SafeNet Agent for Epic 3.0.5

INSTALLATION AND CONFIGURATION GUIDE

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

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as “Thales”) information.

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

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

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

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

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

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

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

CONTENTS

PREFACE: About the SafeNet Agent for Epic Guide

Customer Release Notes

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

Audience

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

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

Document Conventions

This section describes the conventions used in this document.

Command Syntax and Typeface Conventions

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

Format	Convention
bold	The bold attribute is used to indicate the following: > Command-line commands and options that you enter verbatim (Type **dir /p**.) > Button names (Click **Save As**.) > Check box and radio button names (Select the **Print Duplex** check box.) > Dialog box titles (On the **Protect Document** dialog box, click **Yes**.) > Field names (**User Name**: Enter the name of the user.) > Menu names (On the **File** menu, click **Save**.) (Click **Menu** > **Go To** > **Folders**.) > User input (In the **Date** box, type **April 1**.)
italics	In type, the italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[**optional**] [<optional>]	Represent optional **keywords** or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.
{**a**|**b**|**c**} {<a>|<b>|<c>}	Represent required alternate **keywords** or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.
[**a**|**b**|**c**] [<a>|<b>|<c>]	Represent optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.

Notifications and Alerts

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

Tips

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

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

Notes

Notes are used to highlight important or helpful information.

> **NOTE** Take note. Contains important or helpful information.

Cautions

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

> **CAUTION!** Exercise caution. Contains important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury.

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

Support Contacts

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

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

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

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

Telephone

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

CHAPTER 1: Introduction

Overview

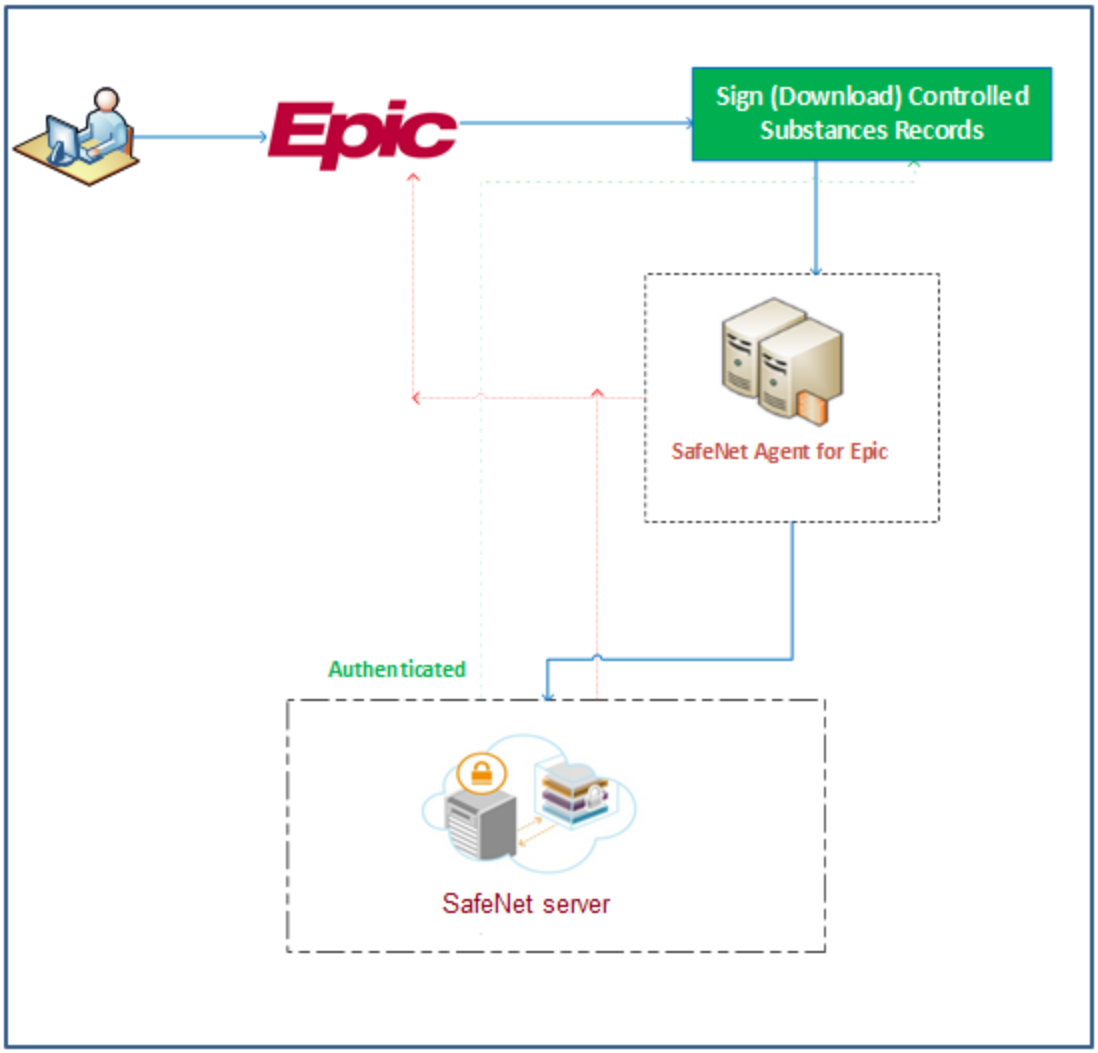
Epic Systems is one of the largest providers of health information technology, used primarily by large U.S. hospitals and health systems to access, organize, store and share electronic medical records. It enables medical organizations (and individuals) to perform actions such as medication scheduling, ordering, dispensing and e-prescription downloading. Hyperspace is legacy client application and they are now moving to a Chromium web-based framework, Hyperdrive.

The SafeNet Agent for Epic is a client-side agent that supports Direct authentication against a user ID. The agent is a best-in-class authentication solution, providing maximum security and performance, certified to the highest security standards.

User Flow

The following steps broadly depict the flow of actions for the agent solution:

1. A user logs in to the Epic using username and password.
2. If the user proceeds to sign the controlled substances patient records, the SafeNet solution is called (through the agent) for elevated access check.
3. The configured authentication for the second factor is displayed.
4. Once authenticated, the user is allowed to sign and download the records.



Agent Authentication Methods

Authentication methods allows to combat online fraud activities (such as phishing) and help maintain password integrity by making it more difficult for customers to lose or share passwords.

The SafeNet Agent for Epic supports the **Direct** method, meaning an ID is needed to authenticate users. The device determines whether the object being authenticated corresponds to the provided ID, or not.

Prerequisites

Ensure that the following prerequisites are met:

> Ensure that the Epic Hyperspace/Hyperdrive application is already installed on the system where the agent is proposed for the installation.

> Ensure that the user has administrative rights for installing and configuring the SafeNet Agent for Epic.

> To successfully configure and implement the SafeNet Agent for Epic solution, the administrator must be familiar with SafeNet Authentication Service (SAS) Cloud or SAS Service Providers Edition (SAS SPE) / SAS Private Cloud Edition (SAS PCE).

  Create an account in SAS Cloud or SAS PCE 3.9.1 (and above). For more information, refer to "Support Contacts" on page 7.

Security Recommendations

If you are using the Transport Layer Security (TLS) channel to secure requests between Token Validator Proxy (TVP) [recommended: TVP v2.0] and the SafeNet Agent for Epic, follow the steps to enable the TLS:

1. To enable TLS on TVP server in the Internet Information Services (IIS) Manager, you need to create a Hypertext Transfer Protocol Secure (HTTPS) binding for the Default website, by following the steps:
   a. Click **Start** > **Control Panel** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
   b. In the left pane of the IIS window, right-click the **Default Web Site** and click **Edit Bindings**.
   c. Create an HTTPS binding by using either a self-signed or a Certificate Authority (CA) certificate.

   > **NOTE** The certificate name should match the Uniform Resource Locator (URL) address of the token validator site.

2. Navigate to the following Registry Editor path: `HKLM\Software\CryptoCard\Token Validator`

   Change URL of the token validator to include HTTPS.
3. On the Client side, import the root CA certificate in the trusted root CA store.
4. On the **Epic Management Console**, select Communication > **Use SSL** checkbox [next to **Primary Server URL** (or Failover Server URL) field] to ensure that the HTTPS is used as the protocol to establish the connection.

System Requirements

Interoperability

Supported Operating Systems

> Windows 10 (32-bit and 64-bit)
> Windows 11
> Windows Server 2016 (64-bit)
> Windows Server 2019 (64-bit)

Software Component

> Microsoft .NET Framework 4.5.2

Configuration Component

> SafeNet Epic Management Console utility

Supported Tokens

> All authentication tokens currently supported by SafeNet Authentication Service except Push OTP.

CHAPTER 2: Installing the SafeNet Agent for Epic

Installing the Agent

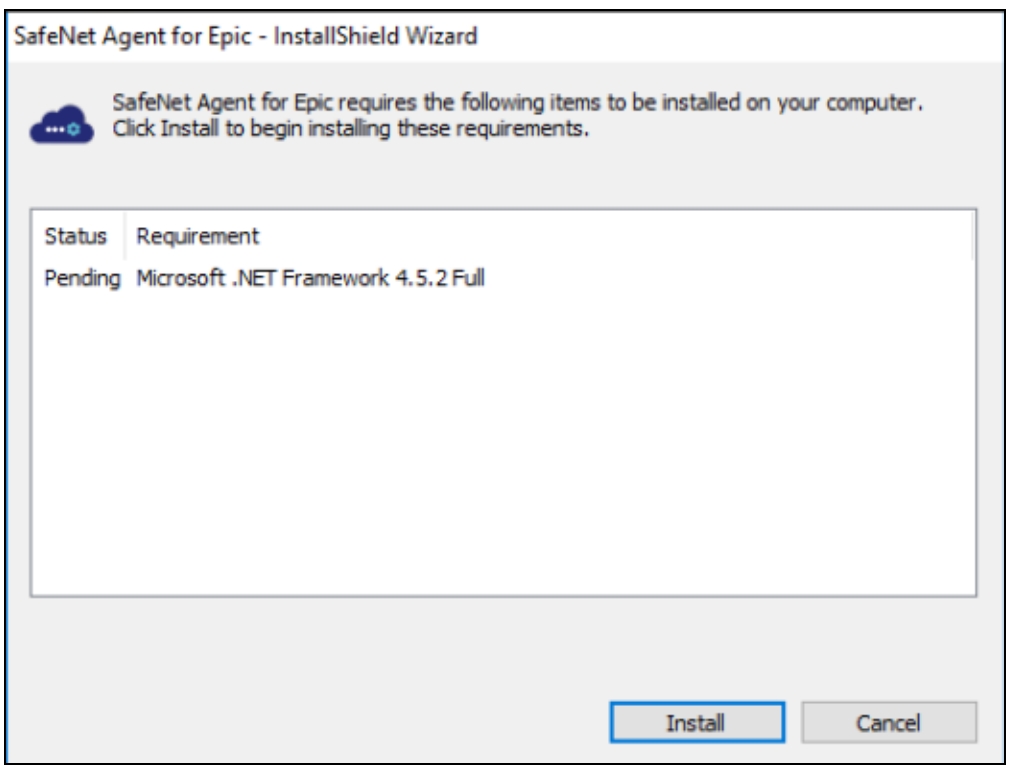
> **NOTE** Always work in **Run as administrator** mode when installing, uninstalling or upgrading the agent.

To install the SafeNet Agent for Epic, perform the following steps:

1. Double-click and execute the installer (***EXE***). Use ***MSI*** for Group Policy Object (GPO) installation.

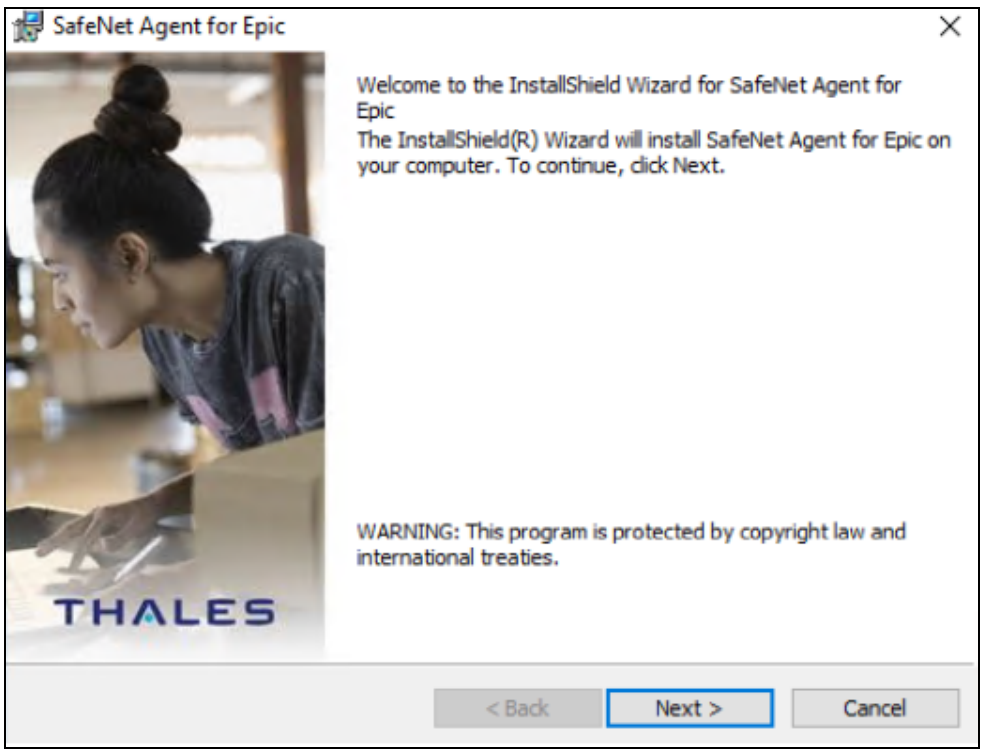
> **NOTE** If a user has logged in to the system as an administrator or if the user(s) is a member of the Domain Admin group, the installation process will execute successfully. Otherwise, a window will prompt to provide the administrator credentials.

