-down and then click **Next**.



7. Under **General** > **General Information**, in the **Name** field, enter a name for the deployment type. For example, WLARegistrySettings and then click **Next**.
8. Under **General** > **Content**,
   a. In the **Content location** field, enter the SCCM-Deployment folder path in the UNC format that you have copied in the Step 1 of Copy the SCCM-Deployment folder from the downloaded package section. For example, \\WIN-8INCV9BLBCT\Shared\SCCM-Deployment
   b. In the **Installation program** field, enter the CMD file name present in SCCM-Deployment folder. For example, ConfigurationSetup.CMD.



   c. Click **Next**.
9. Under **General** > **Detection Method**, click **Add Clause**.
   a. On the **Detection Rule** window, perform the following steps:
   i. In the **Setting Type** field, ensure that **File System** is selected.

ii. In the **Type** field, ensure that **File** is selected.

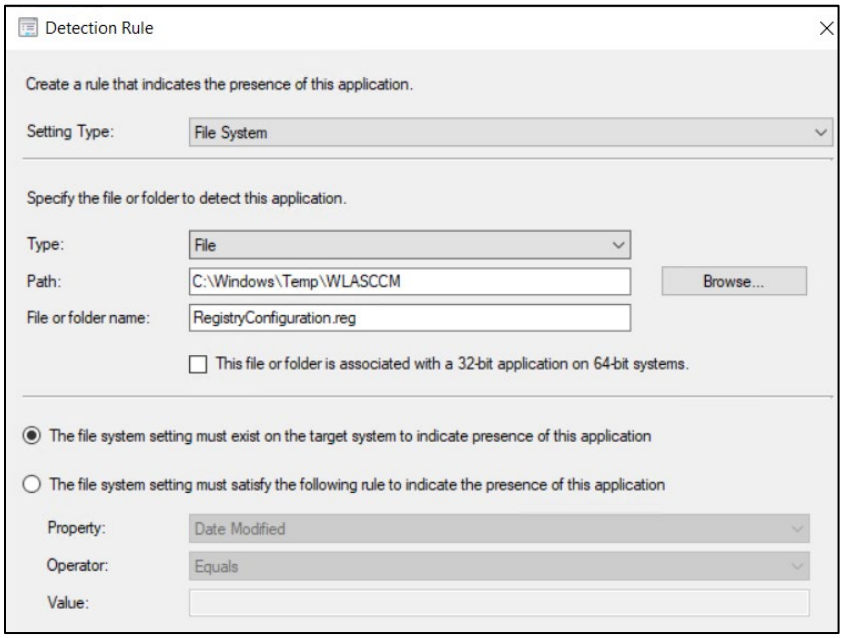
iii. In the **Path** field, enter **C:\Windows\Temp\WLASCCM**.

> **NOTE**: The above path is mentioned in **ConfigurationSetup.CMD** file, which is present in the **SCCM-Deployment** folder.

iv. In the **File or folder name** field, enter the registry file name (for example, RegistryConfiguration.reg) that is present in the SCCM-Deployment folder.

v. Un-check **This file or folder is associated with a 32-bit application on 64-bit systems** checkbox.

vi. Click **OK**.



10. Under **General** > **Detection Method**, click **Next**.

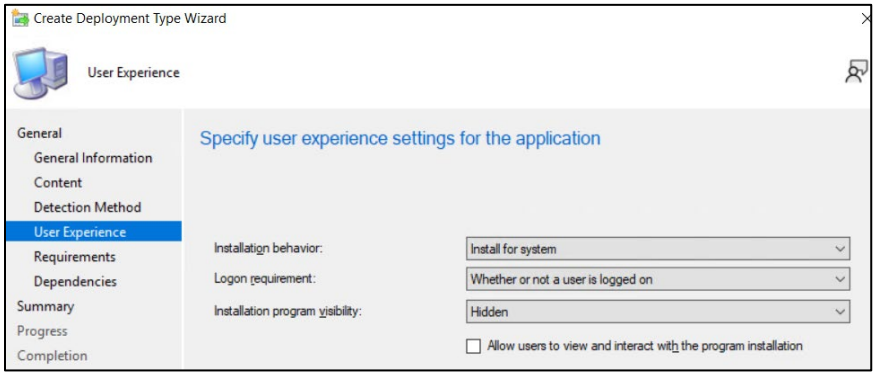
11. Under **General** > **User Experience**, perform the following steps:

a. In **Installation behavior**, select **Install for system** from the drop-down.