> The installer will verify if the Microsoft .NET Framework 4.5.2 is installed on the system, or not. If it is not, the following InstallShield Wizard screen will appear, which will guide the user to install the required framework.



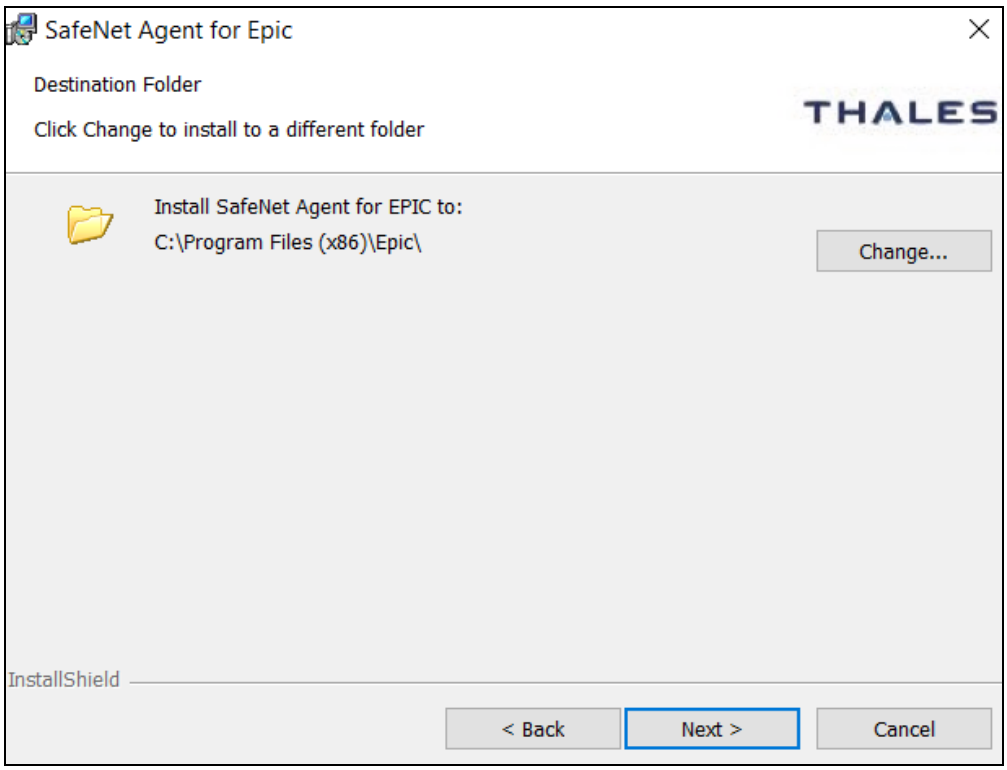
> **NOTE** If the required .NET Framework (4.5.2) is not available during the GPO installation, the installation process will execute successfully, without any interruptions. In such a case, only when the **Epic Management Console** is opened, an error stating the unavailability of .NET Framework is encountered. To proceed, install Microsoft .NET Framework 4.5.2.

2. On the **Welcome to the InstallShield Wizard...** window, click **Next**.

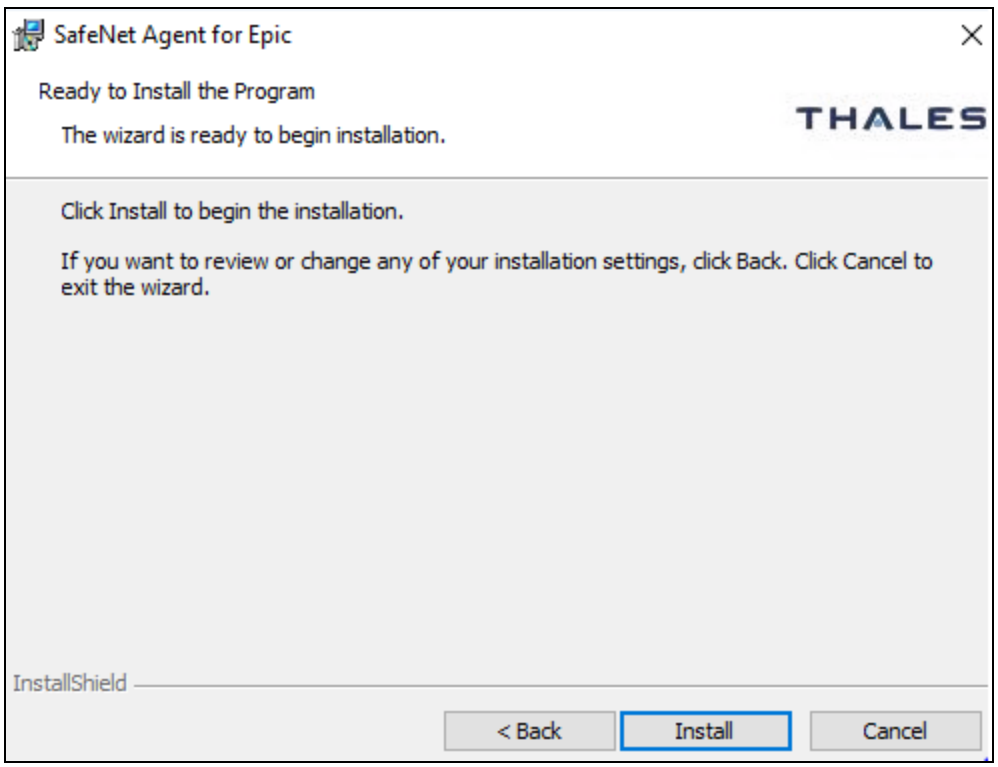


3. On the **License Agreement** window, read the software license agreement and to proceed, select **I accept the terms in the license agreement** option, and click **Next**.

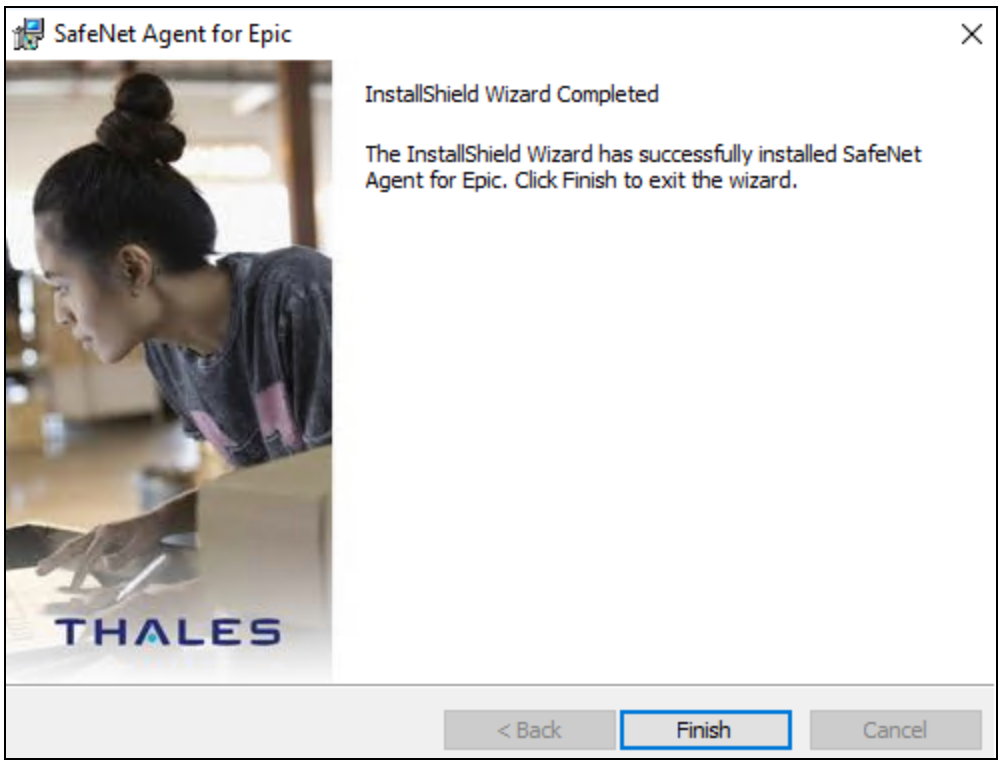
4. On the **Destination Folder** window,
   a. To accept the default installation destination folder, click **Next**.
   b. To change the installation folder, other than the default one, click **Change**, and then browse to provide a different path for agent installation.
   c. Click **Next**.



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



6. When the installation process completes, the **InstallShield Wizard Completed** window is displayed. Click **Finish** to exit the installation wizard.



Installing the Agent Silently

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

1. Open the command prompt in Administrator mode.
2. Navigate to the folder which contains the installer.
3. Execute the following command:

> Using EXE:

```
"SafeNet Agent for Epic.exe" /s /v"/q INSTALLDIR=\"<Path>""
```

For example,

```
"SafeNet Agent for Epic.exe" /s /v"/q INSTALLDIR=\"C:\Program Files (x86)\Epic\""
```

> Using MSI:

```
msiexec /i "SafeNet Agent for Epic.msi" /quiet
```

> **NOTE** Once the agent is successfully installed, an icon of the **SafeNet EPIC Management Console** utility is created on the desktop, to allow editing of the configuration details.

Uninstalling the Agent

> **NOTE**
> **>[IMPORTANT]** Before uninstalling the agent, ensure that the **Epic Hyperspace/Hyperdrive application** is present on that machine.
> **>** Always work in **Run as administrator** mode when installing, uninstalling or upgrading the agent.

To uninstall the SafeNet Agent for Epic:

1. Navigate to **Start** > **Control Panel** > **Programs and Features**, and select the SafeNet Agent for Epic program.
2. Click **Uninstall**.

Uninstalling the Agent Silently

To uninstall the SafeNet Agent for Epic in silent mode, perform the following steps:

1. Open the command prompt in Administrator mode.
2. Navigate to the folder which contains the installer.
3. Execute the following command:

> Using EXE:

```
"SafeNet Agent for Epic.exe" /x /s /v"/q"
```

> Using MSI:

```
msiexec /x "SafeNet Agent for Epic.msi" /quiet
```

CHAPTER 3: Configuring the SafeNet Agent for Epic

Configuring the Agent

You can configure SafeNet Agent for Epic using the **Epic Management Console** utility.