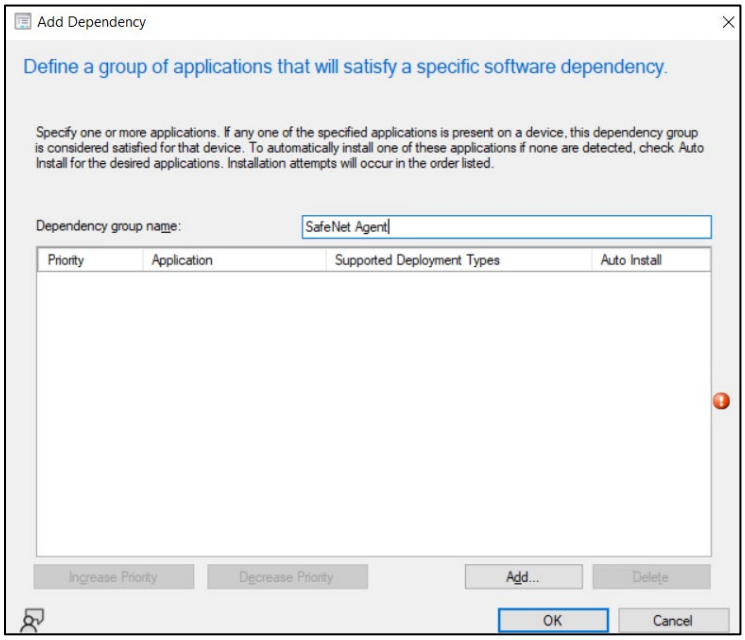
b. In **Logon requirement**, select **Whether or not a user is logged on** from the drop-down.

c. In **Installation program visibility**, select **Hidden** from the drop-down.

d. Click **Next**.



12. Under **General** > **Requirements**, click **Next**.
13. Under **General** > **Dependencies**, click **Add**.
    a. On the **Add Dependency** window, in the **Dependency group name** field, enter the dependency group name. For example, SafeNet Agent and then click **Add**.

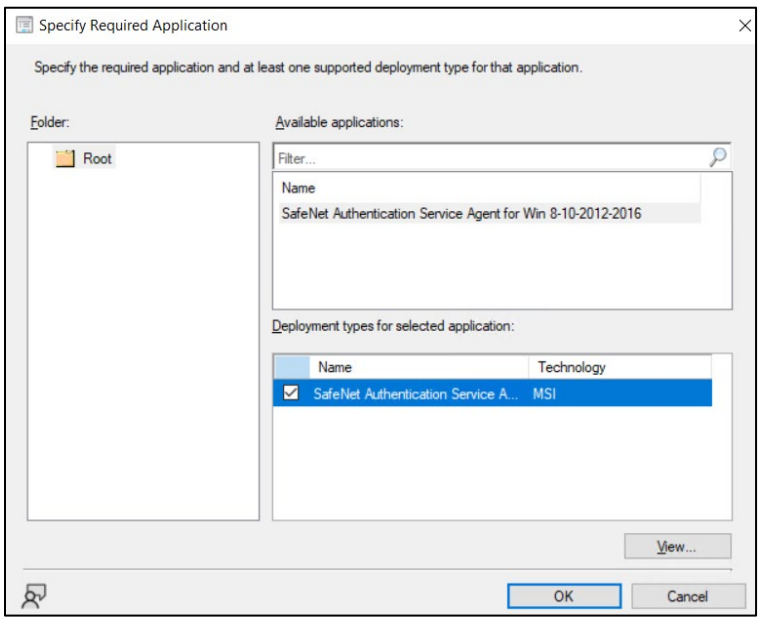


    b. On the **Specify Required Application** window, perform following steps:

    i. Under **Available applications**, click the application name that you have created in Creating an Application in Microsoft Endpoint Configuration Manager section.
    For example, SafeNet Authentication Service Agent for Win 8-10-2012-2016.

    ii. Under **Deployment types for selected application**, select the MSI checkbox.

    iii. Click **OK**.



c. On the **Add Dependency** window, uncheck the checkbox under the **Auto Install** column (displayed against the application that you have selected in previous step) and then click **OK**.

d. Click **Next**.

14. On the **Summary** window, click **Next**.
15. On the **Completion** window, click **Close**.
16. On the **Create Application Wizard**, under **General** > **Deployment Types**, click **Next**.
17. On the **Summary** window, click **Next**.
18. On the **Completion** window, click **Close**.

Distributing the content (Application)

Perform the steps mentioned in **Distributing the content (Application)** section to distribute the **WLARegistrySettings** application, which you have created in the above step.

Deploying the application into client machines

Perform the steps mentioned in **Deploying the application into client machines** section to deploy the **WLARegistrySettings** application, which you have created in the above step.

Pushing computer policy to the client machines

Perform the steps mentioned in **Pushing computer policy to the client machines** section to push the computer policy to the client machines for the **WLARegistrySettings** application, which you have created in the above step.

Uninstalling the agent

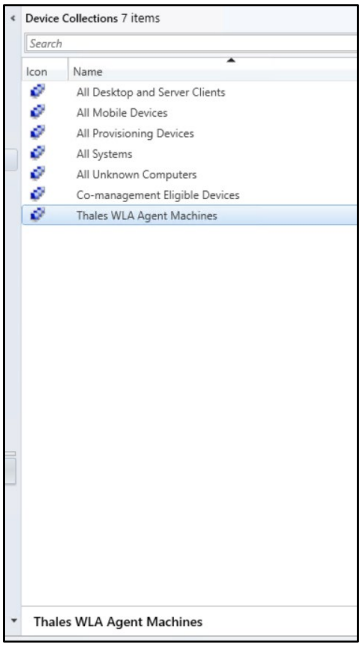
This section involves the following steps to uninstall the agent:

1. Deleting the deployment from Device Collection
2. Deploying the application into client machines for uninstallation
3. Pushing computer policy to the client machines

Deleting the deployment from Device Collection

1. On the left pane, click **Assets and Compliance** > **Overview** > **Device Collections**.

2. Under **Device Collections**, on the right pane, click on the device collection from where you want to uninstall the agent. Then, on the bottom pane, click on your device collection tile to view the **Deployments**.



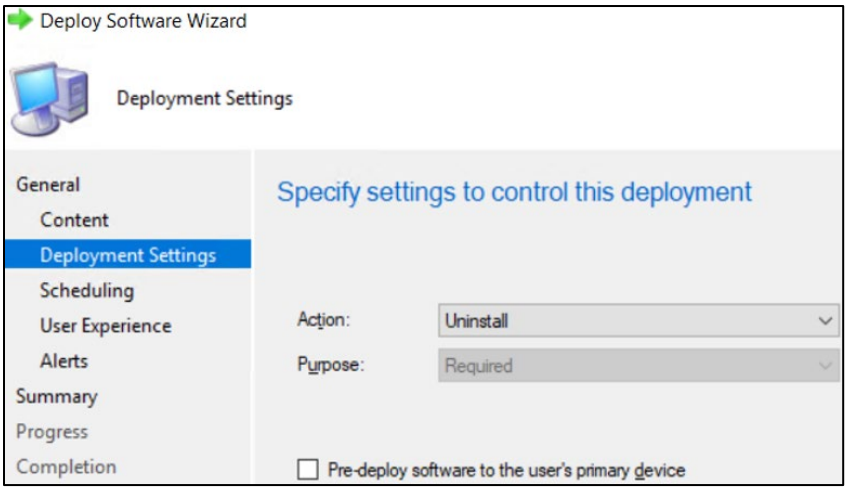
3. Under the **Deployments** tab, right-click on **SafeNet Authentication Service Agent for Win 8-10-2012-2016** deployment and click **Delete**.

NOTE: This deletion will only delete the **SafeNet Authentication Service Agent for Win 8-10-2012-2016 deployment** from the device collection. It will not delete the **SafeNet Authentication Service Agent for Win 8-10-2012-2016 application** from the **Software Library**.

4. On the **Configuration Manager** pop-up, click **Yes**.

Deploying the application into client machines for uninstallation

1. Perform Step 1 to Step 5 of **Deploying the application into client machines** section to deploy the application into client machines for uninstalling the agent.
2. Now, on the **General** > **Deployment Settings** window, select **Uninstall** from the **Action** drop-down, and then click **Next**.



3. To complete the deployment, perform Step 7 to Step 11 of **Deploying the application into client machines** section.

Pushing computer policy to the client machines

Perform the steps mentioned in Pushing computer policy to the client machines section to push computer policy to the client machines for **SafeNet Authentication Service Agent for Win 8-10-2012-2016** application, which you have created for agent installation.

After following the steps, a new computer policy for uninstalling the agent will be pushed to the client machines.

> **NOTE:** This step will uninstall the agent from the client machines. However, in Software Center, sometimes, the uninstall deployment application shows the **Removal failed** error. It can be removed if you delete the uninstall deployment from the **Configuration Manager console** (refer to the steps mentioned in Deleting the deployment from Device Collection section).