Double-click the utility icon to edit / enter the configuration details. The Epic Management Console window has four (4) tabs:

> "Communication" below
> "Configuration" on page 20
> "Logging" on page 22
> "Certificate" on page 24

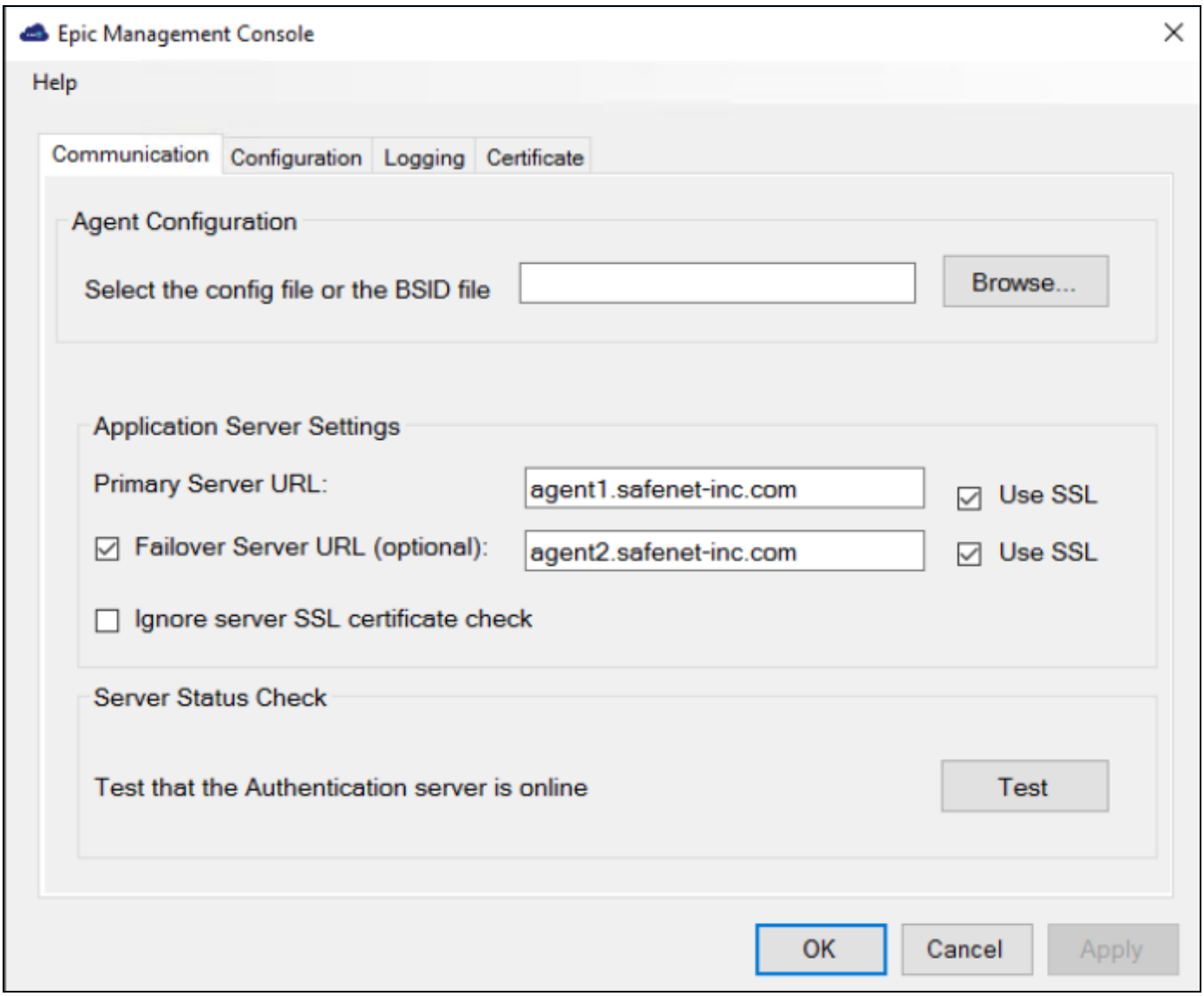
You can click the **Help** link (at the top-left) to know about the version and copyright details of the product.

> **NOTE** After making any change in the management console, ensure to click **Apply** and then **OK** for the changes to take effect.

In addition, policy settings of SafeNet Agent for Epic can be configured using the Group Policy Object (GPO) Editor. For details, refer the section.

Communication

On opening the **Epic Management Console**, the **Communication** tab is displayed by default. On first accessing the console, the following message is displayed: *Agent configuration file not detected. Browse and select the file.*



This tab has the following three sections:

Agent Configuration

> **Select the config file or the BSID file**: Click **Browse...** to select the BSID file and update the required configurations.

Application Server Settings

> **Primary Server URL**: The IP (or URL) address of the primary SafeNet server. Alternatively, **Use SSL** check box option can also be selected to ensure that HTTPS is used as the protocol to establish the connection. If it is not selected, the connection is established using the less secure HTTP.

> **NOTE** The Registry Settings are updated at the following paths:
> `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Thales\Epic` (64-bits Windows)
> `HKEY_LOCAL_MACHINE\SOFTWARE\Thales\Epic` (32-bits Windows)

- **Failover Server URL (optional)**: If the primary SafeNet server is not functioning, the **Failover Server URL** check box can be selected to specify the IP (or URL) address of the secondary / failover server. Alternatively, **Use SSL** check box option can also be selected to ensure that HTTPS is used as the protocol to establish the connection. If it is not selected, the connection is established using the less secure HTTP.
- **Ignore server SSL certificate check**: Select the check box to disable the SSL server certificate error check on the agent. It is unchecked by default. If customers are using the on-premise deployment of SafeNet server within a well-controlled network (where self-signed certificates are used and cannot be properly validated by the SafeNet Agent for Epic), this check box needs to be selected.

> **NOTE** We strongly recommend the use of SSL certificate.

Server Status Check

- **Test that the Authentication Server is online**: Click **Test** to confirm if the Authentication Server is available, or not.

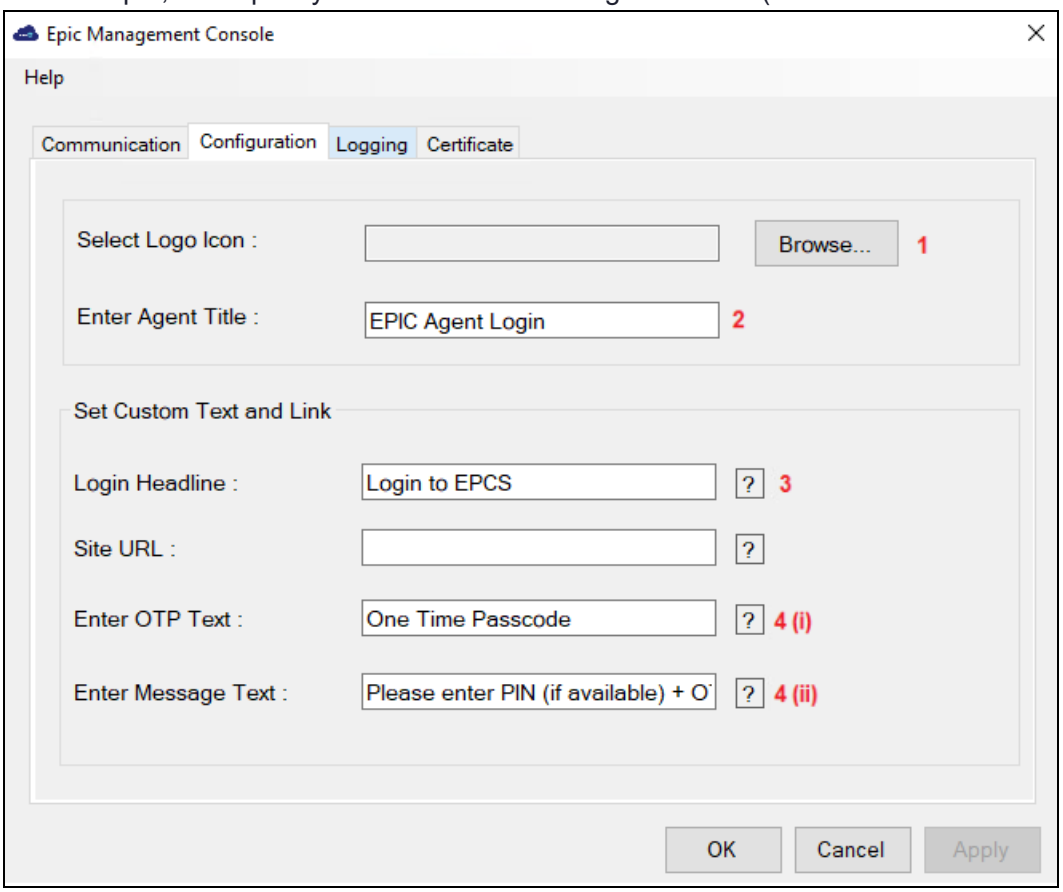
Downloading BSID File

1. Login to your SafeNet server account, and navigate to **COMMS** > **Authentication Processing**.
2. Under **Task** list, click **Authentication Agent Settings** link and download the ***Agent.bsidkey*** file.

Configuration

The **Configuration** tab allows to alter the look and feel of the agent window, so it looks as part of the Epic workflow, and not a third-party add-on. Being able to enforce a consistent user login experience helps protect against account credential attacks.

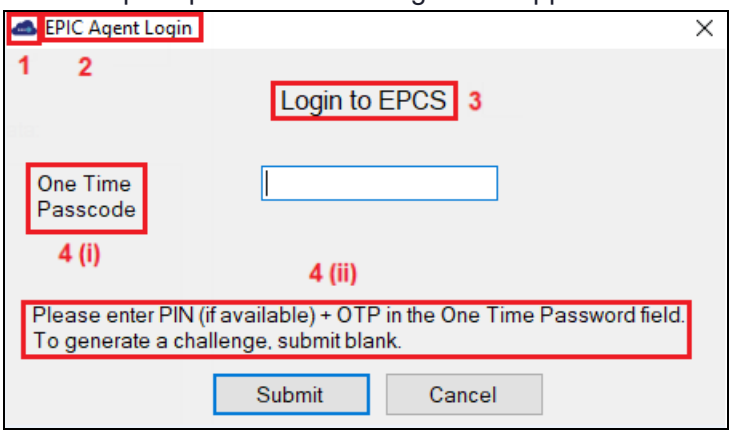
For example, if we specify the details in the Configuration tab (as shown in the following screen):



1. **Select Logo Icon**: The image selected will be the title image in the OTP prompt window of the agent. This field only accepts ICO image format.
2. **Enter Agent Title**: The text entered in this field will be the title in the OTP prompt window of the agent.
3. **Login Headline**: The text entered in this field will be clickable in the OTP prompt window of the agent, hyperlink to which can be specified in the **Site URL** field.
4. **Enter OTP Text** and **Enter Message Text**: These text fields allow to customize the messages on the OTP prompt window of the agent. Based on deployed tokens, customers can control the messages, to make it clear and consistent with their enterprise terminologies.

> **NOTE** Hover over the question mark icon (**?**) (displayed against fields) to view the sample text.

The OTP prompt window of the agent will appear like the following screen:

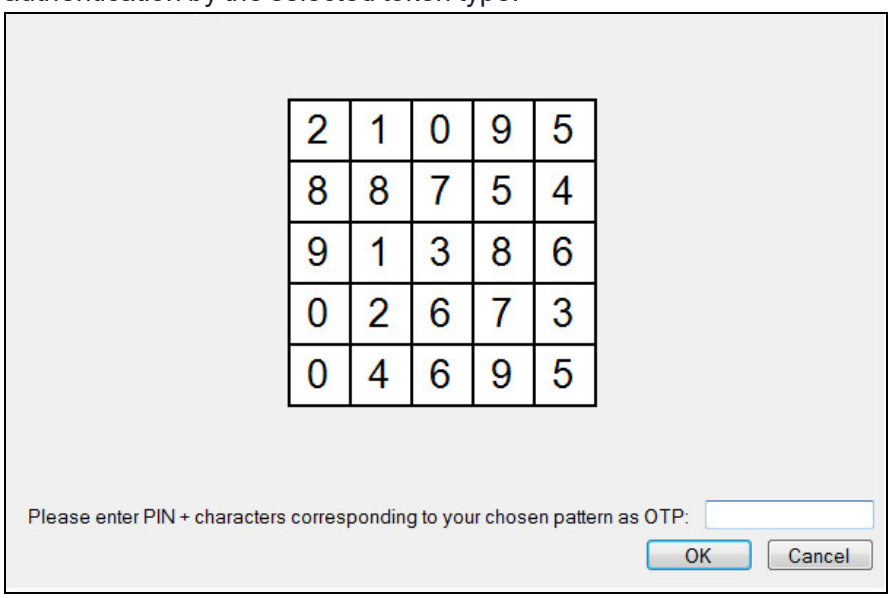


> If the selected token type is **Password**:

  a. Enter password in the **One Time Passcode** field, and click **Submit**.