Upgrading the agent

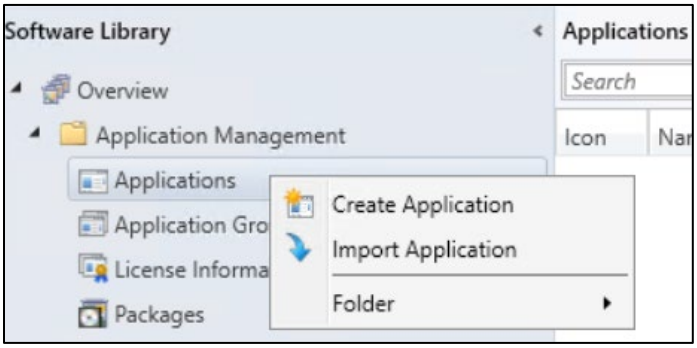
Upgrading the agent involves the following steps:

1. Creating an application with new agent version in Microsoft Endpoint Configuration Manager
2. Creating Supersedence relationship
3. Updating Detection method for the upgrade
4. Distributing the content (Application)
5. Deploying the application into client machines
6. Pushing computer policy to the client machines

Creating an application with new agent version in Microsoft Endpoint Configuration Manager

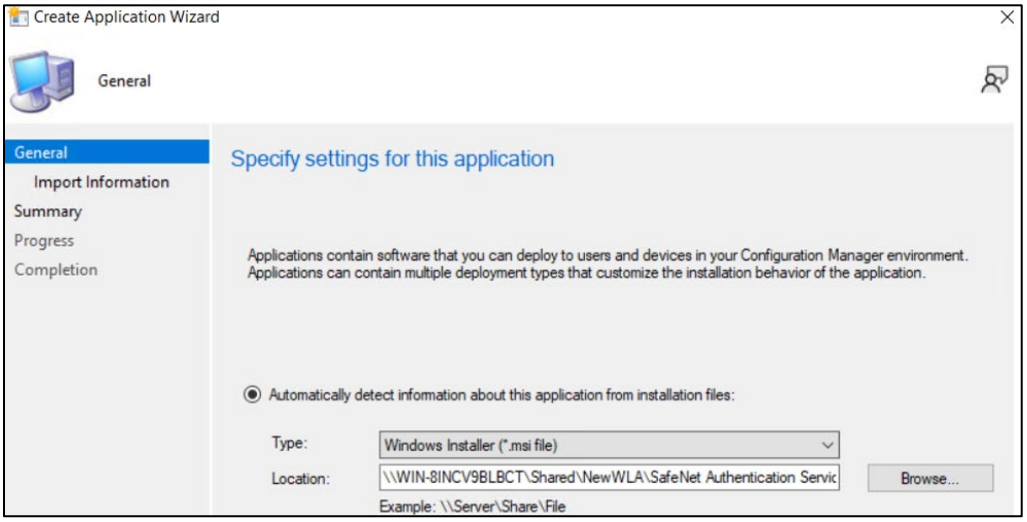
Perform the following steps to create an application for the latest version of the agent. Afterwards, we will link this newly created application with the application that has older version of the agent (for the upgrade).

1. Open the Configuration Manager console. On the left pane, click **Software Library** > **Application Management** > **Applications** > **Create Application**.



2. On the **Create Application Wizard**, under **General**, in the **Location** field, enter the file path in UNC format where new version of the agent MSI is present, and then click **Next**.
For example, **\\WIN-8INCV9BLBCT\Shared\NewWLA\SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64.msi**

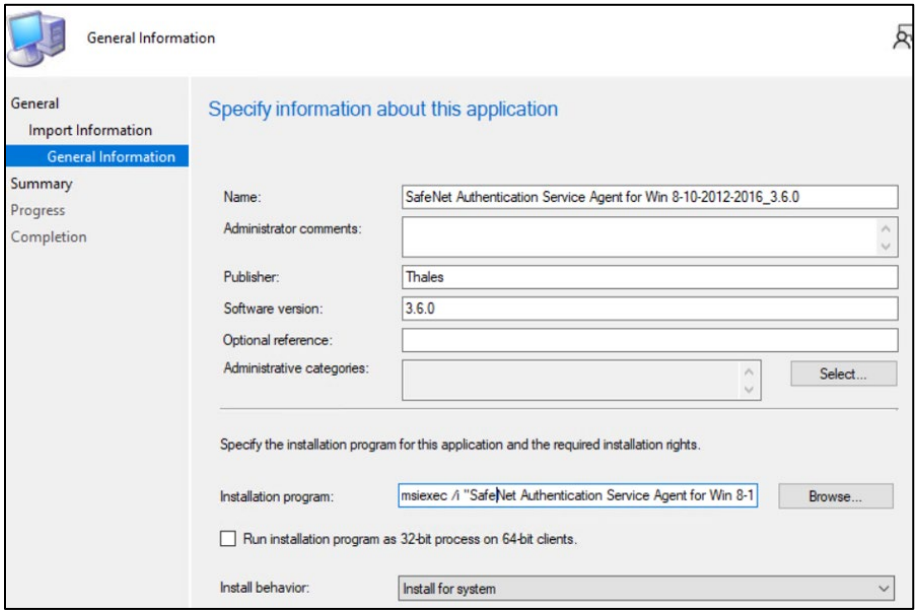
NOTE: Use the default MSI name provided in the downloaded agent package.



3. Under **General** > **Import Information**, click **Next**.
   a. Under **General Information**, perform the following steps:
   i. In the **Name** field, enter the application name of your choice or proceed with the default name, that is, SafeNet Authentication Service Agent for Win 8-10-2012-2016_3.6.0.
   ii. In the **Publisher** field, enter the company name. For example, Thales.
   iii. In the **Software version** field, enter the version of the agent. For example, 3.6.0.
   iv. In the Installation program field, enter the following command:
   `msiexec /i "SafeNet Authentication Service Agent for Win 8-10-2012-2016 x64.msi" /quiet REINSTALLMODE=vomus REINSTALL=ALL`

   NOTE: With the above command, after the agent installation, hard restart will be triggered on the client device. To avoid this, append **/norestart** parameter in the above command and ensure that you restart the client device later (for the agent to work properly).

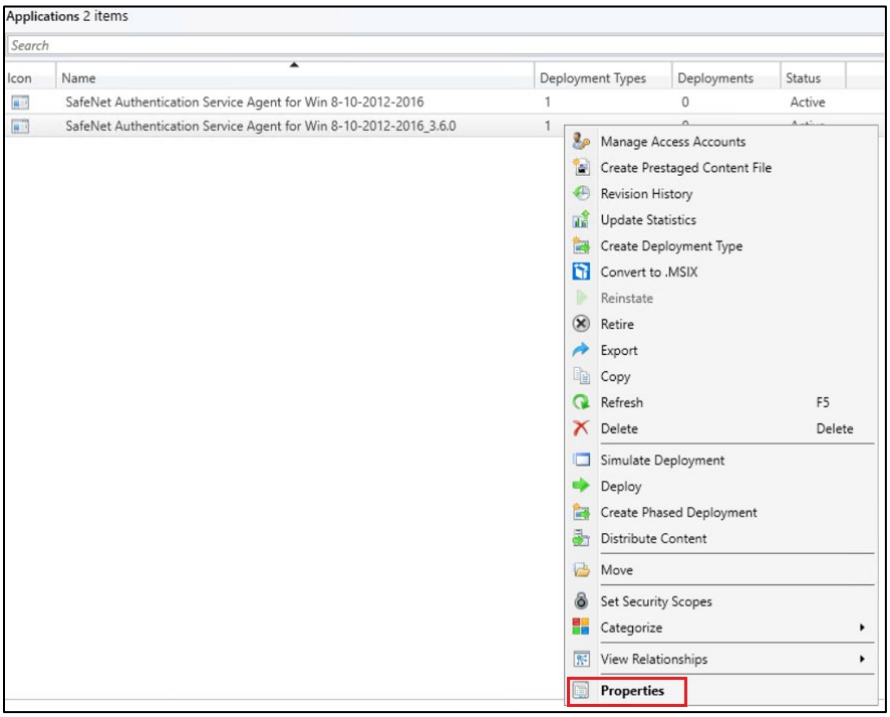
   v. In the **Install behavior** drop-down, ensure that **Install for system** is selected.
   vi. Click **Next**.