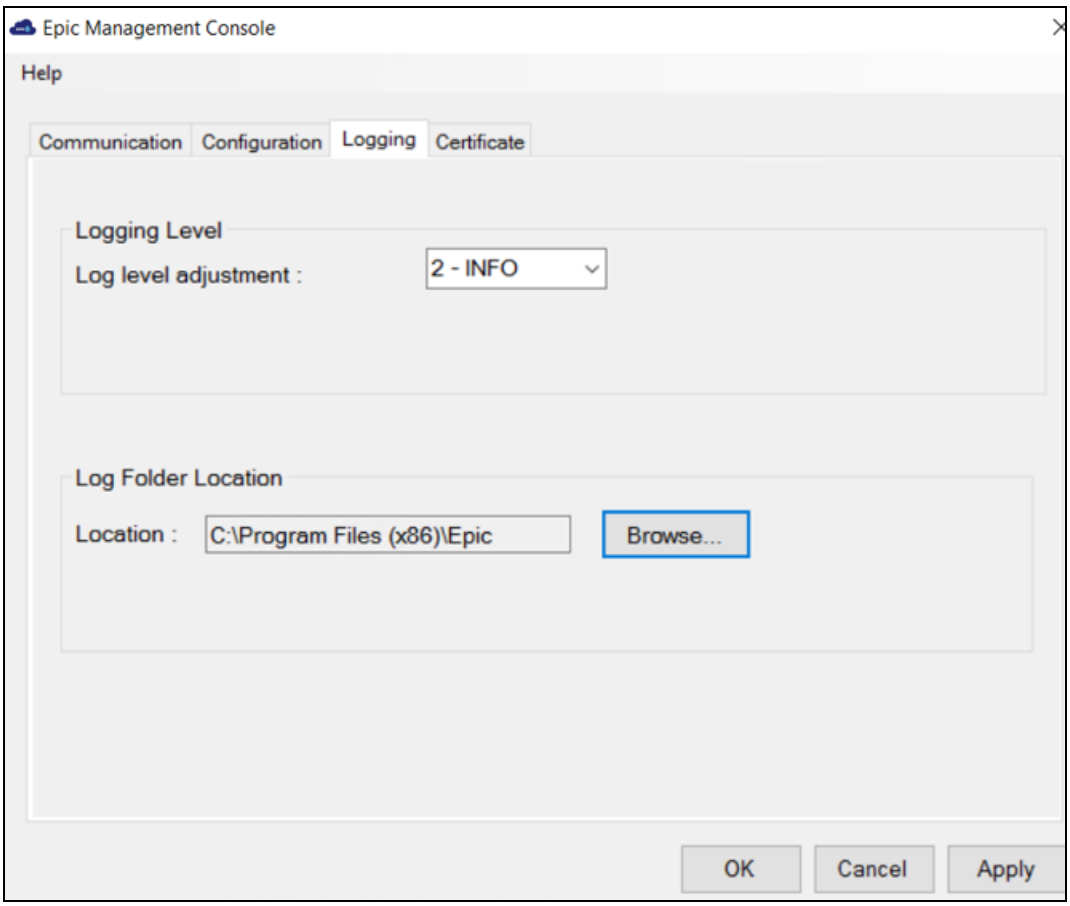
  b. Click **OK** in the Epic Management Console window.

> If the selected token type is **GrIDsure** or **Challenge-Response**, keep the **One Time Passcode** field blank, and click **Submit**. The following window will be displayed, that will help the user to complete the authentication by the selected token type:



Logging

Log files record events that occur during the software execution process.



The **Logging** tab has the following two fields:

1. **Log level adjustment**: The field allows to specify the level of log that will be created. According to debugging needs, the logs are recorded at different levels. Four consecutive levels are configured, namely **DEBUG**, **INFO**, **ERROR**, and **OFF**, wherein **DEBUG** is the highest log level, and **OFF** is the lowest. The higher the log level is, the more detailed the log is recorded. Each log level also contains information for all its following log levels. For example, the **DEBUG** level also contains information for **INFO** and **ERROR** log levels (and thus is more detailed). Similarly, the **INFO** level also contains information for the **ERROR** log level.
   a. **1 - DEBUG**: This option allows to view diagnostic information that is useful to debug the application.
   b. **2 - INFO**: This option allows to view informational messages that highlight the running, management and progress of the application. It includes information, the administrator wants available but usually need not to refer under normal circumstances. Some examples of INFO types:
      - Service Start / Stop Details
      - Configuration Details
      - Authentication Success / Failure Details
      - Assumptions
   c. **3 - ERROR**: This option allows to log all unhandled exceptions. It records errors which are fatal to the operation but not the service or application, and thus require Administrator intervention. Some examples of ERROR types:

- Unable to open (or access) required resources
- Missing data
- Incorrect connection strings
- Missing services

d. **4 - OFF**: This option allows to turn off logging.

> **NOTE** None of the four log levels record events that stop the running of the application. The events recorded are not critical, in the sense that they do not interfere with the functioning of the agent application.

2. **Location**: The field specifies the location where the logs will be created. By default, the logs will be created in the logs folder at the agent's working directory. The location (where the log files will be created) can be secured using standard System Policy settings of the Windows.

   Recommendation: One of the best ways to secure log files is to direct them to a separate server, whenever possible. By storing your log files on a separate server, your log files are always one more step away from hackers.

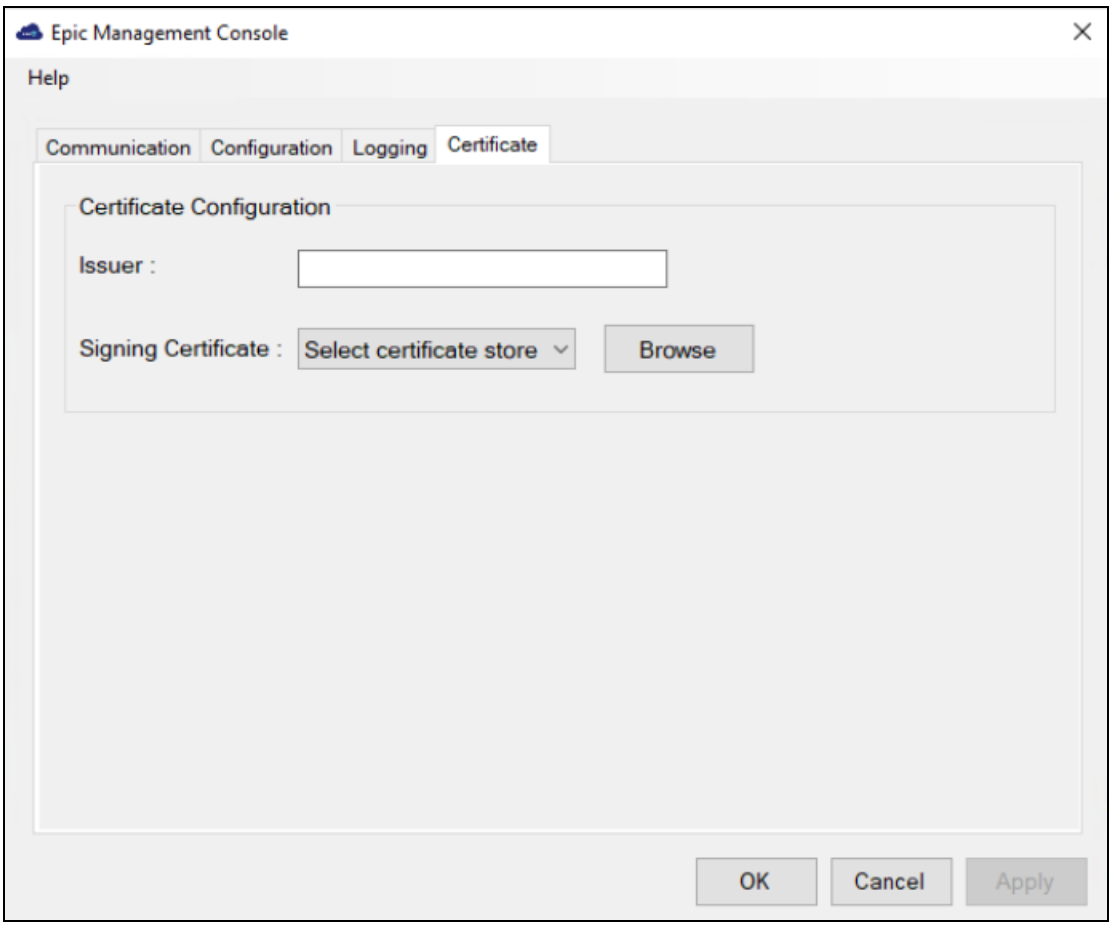
Certificate

The Certificate tab enables to upload the signing certificate issued from a valid authority.

> **NOTE** This is only applicable for Epic Hyperdrive.

Prerequisite

Ensure that the certificate is already deployed on the machine.

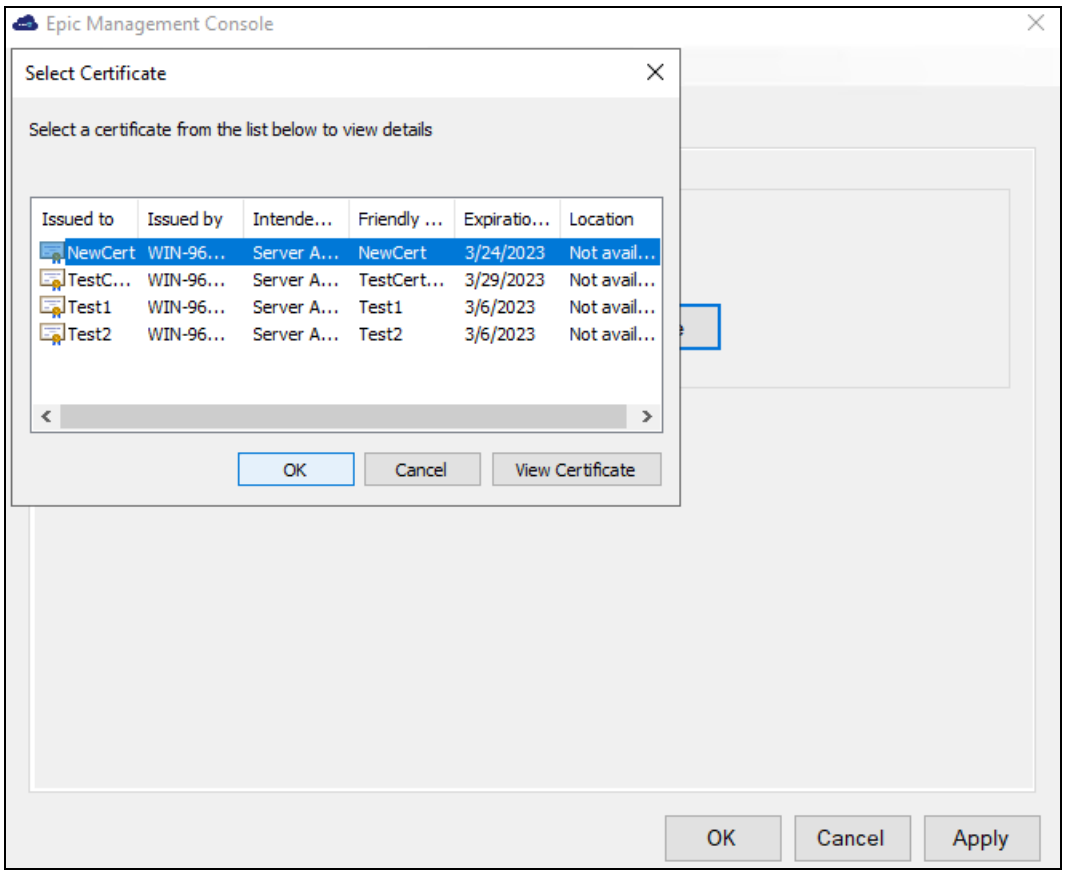


The **Certificate** tab has the following two fields:

1. **Issuer**: Enter the Entity ID of the SAML token. The Issuer in the SAML token must be added to an E0G record in the Epic database. It must be a unique identifier of the authentication device in the Epic environment.
2. **Signing Certificate**: This settings is used to select the certificate for signing in.
   a. Choose the certificate store location by selecting either of the following options from the dropdown:
   - **Current user**
   - **Local machine store**

   b. Click **Browse** to select the certificate, and then click **OK**. The **Select Certificate** window shows all the valid certificates that has a private key.

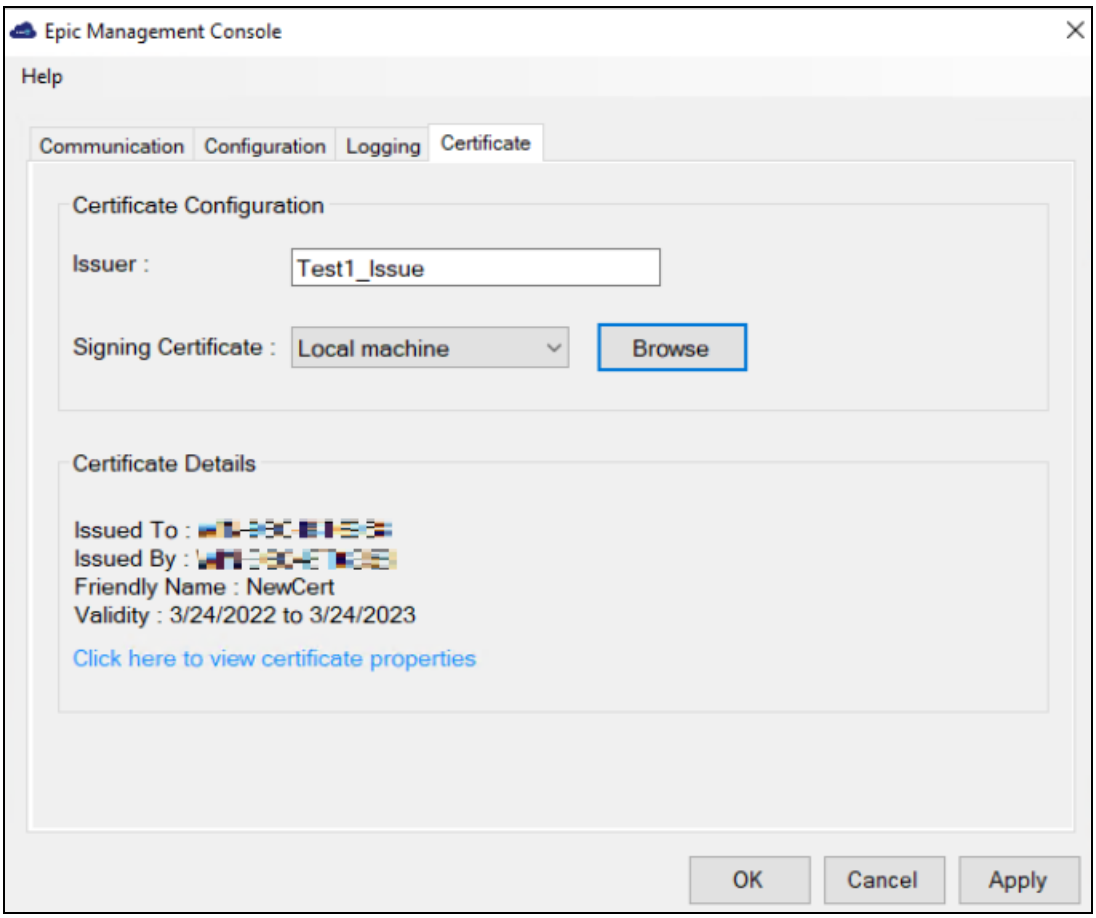
> **NOTE**
> **>** Multiple certificate selection is not allowed.
> **>** In case of a non-admin user, if the certificate is present in the **Personal** folder of the local machine, then the user must be provided with the *read access* for managing the certificate's private key.



The selected certificate is used to sign the SAML token response generated when using with Epic Hyperdrive.

After selecting the certificate, the certificate details gets listed on the **Epic Management Console**.

- **Issued To** - Specifies the entity name to whom the certificate was issued.
- **Issued By** - Specifies the entity name that issued the certificate.
- **Friendly Name** - [Optional] It will be visible if the user selected certificate contains a friendly name.
- **Validity** - Specifies the certificate validity.


Epic Management Console
Help
Communication
Configuration
Logging
Certificate
Certificate Configuration
Issuer :
Test1_Issue
Signing Certificate :
Local machine
Browse
Certificate Details
Issued To :
Issued By :
Friendly Name : NewCert
Validity : 3/24/2022 to 3/24/2023
Click here to view certificate properties
OK
Cancel
Apply

CHAPTER 4: Configuring Settings via Group Policy Object Editor

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.

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

To configure settings, perform the following steps:

1. Add ADMX file to Group Policy Object (GPO) Editor
2. Configure ADMX Settings using GPO Editor
3. Deploy the Certificate via GPO
   - GPO deployment of certificate to a trusted store
   - Sample script for deploying the certificate to a personal store

Prerequisites

> Microsoft .NET Framework 4.5.2

Adding ADMX File to Group Policy Object (GPO) Editor

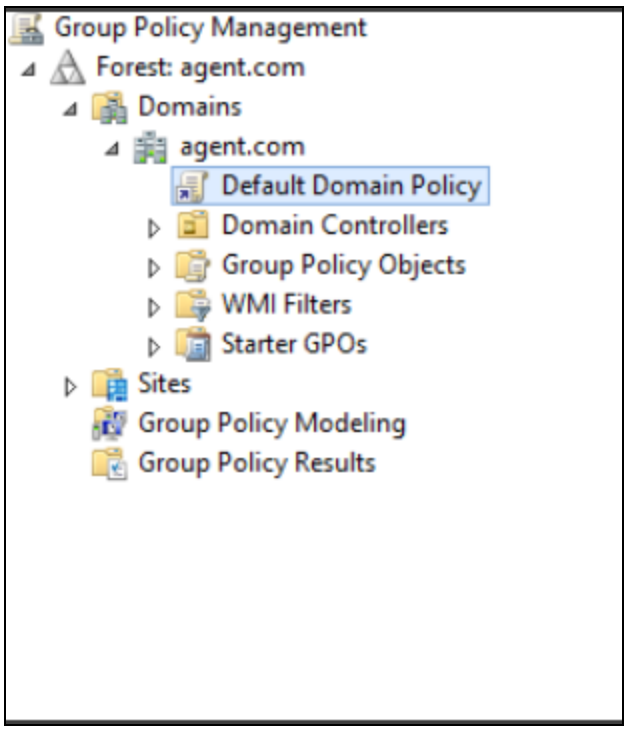
To add ADMX file of the SafeNet Agent for Epic to the GPO Editor, perform the following steps:

1. Copy the ADMX file (*SafeNetEpic.admx*) included in the downloaded agent software package to the following location:
   - For servers: `C:\Windows\PolicyDefinitions`
   - For client computers: `%Systemroot%\PolicyDefinitions`
2. Copy the appropriate ADML language file (*SafeNetEpic.adml*) to a language folder under the `\PolicyDefinitions` folders.
   For example: In Windows Server 2019, the English language file provided should be written to: `C:\Windows\PolicyDefinitions\en-US`
3. Restart GPO Editor.

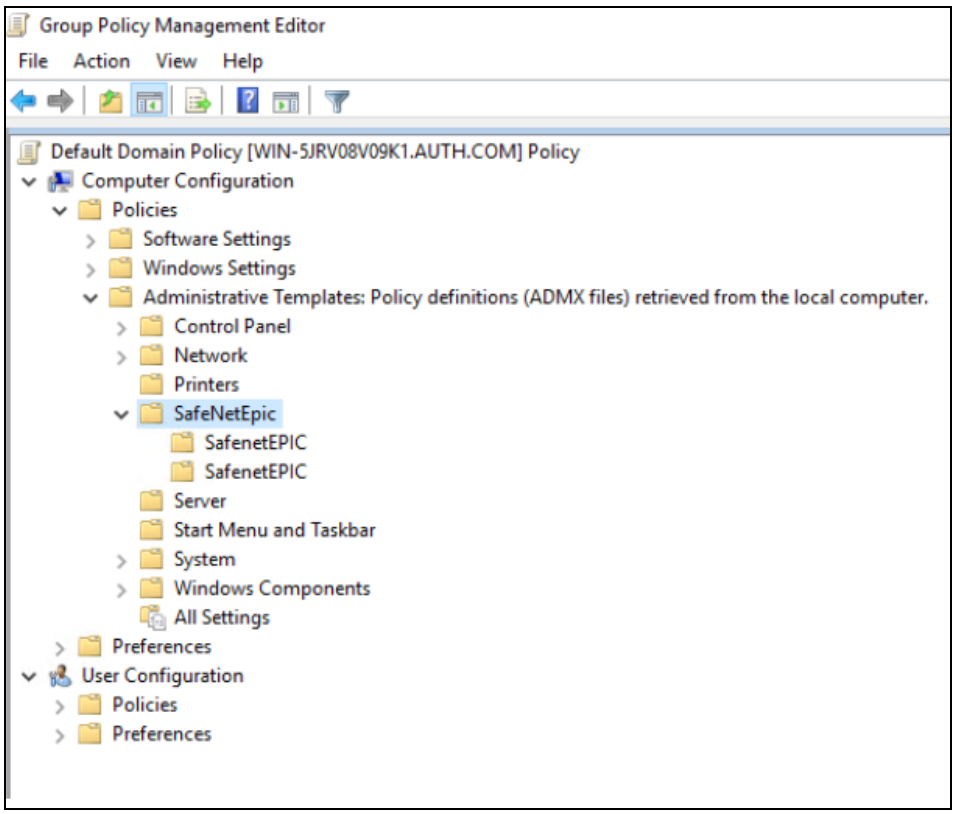
Configuring ADMX Settings using GPO Editor

Once the ADMX file is added, open the template to configure the settings. To open the template and edit the settings:

1. From the Windows taskbar, select **Start** > **All Programs** > **Accessories** > **Run**.
2. In the **Run** window, enter *gpmc.msc*, and click **OK**. The Group Policy Management window is displayed.
3. Complete one of the following actions:
   - To propagate the settings to all clients in the domain, right-click **Default Domain Policy** under the domain node.



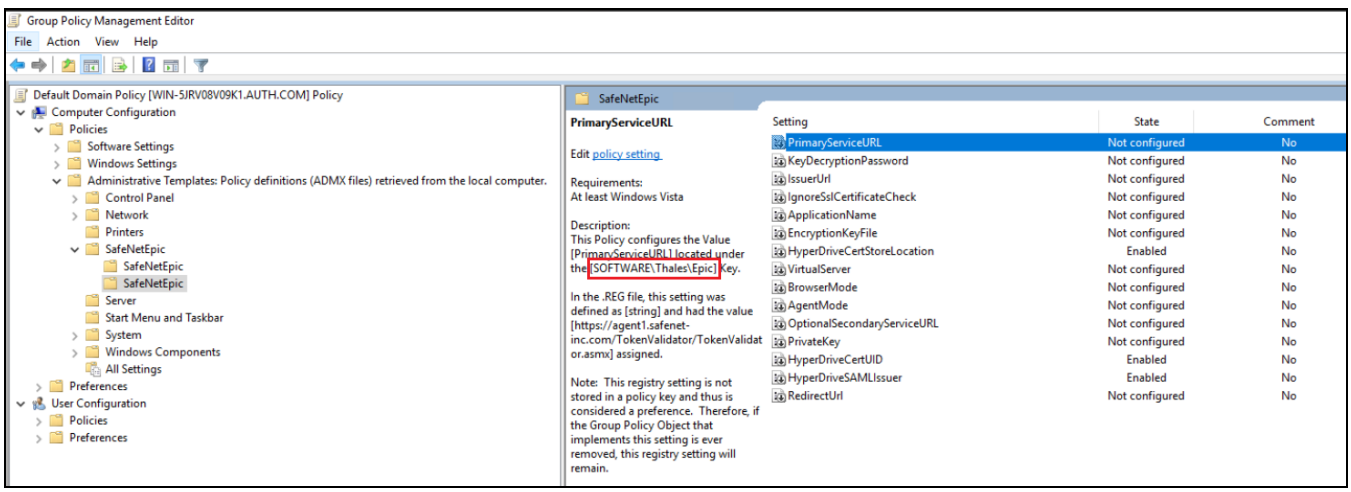
   - To apply the settings to the local machine and any other domain controllers in this domain, under the **Domain Controllers** node, right-click **Default Domain Controllers Policy**.
4. From the dropdown menu, select **Edit**. The **Group Policy Management Editor** window is displayed.
5. In the left pane, navigate to **Computer Configuration** > **Administrative Templates** > **SafeNetEpic** > **SafenetEPIC**.



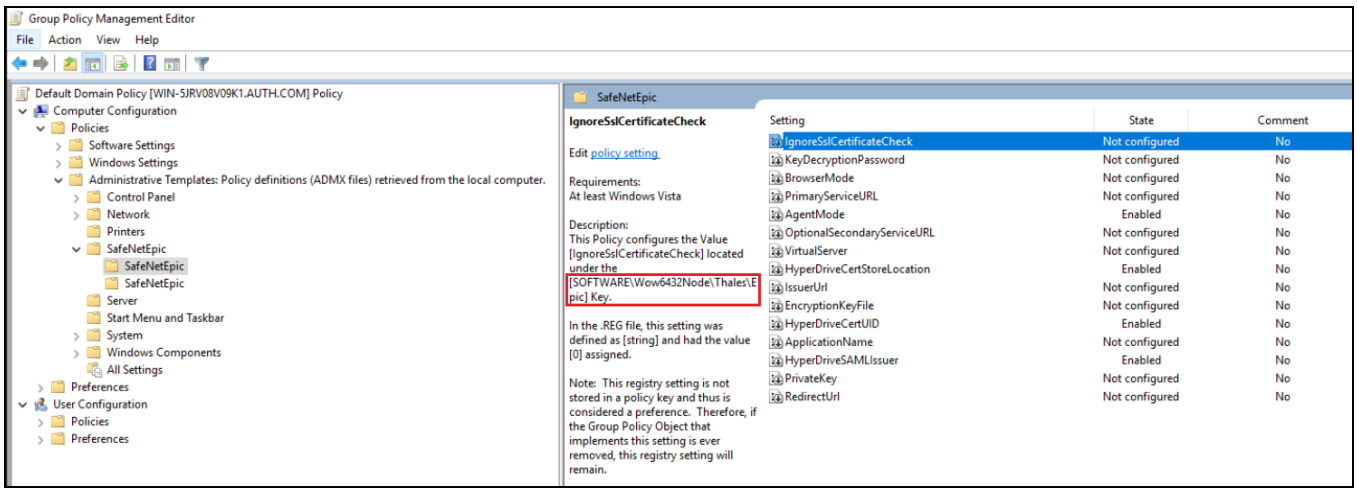
The SafeNet Agent for Epic settings are displayed in the right pane.