4. On the **Summary** window, click **Next**.
5. On the **Completion** window, click **Close**.

Creating Supersedence relationship

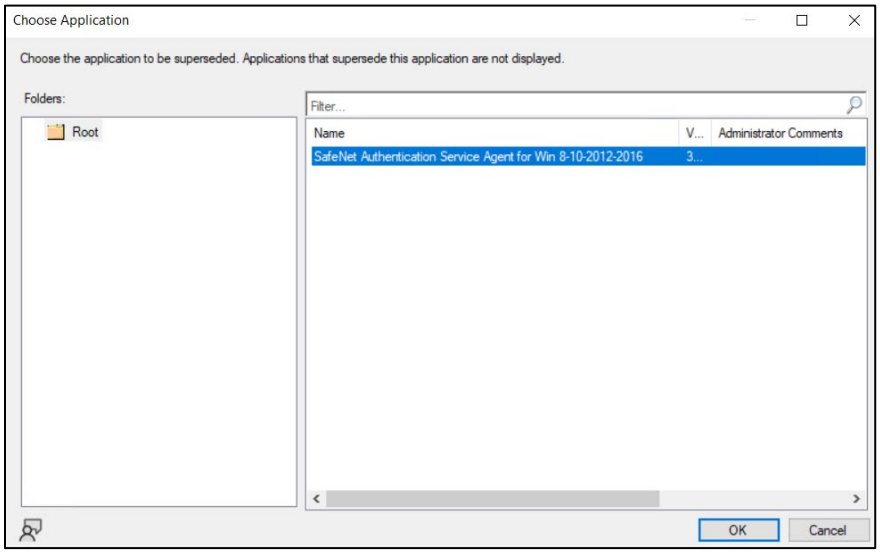
1. Under **Software Library** > **Application Management** > **Applications**, right-click on the new application that you have created in above step, and then click **Properties**.



2. Under **Supersedence** tab, click **Add**.

a. On the **Specify Supersedence Relationship** window, click **Browse** against the **Superseded Application** field.

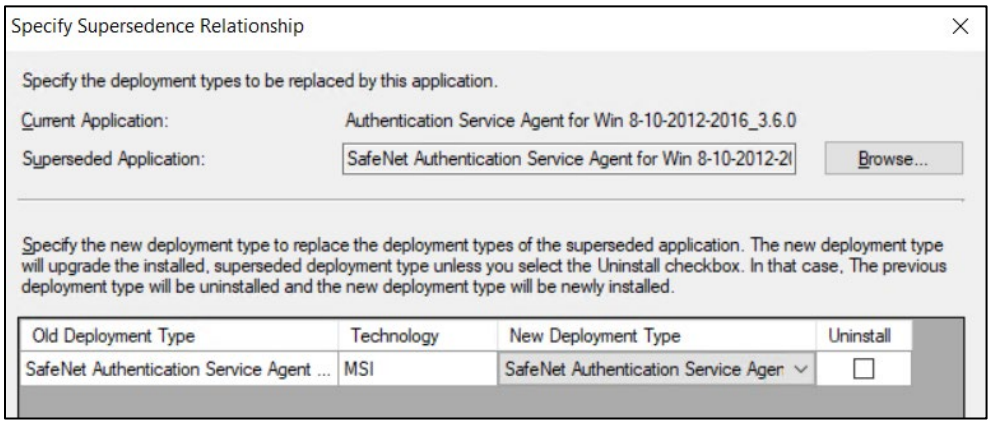
i. On the **Choose Application** window, select the application that has older version of the agent, which needs to be replaced with the new application. Click **OK**.



b. Under the **New Deployment Type** column, select the deployment type of the new application from the drop-down.

c. Under the **Uninstall** column, ensure that the checkbox is not selected.

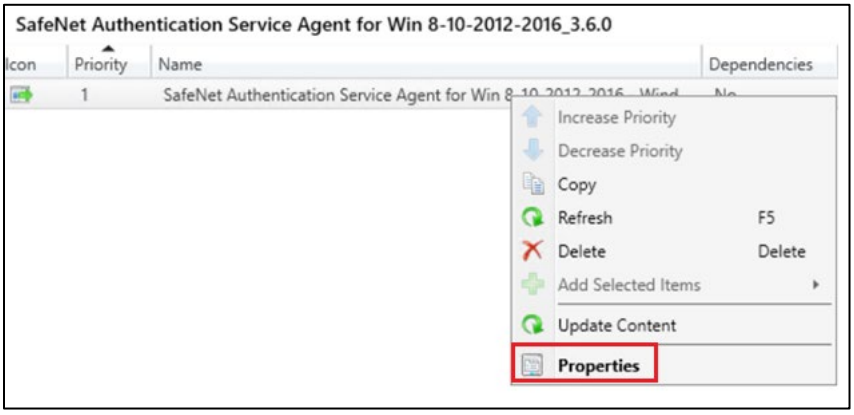
d. Click **OK**.