6. For performing GPO push:

> **On 32-bit clients**: Configure the settings corresponding to `SOFTWARE\Thales\Epic` and ensure the settings related to 64-bit are set to *Not Configured*.



> **On 64-bit clients**: Configure the settings corresponding to `SOFTWARE\Wow6432Node\Thales\Epic` and ensure the settings related to 32-bit are set to *Not Configured*.



7. Double-click the setting to be edited.
8. Select one of the following, and click **OK**.
   - Not Configured
   - Enabled (Enable the settings which you want to deploy, if not enabled with default value or user-defined value)
   - Disabled

Registry Settings

The following table lists the details of the registry settings:

Setting	Description	Accepted Values	Applicability
AgentMode	The mode in which the agent is used for the authentication purpose.	**1**: for Next Generation mode **0**: for Classic installation	Both Classic and Next Generation modes
ApplicationName	Specifies the application name set in STA (fetched from the .agent file).	For example, **a235e78f-4929-477f-9f60-d203eftg73ce**	Next Generation mode
BrowserMode	Specifies the browser mode to work on for the authentication purpose.	**0** (Default): Embedded browser **1**: Windows default browser (For example, Google Chrome/IE) **NOTE**: It is recommended to use Embedded browser.	Next Generation mode
EncryptionKeyFile	Used to set the key file location.	For example, **C:\Program Files (x86)\Epic\Agent.bsidkey**	Classic mode

Setting	Description	Accepted Values	Applicability
HyperDriveCertStoreLocation	Specifies the certificate store location.	**1**: Current User **2**: Local Machine	Both Classic and Next Generation modes
HyperDriveCertUID	Specifies the certificate's Issuer and Thumbprint in the format (Issuer|Thumbprint).	For example, **CN=epicsafenet.com|K4D4O3C 73D79….BC71FF**	Both Classic and Next Generation modes
HyperDriveSAMLIssuer	Depicts the Entity ID or Unique identifier of the SAML token.	For example, **EpicSafenetIssuer**	Both Classic and Next Generation modes
IgnoreSslCertificateCheck	If selected, the agent will not validate the certificate from the SafeNet server.	**0** (Default): SSL certificate check is enabled **1**: SSL certificate check is disabled	Classic mode
IssuerUrl	Specifies the IssuerUrl of your STA tenant (fetched from the .agent file).	For example, **https://idp.eu.safenetid.com/auth/realms/ SR42FOTLS5-STA**	Next Generation mode
KeyDecryptionPassword	If at the time of bsidkey creation, default password is not used, then this setting is required. Otherwise, always keep it empty.	Its default value is empty.	Classic mode
OptionalSecondaryServiceURL	Used to configure the IP address/hostname of the failover SafeNet server.	For example, **https://cloud.us.safenetid.com/ TokenValidator/TokenValidator.asmx**	Classic mode
PrimaryServiceURL	Used to configure the IP address/hostname of the primary SafeNet server.	For example, **https://cloud.eu.safenetid.com/ TokenValidator/TokenValidator.asmx**	Classic mode

Setting	Description	Accepted Values	Applicability
PrivateKey	Used during the authentication process (fetched from the .agent file).	For example, **-----BEGIN RSA PRIVATE KEY----- MIIEowIBAAdctkVf.....d56x5vnuw ----- END RSA PRIVATE KEY-----**	Next Generation mode
RedirectUrl	Redirect to this URL after authentication (fetched from the .agent file). This is only applicable while using Windows default browser (value:1) as the browser mode.	For example, **http://safenetepicredirecturl/**	Next Generation mode
VirtualServer	The STA virtual server/tenant name where the Epic application is created (fetched from the .agent file).	For example, **ThalesEpicTenant**	Next Generation mode

Deploying the Certificate via GPO

Following are the sample ways for deploying the certificate via GPO. You can use your own certificate deployment workflow.

> **NOTE** This section is only applicable for **Epic Hyperdrive**.

Certificate Guidelines:

1. Ensure that the certificate must have a private key.
2. For improved security, the certificate should be deployed with *non-exportable* private key.
3. In case of local machine certificate, the Epic users should have *read access* to the private key.

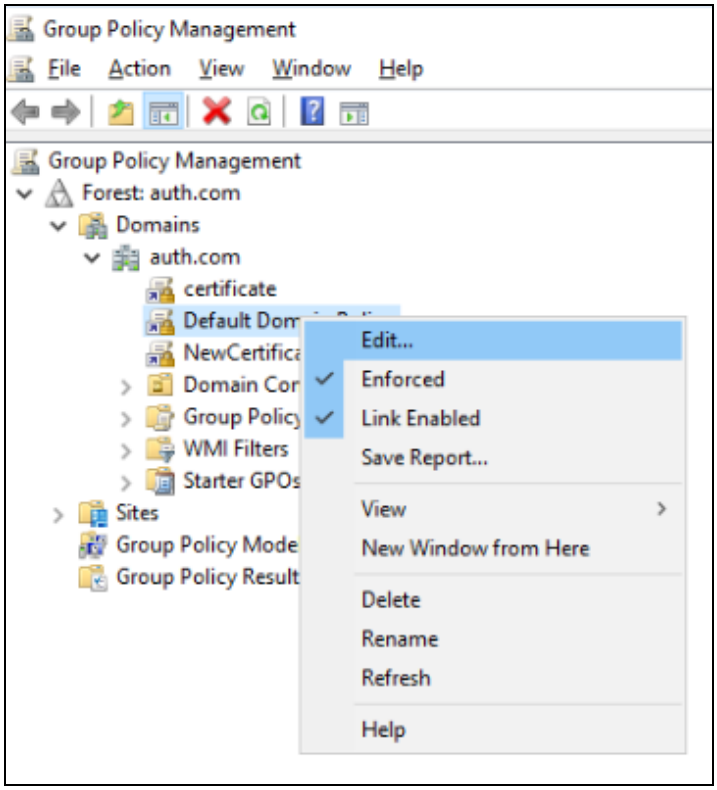
GPO deployment of certificate to a trusted store

To deploy the certificate to a trusted store perform the following steps:

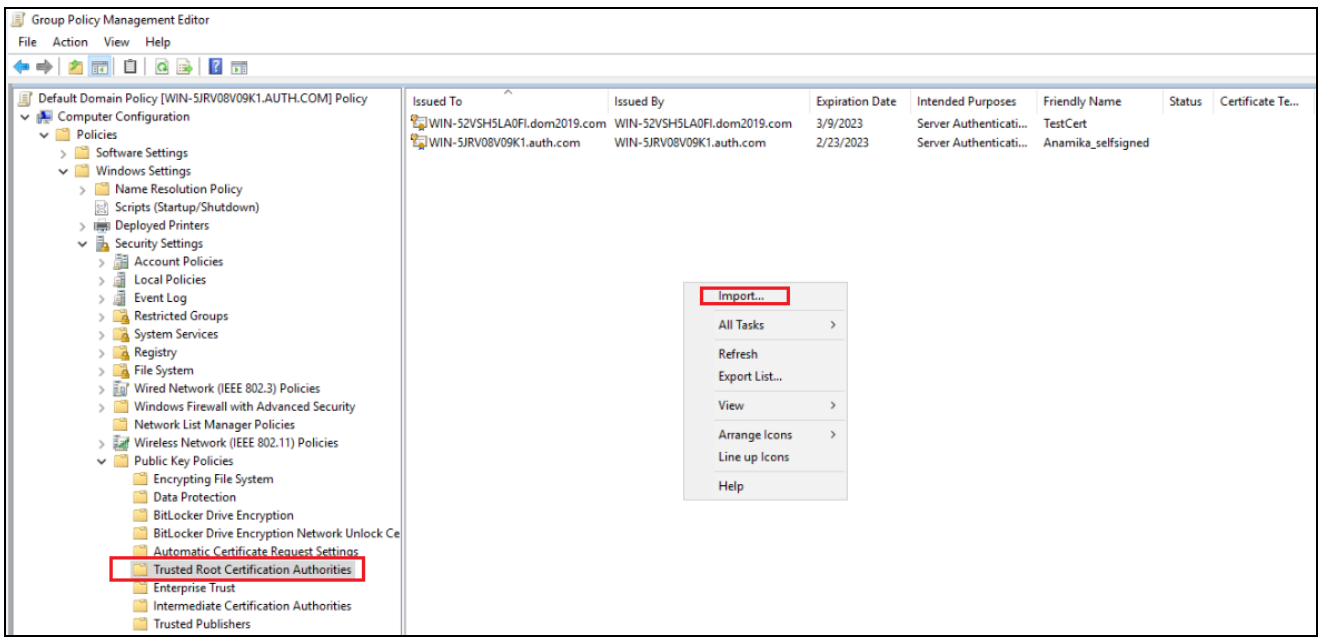
1. From the Windows taskbar, select **Start** > **All Programs** > **Accessories** > **Run**.
2. In the **Run** window, enter *gpmc.msc*, and click **OK**. The **Group Policy Management** window is displayed.
3. Right-click **Default Domain Policy** under the domain node, and click **Edit**.

> **NOTE** Ensure that the GPO is associated with a domain, site, or an organizational unit (OU) where the appropriate user and computer accounts resides.

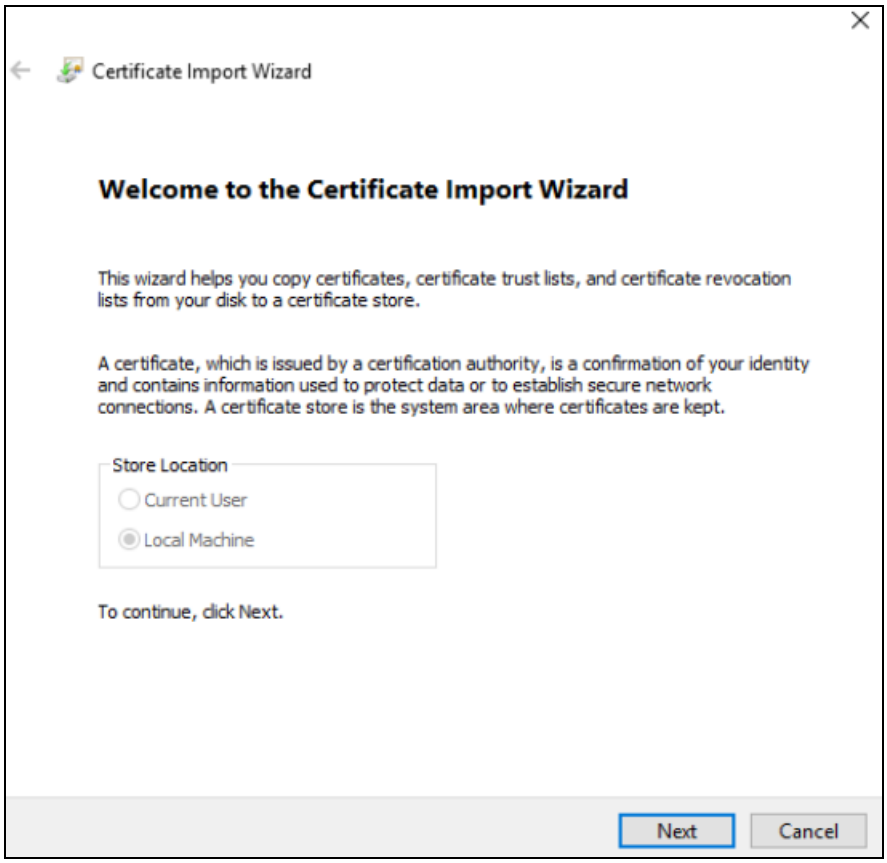
The **Group Policy Management Editor** window is displayed.



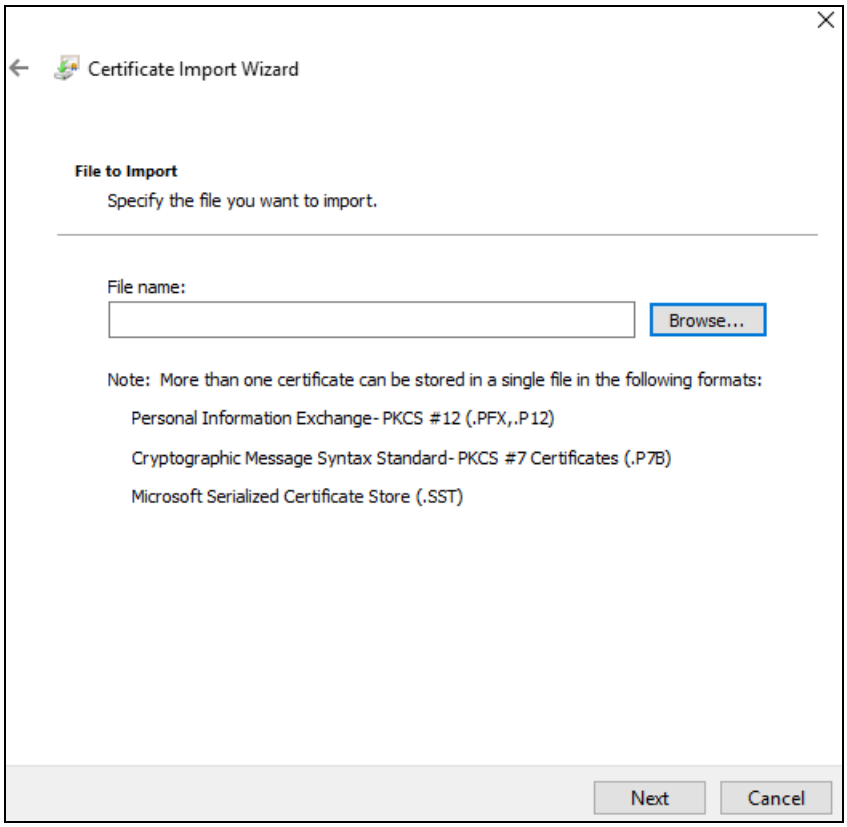
4. In the left pane, navigate to **Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies**, right-click **Trusted Root Certification Authorities**, and then click **Import**.



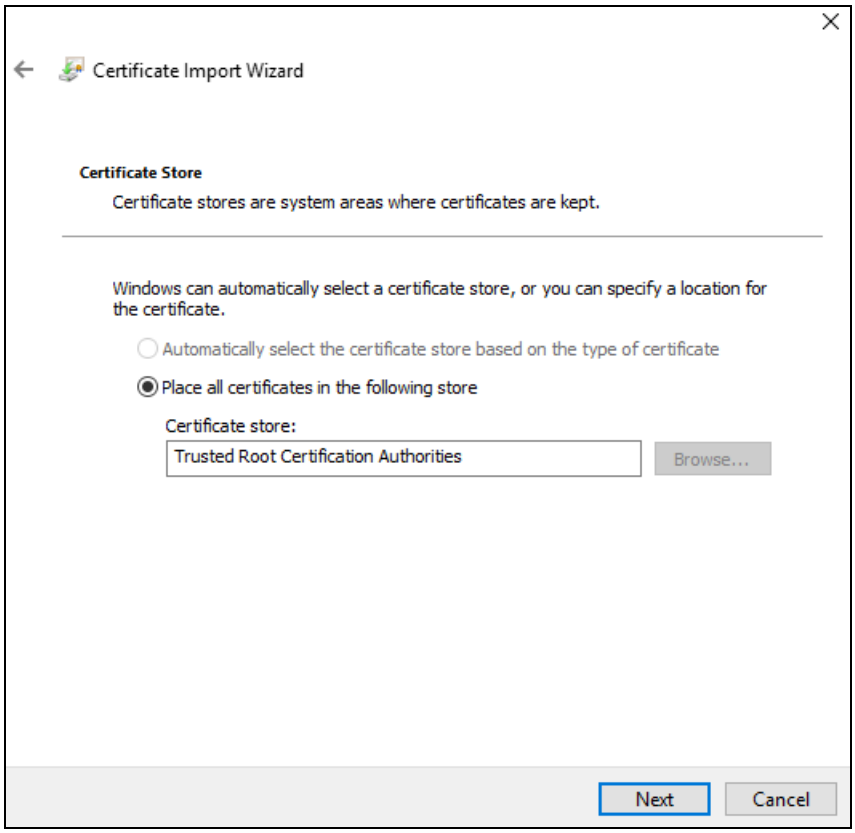
5. On the **Welcome to the Certificate Import Wizard** window, click **Next**.



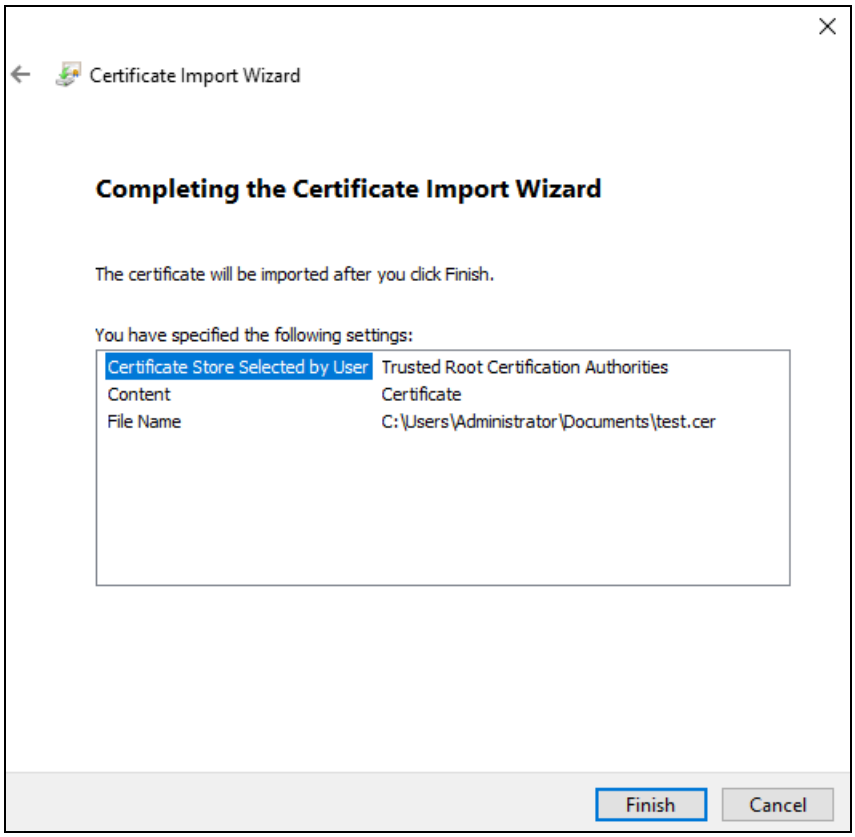
6. On the **File to Import** window, click **Browse** to select the path of certificate file that you have placed in the shared location (for example, \\fs1\c$\fs1.pfx), and then click **Next**.



7. On the **Certificate Store** window, click **Place all certificates in the following store**, and then click **Next**.



8. On the **Completing the Certificate Import Wizard** window, verify that the information you provided is accurate, and then click **Finish**.



9. On the client machine, open the command prompt and run **gpupdate /force**.

Sample script for deploying the certificate to a personal store

Below is the sample script to deploy the certificate to a personal store of local machine with read access on private key:

```
param(
[string]$userorGroupName = "domain\username", //username or groupname
[string]$permission = "read", //Permission to be given on Private key of the certificate
[string]$certStoreLocation ="\LocalMachine\My", //Certificate store location
[string]$certThumbprint = "AF66D91205D80BD547EADF5C1",
[string]$pfxFilePath = "C:\Desktop\share\Cert.pfx", //Expected that the file has been pushed to
the machine
[string]$pfxPassword= "****" //Certificate's password
)
try {
#Convert pfx password to secure string
$password = ConvertTo-SecureString -string $pfxPassword -Force -AsPlainText
#import pfx certificate to a certificate store
Import-PfxCertificate -Password $password -FilePath $pfxFilePath -CertStoreLocation
Cert:$certStoreLocation
#Check if certificate has been successfully installed
$certificateIsInstalled = Get-ChildItem cert:$certStoreLocation | Where thumbprint -eq
$certThumbprint
# Provide read access to a specific user on the installed certificate only
if ($certificateIsInstalled -eq $null)
{
```

```
$message="Certificate with thumbprint:"+$certThumbprint+" does not exist at "+$certStoreLocation
Write-Host $message -ForegroundColor Red
exit 1;
}else
{
$rule = new-object security.accesscontrol.filesystemaccessrule $userorGroupName, $permission,
allow
$root = "c:\programdata\microsoft\crypto\rsa\machinekeys"
$l = ls Cert:$certStoreLocation
$l = $l |? {$_.thumbprint -like $certThumbprint}
$l |%{
$keyname = $_.privatekey.cspkeycontainerinfo.uniquekeycontainername
$p = [io.path]::combine($root, $keyname)
if ([io.file]::exists($p))
{
$acl = get-acl -path $p
$acl.addaccessrule($rule)
#echo $p
set-acl $p $acl
}
}
}
}
catch {
//put your exception here
}
```

CHAPTER 5: Upgrading the SafeNet Agent for Epic

Upgrading the Agent

> **NOTE** Always work in **Run as administrator** mode when installing, uninstalling or upgrading the agent.

The SafeNet Agent for Epic 3.0.5 supports upgrade from version **1.1.0** (or later versions). However, direct upgrade from version **1.1.0** to **3.0.5** is not supported. The administrators needs to:

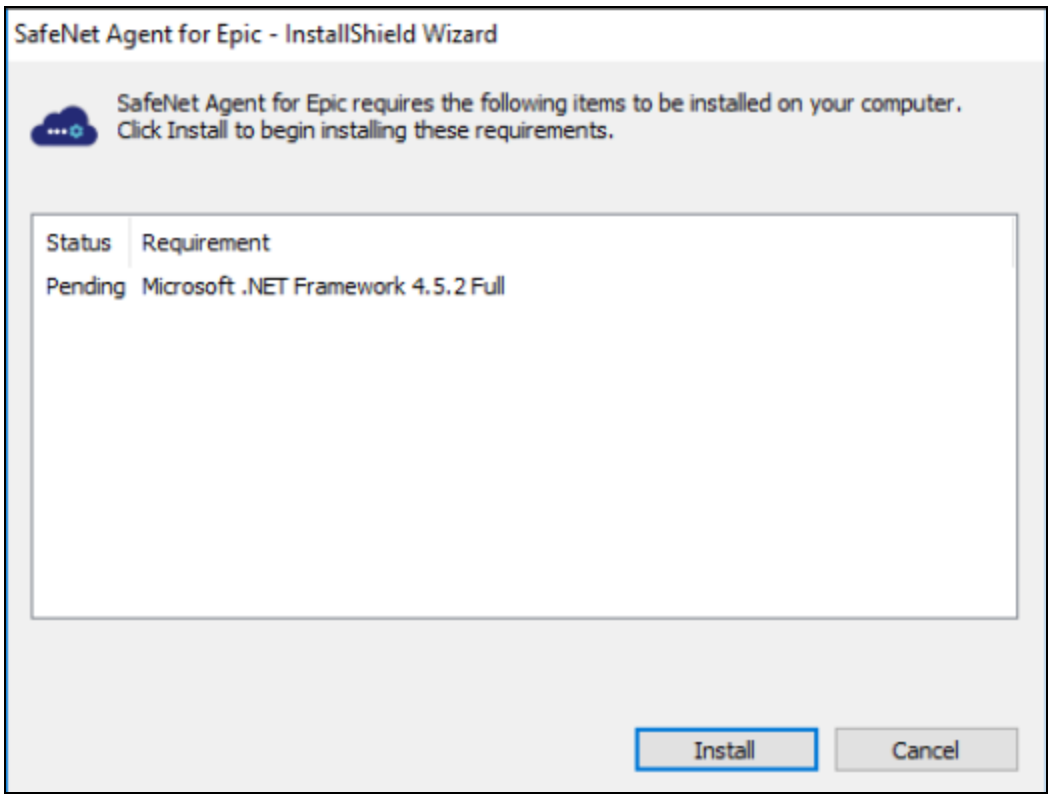
1. Upgrade from version **1.1.0** to version **2.0.1**.
2. Upgrade from version **2.0.1** to version **3.0.5**.

Perform the following steps to upgrade the agent:

1. Double-click and execute the installer (***EXE***). Use ***MSI*** for Group Policy Object (GPO) upgrade.

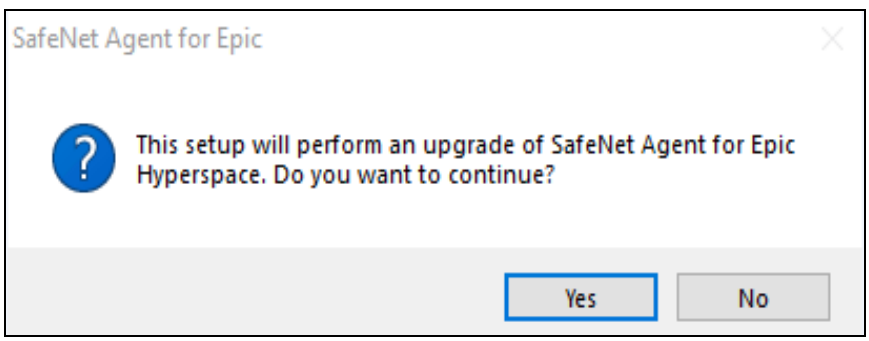
> **NOTE** If a user has logged in to the system as an administrator or if the user(s) is a member of the Domain Admin group, the upgrade process will continue. Otherwise, a window will prompt to provide the administrator credentials.