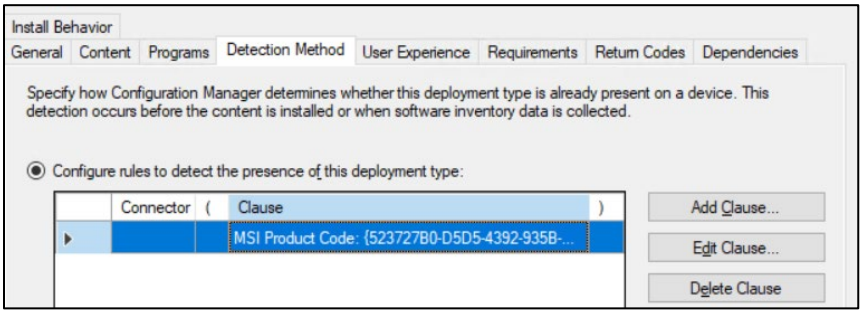
3. Click **Apply** and then click **OK**.

Update Detection method for the upgrade

1. Under **Applications**, click on the new application that you have created in Creating an application with new agent version in Microsoft Endpoint Configuration Manager section.
2. In the bottom pane, click the application tile. Under the **Deployment Types** tab, right-click on the deployment type and then click **Properties**.



3. On the **SafeNet Authentication Service Agent for Win 8-10-2012-2016 - Windows Installer (*.msi file) Properties** window, click the **Detection Method** tab. Select the clause and then click **Edit Clause**.

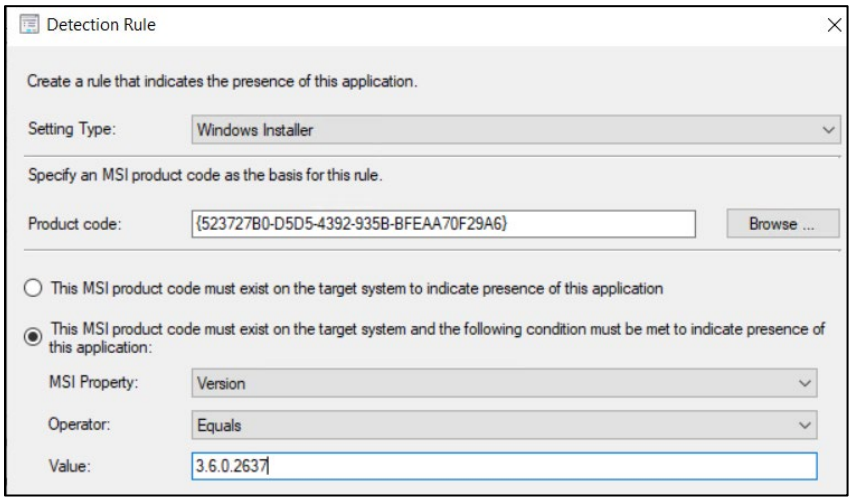


a. On the **Detection Rule** window, perform the following steps:

i. Click **This MSI product code must exist on the target system and the following condition must be met to indicate presence of this application** radio button.

ii. In the **Value** field, enter the **latest product version** of the agent MSI. For example, 3.6.0.2637.

iii. Click **OK**.



b. Click **Apply** and then click **OK**.

Distributing the content (Application)

Perform the steps mentioned in **Distributing the content (Application)** section to distribute the application that you have created in **Creating an application with new agent version in Microsoft Endpoint Configuration Manager**.

Deploying the application into client machines

Perform the steps mentioned in **Deploying an application into client machines** section to deploy the application that you have created in **Creating an application with new agent version in Microsoft Endpoint Configuration Manager**.

Pushing computer policy to the client machines

Perform the steps mentioned in **Pushing computer policy to the client machines** section to push the computer policy to the client machines for the application that you have created in **Creating an application with new agent version in Microsoft Endpoint Configuration Manager**.

After following the above steps, old version of the agent will be replaced with the new version on the client machines.

> **NOTE**: Restart might be required after the upgrade.

CHAPTER 6: Troubleshooting and Advanced Configurations

This chapter provides troubleshooting strategies and solutions for common errors quickly and effectively. For further assistance, contact Thales Customer Support.

1. Remote Users who Lost or Forgot Token
2. Refining Administrator Group Exclusions
3. Configuring Num Lock Settings

Remote Users who Lost or Forgot Token

Following are the steps 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 operator:
   a. Logs in to the SafeNet server, finds the user on the **Secured Users** tab and makes a note of the emergency password.
   b. Provides emergency password to the user.
3. The user logs in to the workstation using the emergency password.
4. The operator assigns a new token to the user or enables a SafeNet server static password.
5. The user establishes a VPN connection to the network, launches the SafeNet Windows Logon Agent Manager, and performs a manual replenish with the new token or SafeNet static password.