> The installer will verify if the Microsoft .NET Framework 4.5.2 is installed on the system, or not. If it is not, the following InstallShield Wizard screen will appear, which will guide the user to install the required framework.

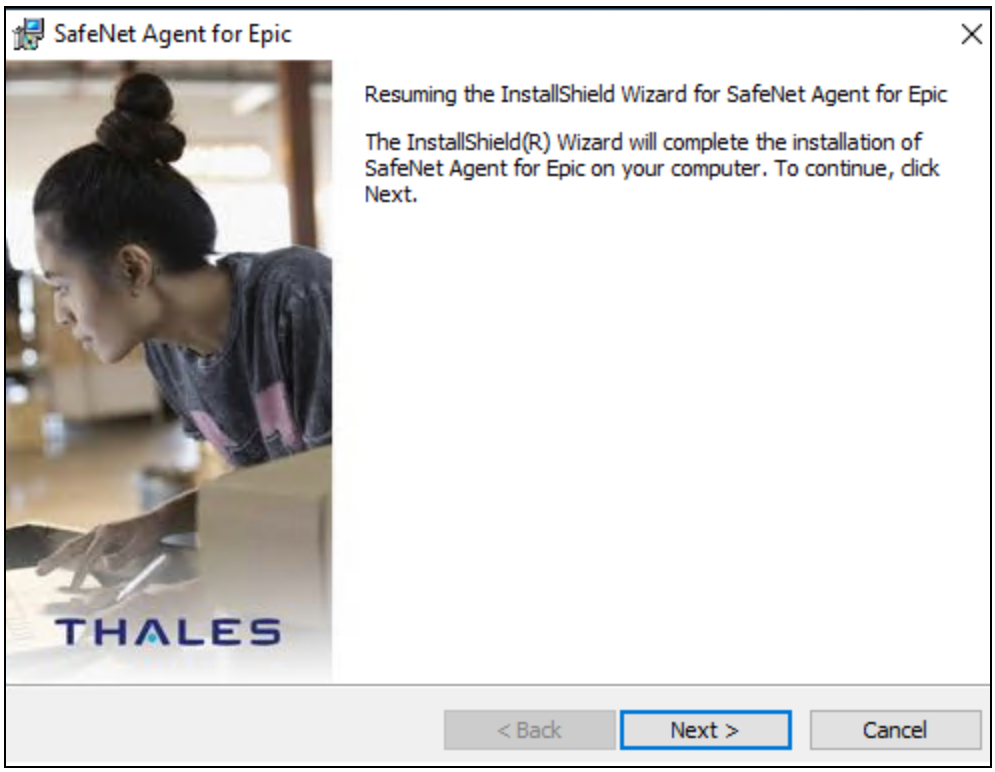


> **NOTE** If the required .NET Framework (4.5.2) is not available during the GPO upgrade, the upgrade process will execute successfully, without any interruptions. In such a case, only when the **Epic Management Console** is opened, an error stating the unavailability of .NET Framework is encountered. To proceed, install Microsoft .NET Framework 4.5.2.

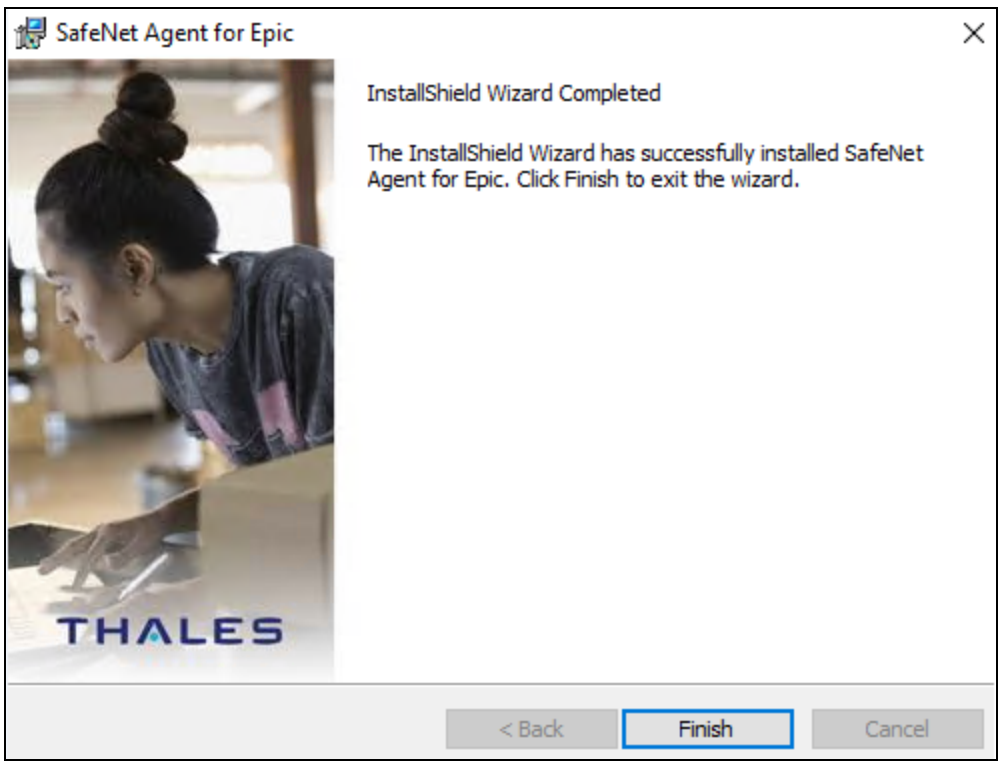
2. If there exists an existing version of the agent, the installer detects it. In case of upgrade from 1.1.0 (and later) to 3.0.5, the installer auto-directs you to the following screen. Click **Yes**.



3. The following **Resuming the InstallShield Wizard for SafeNet Agent for Epic** window is displayed. Click **Next**, and follow the remaining prompts.



4. After the upgrade completes, the **InstallShield Wizard Completed** window is displayed. Click **Finish**.



> **NOTE** If you have created a junction (using mklink) to install the SafeNet Agent for Epic **v1.1.0**, ensure that the junction/ symbolic link should not be removed before, during or after the upgrade process.

Upgrading the Agent Silently

To upgrade the SafeNet Agent for Epic in silent mode, perform the following steps:

1. Open the command prompt in Administrator mode.
2. Navigate to the folder which contains the installer.
3. Execute the following command:

> Using EXE:

```
"SafeNet Agent for Epic.exe" /s /v"/q"
```

> Using MSI:

```
msiexec /i "SafeNet Agent for Epic.msi" /quiet REINSTALLMODE=vomus
REINSTALL=ALL
```

> **NOTE** For major upgrade (using MSI) from v**2.0.1** to the latest version, execute the following command:
> **msiexec /i "SafeNet Agent for Epic.msi" /quiet REINSTALLMODE=vomus UPGRADINGPRODUCTCODE=52D3B65F-73ED-4F75-9BF6-AD93A083CBB5**

> **NOTE** To update settings, the new configuration file needs to be uploaded by opening the **Epic Management Console** > **Communications** and clicking **Browse** displayed against the **Select the config file or the BSID file** field.

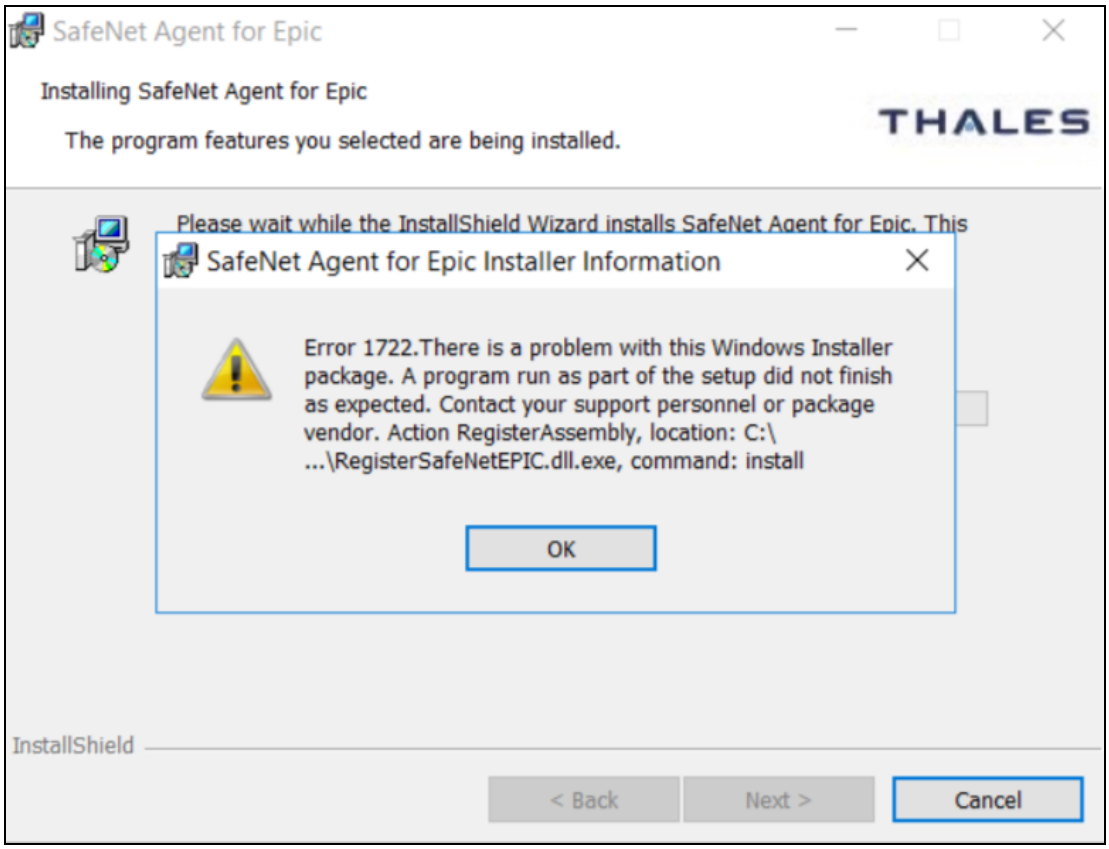
Troubleshooting

This page provides troubleshooting strategies and solutions for the common errors.

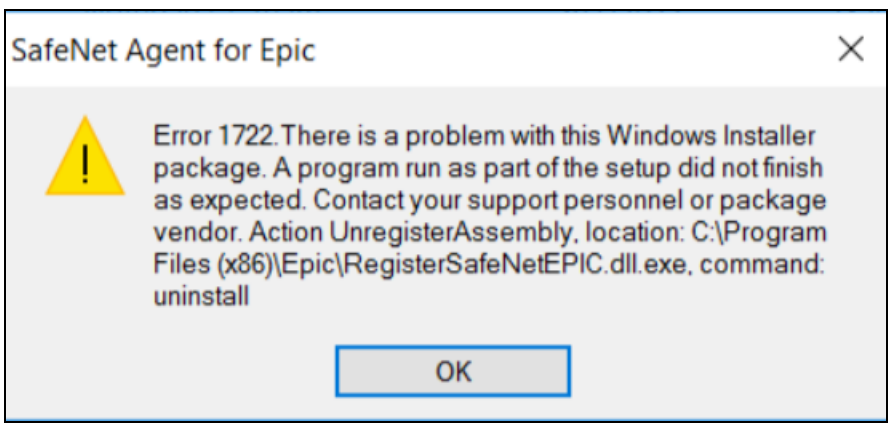
Error: 1722

The following error message displays in the installer window while:

> Installing the agent



> Uninstalling the agent



Possible causes

This error can occur if:

> The **Epic Hyperspace/Hyperdrive application** is not installed / configured properly, which leads to a failure in the **SafeNetEPIC DLL** registration / unregistration.

Solution

> **NOTE** Before proceeding with the below solution, ensure that the **Epic Hyperspace/Hyperdrive application** is present on the agent-installed machine.

Perform the following steps to resolve the issue:

1. Open command prompt as an administrator.
2. Navigate to the agent installation directory. For example,
   - `cd C:\Program Files<x86>\Epic` (for 64-bit operating system)
   - `cd C:\Program File\Epic` (for 32-bit operating system)
3. Now, execute the following command:

> To fix the **Installation** error, register the SafeNetEPIC DLL using:

`RegisterSafeNetEPIC.dll.exe install`

> To fix the **Uninstallation** error, unregister the SafeNetEPIC DLL using:

`RegisterSafeNetEPIC.dll.exe uninstall`