The user can now log in with their SafeNet credentials while being offline.

Refining Administrator Group Exclusions

During installation of the agent, 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. Perform the following steps to achieve the same:

1. During the installation of the agent, clear the option **Exempt Local and Domain Administrator groups from SafeNet Authentication Service Authentication**.
2. Log in to the WLA 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:

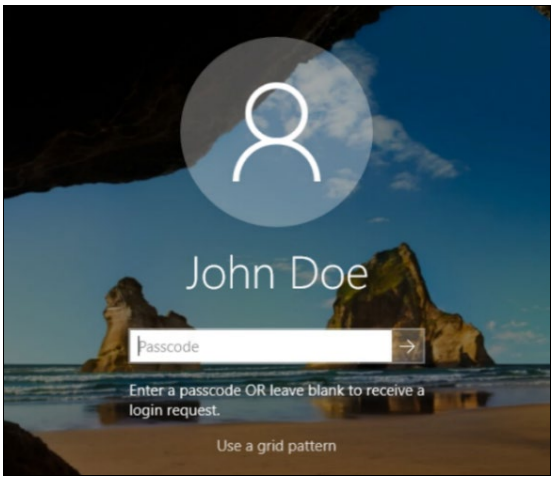
1. Click **Start > Run**.
2. In the **Open** box, type **regedit**, and then click **OK**.
3. In the registry, open one of the following:
   - For a single user: **`HKEY_CURRENT_USER > Control Panel > Keyboard`**
   - For all users: **`KEY_USERS| .Default > Control Panel > Keyboard`**
4. Edit the string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

CHAPTER 7: Running the Solution

This section describes the login and authentication flow with the agent. Windows attaches the credential provider to the same user account and does not create a separate tile.

Following are the login screen for different user types:

1. When SafeNet OTP is not exempted.



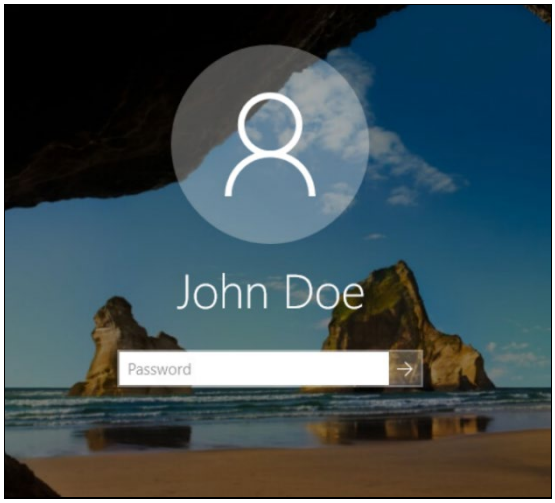
   a. Enter the **SafeNet OTP** and press **Enter** (or click the forward arrow sign).

   - For **Challenge-Response** token, press **Enter** (or click the forward arrow sign) keeping the **Passcode** field blank.

     Depending on the user selected token type, any of the following character passcodes can also be provided:

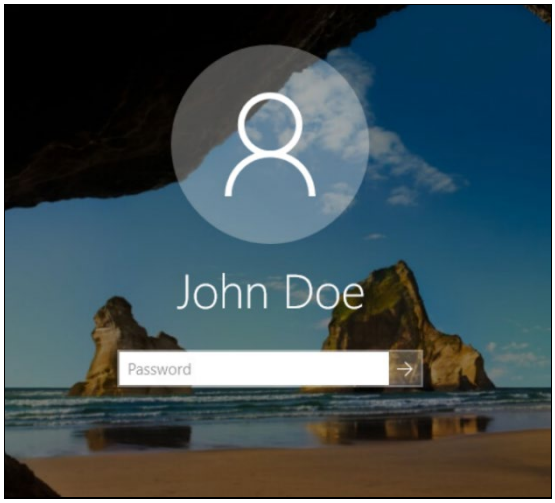
     – **g** for GrIDsure
     – **e** for E-mail
     – **s** for SMS
     – **p** for Push OTP

   b. Enter the **Microsoft password**.



After providing the Microsoft password, you will be successfully logged in to the Windows machine.

2. When SafeNet OTP is exempted.
   a. Enter the **Microsoft password**.



After providing the Microsoft password, you will be successfully logged in to the Windows machine.